Inhomogeneous Models for Random Graphs and Spreading Processes: Applications in Wireless Sensor Networks and Social Networks

Submitted in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Rashad Eletreby
B.Sc. in Electrical and Computer Engineering
Cairo University, Cairo, Egypt
M.Sc. in Electronic and Computer Engineering
Cairo University, Cairo, Egypt

Carnegie Mellon University
Pittsburgh, PA

September, 2019

For my late father, my mother, and my two wonderful sisters.

Thesis Committee Members

Prof. Osman Yağan (Chair/Advisor)
Department of Electrical and Computer Engineering
Carnegie Mellon University

Prof. Virgil Gligor
Department of Electrical and Computer Engineering
Carnegie Mellon University

Prof. Soummya Kar
Department of Electrical and Computer Engineering
Carnegie Mellon University

Dr. Chai Wah Wu
IBM Research

Acknowledgment

I am extremely grateful to Allah for giving me the strength and courage to pursue this degree and for all the blessings He has bestowed on me.

I am so tremendously thankful to be a student of Prof. Osman Yağan who has been a very supportive adviser, a kind friend, and a superb role model who I look up to. I will never forget his sincere support and encouragement during those moments when I would doubt myself, or feel like I am just not good enough. I wholeheartedly enjoyed working with him and I have always felt safe knowing that he is my adviser.Prof. Yağan is always there for his students and I recall countless occasions when I would stop by his office to seek his advise regarding a difficult research problem, or a pressing personal problem. Without his help and mentorship, this dissertation would not have been possible.

I would like to express my deepest appreciation to my committee members: Prof. Virgil Gligor, Prof. Soummya Kar, and Dr. Chai Wah Wu for reading my thesis, taking part in my PhD dissertation defense committee, and providing me with valuable comments and suggestions.

I had great pleasure working with Prof. Swarun Kumar and Diana Zhang during my second year at Carnegie Mellon University. I am wholeheartedly thankful for their tremendous help and support.

I would like to extend my sincere thanks to Vivek Jain, Sushanta Rakshit, and Christoph Lang for the great time I had at Bosch CR/RTC4.1-NA during my summer internship in 2018.

I had great pleasure working with Prof. Marwan Krunz, Mohamed Abdelrahman, Wessam Afifi, Hanif Rahbari, Berk Akgün, and Peyman Siyari during the year I have spent at the University of Arizona.

I am wholeheartedly grateful to my late father Mohamed, my mother Soad, and my two wonderful sisters Rasha (and her husband Ayman) and Rania (and her husband Sherif). They are the reason behind this achievement. Their unconditional love, support, and empowerment have led me to where I am today. I am deeply indebted to them and I will always strive to make them proud. Special thanks to my adorable nephew Mohamed and my three beautiful nieces Youmna, Nada, and Nadine.

I am extremely grateful to the members of my research group at Carnegie Mellon University, Yong Zhuang, Yingrui Zhang, Samarth Gupta, Mansi Sood, and Vaibhav for being great friends and for their support and encouragement. I have also had much fun being one of A-level dwellers at Hamerschlag Hall. I would like to thank Jiyuan Zhang, Guanglin Xu, Doru Thom Popovici, John Filleau, Daniele Spampinato, Ke Wang, Marie Nguyen, Mark Blanco, and Elliot Binder for being such great friends at A-level.

I have been very fortunate to meet many wonderful friends throughout my five years in the US so far. In Pittsburgh: Amr Mahmoud, Mohamed Zaghloul, Mahmoud Ayyad, Khaled Elsayed, Ahmed Ezzat, Yassin Khalifa, Hoda Elbanna, Aya Fawzy, Yasmine Safwat, Büşra Susam, Mazen Soliman, and Mohamed Darwish. In California: Jacqueline Thurston, Amr Essawi, Mamdouh Nassr, Mahmoud Sawaby, Zina Jawadi, Ahmed Eissa, Mohamed Othman, Ahmed Wahba, Belal Salama, and Amr Youssef. In Arizona: Wessam Afifi, Ture Peken, Joe Dupris, Çica Prado, and Peter DuBois. I apologize to all of the friends that I have inadvertently left out who made my graduate study memorable.

Last but not least, I would like to thank my childhood friends who have always been supportive throughout my PhD journey: Ahmed Eldemerdash, Islam Soliman, Hossam Salem, Mohamed Eman, Mohamed Sedky, Mohamed Emad, Mostafa Elredewy, Abdelaziz Saber, Mamdouh Shaaban, and Sherif Anwar.

The work presented in this thesis has been supported in part by National Science Foundation through grant CCF #1617934 and in part by the Army Research Office through grant Number W911NF-17-1-0587. R. Eletreby was funded (in part) by the Dowd Fellowship from the College of Engineering at Carnegie Mellon University. The authors would like to thank Philip and Marsha Dowd for their financial support and encouragement.

Abstract

Random graphs are of great interest as a modeling framework for a wide variety of real-world complex networks, such as social networks, information networks, scientific collaboration networks, and technological networks. In this thesis, we focus on two specific application areas of random graph theory, namely, i) modeling secure connectivity of large-scale wireless sensor networks utilizing random predistribution of cryptographic keys, and ii) modeling real-world social networks. Although these two areas are tied together with random graphs, they are inherently different and each one poses distinct research problems that rise naturally in the corresponding context. Hence, we will tackle each of them separately and focus on the relevant research problems in each area.

In the first part of the thesis, we focus on the role of random graphs in providing a modeling framework for secure connectivity of large-scale, *heterogeneous* wireless sensor networks utilizing random predistribution of cryptographic keys. In this part, we propose a novel composite random graph obtained by the intersection of *inhomogeneous* random key graphs with Erdős-Rényi graphs as a model for a large scale wireless sensor network secured by the heterogeneous random key predistribution scheme under a *uniform* on-off channel model. We derive scaling conditions on the model parameters so that with high probability i) the network has no isolated nodes, ii) is connected, iii) the minimum node degree is no less than k, and iv) the network is k-connected. We then proceed by generalizing the uniform on-off channel model to a *heterogeneous* on-off channel model where the wireless link availability between two nodes is determined based on their respective classes. This induces a novel composite random graph model formed by the intersection of *inhomogeneous* random key graphs with *inhomogeneous* Erdős-Rényi graphs. We derive scaling conditions on the model parameters such that with high probability i) the network has no isolated nodes, and ii) is connected. We close this part by proposing *inhomogeneous* random K-out graphs as a novel modeling framework for secure connectivity of large-scale, *heterogeneous* wireless sensor networks utilizing *random pairwise* *key predistribution schemes*. We derive scaling conditions on the model parameters such that with high probability the resulting network is connected.

In the second part of the thesis, we look at random graphs as models for real-world social networks. In contrast to the first part where we mainly focus on proposing novel random graph models, herein, we utilize existing random graph models of social networks to understand how infectious diseases (or, information) that entail evolutionary adaptations propagate in social contexts. In particular, we consider the propagation of *inhomogeneous* spreading processes, governed by the multiple-strain model, on contact networks modeled by i) random graphs with arbitrary degree distributions (generated by the configuration model) and ii) random graphs with clustering. The former graphs capture the skewed degree sequences observed in real-world social networks, yet it has a vanishing clustering coefficient in the limit of large network size. The latter model generalizes the former as it could also generate graphs with non-trivial clustering, hence, it resembles real-world social networks that are typically clustered. We start by investigating the propagation of spreading processes governed by the multiple-strain model on random graphs with arbitrary degree distributions. We propose a mathematical theory that characterizes the expected epidemic size and the epidemic threshold as functions of the structure of the underlying contact network, the properties of the spreading process, and the evolutionary pathways of the propagating object. We also present extensive simulation results on synthetic and real-world contact networks to validate our theory and reveal the significant shortcomings of the classical epidemic models that do not capture evolutionary adaptations. We then investigate the propagation of the same class of spreading processes, yet on random graphs with clustering. We propose a mathematical theory that accurately captures the probability of emergence (the probability that the spreading process would eventually reach a positive fraction of the nodes) and the epidemic threshold as functions of the structure of the underlying contact network (which takes clustering into consideration), the properties of the spreading process, and the evolutionary pathways of the propagating object. Our theoretical results are validated by a simulation study that also reveals the impact of clustering on the probability of emergence and the epidemic threshold.

A common takeaway from both parts of the thesis is that **homogeneous models are more resource-efficient than their inhomogeneous counterparts**, despite the fact that the latter facilitate a broader modeling framework that accurately captures real-world networks and spreading processes. In particular, in the first part of the thesis, we show that in some cases, inhomogeneous random graph models require orders of magnitude more resources (e.g., number of cryptographic keys per sensor node) than their homogeneous counterparts to be connected with high probability. In addition, in the second part of the thesis, we show that inhomogeneous models for spreading processes entailing evolutionary adaptations (on random graphs with arbitrary degree distribution) could achieve (depending on the initial strain) a lower probability of emergence at a given mean degree as compared to a homogeneous spreading process without evolution.

Contents

List of Figures

List of Tables

Part I

Introduction

Chapter 1

An outline of the thesis

Random graphs are of great interest as a modeling framework for a wide class of real-world complex networks including social networks, information networks, scientific collaboration networks, and biological networks [17, 64, 116]. The study of *random graphs* dates back to 1959 when Paul Erdős and Alfred Rényi [52] introduced the random graph model $\mathbb{G}(n; M)$, as a graph selected uniformly at random from the collection of all graphs with n nodes and M edges. Contemporaneously and independently, Gilbert [59] introduced the random graph model $\mathbb{G}(n; p)$, where each pair of vertices is connected (respectively, not connected) by an edge independently with probability p (respectively, $1 - p$). The pioneering works of Gilbert, Erdős, and Rényi lie at the heart of random graph theory and represent the first endeavor to study random graphs in their own right.

Since their inception, random graphs have received much attention across multiple research domains due to several factors. One factor of particular interest to this thesis is the role of random graphs in *modeling* real-world complex networks. For instance, *random graphs with arbitrary degree distribution* (generated by the configuration model [100, 115]) provide a modeling framework that accurately captures degree sequences observed in real-world complex networks, e.g., social networks which are characterized by their heavy-tailed degree distribution [12, 14, 40]. In addition, *random key graphs* were shown to provide an accurate modeling framework for large-scale wireless sensor networks that utilize random predistribution of cryptographic keys in order to secure communications. *Random geometric graphs* [121] can also be used to model proximity-based social networks, or the connectivity of wireless ad-hoc networks where two nodes could establish communication if they are within range of one another [68].

In addition to their roles in modeling the *structure* of real-world complex networks, random graphs offer a tractable mathematical framework that paves the way for investigating the characteristics of spreading processes, such as information or infectious diseases, in real-world contact networks. For instance, modeling real-world contact networks by random graphs with arbitrary degree distribution (generated by the configuration model) allows the investigation of several key properties of the underlying spreading process, such as its expected epidemic size and probability of emergence, owing to the locally tree-like property of these graphs [61, 115].

In this thesis, we focus on two specific application areas of random graph theory, namely, i) modeling secure connectivity of large-scale wireless sensor networks utilizing random predistribution of cryptographic keys, and ii) modeling real-world social networks. Although these two areas are tied together with random graphs, they are inherently different and each one poses distinct research problems that rise naturally in the corresponding context. Hence, we will tackle each of them separately and focus on relevant research problems in each area. In particular, this thesis is composed of two parts, with each part entirely dedicated to one of the above application areas. As will become apparent soon, there are common takeaways from both parts, albeit being distinct. The structure of the thesis is depicted in Figure 1.1.

In the first part of the thesis, we focus on the role of random graphs in providing a modeling framework for secure connectivity of large-scale wireless sensor networks utilizing random predistribution of cryptographic keys. In this part, our objective is to propose novel *inhomogeneous* random graphs that accurately model the secure connectivity of large-scale, *heterogeneous* wireless sensor networks. In particular, we propose a novel composite random graph obtained by the intersection of *inhomogeneous* random key graphs with Erdős-Rényi graphs as a model for a large scale wireless sensor network secured by the heterogeneous random key predistribution scheme under a *uniform* on-off channel model. We derive scaling conditions on the model parameters so that with high probability i) the network has no isolated nodes, ii) is connected, iii) the minimum node degree is no less than k, and iv) the network is k-connected.

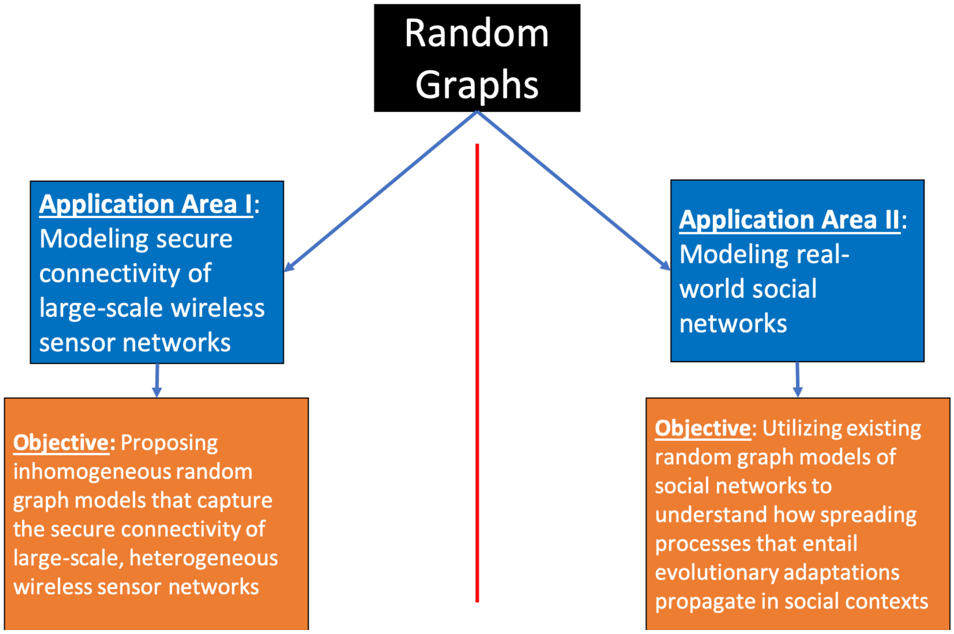

Random Graphs
Application Area I: Modeling secure connectivity of large-scale wireless sensor networks
Application Area II: Modeling real-world social networks
Objective: Proposing inhomogeneous random graph models that capture the secure connectivity of large-scale, heterogeneous wireless sensor networks
Objective: Utilizing existing random graph models of social networks to understand how spreading processes that entail evolutionary adaptations propagate in social contexts

Figure 1.1: In this thesis, we focus on two specific application areas of random graphs, with a different objective associated with each application area.

We then proceed by generalizing the uniform on-off channel model to a *heterogeneous* on-off channel model where the wireless link availability between two nodes is determined based on their respective classes. This induces a novel composite random graph model formed by the intersection of *inhomogeneous* random key graphs with *inhomogeneous* Erdős-Rényi graphs. We derive scaling conditions on the model parameters such that with high probability i) the network has no isolated nodes, and ii) is connected.

We close this part by proposing *inhomogeneous* random K-out graphs as a novel modeling framework for secure connectivity of large-scale, *heterogeneous* wireless sensor networks utilizing *random pairwise key predistribution schemes*. We derive scaling conditions on the model parameters such that with high probability the resulting network is connected.

As will become apparent soon, the scaling conditions derived for the proposed random graph models directly map to conditions on the parameters of the underlying random key predistribution scheme so that the resulting wireless sensor network exhibits a desired property, such as being connected. Since our results are typically presented in the form of *sharp* zero-one laws, they provide a precise threshold for the model parameters, allowing for efficient design of the underlying key predistribution scheme.

In the second part of the thesis, we look at random graphs as models for real-world social networks. In contrast to the first part where we mainly focus on proposing novel random graph models, herein, we utilize existing random graph models of social networks to understand how infectious diseases (or, information) that entail evolutionary adaptations propagate in social contexts. In particular, we consider the propagation of *inhomogeneous* spreading processes, governed by the multiple-strain model on contact networks modeled by i) random graphs with arbitrary degree distributions (generated by the configuration model) and ii) random graphs with clustering. The former graphs capture the skewed degree sequences observed in real-world social networks, yet they have a vanishing clustering coefficient in the limit of large network size. The latter model generalizes the former as it could also generate graphs with non-trivial clustering, hence, it resembles real-world social networks that are typically clustered.

We start by investigating the propagation of spreading processes governed by the multiple-strain model on random graphs with arbitrary degree distributions. We propose a mathematical theory that characterizes the expected epidemic size and the epidemic threshold as functions of the structure of the underlying contact network, the properties of the spreading process, and the evolutionary pathways of the propagating object. We also present extensive simulation results on synthetic and real-world contact networks to validate our theory and reveal the significant shortcomings of the classical epidemic models that do not capture evolutionary adaptations. We close this part by investigating the case where co-infection with multiple pathogen/information strains is possible and show that co-infection could lead the order of phase transition to change from *second-order* to *first-order*.

We then investigate the propagation of the same class of spreading processes, yet on random graphs with clustering. We propose a mathematical theory that accurately captures the probability of emergence (the probability that the spreading process would eventually reach a positive fraction of the nodes) and the epidemic threshold as functions of the structure of the underlying contact network (which takes clustering into consideration), the properties of the spreading process, and the evolutionary pathways of the propagating object. Our theoretical results are validated by a simulation study that also reveals the impact of clustering on the probability of emergence and the epidemic threshold.

A common takeaway from both parts is that **homogeneous models are more resource-efficient than their inhomogeneous counterparts**, despite the fact that the latter facilitate a broader modeling framework that accurately captures real-world networks and spreading processes. In particular, in the first part of the thesis, we show that in some cases, inhomogeneous random graph models require orders of magnitude more resources (e.g., number of cryptographic keys per sensor node) than their homogeneous counterparts to be connected with high probability. In addition, in the second part of the thesis, we show that inhomogeneous models for spreading processes entailing evolutionary adaptations (on random graphs with arbitrary degree distribution) could achieve (depending on the initial strain) a lower probability of emergence (the probability that the spreading process would eventually reach a positive fraction of the nodes) at a given mean degree as compared to a homogeneous spreading process without evolution.

Chapter 2

Application Area I: Modeling secure connectivity of large-scale wireless sensor networks

The proliferation of wireless sensor networks in multiple application domains, such as military applications, health care monitoring, among others, is attributed to their unique characteristics, such as their versatility, small-size, low-cost, ease of use, and scalability [2, 92, 161]. These features, however, give rise to unique security challenges that render wireless sensor networks vulnerable to a variety of security threats such as node capture attacks, node replication attacks, and eavesdropping [142]. Indeed, power-hungry cryptosystems such as *asymmetric* cryptosystems (public-key) are infeasible for securing large-scale wireless sensor networks that typically consist of battery-powered nodes with simple computation and communication architectures [24, 53, 88, 134]. Accordingly, *symmetric* cryptosystems were shown to offer a faster and more energy-efficient alternative than their asymmetric counterpart, and they are deemed as the most feasible choice for securing wireless sensor networks [24, 53].

One key question associated with the use of symmetric cryptosystems is the design of key distribution mechanisms that facilitate the establishment of a secure communication infrastructure upon deploying the network and throughout its operation [24, 37]. These mechanisms shall i) be fully distributed to avoid relying on any third party or a base station, ii) not assume any prior knowledge of post-deployment configuration, and iii) obey the hardware limitations of wireless sensor networks. Additionally, the resulting network shall be securely *connected* in a sense that there exists a secure communication path (not necessarily single-hop) between any pair of sensor nodes. The connectivity of the network is essential to its proper operation as it allows the exchange of control and data messages between any pair of sensor nodes.

Random key predistribution schemes were proposed in the seminal work of Eschenauer and Gligor [53] to provide a feasible solution for key distribution in large-scale wireless sensor networks utilizing symmetric cryptosystems. In Eschenauer-Gligor scheme, each sensor node is assigned (before deployment) K cryptographic keys selected uniformly at random from a large key pool of size P. After deployment, two sensor nodes can communicate securely over an existing wireless channel if they share at least one key. The scheme does not require any prior knowledge of post deployment configuration and the communication infrastructure could be bootstrapped in a fully distributed manner. The resulting notion of adjacency under full visibility case (when all wireless channels are available and reliable, hence the only condition for two nodes to be adjacent is to share a cryptographic key) induces *random key graphs*, denoted $\mathbb{K}(n; K, P)$, on the vertex set $\{1, \ldots, n\}$ where n is the number of sensor nodes.

Random key graphs $\mathbb{K}(n; K, P)$ are constructed as follows. Given the set $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ of n vertices, and an object pool of size P, each vertex v_i is assigned a set Σ_i of K objects selected uniformly at random (without replacement) from the object pool. Two nodes v_x and v_y are said to be adjacent if $\Sigma_x \cap \Sigma_y \neq \emptyset$. Random key graphs provide a modeling framework that enables the investigation of key design questions related to Eschenauer-Gligor scheme. For example, how to choose the parameters of the scheme to ensure that the resulting network is *securely connected* [159]. If the resulting network is securely connected, then there exists a secure communication path between every pair of sensors. This secure path allows the exchange of *control* and *data* messages between participating nodes [80].

Eschenauer and Gligor scheme paved the way for several other random key predistribution schemes, including *random pairwise key predistribution scheme* proposed by Chan et al [24]. The random pairwise key predistribution scheme operates as follows. Each of the n sensor nodes is paired (offline) with K distinct nodes which are randomly selected from among all other nodes. If nodes i and j were paired during the node-pairing stage, a unique (pairwise) key is generated and stored in the memory modules of each of the paired sensors together with both their IDs. After deployment, a secure link can be established between two communicating nodes if they have at least one pairwise key in common. Under full visibility, the random pairwise key predistribution scheme induces the *random K-out graph*, denoted $\mathbb{H}(n;K)$, on the vertex set $\{1,\ldots,n\}$ where n is the number of sensor nodes.

Random K-out graphs $\mathbb{H}(n;K)$ are constructed on the vertex set $\mathcal{V}=\{1,2,\ldots,n\}$ as follows. Each node v selects K distinct nodes uniformly at random from $\mathcal{V}\setminus\{v\}$ without replacement. An *undirected* edge is assigned between nodes u and v if u selects v or v selects u, or both; see [152] for details. Similar to the case with Eschenauer-Gligor scheme, the modeling framework provided by random K-out graphs paves the way for investigating the relationship between the parameters of random pairwise key predistribution scheme, namely the number of choices K, and the secure connectivity of the resulting network [152]. In addition to modeling secure connectivity of wireless sensor networks, a structure similar to random K-out graphs was recently suggested by Fanti et al. [54, Algorithm 1] to provide anonymity guarantees for transactions over cryptocurrency networks.

2.1 Inhomogeneous random graphs as models for heterogeneous wireless sensor networks

A common property among the aforementioned random graph models is their inherent *homogeneity*, characterized by a uniform treatment of all vertices which leads to a homogeneous degree distribution. For instance, each vertex is given the same number of objects in random key graphs, or picks the same number of nodes to be paired to in random K-out graphs. However, real-world complex networks and emerging real-world applications are fundamentally complex and heterogeneous [13, 17], inducing the need for *inhomogeneous* variants of these classical random graph models. In fact, the literature on random graphs is already shifting towards inhomogeneous models initiated by the seminal work of Bollobás et al. on inhomogeneous

Erdős-Reńyi graph [19] (see also [32]).

Emerging wireless sensor networks represent a pronounced example of heterogeneous networks that no longer fit the homogeneous modeling framework provided by the aforementioned random graph models. In fact, many commercial and military applications are envisioned to consist of heterogeneous nodes [38, 91, 148, 150]. Namely, it is expected that participating sensors will have varying level of resources (for communication, computation, storage, power, etc.) and possibly a varying level of security and connectivity requirements. Hence, it may be reasonable to assign more keys to mission-critical nodes to enhance their connectivity and increase their robustness.

2.2 Inhomogeneous random key graphs

In [157], Yağan proposed a new variation of Eschenauer and Gligor scheme, referred to as the *heterogeneous* random key predistribution scheme to tackle the aforementioned class of heterogeneous networks. The scheme is described as follows. Given r classes, each sensor is independently classified as a class-i node with probability $\mu_i > 0$ for each $i = 1, \ldots, r$ such that $\sum_{i=1}^{r} \mu_i = 1$. Then, sensors in class-i are each assigned K_i keys selected uniformly at random from a key pool of size P. Similar to Eschenauer and Gligor scheme, nodes that share key(s) can communicate securely over an available channel after the deployment.

Under full visibility, the *heterogeneous* random key predistribution scheme gives rise to a class of *inhomogeneous* random graphs referred to as *inhomogeneous random key graphs* $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ in [157] (this model is also known in the literature as the *general random intersection graph*; e.g., see [16, 62, 167]). These random graphs are constructed as follows. Given the set $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ of n vertices, and a key pool of size P, each node is assigned to one of r possible classes according to a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for each $i = 1, \ldots, r$ and $\sum_{i=1}^{r} \mu_i = 1$ where r is a fixed integer that does not scale with n. A class-i node selects K_i objects uniformly at random from an object pool of size P. Without loss of generality, it is assumed that $K_1 \leq K_2 \leq \ldots \leq K_r$. As with classical random key graphs, two nodes are said to be adjacent if they have at least one object in common. In [157], Yağan investigated the connectivity of inhomogeneous random key graphs under full visibility. In particular, the analysis given in [157] provides guidelines on how to choose the parameters of the heterogeneous random key predistribution scheme such that the resulting network is securely connected under full visibility.

Note that edges in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ represent pairs of sensors that share at least one cryptographic key, hence the model only encodes *shared-key* connectivity. In other words, it is assumed that all wireless channels are available and reliable, hence the only condition for two nodes to communicate securely is to share a cryptographic key. In practice, the wireless channel is often unreliable and sensor nodes typically have limited communication ranges, hence, two sensor nodes which share a key may not eventually be adjacent due to the unavailability of their corresponding wireless channel. Accordingly, the secure connectivity of the network would not only be governed by the shared-key connectivity discussed above, but also by the wireless connectivity. As a result, the scaling conditions given in [157] would be too optimistic for real-world deployments characterized by unreliable wireless media.

2.3 Thesis contributions I

In this thesis, we aim to extend the results given by Yağan in [157] by modeling the wireless connectivity of the network using an appropriate random graph model $\mathbb{I}(n; \cdot)$, whose edges represent pairs of sensors which have a wireless communication channel available in between. The overall model of the network will then be an intersection of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ and $\mathbb{I}(n; \cdot)$ since a pair of sensors can establish a *secure communication link* if they share a key *and* have a wireless channel available. A good candidate to model the wireless connectivity of a wireless sensor network would be the disk model [68]: Assuming that nodes are distributed over a bounded region $\mathcal{D}$ of a euclidean plane, nodes v_i and v_j located at $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$, respectively, are able to communicate if $\|\boldsymbol{x}_i - \boldsymbol{x}_j\| < \rho$, where ρ denotes the transmission radius. The case when node locations are independently and uniformly distributed over the region $\mathcal{D}$ induces the random geometric graph [121], hereafter denoted $\mathbb{I}(n;\rho)$.

Consider a *composite* random graph obtained by intersecting inhomogeneous random key graphs with random geometric graphs, namely, $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{I}(n;\rho)$. Indeed, the resulting random graph represents an accurate model for a wireless sensor network secured by the heterogeneous random key predistribution scheme, where two nodes are adjacent only if they share a key *and* are within the transmission radius of each other. Unfortunately, analyzing the connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{I}(n;\rho)$ is likely to be very challenging [156]. For example, despite many attempts, the Gupta-Kumar conjecture [68] on the connectivity of $\mathbb{G}(n;\alpha)\cap\mathbb{I}(n;\rho)$ where $\mathbb{G}(n;\alpha)$ represents an Erdős-Rényi graph, has remained unsolved until very recently by Penrose [122]; see [156] for a detailed discussion on the difficulties involved in analyzing the *intersection* of different types of graphs.

The preceding discussion brings about a crucial question, namely, *is there any communication model that provides a good approximation of the classical disk model, but also allows a comprehensive analysis of the resulting composite random graph?* This question was answered in the affirmative in [152, 156], where it was shown that an independent on-off channel model – represented by an Erdős-Rényi graph $\mathbb{G}(n;\alpha)$ – provides a good approximation of the disk model in settings similar to those considered here.

Inspired by the success in these previous approaches, here we also model the wireless communication connectivity of the wireless sensor network by an Erdős-Rényi graph $\mathbb{G}(n;\alpha)$ and investigate key properties of the intersection model $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$. As soon will become apparent, this approach paves the way for i) establishing rigorous results concerning key properties of the intersection model and ii) demonstrating via simulations that these results still appear to apply under the more realistic disk model. In particular, simulation results indicate that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{I}(n;\rho)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ behave similarly with respect to the properties of interest, when α and ρ are *matched* to lead to the same probability of wireless channel availability.

A summary of the results we establish for the composite random graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap$

$\mathbb{G}(n;\alpha)$ is given below.

- A zero-one law for the absence of isolated nodes in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ [47,50].
- A zero-one law for the connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ [47,50].
- A zero-one law for the minimum node degree of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ being no less than k [42,44].
- A zero-one law for the k-connectivity[1] of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ [42,45].

The aforementioned theoretical results are all obtained in the asymptotic regime when the number of nodes tends to infinity, yet they are also supported by simulation studies demonstrating that i) despite their asymptotic nature, they are in fact useful in designing *finite*-node wireless sensor networks so that they achieve secure connectivity with high probability; and ii) despite the simplicity of the on-off communication model, the probability of connectivity in the resulting wireless sensor network approximates very well the case where the disk model is used.

We then proceed by investigating the connectivity of wireless sensor networks secured by the heterogeneous random key predistribution scheme under a *heterogeneous* on-off channel model. In this channel model, the wireless channel between a class-i node and a class-j node is on with probability α_{ij} and off with probability $1-\alpha_{ij}$, independently. This gives rise to a $r \times r$ channel probability matrix $\boldsymbol{\alpha}$ where the element at the ith row and jth column is given by α_{ij}. The heterogeneous on-off channel model accounts for the fact that different nodes could have different radio capabilities, or could be deployed in locations with different channel characteristics. In addition, it offers the flexibility of modeling several interesting scenarios, such as when nodes of the same type are more (or less) likely to be adjacent with one another than with nodes belonging to other classes. The heterogeneous on-off channel model gives rise to inhomogeneous Erdős-Rényi graphs [19,32], denoted hereafter by $\mathbb{G}(n,\boldsymbol{\mu},\boldsymbol{\alpha})$. In these graphs,

[1] Note that a network is said to be k-connected if its connectivity is preserved despite the failure of any $(k-1)$ nodes or links; a network is said to be connected if it is 1-connected.

each of the n vertices is classified as class-i with probability $\mu_i > 0$ such that $\sum_{i=1}^{r} \mu_i = 1$. Two vertices v_x and v_y, which belong to class-i and class-j, respectively, are adjacent if $B(\alpha_{ij}) = 1$, where $B(\alpha_{ij})$ denotes a Bernoulli random variable with success probability α_{ij}.

The overall network in this case can be modeled by a *composite* random graph model formed by the *intersection* of an inhomogeneous random key graph with an inhomogeneous Erdős-Rényi graph. We denote the intersection graph by $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$. An edge exists in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ only if it exists in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$, i.e., both nodes share a key, and $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$, i.e., both nodes share a wireless channel. Hence, edges in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K},P,\boldsymbol{\alpha})$ represent pairs of sensors that both i) share a key and ii) have a wireless channel in between that is on.

A summary of the results we establish for the composite random graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ is given below.

- A zero-one law for the absence of isolated nodes in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ [48].

- A zero-one law for the connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ [41].

Essentially, our results provide design guidelines on how to choose the parameters of the heterogeneous random key predistribution scheme such that the resulting wireless sensor network is securely connected under a heterogeneous on-off channel model. Our results are supported by a simulation study demonstrating that despite their asymptotic nature, our results can in fact be useful in designing finite-node wireless sensor network so that they achieve secure connectivity with high probability.

2.4 Inhomogeneous random K-out graphs

Random K-out graphs provide an accurate modeling framework for a class of wireless sensor networks utilizing random pairwise key predistribution scheme. An inherent assumption, however, is that all nodes are treated uniformly in a sense that each node selects the same number K of other nodes to be paired to. Indeed, the heterogeneity of emerging wireless sensor networks gives rise to the cases where nodes have dissimilar roles, or dissimilar connectivity, centrality, or security requirements, hence different nodes could be paired to a different number of other nodes. This induces the need for a broader modeling framework that generalizes Chan et al. scheme [24] to heterogeneous networks.

2.5 Thesis contributions II

In this thesis, we propose *inhomogeneous random K-out graphs* $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K})$ [46,51] as a modeling framework for a class of random pairwise key predistribution schemes that generalize Chan et al. scheme [24] for heterogeneous networks under full visibility. Inhomogeneous random K-out graphs $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K})$ are constructed as follows. First, each of the n nodes is assigned to class-i with probability $\mu_i > 0$ for $i = 1, \ldots, r$, where r is a fixed positive integer that does not scale with n and $\sum_{i=1}^{r} \mu_i = 1$. Each class-i node chooses K_i distinct nodes selected uniformly at random from among all other nodes. Two nodes u and v are connected by an edge if u selects v, v selects u, or both. Without loss of generality, we assume that $K_1 \leq K_2 \leq \ldots \leq K_r$.

The connectivity of random K-out graphs was studied in [55, 152], where it was shown that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n; K) \text{ is connected}\right] = \begin{cases} 0 & \text{if} \quad K = 1 \\ \\ 1 & \text{if} \quad K \geq 2 \end{cases} \tag{2.1}$$

In other words, it is sufficient to set $K = 2$ to obtain a network that is connected with high probability as the network size tends to infinity. In fact, from the bounds obtained in [152], it is seen that probability that $\mathbb{H}(n; 2)$ is connected exceeds 0.99 already with $n = 50$ nodes.

We investigate the connectivity of $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K})$ for the particular case when $K_1 = 1$ (note that if $K_1 \geq 2$, then the graph is connected with high probability according to (2.1)). More precisely, we seek conditions on $K_2, K_3, \ldots, K_r$ and $\boldsymbol{\mu}$ such that the resulting graph is connected with high probability when $K_1 = 1$. Our main results [49, 51] show that

- $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}\right)$ is connected with high probability if and only if $K_{r,n} = \omega(1)$. In other words, if the largest key ring size $K_{r,n}$ grows unboundedly large as $n \to \infty$, then the probability that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$ is connected approaches one in the same limit.

- However, any bounded choice of $K_{r,n}$, i.e., $K_{r,n} = O(1)$ gives a positive probability of $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}_n\right)$ being *not* connected in the limit of large n.

Comparing our results with (2.1) sheds the light on a striking difference between inhomogeneous random K-out graphs $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}\right)$ and their homogeneous counterparts $\mathbb{H}\left(n; K\right)$. In particular, the flexibility of organizing the nodes into several classes with different characteristics (with $K_1 = 1$) comes at the expense of requiring $\lim_{n\to\infty} K_{r,n} = \infty$, in contrast to the homogeneous case where having $K = 2$ was sufficient to ensure connectivity.

Before we transition into the second application area, we summarize our contributions thus far in Table 2.1.

Application Area I: Modeling secure connectivity of large-scale wireless sensor networks	**Proposed Model I:** $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$	**Modeling** connectivity of wireless sensor networks secured by the heterogeneous random key predistribution scheme under a *uniform* on-off channel model
		Results: • A zero-one for the absence of isolated nodes. • A zero-one law for connectivity. • A zero-one law for the minimum node degree being no less than k. • A zero-one law for k-connectivity.
	Proposed Model II: $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$	**Modeling** connectivity of wireless sensor networks secured by the heterogeneous random key predistribution scheme under a *heterogeneous* on-off channel model
		Results: • A zero-one for the absence of isolated nodes. • A zero-one law for connectivity.
	Proposed Model III: $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$	**Modeling** connectivity of wireless sensor networks secured by the heterogeneous random pairwise predistribution scheme under full visibility
		Results: • Showing that the probability of connectivity is strictly less than one when $K_{r,n}=O(1)$. • Deriving a one law for connectivity when $K_{r,n}=\omega(1)$.

Table 2.1: A summary of the proposed models and contributions with regard to the first application area, namely, modeling secure connectivity of large-scale wireless sensor networks

Chapter 3

Application Area II: Modeling real-world social networks

The study of *Social networks* has attracted great interest and curiosity from a multidisciplinary perspective. In social sciences, theoretical and empirical studies were carried out for over 50 yeas [113, 143] to investigate the patterns of social connections among humans, and their implications on the spread of diseases, rumors, or information [110]. More recently, there has been a surge of interest in social networks from applied mathematics and related fields due to the availability of large-scale datasets representing real-world social networks and the advances in mathematical modeling of networks. We refer the reader to [57, 113, 143] for a brief history of social network analysis.

Social networks represent a class of networks where vertices denote social entities such as individuals, communities, or countries, and an edge between two vertices represents a social relation between them. The social relation could represent a friendship between two individuals, a flow of trade between two countries, etc. Modeling such complex social systems by networks paves the way for investigating the influence of the connection patterns among social entities on the behavior of the network. For example, the prevalence of communities (or clusters) of people who share similar features, such as ethnicity, in a social network reveals the presence of *homophily* [94]. Indeed, homophily has a tremendous effect on the behavior of a social system, as it limits the information people receive and the interactions they experience only to those similar to them [107].

The theory of random graphs is of significant relevance to the area of *social networks*. In particular, a large body of research has proposed several random graph models with the aim of creating networks that resemble the *structure* of real-world social networks. For example, *random graphs with arbitrary degree distribution* [100, 115] are widely used as models for social networks since they can match the skewed degree distribution observed in real-world social networks [116]. In addition, random graphs with clustering [97, 109] (graphs that are generated randomly from given distributions specifying the number of single edges and triangles for any given node) could resemble the structure of *clustered* real-world social networks.

3.1 Spreading processes

Of particular interest in the context of social networks is the study of how spreading processes, such as rumors, information, influence, or diseases propagate over these networks [12, 35, 108, 149, 168]. A typical question in this context is whether an information (or rumor, infectious disease, etc.) starting from an arbitrary individual would eventually reach a significant number of people. A conventional model for spreading processes is the SIR epidemic model. In this context, an individual is either *susceptible* (S) meaning that she has not yet received the information/disease, or infectious (I) meaning that she has received the information/disease and is capable of spreading it to her contacts, or recovered (R) meaning that she is no longer spreading the information/disease. The dynamics of diffusion can be described as in [108]. An infectious individual i transmits the information/disease to a susceptible individual j with probability $T_{ij} = 1 - \exp(-\beta_{ij}\tau_i)$, where β_{ij} denotes the rate of infectious contacts from node i to node j and τ_i denotes the infectious period of node i, i.e., the period of time during which node i remains infective.

The infectious period τ_i is a random variable with a Cumulative Distribution Function (CDF) $F_\tau(u)$, and the infectious contact rate β_{ij} is also a random variable with a CDF $F_\beta(v)$. It was established in [108] that when i) the infectious contact rates between individuals are independent and identically distributed (i.i.d) and that ii) the infectious periods for all individuals are also i.i.d., then the spread of a diseases/information on a contact network is isomorphic to a bond-percolation model on the contact network with a bond percolation parameter given by[1]

$$T = \langle T_{ij} \rangle = 1 - \int_0^\infty e^{-\beta\tau} dF_\beta(\beta) dF_\tau(\tau)$$

where T was called the *transmissibility* of the disease. The isomorphism to a bond-percolation problem allowed for the use of the generating function approach to derive the threshold, probability, and final size of epidemics on a contact network with arbitrary degree distributions.

3.2 Evolutionary adaptations

One inherent assumption related to the classical bond-percolation framework is that the propagating object, i.e., a disease or a piece of information, is transferred across the nodes without going through any modification or *evolution* [10, 35, 114, 124, 149, 168]. However, in real-life spreading processes, pathogens often *evolve* in response to changing environments and medical interventions [3, 7, 86], and information is often modified by individuals before being forwarded [1, 163]. In fact, 60% of the (approximately) 400 emerging infectious diseases that have been identified since 1940 are zoonotic [2] [75, 105]. A zoonotic disease is initially poorly adapted, poorly replicated, and inefficiently transmitted [118], hence its ability to go from animal-to-human transmissions to human-to-human transmissions depends on the pathogen *evolving* to a strain that is well-adapted to the human host. For instance, genetic variations in some critical genes were reported to be essential for the transition from animal-to-human transmission to human-to-human transmission in the severe acute respiratory syndrome (SARS) outbreak of 2002-2003 [136].

In this thesis, we aim to bridge the disconnect between how spreading processes propagate

[1] Later on, Kenah and Robins [78] proved that this isomorphism to a bond-percolation problem is valid only when the distribution of the infectious periods is *degenerate*, i.e., $\tau_i = \tau_0$ for all $i = 1, 2, \ldots$, where τ_0 is a constant.

[2] A zoonosis is any disease or infection that is naturally transmissible from vertebrate animals to humans [117].

and evolve in real-life, and the current propagation models that by and large ignore evolutionary adaptations. In particular, we consider a class of inhomogeneous epidemic models referred to as *multiple-strain* models. These models account for evolutionary adaptations as follows. The initial strain of the pathogen/information could mutate to a different strain with different transmissibility at some point during the propagation. The mutant could also further mutate to another strain, or mutate back to the original strain at some point during the propagation. At any point during the propagation, multiple strains with different transmissibilities may coexist in the population. Hence, multiple-strain models essentially generalize the SIR model by creating several possible substates for the infected state, e.g., infected with strain-1, infected with strain-2, etc., and providing mutation rules governing the transitions among these substates.

We analyze the propagation of spreading processes governed by the multiple-strain model on random graphs with arbitrary degree distribution, generated by the *configuration model* [100, 115]. The configuration model generates random graphs with specified degree sequence (sampled from an arbitrary degree distribution), but are otherwise random, by taking a uniformly random matching on the half-edges of the specified degree sequence. The configuration model provides a tractable mathematical framework that allows the investigation of several key properties related to the spreading process and how it interacts with the structure of the underlying graph, as specified by its degree distribution. In addition, since the model could match the degree sequence of real-world social networks, it would essentially generate graphs that resemble such real-world networks to a great extent.

3.3 Thesis contributions III

We investigate the *evolution* of spreading processes, such as infectious diseases or information, in social networks with the aim of i) revealing the role of evolutionary adaptations on the threshold, probability, and final size of epidemics; and ii) exploring the interplay between the structural properties of the network and the process of evolution. We start by considering the case where *co-infection* with different pathogen strains (respectively, different variations of information) is not possible, i.e., a susceptible individual may only be infected with a *single* pathogen strain (respectively, a single variant of the information). In this case, we develop a mathematical theory that accurately predicts the epidemic threshold and the expected epidemic size as functions of the characteristics of the spreading process, the evolutionary pathways of the pathogen (respectively, information), and the structure of the underlying contact network. In addition to the mathematical theory, we perform extensive simulations on synthetic and real-world contact networks to verify our theory and reveal the significant shortcomings of the classical bond percolation models that do not capture evolution.

Our results reveal that the classical bond percolation models may accurately predict the threshold and final size of epidemics, but their predictions on the probability of emergence are *inaccurate* on both synthetic and real-world networks. This inaccuracy sheds the light on a fundamental disconnect between the classical bond-percolation models and real-life spreading processes that entail evolution. Then, we consider the case when *co-infection* is possible, i.e., a susceptible individual who receives *simultaneous* infections with multiple pathogen strains (respectively, multiple variations of information) becomes co-infected. We show by computer simulations that co-infection gives rise to a rich set of dynamics: it can amplify or inhibit the spreading dynamics, and more remarkably *lead the order of phase transition to change from second-order to first-order.* We investigate the delicate interplay between the characteristics of co-infection, the structure of the underlying contact network, and the evolutionary pathways of the pathogen (respectively, information) and reveal the cases where such interplay induces a *first-order* phase transition for the expected epidemic size.

3.4 Clustered social networks

Although random graphs generated by the configuration model could resemble the degree sequences observed in real-world social networks, they have a vanishingly small clustering coefficient that tends to zero in the limit of large network size. Hence, the random graphs generated by the configuration model can not accurately capture some important aspects of real-world social networks, most notably the property of high clustering [132, 144], which has a significant impact on the behavior of various spreading processes [70, 72].

To better model real-world social networks that are typically clustered, we utilize a model that generates random networks *with clustering* as introduced by Miller [97] and Newman [109], i.e., graphs are generated randomly from given distributions specifying the number of single edges and triangles for any given node. Our objective is to investigate the characteristics of spreading processes that entail evolutionary adaptations on such random graph models with tunable clustering. In particular, we aim to present a mathematical theory that predicts the epidemic threshold and the probability of emergence as functions of the characteristics of the spreading object, the evolutionary pathways of the pathogen/information, and the structure of the underlying network as given by the degree distribution *and* the clustering coefficient.

3.5 Thesis contributions IV

We investigate the *evolution* of spreading processes, such as infectious diseases or information, in *clustered* social networks, hence we extend our previous results for the case when the underlying graph had a vanishingly small clustering coefficient. Our objectives are to i) reveal the role of evolutionary adaptations on the threshold and probability of epidemics when the network exhibits a non-vanishing clustering coefficient; as well as ii) identify the interplay between the structural properties of the network (as given by the degree distribution and clustering coefficient) and evolutionary adaptations. Our results are given in the form of a mathematical theory that accurately predicts the epidemic threshold and the probability of emergence as functions of the characteristics of the spreading process, the evolutionary pathways of the pathogen (respectively, information), and the structure of the underlying contact network (as given by its degree distribution *and* clustering coefficient). Simulation results on synthetic networks are also provided to verify our theory.

A summary of our contributions in this application area is given in Table 3.1.

Application Area II: Modeling real-world social networks	**Proposed Model I:** Inhomogeneous spreading processes governed by the multiple-strain model on random graphs with arbitrary degree distribution generated by the configuration model	**Modeling** the spread of information or infectious diseases entailing evolutionary adaptations on real-world social networks characterized by their degree distribution
		Results: • Proposing a mathematical theory that predicts the threshold and final size of epidemics. • Revealing the shortcomings of classical bond percolation model that do not capture evolutionary adaptations through extensive simulations results on synthetic and real-world networks. • Specifying the interplay between the characteristics of co-infection and the type of phase transition that the expected epidemic size undergoes
	Proposed Model II: Inhomogeneous spreading processes governed by the multiple-strain model on random graphs with clustering	**Modeling** the spread of information or infectious diseases entailing evolutionary adaptations on clustered real-world social networks
		Results: • Proposing a mathematical theory that predicts the threshold and probability of epidemics.

Table 3.1: A summary of the proposed models and contributions with regard to the second application area, namely, modeling real-world social networks

Chapter 4

The structure of the thesis

The rest of the thesis is organized as follows. In the first part of the thesis (Part II), we focus on the first application area, namely, the role of random graphs in providing a modeling framework for secure connectivity of large-scale wireless sensor networks utilizing random predistribution of cryptographic keys. In Chapter 6, we present our results on the connectivity of wireless sensor networks secured by the heterogeneous random key predistribution scheme under a *uniform* on-off channel model where the channel between two nodes is on (respectively, off) with probability α (respectively, $1 - \alpha$), independently and regardless of the class of the two nodes. In particular, we present a novel composite random graph formed by the intersection of inhomogeneous random key graphs and Erdős-Rényi graphs as a model for the shared-key connectivity *and* wireless connectivity of the sensor network. We then establish sharp zero-one laws for the properties that i) the graph has no isolated nodes, ii) the graph is connected, iii) the minimum node degree is no less than k, and iv) the graph is k-connected.

In Chapter 7, we generalize the uniform on-off channel model to a *heterogeneous* on-off channel model, where the channel between a class-i node and a class-j node is on (respectively, off) with probability α_{ij} (respectively, $1 - \alpha_{ij}$) independently. We present a novel composite random graph formed by the intersection of inhomogeneous random key graphs and inhomogeneous Erdős-Rényi graphs as a model for the shared-key connectivity *and* wireless connectivity of the sensor network in this case. We then establish zero-one laws for the properties that i) the graph has no isolated nodes, and ii) the graph is connected.

In Chapter 8, we propose *inhomogeneous* random K-out graphs as a modeling framework for heterogeneous wireless sensor networks utilizing random pairwise key predistribution scheme. In our model, each node is classified as class-i with probability $\mu_i > 0$ for $i = 1, \ldots, r$ and a class-i node selects $K_{i,n}$ other nodes to be paired to. With $K_{1,n} \leq \ldots K_{r,n}$, we focus on the particular case when $K_{1,n} = 1$ and derive i) an upper-bound on the probability of connectivity when the largest number of selections $K_{r,n}$ is finite, and ii) a one-law for connectivity when $K_{r,n} = \omega(1)$.

The second part of the thesis (Part III) focuses on the second application area, namely, random graphs as models for real-world social networks. In this part, we investigate the propagation of *inhomogeneous* spreading processes characterized by the multiple-strain model on contact networks modeled by i) random graphs with arbitrary degree distributions (Chapter 9) and ii) random graphs with clustering (Chapter 10). In Chapter 9, we derive a mathematical theory that characterizes the expected epidemic size and the epidemic threshold for spreading processes governed by the multiple-strain framework on random graphs with arbitrary degree distributions. We also show by computer simulations (on synthetic and real-world networks) the significant shortcomings of the classical bond-percolation models that do not capture evolutionary adaptations. We close the chapter by considering the case where co-infection with multiple pathogen strains is possible and show by computer simulations that co-infection could lead the order of phase transition for the expected epidemic size to change from second-order to first-order.

In Chapter 10, we consider contact networks modeled by random graphs with clustering to account for the fact that many real-world social networks are highly clustered. We derive a mathematical theory that characterizes the probability of emergence and the epidemic threshold for spreading processes governed by the multiple-strain framework on contact networks modeled by random graphs with clustering. Our results are complemented by computer simulations that validate their accuracy and reveal the impact of clustering.

Finally, in Chapter 11, we give the concluding remarks and in Chapter 12, we discuss potential directions for future work.

Chapter 5

Notations and conventions

All limiting statements, including asymptotic equivalence are considered with the number of sensor nodes n going to infinity. The random variables (rvs) under consideration are all defined on the same probability triple $(\Omega, \mathcal{F}, \mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation by $\mathbb{E}$. The indicator function of an event E is denoted by $\mathbf{1}[E]$. We say that an event holds with high probability (whp) if it holds with probability 1 as $n \to \infty$. For any event E, we let $\overline{E}$ denote the complement of E. For any discrete set S, we write $|S|$ for its cardinality. For sets S_a and S_b, the relative complement of S_a in S_b is given by $S_a \setminus S_b$. In comparing the asymptotic behaviors of the sequences $\{a_n\}, \{b_n\}$, we use $a_n = o(b_n)$, $a_n = \omega(b_n)$, $a_n = O(b_n)$, $a_n = \Omega(b_n)$, and $a_n = \Theta(b_n)$, with their meaning in the standard Landau notation. Namely, we write $a_n = o(b_n)$ (respectively, $a_n = \omega(b_n)$) as a shorthand for the relation $\lim_{n\to\infty} \frac{a_n}{b_n} = 0$ (respectively, $\lim_{n\to\infty} \frac{a_n}{b_n} = \infty$), whereas $a_n = O(b_n)$ means that there exists $c > 0$ such that $a_n \le cb_n$ for all n sufficiently large. Also, we have $a_n = \Omega(b_n)$ if $b_n = O(a_n)$, or equivalently, if there exists $c > 0$ such that $a_n \ge cb_n$ for all n sufficiently large. We write $a_n = \Theta(b_n)$ if we have $a_n = O(b_n)$ and $a_n = \Omega(b_n)$ at the same time. We also use $a_n \sim b_n$ to denote the asymptotic equivalence $\lim_{n\to\infty} a_n/b_n = 1$. We write $\mathbb{N}_0$ to denote the set of natural numbers excluding zero, i.e., $\mathbb{N}_0 = \{1, 2, 3, \ldots\}$. Finally, we write $X \overset{d}{=} Y$, for two random variables X and Y, to mean that X and Y are equal in distribution.

Part II

Application Area I: Modeling Secure Connectivity of Large-Scale Wireless Sensor Networks

Chapter 6

Results on inhomogeneous random key graphs intersecting Erdős-Rényi graphs

6.1 Motivation

In their seminal work, Eschenauer and Gligor proposed a *random key predistribution* scheme as a practical and efficient method for key-establishment in large scale wireless sensor networks [53]. Their scheme operates as follows: before deployment, each node is given a *random* set of K cryptographic keys, selected *uniformly* (without replacement) from a large key pool of size P. After deployment, two nodes can communicate *securely* over an existing channel *if* they share at least one key[1]. Eschenauer-Gligor scheme is currently regarded as one of the most feasible solutions for key-establishment among sensor nodes, e.g., see [125, Chapter 13], [22], and references therein, and has led the way to several other variants, including the q-composite scheme [24], the random pairwise scheme [24], and many others.

Eschenauer-Gligor scheme inherently assumes that all nodes are *homogeneous* in terms of their roles and capabilities, hence they are assigned the same number K of keys. However, emerging wireless sensor network applications are complex and are envisioned to require the coexistence of different classes of nodes with different roles and capabilities [150]. For instance,

[1] There are multiple reasons why node-to-node encryption/decryption is vital to wireless sensor networks. Firstly, each node broadcasts an encrypted packet which contains the entire header info; i.e., source and destination addresses are encrypted. Hence, each packet has to be decrypted to be routed. Furthermore, the lack of a trusted third party induces the need for shared-keys between nodes to ensure the *authenticity* of communication among them [24].

a particular class of nodes may act as cluster heads that are used to connect several clusters of nodes together. These cluster heads need to communicate with a large number of nodes in their vicinity and they are also expected to be more powerful than regular nodes. Thus, more keys should be given to the cluster heads to ensure high levels of connectivity and security.

To cope with the expected heterogeneity in wireless sensor network topologies, Yağan proposed a new variation of Eschenauer-Gligor scheme, referred to as the *heterogeneous* random key predistribution scheme [157]. The heterogeneous scheme considers the case when the network includes sensors with varying levels of resources, features, security, or connectivity requirements. The scheme is described as follows. Given r classes, each sensor is independently classified as a class-i node with probability $\mu_i > 0$ for each $i = 1, \ldots, r$. Then, sensors in class-i are each assigned K_i keys selected uniformly at random from a key pool of size P. Similar to Eschenauer-Gligor scheme, nodes that share at least one common key (regardless of their class) can communicate securely over an available channel after deployment.

Given the randomness involved in Eschenauer-Gligor scheme and the heterogeneous scheme, there is a positive probability that a pair of nodes may have no common key, thus can not establish a secure communication link in between. Moreover, two nodes that share a key may not have a wireless channel in between (possibly because of the limited transmission radius). Hence, it is natural to ask whether the resulting network would be securely *connected* or not. Specifically, two nodes are securely connected if they share a key *and* have a communication channel in between. A network is said to be connected if there is a path between every pair of vertices. In essence, one needs to know if it is possible to *control* the parameters of the scheme (possibly as functions of the network size n), such that the resulting network is connected with high probability. Indeed, there is a fundamental interplay between the security and connectivity of the resulting network. To see this, consider the classical Eschenauer-Gligor scheme where all nodes receive the same number of keys K from a key pool of size P. Note that when an adversary captures one node, a K/P fraction of the key pool is revealed to the adversary allowing her to compromise secure communications. Thus, from a security standpoint, it is better to minimize the fraction K/P to improve the resiliency of the network against node capture attacks [33]. However, it is clear that from a connectivity standpoint, it is always better to increase K or decrease P (thus increasing the fraction K/P), to make it more likely for two nodes to end up sharing a key. That is why it is crucial to know the exact minimum conditions required to achieve the desired level of connectivity by means of a *sharp* zero-one law -Only then we can avoid overshooting the parameters and losing from resiliency.

In [157], Yağan considered a wireless sensor network secured by the heterogeneous scheme under *full-visibility* assumption, i.e., all pairs of sensors have a communication channel in between, hence the only condition for two nodes to be connected is to share a key. Therein, they established scaling conditions on the parameters of the heterogeneous scheme as functions of the network size n such that the resulting network is connected with high probability as the number of nodes gets large. In particular, they considered a random graph model naturally induced by the heterogeneous scheme and established scaling conditions on the model parameters such that the resulting graph is connected with high probability as the number of nodes gets large. Specifically, with $\boldsymbol{K} = \{K_1, K_2, \ldots, K_r\}$, $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$, and n denoting the network size, we let $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ denote the random graph induced by the heterogeneous key predistribution scheme, where any pair of vertices are *adjacent* as long as they share a key. This model was referred to as the *inhomogeneous* random key graph in [157], where zero-one laws for absence of isolated nodes and connectivity were established. The inhomogeneous random key graph models the *shared-key* connectivity of the wireless sensor networks under the heterogeneous scheme.

This chapter is motivated by the fact that the full-visibility assumption is not likely to hold in real-world implementations of wireless sensor networks. In particular, the randomness of the wireless channel as well as limited transmission ranges would severely limit the availability of wireless channels between nodes, rendering two nodes disconnected even when they share a key. In fact, as wireless connectivity comes into play, an essential question arises: *Under a given model for wireless connectivity, is it possible to control the parameters of the heterogeneous* *scheme to ensure that the resulting network is connected?*

In [156], it was shown that an independent on-off channel model provides a good approximation of the more-realistic disk model for understanding the critical scalings of connectivity in settings similar to ones we consider here. In the independent on-off channel model, the wireless channel between any given pair of nodes is either on (with probability α) or off (with probability $1-\alpha$) independently from all other channels. The model induces an Erdős-Rényi graph $\mathbb{G}(n;\alpha)$, where an edge exists (respectively does not exist) between two vertices with probability α (respectively $1-\alpha$) independently from all other edges. With this in mind, we model the wireless connectivity of the wireless sensor network by an Erdős-Rényi graph $\mathbb{G}(n;\alpha)$ and study the *connectivity* of the intersecting graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$. This approach allows us to i) establish rigorous results concerning the secure connectivity of wireless sensor networks albeit using a simplified wireless communication model, and ii) demonstrate via simulations that these results still apply under the more realistic disk model.

In addition to having connectivity, *reliability* against the failure of sensors or links is important in wireless sensor network applications where sensors are unattended for long periods of time (e.g., environmental monitoring), or, are prone to node-capture attacks (e.g., battlefield surveillance), or, are used in life-critical applications (e.g., patient monitoring). With this in mind, we will also derive scaling conditions on the parameters of the intersecting graph with respect to the network size n such that i) the minimum node degree of the graph is no less than k and ii) the graph is k-connected. A network is said to be k-connected if its connectivity is preserved despite the failure of any $(k-1)$ nodes or links; a network is simply said to be connected if it is 1-connected. Therefore, k-connectivity provides a guarantee of network reliability against the possible failures of sensors or links due to adversarial attacks, battery depletion, or harsh environmental conditions. Also, k-connectivity ensures that each pair of nodes in the network are connected by at least k mutually disjoint paths [121].

k-connectivity – a fundamental property of graphs – is particularly important in secure sensor networks where nodes operate *autonomously* and are physically *unprotected*. For instance, k-connectivity provides communication security against an adversary that is able to *compromise* up to $(k-1)$ links by launching a sensor capture attack [24]; i.e., two sensors can communicate securely as long as at least one of the k disjoint paths connecting them consists of links that are not compromised by the adversary. Also, k-connectivity improves robustness against network disconnection due to battery depletion, in both normal mode of operation and under battery-depletion attacks [87, 138]. Furthermore, it enables flexible communication-load balancing across multiple paths so that network energy consumption is distributed without penalizing any access path [58]. In addition, k-connectivity is useful in achieving consensus despite adversarial nodes in the network. Specifically, if $k = 2m+1$ where m is the number of adversary-controlled nodes, k-connectivity guarantees that consensus can be reached in any network with $n \gg m$ nodes [36, 166]. Finally, k-connectivity has important implications on *mobile* connectivity of wireless sensor networks. For instance, if a network is k-connected, then any of its $(k-1)$ nodes can be made *mobile*, and move anywhere in the network freely, while the network remains at least 1-connected all the time. So, in applications where only a small number of sensors need to be mobile, whereas others will be static, k-connectivity will be a crucial property that ensures continuous connectivity of the network.

6.2 A roadmap

In this chapter we propose a novel composite random graph that offers a modeling framework for large-scale wireless sensor networks secured by the heterogeneous key predistribution scheme under an independent on-off channel model. The heterogeneous scheme induces an inhomogeneous random key graph, denoted by $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ and the on-off channel model induces an Erdős-Rényi graph, denoted by $\mathbb{G}(n,\alpha)$. Hence, the overall random graph modeling the network is obtained by the intersection of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ and $\mathbb{G}(n,\alpha)$. We start by presenting conditions on how to scale the parameters of the intersecting graph with respect to the network size n such that the graph i) has no isolated nodes and ii) is connected, both with high probability as the number of nodes gets large. Then, we proceed by presenting scaling conditions on the model parameters such that iii) the minimum node degree is no less than k, and iv) the graph is k-connected. Our results are supported by a simulation study demonstrating that i) despite their asymptotic nature, our results can in fact be useful in designing *finite*-node wireless sensor networks so that they achieve secure connectivity with high probability; and ii) despite the simplicity of the on-off communication model, the probability of connectivity in the resulting wireless sensor network approximates very well the case where the disk model is used.

6.3 Model definitions

We consider a network consisting of n sensor nodes labeled as $v_1, v_2, \ldots, v_n$. Each sensor is assigned to one of the r possible classes (e.g., priority levels) according to a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for each $i = 1, \ldots, r$; clearly it is also needed that $\sum_{i=1}^{r} \mu_i = 1$. Prior to deployment, each class-i node is given K_i cryptographic keys selected uniformly at random from a pool of size P. Hence, the key ring Σ_x of node v_x is a $\mathcal{P}_{K_{t_x}}$-valued random variable (rv) where $\mathcal{P}_A$ denotes the collection of all subsets of $\{1, \ldots, P\}$ with exactly A elements and t_x denotes the class of node v_x. The rvs $\Sigma_1, \Sigma_2, \ldots, \Sigma_n$ are then i.i.d. with

$$\mathbb{P}[\Sigma_x = S \mid t_x = i] = \binom{P}{K_i}^{-1}, \quad S \in \mathcal{P}_{K_i}.$$

After the deployment, two sensors can communicate securely over an existing communication channel if they have at least one key in common.

Throughout, we let $\boldsymbol{K} = \{K_1, K_2, \ldots, K_r\}$, and assume without loss of generality that $K_1 \leq K_2 \leq \ldots \leq K_r$. Consider a random graph $\mathbb{K}$ induced on the vertex set $\mathcal{V} = \{v_1, \ldots, v_n\}$ such that distinct nodes v_x and v_y are adjacent in $\mathbb{K}$, denoted by the event K_{xy}, if they have at least one cryptographic key in common, i.e.,

$$K_{xy} := [\Sigma_x \cap \Sigma_y \neq \emptyset]\,. \tag{6.1}$$

The adjacency condition (6.1) characterizes the inhomogeneous random key graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ that has been introduced recently in [157]. This model is also known in the literature as the *general random intersection graph*; e.g., see [16, 62, 167].

The inhomogeneous random key graph models the *cryptographic* connectivity of the underlying wireless sensor network. In particular, the probability p_{ij} that a class-i node and a class-j node have a common key, and thus are adjacent in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$, is given by

$$p_{ij} = \mathbb{P}[K_{xy}] = 1 - \binom{P-K_i}{K_j} \Big/ \binom{P}{K_j} \tag{6.2}$$

as long as $K_i + K_j \leq P$; otherwise if $K_i + K_j > P$, we clearly have $p_{ij} = 1$. We also find it useful to define the *mean* probability λ_i of edge occurrence for a class-i node in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$. With arbitrary nodes v_x and v_y, we have

$$\lambda_i = \mathbb{P}[K_{xy} \mid t_x = i] = \sum_{j=1}^{r} p_{ij}\mu_j, \quad i = 1,\ldots,r, \tag{6.3}$$

as we condition on the class t_y of node v_y. In addition, we define the *mean* key ring size by K_{avg}; i.e.,

$$K_{\text{avg}} = \sum_{j=1}^{r} K_j\mu_j. \tag{6.4}$$

In this work, we consider the communication topology of the wireless sensor network as consisting of independent channels that are either *on* (with probability α) or *off* (with probability $1-\alpha$). More precisely, let $\{B_{ij}(\alpha) : 1 \leq i < j \leq n\}$ denote i.i.d Bernoulli rvs, each with success probability α. The communication channel between two distinct nodes v_x and v_y is on (respectively, off) if $B_{xy}(\alpha) = 1$ (respectively if $B_{xy}(\alpha) = 0$). The on-off channel model induces an Erdős-Rényi graph $\mathbb{G}(n;\alpha)$ [18], defined on the vertices $\mathcal{V} = \{v_1,\ldots,v_n\}$ such that v_x and v_y are adjacent, denoted C_{xy}, if $B_{xy}(\alpha) = 1$.

We model the overall topology of the wireless sensor network by the intersection of an inhomogeneous random key graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ and an Erdős-Rényi graph $\mathbb{G}(n;\alpha)$. Namely, nodes

v_x and v_y are adjacent in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$, denoted E_{xy}, if and only if they are adjacent in both $\mathbb{K}$ *and* $\mathbb{G}$. In other words, the edges in the intersection graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ represent pairs of sensors that can securely communicate as they have i) a communication link in between that is *on*, and ii) a shared cryptographic key. Therefore, studying the connectivity properties of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ amounts to studying the secure connectivity of heterogeneous wireless sensor network under the on-off channel model.

To simplify the notation, we let $\boldsymbol{\theta}=(\boldsymbol{K},P)$ and $\boldsymbol{\Theta}=(\boldsymbol{\theta},\alpha)$. The probability of edge existence between a class-i node v_x and a class-j node v_y in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$ is given by

$$\mathbb{P}[E_{xy}\mid t_x=i,t_y=j]=\mathbb{P}[K_{xy}\cap C_{xy}\mid t_x=i,t_y=j]=\alpha p_{ij}$$

by independence. Similar to (6.3), the mean edge probability for a class-i node in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$, denoted Λ_i, is given by

$$\Lambda_i=\sum_{j=1}^{r}\mu_j\alpha p_{ij}=\alpha\lambda_i,\quad i=1,\ldots,r. \tag{6.5}$$

Throughout, we assume that the number of classes r is fixed and does not scale with n, and so are the probabilities $\mu_1,\ldots,\mu_r$. All of the remaining parameters are assumed to be scaled with n.

6.4 Preliminaries

This is a collection of technical results that would be used throughout. The first result follows easily from the scaling condition (6.15).

Proposition 6.4.1 ([157, Proposition 4.1]). *For any scaling $K_1,K_2,\ldots,K_r,P:\mathbb{N}_0\to\mathbb{N}_0^{r+1}$, we have (in view of (6.15))*

$$\lambda_1(n)\le\lambda_2(n)\le\ldots\le\lambda_r(n) \tag{6.6}$$

for each $n=2,3,\ldots$.

In view of (6.5), Proposition 6.4.1 implies that

$$\Lambda_1(n) \leq \Lambda_2(n) \leq \ldots \leq \Lambda_r(n), \qquad n = 2, 3, \ldots. \tag{6.7}$$

Lemma 6.4.2 ([157, Lemma 4.2]). *Consider any scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$. For any $i, j = 1, \ldots, r$,*

$$\lim_{n\to\infty} p_{ij}(n) = 0 \quad \textit{if and only if} \quad \lim_{n\to\infty} \frac{K_{i,n}K_{j,n}}{P_n} = 0$$

and we have the asymptotic equivalence

$$p_{ij}(n) \sim \frac{K_{i,n}K_{j,n}}{P_n}. \tag{6.8}$$

Proposition 6.4.3 ([157, Proposition 4.4]). *For any set of positive integers $K_1, \ldots, K_r, P$ and any scalar $a \geq 1$, we have*

$$\frac{\binom{P-\lceil aK_i \rceil}{K_j}}{\binom{P}{K_j}} \leq \left(\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}} \right)^a, \quad i, j = 1, \ldots, r. \tag{6.9}$$

Proposition 6.4.4. *Consider a random variable Z defined as*

$$Z = 1 - p_{1i} = \frac{\binom{P-K_1}{K_i}}{\binom{P}{K_i}}, \quad \textit{with probability } \mu_i, \quad i = 1, \ldots, r.$$

We have $var[Z] \leq \frac{1}{4}\left(p_{1r}\right)^2$.

Proof. We start by showing that under (6.103), the quantity $p_{ij}(n)$ is increasing in both i and j. Fix $n = 2, 3, \ldots$ and recall that under (6.103), K_i increases as i increases. For any i, j such that $K_i + K_j > P$, we see from (6.2) that $p_{ij}(n) = 1$; otherwise if $K_i + K_j \leq P$, we have $p_{ij}(n) < 1$. Given that $K_i + K_j$ increases with both i and j, it will be sufficient to show that

$p_{ij}(n)$ increases with both i and j on the range where $K_i + K_j < P$. On that range, we have

$$\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}} = \prod_{\ell=0}^{K_i-1}\left(1 - \frac{K_j}{P-\ell}\right)$$

Hence, $\binom{P-K_i}{K_j}/\binom{P}{K_j}$ decreases with both K_i and K_j, hence with i and j. From (6.2), it follows that $p_{ij}(n)$ increases with i and j. As a consequence, with $Z = 1 - p_{1i}$, we have

$$1 - p_{1r} \leq Z \leq 1 - p_{11}.$$

From Popoviciu's inequality [74, pp. 9], we see that

$$\mathrm{var}\left[Z\right] \leq \frac{1}{4}\left(Z_{\max} - Z_{\min}\right)^2 = \frac{1}{4}\left(p_{1r} - p_{11}\right)^2 \leq \frac{1}{4}\left(p_{1r}\right)^2$$

since $p_{1r} \geq p_{11} \geq 0$. □

Fact 6.4.5. *If $\lambda_1(n) = o(1)$, then*

$$p_{1i}(n) = o(1), \quad i = 1, \ldots, r$$

Proof. Recalling (6.3), we obtain

$$p_{1i}(n) \leq \left(\frac{1}{\mu_i}\right)\lambda_1(n) = O\left(\lambda_1(n)\right) = o(1)$$

under the given assumption that $\lambda_1(n) = o(1)$. □

Fact 6.4.6. *For $0 \leq x \leq 1$, the following properties hold.*

(a) [166, Fact 2] If $0 < y < 1$, then $(1-x)^y \leq 1 - xy$.

(b) Let $a > 1$. Then, $1 - x^a \leq a(1-x)$.

Proof. By a crude bounding, we have

$$1 - x^a = \int_x^1 at^{a-1}\ dt \le \int_x^1 a\ dt = a(1-x).$$

■

Fact 6.4.7 ([166, Fact 5]). *Let a, x, and y be positive integers satisfying $y \geq (2a+1)x$. Then,*

$$\frac{\binom{y-ax}{x}}{\binom{y}{x}} \geq \left[\frac{\binom{y-x}{x}}{\binom{y}{x}}\right]^{2a}$$

Other useful bounds that will be used throughout are

$$\binom{n}{\ell} \leq \left(\frac{en}{\ell}\right)^{\ell}, \quad \ell = 1, \dots, n, \quad n = 1, 2, \dots \tag{6.10}$$

$$\sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \leq 2^n \tag{6.11}$$

$$(1 \pm x) \leq e^{\pm x}, \quad x \in (0,1) \tag{6.12}$$

Finally, we find it useful to write

$$\log(1-x) = -x - \Psi(x) \tag{6.13}$$

where $\Psi(x) = \int_0^x \frac{t}{1-t}$ dt. From L'Hôpital's Rule, we have

$$\lim_{x \to 0} \frac{\Psi(x)}{x^2} = \frac{-x - \log(1-x)}{x^2} = \frac{1}{2}. \tag{6.14}$$

6.5 Connectivity and absence of isolated nodes

In this section, we present conditions (in the form of zero-one laws) on how to scale the parameters of the intersection model so that with high probability i) the graph has no isolated nodes; and ii) the graph is connected. We also present numerical results to support our findings in the finite-node regime.

We refer to a mapping $\boldsymbol{\Theta} = K_1, \ldots, K_r, P, \alpha : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$ as a *scaling* if

$$1 \leq K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{r,n} \leq P_n/2 \tag{6.15}$$

for all $n = 2, 3, \ldots$. We note that under (6.15), the edge probability p_{ij} is given by (6.2).

We first present a zero-one law for the absence of isolated nodes in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$.

6.5.1 A zero-one law for the absence of isolated nodes in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$

Theorem 6.5.1. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$ such that*

$$\Lambda_1(n) = \alpha_n \lambda_1(n) \sim c \frac{\log n}{n} \tag{6.16}$$

for some $c > 0$. We have

$$\lim_{n \to \infty} \mathbb{P} \begin{bmatrix} \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha) \\ \textit{has no isolated nodes} \end{bmatrix} = \begin{cases} 0 & \textit{if } c < 1 \\ 1 & \textit{if } c > 1 \end{cases} \tag{6.17}$$

The scaling condition (6.16) will often be used in the form

$$\Lambda_1(n) = c_n \frac{\log n}{n}, \; n = 2, 3, \ldots \tag{6.18}$$

with $\lim_{n\to\infty} c_n = c > 0$.

Next, we present an analogous result for connectivity.

6.5.2 A zero-one law for the connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$

Theorem 6.5.2. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$ such that (6.16) holds for some $c > 0$. Then, we have*

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha) \text{ is connected}] = \begin{cases} 0 & \text{if } c < 1 \\ \\ 1 & \text{if } c > 1 \end{cases} \tag{6.19}$$

under the additional conditions that

$$P_n \geq \sigma n, \quad n = 1, 2, \ldots \tag{6.20}$$

for some $\sigma > 0$ and

$$p_{11}(n) = \omega\left(\frac{1}{n\alpha_n}\right). \tag{6.21}$$

6.5.3 Discussion

The resemblance of the results presented in Theorem 6.5.1 and Theorem 6.5.2 indicates that absence of isolated nodes and connectivity are asymptotically equivalent properties for $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$. Similar observations were made for other well-known random graph models as well; e.g., inhomogeneous random key graphs [157], Erdős-Rényi graphs [18], and (homogeneous) random key graphs [159].

Conditions (6.20) and (6.21) are enforced mainly for technical reasons and they are only needed in the proof of the one-law of Theorem 6.5.2. In particular, condition (6.20) is essential for real-world implementations of wireless sensor networks in order to ensure the *resilience* of the network against node capture attacks; e.g., see [33, 53]. For instance, assume that an adversary captures a number of sensors, compromising all the keys that belong to the captured nodes. If $P_n = o(n)$, then it would be possible for the adversary to compromise $\Omega(P_n)$ keys by capturing only $o(n)$ sensors (whose type does not matter in this case). In this case, the network would fail to exhibit the *unassailability* property [95, 153] and would be deemed as vulnerable against adversarial attacks.

Also, condition (6.21) is enforced mainly for technical reasons for the proof of the one-law to work. The need of such a lower bound arises from the fact that our scaling condition (6.16) merely scales the minimum *mean* edge probability, not the minimum (or each) edge probability, as $\log n/n$. For instance, the current scaling condition (6.16) gives us an easy upper bound on the minimum edge probability in the network, but does not specify any non-trivial lower bound on that probability. More specifically, it is easy to see that $\alpha_n p_{11}(n) = O\left(\Lambda_1\right) = O\left(\log n/n\right)$, but it is not clear if the sequence $\alpha_n p_{11}(n)$ has a non-trivial lower bound. In fact, authors in [32] investigated the connectivity of an inhomogeneous Erdős-Rényi (ER) graph, while setting the probability of an edge connecting two nodes of classes i and j to $\kappa\left(i,j\right)\log n/n$, where $\kappa\left(i,j\right)$ returns a positive real number for each pair (i,j); i.e., each individual edge was scaled as $\log n/n$.

In summary, condition (6.20) is needed to ensure the resilience of the network against node capture attacks, while condition (6.21) is needed to provide a non-trivial lower bound on the minimum edge probability of the network. To provide a concrete example, one can set $P_n = n\log n$ and have $K_{1,n} = (\log n)^{1/2+\varepsilon}$ with any $\varepsilon > 0$ to satisfy (6.21) for any $\alpha_n \geq 1/(\log n)^{\varepsilon}$ (see Lemma 6.4.2). In this case, setting $K_{\text{avg},n} = \log n^{3/2}$ ensures that the resulting network is connected whp (see Corollary 6.5.3).

Theorem 6.5.1 (resp. Theorem 6.5.2) states that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ has no isolated node (resp. is connected) whp if the mean degree of class-1 nodes (that receive the smallest number $K_{1,n}$ of keys) is scaled as $(1+\epsilon)\log n$ for some $\epsilon > 0$. On the other hand, if this minimal mean degree scales as $(1-\epsilon)\log n$ for some $\epsilon > 0$, then whp $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ has an isolated node, and hence not connected. These results indicate that the minimum key ring size in the network has a significant impact on the connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$.

The importance of the minimum key ring size on connectivity can be seen more explicitly under a mild condition on the scaling, as shown in the next corollary.

Corollary 6.5.3. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$ such that $\lambda_1(n) = o(1)$ and*

$$\alpha_n \frac{K_{1,n} K_{\text{avg},n}}{P_n} \sim c \frac{\log n}{n} \tag{6.22}$$

for some $c > 0$, where $K_{\text{avg},n}$ is as defined at (6.4). Then we have the zero-one law (6.17) for absence of isolated nodes. If, in addition, the conditions (6.20) and (6.21) are satisfied, then we also have the zero-one law (6.19) for connectivity.

Proof. In view of (6.3), we see that $\lambda_1(n) = o(1)$ implies $p_{1j}(n) = o(1)$ for $j = 1, \ldots, r$. From Lemma 6.4.2, this then leads to $p_{1j}(n) \sim \frac{K_{1,n} K_{j,n}}{P_n}$, whence

$$\lambda_1(n) = \sum_{j=1}^{r} \mu_j p_{1j}(n) \sim \frac{K_{1,n} \sum_{j=1}^{r} \mu_j K_{j,n}}{P_n} = \frac{K_{1,n} K_{\text{avg},n}}{P_n}$$

Thus, the scaling conditions (6.16) and (6.22) are equivalent under $\lambda_1(n) = o(1)$ and Corollary 6.5.3 follows from Theorem 6.5.1 and Theorem 6.5.2. ■

We see from Corollary 6.5.3 that for a fixed mean number $K_{\text{avg},n}$ of keys per sensor, network connectivity is directly affected by the minimum key ring size $K_{1,n}$. For example, reducing $K_{1,n}$ by half means that the smallest α_n for which the network becomes connected whp is increased by two-fold (see Figure 6.2 for a numerical example demonstrating this phenomenon).

6.5.4 Effect of heterogeneity

To better understand the effect of heterogeneity, we would focus on the scaling condition (6.22) and compare it with the equivalent one for the homogeneous case, where all nodes receive the same number K of keys from the key pool (which induces random key graphs $\mathbb{K}(n; K, P)$). Since heterogeneity is mainly stemming from inhomogeneous random key graph, we will focus on the case of full-visibility, i.e., when $\alpha_n = 1$ for $n = 2, 3, \ldots$. To compare with the homogeneous case, we set $r = 1$, to get the corresponding scaling condition for random key graphs under full visibility. Namely, with

$$\frac{K_n^2}{P_n} \sim c\frac{\log n}{n}, \quad c > 0 \tag{6.23}$$

analogs of Theorems 6.5.1 and 6.5.2 were obtained for $\mathbb{K}(n; K, P)$ [159]. Put differently, with the scaling condition (6.23), the graph $\mathbb{K}(n; K, P)$ has no isolated node and is connected, both with high probability, if the parameters are chosen such that $c > 1$. The graph has at least one isolated node (hence, not connected) with high probability of the parameters are chosen such that $c < 1$.

Let us focus on the absence of isolated nodes property and set $P_n = n \log n$. The heterogeneity of our model offers the flexibility of having a positive fraction of the sensors, each, being assigned as few as one key per node. However, this would come at the expense of having to assign significantly larger key rings to a positive fraction of other nodes so that (6.22) still holds with $c > 1$. In particular, with $K_{1,n} = O(1)$, we must have $K_{r,n} = \Omega\left((\log n)^2\right)$ to have no isolated nodes as given by Corollary 6.5.3. Observe that (6.23) implies that setting $K_n = (1 + \epsilon) \log n$ is sufficient to ensure the absence of isolated nodes. This sheds the light on the fact that homogeneous models are more resource-efficient than their inhomogeneous counterparts, as the heterogeneity of the latter could come at the expense of requiring more resources for the graph to have no isolated nodes.

6.5.5 Comparison with related work

Our main results extend the work in [157] and [164], where authors established zero-one laws for the connectivity of a wireless sensor network secured by the heterogeneous key predistribution scheme under the *full-visibility* assumption. Although a crucial first step in the study of heterogeneous key predistribution schemes, the assumption that all pairs of sensors have a communication channel in between is not likely to hold in most practical settings. In this regard, our work extends the results in [157] and [164] to more practical wireless sensor network scenarios where the wireless connectivity of the network is taken into account. By setting $\alpha_n = 1$ for each $n = 1, 2, \ldots$ (i.e., by assuming that all links are available), our results reduce to those given in [157].

Authors in [156] (respectively, [165]) investigated the connectivity (respectively, k-connectivity) of wireless sensor networks secured by the classical Eschenauer-Gligor scheme under an independent on/off channel model. However, when the network consists of sensors with varying level of resources (e.g., computational, memory, power), and with varying level of security and connectivity requirements, it may no longer be sensible to assign the same number of keys to all sensors. Our work addresses this issue by generalizing [156] to the cases where nodes can be assigned different number of keys. When $r = 1$, i.e., when all nodes belong to the same class and receive the same number of keys, our result recovers the main result in [156].

6.5.6 Numerical results

We now present numerical results to support Theorems 6.5.1 and Theorem 6.5.2 in the finite node regime. Furthermore, we show by simulations that the on-ff channel model serves as a good approximation of the disk model. In our simulations, we fix the number of nodes at $n = 500$ and the size of the key pool at $P = 10^4$.

The first step in comparing the on-off channel model to the disk model is to propose a *matching* between Erdős-Rényi graph $\mathbb{G}(n; \alpha)$ and the random geometric graph $\mathbb{I}(n; \rho)$ in a way that leads to the same probability of link availability. In particular, consider 500 nodes distributed uniformly and independently over a folded unit square $[0, 1]^2$ with toroidal (continuous) boundary conditions. Since there are no border effects, we get

$$\mathbb{P}\left[\|\boldsymbol{x}_i - \boldsymbol{x}_j\| < \rho\right] = \pi\rho^2, \qquad i \neq j, \quad i, j = 1, \ldots, n$$

whenever $\rho < 0.5$. Thus, in order to match the two communication models we set $\alpha =$

$\pi\rho^2$. Next, we present several simulation results comparing the (empirical) probabilities that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$ are connected, respectively.

We start by considering the channel parameter $\alpha = \pi\rho^2 = 0.2$, $\alpha = \pi\rho^2 = 0.4$, $\alpha = \pi\rho^2 = 0.6$, and $\alpha = \pi\rho^2 = 0.8$, while varying the parameter K_1 (i.e., the smallest key ring size) from 5 to 35. The number of classes is fixed at 2 with $\boldsymbol{\mu} = \{0.5, 0.5\}$ and we set $K_2 = K_1 + 5$. For each parameter pair $(\boldsymbol{K}, \alpha)$ (respectively, $(\boldsymbol{K}, \pi\rho^2)$), we generate 800 independent samples of the graphs $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ (respectively, $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$) and count the number of times (out of a possible 800) that the obtained graphs i) have no isolated nodes and ii) are connected. Dividing the counts by 800, we obtain the (empirical) probabilities for the events of interest. We observed that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ is connected whenever it has no isolated nodes yielding the same empirical probability for both events. This is in parallel with the asymptotic equivalence of the two properties as implied by Theorems 6.5.1 and 6.5.2.

In Figure 6.1, we show the empirical probabilities of the connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ (represented by lines) and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$ (represented by symbols). We observe that the empirical probabilities are almost identical, supporting the claim that the on-ff channel model serves as a good approximation of the disk model under the given matching condition. Furthermore, we show the critical threshold of connectivity *predicted* by Theorem 6.5.2 by a vertical dashed line for each curve. More specifically, for a given α, the vertical dashed lines stand for the minimum integer value of K_1 that satisfies

$$\lambda_1(n) = \sum_{j=1}^{2} \mu_j \left(1 - \frac{\binom{P-K_j}{K_1}}{\binom{P}{K_1}} \right) > \frac{1}{\alpha} \frac{\log n}{n} \tag{6.24}$$

According to Theorem 6.5.2, at this critical value of K_1 the network would be connected with probability 1 as the number of nodes *tends to infinity.* We see from Figure 6.1 that even in the finite-node regime ($n = 500$), the critical value of K_1 results in a connected network with high probability.

Figure 6.2 is generated in a similar manner with Figure 6.1, this time with an eye towards understanding the impact of the minimum key ring size K_1 on network connectivity. We fix

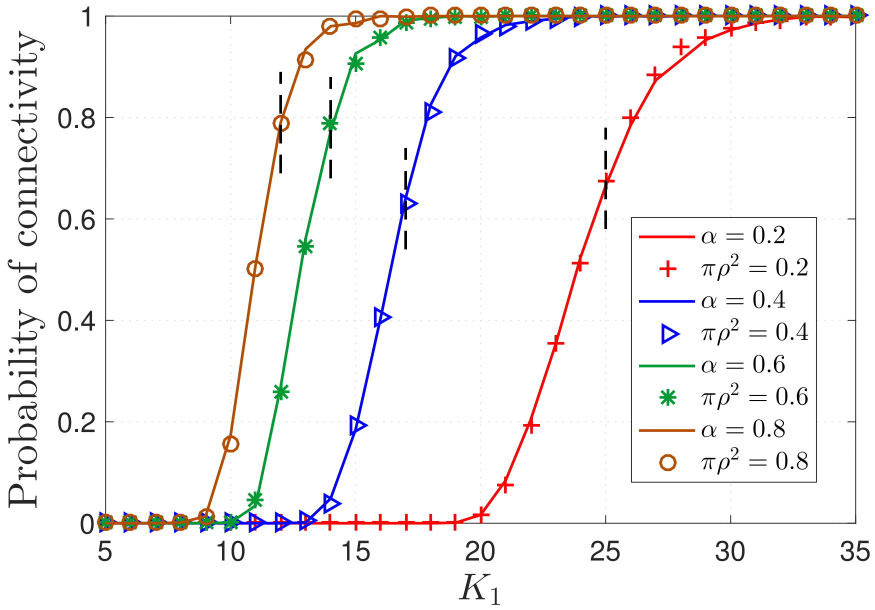


Figure 6.1: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{I}(n;\rho)$ are connected as a function of $\boldsymbol{K}$ for $\alpha = \pi\rho^2 = 0.2$, $\alpha = \pi\rho^2 = 0.4$, $\alpha = \pi\rho^2 = 0.6$, and $\alpha = \pi\rho^2 = 0.8$ with $n = 500$ and $P = 10^4$; in each case, the empirical probability value is obtained by averaging over 800 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Theorem 6.5.2.

the number of classes at 2 with $\boldsymbol{\mu} = \{0.5, 0.5\}$ and consider four different key ring sizes $\boldsymbol{K}$ each with mean 40; we consider $\boldsymbol{K} = \{10, 70\}$, $\boldsymbol{K} = \{20, 50\}$, $\boldsymbol{K} = \{30, 50\}$, and $\boldsymbol{K} = \{40, 40\}$. We compare the probability of connectivity in the resulting networks as α (respectively, $\pi\rho^2$) varies from zero to one. Although the average number of keys per sensor is kept constant in all four cases, network connectivity improves dramatically as the minimum key ring size K_1 increases; e.g., with $\alpha = \pi\rho^2 = 0.2$, the probability of connectivity is one when $K_1 = K_2 = 40$ while it drops to zero if we set $K_1 = 10$ and $K_2 = 70$ so that the mean key ring size is still 40. This confirms the observations made via Corollary 6.5.3.

Finally, we investigate the effect of the network size n on the probability of connectivity. Recall that our scaling condition is equivalent to

$$\alpha_n \frac{K_{1,n} K_{\text{avg},n}}{P} \sim c \frac{\log n}{n}$$

by virtue of Corollary 6.5.3. Thus, as we increase n for fixed P and α, the fraction $\log n/n$

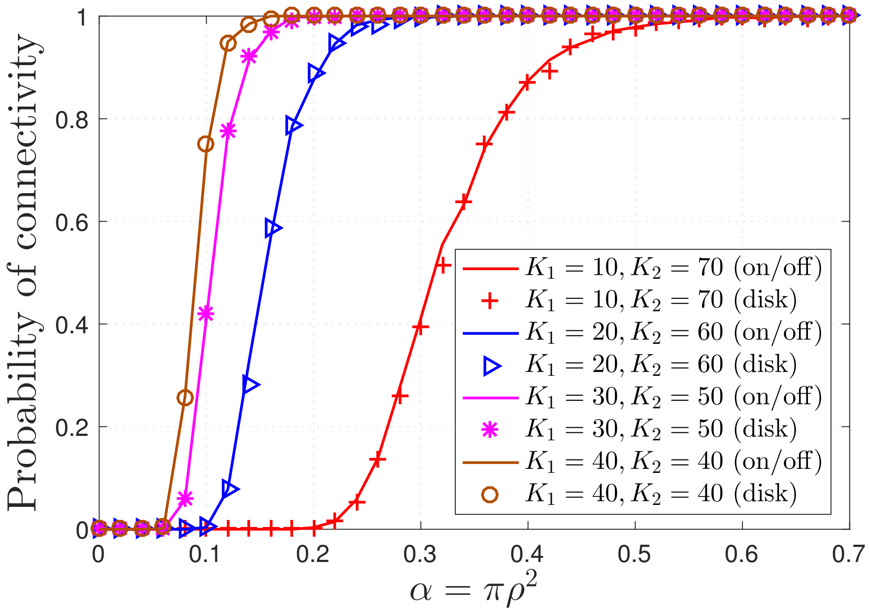


Figure 6.2: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{I}(n;\rho)$ are connected as a function of α and $\pi\rho^2$ for four choices of $\boldsymbol{K} = (K_1, K_2)$, each with the same mean.

decreases, leading to a decrease on the critical value of $K_{1,n}K_{\text{avg},n}$ needed to ensure that $c > 1$. We would also expect the probability of connectivity to exhibit a *sharper transition* between 0 and 1 as we increase n by virtue of Theorem 6.5.2. This is illustrated in Figure 6.3.

6.5.7 Additional preliminaries

Lemma 6.5.4. *Consider a scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (6.16) holds. We have*

$$c_n \frac{\log n}{n\alpha_n} \leq p_{1r}(n) \leq \frac{c_n}{\mu_r}\frac{\log n}{n\alpha_n} \tag{6.25}$$

If in addition (6.21) holds, we have

$$p_{rr}(n) = o\left(\frac{(\log n)^2}{n\alpha_n}\right). \tag{6.26}$$

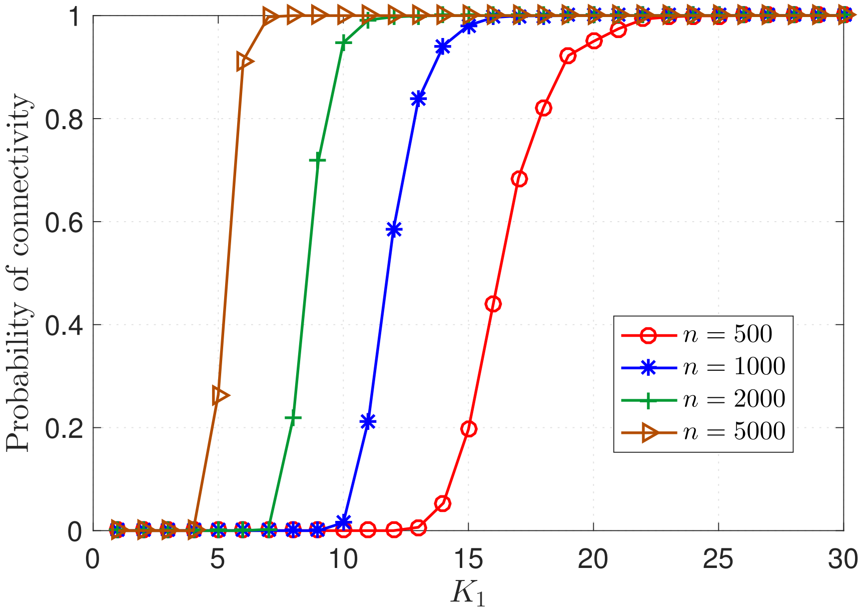


Figure 6.3: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$ is connected as a function of $\boldsymbol{K}$ for $n=500$, $n=1000$, $n=1500$, and $n=2000$. We set $K_2=K_1+5$, $\boldsymbol{\mu}=(0.5,0.5)$, $\alpha=0.4$ and $P=10^4$. In each case, the empirical probability value is obtained by averaging over 2000 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Theorem 3.2.

Proof. We know from (6.18) that

$$\lambda_1(n)=\sum_{j=1}^{r}\mu_j p_{1j}=c_n\frac{\log n}{\alpha_n n}.$$

Since p_{1j} is monotone increasing in $j=1,\ldots,r$ by virtue of (6.6), we readily obtain the bounds

$$c_n\frac{\log n}{n\alpha_n}\leq p_{1r}(n)\leq\frac{c_n}{\mu_r}\frac{\log n}{n\alpha_n}\tag{6.27}$$

which establishes (6.25).

In view of (6.27) that implies $p_{1r}(n)=\Theta(\frac{\log n}{\alpha_n n})$, we will obtain (6.26) if we show that $p_{rr}(n)=o(\log n)p_{1r}(n)$. Here this will be established by showing that

$$p_{rr}(n)\leq\max\left(2,\frac{8c_n}{\mu_r}\frac{\log n}{w_n}\right)p_{1r}(n),\quad n=2,3,\ldots\tag{6.28}$$

for some sequence w_n such that $\lim_{n\to\infty} w_n = \infty$. Fix $n = 2, 3, \ldots$. We have either $p_{1r}(n) > \frac{1}{2}$, or $p_{1r}(n) \leq \frac{1}{2}$. In the former case, it automatically holds that

$$p_{rr}(n) \leq 2p_{1r}(n) \tag{6.29}$$

by virtue of the fact that $p_{rr}(n) \leq 1$.

Assume now that $p_{1r}(n) \leq \frac{1}{2}$. We know from [159, Lemmas 7.1-7.2] that

$$1 - e^{-\frac{K_{j,n}K_{r,n}}{P_n}} \leq p_{jr}(n) \leq \frac{K_{j,n}K_{r,n}}{P_n - K_{j,n}}, \quad j = 1, \ldots, r \tag{6.30}$$

and it follows that

$$\frac{K_{1,n}K_{r,n}}{P_n} \leq \log\left(\frac{1}{1 - p_{1r}(n)}\right) \leq \log 2 < 1. \tag{6.31}$$

Using the fact that $1 - e^{-x} \geq \frac{x}{2}$ with x in $(0, 1)$, we then get

$$p_{1r}(n) \geq \frac{K_{1,n}K_{r,n}}{2P_n}. \tag{6.32}$$

In addition, using the upper bound in (6.30) with $j = r$ gives

$$p_{rr}(n) \leq \frac{K_{r,n}^2}{P_n - K_{r,n}} \leq 2\frac{K_{r,n}^2}{P_n}$$

as we invoke (6.15). Combining the last two bounds we obtain

$$\frac{p_{rr}(n)}{p_{1r}(n)} \leq 4\frac{K_{r,n}}{K_{1,n}} \tag{6.33}$$

In order to bound the term $K_{r,n}/K_{1,n}$, we recall from Lemma 6.5.5 that (6.21) implies (6.35), i.e., that $\frac{K_{1,n}^2}{P_n} = \frac{w_n}{n\alpha_n}$, for some sequence w_n satisfying $\lim_{n\to\infty} w_n = \infty$. Using this together with (6.32) and (6.27) we then get

$$\frac{K_{r,n}}{K_{1,n}} = \frac{\frac{K_{1,n}K_{r,n}}{P_n}}{\frac{K_{1,n}^2}{P_n}} \leq \frac{2p_{1r}(n)}{\frac{w_n}{n\alpha_n}} \leq \frac{2\frac{c_n}{\mu_r}\frac{\log n}{n\alpha_n}}{\frac{w_n}{n\alpha_n}} = \frac{2c_n}{\mu_r}\frac{\log n}{w_n}$$

Reporting this into (6.33) we get

$$p_{rr}(n) \leq \frac{8c_n}{\mu_r}\frac{\log n}{w_n}p_{1r}(n). \tag{6.34}$$

Combining (6.29) and (6.34), we readily obtain (6.28). ■

Lemma 6.5.5. *Under (6.21), we have*

$$\frac{K_{1,n}^2}{P_n} = \omega\left(\frac{1}{n\alpha_n}\right), \tag{6.35}$$

and

$$K_{1,n} = \omega(1). \tag{6.36}$$

Proof. It is a simple matter to check that $p_{11}(n) \leq \frac{K_{1,n}^2}{P_n - K_{1,n}}$; see [159, Proposition 7.1-7.2] for a proof. In view of (6.15) this gives $p_{11}(n) \leq 2\frac{K_{1,n}^2}{P_n}$. Thus, we have

$$\frac{K_{1,n}^2}{P_n} = \Omega\left(p_{11}(n)\right) = \omega\left(\frac{1}{n\alpha_n}\right).$$

From (6.20), (6.35), and $\alpha_n \leq 1$, we readily obtain (6.36). ■

6.5.8 Proof of Theorem 6.5.1

Establishing the one-law

The proof of Theorem 6.5.1 relies on the method of first and second moments applied to the number of isolated nodes in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$. Let $I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the total number of isolated nodes in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$, namely,

$$I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{\ell=1}^{n} \mathbf{1}[v_\ell \text{ is isolated in } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha))] \tag{6.37}$$

The method of first moment [73, Eqn. (3.10), p. 55] gives

$$1 - \mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] \leq \mathbb{P}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n) = 0]$$

It is clear that in order to establish the one-law, namely that $\lim_{n\to\infty} \mathbb{P}\left[I_n(\boldsymbol{\mu},\boldsymbol{\Theta_n}) = 0\right] = 1$, we need to show that

$$\lim_{n\to\infty} \mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] = 0. \tag{6.38}$$

Recalling (6.37), we have

$$\begin{aligned}
\mathbb{E}\left[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] &= n \sum_{i=1}^{r} \mu_i \mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha) \;\middle|\; t_1 = i\right] \\
&= n \sum_{i=1}^{r} \mu_i \mathbb{P}\left[\cap_{j=2}^{n}[v_j \nsim v_1] \mid v_1 \text{ is class i}\right] \\
&= n \sum_{i=1}^{r} \mu_i \left(\mathbb{P}\left[v_2 \nsim v_1 \mid v_1 \text{ is class i}\right]\right)^{n-1} \qquad (6.39)
\end{aligned}$$

where (6.39) follows by the independence of the rvs $\{v_j \nsim v_1\}_{j=1}^{n}$ given Σ_1. By conditioning on the class of v_2, we find

$$\begin{aligned}\mathbb{P}[v_2 \nsim v_1 \mid t_1 = i] &= \sum_{j=1}^{r} \mu_j \mathbb{P}[v_2 \nsim v_1 \mid t_1 = i, t_2 = j] \\ &= \sum_{j=1}^{r} \mu_j (1 - \alpha p_{ij}) = 1 - \Lambda_i \qquad (6.40)\end{aligned}$$

Using (6.40) in (6.39), and recalling (6.6) and (6.12), we obtain

$$\begin{aligned}\mathbb{E}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] &= n \sum_{i=1}^{r} \mu_i \left(1 - \Lambda_i(n)\right)^{n-1} \\ &\leq n \left(1 - \Lambda_1(n)\right)^{n-1} \leq e^{\log n \left(1 - c_n \frac{n-1}{n}\right)}.\end{aligned}$$

Taking the limit as n goes to infinity, we immediately get (6.38) since $\lim_{n\to\infty}(1 - c_n \frac{n-1}{n}) = 1 - c < 0$ under the enforced assumptions (with $c > 1$) and the one-law is established. ■

Establishing the zero-law

Our approach in establishing the zero-law relies on the method of second moment applied to a variable that counts the number of nodes that are class-1 and isolated. Clearly if we can show that whp there exists at least one class-1 node that is isolated under the enforced assumptions (with $c < 1$) then the zero-law would immediately follow.

Let $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the number of nodes that are class-1 and isolated in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$, and let

$$x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \mathbf{1}[t_i = 1 \cap v_i \text{ is isolated in } \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)],$$

then we have $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \sum_{i=1}^{n} x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$. By applying the method of second moments [73, Remark 3.1, p. 55] on $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, we get

$$\mathbb{P}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = 0] \leq 1 - \frac{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2}{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2]} \qquad (6.41)$$

where

$$\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \tag{6.42}$$

and

$$\begin{aligned}\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2] =& n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \\ &+ n(n-1)\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]\end{aligned} \tag{6.43}$$

by exchangeability and the binary nature of the rvs $\{x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)\}_{i=1}^n$. Using (6.42) and (6.43), we get

$$\begin{aligned}\frac{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2]}{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2} =& \frac{1}{n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]} \\ &+ \frac{n-1}{n}\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]}{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2}\end{aligned}$$

In order to establish the zero-law, we need to show that

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty, \tag{6.44}$$

and

$$\limsup_{n\to\infty} \left(\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]}{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]^2} \right) \leq 1. \tag{6.45}$$

Proposition 6.5.6. *Consider a scaling* $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ *and a scaling* $\alpha : \mathbb{N}_0 \to (0,1)$ *such that (6.16) holds with* $\lim_{n\to\infty} c_n = c > 0$*. Then, we have*

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty, \quad \textit{if } c < 1$$

Proof. We have

$$\begin{aligned}
n\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)\right] &= n\mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha) \cap t_1 = 1\right] \\
&= n\mu_1 \mathbb{P}\left[\cap_{j=2}^{n}[v_j \not\sim v_1] \;\middle|\; t_1 = 1\right] \\
&= n\mu_1 \mathbb{P}\left[v_2 \not\sim v_1 \;\middle|\; t_1 = 1\right]^{n-1} \\
&= n\mu_1 \left(\sum_{j=1}^{r} \mu_j \mathbb{P}\left[v_2 \not\sim v_1 \;\middle|\; t_1 = 1, t_2 = j\right]\right)^{n-1} \\
&= n\mu_1 \left(\sum_{j=1}^{r} \mu_j (1 - \alpha_n p_{1j})\right)^{n-1} \qquad (6.46) \\
&= n\mu_1 \left(1 - \Lambda_1(n)\right)^{n-1} = \mu_1 e^{\beta_n} \qquad (6.47)
\end{aligned}$$

where $\beta_n = \log n + (n-1)\log(1 - \Lambda_1(n))$. Recalling (6.13), we get

$$\begin{aligned}
\beta_n &= \log n - (n-1)\left(\Lambda_1(n) + \Psi(\Lambda_1(n))\right) \\
&= \log n - (n-1)\left(c_n \frac{\log n}{n} + \Psi\left(c_n \frac{\log n}{n}\right)\right) \\
&= \log n \left(1 - c_n \frac{n-1}{n}\right) \\
&\quad - (n-1)\left(c_n \frac{\log n}{n}\right)^2 \frac{\Psi\left(c_n \frac{\log n}{n}\right)}{\left(c_n \frac{\log n}{n}\right)^2} \qquad (6.48)
\end{aligned}$$

Recalling (6.14), we have

$$\lim_{n\to\infty} \frac{\Psi\left(c_n \frac{\log n}{n}\right)}{\left(c_n \frac{\log n}{n}\right)^2} = \frac{1}{2} \qquad (6.49)$$

since $c_n \frac{\log n}{n} = o(1)$. Thus, $\beta_n = \log n\left(1 - c_n \frac{n-1}{n}\right) - o(1)$. Using (6.47), (6.48), (6.49), and letting n go to infinity, we get

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty$$

whenever $\lim_{n\to\infty} c_n = c < 1$. □

Proposition 6.5.7. *Consider a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\alpha : \mathbb{N}_0 \to (0,1)$ such that (6.16) holds with $\lim_{n\to\infty} c_n = c > 0$. Then, we have (6.45) if $c < 1$.*

Proof. Consider fixed $\boldsymbol{\Theta}$.

$$\begin{aligned}\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\right] &= \mathbb{E}\left[\mathbf{1}[v_1 \text{ is isolated }, v_2 \text{ is isolated} \cap t_1 = 1, t_2 = 1]\right] \\ &= \mu_1^2 \mathbb{E}\left[\mathbf{1}[v_1 \text{ is isolated }, v_2 \text{ is isolated}] \;\middle|\; t_1 = 1, t_2 = 1\right] \\ &= \mu_1^2 \mathbb{E}\left[\mathbf{1}[v_1 \nsim v_2] \prod_{m=3}^{n} \mathbf{1}[v_m \nsim v_1, v_m \nsim v_2] \;\middle|\; t_1 = t_2 = 1\right]\end{aligned}$$

Now we condition on Σ_1 and Σ_2 and note that i) Σ_1 and Σ_2 determine t_1 and t_2; and ii) the events $[v_1 \nsim v_2], \{[v_m \nsim v_1 \cap v_m \nsim v_2]\}_{m=3}^{n}$ are mutually independent given Σ_1 and Σ_2. Thus, we have

$$\begin{aligned}\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})] = \mu_1^2 \mathbb{E}\Bigg[&\mathbb{P}\left[v_1 \nsim v_2 \;\middle|\; \Sigma_1, \Sigma_2\right] \cdot \\ &\prod_{m=3}^{n} \mathbb{P}\left[v_m \nsim v_1 \cap v_m \nsim v_2 \;\middle|\; \Sigma_1, \Sigma_2\right] \;\Bigg|\; t_1 = t_2 = 1\Bigg]\end{aligned} \tag{6.50}$$

Define the $\{0,1\}$-valued rv $u(\boldsymbol{\theta})$ by

$$u(\boldsymbol{\theta}) := \mathbf{1}[\Sigma_1 \cap \Sigma_2 \neq \emptyset]. \tag{6.51}$$

Recalling (6.75), (6.50) gives

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})] = \mu_1^2 \mathbb{E}\left[(1-\alpha)^{u(\boldsymbol{\theta})} \prod_{m=3}^{n} \frac{\binom{P - \left|\cup_{i\in\nu_{2,m}(\alpha)}\Sigma_i\right|}{|\Sigma_m|}}{\binom{P}{|\Sigma_m|}} \;\middle|\; t_1 = t_2 = 1\right]$$

Conditioned on $u(\boldsymbol{\theta}) = 0$ and v_1, v_2 being class-1, we have

$$\left|\cup_{i\in\nu_{2,m}(\alpha)}\Sigma_i\right| = |\nu_{2,m}(\alpha)|\, K_1.$$

Also, we have

$$\mathbb{P}[u(\boldsymbol{\theta_n}) = 0 \mid t_1 = t_2 = 1] = 1 - p_{11}.$$

Thus, we get

$$\begin{aligned}
\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta})\ \mathbf{1}[u(\boldsymbol{\theta}) = 0]] &= \mu_1^2(1 - p_{11})\mathbb{E}\left[\prod_{m=3}^{n} \frac{\binom{P-|\nu_{2,m}(\alpha)K_1|}{|\Sigma_m|}}{\binom{P}{|\Sigma_m|}}\right] \\
&= \mu_1^2(1 - p_{11})\mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\alpha)|K_1}{|\Sigma_3|}}{\binom{P}{|\Sigma_3|}}\right]^{n-2} \\
&= \mu_1^2(1 - p_{11})\left(\sum_{j=1}^{r} \mu_j \mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\alpha)|K_1}{|\Sigma_3|}}{\binom{P}{|\Sigma_3|}}\ \middle|\ t_3 = j\right]\right)^{n-2} \\
&= \mu_1^2(1 - p_{11})\left(\sum_{j=1}^{r} \mu_j \mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\alpha)|K_1}{K_j}}{\binom{P}{K_j}}\right]\right)^{n-2} \\
&\leq \mu_1^2(1 - p_{11})\mathbb{E}\left[\sum_{j=1}^{r} \mu_j \left(\frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}}\right)^{|\nu_{2,3}(\alpha)|}\right]^{n-2}
\end{aligned}$$

where we use (6.9) in the last step.

Now, let $Z(\boldsymbol{\theta})$ denote a rv that takes the value

$$\frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}} \quad \text{with probability} \quad \mu_j, \quad j = 1, \ldots, r. \tag{6.52}$$

In other words, $Z(\boldsymbol{\theta}) = 1 - p_{1j}$ with probability μ_j so that $\mathbb{E}[Z(\boldsymbol{\theta})] = 1 - \lambda_1$. Then,

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta})\mathbf{1}\left[u(\boldsymbol{\theta}) = 0\right]] \leq \mu_1^2(1 - p_{11})\mathbb{E}\left[Z(\boldsymbol{\theta})^{|\nu_{2,3}(\alpha)|}\right]^{n-2} \tag{6.53}$$

Under the independent on-ff channel model, we have that $|\nu_{2,3}(\alpha)|$ is a Binomial rv, i.e.,

$|\nu_{2,3}(\alpha)| =_{st} \mathrm{Bin}(2, \alpha)$. Hence,

$$\begin{aligned}\mu_1^2(1-p_{11})\mathbb{E}\left[Z(\boldsymbol{\theta})^{|\nu_{2,3}(\alpha)|}\right]^{n-2} &= \mathbb{E}\left[\sum_{i=0}^{2}\binom{2}{i}\alpha^i(1-\alpha)^{2-i}Z(\boldsymbol{\theta})^i\right]^{n-2} \\ &= \mu_1^2(1-p_{11})\mathbb{E}\left[(1-\alpha)^2 + 2\alpha(1-\alpha)Z(\boldsymbol{\theta}) + \alpha^2 Z(\boldsymbol{\theta})^2\right]^{n-2}\end{aligned} \tag{6.54}$$

Conditioning on $u(\boldsymbol{\theta}) = 1$ and $t_1 = t_2 = 1$, we have

$$|\cup_{i\in\nu_{2,m}(\alpha)}\Sigma_i| = \begin{cases} 0 & \text{if } |\nu_{2,m}(\alpha)| = 0 \\ K_1 & \text{if } |\nu_{2,m}(\alpha)| = 1 \\ 2K_1 - |\Sigma_1 \cap \Sigma_2| & \text{if } |\nu_{2,m}(\alpha)| = 2 \end{cases}$$

and by a crude bounding argument, we have

$$|\cup_{i\in\nu_{2,m}(\alpha)}\Sigma_i| \geq K_1\mathbf{1}[|\nu_{2,m}(\alpha)| > 0] \tag{6.55}$$

Using (6.55) and recalling the analysis for $\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta}) = 0]]$, we obtain

$$\begin{aligned}\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta}) = 1]] &\leq \mu_1^2 p_{11}(1-\alpha)\mathbb{E}\left[Z(\boldsymbol{\theta})^{\mathbf{1}[|\nu_{2,3}(\alpha)|>0]}\right]^{n-2} \\ &= \mu_1^2 p_{11}(1-\alpha)\mathbb{E}\left[(1-\alpha)^2 + \left(1-(1-\alpha)^2\right)Z_n\right]^{n-2}\end{aligned} \tag{6.56}$$

Combining (6.53), (6.54), and (6.56), we get

$$\begin{aligned}&\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})] \\ &= \mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\left(\mathbf{1}[u(\boldsymbol{\theta}) = 0] + \mathbf{1}[u(\boldsymbol{\theta}) = 1]\right)] \\ &\leq \mu_1^2(1-p_{11})\left((1-\alpha)^2 + 2\alpha(1-\alpha)\mathbb{E}[Z(\boldsymbol{\theta})] + \alpha^2\mathbb{E}\left[Z(\boldsymbol{\theta})^2\right]\right)^{n-2} \\ &\quad + \mu_1^2 p_{11}(1-\alpha)\left((1-\alpha)^2 + \left(1-(1-\alpha)^2\right)\mathbb{E}[Z(\boldsymbol{\theta})]\right)^{n-2}\end{aligned} \tag{6.57}$$

It is clear from (6.46) and the definition of $Z(\boldsymbol{\theta})$ that

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})] = \mu_1 \left(\sum_{j=1}^{r} \mu_j(1-\alpha p_{1j})\right)^{n-1} = \mu_1 \left((1-\alpha) + \alpha \mathbb{E}\left[Z(\boldsymbol{\theta})\right]\right)^{n-1} \tag{6.58}$$

Combining (6.57) and (6.58), we get

$$\begin{aligned}\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})]}{\mathbb{E}[x_{n,1}(\boldsymbol{\theta})]^2} &\leq (1-p_{11})\frac{\left((1-\alpha)^2 + 2\alpha(1-\alpha)\mathbb{E}[Z(\boldsymbol{\theta})] + \alpha^2\mathbb{E}[Z(\boldsymbol{\theta})^2]\right)^{n-2}}{\left((1-\alpha)+\alpha\mathbb{E}\left[Z(\boldsymbol{\theta})\right]\right)^{2(n-1)}} \\ &\quad + p_{11}\frac{\left((1-\alpha)^2 + \left(1-(1-\alpha)^2\right)\mathbb{E}[Z(\boldsymbol{\theta})]\right)^{n-2}}{\left((1-\alpha)+\alpha\mathbb{E}\left[Z(\boldsymbol{\theta})\right]\right)^{2(n-1)}} \\ &:= A + B \end{aligned} \tag{6.59}$$

where we use the fact that $1-\alpha \leq 1$.

We now consider a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$ as stated in Proposition 6.5.7 and bound the terms A and B in turn. Our goal is to show that

$$\limsup_{n\to\infty}(A+B) \leq 1. \tag{6.60}$$

First, we write $\mathbb{E}[Z(\boldsymbol{\theta}_n)^2] = \mathbb{E}[Z(\boldsymbol{\theta}_n)]^2 + \mathrm{var}[Z(\boldsymbol{\theta}_n)]$, where $\mathrm{var}[Z(\boldsymbol{\theta}_n)]$ can be bounded by the Popoviciu's inequality [74, p. 9] as follows (see Proposition 6.4.4)

$$\mathrm{var}[Z(\boldsymbol{\theta}_n)] \leq \frac{1}{4}\left(p_{1r}(n)\right)^2.$$

Then, we get from the scaling condition (6.18) and (6.27) that

$$\mathbb{E}[Z(\boldsymbol{\theta}_n)^2] \leq \mathbb{E}[Z(\boldsymbol{\theta}_n)]^2 + \frac{1}{4}\left(\frac{c_n}{\mu_r}\frac{\log n}{n\alpha_n}\right)^2$$

Reporting this into (6.59) we get

$$\begin{aligned}
A &\leq (1-p_{11})\frac{\left(((1-\alpha_n)+\alpha_n\mathbb{E}[Z(\boldsymbol{\theta}_n)])^2+\left(\frac{c_n}{2\mu_r}\frac{\log n}{n}\right)^2\right)^{n-2}}{((1-\alpha_n)+\alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n)\right])^{2(n-1)}} \\
&= (1+o(1))(1-p_{11})\left(1+\left(\frac{\frac{c_n}{2\mu_r}\frac{\log n}{n}}{1-\alpha_n+\alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n\right]}\right)^2\right)^{n-2}
\end{aligned}$$

where we used the fact that

$$((1-\alpha_n)+\alpha_n\mathbb{E}[Z(\boldsymbol{\theta}_n)])^2 = (1-\alpha_n\lambda_1(n))^2 = 1-o(1) \tag{6.61}$$

since $\alpha_n\lambda_1(n) = c_n\log n/n$. Finally, we have

$$\left(1+\left(\frac{\frac{c_n}{2\mu_r}\frac{\log n}{n}}{1-\alpha_n+\alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n\right]}\right)^2\right)^{n-2} \leq \exp\left\{n\left(\frac{\frac{c_n}{2\mu_r}\frac{\log n}{n}}{1-c_n\frac{\log n}{n}}\right)^2\right\} = o(1)$$

since $\lim_{n\to\infty}c_n = c > 0$ and $\mu_r > 0$. Thus, we obtain the bound

$$A \leq (1-p_{11})\left(1+o(1)\right). \tag{6.62}$$

We now consider the second term in (6.59). Recall (6.61) and that $\mathbb{E}\left[Z(\boldsymbol{\theta}_n)\right] = 1-\lambda_1(n) = 1-c_n\log n/n$. We have

$$\begin{aligned}
B &= \frac{p_{11}}{\left(1-\alpha_n+\alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n)\right]\right)^2}\cdot\left(1+\frac{\alpha_n^2\mathbb{E}[Z(\boldsymbol{\theta}_n)](1-\mathbb{E}[Z(\boldsymbol{\theta}_n)])}{\left(1-\alpha_n+\alpha_n\mathbb{E}\left[Z(\boldsymbol{\theta}_n)\right]\right)^2}\right)^{n-2} \\
&\leq p_{11}(1+o(1))\exp\left\{n\frac{\alpha_n^2c_n\frac{\log n}{n\alpha_n}(1-c_n\frac{\log n}{n\alpha_n})}{(1-c_n\frac{\log n}{n})^2}\right\} \\
&\leq p_{11}(1+o(1))\exp\left\{\frac{c_n\alpha_n\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}\right\}
\end{aligned} \tag{6.63}$$

We will now establish the desired result (6.60) by using (6.62) and (6.63). Our approach is based on the subsubsequence principle [73, p. 12] and considering the cases $\lim_{n\to\infty}\alpha_n\log n = 0$

and $\lim_{n\to\infty} \alpha_n \log n \in (0, \infty]$ separately.

Assume that $\lim_{n\to\infty} \alpha_n \log n = 0$ From (6.63) we get $B \leq (1 + o(1))p_{11}$ and upon using (6.62) we see that $A + B \leq (1 + o(1))$ establishing (6.60) along subsequences with $\lim_{n\to\infty} \alpha_n \log n = 0$.

Assume that $\lim_{n\to\infty} \alpha_n \log n \in (0, \infty]$ Since p_{1j} is monotonically increasing in $j = 1, \ldots, r$ (see (6.6)), we have

$$\lambda_1 = \sum_{j=1}^{r} \mu_j p_{1j} \geq p_{11} \sum_{j=1}^{r} \mu_j = p_{11}$$

Thus, $p_{11} \leq \lambda_1(n) = c_n \log n/(\alpha_n n)$. Then, (6.63) gives

$$\begin{aligned} B &\leq (1 + o(1)) \frac{c_n \log n}{\alpha_n n} \exp\left\{ \frac{c_n \alpha_n \log n}{(1 - c_n \log n/n)^2} \right\} \\ &= (1 + o(1)) \frac{c_n (\log n)^2}{\alpha_n \log n} n^{-1 + \frac{c_n \alpha_n}{(1 - c_n \log n/n)^2}} \\ &= o(1) \end{aligned}$$

since $\lim_{n\to\infty} \alpha_n \log n > 0$ along this subsequence and

$$\lim_{n\to\infty} -1 + \frac{c_n \alpha_n}{(1 - c_n \log n/n)^2} < 0$$

given that $\lim_{n\to\infty} c_n = c < 1$. From (6.62) and the fact that $p_{11} \leq 1$, we have $A \leq 1 + o(1)$, and (6.60) follows.

The two cases considered cover all the possibilities for the limit of $\alpha_n \log n$. By virtue of the subsubsequence principle [73, p. 12], we get (6.60) without any condition on the sequence $\alpha_n \log n$; i.e., we obtain (6.60) even when the sequence $\alpha_n \log n$ does not have a limit! ■

Collectively, Proposition 6.5.6 and Proposition 6.5.7 establish (6.44) and (6.45) respectively, which in turn establish the zero-law of Theorem 6.5.1.

6.5.9 Proof of Theorem 6.5.2

Let $C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the event that the graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ is connected, and with a slight abuse of notation, let $I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the event that the graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ has no isolated nodes. It is clear that if a random graph is connected then it does not have any isolated node, hence

$$C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \subseteq I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$$

and we get

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \leq \mathbb{P}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \tag{6.64}$$

and

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c] = \mathbb{P}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c] + \mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]. \tag{6.65}$$

In view of (6.64), we obtain the zero-law for connectivity, i.e., that

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha) \text{ is connected}] = 0 \quad \text{if} \quad c < 1,$$

immediately from the zero-law part of Theorem 6.5.1, i.e., from that $\lim_{n\to\infty} \mathbb{P}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = 0$ if $c < 1$. It remains to establish the one-law for connectivity. In the remainder of this section, we assume that (6.16) holds for some $c > 1$. From Theorem 6.5.1 and (6.65), we see that the one-law for connectivity, i.e., that

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha) \text{ is connected}] = 1 \quad \text{if} \quad c > 1,$$

will follow if we show that

$$\lim_{n\to\infty} \mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = 0. \tag{6.66}$$

Our approach will be to find a suitable upper bound for (6.66) and prove that it goes to zero as n goes to infinity with $c > 1$.

We now work towards deriving an upper bound for (6.66); then we will show that the bound goes to zero as n gets large. Define the event $E_n(\boldsymbol{\mu}, \boldsymbol{\theta}, \boldsymbol{X})$ via

$$E_n(\boldsymbol{\mu}, \boldsymbol{\theta}, \boldsymbol{X}) := \cup_{S \subseteq \mathcal{N}: |S| \geq 1} \left[| \cup_{i \in S} \Sigma_i | \leq X_{|S|} \right]$$

where $\mathcal{N} = \{1, \ldots, n\}$ and $\boldsymbol{X} = [X_1 \ \cdots \ X_n]$ is an n-dimensional array of integers. Let

$$L_n := \min \left(\left\lfloor \frac{P}{K_1} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor \right) \tag{6.67}$$

and

$$X_\ell = \begin{cases} \lfloor \beta \ell K_1 \rfloor & \ell = 1, \ldots, L_n \\ \lfloor \gamma P \rfloor & \ell = L_n + 1, \ldots, n \end{cases} \tag{6.68}$$

for some β and γ in $(0, \frac{1}{2})$ that will be specified later. In words, $E_n(\boldsymbol{\mu}, \boldsymbol{\theta}, \boldsymbol{X})$ denotes the event that there exists $\ell = 1, \ldots, n$ such that the number of unique keys stored by at least one subset of ℓ sensors is less than $\lfloor \beta \ell K_1 \rfloor \mathbf{1}[\ell \leq L_n] + \lfloor \gamma P \rfloor \mathbf{1}[\ell > L_n]$. Using a crude bound, we get

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \leq \mathbb{P}[E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)] + \mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \tag{6.69}$$

Thus, (6.66) will be established by showing that

$$\lim_{n \to \infty} \mathbb{P}[E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)] = 0, \tag{6.70}$$

and

$$\lim_{n \to \infty} \mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0 \tag{6.71}$$

Proposition 6.5.8. *Consider scalings* $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ *and* $\alpha : \mathbb{N}_0 \to (0, 1)$ *such* *that (6.16) holds for some $c > 1$, (6.20) and (6.21) hold. Then, we have (6.70) where $\boldsymbol{X}_n$ is as specified in (6.68), $\beta \in (0, \frac{1}{2})$ and $\gamma \in (0, \frac{1}{2})$ are selected such that*

$$\max\left(2\beta\sigma, \beta\left(\frac{e^2}{\sigma}\right)^{\frac{\beta}{1-2\beta}}\right) < 1 \tag{6.72}$$

$$\max\left(2\left(\sqrt{\gamma}\left(\frac{e}{\gamma}\right)^{\gamma}\right)^{\sigma}, \sqrt{\gamma}\left(\frac{e}{\gamma}\right)^{\gamma}\right) < 1 \tag{6.73}$$

Proof. The proof is similar to [157, Proposition 7.2]. Results only require conditions (6.20) and $K_{1,n} = \omega(1)$ to hold. The latter condition is clearly established in Lemma 6.5.5. □

The rest of the chapter is devoted to establishing (6.71) under the enforced assumptions on the scalings and with $\boldsymbol{X}_n$ as specified in (6.68), $\beta \in (0, \frac{1}{2})$ selected small enough such that (6.72) holds, and $\gamma \in (0, \frac{1}{2})$ selected small enough such that (6.73) holds. We denote by $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)(S)$ a subgraph of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ whose vertices are restricted to the set S. Define the events

$$C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) := [\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)(S) \text{ is connected}]$$
$$B_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) := [\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)(S) \text{ is isolated}]$$
$$A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) := C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) \cap B_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)$$

In other words, $A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)$ encodes the event that $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)(S)$ is a *component*, i.e., a connected subgraph that is isolated from the rest of the graph. The key observation is that a graph is *not* connected if and only if it has a component on vertices S with $1 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor$; note that if vertices S form a component then so do vertices $\mathcal{N} - S$. The event $I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ eliminates the possibility of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)(S)$ containing a component of size one (i.e., an isolated node), whence we have

$$C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \subseteq \cup_{S \in \mathcal{N}: 2 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor} A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)$$

and the conclusion

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \leq \sum_{S \in \mathcal{N}: 2 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor} \mathbb{P}[A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)]$$

follows. By exchangeability, we get

$$\begin{aligned} &\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \\ &\leq \sum_{\ell=2}^{\left\lfloor \frac{n}{2} \right\rfloor} \left(\sum_{S \in \mathcal{N}_{n,\ell}} \mathbb{P}[A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \right) \\ &= \sum_{\ell=2}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \end{aligned} \tag{6.74}$$

where $\mathcal{N}_{n,\ell}$ denotes the collection of all subsets of $\{1, \ldots, n\}$ with exactly ℓ elements, and $A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denotes the event that the set $\{1, \ldots, \ell\}$ of nodes form a component. As before we have $A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, where $C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denotes the event that $\{1, \ldots, \ell\}$ is connected and $B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denotes the event that $\{1, \ldots, \ell\}$ is isolated from the rest of the graph.

Next, with $\ell = 1, 2, \ldots, n-1$, define $\nu_{\ell,j}(\alpha)$ by

$$\nu_{\ell,j}(\alpha) := \{i = 1, 2, \ldots, \ell : B_{ij}(\alpha) = 1\} \tag{6.75}$$

for each $j = \ell + 1, \ldots, n$. Namely, $\nu_{\ell,j}(\alpha)$ is the set of nodes in $\{v_1, \ldots, v_\ell\}$ that are adjacent to node v_j in the Erdős-Rényi graph $\mathbb{G}(n;\alpha_n)$. For each $\ell = 1, \ldots, n-1$, we have

$$B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \bigcap_{m=\ell+1}^{n} \left[\left(\cup_{i \in \nu_{\ell,m}(\alpha_n)} \Sigma_i \right) \cap \Sigma_m = \emptyset \right].$$

We have

$$\begin{aligned}
\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \;\middle|\; \Sigma_1, \ldots, \Sigma_\ell \right] &= \mathbb{E}\left[\prod_{m=\ell+1}^{n} \frac{\binom{P - |\cup_{i \in \nu_{\ell,m}(\alpha_n)} \Sigma_i|}{|\Sigma_m|}}{\binom{P}{|\Sigma_m|}} \;\middle|\; \Sigma_1, \ldots, \Sigma_\ell \right] \\
&= \prod_{m=\ell+1}^{n} \mathbb{E}\left[\frac{\binom{P - |\cup_{i \in \nu_{\ell,m}(\alpha_n)} \Sigma_i|}{|\Sigma_m|}}{\binom{P}{|\Sigma_m|}} \;\middle|\; \Sigma_1, \ldots, \Sigma_\ell \right] \\
&= \mathbb{E}\left[\frac{\binom{P - |\cup_{i \in \nu_{\ell}(\alpha_n)} \Sigma_i|}{|\Sigma|}}{\binom{P}{|\Sigma|}} \;\middle|\; \Sigma_1, \ldots, \Sigma_\ell \right]^{n-\ell} \qquad (6.76)
\end{aligned}$$

noting the fact that the collection of rvs $\{\nu_{\ell,m}, \Sigma_m : m = \ell+1, \ldots, n\}$ are mutually independent *and* identically distributed. Here, $\nu_\ell(\alpha_n)$ denotes a generic rv distributed identically with $\nu_{\ell,m}(\alpha_n)$ for any $m = \ell+1, \ldots, n$. Similarly, $|\Sigma|$ denotes a rv that takes the value K_j with probability μ_j.

We will leverage the expression (6.76) in (6.74) in the following manner. Note that on the event $E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c$, we have

$$\left| \cup_{i \in \nu_\ell(\alpha_n)} \Sigma_i \right| \geq \left(X_{n,\nu_\ell(\alpha_n)} + 1 \right) \mathbf{1}[|\nu_\ell(\alpha_n)| > 0] \qquad (6.77)$$

while the crude bound

$$\left| \cup_{i \in \nu_\ell(\alpha_n)} \Sigma_i \right| \geq K_{1,n} \mathbf{1}[|\nu_\ell(\alpha_n)| > 0] \qquad (6.78)$$

always holds. These bounds lead to

$$\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c \;\middle|\; \Sigma_1, \ldots, \Sigma_\ell \right] \leq \mathbb{E}\left[\frac{\binom{P - \max(K_{1,n}, X_{n,\nu_\ell(\alpha_n)} + 1) \mathbf{1}[|\nu_\ell(\alpha_n)| > 0]}{|\Sigma|}}{\binom{P}{|\Sigma|}} \right]^{n-\ell} \qquad (6.79)$$

Conditioning on $\Sigma_1, \ldots, \Sigma_\ell$ and $\{B_{ij}(\alpha_n), 1 \leq i < j \leq \ell\}$, we get

$$\begin{aligned}
&\mathbb{P}\left[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c\right] \\
&= \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \cdot \mathbf{1}[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \,\middle|\, \begin{array}{c} \Sigma_1, \ldots, \Sigma_\ell \\ B_{ij}(\alpha_n), 1 \leq i < j \leq \ell \end{array}\right]\right] \\
&\leq \mathbb{E}\left[\mathbf{1}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \cdot \mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c \,\middle|\, \Sigma_1, \ldots, \Sigma_\ell\right]\right] \qquad (6.80)
\end{aligned}$$

since $C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ is fully determined by $\Sigma_1, \ldots, \Sigma_\ell$ and $\{B_{ij}(\alpha_n), 1 \leq i < j \leq \ell\}$, and $B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ and $E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)$ are independent from $\{B_{ij}(\alpha_n), 1 \leq i, j \leq \ell\}$.

The next result establishes bounds for both terms at (6.80).

Lemma 6.5.9. *Consider a distribution $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_r)$, integers $K_1 \leq \cdots \leq K_r \leq P/2$, and $\alpha \in (0, 1)$. With $\boldsymbol{X}_n$ as specified in (6.68), $\beta \in (0, \frac{1}{2})$ and $\gamma \in (0, \frac{1}{2})$, we have*

$$\mathbb{P}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta})] \leq \min\left\{1, \ell^{\ell-2}\left(\alpha p_{rr}\right)^{\ell-1}\right\} \qquad (6.81)$$

and

$$\begin{aligned}
&\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c \,\middle|\, \Sigma_1, \ldots, \Sigma_\ell\right] \\
&\leq \min\left\{1 - \alpha\lambda_1, \min\{1 - \mu_r + \mu_r e^{-\alpha p_{1r}\beta\ell}, e^{-\alpha p_{11}\beta\ell}\} + e^{-\gamma K_1}\mathbf{1}[\ell > L_n]\right\} \qquad (6.82)
\end{aligned}$$

The proof of Lemma 6.5.9 is given in Section 6.5.10. Note that as we report (6.82) back in (6.80), we get

$$\begin{aligned}
&\mathbb{P}\left[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c\right] \\
&\leq \mathbb{P}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta})] \cdot \min\left\{1 - \alpha\lambda_1, \min\{1 - \mu_r + \mu_r e^{-\alpha p_{1r}\beta\ell}, e^{-\alpha p_{11}\beta\ell}\} + e^{-\gamma K_1}\mathbf{1}[\ell > L_n]\right\} \qquad (6.83)
\end{aligned}$$

Our proof of (6.71) will be completed (see (6.74)) upon establishing

$$\lim_{n\to\infty}\sum_{\ell=2}^{\left\lfloor\frac{n}{2}\right\rfloor}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c]=0 \tag{6.84}$$

by means of (6.83), (6.81), and (6.82). These steps are taken in Section 6.5.11.

6.5.10 Establishing Lemma 6.5.9

The bounds given at Lemma 6.5.9 are valid irrespective of how the parameters involved scale with n. Thus, we consider fixed $\boldsymbol{\Theta}$ with constraints given in the statement of Lemma 6.5.9.

We first establish (6.82) starting with the first bound. Recall that $|\nu_\ell(\alpha)|$ is a Binomial rv with ℓ trials and success probability α. Recall also the rv $Z(\boldsymbol{\theta})$ defined at (6.52). Using a crude bound and then (6.9) we get

$$\begin{aligned}\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c\;\middle|\;\Sigma_1,\ldots,\Sigma_\ell\right] &\le \mathbb{E}\left[\frac{\binom{P-\max(K_1,X_{n,\nu_\ell(\alpha)}+1)\mathbf{1}[|\nu_\ell(\alpha)|>0]}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]\\ &\le \mathbb{E}\left[\frac{\binom{P-K_1\mathbf{1}[|\nu_\ell(\alpha)|>0]}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]\\ &\le \mathbb{E}\left[Z(\boldsymbol{\theta})^{\mathbf{1}[|\nu_\ell(\alpha)|>0]}\right]\\ &= (1-\alpha)^\ell+\left(1-(1-\alpha)^\ell\right)\mathbb{E}[Z(\boldsymbol{\theta})]\\ &\le 1-\alpha+\alpha\mathbb{E}\left[Z(\boldsymbol{\theta})\right]=1-\alpha\lambda_1(n). \end{aligned}\tag{6.85}$$

upon noting that $\mathbb{E}\left[Z(\boldsymbol{\theta})\right]=1-\lambda_1\le 1$.

Next, consider range $\ell=1,\ldots,L_n$, where we have

$$\left(X_{n,\nu_\ell(\alpha)}+1\right)\mathbf{1}[|\nu_\ell(\alpha)|>0]\ge\lceil\beta\,|\nu_\ell(\alpha)|\,K_1\rceil$$

Recalling (6.9), we get

$$\begin{aligned}
\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c \,\middle|\, \Sigma_1,\ldots,\Sigma_\ell\right] &\leq \mathbb{E}\left[\frac{\binom{P-\max(K_1,X_{n,\nu_\ell(\alpha)}+1)\mathbf{1}[|\nu_\ell(\alpha)|>0]}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \\
&\leq \mathbb{E}\left[\frac{\binom{P-\beta|\nu_\ell(\alpha)|K_1}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \\
&= \mathbb{E}\left[Z(\boldsymbol{\theta})^{\beta|\nu_\ell(\alpha)|}\right] \\
&= \mathbb{E}\left[\sum_{j=0}^{\ell}\binom{\ell}{j}\alpha^j(1-\alpha)^{\ell-j}Z(\boldsymbol{\theta})^{\beta j}\right] \\
&= \mathbb{E}\left[\left(1-\alpha\left(1-Z(\boldsymbol{\theta})^{\beta}\right)\right)^{\ell}\right] \\
&\leq \mathbb{E}\left[\left(1-\alpha\beta\left(1-Z(\boldsymbol{\theta})\right)\right)^{\ell}\right] \leq \mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\right]
\end{aligned} \tag{6.86}$$

using the fact that $1-Z(\boldsymbol{\theta})^{\beta}\geq\beta(1-Z(\boldsymbol{\theta}))$ with $Z(\boldsymbol{\theta})\leq 1$ and $0\leq\beta\leq 1$; a proof is available at [156, Lemma 5.2]. On the range $\ell = L_n+1,\ldots,\left\lfloor\frac{n}{2}\right\rfloor$, $|\nu_\ell(\alpha)|$ can be less than or greater than L_n. In the latter case, we have

$$\max(K_1, X_{n,\nu_\ell(\alpha)}+1)\mathbf{1}[|\nu_\ell(\alpha)|>0]\geq\lfloor\gamma P\rfloor+1$$

Using (6.86) and the fact that (see [155, Lemma 5.4.1] for a proof)

$$\binom{P-K_1}{K_2}\Big/\binom{P}{K_2}\leq e^{-\frac{K_2}{P}K_1}$$

for $K_1+K_2\leq P$, we have

$$\begin{aligned}
\mathbb{E}\left[\frac{\binom{P-\max(K_1,X_{n,\nu_\ell(\alpha)}+1)\mathbf{1}[|\nu_\ell(\alpha)|>0]}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] &\leq \mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\mathbf{1}[|\nu_\ell(\alpha)|\leq L_n]\right] \\
&\quad + \mathbb{E}\left[e^{-\frac{|\Sigma|}{P}(\lfloor\gamma P\rfloor+1)}\mathbf{1}[|\nu_\ell(\alpha)|>L_n]\right] \\
&\leq \mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\right]+e^{-\gamma K_1}\mathbf{1}[\ell>L_n]
\end{aligned} \tag{6.87}$$

by virtue of the fact that $|\Sigma| \geq K_1$.

Finally, we get (6.82) from (6.85) and (6.87) by noting that

$$\mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\right] = \sum_{j=1}^{r} \mu_j e^{-\alpha p_{1j}\beta\ell} \leq (1-\mu_r) + \mu_r e^{-\alpha p_{1r}\beta\ell}$$

and that

$$\mathbb{E}\left[e^{-\alpha(1-Z(\boldsymbol{\theta}))\beta\ell}\right] = \sum_{j=1}^{r} \mu_j e^{-\alpha p_{1j}\beta\ell} \leq e^{-\alpha p_{11}\beta\ell} \tag{6.88}$$

The last step used the fact that p_{ij} is monotone increasing in both i and j.

Next, we establish (6.81). This is a version of a fairly standard bound derived previously for various other random graph models including ER graphs [18], random key graphs [159], and random K-out graphs [151,154]. The proof is very similar to that of [157, Proposition 9.1] and [156, Lemma 10.2]. We give it below for completeness.

Let $\mathbb{G}_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ denote the subgraph of $\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ induced on the vertices $\{v_1,\ldots,v_\ell\}$. $\mathbb{G}_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ is connected if and only if it contains a spanning tree; i.e., we have

$$C_\ell(\boldsymbol{\mu},\boldsymbol{\Theta}) = \cup_{T\in\mathcal{T}_\ell}\left[T \subseteq \mathbb{G}_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta})\right]$$

where $\mathcal{T}_\ell$ denotes the collection of all spanning trees on the vertices $\{v_1,\ldots,v_\ell\}$. Thus,

$$\mathbb{P}[C_\ell(\boldsymbol{\mu},\boldsymbol{\Theta})] \leq \sum_{T\in\mathcal{T}_\ell} \mathbb{P}\left[T \subseteq \mathbb{G}_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta})\right]. \tag{6.89}$$

Given that $K_1 \leq K_2 \leq \ldots \leq K_r$, the probability of T being contained in $\mathbb{G}_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta})$ is maximized when all nodes receive the largest possible number K_r of keys. Thus, for any

$T \in \mathcal{T}$ and distribution $\boldsymbol{\mu}$ we have

$$\begin{aligned}\mathbb{P}\left[T \subseteq \mathbb{G}_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta})\right] &\leq \mathbb{P}\left[T \subseteq \mathbb{G}_\ell(n;\boldsymbol{\mu}=\{0,0,\ldots,1\},\boldsymbol{\Theta})\right] \\ &= (\alpha p_{rr})^{\ell-1} \qquad (6.90)\end{aligned}$$

where the last equality follows from the facts that i) a tree on ℓ vertices contain $\ell-1$ edges, and ii) since all nodes have the same key ring size, edges in $\mathbb{G}_\ell(n;\boldsymbol{\mu}=\{0,0,\ldots,1\},\boldsymbol{\Theta})$ are *pairwise* independent; see [159, Lemma 9.1] and [156, Eq. 64]. We obtain (6.81) upon using (6.90) in (6.89) and noting by Cayley's formula [93] that there are $\ell^{\ell-2}$ trees on ℓ vertices, i.e., $|\mathcal{T}_\ell| = \ell^{\ell-2}$.

6.5.11 Establishing (6.84)

We will establish (6.84) in several steps with each step focusing on a specific range of the summation over ℓ. Throughout, we consider a scalings $K_1,\ldots,K_r,P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$ such that (6.16) holds with $c>1$, (6.21), and (6.20) hold.

The case where $2 \leq \ell \leq R$

This range considers fixed values of ℓ. Pick an integer R to be specified later at (6.96). Use (6.16), (6.26), (6.10), (6.80), (6.81), and the first bound in (6.82) to get

$$\begin{aligned}\sum_{\ell=2}^{R}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] &\leq \sum_{\ell=2}^{R}\left(\frac{en}{\ell}\right)^\ell \ell^{\ell-2}\left(\alpha_n p_{rr}(n)\right)^{\ell-1}\left(1-\alpha_n\lambda_1(n)\right)^{n-\ell} \\ &\leq \sum_{\ell=2}^{R}(en)^\ell\left(\frac{(\log n)^2}{n}\right)^{\ell-1}\left(1-c_n\frac{\log n}{n}\right)^{n-\ell} \\ &\leq \sum_{\ell=2}^{R} n\left(e(\log n)^2\right)^\ell e^{-c_n \log n\frac{n-\ell}{n}} \\ &= \sum_{\ell=2}^{R}\left(e(\log n)^2\right)^\ell n^{1-c_n\frac{n-\ell}{n}}\end{aligned}$$

With $c > 1$, we have $\lim_{n\to\infty}\left(1 - c_n\frac{n-\ell}{n}\right) = 1 - c < 0$. Thus, for each $\ell = 2, 3, \ldots$, we have

$$\left(e(\log n)^2\right)^{\ell-1} n^{1-c_n\frac{n-\ell}{n}} = o(1),$$

whence we get

$$\lim_{n\to\infty}\sum_{\ell=2}^{R}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] = 0.$$

The case where $R + 1 \leq \ell \leq \min\{L_n, \lfloor\frac{\mu_r n}{\beta c_n \log n}\rfloor\}$

Our goal in this and the next subsubsection is to cover the range $R + 1 \leq \ell \leq \lfloor\frac{\mu_r n}{\beta c_n \log n}\rfloor$. Since the bound given at (6.82) takes a different form when $\ell > L_n$, we first consider the range $R + 1 \leq \ell \leq \min\{L_n, \lfloor\frac{\mu_r n}{\beta c_n \log n}\rfloor\}$. Using (6.26), (6.10), (6.80), (6.81), and the second bound in (6.82) we get

$$\begin{aligned}&\sum_{\ell=R+1}^{\min\{L_n,\lfloor\frac{\mu_r n}{\beta c_n \log n}\rfloor\}}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c]\\ &\leq \sum_{\ell=R+1}^{\min\{L_n,\lfloor\frac{\mu_r n}{\beta c_n \log n}\rfloor\}}\left(\frac{en}{\ell}\right)^{\ell}\ell^{\ell-2}\left(\frac{(\log n)^2}{n}\right)^{\ell-1}\cdot\left(1-\mu_r\left(1-e^{-\alpha_n\beta\ell p_{1r}(n)}\right)\right)^{n-\ell}\end{aligned} \tag{6.91}$$

From the upper bound in (6.25) and $\ell \leq \frac{\mu_r n}{\beta c_n \log n}$, we have

$$\alpha_n\beta\ell p_{1r}(n) \leq \alpha_n\beta\frac{\mu_r n}{\beta c_n \log n}\frac{c_n}{\mu_r}\frac{\log n}{n\alpha_n} = 1.$$

Using the fact that $1 - e^{-x} \geq \frac{x}{2}$ for all $0 \leq x \leq 1$, we get

$$1-\mu_r\left(1-e^{-\alpha_n\beta\ell p_{1r}(n)}\right) \leq 1 - \frac{\mu_r\alpha_n\beta\ell p_{1r}(n)}{2} \leq e^{-\beta\ell c_n\mu_r\frac{\log n}{2n}} \tag{6.92}$$

using the lower bound in (6.25). Reporting this last bound in to (6.91) and noting that

$$n - \ell \geq \frac{n}{2}, \qquad \ell = 2, 3, \ldots, \left\lfloor\frac{n}{2}\right\rfloor, \tag{6.93}$$

we get

$$
\begin{aligned}
\sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] &\leq \sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} n \left(e(\log n)^2\right)^\ell e^{-\beta \ell c_n \mu_r \frac{\log n}{2n} \frac{n}{2}} \\
&\leq n \sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \left(e\left(\log n\right)^2 e^{-\beta c_n \frac{\mu_r}{4} \log n}\right)^\ell \\
&\leq n \sum_{\ell=R+1}^{\infty} \left(e\left(\log n\right)^2 e^{-\beta c_n \frac{\mu_r}{4} \log n}\right)^\ell \quad (6.94)
\end{aligned}
$$

Given that $\beta, \mu_r > 0$ and $\lim_{n\to\infty} c_n = c > 0$ we clearly have

$$
e\left(\log n\right)^2 e^{-\beta c_n \log n \frac{\mu_r}{4}} = o(1). \quad (6.95)
$$

Thus, the geometric series in (6.94) is summable, and we have

$$
\begin{aligned}
\sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] &\leq (1+o(1))\, n \left(e\left(\log n\right)^2 e^{-\beta c_n \log n \frac{\mu_r}{4}}\right)^{R+1} \\
&= (1+o(1))\, n^{1-(R+1)\beta c_n \frac{\mu_r}{4}} \left(e(\log n)^2\right)^{R+1} \\
&= o(1)
\end{aligned}
$$

for any positive integer R with

$$
R > \frac{8}{\beta c \mu_r}. \quad (6.96)
$$

This choice is permissible given that $c, \beta, \mu_r > 0$.

The case where $\min\{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor, \max(R, L_n)\} < \ell \leq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$

Clearly, this range becomes obsolete if $\max(R, L_n) \geq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$. Thus, it suffices to consider the subsequences for which the range $\max(R, L_n) + 1 \leq \ell \leq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$ is non-empty. There, we use (6.26), (6.10), (6.80), (6.81), and the second bound in (6.82) to get

$$
\begin{aligned}
&\sum_{\ell=\max(R,L_n)+1}^{\left\lfloor \frac{\mu_r n}{\beta c_n \log n} \right\rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] && (6.97)\\
&\leq \sum_{\ell=\max(R,L_n)+1}^{\left\lfloor \frac{\mu_r n}{\beta c_n \log n} \right\rfloor} \left(\frac{en}{\ell}\right)^{\ell} \ell^{\ell-2} \left(\frac{(\log n)^2}{n}\right)^{\ell-1} \left(1 - \mu_r\left(1 - e^{-\beta \ell \alpha_n p_{1r}(n)}\right) + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\
&\leq \sum_{\ell=\max(R,L_n)+1}^{\left\lfloor \frac{\mu_r n}{2\beta c \log n} \right\rfloor} n\left(e\left(\log n\right)^2\right)^{\ell} \left(e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}
\end{aligned}
$$

where in the last step we used (6.92) in view of $\ell \leq \frac{\mu_r n}{\beta c_n \log n}$.

Next, we write

$$
\begin{aligned}
e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} + e^{-\gamma K_{1,n}} &= e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} \left(1 + e^{-\gamma K_{1,n} + \beta \ell c_n \mu_r \frac{\log n}{2n}}\right) \\
&\leq \exp\left\{-\beta \ell c_n \mu_r \frac{\log n}{2n} + e^{-\gamma K_{1,n} + \beta \ell c_n \mu_r \frac{\log n}{2n}}\right\} \\
&\leq \exp\left\{-\beta \ell c_n \mu_r \frac{\log n}{2n}\left(1 - \frac{e^{-\gamma K_{1,n} + \frac{\mu_r^2}{2}}}{\beta \ell c_n \mu_r \frac{\log n}{2n}}\right)\right\} \qquad (6.98)
\end{aligned}
$$

where the last inequality is obtained from $\ell \leq \frac{\mu_r n}{\beta c_n \log n}$. Using the fact that $\ell > L_n = \min\{\lfloor \frac{P_n}{K_{1,n}} \rfloor, \lfloor \frac{n}{2} \rfloor\}$ and (6.20) we have

$$
\begin{aligned}
\frac{e^{-\gamma K_{1,n}}}{\beta \ell c_n \mu_r \frac{\log n}{2n}} &\leq \max\left\{\frac{K_{1,n}}{P_n}, \frac{2}{n}\right\} 2n \frac{e^{-\gamma K_{1,n}}}{\beta c_n \mu_r \log n} \\
&\leq \max\left\{\frac{2K_{1,n} e^{-\gamma K_{1,n}}}{\beta c_n \mu_r \sigma \log n}, \frac{4e^{-\gamma K_{1,n}}}{\beta c_n \mu_r \log n}\right\} \\
&= o(1)
\end{aligned}
$$

by virtue of (6.36) and the facts that $\beta, \mu_r, \sigma, c_n > 0$. Reporting this into (6.98), we see that for for any $\epsilon > 0$, there exists a finite integer $n^*(\epsilon)$ such that

$$
\left(e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}} + e^{-\gamma K_{1,n}}\right) \leq e^{-\beta \ell c_n \mu_r \frac{\log n}{2n}(1-\epsilon)} \qquad (6.99)
$$

for all $n \geq n^*(\epsilon)$. Using (6.99) in (6.97), we get

$$\begin{aligned}\sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{\beta c_n \log n}\rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] &\leq n \sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{\beta c_n \log n}\rfloor} \left(e \left(\log n\right)^2 e^{-\beta c_n \mu_r \frac{\log n}{2n}(1-\epsilon)\frac{n}{2}} \right)^{\ell} \\ &\leq n \sum_{\ell=\max(R,L_n)+1}^{\infty} \left(e \left(\log n\right)^2 e^{-\beta c_n \mu_r \frac{\log n}{4}(1-\epsilon)} \right)^{\ell}\end{aligned} \tag{6.100}$$

Similar to (6.95), we have $e \left(\log n\right)^2 e^{-\beta c_n \mu_r \frac{\log n}{4}(1-\epsilon)} = o(1)$ so that the sum in (6.100) converges. Following a similar approach to that in Section 6.5.11, we then see that

$$\lim_{n\to\infty} \sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{2\beta c \log n}\rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0$$

with R selected according to (6.96) and $\epsilon < 1/2$.

The case where $\lfloor \frac{\mu_r n}{\beta c_n \log n}\rfloor + 1 \leq \ell \leq \lfloor \nu n \rfloor$

We consider $\lfloor \frac{\mu_r n}{\beta c_n \log n}\rfloor + 1 \leq \ell \leq \lfloor \nu n \rfloor$ for some $\nu \in (0, \frac{1}{2})$ to be specified later. Recall (6.25), (6.10), (6.80), the first bound in (6.81), and the second bound in (6.82). Noting that $\binom{n}{\ell}$ is monotone increasing in ℓ when $0 \leq \ell \leq \lfloor \frac{n}{2} \rfloor$ and using (6.93) we get

$$\begin{aligned}&\sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n}\rfloor+1}^{\lfloor \nu n \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \\ &\leq \sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n}\rfloor+1}^{\lfloor \nu n \rfloor} \binom{n}{\lfloor \nu n \rfloor} \left(1 - \mu_r + \mu_r e^{-\alpha_n \beta \ell p_{1r}(n)} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\ &\leq \sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n}\rfloor+1}^{\lfloor \nu n \rfloor} \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\alpha_n \beta \frac{\mu_r n}{\beta c_n \log n} \frac{c_n \log n}{n \alpha_n}} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\ &\leq n \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\mu_r} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\ &= n \left(\left(\frac{e}{\nu}\right)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\mu_r} + e^{-\gamma K_{1,n}}\right) \right)^{\frac{n}{2}}\end{aligned} \tag{6.101}$$

We have $1-\mu_r+\mu_r e^{-\mu_r}<1$ from $\mu_r>0$ and $e^{-\gamma K_{1,n}}=o(1)$ from (6.36). Also, it holds that $\lim_{\nu\to 0}\left(\frac{e}{\nu}\right)^{2\nu}=1$. Thus, if we pick ν small enough to ensure that

$$\left(\frac{e}{\nu}\right)^{2\nu}\left(1-\mu_r+\mu_r e^{-\mu_r}\right)<1, \tag{6.102}$$

then for any $0<\epsilon<1-(e/\nu)^{2\nu}\left(1-\mu_r+\mu_r e^{-\mu_r}\right)$ there exists a finite integer $n^\star(\epsilon)$ such that

$$\left(\frac{e}{\nu}\right)^{2\nu}\left(1-\mu_r+\mu_r e^{-\mu_r}+e^{-\gamma K_{1,n}}\right)\le 1-\epsilon, \quad \forall n\ge n^\star(\epsilon).$$

Reporting this into (6.101), we get

$$\lim_{n\to\infty}\sum_{\ell=\left\lfloor\frac{\mu_r n}{2\beta c\log n}\right\rfloor+1}^{\lfloor\nu n\rfloor}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c]=0$$

since $\lim_{n\to\infty} n(1-\epsilon)^{n/2}=0$.

The case where $\lfloor\nu n\rfloor+1\le\ell\le\lfloor\frac{n}{2}\rfloor$

In this range, we use (6.11), (6.80), the first bound in (6.81), the last bound in (6.82), and (6.93) to get

$$\begin{aligned}\sum_{\ell=\lfloor\nu n\rfloor+1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] &\le \sum_{\ell=\lfloor\nu n\rfloor+1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{\ell}\left(e^{-\beta\ell\alpha_n p_{11}(n)}+e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}\\ &\le\left(\sum_{\ell=\lfloor\nu n\rfloor+1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{\ell}\right)\left(e^{-\beta\nu n\alpha_n p_{11}(n)}+e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}\\ &\le\left(4e^{-\beta\nu n\alpha_n p_{11}(n)}+4e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}\end{aligned}$$

With $\beta,\nu,\gamma>0$ have $e^{-\beta\nu n\alpha_n p_{11}(n)}=o(1)$ from (6.21) and $e^{-\gamma K_{1,n}}=o(1)$ from (6.36). The conclusion

$$\lim_{n\to\infty} \sum_{\ell=\lfloor \nu n \rfloor +1}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0$$

immediately follows and the proof of one-law is completed. ■

6.6 *k*-connectivity and minimum node degree

In this section, we present conditions (in the form of zero-one laws) on how to scale the parameters of the intersection model so that with high probability i) all of its nodes are connected to at least k other nodes, i.e., the minimum node degree of the graph is no less than k; and ii) the graph is k-connected, i.e., the graph remains connected even if *any* $k-1$ nodes leave the network. These results are shown to complement and generalize several previous results in the literature. We also present numerical results to support our findings in the finite-node regime.

We start by noting some additional notation that will be useful in this section. For any three distinct nodes v_x , v_y and v_j, we define $E_{xj\cap yj} := E_{xj} \cap E_{yj}$, $E_{xj\cap\overline{yj}} := E_{xj} \cap \overline{E_{yj}}$, $E_{\overline{xj}\cap yj} := \overline{E_{xj}} \cap E_{yj}$, and $E_{\overline{xj}\cap\overline{yj}} := \overline{E_{xj}} \cap \overline{E_{yj}}$. Consider the vertex set $\mathcal{V} = \{v_1, \ldots, v_n\}$. For each node $v_i \in \mathcal{V}$, we define N_i as the set of neighbors of node v_i. Also, for any pair of vertices v_x, v_y, we let N_{xy} be the set of nodes in $\mathcal{V} \setminus \{v_x, v_y\}$ that are neighbors of both v_x and v_y; i.e., $N_{xy} = N_x \cap N_y$. We also let $N_{x\overline{y}}$ denote the set of nodes in $\mathcal{V} \setminus \{v_x, v_y\}$ that are neighbors of v_x, but are not neighbors of v_y. Similarly, $N_{\overline{x}y}$ is defined as the set of nodes in $\mathcal{V} \setminus \{v_x, v_y\}$ that are not neighbors of v_x, but are neighbors of v_y. Finally, $N_{\overline{xy}}$ is the set of nodes in $\mathcal{V} \setminus \{v_x, v_y\}$ that are not neighbors of either v_x or v_y. We also define $S_{xy} = \Sigma_x \cap \Sigma_y$.

We refer to a mapping $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ as a *scaling* (for the inhomogeneous random key graph) as long as the conditions

$$2 \leq K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{r,n} \leq P_n/2 \tag{6.103}$$

are satisfied for all $n = 2, 3, \ldots$. Similarly any mapping $\alpha : \mathbb{N}_0 \to (0,1)$ defines a scaling for Erdős-Rényi graphs. As a result, a mapping $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$ defines a scaling for the intersection graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ given that condition (6.103) holds. We remark that under (6.103), the edge probabilities p_{ij} will be given by (6.2).

We first present a zero-one law for the minimum node degree being no less than k in the inhomogeneous random key graph intersecting Erdős-Rényi graph.

6.6.1 A zero-one law for the minimum node degree being no less than k

Theorem 6.6.1. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$. Let the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ be defined through*

$$\Lambda_1(n) = \alpha_n \lambda_1(n) = \frac{\log n + (k-1)\log\log n + \gamma_n}{n}, \tag{6.104}$$

for each $n = 1, 2, \ldots$.

(a) If $\lambda_1(n) = o(1)$, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{l}\textit{Minimum node degree}\\ \textit{of } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha) \geq k\end{array}\right] = 0 \quad \textit{if } \lim_{n\to\infty} \gamma_n = -\infty$$

(b) We have

$$\lim_{n\to\infty} \mathbb{P}\left[\begin{array}{l}\textit{Minimum node degree}\\ \textit{of } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha) \geq k\end{array}\right] = 1 \quad \textit{if } \lim_{n\to\infty} \gamma_n = \infty.$$

Next, we present a zero-one law for the k-connectivity of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$.

6.6.2 A zero-one law for k-connectivity

Theorem 6.6.2. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)$. Let the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ be defined through (6.104) for each $n = 1, 2, \ldots$.*

(a) If $\lambda_1(n) = o(1)$, we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha) \text{ is } k\text{-connected}\right] = 0 \quad \text{if } \lim_{n\to\infty} \gamma_n = -\infty$$

(b) If

$$P_n = \Omega(n), \tag{6.105}$$

$$\frac{K_{r,n}}{P_n} = o(1), \tag{6.106}$$

$$\frac{K_{r,n}}{K_{1,n}} = o(\log n), \tag{6.107}$$

we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha) \text{ is } k\text{-connected}\right] = 1 \quad \text{if } \lim_{n\to\infty} \gamma_n = \infty. \tag{6.108}$$

6.6.3 Discussion

Theorem 6.6.1 (respectively Theorem 6.6.2) states that the minimum node degree in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ is greater than or equal to k (respectively $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ is k-connected) whp if the mean degree of class-1 nodes, i.e., $n\Lambda_1(n)$, is scaled as $(\log n + (k-1)\log\log n + \gamma_n)$ for some sequence γ_n satisfying $\lim_{n\to\infty} \gamma_n = \infty$. On the other hand, if the sequence γ_n satisfies $\lim_{n\to\infty} \gamma_n = -\infty$, then whp $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ has at least one node with degree strictly less than k, and hence is *not* k-connected. This shows that the critical scaling for the minimum node degree of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ being greater than or equal to k (respectively for $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ to be k-connected) is given by $\Lambda_1(n) = \frac{\log n + (k-1)\log\log n}{n}$, with the sequence $\gamma_n : \mathbb{N}_0 \to \mathbb{R}$ measuring the deviation of $\Lambda_1(n)$ from the critical scaling.

The scaling condition (6.104) can be given a more explicit form under some additional constraints. In particular, it was shown in [157, Lemma 4.2] that if $\lambda_1(n) = o(1)$ then

$$\lambda_1(n) \sim \frac{K_{1,n} K_{\text{avg},n}}{P_n} \tag{6.109}$$

where $K_{\text{avg},n} = \sum_{j=1}^{r} \mu_j K_{j,n}$ denotes the *mean* key ring size in the network. This shows that the minimum key ring size $K_{1,n}$ is of paramount importance in controlling the connectivity and reliability of the network; as explained previously, it then also controls the number of *mobile* sensors that can be accommodated in the network. For example, with the mean number $K_{\text{avg},n}$ of keys per sensor is fixed, we see that reducing $K_{1,n}$ by half means that the smallest α_n (that gives the largest link failure probability $1 - \alpha_n$) for which the network remains k-connected whp is increased by two-fold for any given k; e.g., see Figure 6.6 for a numerical example demonstrating this.

We first comment on the additional technical condition $\lambda_1(n) = o(1)$. This is enforced here mainly for technical reasons for the proof of the zero-law of Theorem 6.6.1 (and thus of Theorem 6.6.2) to work. A similar condition was also required in [166, Thm 1] for establishing the zero-law for the minimum node degree being no less than k in the *homogeneous* random key graph intersecting Erdős-Rényi graph. In view of (6.109), this condition is equivalent to

$$K_{1,n} K_{\text{avg},n} = o(P_n). \tag{6.110}$$

In real-world wireless sensor network applications the key pool size P_n is envisioned to be orders of magnitude larger than any key ring size in the network [33, 53]. As discussed below in more details, this is needed to ensure the resilience of the network against adversarial attacks. In conclusion, (6.110) (and thus $\lambda_1(n) = o(1)$) is indeed likely to hold in most applications.

Conditions (6.105) and (6.106) are also likely to be needed in practical implementations of wireless sensor networks in order to ensure the *resilience* of the network against node capture attacks; e.g., see [33, 53]. To see this, assume that an adversary captures a number of sensors, compromising all the keys that belong to the captured nodes. If $P_n = O(K_{r,n})$ contrary to (6.106), then it would be possible for the adversary to compromise a positive fraction of the key pool (i.e., $\Omega(P_n)$ keys) by capturing only a constant number of sensors that are of type r. Similarly, if $P_n = o(n)$, contrary to (6.105), then again it would be possible for the adversary to compromise $\Omega(P_n)$ keys by capturing only $o(n)$ sensors (whose type does not matter in this case). In both cases, the network would fail to exhibit the *unassailability* property [95,153] and would be deemed as vulnerable against adversarial attacks. We remark that both (6.105) and (6.106) were required in [157,166] for obtaining the one-law for connectivity and k-connectivity, respectively, in similar settings to ours.

Finally, the condition (6.107) is enforced mainly for technical reasons and takes away from the flexibility of assigning very small key rings to a certain fraction of sensors when k-connectivity is considered; we remark that (6.107) is not needed for the minimum node degree result given at Theorem 6.6.1. An equivalent condition was also needed in [157] for establishing the one-law for connectivity in inhomogeneous random key graphs. We refer the reader to [157, Section 3.2] for an extended discussion on the feasibility of (6.107) for real-world implementations of wireless sensor networks, as well as possible ways to replace it with milder conditions.

We close by providing a concrete example that demonstrates how all the conditions required by Theorem 6.6.2 can be met in a real-world implementation. Consider any number r of sensor types, and pick any probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for all $i = 1, \ldots, r$. For any channel probability $\alpha_n = \Omega(\frac{\log n}{n})$, set $P_n = \lceil n \log n \rceil$ and use

$$K_{1,n} = \left\lceil \frac{(\log n)^{1/2+\varepsilon}}{\sqrt{\alpha_n}} \right\rceil \quad \text{and} \quad K_{r,n} = \left\lceil \frac{(1+\varepsilon)(\log n)^{3/2-\varepsilon}}{\mu_r \sqrt{\alpha_n}} \right\rceil$$

with any $0 < \varepsilon < 0.5$. Other key ring sizes $K_{1,n} \leq K_{2,n}, \ldots, K_{r-1,n} \leq K_{r,n}$ can be picked arbitrarily. In view of Theorem 6.6.2 and the fact [157, Lemma 4.2] that $\lambda_1(n) \sim \frac{K_{1,n} K_{\text{avg},n}}{P_n}$, the resulting network will be k-connected whp for any $k = 1, 2, \ldots$. Of course, there are many other parameter scalings that one can choose.

6.6.4 Comparison with related work

Several properties of the homogeneous random key graph, $\mathbb{K}(n;K,P)$, have been extensively studied in literature. In particular, the 1-connectivity of $\mathbb{K}(n;K,P)$ has been investigated in [15, 33, 128, 159] under *full* visibility, i.e., when all pairs of nodes have a communication channel in between. Therein, authors provided scaling conditions on the key ring size K_n and the key pool size P_n as functions of the network size n such that the resulting network is connected with high probability as the number of nodes gets large. Moreover, the k-connectivity property of $\mathbb{K}(n;K,P)$ was investigated under full visibility in [129].

Our work extends these results to the heterogeneous setting, where sensor nodes have different levels of resources and security/connectivity requirements, thus possibly belonging to different classes. Such heterogeneity induces the need for the *inhomogeneous* random key graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ as an accurate model for the crypto-connectivity of the resulting network. Also, unlike the aforementioned results that assume full visibility, our work considers the wireless connectivity of the network through the on-ff channel model.

In [166], Zhao et al. investigated the k-connectivity property of $\mathbb{K}(n;K,P)$ under an an/off channel model. There, zero-one laws for the property that the minimum node degree is no less than k and the property that the graph is k-connected were established for $\mathbb{K}(n;K,P) \cap \mathbb{G}(n;\alpha)$. Clearly, our work extends these results to the heterogeneous setting as we consider the intersection of the *inhomogeneous* random key graph with Erdős-Rényi graph. In particular, with $r = 1$, i.e., when all nodes belong to the same class and thus receive the same number K of keys, Theorem 6.6.1 and Theorem 6.6.2 recover the results of Zhao et al. (See [166, Theorems 1-2]).

In comparison with the existing literature on similar models, our result can be seen to extend the work by Eletreby and Yağan in [50]. Therein, the authors established a zero-one law for the 1-connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$, i.e., for a wireless sensor network under the heterogeneous key predistribution scheme and on-off channel model. Although these results form a crucial starting point towards the analysis of the heterogeneous key predistribution scheme, they do not guarantee that the wireless sensor network would remain connected when sensors fail due to battery depletion or get captured by an adversary. Moreover, the results in [50] are not applicable for *mobile* wireless sensor networks since the mobility of even a single sensor may render the network disconnected. The results established here fill these gaps by establishing k-connectivity results.

Our work also generalizes the work by Yağan [157] who considered the inhomogeneous random key graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$ under *full* visibility; i.e., when all pairs of nodes have a communication channel in between. There, Yağan established zero-one laws for the absence of isolated nodes (i.e., absence of nodes with degree zero) and 1-connectivity. Our work generalizes Yağan's results on two fronts. Firstly, we consider more practical wireless sensor network scenarios where the unreliability of wireless communication channels are taken into account through the on-ff channel model. Secondly, in addition to the properties that the graph has no isolated nodes (i.e., the minimum node degree is no less than 1) and is 1-connected, we consider general minimum node degree and connectivity values, $k = 0, 1, \ldots$.

6.6.5 Numerical results

We now present numerical results to support Theorems 6.6.1 and 6.6.2 in the finite node regime. Moreover, we also verify the validity of our claim that the on-off channel model serves as a good approximation of the disk model in the context of k-connectivity property. In all experiments, we fix the number of nodes at $n = 500$ and the size of the key pool at $P = 10^4$.

To compare the connectivity behavior of the heterogeneous key predistribution scheme under the disk model with that of the on-off channel model, we use the matching condition (see Section 6.5.6) $\alpha = \pi\rho^2$. In what follows, we present several simulation results comparing the (empirical) probabilities that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$ are k-connected, respectively.

In our first set of experiments, we consider the channel parameters $\alpha = \pi\rho^2 = 0.2$, $\alpha = \pi\rho^2 = 0.4$, $\alpha = \pi\rho^2 = 0.6$, and $\alpha = \pi\rho^2 = 0.8$, while varying the parameter K_1, i.e., the smallest key ring size, from 10 to 40. The number of classes is fixed to 2, with $\boldsymbol{\mu} = \{0.5, 0.5\}$. For each value of K_1, we set $K_2 = K_1 + 5$. For each parameter pair $(\boldsymbol{K}, \alpha)$, we generate 1000 independent samples of the graphs $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ and $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{I}(n; \rho)$, and count the number of times (out of a possible 1000) that the obtained graphs i) have minimum node degree no less than 2 and ii) are 2-connected. Dividing the counts by 1000, we obtain the (empirical) probabilities for the events of interest. In all cases considered here, we observe that $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ (resp. $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{I}(n; \rho)$) is 2-connected whenever it has minimum node degree no less than 2 yielding the same empirical probability for both events. This supports the fact that the properties of k-connectivity and minimum node degree being larger than k are asymptotically equivalent in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$.

The results obtained for the empirical probabilities of 2-connectivity are depicted in Figure 6.4, where lines represent the results under the on-off model and symbols represent the results under the disk model. In all cases, we see that empirical probabilities are almost identical, supporting the claim that the on-ff channel model serves as a good approximation of the disk model (under $\alpha = \pi\rho^2$). More importantly, this shows that our main results are likely to hold also under the disk communication model. For each curve in Figure 6.4, we also show the critical threshold of connectivity "predicted" by Theorem 6.6.2 by a vertical dashed line. More specifically, the vertical dashed lines stand for the minimum integer value of K_1 that satisfies

$$\lambda_1(n) = \sum_{j=1}^{2} \mu_j \left(1 - \frac{\binom{P-K_j}{K_1}}{\binom{P}{K_1}} \right) > \frac{1}{\alpha} \frac{\log n + (k-1)\log\log n}{n} \tag{6.111}$$

with any given k and α. We see from Figure 6.4 that the probability of k-connectivity transitions from zero to one within relatively small variations in K_1. Moreover, the critical values of K_1 obtained by (6.111) lie within the transition interval.

In Figure 6.5, we consider four different values for k, namely we set $k = 4$, $k = 6$, $k = 8$, and $k = 10$ while varying K_1 from 10 to 40 and fixing $\alpha = \pi\rho^2 = 0.4$. The number of classes is fixed to 2 with $\boldsymbol{\mu} = \{0.5, 0.5\}$ and we set $K_2 = K_1 + 5$ for each value of K_1. Using the same procedure that produced Figure 6.4, we obtain the empirical probability that $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ and

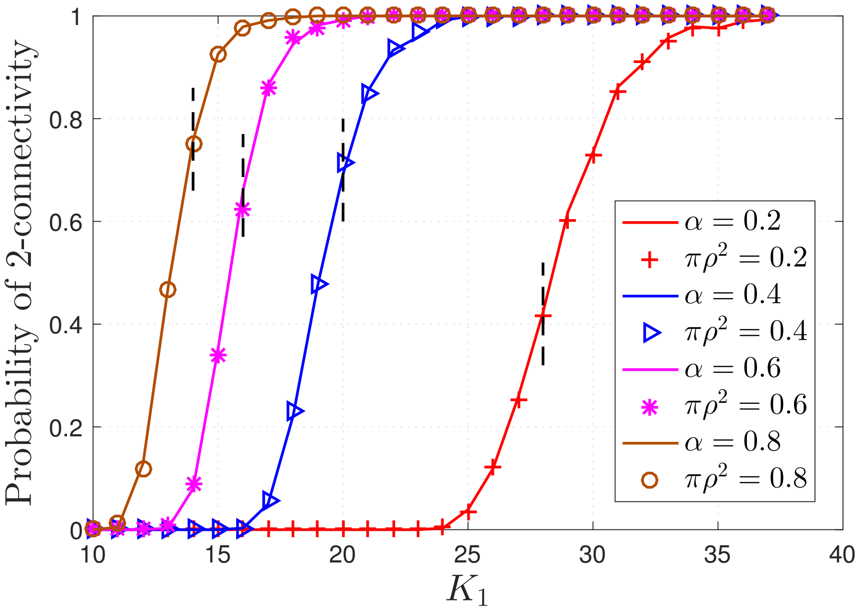


Figure 6.4: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$ are 2-connected as a function of $\boldsymbol{K}$ for $\alpha = \pi\rho^2 = 0.2$, $\alpha = \pi\rho^2 = 0.4$, $\alpha = \pi\rho^2 = 0.6$, and $\alpha = \pi\rho^2 = 0.8$ with $n = 500$ and $P = 10^4$; in each case, the empirical probability value is obtained by averaging over 1000 experiments. Vertical dashed lines correspond to the critical values of K_1 obtained from (6.111).

$\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$ are k-connected versus K_1. The critical threshold of connectivity asserted by Theorem 6.6.2 is again shown by a vertical dashed line. Again, we see that numerical results are in parallel with Theorem 6.6.2, and that the k-connectivity behaviors of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$ are very close to each other.

Figure 6.6 is generated in a similar manner with Figure 6.4, this time with an eye towards understanding the impact of the minimum key ring size K_1 on network connectivity. To that end, we fix the number of classes at 2 with $\boldsymbol{\mu} = \{0.5, 0.5\}$ and consider four different key ring sizes $\boldsymbol{K}$ each with mean 40; we consider $\boldsymbol{K} = \{10, 70\}$, $\boldsymbol{K} = \{20, 60\}$, $\boldsymbol{K} = \{30, 50\}$, and $\boldsymbol{K} = \{40, 40\}$. We compare the probability of 2-connectivity in the resulting networks while varying α (and consequently $\pi\rho^2$) from zero to one. We see that although the average number of keys per sensor is kept constant in all four cases, network connectivity improves dramatically as the minimum key ring size K_1 increases; e.g., with $\alpha = \pi\rho^2 = 0.2$, the probability of connectivity is one when $K_1 = K_2 = 40$ while it drops to zero if we set $K_1 = 10$ while

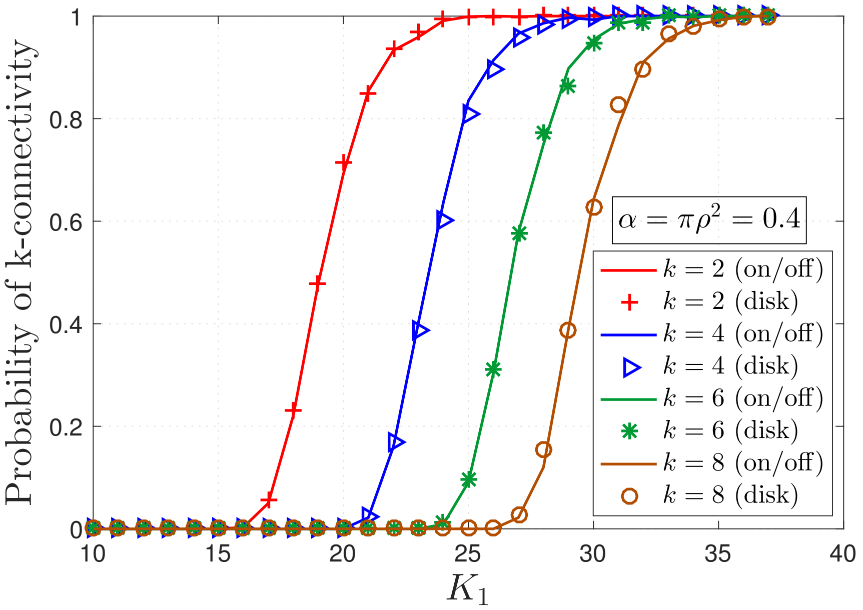


Figure 6.5: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$ are k-connected as a function of K_1 for $k = 4$, $k = 6$, $k = 8$, and $k = 10$, with $n = 500$ and $P = 10^4$; in each case, the empirical probability value is obtained by averaging over 1000 experiments. Vertical dashed lines stand for the critical threshold of connectivity asserted by Theorem 6.6.2.

increasing K_2 to 70 so that the mean key ring size is still 40. Once again, we see that the results under the on-off model are very similar to those obtained under the disk model. In fact, Figure 6.6 suggests that our work can be useful in determining the minimum transmission radius ρ needed to achieve a certain probability of k-connectivity in the network; e.g., to guarantee 2-connectivity almost surely with $K_1 = 20$ and $K_2 = 60$ (with other parameters as in the caption of Figure 6.6), we need to have at least $\pi\rho^2 = 0.38$.

In Figure 6.7, we examine the reliability of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ by looking at the probability of 1-connectivity as the number of deleted (i.e., failed) nodes increases. From a mobility perspective, this is equivalent to investigating the probability of a wireless sensor network remaining connected as the number of *mobile* sensors leaving the network increases. We set $n = 500, \boldsymbol{\mu} = \{1/2, 1/2\}, \alpha = 0.4, P = 10^4$, and select K_1 and $K_2 = K_1 + 10$ from (6.111) for $k = 8$, $k = 10$, $k = 12$, and $k = 14$. With these settings, we would expect (for very large n) the network to remain connected whp after the deletion of up to 7, 9, 11, and 13 nodes,

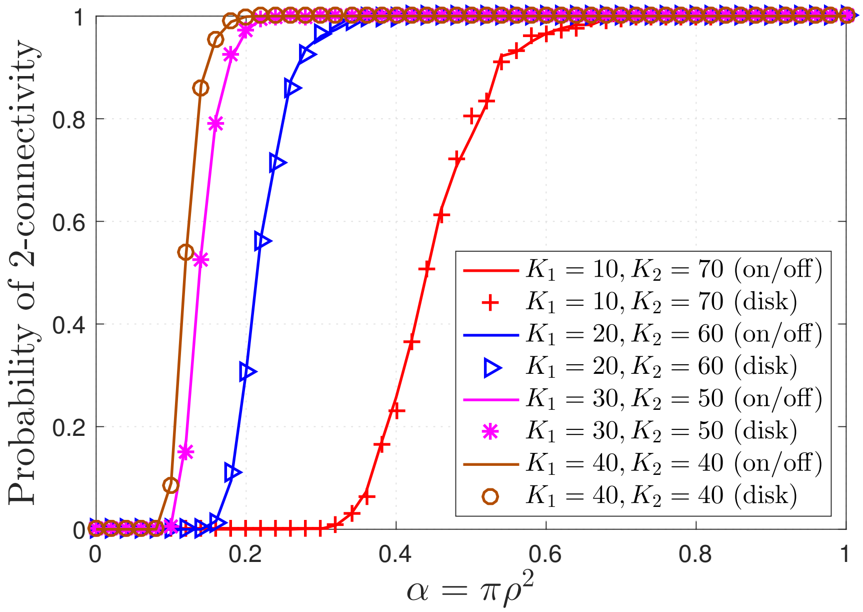


Figure 6.6: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ and $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{I}(n;\rho)$ are 2-connected with $n = 500, \boldsymbol{\mu} = (1/2, 1/2)$, and $P = 10^4$; we consider four choices of $\boldsymbol{K} = (K_1, K_2)$ each with the same mean.

respectively. Using the same procedure that produced Figure 6.4, we obtain the empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ is connected as a function of the number of deleted nodes[2] in each case. We see that even with $n = 500$ nodes, the resulting reliability is close to the levels expected to be attained asymptotically as n goes to infinity. In particular, we see that the probability of remaining connected when $(k-1)$ nodes leave the network is around 0.75 for the first two cases and around 0.90 for the other two cases.

Finally, we provide a simulation study that characterizes the effect of network size n on the probability of k-connectivity. Our objective is to observe the influence of n on the behavior of the probability of k-connectivity. In Figure 6.8, we examine the probability of 4-connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ as we set $P = 10^4$, $\alpha = 0.4$, vary K_1 from 4 to 40, and set $K_2 = K_1 + 5$. To characterize the effect of n, we compute the empirical probability for the cases when $n = 300$, $n = 500$, $n = 1000$, and $n = 10000$. We observe that the probability of connectivity exhibits a

[2] We choose the nodes to be deleted from the *minimum vertex cut* of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$, defined as the minimum cardinality set whose removal renders it disconnected. This captures the worst-case nature of the k-connectivity property in a computationally efficient manner (as compared to searching over all k-sized subsets and deleting the one that gives maximum damage).

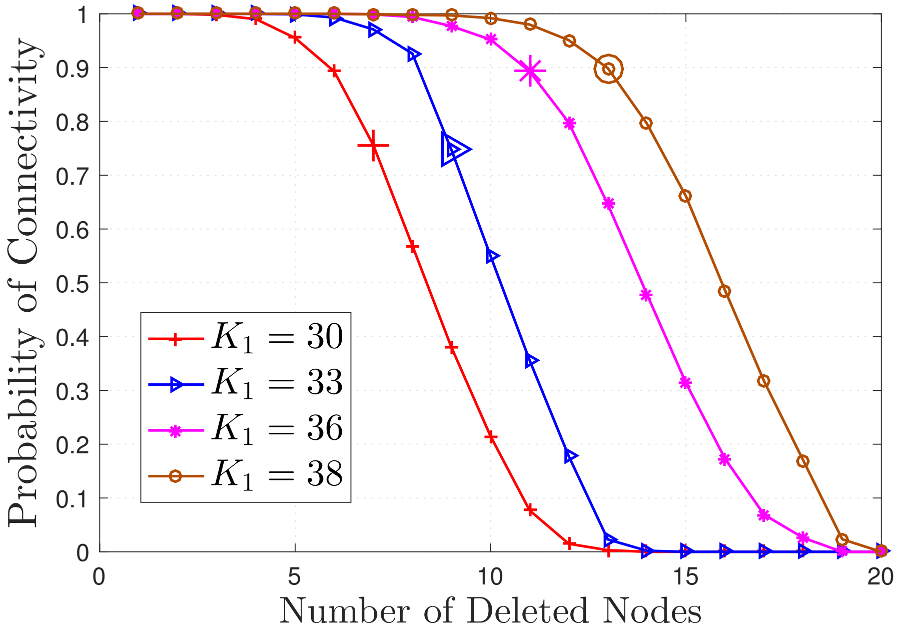


Figure 6.7: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ remains connected after deleting nodes from the *minimum vertex cut* set. We fix $n = 500, \boldsymbol{\mu} = (1/2, 1/2), \alpha = 0.4, P = 10^4$, and choose K_1 and $K_2 = K_1 + 10$ from (6.111) for each $k = 8$, $k = 10$, $k = 12$, and $k = 14$; i.e., we use $K_1 = 30, 33, 36, 38$, respectively.

sharper transition between 0 and 1 as we increase n, which is expected by virtue of Theorem 3.2 that provides sharp zero-one law in the limit of large network size. In addition, we observe that as we increase n, the fraction $\frac{\log n+(k-1)\log\log n}{n}$ decreases, leading to a decrease on the critical value of $K_{1,n}$ needed to ensure k-connectivity (for fixed P, α, and K_2.).

6.6.6 Additional preliminaries

A number of technical results are collected here for easy referencing.

Proposition 6.6.3. *Consider a scaling $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\alpha : \mathbb{N}_0 \to (0, 1)$. Let the sequence $\gamma : \mathbb{N}_0 \to \mathbb{R}$ be defined through (6.104) for each $n = 1, 2, \ldots$. Under (6.105) and (6.107), we have*

$$K_{1,n} = \omega(1) \tag{6.112}$$

when $\lim_{n\to\infty} \gamma_n = +\infty$.

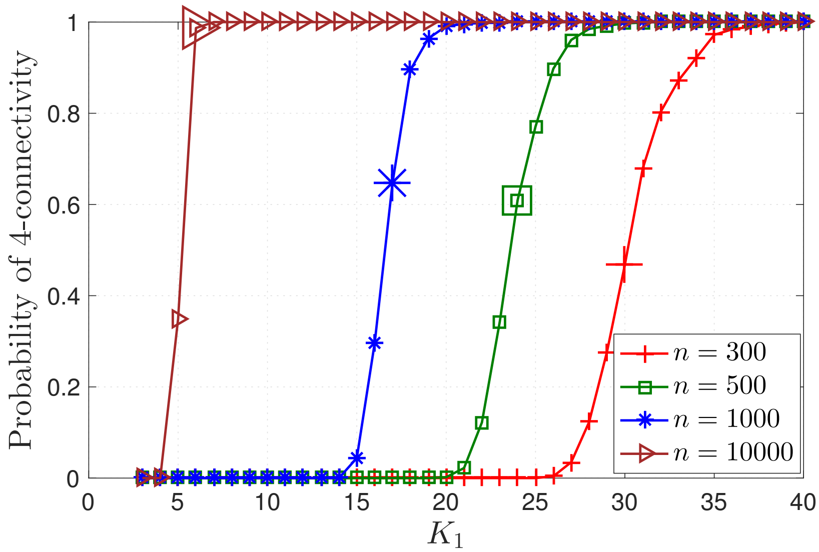


Figure 6.8: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ is 4-connected as a function of K_1 for $n = 300$, $n = 500$, $n = 1000$, and $n = 10000$, with $P = 10^4$; in each case, the empirical probability value is obtained by averaging over 1000 experiments. Highlighted symbols correspond to the critical values of K_1 obtained from (6.111).

Proof. From (6.104), we clearly have

$$\lambda_1(n) > \frac{\log n}{n\alpha_n} \tag{6.113}$$

for all n sufficiently large when $\lim_{n\to\infty} \gamma_n = +\infty$. We also know from [159, Lemmas 7.1-7.2] that

$$p_{1j}(n) \leq \frac{K_{1,n}K_{j,n}}{P_n - K_{j,n}} \leq 2\frac{K_{1,n}K_{j,n}}{P_n}, \quad j = 1, \ldots, r$$

where the last bound follows from (6.103). This leads to

$$\lambda_1(n) = \sum_{j=1}^{r} \mu_j p_{1j} \leq 2\sum_{j=1}^{r} \mu_j \frac{K_{1,n}K_{j,n}}{P_n} \leq 2\frac{K_{1,n}K_{r,n}}{P_n} \tag{6.114}$$

Combining (6.113) and (6.114) we get

$$K_{1,n}^2 \frac{K_{r,n}}{K_{1,n}} > \frac{P_n}{2} \frac{\log n}{n\alpha_n}$$

for all n sufficiently large. Under (6.105) and (6.107), this immediately establishes (6.112) since $\alpha_n \leq 1$. □

Fact 6.6.4. *For any positive constants ℓ_1, ℓ_2, the function*

$$f(x) = x^{\ell_1}(1-x)^{n-\ell_2}, \quad x \in (0,1) \tag{6.115}$$

is monotone decreasing in x for all n sufficiently large.

Proof. Differentiating $f(x)$ with respect to $x \in (0,1)$, we get

$$\begin{aligned} \frac{d}{dx} f(x) &= \ell_1 x^{\ell_1 - 1}(1-x)^{n-\ell_2} - (n-\ell_2)x^{\ell_1}(1-x)^{n-\ell_2-1} \\ &= x^{\ell_1-1}(1-x)^{n-\ell_2-1}(\ell_1(1-x) - (n-\ell_2)x). \end{aligned}$$

The conclusion follows since $(\ell_1(1-x) - (n-\ell_2)x) < 0$ for all n sufficiently large, for any positive ℓ_1, ℓ_2 and $x \in (0,1)$. □

Fact 6.6.5 ([166, Fact 3])**.** *Let x and y be positive functions of n. If $x = o(1)$, and $x^2 y = o(1)$ hold, then*

$$(1-x)^y \sim e^{-xy}$$

We will use several bounds given below throughout the chapter:

$$(x+y)^p \leq 2^{p-1}\left(x^p + y^p\right), \quad x, y \geq 0, \quad p \geq 1 \tag{6.116}$$

$$\binom{n}{\ell} \leq n^{\ell}, \quad \ell = 1, \ldots, n, \quad n = 1, 2, \ldots \tag{6.117}$$

6.6.7 Proof of Theorem 6.6.1

A roadmap

The proof of Theorem 6.6.1 consists of two parts. Namely, in Section 6.6.7, we establish the *one-law* part of Theorem 6.6.1, while in Section 6.6.7, we establish the *zero-law* part. In establishing the one-law part, we utilize the first moment method [73, Eqn. (3.1), p.54] to show that under the scaling condition (6.104) with $\lim_{n\to\infty}\gamma_n = \infty$, the number of nodes with degree ℓ in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$ is zero for $\ell = 0, 1, \ldots, k-1$ with high probability in the limit of large network size. The result implies that the *minimum* node degree of the graph is no less than k, which establishes the one-law part of Theorem 6.6.1. In establishing the zero-law part, we utilize the second moment method [73, Remark 3.1, p. 54] to show that under the scaling condition (6.104) with $\lim_{n\to\infty}\gamma_n = -\infty$, there exists at least one class-1 node with degree $\ell < k$ with high probability in the limit of large network size, which readily implies that the minimum node degree of the graph is less than k, i.e., the zero-law part of Theorem 6.6.1.

Establishing the one-law

The proof of Theorem 6.6.1 relies on the method of first and second moments applied to the number of nodes with degree ℓ in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$. Let $X_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the total number of nodes with degree ℓ in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$, namely,

$$X_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{i=1}^{n} \mathbf{1}\left[v_i \text{ is of degree } \ell \text{ in } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)\right]$$

The first moment method [73, Eqn. (3.1), p. 54] gives

$$\mathbb{P}\left[X_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = 0\right] \geq 1 - \mathbb{E}\left[X_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] \tag{6.118}$$

The one-law states that the minimum node degree in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$ is no less than k asymptotically almost surely (a.a.s.); i.e., $\lim_{n\to\infty}\mathbb{P}\left[X_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = 0\right] = 1$, for all $\ell =$

$0, 1, \ldots, k-1$. Thus, the one-law will follow if we show that

$$\lim_{n \to \infty} \mathbb{E}\left[X_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)\right] = 0, \quad \ell = 0, 1, \ldots, k-1. \tag{6.119}$$

We let $D_{i,\ell}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the event that node v_i in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$ has degree ℓ for each $i = 1, 2, \ldots, n$. Throughout, we simplify the notation by writing $D_{i,\ell}$ instead of $D_{i,\ell}(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)$. By definition, we have $X_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \sum_{i=1}^n \mathbf{1}\left[D_{i,\ell}\right]$ and it follows that

$$\mathbb{E}\left[X_\ell(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n)\right] = \sum_{i=1}^n \mathbb{P}\left[D_{i,\ell}\right] = n\mathbb{P}\left[D_{x,\ell}\right] \tag{6.120}$$

by the exchangeability of the indicator rvs $\{\mathbf{1}\left[D_{i,\ell}\right]; i = 1, \ldots, n\}$.

In view of (6.118) and (6.120), we see that (6.119) and hence the one-law would follow upon showing

$$\lim_{n \to \infty} n\mathbb{P}\left[D_{x,\ell}\right] = 0, \quad \ell = 0, 1, \ldots, k-1. \tag{6.121}$$

We start by deriving the probability of $D_{x,\ell}$. For any node v_x, the events[3]

$$E_{1x}, E_{2x}, \ldots, E_{(x-1)x}, E_{(x+1)x}, \ldots, E_{nx}$$

are mutually independent *conditionally* on the type t_x. It follows from (6.5) that the degree of a node v_x, i.e., D_x, is conditionally binomial leading to

$$D_x \overset{d}{=} \mathrm{Bin}(n-1, \Lambda_i), \quad \text{with probability } \mu_i, \quad i = 1, \ldots, r.$$

[3] Recall that E_{xy} denotes the event that nodes v_x and v_y are adjacent in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha)$.

Thus, we get

$$
\begin{aligned}
\mathbb{P}\left[D_{x,\ell}\right] &= \sum_{i=1}^{r} \mu_i \mathbb{P}\left[D_{x,\ell} \,\middle|\, t_x = i\right] \\
&= \sum_{i=1}^{r} \mu_i \binom{n-1}{\ell} \left(\Lambda_i(n)\right)^{\ell} \left(1-\Lambda_i(n)\right)^{n-\ell-1} \\
&\leq \left((\ell!)^{-1} \sum_{i=1}^{r} \mu_i \left(n\Lambda_i(n)\right)^{\ell} \left(1-\Lambda_i(n)\right)^{n-\ell-1} \right) \\
&\leq (\ell!)^{-1} \left(n\Lambda_1(n)\right)^{\ell} \left(1-\Lambda_1(n)\right)^{n-\ell-1} \\
&\leq (\ell!)^{-1} \left(n\Lambda_1(n)\right)^{\ell} e^{-(n-\ell-1)\Lambda_1(n)}
\end{aligned}
$$

for all n sufficiently large, as we invoke Fact 6.6.4 together with (6.7), and noting that ℓ is a non-negative integer constant and that $\binom{n-1}{\ell} \leq (\ell!)^{-1} n^{\ell}$. Combining (6.104) and (6.116), and using the fact that $\Lambda_1(n) \leq 1$, we see that

$$
\begin{aligned}
n\mathbb{P}\left[D_{x,\ell}\right] &\leq n\,(\ell!)^{-1} \left(\log n + (k-1)\log\log n + \gamma_n\right)^{\ell} e^{-\log n-(k-1)\log\log n-\gamma_n} e^{(\ell+1)\Lambda_1(n)} \\
&\leq 2^{\ell-1} \left((\log n)^{\ell} \left(1+o(1)\right)^{\ell} + \gamma_n^{\ell} \right) e^{-(k-1)\log\log n-\gamma_n} e^{O(1)} \\
&= O(1) e^{-(k-1-\ell)\log\log n-\gamma_n} + O(1)\gamma_n^{\ell} e^{-(k-1)\log\log n-\gamma_n}.
\end{aligned}
$$

When $\lim_{n\to\infty} \gamma_n = \infty$, we readily get the desired conclusion (6.121). This establishes the one-law.

Establishing the zero-law

Our approach in establishing the zero-law relies on the method of second moment applied to a variable that counts the number of nodes in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ that are *class*-1 and with degree ℓ. Similar to the discussion given before, we let $Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the total number of nodes that are class-1 and with degree ℓ in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$, namely,

$$Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{i=1}^{n} \mathbf{1}\left[v_i \text{ is class 1 and has degree } \ell \text{ in } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)\right] \tag{6.122}$$

Clearly, if we can show that whp there exists at least one class-1 node with a degree strictly less than k under the enforced assumptions (with $\lim_{n\to\infty}\gamma_n = -\infty$) then the zero-law immediately follows.

With a slight abuse of notations, we let $D_{i,\ell}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the event that node v_i in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ is class-1 and has degree ℓ for each $i = 1, 2, \ldots, n$. Throughout, we simplify the notation by writing $D_{i,\ell}$ instead of $D_{i,\ell}(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)$. Thus, we have $Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{i=1}^{n}\mathbf{1}\left[D_{i,\ell}\right]$. The second moment method [73, Remark 3.1, p. 54] gives

$$\mathbb{P}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = 0\right] \le 1 - \frac{\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right]^2}{\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)^2\right]}. \tag{6.123}$$

We have $\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] = n\mathbb{P}\left[D_{x,\ell}\right]$ and

$$\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)^2\right] = n\mathbb{P}\left[D_{x,\ell}\right] + n(n-1)\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell}\right],$$

whence

$$\frac{\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)^2\right]}{\mathbb{E}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right]^2} = \frac{1}{n\mathbb{P}\left[D_{x,\ell}\right]} + \frac{n-1}{n}\frac{\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell}\right]}{\left(\mathbb{P}\left[D_{x,\ell}\right]\right)^2}. \tag{6.124}$$

In view of (6.123) and (6.124), we will get $\lim_{n\to\infty}\mathbb{P}\left[Y_\ell(n;\boldsymbol{\mu},\boldsymbol{\Theta}_n) = 0\right] = 0$, for some $\ell = 0, 1, \ldots, k-1$ (which in turns establishes the zero-law) if we show that

$$\lim_{n\to\infty} n\mathbb{P}\left[D_{x,\ell}\right] = \infty, \tag{6.125}$$

and

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell}\right] \sim \left(\mathbb{P}\left[D_{x,\ell}\right]\right)^2 \tag{6.126}$$

for some $\ell = 0, 1, \ldots, k-1$.

The next two results will help establish (6.125) and (6.126) along two specific subsequences (on which $n\Lambda_1(n)$ has a limit) with a different value of ℓ for each particular subsequence.

Lemma 6.6.6. *If $\Lambda_1(n) = o\left(\frac{1}{\sqrt{n}}\right)$, then for any non-negative integer constant ℓ and any node v_x, we have*

$$\mathbb{P}\left[D_{x,\ell}\right] \sim \mu_1 \left(\ell!\right)^{-1} \left(n\Lambda_1(n)\right)^{\ell} e^{-n\Lambda_1(n)} \tag{6.127}$$

Proof. Considering any class-1 node v_i, and recalling (6.5), we know that the events

$$E_{1i}, E_{2i}, \ldots, E_{(i-1)i}, E_{(i+1)i}, \ldots, E_{ni}$$

are mutually independent. Thus, it follows that the degree of a given node v_i, conditioned on being class-1, follows a Binomial distribution $\mathrm{Bin}(n-1, \Lambda_1(n))$. Thus,

$$\begin{aligned}\mathbb{P}\left[D_{i,\ell}\right] &= \mu_1 \mathbb{P}\left[D_{i,\ell} \,\middle|\, t_i = 1\right] \\ &= \mu_1 \binom{n-1}{\ell} \Lambda_1(n)^{\ell} \left(1 - \Lambda_1(n)\right)^{n-\ell-1}\end{aligned}$$

Next, given that $\Lambda_1(n) = o\left(\frac{1}{\sqrt{n}}\right)$ and ℓ is constant, it follows that $\Lambda_1(n) = o(1)$ and $\Lambda_1(n)^2(n-\ell-1) = o(1)$. Invoking Fact 6.6.5, and the fact that $\binom{n-1}{\ell} \sim \left(\ell!\right)^{-1} n^{\ell}$, the conclusion (6.127) follows. □

Lemma 6.6.7. *Consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \to (0,1)$, such that $\lambda_1(n) = o(1)$ and (6.104) holds with $\lim_{n\to\infty} \gamma_n = -\infty$. The following two properties hold*

(a) If $n\Lambda_1(n) = \Omega(1)$, then for any non-negative integer constant ℓ and any two distinct nodes v_x and v_y, we have

$$\mathbb{P}\left[D_{x,\ell} \cap D_{y,\ell}\right] \sim \mu_1^2 \left(\ell!\right)^{-2} \left(n\Lambda_1(n)\right)^{2\ell} e^{-2n\Lambda_1(n)} \tag{6.128}$$

(b) For any two distinct nodes v_x and v_y, we have

$$\mathbb{P}\left[D_{x,0} \cap D_{y,0}\right] \sim \mu_1^2 e^{-2n\Lambda_1(n)} \tag{6.129}$$

Note that the events $D_{x,\ell}$ and $D_{y,\ell}$ already imply that nodes v_x and v_y are class-1, i.e., $|\Sigma_x| = |\Sigma_y| = K_1$. In this case, one may conjecture that the proof of Lemma 6.6.7 would precisely follow that of [166, Lemma 3] for the homogeneous case where all nodes receive the same number of keys K_1. Although the proof does follow that of [166, Lemma 3], we remark that even when we explicitly fix the class of the two particular nodes v_x and v_y, their adjacent nodes could still belong to any class. Hence, extra effort has to be made to precisely bound the probability that some vertex, say v_j, is adjacent to both v_x and v_y, as v_j could be class-i with probability μ_i. Since the proof of Lemma 6.6.7 closely (although, not entirely as we mentioned above) follows that of [166, Lemma 3], it is skipped here for brevity and given in [42, Appendix B] for completeness.

We now show why the zero-law follows from Lemma 6.6.6 and Lemma 6.6.7 by means of establishing (6.125) and (6.126) for some $\ell = 0, 1, \ldots, k-1$.

Let

$$P\left(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n\right) := \mathbb{P}\left[\text{ Minimum node degree of } \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{\theta}) \cap \mathbb{G}(n; \alpha) \geq k\right]$$

In what follows, we will consider the cases where $n\Lambda_1(n) = \Omega(1)$ and $n\Lambda_1(n) = o(1)$, separately. We will show that: i) when $n\Lambda_1(n) = \Omega(1)$, conditions (6.125) and (6.126) hold for $\ell = k-1$, thus we have $\lim_{n\to\infty} P\left(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n\right) = 0$; ii) when $n\Lambda_1(n) = o(1)$, conditions (6.125) and (6.126) hold for $\ell = 0$, hence we have $\lim_{n\to\infty} P\left(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n\right) = 0$. Collectively, we have $\lim_{n\to\infty} P\left(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n\right) = 0$ whenever $n\Lambda_1(n) = \Omega(1)$ or $n\Lambda_1(n) = o(1)$. By virtue of the *subsubsequence principle* [73, p. 12], this readily implies that $\lim_{n\to\infty} P\left(n; \boldsymbol{\mu}, \boldsymbol{\Theta}_n\right) = 0$ holds even when the sequence $n\Lambda_1(n)$ does not have a limit.

The case where there exists an $\epsilon > 0$ such that $n\Lambda_1(n) > \epsilon$ for all n sufficiently

large: In this case we will establish (6.125) and (6.126) for $\ell = k-1$. First, we see from (6.104) that $\Lambda_1(n) \leq \frac{\log n+(k-1)\log\log n}{n} = o\left(\frac{1}{\sqrt{n}}\right)$ when $\lim_{n\to\infty} \gamma_n = -\infty$. Invoking Lemma 6.6.6, this gives

$$n\mathbb{P}\left[D_{x,\ell}\right] \sim n\mu_1 \left(\ell!\right)^{-1} \left(n\Lambda_1(n)\right)^{\ell} e^{-n\Lambda_1(n)} \tag{6.130}$$

for each $\ell = 0, 1, \ldots$. Setting $\ell = k-1$ and substituting (6.104) into (6.130), we get

$$\begin{aligned} n\mathbb{P}\left[D_{x,\ell}\right] &\sim n\mu_1 \left[(k-1)!\right]^{-1} \left(n\Lambda_1(n)\right)^{k-1} e^{-\log n-(k-1)\log\log n-\gamma_n} \\ &= \mu_1 \left[(k-1)!\right]^{-1} \left(\log n + (k-1)\log\log n + \gamma_n\right)^{k-1} e^{-(k-1)\log\log n-\gamma_n} \end{aligned} \tag{6.131}$$

Let

$$f_n(k;\gamma_n) := \left(\log n + (k-1)\log\log n + \gamma_n\right)^{k-1} e^{-(k-1)\log\log n-\gamma_n},$$

and note that $(\log n + (k-1)\log\log n + \gamma_n) \geq \epsilon$ for all n sufficiently large by virtue of the fact that $n\Lambda_1(n) > \epsilon$. Fix n sufficiently large, pick $\zeta \in (0,1)$ and consider the cases when $\gamma_n \leq -(1-\zeta)\log n$ and $\gamma_n > -(1-\zeta)\log n$, separately. In the former case, we get

$$f_n(k;\gamma_n) \geq \epsilon e^{-(k-1)\log\log n+(1-\zeta)\log n},$$

and in the latter case, we get

$$f_n(k;\gamma_n) \geq \left(\zeta\log n\right)^{k-1} e^{-(k-1)\log\log n-\gamma_n} = \zeta^{k-1}e^{-\gamma_n}.$$

Thus, for all n sufficiently large, we have

$$f_n(k;\gamma_n) \geq \min\left\{\epsilon e^{-(k-1)\log\log n+(1-\zeta)\log n}, \zeta^{k-1}e^{-\gamma_n}\right\}.$$

It is now clear that

$$\lim_{n\to\infty} f_n(k;\gamma_n) = \infty, \tag{6.132}$$

since $\zeta \in (0,1)$ and $\lim_{n\to\infty}\gamma_n = -\infty$. Reporting (6.132) into (6.131), we establish (6.125). Furthermore, from Lemma 6.6.6 and Lemma 6.6.7, it is clear that (6.126) follows for $\ell = k-1$.

The case where $\lim_{n\to\infty} n\Lambda_1(n) = 0$**:** In this case, we will establish (6.125) and (6.126) for $\ell = 0$. Setting $\ell = 0$ in (6.130), we obtain

$$n\mathbb{P}\left[D_{x,0}\right] \sim n\mu_1 e^{n\Lambda_1(n)} \sim n\mu_1$$

by virtue of the fact that $n\Lambda_1(n) = o(1)$. This readily gives (6.125). Furthermore, from Lemma 6.6.6 (with $\ell = 0$) and Lemma 6.6.7, (6.126) immediately follows.

The two cases considered cover all the possibilities for the limit of $n\Lambda_1(n)$. By virtue of the subsubsequence principle [73, p. 12], we get the zero-law of Theorem 6.6.1 without any condition on the sequence $n\Lambda_1(n)$.

6.6.8 Proof of Theorem 6.6.2

A roadmap

The proof of Theorem 6.6.2 consists of two parts. Namely, in Section 6.6.8, we establish the *zero-law* part of Theorem 6.6.2, while in Section 6.6.8, we establish the *one-law* part. In establishing the zero-law part, we note that if the minimum node degree of a graph is strictly less than k, then the graph is certainly not k-connected. This follows from the fact that for a k-connected graph, there is no node with degree strictly less than k. The aforementioned observation indicates the zero-law part of Theorem 6.6.1 already implies the zero-law part of Theorem 6.6.2. The proof of the one-law part of Theorem 6.6.2 consists of several steps. The crux of the proof lies in showing that the probability of the vertex connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ being ℓ is zero for $\ell = 0, 1, \ldots, k-1$ in the limit of large network size. Specifically, we derive an upper bound on the probability of vertex connectivity being ℓ (for $\ell = 0, 1, \ldots, k-1$)

and show that each term appearing in the upper bound approaches zero as n tends to infinity under the scaling condition (6.104) with $\lim_{n\to\infty} \gamma_n = \infty$.

Establishing the zero-law

Let κ denote the vertex connectivity of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$, i.e., the minimum number of nodes to be deleted to make the graph disconnected. Also, let δ denote the minimum node degree in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta})\cap\mathbb{G}(n;\alpha)$. It is clear that if a random graph is k-connected, meaning that $\kappa \geq k$, then it does not have any node with degree less than k. Thus $[\kappa \geq k] \subseteq [\delta \geq k]$ and the conclusion

$$\mathbb{P}[\kappa \geq k] \leq \mathbb{P}[\delta \geq k] \tag{6.133}$$

immediately follows. In view of (6.133), we obtain the zero-law for k-connectivity, i.e., that

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha) \text{ is } k\text{-connected}] = 0,$$

when $\lim_{n\to\infty} \gamma_n = -\infty$ from the zero-law part of Theorem 6.6.1. Put differently, the conditions that lead to the zero-law part of Theorem 6.6.1, i.e., $\lambda_1(n) = o(1)$ and $\lim_{n\to\infty} \gamma_n = -\infty$, automatically lead to the zero-law part of Theorem 6.6.2.

Establishing the one-law

Before we proceed with the proof of the one-law of Theorem 6.6.2, we take a moment to explain why the probabilistic bounds that we derive next look substantially different than those given in [166] for the homogeneous case. In establishing the zero-law of Theorem 6.6.1, it was sufficient to show that there exists at least one node of class-1 with degree less than k to prove that the minimum node degree is less than k with high probability. As we fixed the key ring size of the node(s) under consideration, the heterogeneity *partially* vanished, rendering our probabilistic bounds closely related to the ones given in [166], except for some cases, as discussed in Section 6.6.7. However, as we establish the one-law of Theorem 6.6.2, the heterogeneity of the key ring sizes comes into play, leading to considerably more difficult expressions and substantially different bounds than the ones given in [166] for the homogeneous case. This will become apparent in Sections 6.6.9 and 6.6.10, where we prove a key result that establishes the one-law for k-connectivity.

An important step towards establishing the one-law of Theorem 6.6.2 is presented in Section 6.6.11. There, we show that it suffices to establish the one law in Theorem 6.6.2 under the additional condition that $\gamma_n = o\left(\log n\right)$, which leads to a number of useful consequences. Let a sequence $\beta_{\ell,n} : \mathbb{N} \times \mathbb{N}_0 \to \mathbb{R}$ be defined through the relation

$$\Lambda_1(n) = \frac{\log n + \ell \log\log n + \beta_{\ell,n}}{n} \tag{6.134}$$

for each $n \in \mathbb{N}_0$ and $\ell \in \mathbb{N}$. Put differently, we have

$$\beta_{\ell,n} := n\Lambda_1(n) - \log n - \ell \log\log n, \qquad \begin{array}{l} n = 1, 2, \ldots \\ \ell = 0, 1, \ldots, \end{array}$$

where as in (6.5), $\Lambda_1(n)$ is given by

$$\Lambda_1(n) = \sum_{j=1}^{r} \mu_j \alpha_n p_{1j} = \sum_{j=1}^{r} \mu_j \alpha_n \left(1 - \frac{\binom{P_n - K_{1,n}}{K_{j,n}}}{\binom{P_n}{K_{j,n}}}\right).$$

In view of the arguments in Section 6.6.11, the one-law (6.108) follows from the next result.

Theorem 6.6.8. *Let ℓ be a non-negative constant integer. Under (6.105), (6.106), (6.107), and (6.134) with $\beta_{\ell,n} = o\left(\log n\right)$ and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[\kappa = \ell\right] = 0.$$

Before we give a formal proof, we first explain why the one-law (6.108) follows from Theorem 6.6.8. Comparing (6.134) with (6.104) and noting that $\gamma_n = o\left(\log n\right)$, we get

$$\beta_{\ell,n} = (k-1-\ell)\log\log n + \gamma_n = o\left(\log n\right) \tag{6.135}$$

Moreover, for $\ell = 0, 1, \ldots, k-1$, we have

$$\lim_{n\to\infty} \beta_{\ell,n} = +\infty \tag{6.136}$$

by recalling the fact that $\lim_{n\to\infty} \gamma_n = +\infty$. Recalling (6.135) and (6.136), we notice that the conditions needed for Theorem 6.6.8 are met when $\ell = 0, 1, \ldots, k-1$; thus, we have $\mathbb{P}\left[\kappa = \ell\right] = o(1)$ for $\ell = 0, 1, \ldots, k-1$, which in turn implies that $\lim_{n\to\infty} \mathbb{P}\left[\kappa \geq k\right] = 1$, i.e., the one-law.

We now give a road map to the proof of Theorem 6.6.8. By a simple union bound, we get

$$\mathbb{P}\left[\kappa = \ell\right] \leq \mathbb{P}\left[\delta \leq \ell\right] + \mathbb{P}\left[(\kappa = \ell) \cap (\delta > \ell)\right].$$

It is now immediate that Theorem 6.6.8 is established once we show that

$$\lim_{n\to\infty} \mathbb{P}\left[\delta \leq \ell\right] = 0 \tag{6.137}$$

and

$$\lim_{n\to\infty} \mathbb{P}\left[(\kappa = \ell) \cap (\delta > \ell)\right] = 0 \tag{6.138}$$

under the enforced assumptions of Theorem 6.6.8. We start by establishing (6.137). Following the analysis of Section 6.6.7, it is easy to see that

$$\begin{aligned} n\mathbb{P}\left[D_{x,\ell}\right] &\leq 2^{\ell-1}\left(\left(\log n\right)^{\ell}\left(1+o(1)\right)^{\ell} + \beta_{\ell,n}^{\ell}\right) e^{-\ell\log\log n - \beta_{\ell,n}} e^{O(1)} \\ &= O(1)e^{-\beta_{\ell,n}} + O(1)\beta_{\ell,n}^{\ell} e^{-\ell\log\log n - \beta_{\ell,n}}, \end{aligned}$$

and it follows that $\lim_{n\to\infty} n\mathbb{P}\left[D_{x,\ell}\right] = 0$ as long as $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$. From (6.118) and (6.120), this yields

$$\lim_{n\to\infty} \mathbb{P}\left[\delta = \ell\right] = 0 \quad \text{when } \lim_{n\to\infty} \beta_{\ell,n} = +\infty \tag{6.139}$$

However, from (6.134) it is easy to see that $\beta_{\ell,n}$ is monotonically decreasing in ℓ. Thus, the fact that $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$ for some ℓ implies

$$\lim_{n\to\infty} \beta_{\hat{\ell},n} = +\infty, \quad \hat{\ell} = 0, 1, \ldots, \ell$$

From (6.139) this in turn implies that $\mathbb{P}[\delta = \hat{\ell}] = o(1)$ for $\hat{\ell} = 0, 1, \ldots, \ell$, or equivalently (6.137).

We now focus on establishing (6.138) under the enforced assumptions of Theorem 6.6.8. The proof is based on finding a tight upper bound on the probability $\mathbb{P}\left[(\kappa = \ell) \cap \delta > \ell\right]$ and showing that this bound goes to zero as n goes to infinity. Let $\mathcal{N}$ denote the collection of all non-empty subsets of $\{v_1, v_2, \ldots, v_n\}$. Define $\mathcal{N}_* = \{T : T \in \mathcal{N}, \ |T| \geq 2\}$ and

$$\mathcal{E}(\boldsymbol{J}) = \cup_{T\in\mathcal{N}_*} \left[\left| \cup_{v_i \in T} \Sigma_i\right| \leq J_{|T|}\right]$$

where $\boldsymbol{J} = [J_2, J_3, \ldots, J_n]$ is an $(n-1)$-dimensional integer-valued array. $\mathcal{E}(\boldsymbol{J})$ encodes the event that for at least one $|T| = 2, \ldots, n$, the total number of distinct keys held by at least one set of $|T|$ sensors is less than or equal to $J_{|T|}$. Now, define

$$m_n := \min\left(\left\lfloor \frac{P_n}{K_{1,n}} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor\right) \tag{6.140}$$

and let

$$J_i = \begin{cases} \max\left(\left\lfloor (1+\epsilon) K_{1,n} \right\rfloor, \left\lfloor i\zeta K_{1,n} \right\rfloor\right) & i = 2, \ldots, m_n \\ \left\lfloor \psi P_n \right\rfloor & i = m_n + 1, \ldots, n \end{cases} \tag{6.141}$$

for some ϵ chosen arbitrarily in $(0,1)$ and for some ζ, ψ in $(0,1)$ to be specified later at (6.142) and (6.143), respectively. A crude bounding argument gives

$$\mathbb{P}\left[(\kappa = \ell) \cap \delta > \ell\right] \leq \mathbb{P}\left[\mathcal{E}(\boldsymbol{J})\right] + \mathbb{P}\left[(\kappa = \ell) \cap \delta > \ell \cap \overline{\mathcal{E}(\boldsymbol{J})}\right]$$

Hence, establishing (6.138) consists of establishing the following two results.

Proposition 6.6.9. *Let ℓ be a non-negative constant integer. Assume that (6.134) holds with $\beta_{\ell,n} > 0$, and that we have (6.106) and (6.107). Also, assume that (6.105) holds such that*

$$P_n \geq \sigma n$$

for some $\sigma > 0$ for all n sufficiently large. Then

$$\lim_{n\to\infty} \mathbb{P}\left[\mathcal{E}(\boldsymbol{J})\right] = 0,$$

where $\boldsymbol{J}$ is as defined in (6.141) with arbitrary $\epsilon \in (0,1)$, constant $\zeta \in (0, \frac{1}{2})$ selected small enough such that

$$\max\left(2\zeta\sigma, \zeta\left(\frac{e^2}{\sigma}\right)^{\frac{\zeta}{1-2\zeta}}\right) < 1 \tag{6.142}$$

and $\psi \in (0, \frac{1}{2})$ selected small enough such that

$$\max\left(2\left(\sqrt{\psi}\left(\frac{e}{\psi}\right)^{\psi}\right)^{\sigma}, \sqrt{\psi}\left(\frac{e}{\psi}\right)^{\psi}\right) < 1 \tag{6.143}$$

Proof. The proof follows the same steps with [157, Proposition 7.2] to show that it suffices to establish Proposition 6.6.9 for the homogeneous case where all key rings are of the same size $K_{1,n}$. This is evident upon realizing that with $U_\ell(\boldsymbol{\mu},\boldsymbol{\theta}) = |\cup_{i=1}^{\ell} \Sigma_i|$ and $U_\ell(K_{1,n}, P_n) \overset{d}{=} U_\ell(\boldsymbol{\mu} = \{1, 0, \ldots, 0\}, \boldsymbol{\theta})$, we have

$$U_\ell(K_{1,n}, P_n) \preceq U_\ell(\boldsymbol{\mu},\boldsymbol{\theta}),$$

where $\preceq$ denotes the usual stochastic ordering. After this reduction, the proof reduces to [166, Proposition 3]. The proof only require conditions (6.105), (6.112), and $K_{1,n} = o(P_n)$ to hold. We note that $K_{1,n} = o(P_n)$ follows from (6.106) and the fact that $K_{1,n} \leq K_{r,n}$. Also, (6.112) follows under the enforced assumptions as shown in Proposition 6.6.3. □

Proposition 6.6.10. *Let ℓ be a non-negative constant integer. Under (6.105), (6.106), (6.107), and (6.134) with $\beta_{\ell,n} = o\left(\log n\right)$ and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[(\kappa = \ell) \cap (\delta > \ell) \cap \overline{\mathcal{E}(\boldsymbol{J})}\right] = 0$$

The proof of Proposition 6.6.10 is given in Section 6.6.9. Proposition 6.6.9 and Proposition 6.6.10 establish (6.138) which, combined with (6.137), establish Theorem 6.6.8. We recall that Theorem 6.6.8 establishes the one-law.

6.6.9 Proof of Proposition 6.6.10

For notational simplicity, we denote $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{\theta}) \cap \mathbb{G}(n;\alpha)$ by $\mathbb{KG}$. Let $\mathbb{KG}(U)$ be a subgraph of $\mathbb{KG}$ restricted to the vertex set U. For any subset of nodes U, define $U^c := \{v_1, \ldots, v_n\} \setminus U$. We also let $\mathcal{N}_{U^c}$ denote the collection of all non-empty subsets of $\{v_1, v_2, \ldots, v_n\} \setminus U$. We note that a subset T of $\mathcal{N}_{U^c}$ is isolated in $\mathbb{KG}(U^c)$ if there are no edges in $\mathbb{KG}$ between nodes in T and nodes in $U^c \setminus T$, i.e.,

$$\overline{E_{ij}}, \quad v_i \in T, \quad v_j \in U^c \setminus T.$$

Next, we present key observations that pave the way to establishing Proposition 6.6.10. If $\kappa = \ell$ but $\delta > \ell$, then there exists subsets U and T of nodes with $U \in \mathcal{N}$, $|U| = \ell$, $T \in \mathcal{N}_{U^c}$, $|T| \geq 2$ such that $\mathbb{KG}(T)$ is connected while T is isolated in $\mathbb{KG}(U^c)$. This ensures that $\mathbb{KG}$ can be disconnected by deleting a properly selected set of ℓ nodes, i.e., the set U. This would not be possible for sets $T \in \mathcal{N}_{U^c}$ with $|T| = 1$ since we have $\delta \geq \ell + 1$ which implies that the single node in T is connected to at least one node in $U^c \setminus T$. Finally, having $\kappa = \ell$ ensures that $\mathbb{KG}$ remains connected after removing $(\ell - 1)$ nodes. Then, if there exists a subset U with

$|U| = \ell$ such that some $T \in \mathcal{N}_{U^c}$ is isolated in $\mathbb{KG}(U^c)$, each node in U must be connected to at least one node in T and at least one node in $U^c \setminus T$. This can be proved by contradiction. Consider subsets $U \in \mathcal{N}$ with $|U| = \ell$, and $T \in \mathcal{N}_{U^c}$ with $|T| \geq 2$, such that T is isolated from $U^c \setminus T$. Suppose there exists a node $v_i \in U$ such that v_i is adjacent to at least one node in T but not adjacent to any node in $U^c \setminus T$. In this case, it is easy to see that there are no edges between nodes in $U^c \setminus T$ and nodes in $\{v_i\} \cup T$. Thus, the graph could have been made disconnected by removing nodes in $U \setminus \{v_i\}$. But $|U \setminus \{v_i\}| = \ell - 1$, and this contradicts the fact that $\kappa = \ell$.

We now present several events that characterize the aforementioned observations. For each non-empty subset $T \subseteq U^c$, we define $\mathcal{C}_T$ as the event that $\mathbb{KG}(T)$ is itself connected, and $\mathcal{D}_{U,T}$ as the event that T is isolated in $\mathbb{KG}(U^c)$, i.e.,

$$\mathcal{D}_{U,T} := \bigcap_{\substack{v_i \in T \\ v_j \in U^c \setminus T}} \overline{E_{ij}},$$

Moreover, we define $\mathcal{B}_{U,T}$ as the event that each node in U is adjacent to at least one node in T, i.e.,

$$\mathcal{B}_{U,T} := \bigcap_{v_i \in U} \bigcup_{v_j \in T} E_{ij},$$

and finally, we let $\mathcal{A}_{U,T} := \mathcal{B}_{U,T} \cap \mathcal{D}_{U,T} \cap \mathcal{C}_T$. It is clear that $\mathcal{A}_{U,T}$ encodes the event that $\mathbb{KG}(T)$ is itself connected, each node in U is adjacent to at least one node in T, but T is isolated in $\mathbb{KG}(U^c)$. The aforementioned observations enable us to express the event $[(\kappa = \ell) \cap (\delta > \ell)]$ in terms of the event sequence $\mathcal{A}_{U,T}$. In particular, we have

$$[(\kappa = \ell) \cap (\delta > \ell)] \subseteq \bigcup_{U \in \mathcal{N}_{n,\ell}, T \in \mathcal{N}_{U^c}, |T| \geq 2} \mathcal{A}_{U,T}$$

with $\mathcal{N}_{n,\ell}$ denoting the collection of all subsets of $\{v_1, \ldots, v_n\}$ with exactly ℓ elements. We also note that the union need only to be taken over all subsets T with $2 \leq |T| \leq \left\lfloor \frac{n-\ell}{2} \right\rfloor$. This is because if the vertices in T form a component then so do the vertices in $\mathcal{N}_{U^c} \setminus T$. Now, using a standard union bound, we obtain

$$\begin{aligned}\mathbb{P}\left[(\kappa=\ell)\cap(\delta>\ell)\cap\overline{\mathcal{E}(\boldsymbol{J})}\right] &\leq \sum_{U\in\mathcal{N}_{n,\ell},T\in\mathcal{N}_{U^c},2\leq|T|\leq\left\lfloor\frac{n-\ell}{2}\right\rfloor}\mathbb{P}\left[\mathcal{A}_{U,T}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]\\ &=\sum_{m=2}^{\left\lfloor\frac{n-\ell}{2}\right\rfloor}\sum_{U\in\mathcal{N}_{n,\ell},T\in\mathcal{N}_{U^c,m}}\mathbb{P}\left[\mathcal{A}_{U,T}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]\end{aligned}$$

where $\mathcal{N}_{U^c,m}$ denotes the collection of all subsets of U^c with exactly m elements. Now, for each $m=1,\ldots,n-\ell-1$, we simplify the notation by writing $\mathcal{A}_{\ell,m}:=\mathcal{A}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+m}\}}$, $\mathcal{D}_{\ell,m}:=\mathcal{D}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+m}\}}$, $\mathcal{B}_{\ell,m}:=\mathcal{B}_{\{v_1,\ldots,v_\ell\},\{v_{\ell+1},\ldots,v_{\ell+m}\}}$, and $\mathcal{C}_m:=\mathcal{C}_{\{v_{\ell+1},\ldots,v_{\ell+m}\}}$. From exchangeability, we get

$$\mathbb{P}\left[\mathcal{A}_{U,T}\right]=\mathbb{P}\left[\mathcal{A}_{\ell,m}\right],\quad U\in\mathcal{N}_{n,\ell},\quad T\in\mathcal{N}_{U^c,m}$$

and the key bound

$$\mathbb{P}\left[(\kappa=\ell)\cap(\delta>\ell)\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]\leq\sum_{m=2}^{\left\lfloor\frac{n-\ell}{2}\right\rfloor}\binom{n}{\ell}\binom{n-\ell}{m}\mathbb{P}\left[\mathcal{A}_{\ell,m}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]\tag{6.144}$$

is readily obtained upon noting that $|\mathcal{N}_{n,\ell}|=\binom{n}{\ell}$ and $|\mathcal{N}_{U^c,m}|=\binom{n-\ell}{m}$. Thus, Proposition 6.6.10 will be established if we show that

$$\lim_{n\to\infty}\sum_{m=2}^{\left\lfloor\frac{n-\ell}{2}\right\rfloor}\binom{n}{\ell}\binom{n-\ell}{m}\mathbb{P}\left[\mathcal{A}_{\ell,m}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]=0.\tag{6.145}$$

We now derive bounds for the probabilities $\mathbb{P}\left[\mathcal{A}_{\ell,m}\cap\overline{\mathcal{E}(\boldsymbol{J})}\right]$. First, for $m=2,\ldots,n-\ell-1$, we have

$$\mathcal{D}_{\ell,m}=\bigcap_{j=m+\ell+1}^{n}\left[\left(\cup_{i\in\nu_{m,j}}\Sigma_i\right)\cap\Sigma_j=\emptyset\right]\tag{6.146}$$

where $\nu_{m,j}$ is defined as

$$\nu_{m,j}:=\{i=\ell+1,\ldots,\ell+m:C_{ij}\}$$

for each $j = 1, \ldots, \ell$ and $j = m + \ell + 1, \ldots, n$. Put differently, $\nu_{m,j}$ is the set of indices in $i = \ell + 1, \ldots, \ell + m$ for which nodes v_j and v_i are adjacent in the Erdős-Rényi graph $\mathbb{G}(n; \alpha_n)$. Then, (6.146) follows from the fact that for v_j to be isolated from $\{v_{\ell+1}, \ldots, v_{\ell+m}\}$ in $\mathbb{KG}$, Σ_j needs to be disjoint from each of the key rings $\{\Sigma_i : i \in \nu_{m,j}\}$.

Now, using the law of iterated expectation, we get

$$\begin{aligned}
\mathbb{P}\left[\mathcal{D}_{\ell,m} \;\middle|\; \Sigma_{\ell+1}, \ldots, \Sigma_{\ell+m}\right] &= \mathbb{E}\left[\mathbf{1}\left[\mathcal{D}_{\ell,m}\right] \;\middle|\; \Sigma_{\ell+1}, \ldots, \Sigma_{\ell+m}\right] \\
&= \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[\mathcal{D}_{\ell,m}\right] \;\middle|\; \substack{\Sigma_{\ell+1}, \ldots, \Sigma_n \\ C_{ij}, i=\ell+1,\ldots,\ell+m \\ j=\ell+m+1,\ldots,n}\right] \;\middle|\; \Sigma_{\ell+1}, \ldots, \Sigma_{\ell+m}\right] \\
&= \mathbb{E}\left[\prod_{j=\ell+m+1}^{n}\left(\frac{\binom{P-|\cup_{i\in\nu_{m,j}}\Sigma_i|}{|\Sigma_j|}}{\binom{P}{|\Sigma_j|}}\right) \;\middle|\; \Sigma_{\ell+1}, \ldots, \Sigma_{\ell+m}\right] \\
&= \mathbb{E}\left[\frac{\binom{P-|\cup_{i\in\nu_m}\Sigma_i|}{|\Sigma|}}{\binom{P}{|\Sigma|}} \;\middle|\; \Sigma_{\ell+1}, \ldots, \Sigma_{\ell+m}\right]^{n-\ell-m} \qquad (6.147)
\end{aligned}$$

by independence of the random variables $\nu_{m,j}$ and $|\Sigma_j|$ for $j = \ell + m + 1, \ldots, n$. Here we define ν_m and $|\Sigma|$ as generic random variables following the same distribution with any of $\{\nu_{m,j}, j = \ell + m + 1, \ldots, n\}$ and $\{|\Sigma_j|, j = \ell + m + 1, \ldots, n\}$, respectively. Put differently, $|\nu_m|$ is a Binomial rv with parameters m and α, while $|\Sigma|$ is a rv that takes the value K_j with probability μ_j.

Next, we bound the probabilities $\mathbb{P}\left[\mathcal{B}_{\ell,m}\right]$. We know that

$$\mathcal{B}_{\ell,m} = \cap_{i=1}^{\ell} \cup_{j=\ell+1}^{m} E_{ij}.$$

Thus,

$$\begin{aligned}\mathbb{P}\left[\mathcal{B}_{\ell,m} \,\middle|\, \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] &= \mathbb{E}\left[\mathbf{1}\left[\mathcal{B}_{\ell,m}\right] \,\middle|\, \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] \\ &= \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[\mathcal{B}_{\ell,m}\right] \,\middle|\, {}_{\substack{\Sigma_1,\ldots,\Sigma_{\ell+m} \\ C_{ij}, i=\ell+1,\ldots,\ell+m \\ j=1,\ldots,\ell}}\right] \,\middle|\, \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] \\ &= \mathbb{E}\left[\prod_{j=1}^{\ell}\left(1-\frac{\binom{P-|\cup_{i\in\nu_{m,j}}\Sigma_i|}{|\Sigma_j|}}{\binom{P}{|\Sigma_j|}}\right) \,\middle|\, \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right] \\ &= \mathbb{E}\left[1-\frac{\binom{P-|\cup_{i\in\nu_m}\Sigma_i|}{|\Sigma|}}{\binom{P}{|\Sigma|}} \,\middle|\, \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right]^{\ell} \qquad (6.148)\end{aligned}$$

by independence of the random variables $\nu_{m,j}$ and $|\Sigma_j|$ for $j = 1,\ldots,\ell$.

We note that, on the event $\overline{\mathcal{E}(\boldsymbol{J})}$, we have

$$|\cup_{i\in\nu_m}\Sigma_i| \geq \left(J_{|\nu_m|}+1\right)\mathbf{1}\left[|\nu_m|>1\right]$$

and it is always the case that $|\cup_{i\in\nu_m}\Sigma_i| \geq K_1\mathbf{1}\left[|\nu_m|>0\right]$ and

$$|\cup_{i\in\nu_m}\Sigma_i| \leq |\nu_m|K_r. \qquad (6.149)$$

Next, we define

$$L(\nu_m) = \max\left(K_1\mathbf{1}\left[|\nu_m|>0\right], \left(J_{|\nu_m|}+1\right)\mathbf{1}\left[|\nu_m|>1\right]\right)$$

so that on $\overline{\mathcal{E}(\boldsymbol{J})}$, we have

$$|\cup_{i\in\nu_m}\Sigma_i| \geq L(\nu_m). \qquad (6.150)$$

Using (6.150) in (6.147) and (6.149) in (6.148), we get

$$\begin{aligned}
\mathbb{P}\left[\mathcal{A}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}\right] &= \mathbb{E}\left[\mathbf{1}\left[\mathcal{C}_m\right]\mathbf{1}\left[\mathcal{B}_{\ell,m}\right]\mathbf{1}\left[\mathcal{D}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}\right]\right] \\
&= \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[\mathcal{C}_m\right]\mathbf{1}\left[\mathcal{B}_{\ell,m}\right]\mathbf{1}[\mathcal{D}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}] \;\middle|\; {}^{\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}}_{C_{ij},i,j=\ell+1,\ldots,\ell+m}\right]\right] \\
&= \mathbb{E}\left[\mathbf{1}\left[\mathcal{C}_m\right]\mathbb{P}\left[\mathcal{B}_{\ell,m} \;\middle|\; \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right]\mathbb{P}\left[\mathcal{D}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})} \;\middle|\; \Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\right]\right]
\end{aligned} \tag{6.151}$$

since $\mathcal{C}_m$ is fully determined by the rvs $\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}$ and $\{C_{ij}, i,j = \ell+1,\ldots,\ell+m\}$ while $\mathcal{B}_{\ell,m}$, $\mathcal{D}_{\ell,m}$, and $\mathcal{E}(\boldsymbol{J})$ are independent from $\{C_{ij}, i,j = \ell+1,\ldots,\ell+m\}$. Here, we also used the fact that given $\{\Sigma_{\ell+1},\ldots,\Sigma_{\ell+m}\}$, $\mathcal{D}_{\ell,m}$ is independent from $\mathcal{B}_{\ell,m}$.

The following lemma provides upper bounds for (6.151).

Lemma 6.6.11. *Let $\boldsymbol{J}$ be defined as in (6.141) for some $\epsilon \in (0,1)$, $\zeta \in \left(0,\frac{1}{2}\right)$ such that (6.142) holds, $\psi \in \left(0,\frac{1}{2}\right)$ such that (6.143) holds. Assume that $\Lambda_1(n) = o(1)$ and (6.105), (6.106), and (6.107) hold. Then for all n sufficiently large, and for each $m = 2,3,\ldots,n$, we have*

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{A}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}\right] \\
&\leq \min\left\{1, m^{m-2}\left(\alpha_n p_{rr}(n)\right)^{m-1}\right\}\left(\mathbf{1}\left[m > \left\lfloor\frac{P_n - K_{r,n}}{2K_{r,n}}\right\rfloor\right] + \mathbf{1}\left[m \leq \left\lfloor\frac{P_n - K_{r,n}}{2K_{r,n}}\right\rfloor\right]\left(1 - e^{-3m\alpha_n p_{rr}(n)}\right)^{\ell}\right)\cdot \\
&\cdot\left(\min\left\{1 - \Lambda_1(n), e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)}, e^{-\psi K_{1,n}}\mathbf{1}\left[m > m_n\right] + \min\left\{1 - \mu_r + \mu_r e^{-\alpha_n p_{1r}(n)\zeta m}, e^{-\alpha_n p_{11}(n)\zeta m}\right\}\right\}\right)^{n-m-\ell}
\end{aligned} \tag{6.152}$$

The proof of Lemma 6.6.11 is given in Section 6.6.12. Now, the proof of Proposition 6.6.10 will be completed upon establishing (6.145) by means of Lemma 6.6.11. We devote Section 6.6.10 to establishing (6.145).

6.6.10 Establishing (6.145)

A roadmap

Our objective is to establish (6.145) using the bounds given by Lemma 6.6.11. We start by defining $f_{n,\ell,m}$ as

$$f_{n,\ell,m} = \binom{n}{\ell}\binom{n-\ell}{m}\mathbb{P}\left[\mathcal{A}_{\ell,m} \cap \overline{\mathcal{E}(\boldsymbol{J})}\right]$$

Thus, establishing (6.145) becomes equivalent to showing

$$\lim_{n\to\infty} \sum_{m=2}^{\left\lfloor \frac{n-\ell}{2} \right\rfloor} f_{n,\ell,m} = 0. \tag{6.153}$$

Our approach is to establish (6.153) in several steps with each step focusing on a specific range of m. In particular, we can write

$$\sum_{m=2}^{\left\lfloor \frac{n-\ell}{2} \right\rfloor} f_{n,\ell,m} = \sum_{m=2}^{M} f_{n,\ell,m} + \sum_{M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} f_{n,\ell,m} + \sum_{\min\{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor, m_n\}}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} f_{n,\ell,m} + \sum_{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} f_{n,\ell,m} + \sum_{\lfloor \nu n \rfloor + 1}^{\left\lfloor \frac{n-\ell}{2} \right\rfloor} f_{n,\ell,m}, \tag{6.154}$$

where M is an integer to be specified later at (6.164) and $\nu \in \left(0, \frac{1}{2}\right)$ is to be specified later at (6.170). In establishing (6.153), we will show that each term appearing in (6.154) approaches zero as n tends to infinity using the bounds given by Lemma 6.6.11. This will be established in Section 6.6.10 through Section 6.6.10, where we use different approaches and utilize different bounds from Lemma 6.6.11 to show that each term appearing in (6.154) approaches zero as n tends to infinity. Finally, in this section, we make use of the following lemma several times.

Lemma 6.6.12. *Consider a scaling* $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ *and a scaling* $\alpha : \mathbb{N}_0 \to (0,1)$ *such that (6.134) holds with* $\beta_{\ell,n} = o(\log n)$*. We have*

$$\frac{1}{2}\frac{\log n}{n} \leq \alpha_n p_{1r}(n) \leq \frac{2}{\mu_r}\frac{\log n}{n}, \tag{6.155}$$

for all n sufficiently large, i.e., $\alpha_n p_{1r}(n) = \Theta\left(\frac{\log n}{n}\right)$. If in addition (6.107) holds, we have

$$\alpha_n p_{rr}(n) = o\left(\log n\right)\alpha_n p_{1r}(n) = o\left(\frac{(\log n)^2}{n}\right) \tag{6.156}$$

and

$$\alpha_n p_{1r}(n) = o\left(\log n\right)\alpha_n p_{11}(n) \tag{6.157}$$

The proof of Lemma 6.6.12 is given in Section 6.6.15.

We now proceed with establishing (6.145). Throughout, we consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \rightarrow \mathbb{N}_0^{r+1}$ and $\alpha : \mathbb{N}_0 \rightarrow (0,1)$ such that (6.134) holds with $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$ and $\beta_{\ell,n} = o(\log n)$, and (6.105), (6.106), (6.107) hold. We will make repeated use of the bounds (6.10), (6.11), (6.117), and (6.156).

The case where $2 \leq m \leq M$

This range considers fixed values of m. Pick an integer M to be specified later at (6.164). We note that on this range we have $m \leq \lfloor \frac{P_n - K_{r,n}}{2K_{r,n}} \rfloor$ for all n sufficiently large by virtue of (6.106). On the same range we also have

$$1 - e^{-3m\alpha_n p_{rr}(n)} \leq 3m\alpha_n p_{rr}(n) \tag{6.158}$$

by virtue of (6.156), (6.12), and the fact that m is bounded.

Using (6.117), (6.152), (6.156), and (6.158), and noting that $\Lambda_1(n) = o(1)$ under (6.134) with $\beta_{\ell,n} = o(\log n)$, we get

$$\begin{aligned}
f_{n,\ell,m} &\leq n^\ell n^m m^{m-2} \left(\alpha_n p_{rr}(n)\right)^{m-1} (3m)^\ell \left(\alpha_n p_{rr}(n)\right)^\ell e^{-\left(1+\frac{\epsilon}{2}\right)(n-m-\ell)\Lambda_1(n)} \\
&= O(1) n^{\ell+m} \left(\alpha_n p_{rr}(n)\right)^{\ell+m-1} e^{-\left(1+\frac{\epsilon}{2}\right)(n-m-\ell)\Lambda_1(n)} \\
&= o(1) n^{\ell+m} \left(\frac{(\log n)^2}{n}\right)^{\ell+m-1} e^{-\left(1+\frac{\epsilon}{2}\right)\left(\log n + \ell \log\log n + \beta_{\ell,n}\right)} \\
&= o(1) n^{-\frac{\epsilon}{2}} (\log n)^{\ell\left(1-\frac{\epsilon}{2}\right)+2(m-1)} e^{-\left(1+\frac{\epsilon}{2}\right)\beta_{\ell,n}} \\
&= o(1)
\end{aligned}$$

since ℓ is non-negative integer constant, m is bounded, and $\lim_{n\to\infty} \beta_{\ell,n} = +\infty$. This establishes

$$\lim_{n\to\infty} \sum_{m=2}^{M} f_{n,\ell,m} = 0.$$

The case where $M + 1 \leq m \leq \min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}$

Our goal in this and the next subsubsection is to cover the range $M+1 \leq m \leq \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor$. Since the bound given at (6.152) takes a different form when $m > m_n$ (with m_n defined at (6.140)), we first consider the range $M+1 \leq m \leq \min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}$; we note from (6.106) and (6.103) that $\lim_{n\to\infty} m_n = \infty$.

On the range considered here, we have from (6.10), (6.117), and (6.152) that

$$\sum_{m=M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} f_{n,\ell,m} \leq \sum_{m=M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} n^\ell \left(\frac{en}{m}\right)^m m^{m-2} \left(\alpha_n p_{rr}(n)\right)^{m-1} \left(1 - \mu_r \left(1 - e^{-\alpha_n p_{1r}(n)\zeta m}\right)\right)^{n-m-\ell}. \tag{6.159}$$

From the upper bound in (6.155) and the fact that $m \leq \frac{\mu_r n}{2\zeta \log n}$ for all n sufficiently large, we have

$$\alpha_n p_{1r}(n) \zeta m \leq \frac{2\log n}{\mu_r n} \zeta \frac{\mu_r n}{2\zeta \log n} = 1.$$

Using the fact that $1 - e^{-x} \geq \frac{x}{2}$ for all $0 \leq x \leq 1$, we get

$$\begin{aligned} 1 - \mu_r \left(1 - e^{-\alpha_n p_{1r}(n)\zeta m}\right) &\leq 1 - \frac{\mu_r \alpha_n p_{1r}(n)\zeta m}{2} \\ &\leq e^{-\zeta m \mu_r \frac{\log n}{4n}} \end{aligned} \tag{6.160}$$

as we invoke (6.12) and the lower bound in (6.155). Reporting this last bound and (6.156) into (6.159), and noting that

$$n - m - \ell \geq \frac{n-\ell}{2} \geq \frac{n}{3}, \qquad m = 2, 3, \ldots, \left\lfloor \frac{n-\ell}{2} \right\rfloor, \tag{6.161}$$

we get

$$\begin{aligned} \sum_{m=M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} f_{n,\ell,m} &\leq \sum_{m=M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} n^{\ell+m} e^m \left(\frac{(\log n)^2}{n}\right)^{m-1} e^{-\zeta m \mu_r \log n \frac{n-m-\ell}{4n}} \\ &\leq n^{\ell+1} \sum_{m=M+1}^{\infty} \left(e \left(\log n\right)^2 e^{-\zeta \frac{\mu_r}{12} \log n}\right)^m \end{aligned} \tag{6.162}$$

for all n sufficiently large. Given that $\zeta, \mu_r > 0$ we have

$$e \left(\log n\right)^2 e^{-\zeta \frac{\mu_r}{12} \log n} = o(1). \tag{6.163}$$

Thus, the geometric series in (6.162) is summable for n sufficiently large, and we have

$$\sum_{m=M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} f_{n,\ell,m} \leq O(1) n^{\ell+1-(M+1)\zeta \frac{\mu_r}{12}} \left(e \log n\right)^{2(M+1)}$$

and it follows that

$$\lim_{n\to\infty} \sum_{m=M+1}^{\min\{m_n, \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor\}} f_{n,\ell,m} = 0$$

for any positive integer M with

$$M > \frac{12(\ell+1)}{\zeta \mu_r}. \tag{6.164}$$

This choice is permissible given that $\zeta, \mu_r > 0$.

The case where $\min\{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor, m_n\} < m \leq \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor$

Clearly, this range becomes obsolete if $m_n \geq \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor$. Thus, it suffices to consider the subsequences for which the range $m_n + 1 \leq m \leq \lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor$ is non-empty. On this range, following the same arguments that lead to (6.159) and (6.162) gives

$$\begin{aligned}\sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} f_{\ell,n,m} &\leq \sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} n^{\ell+1} \left(e(\log n)^2\right)^m \left(1 - \mu_r \left(1 - e^{-\zeta m \alpha_n p_{1r}(n)}\right) + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \\ &\leq n^{\ell+1} \sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} \left(e\left(\log n\right)^2\right)^m \left(e^{-\zeta m \mu_r \frac{\log n}{4n}} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \qquad (6.165)\end{aligned}$$

where in the last step we used (6.160) in view of $m \leq \frac{\mu_r n}{2\zeta \log n}$. Next, we write

$$\begin{aligned}e^{-\zeta m \mu_r \frac{\log n}{4n}} + e^{-\psi K_{1,n}} &= e^{-\zeta m \mu_r \frac{\log n}{4n}} \left(1 + e^{-\psi K_{1,n} + \zeta m \mu_r \frac{\log n}{4n}}\right) \\ &\leq \exp\left\{-\zeta m \mu_r \frac{\log n}{4n} + e^{-\psi K_{1,n} + \zeta m \mu_r \frac{\log n}{4n}}\right\} \\ &\leq \exp\left\{-\zeta m \mu_r \frac{\log n}{4n} \left(1 - \frac{e^{-\psi K_{1,n} + \frac{\mu_r^2}{8}}}{\zeta m \mu_r \frac{\log n}{4n}}\right)\right\} \qquad (6.166)\end{aligned}$$

where the last inequality is obtained from $m \leq \frac{\mu_r n}{2\zeta \log n}$. Using the fact that $m > m_n = \min\{\lfloor \frac{P_n}{K_{1,n}} \rfloor, \lfloor \frac{n}{2} \rfloor\}$ and that $P_n \geq \sigma n$ for some $\sigma > 0$ under (6.105), we have

$$\begin{aligned}\frac{e^{-\psi K_{1,n} + \frac{\mu_r^2}{8}}}{\zeta m \mu_r \frac{\log n}{4n}} &\leq \max\left\{\frac{K_{1,n}}{P_n}, \frac{2}{n}\right\} 4n \frac{e^{-\psi K_{1,n}}}{\zeta \mu_r \log n} \cdot e^{\frac{\mu_r^2}{8}} \\ &\leq \max\left\{\frac{4K_{1,n} e^{-\psi K_{1,n}}}{\zeta \mu_r \sigma \log n}, \frac{8 e^{-\psi K_{1,n}}}{\zeta \mu_r \log n}\right\} \cdot e^{\frac{\mu_r^2}{8}} \\ &= o(1)\end{aligned}$$

by virtue of (6.112) and the facts that $\zeta, \mu_r, \sigma > 0$. Reporting this into (6.166), we see that for for any $\varepsilon > 0$, there exists a finite integer $n^*(\varepsilon)$ such that

$$\left(e^{-\zeta m \mu_r \frac{\log n}{4n}} + e^{-\psi K_{1,n}}\right) \leq e^{-\zeta m \mu_r \frac{\log n}{4n}(1-\varepsilon)} \tag{6.167}$$

for all $n \geq n^*(\varepsilon)$. Using (6.167) in (6.165), we get

$$\begin{aligned}\sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} f_{\ell,n,m} &\leq n^{\ell+1} \sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} \left(e\left(\log n\right)^2\right)^m \left(e^{-\zeta m \mu_r \frac{\log n}{4n}(1-\varepsilon)}\right)^{\frac{n}{3}} \\ &\leq n^{\ell+1} \sum_{m=m_n+1}^{\infty} \left(e\left(\log n\right)^2 e^{-\zeta \mu_r \frac{\log n}{12}(1-\varepsilon)}\right)^m \end{aligned} \tag{6.168}$$

Similar to (6.163), we have $e\left(\log n\right)^2 e^{-\zeta \mu_r \frac{\log n}{12}(1-\varepsilon)} = o(1)$ so that the sum in (6.168) converges for n sufficiently large. Following a similar approach to that in Section 6.6.10, we then see that

$$\sum_{m=m_n+1}^{\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor} f_{n,\ell,m} = O(1) n^{\ell+1-m_n \frac{\zeta \mu_r (1-\varepsilon)}{12}} (e \log n)^{2(m_n+1)} = o(1)$$

since $\lim_{n\to\infty} m_n = \infty$ under the enforced assumptions.

The case where $\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1 \leq m \leq \lfloor \nu n \rfloor$

We consider $\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1 \leq m \leq \lfloor \nu n \rfloor$ for some $\nu \in \left(0, \frac{1}{2}\right)$ to be specified later at (6.170). Recalling (6.10), (6.117), (6.152), (6.155), and (6.161), and noting that $\binom{n}{m}$ is monotone increasing in m when $0 \leq m \leq \left\lfloor \frac{n}{2} \right\rfloor$, we get

$$\begin{aligned}
\sum_{m=\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} f_{n,\ell,m} &\leq \sum_{m=\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} n^{\ell} \binom{n}{\lfloor \nu n \rfloor} \left(1 - \mu_r + \mu_r e^{-\zeta m \alpha_n p_{1r}(n)} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \\
&\leq n^{\ell} \sum_{m=\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\zeta \frac{\mu_r n}{2\zeta \log n} \frac{\log n}{2n}} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \\
&\leq n^{\ell+1} \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}} + e^{-\psi K_{1,n}}\right)^{\frac{n}{3}} \\
&= n^{\ell+1} \left(\left(\frac{e}{\nu}\right)^{3\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}} + e^{-\psi K_{1,n}}\right)\right)^{\frac{n}{3}} \qquad (6.169)
\end{aligned}$$

for all n sufficiently large.

We have $1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}} < 1$ from $\mu_r > 0$ and $e^{-\psi K_{1,n}} = o(1)$ from (6.112). Also, it holds that $\lim_{\nu \to 0} \left(\frac{e}{\nu}\right)^{3\nu} = 1$. Thus, if we pick ν small enough to ensure that

$$\left(\frac{e}{\nu}\right)^{3\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}}\right) < 1, \qquad (6.170)$$

then for any $0 < \varepsilon < 1 - (e/\nu)^{3\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}}\right)$ there exists a finite integer $n^{\star}(\varepsilon)$ such that

$$\left(\frac{e}{\nu}\right)^{3\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\mu_r}{4}} + e^{-\psi K_{1,n}}\right) \leq 1 - \varepsilon, \quad \forall n \geq n^{\star}(\varepsilon).$$

Reporting this into (6.169), we get

$$\lim_{n \to \infty} \sum_{m=\lfloor \frac{\mu_r n}{2\zeta \log n} \rfloor + 1}^{\lfloor \nu n \rfloor} f_{n,\ell,m} = 0$$

since $\lim_{n \to \infty} n^{\ell+1} (1 - \varepsilon)^{n/3} = 0$ for any positive constant integer ℓ.

The case where $\lfloor \nu n \rfloor + 1 \leq m \leq \lfloor \frac{n-\ell}{2} \rfloor$

In this range, we use (6.11), (6.117), (6.152), and (6.161) to get

$$\begin{aligned}
\sum_{m=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n-\ell}{2} \rfloor} f_{n,\ell,m} &\leq n^{\ell} \sum_{m=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n-\ell}{2} \rfloor} \binom{n}{m} \left(e^{-\zeta m \alpha_n p_{11}(n)} + e^{-\psi K_{1,n}} \right)^{\frac{n}{3}} \\
&\leq n^{\ell} \left(\sum_{m=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n-\ell}{2} \rfloor} \binom{n}{m} \right) \left(e^{-\zeta \nu n \alpha_n p_{11}(n)} + e^{-\psi K_{1,n}} \right)^{\frac{n}{3}} \\
&\leq n^{\ell} \left(8 e^{-\zeta \nu n \alpha_n p_{11}(n)} + 8 e^{-\psi K_{1,n}} \right)^{\frac{n}{3}}
\end{aligned}$$

Noting that $\zeta, \nu, \psi > 0$ and recalling (6.157) and the lower bound of (6.155), we get

$$e^{-\zeta \nu n \alpha_n p_{11}(n)} = e^{-\zeta \nu n \frac{w_n}{\log n} \alpha_n p_{1r}(n)} \leq e^{-\frac{\zeta \nu w_n}{2}}$$

for some sequence w_n satisfying $\lim_{n\to\infty} w_n = +\infty$. It is now obvious that $e^{-\zeta \nu n \alpha_n p_{11}(n)} = o(1)$. Moreover, we have $e^{-\psi K_{1,n}} = o(1)$ from (6.112). The conclusion

$$\lim_{n\to\infty} \sum_{m=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n-\ell}{2} \rfloor} f_{n,\ell,m} = 0$$

immediately follows and the proof of one-law is completed.

6.6.11 Confining γ_n

In this section, we show that establishing the one-law of Theorem 6.6.2 under the additional constraint

$$\gamma_n = o(\log n) \tag{6.171}$$

establishes the one-law for the case when that additional constraint is not present. Namely, we will show that for any scaling that satisfies conditions (6.105), (6.106), (6.107), and (6.104) with $\lim_{n\to\infty} \gamma_n = +\infty$, there exists a scaling that satisfies the same conditions with $\lim_{n\to\infty} \gamma_n =$

$+\infty$ *and* $\gamma_n = o(\log n)$, such that the probability of k-connectivity under the latter scaling (with $\gamma_n = o(\log n)$) is less than or equal to that under the former scaling.

Firstly, consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$, a scaling $K_1^*, K_2^*, \ldots, K_r^*, P^* : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, and a scaling $\alpha^* : \mathbb{N}_0 \to (0,1)$ such that

$$\Lambda_1^*(n) = \alpha_n^* \lambda_1^*(n) = \frac{\log n + (k-1)\log\log n + \gamma_n^*}{n}, \tag{6.172}$$

for each $n = 1, 2, \ldots$. Assume that

$$P_n^* = \Omega(n), \quad \frac{K_{r,n}^*}{P_n^*} = o(1), \quad \text{and} \quad \frac{K_{r,n}^*}{K_{1,n}^*} = o(\log n) \tag{6.173}$$

and that we have $\lim_{n\to\infty} \gamma_n^* = +\infty$; i.e., the *-scaling satisfies all conditions enforced by part (b) of Theorem 6.6.2.

Now, with the same distribution $\boldsymbol{\mu}$, consider a scaling $\hat{K}_1, \hat{K}_2, \ldots, \hat{K}_r, \hat{P} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and a scaling $\hat{\alpha} : \mathbb{N}_0 \to (0,1)$ such that $\hat{P}_n = P_n^*$ and $\hat{\boldsymbol{K}}_n = \boldsymbol{K}_n^*$. Obviously, we have $\hat{\lambda}_1(n) = \lambda_1^*(n)$ by recalling (6.2) and (6.3) and also that

$$\hat{P}_n = \Omega(n), \quad \frac{\hat{K}_{r,n}}{\hat{P}_n} = o(1), \quad \text{and} \quad \frac{\hat{K}_{r,n}}{\hat{K}_{1,n}} = o(\log n).$$

Next, let $\hat{\gamma}_n := \min(\gamma_n^*, \log\log n)$ and define $\hat{\alpha}_n$ through

$$\hat{\alpha}_n \hat{\lambda}_1(n) = \frac{\log n + (k-1)\log\log n + \hat{\gamma}_n}{n}. \tag{6.174}$$

Clearly, we have $\hat{\gamma}_n = o(\log n)$ and $\lim_{n\to\infty} \hat{\gamma}_n = +\infty$. This establishes that for any scaling satisfying the conditions of part (b) of Theorem 6.6.2, there exists another scaling (with the same $\boldsymbol{\mu}, \boldsymbol{K}_n$, and P_n) that satisfies all of the same conditions *and* (6.171). In addition, this latter scaling has a smaller probability of a channel being *on* than the original scaling; i.e., we have

$$\hat{\alpha}_n \leq \alpha_n^*, \qquad n = 2, 3, \ldots \tag{6.175}$$

by virtue of the fact that $\hat{\gamma}_n \leq \gamma_n^*$ for all n.

In view of the above, we will establish that part (b) of Theorem 6.6.2 under $\gamma_n = o(\log n)$ implies Theorem 6.6.2 if we show that

$$\mathbb{P}\left[\begin{array}{l}\mathbb{KG}(n; \boldsymbol{\mu}, \boldsymbol{K}_n^*, P_n^*, \alpha_n^*) \\ \text{is } k-\text{connected}\end{array}\right] \geq \mathbb{P}\left[\begin{array}{l}\mathbb{KG}(n; \boldsymbol{\mu}, \hat{\boldsymbol{K}}_n, \hat{P}_n, \hat{\alpha}_n) \\ \text{is } k-\text{connected}\end{array}\right] \tag{6.176}$$

This is clear since (6.176) would ensure that if $\mathbb{KG}(n; \boldsymbol{\mu}, \hat{\boldsymbol{K}}_n, \hat{P}_n, \hat{\alpha}_n)$ is k-connected asymptotically almost surely (as would be deduced from Theorem 6.6.2 under $\gamma_n = o(\log n)$), then so would $\mathbb{KG}(n; \boldsymbol{\mu}, \boldsymbol{K}_n^*, P_n^*, \alpha_n^*)$.

In view of (6.175), we get (6.176) by means of an easy coupling argument showing that $\mathbb{KG}(n; \boldsymbol{\mu}, \hat{\boldsymbol{K}}_n, \hat{P}_n, \hat{\alpha}_n)$ is a spanning subgraph of $\mathbb{KG}(n; \boldsymbol{\mu}, \boldsymbol{K}_n^*, P_n^*, \alpha_n)$. This follows from the fact that under (6.175) the corresponding Erdős-Rényi graphs satisfy

$$\mathbb{G}(n; \hat{\alpha}_n) \subseteq \mathbb{G}(n; \alpha_n^*)$$

meaning that for any monotone increasing graph property $\mathcal{P}$ (e.g., k-connectivity), the probability that $\mathbb{G}(n; \alpha_n^*)$ has $\mathcal{P}$ is larger than that of $\mathbb{G}(n; \hat{\alpha}_n)$; see [166, Section V.B] for details.

6.6.12 Proof of Lemma 6.6.11

The following result will be utilized in the proof of Lemma 6.6.11.

Lemma 6.6.13. *With $m \geq 2$ and $\Lambda_1(n) = o(1)$, we have*

$$\mathbb{E}\left[\frac{\binom{P_n - Q(\nu_m)}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)},$$

for all n sufficiently large and any $\epsilon \in (0,1)$, where we define

$$Q(\nu_m) = K_{1,n}\mathbf{1}\left[|\nu_m| = 1\right] + \left(\lfloor (1+\epsilon)\, K_{1,n} \rfloor + 1\right)\mathbf{1}\left[|\nu_m| > 1\right].$$

Proof. Consider fixed $\boldsymbol{K}, P$. We have

$$Q(\nu_m) \geq K_1 \left(\mathbf{1}\left[|\nu_m| = 1\right] + (1+\epsilon)\mathbf{1}\left[|\nu_m| > 1\right]\right)$$

Thus, by recalling (6.9), we get

$$\begin{aligned}\mathbb{E}\left[\frac{\binom{P-Q(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] &\leq \mathbb{E}\left[\frac{\binom{P-K_1}{|\Sigma|}}{\binom{P}{|\Sigma|}}^{\mathbf{1}[|\nu_m|=1]+(1+\epsilon)\mathbf{1}[|\nu_m|>1]}\right] \\ &= \mathbb{E}\left[Z^{\mathbf{1}[|\nu_m|=1]+(1+\epsilon)\mathbf{1}[|\nu_m|>1]}\right]\end{aligned}$$

where $Z = \frac{\binom{P-K_1}{|\Sigma|}}{\binom{P}{|\Sigma|}}$. Taking the expectation over $|\nu_m|$, we get

$$\begin{aligned}\mathbb{E}\left[\frac{\binom{P-Q(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] &\leq \mathbb{E}\Big[(1-\alpha)^m + m\alpha\,(1-\alpha)^{m-1} Z + \left(1-(1-\alpha)^m - m\alpha\,(1-\alpha)^{m-1}\right) Z^{1+\epsilon}\Big] \\ &\leq \mathbb{E}\Big[(1-\alpha)^2 + 2\alpha\,(1-\alpha)\,Z + \left(1-(1-\alpha)^2 - 2\alpha\,(1-\alpha)\right) Z^{1+\epsilon}\Big] \\ &= (1-\alpha)^2 + 2\alpha\,(1-\alpha)\,\mathbb{E}[Z] + \alpha^2\mathbb{E}\left[Z^{1+\epsilon}\right]\end{aligned}$$

by virtue of the fact that

$$(1-\alpha)^m + m\alpha\,(1-\alpha)^{m-1}\,T + \left(1-(1-\alpha)^m - m\alpha\,(1-\alpha)^{m-1}\right) T^{1+\epsilon}$$

is monotonically decreasing in m (see [166, Lemma 12]).

Next, we have

$$\mathbb{E}\left[Z\right] = \sum_{j=1}^{r} \mu_j \frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}} = 1 - \lambda_1$$

Also by recalling Fact 6.4.6, we get

$$\begin{aligned}
\mathbb{E}\left[Z^{1+\epsilon}\right] &= \mathbb{E}\left[\left(\frac{\binom{P-K_1}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right)^{1+\epsilon}\right] \\
&= \sum_{j=1}^{r} \mu_j \left(\frac{\binom{P-K_1}{K_j}}{\binom{P}{K_j}}\right)^{1+\epsilon} \\
&= \sum_{j=1}^{r} \mu_j (1-p_{1j})(1-p_{1j})^{\epsilon} \\
&\leq \sum_{j=1}^{r} \mu_j (1-p_{1j})(1-\epsilon p_{1j}) \\
&= 1-\lambda_1(1+\epsilon)+\epsilon\sum_{j=1}^{r}\mu_j p_{1j}^2.
\end{aligned}$$

From Proposition 6.4.4, we have

$$\begin{aligned}
\sum_{j=1}^{r} \mu_j \left(1-p_{1j}\right)^2 &= \mathbb{E}\left[Z\right]^2 + \mathrm{var}\left[Z\right] \\
&\leq \left(1-\lambda_1\right)^2 + \frac{1}{4}\left(p_{1r}\right)^2 \\
&\leq 1-2\lambda_1+\lambda_1^2\left(1+\frac{1}{4\mu_r^2}\right)
\end{aligned}$$

since $p_{1r} \leq \lambda_1/\mu_r$. This gives

$$\sum_{j=1}^{r} \mu_j p_{1j}^2 \leq \lambda_1^2\left(1+\frac{1}{4\mu_r^2}\right)$$

and we get

$$\begin{aligned}
\mathbb{E}\left[\frac{\binom{P-Q(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] &\leq \left(1-\alpha\right)^2 + 2\alpha\left(1-\alpha\right)\left(1-\lambda_1\right) + \alpha^2\left(1-\lambda_1\left(1+\epsilon\right)+\epsilon\lambda_1^2\left(1+\frac{1}{4\mu_r^2}\right)\right) \\
&= 1-\Lambda_1\left(2-(1-\epsilon)\alpha-\epsilon\left(1+\frac{1}{4\mu_r^2}\right)\Lambda_1\right)
\end{aligned}$$

Now, consider a scaling such that $\Lambda_1(n) = o(1)$. We have $\Lambda_1(n) \leq \frac{4\mu_r^2}{2(4\mu_r^2+1)}$ for all n

sufficiently large. Given also that $\alpha_n \leq 1$, we get

$$\mathbb{E}\left[\frac{\binom{P_n - Q(\nu_m)}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq 1 - \Lambda_1(n)\left(2 - (1-\epsilon) - \frac{\epsilon}{2}\right) \leq e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)}$$

by virtue of (6.12) for all n sufficiently large. This completes the proof. □

Lemma 6.6.11 will be established by bounding each term in (6.151). First, we note from [157, Proposition 9.1] that

$$\mathbb{P}\left[\mathcal{C}_m\right] \leq m^{m-2}\left(\alpha_n p_{rr}(n)\right)^{m-1}$$

Next, we derive upper bounds on the terms $\mathbb{E}\left[1 - \frac{\binom{P-|\nu_m|K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]$ and $\mathbb{E}\left[\frac{\binom{P-L(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]$, respectively. It is clear that Lemma 6.6.11 will follow if we show that

$$\mathbb{E}\left[1 - \frac{\binom{P_n - |\nu_m|K_{r,n}}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq 1 - e^{-3\alpha_n p_{rr}(n)m} \tag{6.177}$$

for all $m \leq \lfloor \frac{P-K_{r,n}}{2K_{r,n}} \rfloor$ and that

$$\mathbb{E}\left[\frac{\binom{P_n - L(\nu_m)}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq \min\left(1 - \Lambda_1(n), e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)}, \min\left(1 - \mu_r + \mu_r e^{-\alpha_n p_{1r}(n)\zeta m}, e^{-\alpha_n p_{11}(n)\zeta m}\right) + e^{-\psi K_{1,n}}\mathbf{1}\left[m > m_n\right]\right). \tag{6.178}$$

We establish (6.177) and (6.178) in turn in the next two sections.

6.6.13 Establishing (6.177)

First, with $m \leq \frac{P-K_r}{2K_r}$, we have $|\nu_m| \leq m \leq \frac{P-K_r}{2K_r}$ and using Fact 6.4.7 we get

$$\mathbb{E}\left[1 - \frac{\binom{P-|\nu_m|K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \leq \mathbb{E}\left[1 - \left(\frac{\binom{P-K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right)^{2|\nu_m|}\right] = 1 - \mathbb{E}\left[W^{2|\nu_m|}\right] \tag{6.179}$$

where we set $W = \frac{\binom{P-K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}}$. We also have

$$\begin{aligned}\mathbb{E}\left[W^{2|\nu_m|}\right] &= \mathbb{E}\left[\sum_{j=0}^{m}\binom{m}{j}\alpha^j\left(1-\alpha\right)^{m-j}W^{2j}\right] \\ &= \mathbb{E}\left[\left(1-\alpha\left(1-W^2\right)\right)^m\right] \\ &\geq \mathbb{E}\left[\left(1-2\alpha\left(1-W\right)\right)^m\right] \end{aligned} \tag{6.180}$$

using Fact 6.4.6 in the last step. We also know that

$$W = \frac{\binom{P-K_r}{|\Sigma|}}{\binom{P}{|\Sigma|}} \geq \frac{\binom{P-K_r}{K_r}}{\binom{P}{K_r}} = 1 - p_{rr} \tag{6.181}$$

Thus,

$$\alpha_n(1-W_n) \leq \alpha_n p_{rr}(n) \leq \frac{1}{4}$$

for all n sufficiently large by virtue of (6.156) and that $\beta_{\ell,n} = o\left(\log n\right)$. Using the fact that $1 - 2x \geq e^{-3x}$ for all $0 \leq x \leq \frac{1}{4}$, we then get from (6.180) and (6.181) that

$$\mathbb{E}\left[W_n^{2|\nu_m|}\right] \geq \mathbb{E}\left[e^{-3\alpha_n(1-W_n)m}\right] \geq e^{-3\alpha_n p_{rr}(n)m}$$

for all n sufficiently large. The desired conclusion (6.177) now follows immediately by means of (6.179).

6.6.14 Establishing (6.178)

Let $\boldsymbol{Y}$ be defined as follows

$$Y_i = \begin{cases} \lfloor i\zeta K_{1,n} \rfloor & i = 2, \ldots, m_n \\ \lfloor \psi P_n \rfloor & i = m_n + 1, \ldots, n \end{cases}$$

where $\zeta \in (0, \frac{1}{2})$ selected small enough such that (6.142) holds, and $\psi \in (0, \frac{1}{2})$ selected small enough such that (6.143) holds. Recalling (6.141), we see that

$$J_i = \begin{cases} \max\left(\lfloor (1+\epsilon)\, K_{1,n} \rfloor, Y_i\right) & i = 2, \ldots, m_n \\ Y_i & i = m_n + 1, \ldots, n \end{cases}$$

Next, we let

$$M(\nu_m) = K_{1,n}\mathbf{1}\left[|\nu_m| = 1\right] + \max\left(K_{1,n}, Y_{|\nu_m|} + 1\right)\mathbf{1}\left[|\nu_m| > 1\right],$$

and

$$Q(\nu_m) = K_{1,n}\mathbf{1}\left[|\nu_m| = 1\right] + \left(\lfloor (1+\epsilon)\, K_{1,n} \rfloor + 1\right)\mathbf{1}\left[|\nu_m| > 1\right].$$

We also recall that

$$L(\nu_m) = \max\left(K_{1,n}\mathbf{1}\left[|\nu_m| > 0\right], \left(J_{|\nu_m|} + 1\right)\mathbf{1}\left[|\nu_m| > 1\right]\right)$$

Let's consider the following three cases:

1. $|\nu_m| = 0$: In this case we have $L(\nu_m) = M(\nu_m) = Q(\nu_m) = 0$.
2. $|\nu_m| = 1$: In this case we have $L(\nu_m) = M(\nu_m) = Q(\nu_m) = K_{1,n}$.
3. $|\nu_m| \geq 2$: In this case we have
   - $M(\nu_m) = \max\left(K_{1,n}, Y_{|\nu_m|} + 1\right)$.
   - $Q(\nu_m) = \lfloor (1+\epsilon)\, K_{1,n} \rfloor + 1$.
   - $L(\nu_m) = \max\left(K_{1,n}, J_{|\nu_m|} + 1\right)$.

More specifically, considering the case when $|\nu_m| = 2, 3, \ldots, m_n$, we have

$$J_{|\nu_m|} = \max\left((1+\epsilon)K_{1,n}, Y_{|\nu_m|}\right)$$

and it follows that

$$\begin{aligned}L(\nu_m) &= \max\left(K_{1,n}, \lfloor(1+\epsilon)K_{1,n}\rfloor + 1, Y_{|\nu_m|}+1\right)\\ &= \max\left(\lfloor(1+\epsilon)K_{1,n}\rfloor + 1, M(\nu_m)\right)\\ &= \max\left(Q(\nu_m), M(\nu_m)\right)\end{aligned}$$

Also, when $|\nu_m| = m_n+1, \ldots, n$, we clearly have $J_{|\nu_m|} = Y_{|\nu_m|}$, and thus

$$L(\nu_m) = M(\nu_m) = \max\left(K_{1,n}, \lfloor\psi P_n\rfloor + 1\right).$$

Since $K_{1,n} \leq K_{r,n} = o(P_n)$ in view of (6.106), we have

$$\lfloor\psi P_n\rfloor \geq \lfloor(1+\epsilon)\, K_{1,n}\rfloor$$

for all n sufficiently large. Thus, we can rewrite $L(\nu_m)$ as

$$\begin{aligned}L(\nu_m) &= \max\left(K_{1,n}, \lfloor\psi P_n\rfloor + 1, \lfloor(1+\epsilon)\, K_{1,n}\rfloor + 1\right)\\ &= \max\left(Q(\nu_m), M(\nu_m)\right).\end{aligned}$$

Combining, we conclude that it always holds that $L(\nu_m) = \max\left(Q(\nu_m), M(\nu_m)\right)$, whence

$$\mathbb{E}\left[\frac{\binom{P-L(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \leq \min\left(\mathbb{E}\left[\frac{\binom{P-M(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right], \mathbb{E}\left[\frac{\binom{P-Q(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right]\right) \tag{6.182}$$

Note that it was shown in [50, Lemma 7.2] that

$$\mathbb{E}\left[\frac{\binom{P-M(\nu_m)}{|\Sigma|}}{\binom{P}{|\Sigma|}}\right] \leq \min\left(1-\Lambda_1(n), \min\left(1-\mu_r+\mu_r e^{-\alpha_n p_{1r}(n)\zeta m}, e^{-\alpha_n p_{11}(n)\zeta m}\right) + e^{-\psi K_{1,n}}\mathbf{1}\left[m > m_n\right]\right)$$

for all n sufficiently large. On the same range, we also get from Lemma 6.6.13 that

$$\mathbb{E}\left[\frac{\binom{P_n - Q(\nu_m)}{|\Sigma|}}{\binom{P_n}{|\Sigma|}}\right] \leq e^{-\left(1+\frac{\epsilon}{2}\right)\Lambda_1(n)}$$

upon noting that $\Lambda_1(n) = o(1)$ under (6.134) with $\beta_{\ell,n} = o(\log n)$. Reporting the last two bounds into (6.182), we establish (6.178).

6.6.15 Proof of Lemma 6.6.12

From (6.134) and the fact that $\beta_{\ell,n} = o(\log n)$, we clearly have

$$\frac{1}{2}\frac{\log n}{n} \leq \Lambda_1(n) \leq 2\frac{\log n}{n} \tag{6.183}$$

for all n sufficiently large. We also have

$$\Lambda_1(n) = \alpha_n \sum_{j=1}^{r} \mu_j p_{1j}(n) \geq \mu_r \alpha_n p_{1r}(n)$$

Now, since p_{1j} is monotone increasing in $j = 1, \ldots, r$ (see the proof of Proposition 6.4.4), we also see that

$$\Lambda_1(n) = \alpha_n \sum_{j=1}^{r} \mu_j p_{1j}(n) \leq \alpha_n p_{1r}(n) \sum_{j=1}^{r} \mu_j = \alpha_n p_{1r}(n)$$

Thus, we obtain that

$$\Lambda_1(n) \leq \alpha_n p_{1r}(n) \leq \frac{1}{\mu_r}\Lambda_1(n)$$

and the conclusion (6.155) immediately follows by virtue of (6.183) for all n sufficiently large.

Next, we establish (6.156). Here this will be established by showing that

$$p_{rr}(n) \leq \max\left(2, 4\frac{\log n}{w_n}\right) p_{1r}(n), \quad n = 2, 3, \ldots \tag{6.184}$$

for some sequence w_n such that $\lim_{n\to\infty} w_n = \infty$. Fix $n = 2, 3, \ldots$. We have either $p_{1r}(n) > \frac{1}{2}$, or $p_{1r}(n) \leq \frac{1}{2}$. In the former case, it automatically holds that

$$p_{rr}(n) \leq 2p_{1r}(n) \tag{6.185}$$

by virtue of the fact that $p_{rr}(n) \leq 1$.

Assume now that $p_{1r}(n) \leq \frac{1}{2}$. We know from [159, Lemmas 7.2] that

$$1 - e^{-\frac{K_{j,n}K_{r,n}}{P_n}} \leq p_{jr}(n) \leq \frac{K_{j,n}K_{r,n}}{P_n - K_{j,n}}, \quad j = 1, \ldots, r \tag{6.186}$$

and it follows that

$$\frac{K_{1,n}K_{r,n}}{P_n} \leq \log\left(\frac{1}{1 - p_{1r}(n)}\right) \leq \log 2 < 1. \tag{6.187}$$

Using the fact that $1 - e^{-x} \geq \frac{x}{2}$ with x in $(0, 1)$, we then get

$$p_{1r}(n) \geq \frac{K_{1,n}K_{r,n}}{2P_n}. \tag{6.188}$$

In addition, using the upper bound in (6.186) with $j = r$ gives

$$p_{rr}(n) \leq \frac{K_{r,n}^2}{P_n - K_{r,n}} \leq 2\frac{K_{r,n}^2}{P_n}$$

as we invoke (6.103). Combining the last two bounds we obtain

$$\frac{p_{rr}(n)}{p_{1r}(n)} \leq 4\frac{K_{r,n}}{K_{1,n}} \tag{6.189}$$

Next, combining (6.107) and (6.189), we get

$$p_{rr}(n) \leq 4\frac{\log n}{w_n} p_{1r}(n) \tag{6.190}$$

for some sequence w_n such that $\lim_{n\to\infty} w_n = \infty$. Combining (6.185) and (6.190), we readily obtain (6.184).

It is easy to see that (6.157) can be established using the same steps with the proof of (6.184).

6.7 Conclusion

In this chapter, we have investigated the secure and reliable connectivity of wireless sensor networks secured by the heterogeneous random key predistribution scheme under an on-ff channel model. The heterogeneous random key predistribution scheme induced an inhomogeneous random key graph, denoted $\mathbb{K}\left(n;\boldsymbol{\mu},\boldsymbol{K},P\right)$, while the on-ff channel model induced an Erdős-Rényi graph, denoted $\mathbb{G}\left(n;\alpha\right)$. Hence, we modeled the overall network by the intersection of both graphs, denoted $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\alpha)$. Namely, two vertices v_i and v_j are adjacent in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\alpha)$ if i) they share a cryptographic key and ii) have a communication channel in between that is on. We have presented conditions on how to scale the parameter of the intersection model $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\alpha)$ so that i) it has no isolated node, ii) is connected, iii) the minimum node degree of is no less than k , and iv) is k-connected, all with high probability in the limit of large network size. We then proceeded by presenting numerical results that supported our theorems in the *finite*-node regime. Moreover, we demonstrated via simulations that our results are also useful when the on-ff channel model is replaced with the more realistic *disk communication model.*

Chapter 7

Results on inhomogeneous random key graphs intersecting inhomogeneous Erdős-Rényi graphs

7.1 Motivation

In Chapter 6, we investigated the connectivity of wireless sensor networks secured by the heterogeneous random key predistribution scheme [157] under a *uniform* on-off channel model, where the channel between two nodes is on (respectively, off) with probability α (respectively, $1-\alpha$). The heterogeneous scheme induces inhomogeneous random key graphs $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$, while the independent on-off channel model induces an Erdős-Rényi graph $\mathbb{G}(n;\alpha)$. Hence, the overall model is given by a composite random graph formed by the intersection of inhomogeneous random key graphs and Erdős-Rényi graph, i.e., $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\alpha)$. An edge exists in the intersection graph if it exists in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)$, i.e., both node share at least a key, and $\mathbb{G}(n;\alpha)$, i.e., both nodes have an available wireless channel.

In this chapter, we consider a *heterogeneous* on-off channel model, instead of the uniform on-off model used in Chapter 6. In this channel model, the wireless channel between a class-i node and a class-j node is on with probability α_{ij} and off with probability $1-\alpha_{ij}$, independently. This gives rise to a $r\times r$ channel probability matrix $\boldsymbol{\alpha}$ where the element at the ith row and jth column is given by α_{ij}. The heterogeneous on-off channel model accounts for the fact that different nodes could have different radio capabilities, or could be deployed in locations with different channel characteristics. In addition, it offers the flexibility of modeling several interesting scenarios, such as when nodes of the same type are more (or less) likely to be adjacent with one another than with nodes belonging to other classes. The heterogeneous on-off channel model gives rise to inhomogeneous Erdős-Rényi graphs [19, 32], denoted hereafter by $\mathbb{G}(n, \boldsymbol{\mu}, \boldsymbol{\alpha})$. In these graphs, each of the n vertices is classified as class-i with probability $\mu_i > 0$ such that $\sum_{i=1}^{r} \mu_i = 1$. Two vertices v_x and v_y, which belong to class-i and class-j, respectively, are adjacent if $B(\alpha_{ij}) = 1$, where $B(\alpha_{ij})$ denotes a Bernoulli random variable with success probability α_{ij}.

Edges in inhomogeneous random keys graphs encode shared-key relationships, while edges in inhomogeneous Erdős-Rényi graphs encode the availability of wireless channels. Hence, the overall network can be modeled by a *composite* random graph model formed by the *intersection* of an inhomogeneous random key graph with an inhomogeneous Erdős-Rényi graph. An edge exists in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ only if it exists in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$, i.e., both nodes share a key, and $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$, i.e., both nodes share a wireless channel. Hence, edges in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ represent pairs of sensors that both i) share a key and ii) have a wireless channel in between that is on.

7.2 A roadmap

In this chapter, we investigate the connectivity of the composite random graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ and present conditions (in the form of zero-one laws) on how to scale its parameters, i.e., $\boldsymbol{\mu}$, $\boldsymbol{K}$, P, and $\boldsymbol{\alpha}$, so that it i) has no secure node which is isolated and ii) is securely connected, both with high probability when the number of nodes gets large. Essentially, our results provide design guidelines on how to choose the parameters of the heterogeneous random key predistribution scheme such that the resulting wireless sensor network is securely connected under a heterogeneous on-off channel model. Our results are supported by a simulation study demonstrating that despite their asymptotic nature, our results can in fact be useful in designing finite-node wireless sensor network so that they achieve secure connectivity with high probability.

7.3 Model definitions

In practical deployments of wireless sensor networks, nodes typically have limited communication ranges and the channel between two nodes may not be available, e.g., due to excessive interference. In other words, two sensor nodes which share a key may not eventually be adjacent due to the unavailability of their corresponding wireless channel. Hence, the secure connectivity of the network would not only be governed by the shared-key connectivity discussed above, but also by the wireless connectivity.

In modeling the wireless connectivity of the network, we utilize a heterogeneous on-off channel model, where the wireless channel between a class-i node and a class-j node is on (respectively, off) with probability α_{ij} (respectively, $1 - \alpha_{ij}$) for $i, j = 1, \ldots, r$. Note that the heterogeneous on-off channel model accounts for the fact that different nodes could have different radio capabilities, or could be deployed in locations with different channel characteristics. This is indeed a generalization of the uniform on-off channel model, where the channel between any two nodes is on (respectively, off) with probability α (respectively, $1-\alpha$) regardless of the corresponding classes. Hence, the heterogeneous on-off channel model offers the flexibility of modeling several interesting scenarios, such as when nodes of the same type are more (or less) likely to be adjacent with one another than with nodes belonging to other classes.

Consider a random graph $\mathbb{G}$ induced on the vertex set $\mathcal{V} = \{v_1, \ldots, v_n\}$ such that each node is classified into one of the r classes with a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$ and $\sum_{i=1}^{r} \mu_i = 1$. Then, a distinct class-i node v_x and a distinct class-j node v_y are adjacent in $\mathbb{G}$, denoted by $v_x \sim_G v_y$, if $B_{xy}(\alpha_{ij}) = 1$ where $B_{xy}(\alpha_{ij})$ denotes a Bernoulli rv with success probability α_{ij}. This gives rise to an $r \times r$ edge probability matrix $\boldsymbol{\alpha}$ where α_{ij} denotes the element of row i and column j of $\boldsymbol{\alpha}$. The aforementioned adjacency conditions induces the inhomogeneous Erdős-Rényi graph $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ on the vertex set $\mathcal{V}$, which has received interest recently [19, 32].

Although the on-off channel model may be considered too simple, it allows a comprehensive analysis of the properties of interest and is often a good approximation of more realistic channel models, e.g., the disk model [68]. In fact, the simulations results in [43] suggest that the k-connectivity behavior of wireless sensor networks secured by the heterogeneous random key predistribution scheme under the uniform on-off channel model (where $\alpha_{ij} = \alpha$ for $i, j = 1, \ldots, r$) is asymptotically equivalent to that under the more-realistic disk model.

Inhomogeneous random key graphs (see Section 6.3) and inhomogeneous Erdős-Rényi graphs, each, captures a particular notion of connectivity, namely shared-key connectivity and wireless connectivity, respectively. In what follows, we construct a random graph model that jointly considers both notions, hence, it accurately describes practical deployments of wireless sensor networks, where two nodes are adjacent if they both share a key *and* have an available wireless channel in between.

We consider a composite random graph obtained by the intersection of inhomogeneous random key graphs $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ with inhomogeneous Erdős-Rényi graphs $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$. Hence, edges in the intersection graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ represent pairs of sensor which i) share a key and ii) have a wireless channel in between that is on. In particular, a distinct class-i node v_x is adjacent to a distinct class-j node v_y in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ if and only if they are adjacent in both $\mathbb{K}$ *and* $\mathbb{G}$.

To simplify the notation, we let $\boldsymbol{\theta} = (\boldsymbol{K}, P)$, and $\boldsymbol{\Theta} = (\boldsymbol{\theta}, \boldsymbol{\alpha})$. By independence, we see that the probability of edge assignment between a class-i node v_x and a class-j node v_y in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ is given by

$$\mathbb{P}[v_x \sim v_y \mid t_x = i, t_y = j] = \alpha_{ij} p_{ij}$$

Similar to (6.3), we denote the mean edge probability for a class-i node in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ as Λ_i. It is clear that

$$\Lambda_i = \sum_{j=1}^{r} \mu_j \alpha_{ij} p_{ij}, \quad i = 1, \ldots, r. \tag{7.1}$$

We write Λ_m to denote the *minimum* mean edge probability in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$, i.e.,

$$m := \arg\min_i \Lambda_i. \tag{7.2}$$

We further let $\alpha_{\min} := \min_{i,j}\{\alpha_{ij}\}$ and $\alpha_{\max} := \max_{i,j}\{\alpha_{ij}\}$. Finally, we define d and s as follows

$$d := \arg\max_j\{\alpha_{mj}\}, \tag{7.3}$$

$$s := \arg\max_j\{\alpha_{mj}p_{mj}\}. \tag{7.4}$$

Throughout, we assume that the number of classes r is fixed and does not scale with n, and so are the probabilities $\mu_1,\ldots,\mu_r$. All of the remaining parameters are assumed to be scaled with n.

7.4 Preliminaries

Several technical results are collected here for convenience. Some of the results already appeared in Chapter 6, but we provide them below (without a proof) for completeness.

Proposition 7.4.1 ([157, Proposition 4.1]). *For any scaling $K_1,K_2,\ldots,K_r,P:\mathbb{N}_0\to\mathbb{N}_0^{r+1}$, we have*

$$\lambda_1(n)\le\lambda_2(n)\le\ldots\le\lambda_r(n) \tag{7.5}$$

for each $n=2,3,\ldots$.

Proposition 7.4.2 ([157, Proposition 4.4]). *For any set of positive integers $K_1,\ldots,K_r,P$ and any scalar $a\ge 1$, we have*

$$\frac{\binom{P-\lceil aK_i\rceil}{K_j}}{\binom{P}{K_j}}\le\left(\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}}\right)^a,\quad i,j=1,\ldots,r \tag{7.6}$$

Lemma 7.4.3. *Consider a scaling* $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ *and a scaling* $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r\times r}$ *such that (7.29) and (7.32) hold. We have*

$$\alpha_{\min}(n) p_{1r}(n) = \Theta\left(\frac{\log n}{n}\right) \tag{7.7}$$

Proof. We note from (7.32) that

$$\alpha_{mr}(n) p_{mr}(n) \leq \frac{\Lambda_m(n)}{\mu_r} = \frac{c_n}{\mu_r}\frac{\log n}{n},$$

Next, we show that under (6.15), the quantity $p_{ij}(n)$ is increasing in both i and j. Fix $n = 2, 3, \ldots$ and recall that under (7.26), K_i increases as i increases. For any i, j such that $K_i + K_j > P$, we see from (6.2) that $p_{ij}(n) = 1$; otherwise if $K_i + K_j \leq P$, we have $p_{ij}(n) < 1$. Given that $K_i + K_j$ increases with both i and j, it will be sufficient to show that $p_{ij}(n)$ increases with both i and j on the range where $K_i + K_j < P$. On that range, we have

$$\frac{\binom{P-K_i}{K_j}}{\binom{P}{K_j}} = \prod_{\ell=0}^{K_i-1}\left(1 - \frac{K_j}{P-\ell}\right)$$

Hence, $\binom{P-K_i}{K_j}/\binom{P}{K_j}$ decreases with both K_i and K_j, hence with i and j. From (6.2), it follows that $p_{ij}(n)$ increases with i and j. As a consequence, we have $p_{1r} \leq p_{mr}$ and it follows that

$$\alpha_{\min}(n) p_{1r}(n) \leq \alpha_{mr}(n) p_{mr}(n) \leq \frac{c_n}{\mu_r}\frac{\log n}{n}. \tag{7.8}$$

Combining (7.29) and (7.8) we readily obtain (7.7). ■

Lemma 7.4.4. *Consider a scaling* $K_1, K_2, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ *and a scaling* $\boldsymbol{\alpha} = \{\alpha_{ij}\}$:

$\mathbb{N}_0 \to (0,1)^{r\times r}$ *such that (7.27) holds. From (7.29), (7.30), (7.31), and (7.8), we have*

$$\alpha_{\max}(n)p_{rr}(n) = o\left(\frac{(\log n)^{\tau+2}}{n}\right) \tag{7.9}$$

and

$$\alpha_{\min}p_{11}(n) = \omega\left(\frac{1}{n}\right), \tag{7.10}$$

Proof. From (7.31) and (7.8), we have

$$\alpha_{\max}(n)p_{1r}(n) = \left(\frac{\alpha_{\max}(n)}{\alpha_{\min}(n)}\right)\alpha_{\min}(n)p_{1r}(n) = O\left(\frac{(\log n)^{\tau+1}}{n}\right) \tag{7.11}$$

It is now immediate that Lemma 7.4.4 is established once we show that

$$\frac{p_{rr}(n)}{p_{1r}(n)} = o\left(\log n\right), \tag{7.12}$$

leading to

$$\alpha_{\max}(n)p_{rr}(n) = \left(\frac{p_{rr}(n)}{p_{1r}(n)}\right)\alpha_{\max}(n)p_{1r}(n) = o\left(\frac{(\log n)^{\tau+2}}{n}\right)$$

We proceed by establishing (7.12). The proof is similar with [50, Lemma 5.4], but we give it below for completeness.

In particular, we will show that

$$p_{rr}(n) \leq \max\left(2, \frac{\log n}{w_n}\right)p_{1r}(n), \quad n = 2,3,\ldots \tag{7.13}$$

for some sequence w_n such that $\lim_{n\to\infty} w_n = \infty$. Fix $n = 2,3,\ldots$. We have either $p_{1r}(n) > \frac{1}{2}$, or $p_{1r}(n) \leq \frac{1}{2}$. In the former case, it automatically holds that

$$p_{rr}(n) \leq 2p_{1r}(n) \tag{7.14}$$

by virtue of the fact that $p_{rr}(n) \leq 1$.

Assume now that $p_{1r}(n) \leq \frac{1}{2}$. We know from [159, Lemmas 7.1-7.2] that

$$1 - e^{-\frac{K_{j,n}K_{r,n}}{P_n}} \leq p_{jr}(n) \leq \frac{K_{j,n}K_{r,n}}{P_n - K_{j,n}}, \quad j = 1, \ldots, r \tag{7.15}$$

and it follows that

$$\frac{K_{1,n}K_{r,n}}{P_n} \leq \log\left(\frac{1}{1 - p_{1r}(n)}\right) \leq \log 2 < 1. \tag{7.16}$$

Using the fact that $1 - e^{-x} \geq \frac{x}{2}$ with x in $(0, 1)$, we then get

$$p_{1r}(n) \geq \frac{K_{1,n}K_{r,n}}{2P_n}. \tag{7.17}$$

In addition, using the upper bound in (7.15) with $j = r$ gives

$$p_{rr}(n) \leq \frac{K_{r,n}^2}{P_n - K_{r,n}} \leq 2\frac{K_{r,n}^2}{P_n}$$

as we invoke (7.26). Combining the last two bounds we obtain

$$\frac{p_{rr}(n)}{p_{1r}(n)} \leq 4\frac{K_{r,n}}{K_{1,n}} = 4\frac{\log n}{w_n} \tag{7.18}$$

by virtue of (7.30) for some sequence w_n satisfying $\lim_{n\to\infty} w_n = \infty$. Combining (7.14) and (7.18), we readily obtain (7.13). This establishes (7.9).

Next, Combining (7.29), and the fact that $p_{1r}(n)/p_{11}(n) = o(\log n)$ (see (7.13)), we get

$$\alpha_{\min}(n)p_{11}(n) = \left(\frac{p_{11}(n)}{p_{1r}(n)}\right)\alpha_{\min}(n)p_{1r}(n) = \omega\left(\frac{1}{n}\right)$$

which readily establishes (7.10). ■

Lemma 7.4.5. *Under (7.10), we have*

$$\frac{K_{1,n}^2}{P_n} = \omega\left(\frac{1}{n\alpha_{\min}}\right), \tag{7.19}$$

and

$$K_{1,n} = \omega(1). \tag{7.20}$$

Proof. It is a simple matter to check that $p_{11}(n) \leq \frac{K_{1,n}^2}{P_n - K_{1,n}}$; see [159, Proposition 7.1-7.2] for a proof. In view of (7.26) this gives $p_{11}(n) \leq 2\frac{K_{1,n}^2}{P_n}$. Thus, we have

$$\frac{K_{1,n}^2}{P_n} = \Omega\left(p_{11}(n)\right) = \omega\left(\frac{1}{n\alpha_{\min}}\right).$$

From (7.28), (7.19), and $\alpha_{\min} \leq 1$, we readily obtain (7.20). ■

Other useful bound that will be used throughout is

$$(1 \pm x) \leq e^{\pm x}, \quad x \in (0,1) \tag{7.21}$$

$$\binom{n}{\ell} \leq \left(\frac{en}{\ell}\right)^{\ell}, \quad \ell = 1, \ldots, n, \quad n = 1, 2, \ldots \tag{7.22}$$

$$\sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \leq 2^n \tag{7.23}$$

Finally, we find it useful to write

$$\log(1-x) = -x - \Psi(x), \quad x \in (0,1) \tag{7.24}$$

where $\Psi(x) = \int_0^x \frac{t}{1-t}$ dt. From L'Hôpital's Rule, we have

$$\lim_{x \to 0} \frac{\Psi(x)}{x^2} = \frac{-x - \log(1-x)}{x^2} = \frac{1}{2}. \tag{7.25}$$

7.5 Connectivity and absence of isolated nodes

We refer to a mapping $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ as a *scaling* (for inhomogeneous random key graphs) if

$$1 \le K_{1,n} \le K_{2,n} \le \ldots \le K_{r,n} \le P_n/2 \tag{7.26}$$

hold for all $n = 2, 3, \ldots$. Similarly any mapping $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r \times r}$ defines a scaling for inhomogeneous Erdős-Rényi graphs. A mapping $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0,1)^{r\times r}$ defines a scaling for the intersection graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ given that condition (7.26) holds. We remark that under (7.26), the edge probabilities p_{ij} will be given by (6.2).

We first present a zero-one law for the absence of isolated nodes in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$.

7.5.1 A zero-one law for the absence of isolated nodes

Theorem 7.5.1. *Consider a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$ for $i = 1, \ldots, r$, a scaling $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$, and a scaling $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r\times r}$ such that*

$$\Lambda_m(n) \sim c \frac{\log n}{n} \tag{7.27}$$

holds for some $c > 0$.

i) If

$$\lim_{n\to\infty} \alpha_{md}(n) \log n = 0 \qquad \text{or} \qquad \lim_{n\to\infty} \alpha_{mm}(n) \log n = \alpha^* \in (0, \infty]$$

holds, then we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha}) \text{ has no isolated nodes}\right] = 0 \qquad \text{if } c < 1$$

ii) We have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha}) \text{ has no isolated nodes}\right] = 1 \qquad \text{if } c > 1$$

Next, we present an analogous result for connectivity.

7.5.2 A zero-one law for connectivity

Theorem 7.5.2. *Consider a probability distribution* $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ *with* $\mu_i > 0$ *for* $i = 1, \ldots, r$*, a scaling* $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$*, and a scaling* $\boldsymbol{\alpha} = \{\alpha_{ij}\} : \mathbb{N}_0 \to (0,1)^{r \times r}$ *such that (7.27) holds for some* $c > 0$.

i) If

$$\lim_{n\to\infty} \alpha_{md}(n) \log n = 0 \qquad \text{or} \qquad \lim_{n\to\infty} \alpha_{mm}(n) \log n = \alpha^* \in (0, \infty]$$

holds, then we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha}) \text{ is connected}\right] = 0 \quad \text{if } c < 1$$

ii) If

$$P_n \geq \sigma n, \quad n = 1, 2, \ldots \tag{7.28}$$

for some $\sigma > 0$*, and*

$$\alpha_{\min}(n) p_{1r}(n) = \Omega\left(\frac{\log n}{n}\right) \tag{7.29}$$

$$\frac{K_{r,n}}{K_{1,n}} = o\left(\log n\right) \tag{7.30}$$

$$\frac{\alpha_{\max}(n)}{\alpha_{\min}(n)} = O\left((\log n)^{\tau}\right) \tag{7.31}$$

for any finite $\tau > 0$*. Then, we have*

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha}) \text{ is connected}\right] = 1 \quad \text{if } c > 1$$

The scaling condition (7.27) will often be used in the form

$$\Lambda_m(n) = c_n \frac{\log n}{n}, \; n = 2, 3, \ldots \tag{7.32}$$

with $\lim_{n\to\infty} c_n = c > 0$. Also, condition (7.29) will often be used in the form

$$\alpha_{\min}(n) p_{1r}(n) \geq \rho \frac{\log n}{n}, \quad \text{for } \rho > 0 \text{ and } n = 2, 3, \ldots \tag{7.33}$$

7.5.3 Discussion

Theorems 7.5.1 and 7.5.2 state that $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ has no isolated node (and is connected) with high probability if the minimum mean degree, i.e., $n\Lambda_m$, is scaled as $(1+\epsilon)\log n$ for some $\epsilon > 0$. On the other hand, if this minimum mean degree scales as $(1-\epsilon)\log n$ for some $\epsilon > 0$, then with high probability $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ has an isolated node, and hence is not connected. The resemblance of the results presented in Theorem 7.5.1 and Theorem 7.5.2 indicates that absence of isolated nodes and connectivity are asymptotically equivalent properties for $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$. Similar observations were made for other well-known random graph models as well; e.g., inhomogeneous random key graphs [157], Erdős-Rényi graphs [18], and (homogeneous) random key graphs [159].

Note that if the matrix $\boldsymbol{\alpha}$ is designed in such a way that $\alpha_{ii} = \max_j\{\alpha_{ij}\}$, i.e., two nodes of the same type are more likely to be adjacent in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$, then we have $\alpha_{md} = \alpha_{mm}$ and the condition of the zero-law of Theorems 7.5.1 and 7.5.2 would collapse to i) $\lim_{n\to\infty} \alpha_{mm}(n) \log n = 0$ or ii) $\lim_{n\to\infty} \alpha_{mm}(n) \log n \in (0, \infty]$. At this point, the zero-law follows even when the sequence $\alpha_{mm} \log n$ does not have a limit by virtue of the *subsubsequence principle* [73, p. 12] (see also [43, Section 7.3]). In other words, if $\alpha_{md} = \alpha_{mm}$, then the zero-law of Theorems 7.5.1 and 7.5.2 follows without any conditions on the sequence $\alpha_{mm}(n) \log n$.

We now comment on the additional technical conditions needed for the one-law of Theorem 7.5.2. Condition (7.28) is likely to be needed in practical deployments of wireless sensor networks in order to ensure the *resilience* of the network against node capture attacks; e.g., see [33, 53]. To see this, assume that an adversary captures a number of sensors, compromising all the keys that belong to the captured nodes. If $P_n = o(n)$, contrary to (7.28), then it would be possible for the adversary to compromise $\Omega(P_n)$ keys by capturing only $o(n)$ sensors (whose type does not matter). In this case, the wireless sensor network would fail to exhibit the *unassailability* property [95, 153] and would be deemed as vulnerable against adversarial attacks. We remark that (7.28) was required in [43, 50, 157, 166] in similar settings to ours.

Condition (7.29) provides a non-trivial lower bound on the edge probability $\alpha_{\min}(n)p_{1r}(n)$ and is enforced mainly for technical reasons for the proof of the one-law of Theorem 7.5.2 to work. Note that it is easy to show that $\alpha_{\min}(n)p_{1r}(n) = O(\log n/n)$ from (7.32) (see Lemma 7.4.3 for a proof), however, the scaling condition given by (7.32) does not provide any non-trivial lower-bound on the product $\alpha_{\min}(n)p_{1r}(n)$. Observe that, even with condition (7.29), our results do not require *each* edge probability to scale as $\log n/n$, in contrast to the results given in [32] on the connectivity of inhomogeneous Erdős-Rényi graphs. In particular, the probability of an edge between a class-i node and a class-j node was set to $\kappa(i,j)\log n/n$ in [32], where $\kappa(i,j)$ returns a positive real number for each pair (i,j); i.e., each individual edge was scaled as $\Theta(\log n/n)$.

Condition (7.30) is also enforced mainly for technical reasons and it takes away from the flexibility of assigning very small key key rings to a certain fraction of sensors when connectivity is considered. An equivalent condition was also needed in [157] for establishing the one-law for connectivity in inhomogeneous random key graphs. We refer the reader to [157, Section 3.2] for an extended discussion on the feasibility of (7.30) for real-world implementations of wireless sensor networks. Condition (7.31) also limits the flexibility of assigning very small values for $\alpha_{\min}$, but it is much milder than condition (7.30) in a sense that it requires $\alpha_{\max}(n)/\alpha_{\min}(n)$ to be $O\left((\log n)^{\tau}\right)$ for some finite $\tau > 0$, i.e., one can still afford to have a large deviation between $\alpha_{\min}(n)$ and $\alpha_{\max}(n)$ as compared to the case if $\alpha_{\max}(n)/\alpha_{\min}(n)$ had to be scaled as $o(\log n)$, similar to the case in (7.30).

We close by providing a concrete example that demonstrates how all the conditions required by Theorem 7.5.2 can be met in a real-world implementation. Consider a sensor network consisting of two classes, i.e., $r = 2$. Pick any probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2\}$ with $\mu_i > 0$ for all $i = 1, 2$. Set $P_n = \lceil n \log n \rceil$ as well as

$$K_{1,n} = \left\lceil \frac{(\log n)^{1/2+\varepsilon}}{\sqrt{\alpha_{\min}(n)}} \right\rceil \quad \text{and} \quad K_{2,n} = \left\lceil \frac{(1+\varepsilon)(\log n)^{3/2-\varepsilon}}{\mu_2 \sqrt{\alpha_{\min}(n)}} \right\rceil$$

with any $0 < \varepsilon < 0.5$. Observe that the above selection satisfies (7.28) as well as (7.30). Next, set

$$\boldsymbol{\alpha} = \alpha_{\min}(n) \begin{bmatrix} \frac{1+\epsilon}{\mu_1} (\log n)^{1-2\epsilon} & 1 \\ 1 & \frac{\mu_2}{1+\epsilon} (\log n)^{1+2\epsilon} \end{bmatrix}$$

Note that the above selection satisfies (7.31) with $\tau = 1 + 2\epsilon$. For simplicity, assume that $\lambda_1(n) = o(1)$ which implies that $p_{1j}(n) = o(1)$ for $j = 1, 2$. In this case, we have $p_{1j}(n) \sim \frac{K_{1,n}K_{j,n}}{P_n}$ for $j = 1, 2$ (see [157, Lemma 4.2]). With this parameter selection, we have

$$\alpha_{\min}(n) p_{12}(n) \sim \alpha_{\min}(n) \frac{K_{1,n}K_{2,n}}{P_n} = \frac{1+\epsilon}{\mu_2} \frac{\log n}{n}$$

which satisfies (7.29).

Finally, observe that with the above parameter selection, both $\Lambda_1(n)$ and $\Lambda_2(n)$ are strictly larger than $\log n/n$. Hence, in view of Theorem 7.5.2, the resulting network will be connected with high probability. Of course, there are many other parameter scalings that one can choose.

7.5.4 Comparison with related work

The connectivity (respectively, k-connectivity) of wireless sensor networks secured by the classical Eschenauer-Gligor scheme under a *uniform* on/off channel model was investigated in [156] (respectively, [166]). The network was modeled by a composite random graph formed by the intersection of random key graphs $\mathbb{K}(n; K, P)$ (induced by Eschenauer-Gligor scheme) with Erdős-Rényi graphs $\mathbb{G}(n; \alpha)$ (induced by the uniform on-off channel model). Our work generalizes this model to heterogeneous setting where different nodes could be given different number of keys depending on their respective classes and the availability of a wireless channel between two nodes depends on their respective classes. Hence, our model highly resembles emerging wireless sensor networks which are essentially complex and heterogeneous.

In [157], Yağan considered the connectivity of wireless sensor networks secured by the heterogeneous random key predistribution scheme under the full visibility assumption, i.e., all wireless channels are available and reliable, hence the only condition for two nodes to be adjacent is to share a key. It is clear that the full visibility assumption is not likely to hold in most practical deployments of wireless sensor networks as the wireless medium is typically unreliable. Our work extends the results given in [157] to more practical scenarios where the wireless connectivity is taken into account through the heterogeneous on-off channel model. In fact, by setting $\alpha_{ij}(n) = 1$ for $i, j = 1, \ldots, r$ and each $n = 1, 2, \ldots$ (i.e., by assuming that all wireless channels are *on*), our results reduce to those given in [157].

In comparison with the existing literature on similar models, our result can be seen to extend the work by Eletreby and Yağan in [50] (respectively, [43]). Therein, the authors established a zero-one law for the 1-connectivity (respectively, k-connectivity) of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \alpha)$, i.e., for a wireless sensor network under the *heterogeneous* key predistribution scheme and a *uniform* on-off channel model. Although these results form a crucial starting point towards the analysis of the heterogeneous key predistribution scheme under a wireless connectivity model, they are limited to uniform on-off channel model where all channels are on (respectively, off) with the same probability α (respectively, $1 - \alpha$). The heterogeneous on-off channel model accounts for the fact that different nodes could have different radio capabilities, or could be deployed in locations with different channel characteristics. In addition, it offers the flexibility of modeling several interesting scenarios, such as when nodes of the same type are more (or less) likely to be adjacent with one another than with nodes belonging to other classes. Indeed, by setting $\alpha_{ij}(n) = \alpha$ for $i, j = 1, \ldots, r$ and each $n = 1, 2, \ldots$, our results reduce to those given in [50].

7.5.5 Numerical results

In this section, we present a simulation study to validate our results in the finite-node regime. In all experiments, we fix the number of nodes at $n = 500$, the size of the key pool at $P = 10^4$, and the number of experiments to 400.

In Figure 7.1, we set the channel matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} 0.3 & \alpha_{12} \\ \alpha_{12} & 0.3 \end{bmatrix}$$

and consider three different values for the parameter α_{12}, namely, $\alpha_{12} = 0.2$, $\alpha_{12} = 0.4$, and $\alpha_{12} = 0.6$. We also vary K_1 (i.e., the smallest key ring size) from 5 to 25. The number of classes is fixed to 2, with $\boldsymbol{\mu} = \{0.5, 0.5\}$. For each value of K_1, we set $K_2 = K_1 + 5$. For each parameter pair $(\boldsymbol{K}, \boldsymbol{\alpha})$, we generate 400 independent samples of the graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ and count the number of times (out of a possible 400) that the obtained graphs i) have no isolated nodes and ii) are connected. Dividing the counts by 400, we obtain the (empirical) probabilities for the events of interest. In all cases considered here, we observe that $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ is connected whenever it has no isolated nodes yielding the same empirical probability for both events. This confirms the asymptotic equivalence of the connectivity and absence of isolated nodes properties in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ as is illustrated in Theorems 7.5.1 and 7.5.2.

For each value of α_{12}, we show the critical threshold of connectivity given by Theorem 7.5.2 in the form of highlighted symbols. More specifically, highlighted symbols stand for the minimum integer value of K_1 that satisfies

$$\Lambda_m(n) = \sum_{j=1}^{2} \mu_j \alpha_{mj} \left(1 - \frac{\binom{P-K_j}{K_m}}{\binom{P}{K_m}} \right) > \frac{\log n}{n}. \tag{7.34}$$

upon noting that $K_2 = K_1 + 5$. We see from Figure 7.1 that the probability of connectivity transitions from zero to one within relatively small variations of K_1. Moreover, the critical values of K_1 obtained by (7.34) lie within this transition interval and correspond to high

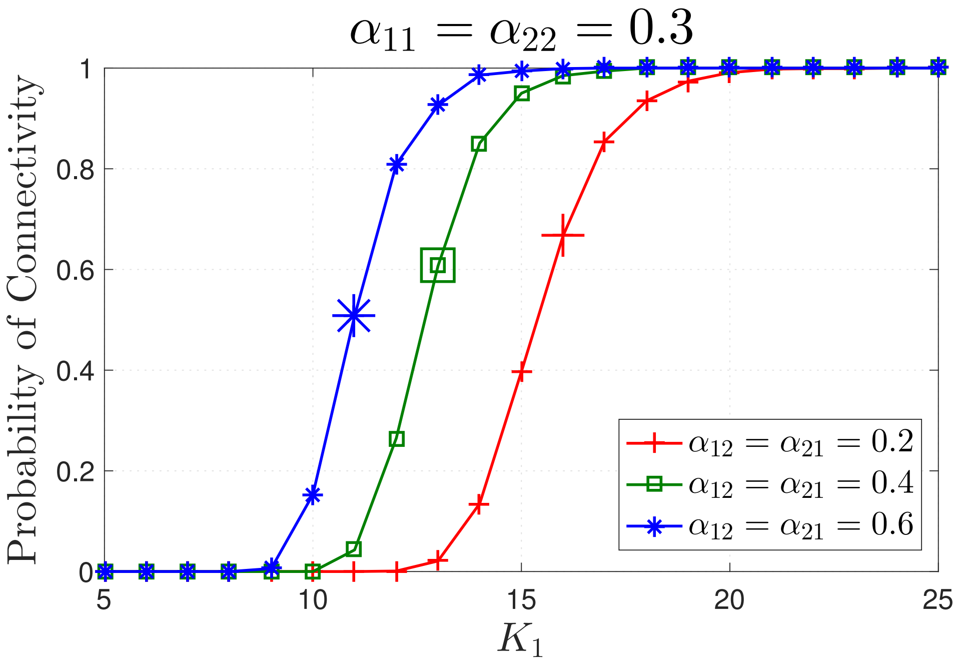


Figure 7.1: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ is connected as a function of $\boldsymbol{K}$ for $\alpha_{12} = 0.2$, $\alpha_{12} = 0.4$, and $\alpha_{12} = 0.6$. We set $\alpha_{11} = \alpha_{22} = 0.3$. Highlighted symbols stand for the critical threshold of connectivity asserted by Theorem 7.5.2.

probability of connectivity. Note that for each parameter pair $(\boldsymbol{K},\boldsymbol{\alpha})$ in Figure 7.1, we have $\Lambda_m = \Lambda_1$ by construction.

Next, we set the channel matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha_{11} & 0.2 \\ 0.2 & 0.2 \end{bmatrix}$$

in Figure 7.2, and consider three different values for the parameter α_{11}, namely, $\alpha_{11} = 0.2$, $\alpha_{11} = 0.4$, and $\alpha_{11} = 0.6$. We also vary K_1 from 10 to 25. The number of classes is fixed to 2, with $\boldsymbol{\mu} = \{0.5, 0.5\}$. For each value of K_1, we set $K_2 = K_1 + 5$. Similar to Figure 7.1, we obtain the empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ is connected versus K_1. As before, the critical threshold of connectivity asserted by Theorem 7.5.2 is shown by highlighted symbols in each curve.

Note that for $\alpha_{11} \geq 0.4$, fixed α_{12}, and fixed α_{22}, the probability of connectivity (along with

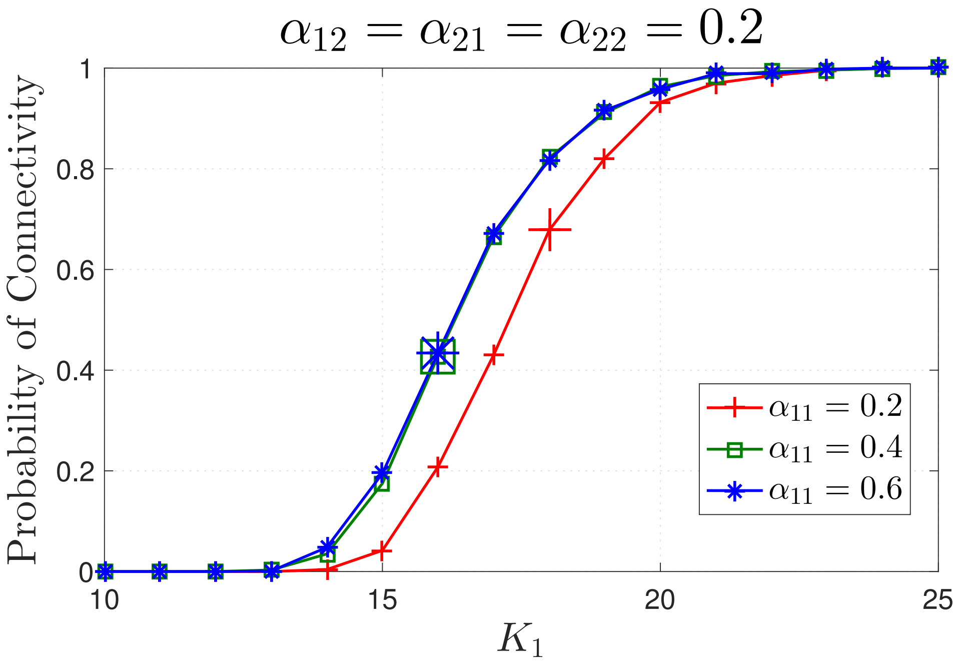


Figure 7.2: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ is connected as a function of $\boldsymbol{K}$ for $\alpha_{11}=0.2$, $\alpha_{11}=0.4$, and $\alpha_{11}=0.6$. We set $\alpha_{12}=\alpha_{22}=0.2$. Highlighted symbols stand for the critical threshold of connectivity asserted by Theorem 7.5.2.

the critical value of K_1) behave in a similar fashion regardless of the particular value of α_{11}. The reason behind this is intuitive. When $\alpha_{11}=0.2$, we have $\Lambda_m=\Lambda_1$, while for $\alpha_{11}\geq 0.4$, we have $\Lambda_m=\Lambda_2$. Consequently, the value of α_{11} (which only appears in Λ_1) becomes irrelevant to the scaling condition given by (7.34).

Finally, we set the channel matrix to

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha & 0.2 \\ 0.2 & \alpha \end{bmatrix}$$

and consider four different values for the parameter K_1, namely, $K_1=20$, $K_1=25$, $K_1=30$, and $K_1=35$ while varying the parameter α from 0 to 1. The number of classes is fixed to 2 with $\boldsymbol{\mu}=\{0.5,0.5\}$ and we set $K_2=K_1+5$ for each value of K_1. We plot the empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ is connected versus α and highlight the critical threshold of connectivity asserted by Theorem 7.5.2. Note that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ has a positive

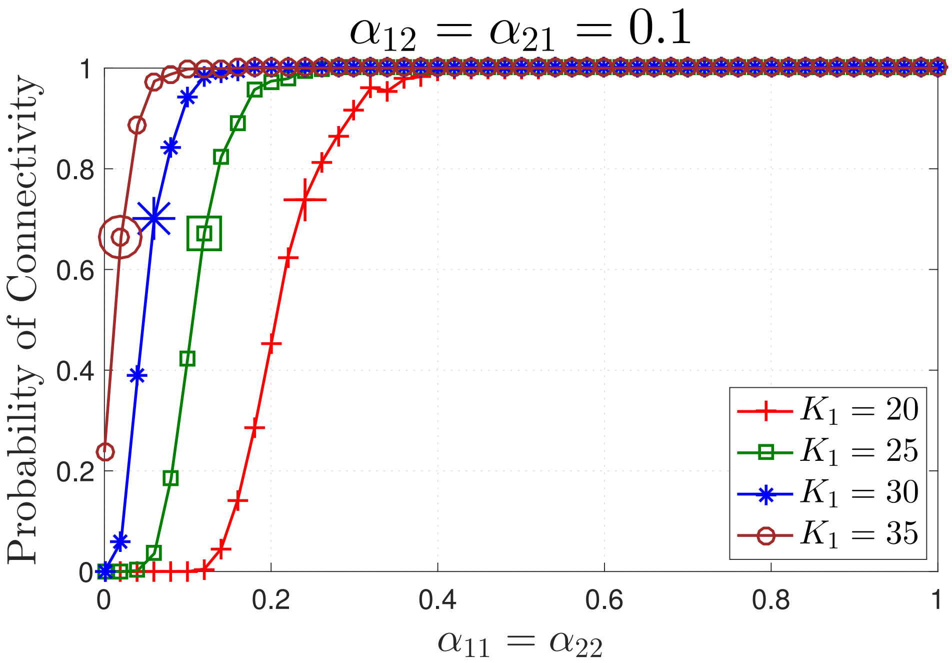


Figure 7.3: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ is connected as a function of α for $K_1 = 20$, $K_1 = 25$, $K_1 = 30$, and $K_1 = 35$. We set $\alpha_{12} = 0.2$. Highlighted symbols stand for the critical threshold of connectivity asserted by Theorem 7.5.2.

probability to be connected with $\alpha_{12} > 0$ even when $\alpha = 0$. In this case, the connected instances of $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ represent *connected bipartite graphs*, where one set of the bipartite graph represents class-1 nodes and the other represents class-2 nodes. The results given by Figure 7.3 reveal the importance of cross-type edge probability in establishing a connected graph. In particular, when $\alpha_{11} = \alpha_{22} = 0$, the graph could still be connected owing to cross-type edges. Indeed, the graph cannot be connected when cross-type edges have zero probability, even when same-type edges have positive probability since the graph would consist of at least two isolated components, as captured by Figure 7.4.

7.5.6 Proof of Theorem 7.5.1

The proof of Theorem 7.5.1 relies on the method of first and second moments applied to the number of isolated nodes in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$. Let $I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denote the total number

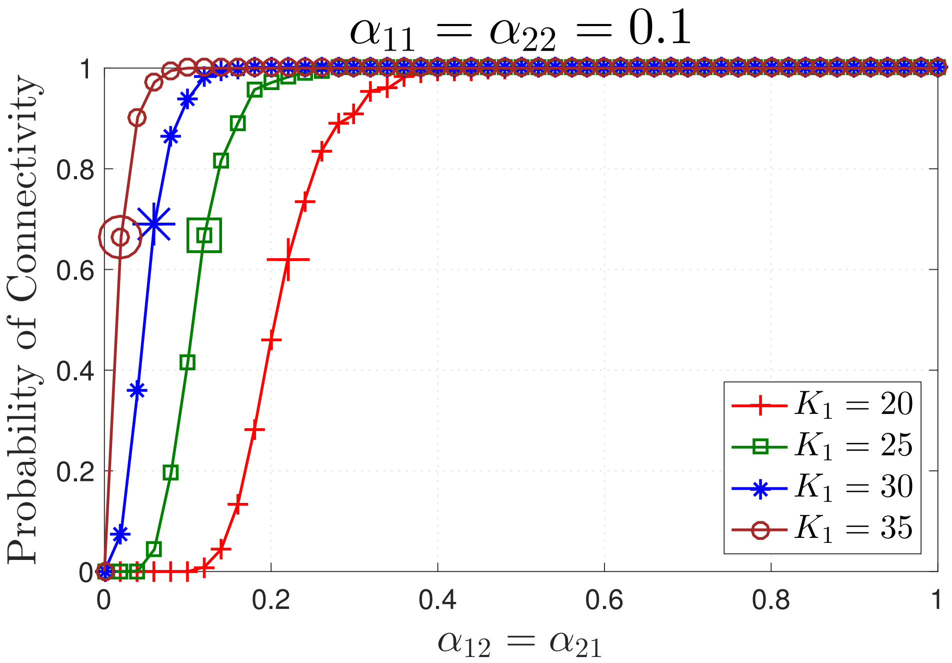


Figure 7.4: Empirical probability that $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ is connected as a function of α_{12} for $K_1 = 20$, $K_1 = 25$, $K_1 = 30$, and $K_1 = 35$. We set $\alpha_{11} = \alpha_{22} = 0.2$. Highlighted symbols stand for the critical threshold of connectivity asserted by Theorem 7.5.2.

of isolated nodes in $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$, namely,

$$I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n) = \sum_{\ell=1}^{n}\mathbf{1}[v_\ell \text{ is isolated in } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})] \tag{7.35}$$

The method of first moment [73, Eqn. (3.1), p. 54] gives

$$1-\mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] \leq \mathbb{P}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)=0]$$

Establishing the one-law

It is clear that in order to establish the one-law, namely that $\lim_{n\to\infty}\mathbb{P}\left[I_n(\boldsymbol{\mu},\boldsymbol{\Theta_n})=0\right]=1$, we need to show that

$$\lim_{n\to\infty}\mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)]=0.$$

Recalling (7.35), we have

$$\begin{aligned}\mathbb{E}\left[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] &= n\sum_{i=1}^{r}\mu_i\mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha}) \;\middle|\; t_1=i\right] &(7.36)\\ &= n\sum_{i=1}^{r}\mu_i\mathbb{P}\left[\cap_{j=2}^{n}[v_j \nsim v_1] \mid t_1=i\right] &\\ &= n\sum_{i=1}^{r}\mu_i\left(\mathbb{P}\left[v_2 \nsim v_1 \mid t_1=i\right]\right)^{n-1} &(7.37)\end{aligned}$$

where (7.36) follows by the exchangeability of the indicator functions appearing at (7.35) and (7.37) follows by the conditional independence of the rvs $\{v_j \nsim v_1\}_{j=1}^{n}$ given t_1. By conditioning on the class of v_2, we find

$$\mathbb{P}[v_2 \nsim v_1 \mid t_1=i] = \sum_{j=1}^{r}\mu_j\mathbb{P}[v_2 \nsim v_1 \mid t_1=i, t_2=j] = \sum_{j=1}^{r}\mu_j(1-\alpha p_{ij}) = 1-\Lambda_i(n). \quad (7.38)$$

Using (7.38) in (7.37), and recalling (7.2), (7.21) we obtain

$$\begin{aligned}\mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] &= n\sum_{i=1}^{r}\mu_i\left(1-\Lambda_i(n)\right)^{n-1}\\ &\leq n\left(1-\Lambda_m(n)\right)^{n-1}\\ &= n\left(1-c_n\frac{\log n}{n}\right)^{n-1}\\ &\leq e^{\log n\left(1-c_n\frac{n-1}{n}\right)}\end{aligned}$$

Taking the limit as n goes to infinity, we immediately get

$$\lim_{n\to\infty}\mathbb{E}[I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] = 0.$$

since $\lim_{n\to\infty}(1-c_n\frac{n-1}{n}) = 1-c < 0$ under the enforced assumptions (with $c>1$) and the one-law is established.

Establishing the zero-law

Our approach in establishing the zero-law relies on the method of second moment applied to a variable that counts the number of nodes that are class-m and isolated. Clearly if we can show that whp there exists at least one class-m node that is isolated under the enforced assumptions (with $c < 1$) then the zero-law would immediately follow.

Let $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the number of nodes that are class-m and isolated in $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$, and let

$$x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \mathbf{1}[t_i = m \cap v_i \text{ is isolated in } \mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})],$$

then we have $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = \sum_{i=1}^{n} x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$. By applying the method of second moments [73, Remark 3.1, p. 54] on $Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, we get

$$\mathbb{P}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = 0] \leq 1 - \frac{(\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)])^2}{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2]} \tag{7.39}$$

where

$$\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \tag{7.40}$$

and

$$\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2] = n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] + n(n-1)\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \tag{7.41}$$

by exchangeability and the binary nature of the rvs $\{x_{n,i}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)\}_{i=1}^{n}$. Using (7.40) and (7.41), we get

$$\frac{\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^2]}{(\mathbb{E}[Y_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)])^2} = \frac{1}{n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]} + \frac{n-1}{n}\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]}{(\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)])^2}$$

In order to establish the zero-law, we need to show that

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty,$$

and

$$\limsup_{n\to\infty}\left(\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)]}{\left(\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)]\right)^2}\right)\leq 1. \tag{7.42}$$

Proposition 7.5.3. *Consider a scaling $K_1,\ldots,K_r,P:\mathbb{N}_0\to\mathbb{N}_0^{r+1}$ and a scaling $\boldsymbol{\alpha}=\{\alpha_{ij}\}:=\mathbb{N}_0\to(0,1)^{r\times r}$ such that (7.27) holds with $\lim_{n\to\infty}c_n=c>0$. Then, we have*

$$\lim_{n\to\infty}n\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)]=\infty,\quad \textit{if } c<1$$

Proof. We have

$$\begin{aligned}
n\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right] &= n\mathbb{E}\left[\mathbf{1}[t_1=m\cap v_1 \text{ is isolated in } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})]\right]\\
&= n\mu_m\mathbb{P}\left[v_1 \text{ is isolated in } \mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})\;\middle|\;t_1=m\right]\\
&= n\mu_m\mathbb{P}\left[\cap_{j=2}^{n}[v_j\nsim v_1]\;\middle|\;t_1=m\right]\\
&= n\mu_m\mathbb{P}\left[v_2\nsim v_1\;\middle|\;t_1=m\right]^{n-1}\\
&= n\mu_m\left(\sum_{j=1}^{r}\mu_j\mathbb{P}\left[v_2\nsim v_1\;\middle|\;t_1=1,t_2=j\right]\right)^{n-1}\\
&= n\mu_m\left(\sum_{j=1}^{r}\mu_j(1-\alpha_{mj}p_{mj})\right)^{n-1} &(7.43)\\
&= n\mu_m\left(1-\Lambda_m(n)\right)^{n-1}=\mu_m e^{\beta_n} &(7.44)
\end{aligned}$$

where

$$\beta_n=\log n+(n-1)\log(1-\Lambda_m(n)).$$

Recalling (7.24), we get

$$\begin{aligned}\beta_n &= \log n - (n-1)\left(\Lambda_m(n) + \Psi(\Lambda_m(n))\right)\\ &= \log n - (n-1)\left(c_n\frac{\log n}{n} + \Psi\left(c_n\frac{\log n}{n}\right)\right)\\ &= \log n\left(1 - c_n\frac{n-1}{n}\right) - (n-1)\left(c_n\frac{\log n}{n}\right)^2 \frac{\Psi\left(c_n\frac{\log n}{n}\right)}{\left(c_n\frac{\log n}{n}\right)^2} \qquad (7.45)\end{aligned}$$

Recalling (7.25), we have

$$\lim_{n\to\infty} \frac{\Psi\left(c_n\frac{\log n}{n}\right)}{\left(c_n\frac{\log n}{n}\right)^2} = \frac{1}{2} \qquad (7.46)$$

since $c_n\frac{\log n}{n} = o(1)$. Thus, $\beta_n = \log n\left(1 - c_n\frac{n-1}{n}\right) - o(1)$. Using (7.44), (7.45), (7.46), and letting n go to infinity, we get

$$\lim_{n\to\infty} n\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = \infty$$

whenever $\lim_{n\to\infty} c_n = c < 1$. □

Proposition 7.5.4. *Consider a scaling* $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ *and a scaling* $\boldsymbol{\alpha} = \{\alpha_{ij}\} := \mathbb{N}_0 \to (0,1)^{r\times r}$ *such that (7.27) holds with* $\lim_{n\to\infty} c_n = c > 0$*. Then, we have (7.42) if* $c < 1$*.*

Proof. Consider fixed $\boldsymbol{\Theta}$.

$$\begin{aligned}\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\right] &= \mathbb{E}\left[\mathbf{1}[v_1 \text{ is isolated }, v_2 \text{ is isolated} \cap t_1 = m, t_2 = m]\right]\\ &= \mu_m^2\mathbb{E}\left[\mathbf{1}[v_1 \text{ is isolated }, v_2 \text{ is isolated}] \;\middle|\; t_1 = m, t_2 = m\right]\\ &= \mu_m^2\mathbb{E}\left[\mathbf{1}[v_1 \nsim v_2]\prod_{k=3}^{n}\mathbf{1}[v_k \nsim v_1, v_k \nsim v_2] \;\middle|\; t_1 = t_2 = m\right]\end{aligned}$$

Now we condition on Σ_1 and Σ_2 and note that i) Σ_1 and Σ_2 determine t_1 and t_2; and ii) the events $[v_1 \nsim v_2], \{[v_k \nsim v_1 \cap v_k \nsim v_2]\}_{k=3}^n$ are mutually independent given Σ_1 and Σ_2. Thus, we have

$$\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\right] = \mu_m^2\mathbb{E}\left[\mathbb{P}\left[v_1 \not\sim v_2 \,\middle|\, \Sigma_1, \Sigma_2\right] \times \prod_{k=3}^{n} \mathbb{P}\left[v_k \not\sim v_1 \cap v_k \not\sim v_2 \,\middle|\, \Sigma_1, \Sigma_2\right] \,\middle|\, t_1 = t_2 = m\right] \tag{7.47}$$

Define the $\{0,1\}$-valued rv $u(\boldsymbol{\theta})$ by

$$u(\boldsymbol{\theta}) := \mathbf{1}[\Sigma_1 \cap \Sigma_2 \neq \emptyset]. \tag{7.48}$$

Next, with $\ell = 1, 2, \ldots, n-1$, define $\nu_{\ell,j}(\boldsymbol{\alpha})$ by

$$\nu_{\ell,j}(\boldsymbol{\alpha}) := \{i = 1, 2, \ldots, \ell : B_{ij}(\boldsymbol{\alpha}) = 1\} \tag{7.49}$$

for each $j = \ell+1, \ldots, n$. Namely, $\nu_{\ell,j}(\boldsymbol{\alpha})$ is the set of nodes in $\{1, \ldots, \ell\}$ that are adjacent to node j in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$. With these definitions in mind, (7.47) gives

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})] = \mu_m^2\mathbb{E}\left[(1-\alpha_{mm})^{u(\boldsymbol{\theta})}\prod_{k=3}^{n}\frac{\binom{P - \left|\cup_{i\in\nu_{2,k}(\boldsymbol{\alpha})}\Sigma_i\right|}{|\Sigma_k|}}{\binom{P}{|\Sigma_k|}} \,\middle|\, t_1 = t_2 = m\right]$$

Conditioned on $u(\boldsymbol{\theta}) = 0$ and v_1, v_2 being class-m, we have

$$\left|\cup_{i\in\nu_{2,m}(\boldsymbol{\alpha})}\Sigma_i\right| = \left|\nu_{2,k}(\boldsymbol{\alpha})\right| K_m.$$

Also, we have

$$\mathbb{P}[u(\boldsymbol{\theta_n}) = 0 \mid t_1 = t_2 = m] = 1 - p_{mm}.$$

Thus, we get

$$
\begin{aligned}
&\mathbb{E}\left[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\ \mathbf{1}[u(\boldsymbol{\theta})=0]\right]\\
&=\mu_m^2(1-p_{mm})\mathbb{E}\left[\prod_{k=3}^{n}\frac{\binom{P-|\nu_{2,k}(\boldsymbol{\alpha})K_m|}{|\Sigma_k|}}{\binom{P}{|\Sigma_k|}}\ \middle|\ t_1=t_2=m\right]\\
&=\mu_m^2(1-p_{mm})\mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\boldsymbol{\alpha})|K_m}{|\Sigma_3|}}{\binom{P}{|\Sigma_3|}}\ \middle|\ t_1=t_2=m\right]^{n-2} \qquad (7.50)\\
&=\mu_m^2(1-p_{mm})\left(\sum_{j=1}^{r}\mu_j\mathbb{E}\left[\frac{\binom{P-|\nu_{2,3}(\boldsymbol{\alpha})|K_m}{|\Sigma_3|}}{\binom{P}{|\Sigma_3|}}\ \middle|\ \begin{array}{c}t_1=t_2=m\\ t_3=j\end{array}\right]\right)^{n-2}\\
&\le\mu_m^2(1-p_{mm})\left(\sum_{j=1}^{r}\mu_j\mathbb{E}\left[\left(\frac{\binom{P-K_m}{K_j}}{\binom{P}{K_j}}\right)^{|\nu_{2,3}(\boldsymbol{\alpha})|}\ \middle|\ \begin{array}{c}t_1=t_2=m\\ t_3=j\end{array}\right]\right)^{n-2}, \qquad (7.51)
\end{aligned}
$$

where we use (7.6) in the last step. Note that conditioned on $t_1=t_2=m$, the random variables $\{|\nu_{2,k}(\boldsymbol{\alpha})|\}_{k=3}^{n}$ are independent and identically distributed, hence (7.50) follows. In particular

$$
|\nu_{2,k}(\boldsymbol{\alpha})|\ \Big|\ t_1=t_2=m\sim\text{Binomial}\left(2,\alpha_{mj}\right)\quad\text{with probability }\mu_j,\quad k=3,4,\ldots,n
$$

The above distributional equality could be explained as follows. We may write $|\nu_{2,k}(\boldsymbol{\alpha})|=\mathbf{1}\left[v_1\sim_G v_k\right]+\mathbf{1}\left[v_2\sim_G v_k\right]$. Observe that conditioned on $t_1=t_2=m$, we know that nodes v_1 and v_2 belong to class-m in $\mathbb{G}\left(n;\boldsymbol{\mu},\boldsymbol{\alpha}\right)$. If node v_k is class-j (an event that has probability μ_j), then $\mathbf{1}\left[v_1\sim_G v_k\right]$ and $\mathbf{1}\left[v_2\sim_G v_k\right]$ are each distributed as Bernoulli random variable with parameter α_{mj}.

Now, let

$$
Z_j=\frac{\binom{P-K_m}{K_j}}{\binom{P}{K_j}}=1-p_{mj},\quad j=1,\ldots,r. \qquad (7.52)
$$

Then,

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}\left[u(\boldsymbol{\theta})=0\right]] \leq \mu_m^2(1-p_{mm})\left(\sum_{j=1}^{r}\mu_j\mathbb{E}\left[Z_j^{|\nu_{2,3}(\boldsymbol{\alpha})|}\,\middle|\,\begin{array}{c} t_1=t_2=m \\ t_3=j\end{array}\right]\right)^{n-2} \tag{7.53}$$

Note that

$$|\nu_{2,3}(\boldsymbol{\alpha})|\,\left|\,\begin{array}{c} t_1=t_2=m \\ t_3=j\end{array}\right. \sim \text{Binomial}(2,\alpha_{mj})$$

Hence,

$$\begin{aligned}\mathbb{E}\left[Z_j^{|\nu_{2,3}(\boldsymbol{\alpha})|}\,\middle|\,\begin{array}{c} t_1=t_2=m \\ t_3=j\end{array}\right] &= \sum_{i=0}^{2}\binom{2}{i}\alpha_{mj}^i(1-\alpha_{mj})^{2-i}Z_j^i \\ &= \sum_{i=0}^{2}\binom{2}{i}\alpha_{mj}^i(1-\alpha_{mj})^{2-i}\left(1-p_{mj}\right)^i \\ &= 1-2\alpha_{mj}p_{mj}+\left(\alpha_{mj}p_{mj}\right)^2 \end{aligned} \tag{7.54}$$

upon recalling (7.52). Next, let W be a rv that takes the value $\alpha_{mj}p_{mj}$ with probability μ_j. It follows that

$$\sum_{j=1}^{r}\mu_j\mathbb{E}\left[Z_j^{|\nu_{2,3}(\boldsymbol{\alpha})|}\,\middle|\,\begin{array}{c} t_1=t_2=m \\ t_3=j\end{array}\right] = 1-2\Lambda_m+\sum_{j=1}^{r}\mu_j\left(\alpha_{mj}p_{mj}\right)^2 = 1-2\Lambda_m+\mathbb{E}\left[W^2\right]$$

Next, we recall (7.4) and let

$$k := \arg\min_j \alpha_{mj}p_{mj}$$

Now, in view of Popoviciu's inequality [74, pp. 9], we see that

$$\begin{aligned} \mathrm{var}(W) &\leq \frac{1}{4}\left(W_{\max} - W_{\min}\right)^2 \\ &= \frac{1}{4}\left(\alpha_{ms}p_{ms} - \alpha_{mk}p_{mk}\right)^2 \\ &\leq \frac{1}{4}\left(\alpha_{ms}p_{ms}\right)^2 \end{aligned} \tag{7.55}$$

We also know from (7.1) that

$$\alpha_{ms}p_{ms} \leq \frac{1}{\mu_s}\Lambda_m \tag{7.56}$$

From (7.55) and (7.56), we get

$$\mathrm{var}(W) \leq \frac{1}{4\mu_s^2}\Lambda_m^2 \tag{7.57}$$

It is now immediate that

$$\mathbb{E}\left[W^2\right] = \left(\mathbb{E}\left[W\right]\right)^2 + \mathrm{var}(W) \leq \left(1 + \frac{1}{4\mu_s^2}\right)\Lambda_m^2 \tag{7.58}$$

by virtue of the fact that $\mathbb{E}\left[W\right] = \Lambda_m$. Using (7.58) into (7.53), we readily obtain

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}\left[u(\boldsymbol{\theta}) = 0\right]] \leq \mu_m^2(1 - p_{mm})\left(1 - 2\Lambda_m + \left(1 + \frac{1}{4\mu_s^2}\right)\Lambda_m^2\right)^{n-2} \tag{7.59}$$

Next, conditioning on $u(\boldsymbol{\theta}) = 1$ and $t_1 = t_2 = m$, we have

$$|\cup_{i \in \nu_{2,k}(\boldsymbol{\alpha})} \Sigma_i| = \begin{cases} 0 & \text{if } |\nu_{2,k}(\boldsymbol{\alpha})| = 0 \\ K_m & \text{if } |\nu_{2,k}(\boldsymbol{\alpha})| = 1 \\ 2K_m - |\Sigma_1 \cap \Sigma_2| & \text{if } |\nu_{2,k}(\boldsymbol{\alpha})| = 2 \end{cases}$$

and by a crude bounding argument, we have

$$|\cup_{i \in \nu_{2,k}(\boldsymbol{\alpha})} \Sigma_i| \geq K_m \mathbf{1}[|\nu_{2,k}(\boldsymbol{\alpha})| > 0] \tag{7.60}$$

Using (7.60) and recalling the analysis for $\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta})=0]]$, we obtain

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}[u(\boldsymbol{\theta})=1]] \leq \mu_m^2(1-\alpha_{mm})p_{mm}\left(\sum_{j=1}^{r}\mu_j\mathbb{E}\left[Z_j^{\mathbf{1}[|\nu_{2,3}(\boldsymbol{\alpha})|>0]} \;\middle|\; \begin{array}{c} t_1=t_2=m \\ t_3=j \end{array}\right]\right)^{n-2} \tag{7.61}$$

where

$$\mathbb{E}\left[Z_j^{\mathbf{1}[|\nu_{2,3}(\boldsymbol{\alpha})|>0]} \;\middle|\; \begin{array}{c} t_1=t_2=m \\ t_3=j \end{array}\right] = (1-\alpha_{mj})^2 + \left(1-(1-\alpha_{mj})^2\right)Z_j = 1-2\alpha_{mj}p_{mj}+\alpha_{mj}^2p_{mj}$$

and it follows that

$$\begin{aligned}\sum_{j=1}^{r}\mu_j\mathbb{E}\left[Z_j^{\mathbf{1}[|\nu_{2,3}(\boldsymbol{\alpha})|>0]} \;\middle|\; \begin{array}{c} t_1=t_2=m \\ t_3=j \end{array}\right] &= 1-2\Lambda_m+\sum_{j=1}^{r}\mu_j\alpha_{mj}^2p_{mj} \\ &\leq 1-2\Lambda_m+\alpha_{md}\sum_{j=1}^{r}\mu_j\alpha_{mj}p_{mj} \\ &= 1-(2-\alpha_{md})\Lambda_m \end{aligned} \tag{7.62}$$

upon recalling (7.3). From (7.61) and (7.62), we readily obtain

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\mathbf{1}\left[u(\boldsymbol{\theta})=1\right]] \leq \mu_m^2(1-\alpha_{mm})p_{mm}\left(1-(2-\alpha_{md})\Lambda_m\right)^{n-2} \tag{7.63}$$

Combining (7.59) and (7.63), we get

$$\begin{aligned}\mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})] &= \mathbb{E}[x_{n,1}(\boldsymbol{\mu},\boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu},\boldsymbol{\Theta})\left(\mathbf{1}[u(\boldsymbol{\theta})=0]+\mathbf{1}[u(\boldsymbol{\theta})=1]\right)] \\ &\leq \mu_m^2(1-p_{mm})\left(1-2\Lambda_m+\left(1+\frac{1}{4\mu_s^2}\right)\Lambda_m^2\right)^{n-2} \\ &\quad + \mu_m^2(1-\alpha_{mm})p_{mm}\left(1-(2-\alpha_{md})\Lambda_m\right)^{n-2} \end{aligned} \tag{7.64}$$

It is also clear that

$$\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta})] = \mu_m (1 - \Lambda_m)^{n-1} \tag{7.65}$$

Combining (7.64) and (7.65), we get

$$\begin{aligned}\frac{\mathbb{E}[x_{n,1}(\boldsymbol{\mu}, \boldsymbol{\Theta})x_{n,2}(\boldsymbol{\mu}, \boldsymbol{\Theta})]}{\mathbb{E}[x_{n,1}(\boldsymbol{\theta})]^2} &\leq (1 - p_{mm}) \frac{\left(1 - 2\Lambda_m + \left(1 + \frac{1}{4\mu_s^2}\right) \Lambda_m^2\right)^{n-2}}{(1 - \Lambda_m)^{2(n-1)}} + p_{mm} \frac{(1 - 2\Lambda_m + \alpha_{md}\Lambda_m)^{n-2}}{(1 - \Lambda_m)^{2(n-1)}} \\ &:= A + B \end{aligned} \tag{7.66}$$

where we use the fact that $1 - \alpha_{mm} \leq 1$.

We now consider a scaling $\boldsymbol{\Theta} : \mathbb{N}_0 \to \mathbb{N}_0^{r+1} \times (0, 1)^{r \times r}$ as stated in Proposition 7.5.4 and bound the terms A and B in turn. Our goal is to show that

$$\limsup_{n \to \infty} (A + B) \leq 1. \tag{7.67}$$

We have

$$A = \frac{1 - p_{mm}}{(1 - \Lambda_m)^2} \left(1 + \frac{1}{4\mu_s^2} \left(\frac{\Lambda_m}{1 - \Lambda_m}\right)^2\right)^{n-2} \leq \frac{1 - p_{mm}}{(1 - \Lambda_m)^2} e^{\rho_n}$$

where

$$\rho_n \leq \left(\frac{c_n}{2\mu_s}\right)^2 n \left(\frac{\log n}{n - c_n \log n}\right)^2 = o(1)$$

and

$$(1 - \Lambda_m(n))^2 = 1 - o(1) \tag{7.68}$$

since $\Lambda_m(n) = c_n \log n / n$. Thus, we have

$$A \leq (1 - p_{mm}) \left((1 + o(1))\, e^{o(1)}\right) \tag{7.69}$$

We now consider the second term in (7.66). Recall (7.68), we have

$$B = \frac{p_{mm}}{(1-\Lambda_m)^2}\left(1+\frac{\Lambda_m(\alpha_{md}-\Lambda_m)}{(1-\Lambda_m)^2}\right)^{n-2} \leq \frac{p_{mm}}{(1-\Lambda_m)^2}e^{\psi_n}$$

Now, recalling (7.32), we get

$$\psi_n \leq n\frac{\Lambda_m(\alpha_{md}-\Lambda_m)}{(1-\Lambda_m)^2} = \frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2} - \frac{c_n^2\frac{(\log n)^2}{n}}{\left(1-c_n\frac{\log n}{n}\right)^2} = \frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2} - o(1)$$

Thus, we have

$$B \leq p_{mm}.\exp\left(\frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}\right).\left((1+o(1))\,e^{o(1)}\right) \tag{7.70}$$

We will now establish the desired result (7.67) by using (7.69) and (7.70). Our approach is to consider the cases i) $\lim_{n\to\infty}\alpha_{md}(n)\log n = 0$ and ii) $\lim_{n\to\infty}\alpha_{mm}(n)\log n \in (0,\infty]$ separately.

Assume that $\lim_{n\to\infty}\alpha_{md}(n)\log n = 0$. From (7.70) we get $B \leq (1+o(1))p_{mm}$ and upon using (7.69) we see that $A+B \leq (1+o(1))$ establishing (7.67) along subsequences with $\lim_{n\to\infty}\alpha_{md}(n)\log n = 0$.

Assume that $\lim_{n\to\infty}\alpha_{mm}(n)\log n \in (0,\infty]$. From (7.1), we have

$$\Lambda_m = \sum_{j=1}^{r}\mu_j\alpha_{mj}p_{mj} \geq \mu_m\alpha_{mm}p_{mm}$$

Thus,

$$B \leq \frac{1}{\mu_m}\frac{\Lambda_m}{\alpha_{mm}}.\exp\left(\frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}\right) = \frac{1}{\mu_m}\Lambda_m\log n.\frac{\exp\left(\frac{c_n\alpha_{md}\log n}{\left(1-c_n\frac{\log n}{n}\right)^2}\right)}{\alpha_{mm}\log n} \leq \frac{1}{\mu_m}c_n(\log n)^2\,\frac{n^{-1+\frac{c_n}{\left(1-c_n\frac{\log n}{n}\right)^2}}}{\alpha_{mm}\log n}$$

since $\alpha_{md} \leq 1$. We note that

$$\lim_{n\to\infty} -1+\frac{c_n}{\left(1-c_n\frac{\log n}{n}\right)^2} = -1+c < 0$$

for $c < 1$. Thus, it follows that $B = o(1)$ upon noting that $\lim_{n\to\infty} \alpha_{mm} \log n = \alpha_* \in (0, \infty]$. From (7.69) and the fact that $p_{mm} \leq 1$, we have $A + B \leq 1 + o(1)$, and (7.67) follows.

Note that if the matrix $\boldsymbol{\alpha}$ is designed in such a way that $\alpha_{ii} = \max_j\{\alpha_{ij}\}$, i.e., two nodes of the same type are more likely to be adjacent in $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$, then we have $\alpha_{md} = \alpha_{mm}$ and the above two cases collapse to i) $\lim_{n\to\infty} \alpha_{mm}(n) \log n = 0$ or ii) $\lim_{n\to\infty} \alpha_{mm}(n) \log n \in (0, \infty]$. At this point, the zero-law follows even when the sequence $\alpha_{mm} \log n$ does not have a limit by virtue of the *subsubsequence principle* [73, p. 12] (see also [43, Section 7.3]). In other words, if $\alpha_{md} = \alpha_{mm}$, then the zero-law follows without any conditions on the sequence $\alpha_{mm}(n) \log n$. $\square$

7.5.7 Proof of Theorem 7.5.2

Let $C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the event that the graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ is connected, and with a slight abuse of notation, let $I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denote the event that the graph $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ has no isolated nodes. It is clear that if a random graph is connected then it does not have any isolated node, hence

$$C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \subseteq I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$$

and we get

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \leq \mathbb{P}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \tag{7.71}$$

and

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c] = \mathbb{P}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c] + \mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)]. \tag{7.72}$$

In view of (7.71), we obtain the zero-law for connectivity, i.e., that

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha}) \text{ is connected}] = 0 \quad \text{if} \quad c < 1,$$

immediately from the zero-law part of Theorem 7.5.1, i.e., from that $\lim_{n\to\infty} \mathbb{P}[I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] = 0$

if $c < 1$ under the enforced assumptions. It remains to establish the one-law for connectivity. In the remainder of this section, we assume that (7.27) holds for some $c > 1$. From Theorem 7.5.1 and (7.72), we see that the one-law for connectivity, i.e., that

$$\lim_{n\to\infty} \mathbb{P}[\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P) \cap \mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha}) \text{ is connected}] = 1 \quad \text{if} \quad c > 1,$$

will follow if we show that

$$\lim_{n\to\infty} \mathbb{P}[C_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu},\boldsymbol{\Theta}_n)] = 0. \tag{7.73}$$

Our approach will be to find a suitable upper bound for (7.73) and prove that it goes to zero as n goes to infinity with $c > 1$.

We now work towards deriving an upper bound for (7.73); then in Section 7.5.8 we will show that the bound goes to zero as n gets large. Define the event $E_n(\boldsymbol{\mu},\boldsymbol{\theta},\boldsymbol{X})$ via

$$E_n(\boldsymbol{\mu},\boldsymbol{\theta},\boldsymbol{X}) := \cup_{S\subseteq\mathcal{N}:|S|\geq 1}\left[|\cup_{i\in S}\Sigma_i| \leq X_{|S|}\right]$$

where $\mathcal{N} = \{1,\ldots,n\}$ and $\boldsymbol{X} = [X_1 \ \cdots \ X_n]$ is an n-dimensional array of integers. Let

$$L_n := \min\left(\left\lfloor\frac{P}{K_1}\right\rfloor, \left\lfloor\frac{n}{2}\right\rfloor\right) \tag{7.74}$$

and

$$X_\ell = \begin{cases} \lfloor\beta\ell K_1\rfloor & \ell = 1,\ldots,L_n \\ \lfloor\gamma P\rfloor & \ell = L_n+1,\ldots,n \end{cases} \tag{7.75}$$

for some β and γ in $(0,\frac{1}{2})$ that will be specified later. In words, $E_n(\boldsymbol{\mu},\boldsymbol{\theta},\boldsymbol{X})$ denotes the event that there exists $\ell = 1,\ldots,n$ such that the number of unique keys stored by at least one subset of ℓ sensors is less than $\lfloor \beta\ell K_1 \rfloor \mathbf{1}[\ell \leq L_n] + \lfloor \gamma P \rfloor \mathbf{1}[\ell > L_n]$. Using a crude bound, we get

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \leq \mathbb{P}[E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)] + \mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \tag{7.76}$$

Thus, (7.73) will be established by showing that

$$\lim_{n\to\infty} \mathbb{P}[E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)] = 0, \tag{7.77}$$

and

$$\lim_{n\to\infty} \mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0 \tag{7.78}$$

The next proposition establishes (7.77).

Proposition 7.5.5. *Consider scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ such that (7.27) holds for some $c > 1$, (7.10) , and (7.28) hold. Then, we have (7.77) where $\boldsymbol{X}_n$ is as specified in (7.75), $\beta \in (0, \frac{1}{2})$ and $\gamma \in (0, \frac{1}{2})$ are selected such that*

$$\max\left(2\beta\sigma, \beta\left(\frac{e^2}{\sigma}\right)^{\frac{\beta}{1-2\beta}}\right) < 1 \tag{7.79}$$

$$\max\left(2\left(\sqrt{\gamma}\left(\frac{e}{\gamma}\right)^{\gamma}\right)^{\sigma}, \sqrt{\gamma}\left(\frac{e}{\gamma}\right)^{\gamma}\right) < 1 \tag{7.80}$$

Proof. The proof is similar to [157, Proposition 7.2]. Results only require the conditions (7.28) and (7.20) to hold. The latter condition is clearly established in Lemma 7.4.5. □

The rest of the chapter is devoted to establishing (7.78) under the enforced assumptions on the scalings and with $\boldsymbol{X}_n$ as specified in (7.75), $\beta \in (0, \frac{1}{2})$ selected small enough such that (7.79) holds, and $\gamma \in (0, \frac{1}{2})$ selected small enough such that (7.80) holds. We denote by $\mathbb{KG}(S)$ a subgraph of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ whose vertices are restricted to the set S. Define the events

$$\begin{aligned} C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) &:= [\mathbb{KG}(S) \text{ is connected}] \\ B_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) &:= [\mathbb{KG}(S) \text{ is isolated}] \\ A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) &:= C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) \cap B_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) \end{aligned}$$

In other words, $A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)$ encodes the event that $\mathbb{KG}$ is a *component*, i.e., a connected subgraph that is isolated from the rest of the graph. The key observation is that a graph is *not* connected if and only if it has a component on vertices S with $1 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor$; note that if vertices S form a component then so do vertices $\mathcal{N} - S$. The event $I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ eliminates the possibility of $\mathbb{KG}(S)$ containing a component of size one (i.e., an isolated node), whence we have

$$C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \subseteq \cup_{S \in \mathcal{N}: 2 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor} A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)$$

and the conclusion

$$\mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)] \leq \sum_{S \in \mathcal{N}: 2 \leq |S| \leq \left\lfloor \frac{n}{2} \right\rfloor} \mathbb{P}[A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S)]$$

follows.

By exchangeability, we get

$$\begin{aligned} \mathbb{P}[C_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)^c \cap I_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] &\leq \sum_{\ell=2}^{\left\lfloor \frac{n}{2} \right\rfloor} \left(\sum_{S \in \mathcal{N}_{n,\ell}} \mathbb{P}[A_n(\boldsymbol{\mu}, \boldsymbol{\Theta}_n, S) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \right) \\ &= \sum_{\ell=2}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \quad (7.81) \end{aligned}$$

where $\mathcal{N}_{n,\ell}$ denotes the collection of all subsets of $\{1, \ldots, n\}$ with exactly ℓ elements, and $A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denotes the event that the set $\{1, \ldots, \ell\}$ of nodes form a component. As before we have $A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) = C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$, where $C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}_n)$ denotes the event that the set

$\{1,\ldots,\ell\}$ of nodes is connected and $B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ denotes the event that the set $\{1,\ldots,\ell\}$ of nodes is isolated from the rest of the graph.

It is now clear that (7.78) is established once we show that

$$\lim_{n\to\infty}\sum_{\ell=2}^{\left\lfloor\frac{n}{2}\right\rfloor}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c=0. \tag{7.82}$$

We proceed by deriving bounds on the probabilities appearing in (7.82). Conditioning on $\Sigma_1,\ldots,\Sigma_\ell$ and $\{B_{ij}(\boldsymbol{\alpha}), 1\le i<j\le\ell\}$, we get

$$\begin{aligned}
&\mathbb{P}\left[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c\right]\\
&=\mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[C_\ell\left(\boldsymbol{\mu},\boldsymbol{\Theta}_n\right)\cap B_{n,\ell}\left(\boldsymbol{\mu},\boldsymbol{\Theta}_n\right)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c\right]\;\middle|\;\begin{array}{c}\Sigma_1,\ldots,\Sigma_\ell\\ B_{ij}(\boldsymbol{\alpha}),\ i,j=1,\ldots,\ell\end{array}\right]\right]\\
&=\mathbb{E}\left[\mathbf{1}\left[C_\ell\left(\boldsymbol{\mu},\boldsymbol{\Theta}_n\right)\right]\cdot\mathbb{P}\left[B_{n,\ell}\left(\boldsymbol{\mu},\boldsymbol{\Theta}_n\right)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c\;\middle|\;\Sigma_1,\ldots,\Sigma_\ell\right]\right]
\end{aligned} \tag{7.83}$$

since $C_\ell(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ is fully determined by $\Sigma_1,\ldots,\Sigma_\ell$ and $\{B_{ij}(\alpha_n), 1\le i<j\le\ell\}$, and $B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)$ and $E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)$ are independent from $\{B_{ij}(\boldsymbol{\alpha}), 1\le i,j\le\ell\}$.

Next, we consider the probabilities appearing in (7.83). For each $\ell=1,\ldots,n-1$, we have

$$B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)=\bigcap_{k=\ell+1}^{n}\left[\left|\cup_{i\in\nu_{\ell,k}(\boldsymbol{\alpha})}\Sigma_i\right|\cap\Sigma_k=\emptyset\right]$$

with $\nu_{\ell,k}(\boldsymbol{\alpha})$ as defined in (7.49). We have

$$\begin{aligned}
\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\;\middle|\;\Sigma_1,\ldots,\Sigma_\ell\right]&=\mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\right]\;\middle|\;\begin{array}{r}\Sigma_1,\ldots,\Sigma_n,\\ B_{ij}(\boldsymbol{\alpha}):i=1,\ldots,\ell,\\ j=\ell+1,\ldots,n\end{array}\right]\;\middle|\;\Sigma_1,\ldots,\Sigma_\ell\right]\\
&=\mathbb{E}\left[\prod_{k=\ell+1}^{n}\frac{\binom{P-|\cup_{i\in\nu_{\ell,k}(\boldsymbol{\alpha})}\Sigma_i|}{|\Sigma_k|}}{\binom{P}{|\Sigma_k|}}\;\middle|\;\Sigma_1,\ldots,\Sigma_\ell\right]
\end{aligned}$$

Observe that on the event $E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c$ we have

$$\left|\cup_{i\in\nu_{\ell,k}(\boldsymbol{\alpha})}\Sigma_i\right| \geq \left(X_{n,|\nu_{\ell,k}(\boldsymbol{\alpha})|}+1\right)\mathbf{1}[|\nu_{\ell,k}(\boldsymbol{\alpha})|>0]$$

Moreover, the crude bound

$$\left|\cup_{i\in\nu_{\ell,k}(\boldsymbol{\alpha})}\Sigma_i\right| \geq K_{t_{\min,\ell}}\mathbf{1}[|\nu_{\ell,k}(\boldsymbol{\alpha})|>0]$$

always holds with $t_{\min,\ell} = \min\{t_1, \ldots, t_\ell\}$. Hence, we can write

$$\begin{aligned}&\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c \;\middle|\; \Sigma_1, \ldots, \Sigma_\ell\right]\\ &\quad\leq \mathbb{E}\left[\prod_{k=\ell+1}^{n}\frac{\binom{P-\max\left(K_{t_{\min,\ell}},\, X_{n,|\nu_{\ell,k}(\boldsymbol{\alpha})|}+1\right)\mathbf{1}[|\nu_{\ell,k}(\boldsymbol{\alpha})|>0]}{|\Sigma_k|}}{\binom{P}{|\Sigma_k|}} \;\middle|\; \Sigma_1, \ldots, \Sigma_\ell\right]\end{aligned}$$

Note that conditioned on $\Sigma_1, \Sigma_2, \ldots, \Sigma_\ell$, we can determine the class of each node in $\{1, \ldots, \ell\}$, i.e., $t_i = 1\cdot\mathbf{1}\left[|\Sigma_i| = K_1\right]+2\cdot\mathbf{1}\left[|\Sigma_i| = K_2\right]+\ldots+r\cdot\mathbf{1}\left[|\Sigma_i| = K_r\right]$ for $i = 1, \ldots, \ell$. Moreover, since $|\nu_{\ell,k}(\boldsymbol{\alpha})| = \mathbf{1}\left[v_1 \sim_G v_k\right]+\mathbf{1}\left[v_2 \sim_G v_k\right]+\ldots+\mathbf{1}\left[v_\ell \sim_G v_k\right]$, the random variables $\{|\nu_{\ell,k}(\boldsymbol{\alpha})|\}_{k=\ell+1}^{n}$ are independent and identically distributed. In particular

$$|\nu_{\ell,k}(\boldsymbol{\alpha})| \;\Big|\; \Sigma_1, \ldots, \Sigma_\ell \sim \text{Poisson-Binomial}\left(\ell, \boldsymbol{p} = (\alpha_{t_1 j}, \alpha_{t_2 j}, \ldots, \alpha_{t_\ell j})\right) \quad \text{with probability } \mu_j$$

for $k = \ell + 1, 4, \ldots, n$. It follows that

$$\begin{aligned}
&\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c \,\middle|\, \Sigma_1, \ldots, \Sigma_\ell\right] \\
&\leq \left(\mathbb{E}\left[\frac{\binom{P - \max\left(K_{t_{\min,\ell}}, X_{n,|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|} + 1\right) \mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > 0]}{|\Sigma_k|}}{\binom{P}{|\Sigma_k|}} \,\middle|\, \Sigma_1, \ldots, \Sigma_\ell \right] \right)^{n-\ell} \\
&= \left(\sum_{j=1}^{r} \mu_j \mathbb{E}\left[\frac{\binom{P - \max\left(K_{t_{\min,\ell}}, X_{n,|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|} + 1\right) \mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > 0]}{K_j}}{\binom{P}{K_j}} \,\middle|\, \begin{array}{c} \Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j \end{array} \right] \right)^{n-\ell}
\end{aligned} \tag{7.84}$$

by the law of total expectation. Reporting (7.84) into (7.83), we then get

$$\begin{aligned}
&\mathbb{P}\left[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c\right] \leq \mathbb{E}\Bigg[\mathbf{1}\left[C_\ell\left(\boldsymbol{\mu}, \boldsymbol{\Theta}_n\right)\right] \cdot \\
&\cdot \left(\sum_{j=1}^{r} \mu_j \mathbb{E}\left[\frac{\binom{P - \max\left(K_{t_{\min,\ell}}, X_{n,|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|} + 1\right) \mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > 0]}{K_j}}{\binom{P}{K_j}} \,\middle|\, \begin{array}{c} \Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j \end{array} \right] \right)^{n-\ell} \Bigg]
\end{aligned} \tag{7.85}$$

The following lemma gives bounds on the terms appearing in (7.85). The proof is given in Section 7.5.9.

Lemma 7.5.6. *Consider a probability distribution $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_r)$, integers $K_1 \leq \cdots \leq K_r \leq P/2$, and $\boldsymbol{\alpha} = \{\alpha_{ij}\}$ for $i, j = 1, \ldots, r$ with $\alpha_{ij} \in (0, 1)$. With $\boldsymbol{X}_n$ as specified in (7.75), $\beta \in (0, \frac{1}{2})$ and $\gamma \in (0, \frac{1}{2})$ as specified in (7.79) and (7.80) respectively, we have*

$$\mathbb{P}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta})] \leq \min\left\{1, \ell^{\ell-2} \left(\max_{i,j} \{\alpha_{ij} p_{ij}\} \right)^{\ell-1} \right\} \tag{7.86}$$

and

$$\left(\sum_{j=1}^{r}\mu_j\mathbb{E}\left[\frac{\binom{P-\max\left(K_{t_{\min,\ell}},X_{n,|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|}+1\right)\mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|>0]}{K_j}}{\binom{P}{K_j}}\;\middle|\;\begin{matrix}\Sigma_1,\ldots,\Sigma_\ell,\\ t_{\ell+1}=j\end{matrix}\right]\right)^{n-\ell}$$
$$\leq\left(\min\left\{1-\Lambda_m,\min\left\{1-\mu_r+\mu_r e^{-\alpha_{\min}p_{1r}\beta\ell},e^{-\alpha_{\min}p_{11}\beta\ell}\right\}+e^{-\gamma K_1}\mathbf{1}\left[\ell>L_n\right]\right\}\right)^{n-\ell}\qquad(7.87)$$

Note that as we report (7.87) back into (7.85), we get

$$\begin{aligned}&\mathbb{P}\left[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c\right]\\&\leq\mathbb{E}\Bigg[\mathbf{1}\left[C_\ell\left(\boldsymbol{\mu},\boldsymbol{\Theta}_n\right)\right]\cdot\\&\qquad\cdot\left(\min\left\{1-\Lambda_m,\min\left\{1-\mu_r+\mu_r e^{-\alpha_{\min}p_{1r}\beta\ell},e^{-\alpha_{\min}p_{11}\beta\ell}\right\}+e^{-\gamma K_1}\mathbf{1}\left[\ell>L_n\right]\right\}\right)^{n-\ell}\Bigg]\\&=\mathbb{P}[C_\ell(\boldsymbol{\mu},\boldsymbol{\Theta})]\cdot\left(\min\left\{1-\Lambda_m,\min\left\{1-\mu_r+\mu_r e^{-\alpha_{\min}p_{1r}\beta\ell},e^{-\alpha_{\min}p_{11}\beta\ell}\right\}+e^{-\gamma K_1}\mathbf{1}\left[\ell>L_n\right]\right\}\right)^{n-\ell}\end{aligned}\qquad(7.88)$$

In addition, it holds that

$$\max_{i,j}\left\{\alpha_{ij}p_{ij}\right\}\leq\alpha_{\max}p_{rr}\qquad(7.89)$$

Our proof of (7.78) will be completed (see (7.81)) upon establishing

$$\lim_{n\to\infty}\sum_{\ell=2}^{\left\lfloor\frac{n}{2}\right\rfloor}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c]=0\qquad(7.90)$$

by means of (7.86), (7.87), and (7.88). These steps are taken in the next section.

7.5.8 Establishing (7.90)

We will establish (7.90) in several steps with each step focusing on a specific range of the summation over ℓ. Throughout, we consider a scalings $K_1, \ldots, K_r, P : \mathbb{N}_0 \to \mathbb{N}_0^{r+1}$ and $\boldsymbol{\alpha} : \mathbb{N}_0 \to (0,1)^{r\times r}$ such that (7.27) holds with $c > 1$, (7.10), (7.29), (7.31), and (7.28) hold.

The case where $2 \le \ell \le R$

This range considers fixed values of ℓ. Pick an integer R to be specified later at (7.96). Use (7.27), (7.9), (7.21), (7.22), (7.86), the first bound in (7.87), and (7.89) to get

$$\begin{aligned}
\sum_{\ell=2}^{R} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] &\le \sum_{\ell=2}^{R} \left(\frac{en}{\ell}\right)^{\ell} \ell^{\ell-2} \left(\alpha_{\max}(n) p_{rr}(n)\right)^{\ell-1} \left(1 - \Lambda_m(n)\right)^{n-\ell} \\
&\le \sum_{\ell=2}^{R} (en)^{\ell} \left(\frac{(\log n)^{\tau+2}}{n}\right)^{\ell-1} \left(1 - c_n \frac{\log n}{n}\right)^{n-\ell} \\
&\le \sum_{\ell=2}^{R} n \left(e (\log n)^{\tau+2}\right)^{\ell} e^{-c_n \log n \frac{n-\ell}{n}} \\
&= \sum_{\ell=2}^{R} \left(e (\log n)^{\tau+2}\right)^{\ell} n^{1 - c_n \frac{n-\ell}{n}}
\end{aligned}$$

With $c > 1$, we have $\lim_{n\to\infty} \left(1 - c_n \frac{n-\ell}{n}\right) = 1 - c < 0$. Thus, for each $\ell = 2, 3, \ldots, R$ and a finite $\tau > 0$, we have

$$\left(e (\log n)^{\tau+2}\right)^{\ell-1} n^{1 - c_n \frac{n-\ell}{n}} = o(1),$$

whence we get

$$\lim_{n\to\infty} \sum_{\ell=2}^{R} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0.$$

The case where $R + 1 \le \ell \le \min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}$

Our goal in this and the next subsection is to cover the range $R + 1 \le \ell \le \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$. Since the bound given at (7.87) takes a different form when $\ell > L_n$, we first consider the range $R + 1 \le \ell \le \min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}$. Using (7.9), (7.21), (7.22), (7.86), the second bound in (7.87), and (7.89) we get

$$\begin{aligned}&\sum_{\ell=R+1}^{\min\{L_n,\lfloor\frac{\mu_r n}{\beta c_n\log n}\rfloor\}}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c]\\ \leq&\sum_{\ell=R+1}^{\min\{L_n,\lfloor\frac{\mu_r n}{\beta c_n\log n}\rfloor\}}\left(\frac{en}{\ell}\right)^{\ell}\ell^{\ell-2}\left(\frac{(\log n)^{\tau+2}}{n}\right)^{\ell-1}\cdot\left(1-\mu_r\left(1-e^{-\alpha_{\min}(n)\beta\ell p_{1r}(n)}\right)\right)^{n-\ell}\end{aligned}\qquad(7.91)$$

From the upper bound in (7.8) and $\ell\leq\frac{\mu_r n}{\beta c_n\log n}$, we have

$$\alpha_{\min}(n)\beta\ell p_{1r}(n)\leq\beta\frac{\mu_r n}{\beta c_n\log n}\frac{c_n}{\mu_r}\frac{\log n}{n}=1.$$

Using the fact that $1-e^{-x}\geq\frac{x}{2}$ for all $0\leq x\leq 1$, we get

$$1-\mu_r\big(1-e^{-\alpha_{\min}(n)\beta\ell p_{1r}(n)}\big)\leq 1-\frac{\mu_r\alpha_{\min}(n)\beta\ell p_{1r}(n)}{2}\leq e^{-\beta\ell\mu_r\rho\frac{\log n}{2n}}\qquad(7.92)$$

using the lower bound in (7.33). Reporting this last bound in to (7.91) and noting that

$$n-\ell\geq\frac{n}{2},\qquad\ell=2,3,\ldots,\left\lfloor\frac{n}{2}\right\rfloor,\qquad(7.93)$$

we get

$$\begin{aligned}\sum_{\ell=R+1}^{\min\{L_n,\left\lfloor\frac{\mu_r n}{\beta c_n\log n}\right\rfloor\}}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c]\leq&\sum_{\ell=R+1}^{\min\{L_n,\lfloor\frac{\mu_r n}{\beta c_n\log n}\rfloor\}}n\left(e(\log n)^{\tau+2}\right)^{\ell}e^{-\beta\ell\mu_r\rho\frac{\log n}{2n}\frac{n}{2}}\\ \leq&\, n\sum_{\ell=R+1}^{\min\{L_n,\lfloor\frac{\mu_r n}{\beta c_n\log n}\rfloor\}}\left(e\left(\log n\right)^{\tau+2}e^{-\beta\rho\frac{\mu_r}{4}\log n}\right)^{\ell}\\ \leq&\, n\sum_{\ell=R+1}^{\infty}\left(e\left(\log n\right)^{\tau+2}e^{-\beta\rho\frac{\mu_r}{4}\log n}\right)^{\ell}\end{aligned}\qquad(7.94)$$

Given that $\beta, \rho, \mu_r > 0$ and τ is finite, we clearly have

$$e\,(\log n)^{\tau+2}\, e^{-\beta\rho \log n \frac{\mu_r}{4}} = o(1). \tag{7.95}$$

Thus, the geometric series in (7.94) is summable for n sufficiently large, and we have

$$\begin{aligned}
\sum_{\ell=R+1}^{\min\{L_n, \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor\}} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] &\leq (1+o(1))\, n \left(e\,(\log n)^{\tau+2}\, e^{-\beta\rho \log n \frac{\mu_r}{4}}\right)^{R+1} \\
&= (1+o(1))\, n^{1-(R+1)\beta\rho\frac{\mu_r}{4}} \left(e(\log n)^{\tau+2}\right)^{R+1} \\
&= o(1)
\end{aligned}$$

for any positive integer R with

$$R > \frac{8}{\beta\rho\mu_r}. \tag{7.96}$$

This choice is permissible given that $\rho, \beta, \mu_r > 0$.

The case where $\min\{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor, \max(R, L_n)\} < \ell \leq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$

Clearly, this range becomes obsolete if $\max(R, L_n) \geq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$. Thus, it suffices to consider the subsequences for which the range $\max(R, L_n) + 1 \leq \ell \leq \lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor$ is non-empty. There, we use (7.9), (7.21), (7.22), (7.86), the second bound in (7.87), and (7.89) to get

$$\begin{aligned}
&\sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \qquad (7.97) \\
&\leq \sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor} \left(\frac{en}{\ell}\right)^{\ell} \ell^{\ell-2} \left(\frac{(\log n)^{\tau+2}}{n}\right)^{\ell-1} \cdot \left(1 - \mu_r\left(1 - e^{-\beta\ell\alpha_{\min}(n) p_{1r}(n)}\right) + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\
&\leq \sum_{\ell=\max(R,L_n)+1}^{\lfloor \frac{\mu_r n}{2\beta c \log n} \rfloor} n\left(e\,(\log n)^{\tau+2}\right)^{\ell} \left(e^{-\beta\ell\rho\mu_r \frac{\log n}{2n}} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}
\end{aligned}$$

where in the last step we used (7.92) in view of $\ell \leq \frac{\mu_r n}{\beta c_n \log n}$.

Next, we write

$$\begin{aligned}
e^{-\beta\ell\rho\mu_r\frac{\log n}{2n}} + e^{-\gamma K_{1,n}} &= e^{-\beta\ell\rho\mu_r\frac{\log n}{2n}}\left(1 + e^{-\gamma K_{1,n}+\beta\ell\rho\mu_r\frac{\log n}{2n}}\right) \\
&\leq \exp\left\{-\beta\ell\rho\mu_r\frac{\log n}{2n} + e^{-\gamma K_{1,n}+\beta\ell\rho\mu_r\frac{\log n}{2n}}\right\} \\
&\leq \exp\left\{-\beta\ell\rho\mu_r\frac{\log n}{2n}\left(1 - \frac{e^{-\gamma K_{1,n}+\frac{\rho\mu_r^2}{2c_n}}}{\beta\ell\rho\mu_r\frac{\log n}{2n}}\right)\right\} \qquad (7.98)
\end{aligned}$$

where the last inequality is obtained from $\ell \leq \frac{\mu_r n}{\beta c_n \log n}$. Using the fact that $\ell > L_n = \min\{\lfloor\frac{P_n}{K_{1,n}}\rfloor, \lfloor\frac{n}{2}\rfloor\}$ and (7.28) we have

$$\frac{e^{-\gamma K_{1,n}}}{\beta\ell\rho\mu_r\frac{\log n}{2n}} \leq \max\left\{\frac{K_{1,n}}{P_n}, \frac{2}{n}\right\} 2n\frac{e^{-\gamma K_{1,n}}}{\beta\rho\mu_r\log n} \leq \max\left\{\frac{2K_{1,n}e^{-\gamma K_{1,n}}}{\beta\rho\mu_r\sigma\log n}, \frac{4e^{-\gamma K_{1,n}}}{\beta\rho\mu_r\log n}\right\} = o(1)$$

by virtue of (7.20) and the facts that $\beta, \mu_r, \sigma, \rho > 0$. Reporting this into (7.98), we see that for for any $\epsilon > 0$, there exists a finite integer $n^*(\epsilon)$ such that

$$\left(e^{-\beta\ell\rho\mu_r\frac{\log n}{2n}} + e^{-\gamma K_{1,n}}\right) \leq e^{-\beta\ell\rho\mu_r\frac{\log n}{2n}(1-\epsilon)} \qquad (7.99)$$

for all $n \geq n^*(\epsilon)$. Using (7.99) in (7.97), we get

$$\begin{aligned}
\sum_{\ell=\max(R,L_n)+1}^{\lfloor\frac{\mu_r n}{\beta c_n\log n}\rfloor}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] &\leq n\sum_{\ell=\max(R,L_n)+1}^{\lfloor\frac{\mu_r n}{\beta c_n\log n}\rfloor}\left(e\,(\log n)^{\tau+2}\,e^{-\beta\rho\mu_r\frac{\log n}{2n}(1-\epsilon)\frac{n}{2}}\right)^\ell \\
&\leq n\sum_{\ell=\max(R,L_n)+1}^{\infty}\left(e\,(\log n)^{\tau+2}\,e^{-\beta\rho\mu_r\frac{\log n}{4}(1-\epsilon)}\right)^\ell
\end{aligned}$$

(7.100)

Similar to (7.95), we have $\left(e\,(\log n)^{\tau+2}\,e^{-\beta\rho\mu_r\frac{\log n}{4}(1-\epsilon)}\right) = o(1)$ so that the sum in (7.100) converges. Following a similar approach to that in Section 7.5.8, we then see that

$$\lim_{n\to\infty}\sum_{\ell=\max(R,L_n)+1}^{\lfloor\frac{\mu_r n}{2\beta c\log n}\rfloor}\binom{n}{\ell}\mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n)\cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] = 0$$

with R selected according to (7.96) and $\epsilon < 1/2$.

The case where $\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor + 1 \leq \ell \leq \lfloor \nu n \rfloor$

We consider $\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor + 1 \leq \ell \leq \lfloor \nu n \rfloor$ for some $\nu \in (0, \frac{1}{2})$ to be specified later. Recall (7.33), (7.22), the first bound in (7.86), and the second bound in (7.87). Noting that $\binom{n}{\ell}$ is monotone increasing in ℓ when $0 \leq \ell \leq \lfloor \frac{n}{2} \rfloor$ and using (7.93) we get

$$\begin{aligned}
&\sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor+1}^{\lfloor \nu n \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] \\
&\leq \sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor+1}^{\lfloor \nu n \rfloor} \binom{n}{\lfloor \nu n \rfloor} \cdot \left(1 - \mu_r + \mu_r e^{-\alpha_{\min}(n)\beta \ell p_{1r}(n)} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\
&\leq \sum_{\ell=\lfloor \frac{\mu_r n}{\beta c_n \log n} \rfloor+1}^{\lfloor \nu n \rfloor} \left(\frac{e}{\nu}\right)^{\nu n} \cdot \left(1 - \mu_r + \mu_r e^{-\beta \frac{\mu_r n}{\beta c_n \log n} \frac{\rho \log n}{n}} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\
&\leq n \left(\frac{e}{\nu}\right)^{\nu n} \left(1 - \mu_r + \mu_r e^{-\frac{\rho \mu_r}{c_n}} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\
&= n \left(\left(\frac{e}{\nu}\right)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\rho \mu_r}{c_n}} + e^{-\gamma K_{1,n}}\right)\right)^{\frac{n}{2}} \qquad (7.101)
\end{aligned}$$

We have $1 - \mu_r + \mu_r e^{-\frac{\rho \mu_r}{c_n}} < 1$ from $\mu_r, \rho, c > 0$ and $e^{-\gamma K_{1,n}} = o(1)$ from (7.20). Also, it holds that $\lim_{\nu \to 0} \left(\frac{e}{\nu}\right)^{2\nu} = 1$. Thus, if we pick ν small enough to ensure that

$$\left(\frac{e}{\nu}\right)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\rho \mu_r}{c_n}}\right) < 1, \qquad (7.102)$$

then for any $0 < \epsilon < 1 - (e/\nu)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\rho \mu_r}{c_n}}\right)$ there exists a finite integer $n^\star(\epsilon)$ such that

$$\left(\frac{e}{\nu}\right)^{2\nu} \left(1 - \mu_r + \mu_r e^{-\frac{\rho \mu_r}{c_n}} + e^{-\gamma K_{1,n}}\right) \leq 1 - \epsilon, \quad \forall n \geq n^\star(\epsilon).$$

Reporting this into (7.101), we get

$$\lim_{n \to \infty} \sum_{\ell=\lfloor \frac{\mu_r n}{2\beta c \log n} \rfloor+1}^{\lfloor \nu n \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu}, \boldsymbol{\theta}_n, \boldsymbol{X}_n)^c] = 0$$

since $\lim_{n\to\infty} n(1-\epsilon)^{n/2} = 0$.

The case where $\lfloor \nu n \rfloor + 1 \leq \ell \leq \lfloor \frac{n}{2} \rfloor$

In this range, we use (7.23), the first bound in (7.86), the last bound in (7.87), and (7.93) to get

$$\begin{aligned}
\sum_{\ell=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] &\leq \sum_{\ell=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \left(e^{-\beta \ell \alpha_{\min}(n) p_{11}(n)} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\
&\leq \left(\sum_{\ell=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \right) \left(e^{-\beta \nu n \alpha_{\min}(n) p_{11}(n)} + e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}} \\
&\leq \left(4e^{-\beta \nu n \alpha_{\min}(n) p_{11}(n)} + 4e^{-\gamma K_{1,n}}\right)^{\frac{n}{2}}
\end{aligned}$$

With $\beta, \nu, \gamma > 0$ have $e^{-\beta \nu n \alpha_{\min}(n) p_{11}(n)} = o(1)$ from (7.10) and $e^{-\gamma K_{1,n}} = o(1)$ from (7.20). The conclusion

$$\lim_{n\to\infty} \sum_{\ell=\lfloor \nu n \rfloor+1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \mathbb{P}[A_{n,\ell}(\boldsymbol{\mu},\boldsymbol{\Theta}_n) \cap E_n(\boldsymbol{\mu},\boldsymbol{\theta}_n,\boldsymbol{X}_n)^c] = 0$$

immediately follows and the proof of one-law is completed. ■

7.5.9 Establishing Lemma 7.5.6

The bounds given at Lemma 7.5.6 are valid irrespective of how the parameters involved scale with n. Thus, we consider fixed $\boldsymbol{\Theta}$ with constraints given in the statement of Lemma 7.5.6.

Recall that conditioned on $\Sigma_1, \Sigma_2, \ldots, \Sigma_\ell$ and $t_{\ell+1} = j$, the rv $|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|$ is distributed as a Poisson-Binomial rv with ℓ trials and success probability vector $\boldsymbol{p} = \{\alpha_{t_1 j}, \ldots, \alpha_{t_\ell j}\}$. With a slight abuse of notation, let $W_{\ell,j} = 1 - p_{t_{\min,\ell}j}$. Using a crude bound and then (7.6) we get

$$\begin{aligned}
&\mathbb{E}\left[\left.\frac{\dbinom{P - \max\left(K_{t_{\min,\ell}}, X_{n,\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|} + 1\right)\mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > 0]}{K_j}}{\dbinom{P}{K_j}}\,\right|\, \begin{matrix}\Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j\end{matrix}\right] \\
&\leq \mathbb{E}\left[\left.\frac{\dbinom{P - K_{t_{\min,\ell}}\mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > 0]}{K_j}}{\dbinom{P}{K_j}}\,\right|\, \begin{matrix}\Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j\end{matrix}\right] \\
&\leq \mathbb{E}\left[\left. W_{\ell,j}^{\mathbf{1}\left[\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|>0\right]}\,\right|\, \begin{matrix}\Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j\end{matrix}\right] \\
&= \prod_{k=1}^{\ell}(1 - \alpha_{t_k j}) + \left(1 - \prod_{k=1}^{\ell}(1 - \alpha_{t_k j})\right) W_{\ell,j} \\
&= \prod_{k=1}^{\ell}(1 - \alpha_{t_k j})\,(1 - W_{\ell,j}) + W_{\ell,j} \\
&\leq \left(1 - \alpha_{t_{\min,\ell}j}\right)(1 - W_{\ell,j}) + W_{\ell,j} \\
&= 1 - \alpha_{t_{\min,\ell}j}\, p_{t_{\min,\ell}j}. && (7.103)
\end{aligned}$$

upon noting that $\alpha_{t_k j} < 1$ for $k = 1, \ldots, \ell$ and $j = 1, \ldots, r$. It is now immediate that

$$\sum_{j=1}^{r} \mu_j \left(1 - \alpha_{t_{\min,\ell}j}\, p_{t_{\min,\ell}j}\right) = 1 - \Lambda_{t_{\min,\ell}} \leq 1 - \Lambda_m \tag{7.104}$$

Next, consider range $\ell = 1, \ldots, L_n$, where we have

$$\left(X_{n,\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|} + 1\right)\mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > 0] \geq \lceil \beta \left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right| K_1 \rceil$$

With a slight abuse of notation, let $Z_j = 1 - p_{1j}$. Recalling (7.6), we get

$$
\begin{aligned}
&\mathbb{E}\left[\frac{\binom{P - \max\left(K_{t_{\min,\ell}}, X_{n,\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|} + 1\right) \mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > 0]}{K_j}}{\binom{P}{K_j}} \;\middle|\; \begin{matrix} \Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j \end{matrix} \right] \\
&\leq \mathbb{E}\left[\frac{\binom{P - \lceil \beta \, |\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| \, K_1 \rceil}{K_j}}{\binom{P}{K_j}} \;\middle|\; \begin{matrix} \Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j \end{matrix} \right] \\
&\leq \mathbb{E}\left[Z_j^{\beta\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|} \;\middle|\; \begin{matrix} \Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j \end{matrix} \right]
\end{aligned}
\tag{7.105}
$$

Recall that

$$
|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| = \mathbf{1}\left[v_1 \sim_G v_{\ell+1}\right] + \mathbf{1}\left[v_2 \sim_G v_{\ell+1}\right] + \ldots + \mathbf{1}\left[v_\ell \sim_G v_{\ell+1}\right]
$$

and note that conditioned on $\Sigma_1, \ldots, \Sigma_\ell$ and that $t_{\ell+1} = j$, the indicator random variables $\mathbf{1}\left[v_i \sim_G v_{\ell+1}\right]$ are each distributed as a Bernoulli random variable with parameter $\alpha_{t_i j}$ for $i = 1, \ldots, r$, where t_i denotes the class of node v_i. Let $\alpha_{\min_j} = \min\left\{\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{rj}\right\}$. It follows that

$$
|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| \succeq \left|\nu_{\ell,\ell+1}(\alpha_{\min_j})\right|
$$

where $\left|\nu_{\ell,\ell+1}(\alpha_{min_j})\right|$ denotes a binomial rv with parameters ℓ and $\alpha_{\min_j}$, and the operator $\succeq$

denotes the usual stochastic ordering. It follows that

$$\begin{aligned}
&\mathbb{E}\left[\left.\frac{\binom{P-\max(K_{t_{\min,\ell}}, X_{n,\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|}+1)\mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|>0]}{K_j}}{\binom{P}{K_j}}\ \right|\ \begin{matrix}\Sigma_1,\ldots,\Sigma_\ell,\\ t_{\ell+1}=j\end{matrix}\right]\\
&\le \mathbb{E}\left[Z_j^{\beta\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|}\ \middle|\ \begin{matrix}\Sigma_1,\ldots,\Sigma_\ell\\ t_{\ell+1}=j\end{matrix}\right],\\
&\le \mathbb{E}\left[Z_j^{\beta\left|\nu_{\ell,\ell+1}(\alpha_{\min_j})\right|}\ \middle|\ \begin{matrix}\Sigma_1,\ldots,\Sigma_\ell,\\ t_{\ell+1}=j\end{matrix}\right]\\
&= \sum_{k=0}^{\ell}\binom{\ell}{k}\alpha_{\min_j}^k(1-\alpha_{\min_j})^{\ell-k}Z_j^{\beta k}\\
&= \left(1-\alpha_{\min_j}\left(1-Z_j^\beta\right)\right)^\ell\\
&\le \left(1-\alpha_{\min_j}\beta\left(1-Z_j\right)\right)^\ell\\
&\le e^{-\alpha_{\min_j}(1-Z_j)\beta\ell}\\
&= e^{-\alpha_{\min_j}p_{1j}\beta\ell} \qquad (7.106)
\end{aligned}$$

using the fact that $1-Z_j^\beta \ge \beta(1-Z_j)$ with $Z_j \le 1$ and $0\le\beta\le 1$; a proof is available at [156, Lemma 5.2]. On the range $\ell = L_n+1,\ldots,\left\lfloor\frac{n}{2}\right\rfloor$, $|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|$ can be less than or equal to L_n or greater than L_n. In the latter case, we have

$$\max(K_{t_{\min,\ell}}, X_{n,\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|}+1)\mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})|>0] \ge \lfloor\gamma P\rfloor + 1$$

Using (7.105), (7.106), and the fact that (see [155, Lemma 5.4.1] for a proof)

$$\binom{P-K_1}{K_2}\Big/\binom{P}{K_2} \le e^{-\frac{K_2}{P}K_1}$$

for $K_1 + K_2 \leq P$, we have

$$\begin{aligned}
&\mathbb{E}\left[\frac{\binom{P - \max\left(K_{t_{\min,\ell}}, X_{n,\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|} + 1\right)\mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > 0]}{K_j}}{\binom{P}{K_j}} \;\middle|\; \begin{array}{c} \Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j \end{array} \right] \\
&\leq \mathbb{E}\left[Z_j^{\beta\left|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})\right|} \mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| \leq L_n] \;\middle|\; \begin{array}{c} \Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j \end{array} \right] \\
&\quad + \mathbb{E}\left[e^{-\frac{K_j}{P}(\lfloor \gamma P \rfloor + 1)} \mathbf{1}[|\nu_{\ell,\ell+1}(\boldsymbol{\alpha})| > L_n] \;\middle|\; \begin{array}{c} \Sigma_1, \ldots, \Sigma_\ell, \\ t_{\ell+1} = j \end{array} \right] \\
&\leq e^{-\alpha_{\min_j} p_{1j} \beta \ell} + e^{-\gamma K_1} \mathbf{1}[\ell > L_n] \qquad (7.107)
\end{aligned}$$

by virtue of the fact that $K_j \geq K_1$.

Finally, we note the bounds

$$\begin{aligned}
\sum_{j=1}^{r} \mu_j e^{-\alpha_{\min_j} p_{1j} \beta \ell} &\leq (1 - \mu_r) + \mu_r e^{-\alpha_{\min_r} p_{1r} \beta \ell} \\
&\leq (1 - \mu_r) + \mu_r e^{-\alpha_{\min} p_{1r} \beta \ell}
\end{aligned}$$

and that

$$\sum_{j=1}^{r} \mu_j e^{-\alpha_{\min_j} p_{1j} \beta \ell} \leq e^{-\alpha_{\min} p_{11} \beta \ell} \qquad (7.108)$$

The last step used the fact that p_{ij} is monotone increasing in both i and j and $\alpha_{\min_j} \geq \alpha_{\min}$.

Next, we establish (7.86). Let $\mathbb{KG}_\ell$ denote the subgraph of $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P) \cap \mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$ induced on the vertices $\{v_1, \ldots, v_\ell\}$. $\mathbb{KG}_\ell$ is connected if and only if it contains a spanning tree; i.e., we have

$$C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta}) = \cup_{T \in \mathcal{T}_\ell} [T \subseteq \mathbb{KG}_\ell]$$

where $\mathcal{T}_\ell$ denotes the collection of all spanning trees on the vertices $\{v_1, \ldots, v_\ell\}$. Thus,

$$\mathbb{P}[C_\ell(\boldsymbol{\mu}, \boldsymbol{\Theta})] \leq \sum_{T \in \mathcal{T}_\ell} \mathbb{P}\left[T \subseteq \mathbb{KG}_\ell\right]. \tag{7.109}$$

Observe that

$$\begin{aligned}
\mathbb{P}\left[T \subseteq \mathbb{KG}_\ell\right] &= \mathbb{E}\left[\mathbb{E}\left[\mathbf{1}\left[T \subseteq \mathbb{KG}_\ell\right] \mid \Sigma_1, \ldots, \Sigma_\ell\right]\right] \\
&= \mathbb{E}\left[\mathbb{P}\left[T \subseteq \mathbb{KG}_\ell \mid \Sigma_1, \ldots, \Sigma_\ell\right]\right] \\
&\leq \left(\max_{i,j}\left\{\alpha_{ij} p_{ij}\right\}\right)^{\ell-1} \qquad (7.110)
\end{aligned}$$

where the last inequality follows from the facts that i) a tree on ℓ vertices contain $\ell - 1$ edges, and ii) conditioned on $\Sigma_1, \ldots, \Sigma_\ell$, edge assignments in $\mathbb{KG}_\ell$ are independent and each edge probability is upper bounded by $(\max_{i,j}\{\alpha_{ij}p_{ij}\})$. Note that as we use this upper bound, the randomness (stemming from the random variables Σ_1, Σ_2, etc.) disappears and (7.110) follows. We obtain (7.86) upon using (7.110) in (7.109) and noting by Cayley's formula [93] that there are $\ell^{\ell-2}$ trees on ℓ vertices, i.e., $|\mathcal{T}_\ell| = \ell^{\ell-2}$. ■

7.6 Conclusion

In this chapter, we investigated the secure connectivity of wireless sensor networks utilizing the heterogeneous random key predistribution scheme under a heterogeneous on-off channel model, where the channel between a class-i node and a class-j node is on (respectively, off) with probability α_{ij} (respectively, $1 - \alpha_{ij}$) for $i, j = 1, \ldots, r$ inducing a channel probability matrix $\boldsymbol{\alpha} = [\alpha_{ij}]$. We modeled the overall network using a composite random graph obtained by the intersection of inhomogeneous random key graphs $\mathbb{K}(n; \boldsymbol{\mu}, \boldsymbol{K}, P)$ with inhomogeneous Erdős-Rényi graphs $\mathbb{G}(n; \boldsymbol{\mu}, \boldsymbol{\alpha})$. The former graph is naturally induced by the heterogeneous random key predistribution scheme, while the latter is induced by the heterogeneous on-off channel model. We investigated the connectivity of the composite random graph $\mathbb{K}(n;\boldsymbol{\mu},\boldsymbol{K},P)\cap\mathbb{G}(n;\boldsymbol{\mu},\boldsymbol{\alpha})$ and presented conditions (in the form of zero-one laws) on how to scale its parameters so that it i) has no secure node which is isolated and ii) is securely connected, both with high probability when the number of nodes gets large. We also presented numerical results to support these zero-one laws in the finite-node regime.

Chapter 8

Results on inhomogeneous random K-out graphs

8.1 Motivation

The previous discussion in Chapters 6 and 7 focuses on the secure connectivity of wireless sensor networks secured by the heterogeneous random key predistribution scheme under a channel model. In this chapter, we focus instead on random pairwise scheme of Chan, Perrig and Song [24] which was proposed as an alternative to Eschenauer-Gligor scheme. The random pairwise predistribution scheme has a number of advantages over the original scheme of Eschenauer and Gligor: (i) It is *perfectly resilient* against node capture attacks [24]; (ii) Unlike earlier schemes, this pairwise scheme enables both distributed node-to-node authentication and quorum-based node revocation.

The random pairwise scheme is described as follows: Before deployment, each of the n sensor nodes is paired (offline) with K distinct nodes which are randomly selected from among all other nodes. If nodes i and j were paired during the node-pairing stage (i.e., which happens if either node i gets paired with node j, node j gets paired with node i, or both), a unique (pairwise) key is generated and stored in the memory modules of each of the paired sensors together with both their IDs. After deployment, a secure link can be established between two communicating nodes if they have at least one pairwise key in common. The random pairwise scheme gives rise to a class of random graphs denoted by *random K-out graphs* [18, 55]. In particular, Let $\mathbb{H}(n; K)$ denote the random graph on the vertex set $\{1, \ldots, n\}$ where each node selects K other nodes uniformly at random (without replacement) to be paired to. Two distinct nodes i and j are adjacent if i selects j, j selects i, or both. This random graph models the random pairwise key predistribution scheme under full visibility (whereby all nodes are within wireless communication range of each other).

Consider a wireless sensor network secured by the random pairwise scheme. A natural question to ask is: *How should the value of K be selected so that the resulting network is securely connected?*, i.e., there exists a secure communication path between every pair of nodes. After all, the randomness involved in the node-pairing process could give rise to isolated components of nodes that are paired with each others but not to other nodes, rendering the network *disconnected.* The connectivity of wireless sensor networks secured by the random pairwise scheme was investigated in [152], where it was shown that

$$\lim_{n\to\infty} \mathbb{P}\left[\mathbb{H}(n;K) \text{ is connected}\right] = \begin{cases} 0 & \text{if} \quad K=1 \\ 1 & \text{if} \quad K\geq 2 \end{cases} \tag{8.1}$$

In other words, it is sufficient to set $K = 2$ to obtain a network that is connected with high probability as the network size tends to infinity. In fact, it was shown in [152] that the probability of $\mathbb{H}(n;2)$ being connected exceeds 0.99 with as little as $n = 50$ nodes.

Random K-out graphs provide an accurate modeling framework for a class of wireless sensor network utilizing random pairwise key predistribution scheme. An inherent assumption, however, is that all nodes are treated uniformly in a sense that each node selects the same number K of other nodes to be paired to. Indeed, the heterogeneity of emerging wireless sensor networks gives rise to the cases where nodes have dissimilar roles, or dissimilar connectivity, centrality, or security requirements, hence different nodes could be paired to a different number of other nodes. This induces the need for a broader modeling framework that generalizes Chan et al. scheme [24] to heterogeneous networks.

In this chapter, we propose inhomogeneous random K-out graphs $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$, where each of the n nodes is assigned to one of r classes independently with a probability distribution $\boldsymbol{\mu} = \{\mu_1,\ldots,\mu_r\}$. In particular, each node is classified as class-i with probability $\mu_i > 0$, independently. Each class-i node *selects* $K_{i,n}$ distinct nodes uniformly at random from among all other nodes. A pair of nodes are adjacent in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ if at least one selects the other. Without loss of generality, we assume that $K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{r,n}$. Inhomogeneous random K-out graphs generalize standard random K-out graphs to heterogeneous setting where different nodes make different number of selections depending on their corresponding classes. As a result, it might be expected that inhomogeneous K-out graphs would serve as a more natural model in many of the envisioned applications of K-out graphs including pairwise key predistribution in sensor networks and anonymous transactions in cryptocurrency networks [54].

Earlier results on *homogeneous* random K-out graphs $\mathbb{H}(n;K_n)$, where all nodes select the same number K of other nodes, reveal that $\mathbb{H}(n;K_n)$ is connected with high probability (whp) if $K_n \geq 2$ which implies that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ is connected whp if $K_{1,n} \geq 2$. In this chapter, we investigate the connectivity of inhomogeneous random K-out graphs $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ for the special case when $K_{1,n} = 1$, i.e., when each class-1 node selects only one other node. We show that $\mathbb{H}\left(n;\boldsymbol{\mu},\boldsymbol{K}_n\right)$ is connected whp if $K_{r,n}$ is chosen such that $\lim_{n\to\infty} K_{r,n} = \infty$. However, any bounded choice of the sequence $K_{r,n}$ gives a positive probability of $\mathbb{H}\left(n;\boldsymbol{\mu},\boldsymbol{K}_n\right)$ being *not* connected. Simulation results are provided to validate our results in the finite node regime.

8.2 Model definitions

The inhomogeneous random K-out graph, denoted $\mathbb{H}\left(n;\boldsymbol{\mu},\boldsymbol{K}_n\right)$, is constructed on the vertex set $\mathcal{V} = \{1, 2, \ldots, n\}$ as follows. First, each node is assigned a class $i \in \{1, \ldots, r\}$ independently according to a probability distribution $\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_r\}$; i.e., μ_i denotes the probability that a node is class-i and we have $\sum_{i=1}^{r} \mu_i = 1$. We assume $\mu_i > 0$ for all $i = 1, 2, \ldots, r$ and that r is a fixed integer that does not scale with n. Each class-i node selects $K_{i,n}$ distinct nodes uniformly at random from $\mathcal{V} \setminus \{v\}$ and an undirected edge is assigned between a pair of nodes if at least one selects the other. Formally, each node v is associated (independently from others) with a subset $\Gamma_{n,v}(\boldsymbol{\mu},\boldsymbol{K}_n)$ (whose size depends on the class of node v) of nodes selected uniformly at *random* from $\mathcal{V} \setminus \{v\}$. Specifically, for any $A \subseteq \mathcal{V} \setminus \{v\}$, we have

$$\mathbb{P}\left[\Gamma_{n,v}(\boldsymbol{\mu}, \boldsymbol{K}_n) = A \;\middle|\; t_v = i\right] = \begin{cases} \binom{n-1}{K_i}^{-1} & \text{if } |A| = K_i \\ \\ 0 & \text{otherwise} \end{cases} \tag{8.2}$$

where t_v denotes the class of node v. Then, vertices u and v are said to be adjacent in $\mathbb{H}\,(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$, written $u \sim v$, if at least one selects the other; i.e., if

$$u \sim v \quad \text{iff} \quad u \in \Gamma_{n,v}(\boldsymbol{\mu}, \boldsymbol{K}_n) \vee v \in \Gamma_{n,u}(\boldsymbol{\mu}, \boldsymbol{K}_n). \tag{8.3}$$

When $r = 1$, all vertices belong to the same class and thus select the same number (say, K) of other nodes, leading to the *homogeneous* random K-out graph $\mathbb{H}(n; K)$ [18, 55, 152].

Throughout, we set

$$K_{\text{avg},n} = \sum_{i=1}^{r} \mu_i K_{i,n} \tag{8.4}$$

For any distinct nodes $u, v \in \mathcal{V}$, we have

$$\mathbb{P}\left[u \sim v\right] = 1 - \mathbb{P}\left[u \notin \Gamma_{n,v}(\boldsymbol{\mu}, \boldsymbol{K}_n) \cap v \notin \Gamma_{n,u}(\boldsymbol{\mu}, \boldsymbol{K}_n)\right] = 1 - \left(\sum_{i=1}^{r} \mu_i \frac{\binom{n-2}{K_i}}{\binom{n-1}{K_i}}\right)^2 = 1 - \left(1 - \frac{K_{\text{avg},n}}{n-1}\right)^2$$

8.3 Preliminaries

Throughout, we will make use of the following results.

Fact 8.3.1 ([166, Fact 2]). *For $0 \leq x < 1$, and $y = 0, 1, 2, \ldots$, we have*

$$1 - xy \leq (1 - x)^y \leq 1 - xy + \frac{1}{2}x^2y^2$$

Fact 8.3.2 ([166, Fact 4]). *Let integers x and y be both positive functions of n, where $y \geq 2x$.*

For $z = 0, 1, \ldots, x$, we have

$$\frac{\binom{y-z}{x}}{\binom{y}{x}} \geq 1 - \frac{zx}{y-z}, \tag{8.5}$$

and

$$\frac{\binom{y-z}{x}}{\binom{y}{x}} = 1 - \frac{xz}{y} \pm O\left(\frac{x^4}{y^2}\right). \tag{8.6}$$

Fact 8.3.3. *For $r = 1, \ldots, \lfloor \frac{n}{2} \rfloor$ and $n = 1, 2, \ldots,$ we have*

$$\binom{n}{r} \leq \left(\frac{n}{r}\right)^r \left(\frac{n}{n-r}\right)^{n-r} \tag{8.7}$$

Proof. The following bound, established in [127], is valid for all $x = 1, 2, \ldots$

$$\sqrt{2\pi} x^{x+0.5} e^{-x} e^{\frac{1}{12x+1}} < x! < \sqrt{2\pi} x^{x+0.5} e^{-x} e^{\frac{1}{12x}}. \tag{8.8}$$

Observe that

$$\sqrt{2\pi} e^{\frac{1}{12x}} \leq e$$

for all $x \geq 2$. and

$$e^{\frac{1}{12x+1}} \geq 1$$

Hence, (8.8) can be written as

$$\sqrt{2\pi} x^{x+0.5} e^{-x} < x! < e x^{x+0.5} e^{-x} \tag{8.9}$$

Using (8.9), we get

$$\begin{aligned}\binom{n}{r} &= \frac{n!}{r!(n-r)!} \\ &< \frac{en^{n+0.5}e^{-n}}{\sqrt{2\pi}r^{r+0.5}e^{-r}\sqrt{2\pi}(n-r)^{n-r+0.5}e^{-(n-r)}} \\ &= \frac{e}{2\pi}\frac{1}{\sqrt{r}\sqrt{1-\frac{r}{n}}}\frac{1}{\left(\frac{r}{n}\right)^r\left(1-\frac{r}{n}\right)^{n-r}} \\ &\leq \frac{e}{2\pi\sqrt{0.5}}\frac{1}{\left(\frac{r}{n}\right)^r\left(1-\frac{r}{n}\right)^{n-r}} \\ &\leq \left(\frac{n}{r}\right)^r\left(\frac{n}{n-r}\right)^{n-r} \qquad (8.10)\end{aligned}$$

as we use the crude bounds $r \geq 1$ and $r \leq n/2$. ■

For $0 \leq K \leq x \leq y$, we have

$$\frac{\binom{x}{K}}{\binom{y}{K}} = \prod_{\ell=0}^{K-1}\left(\frac{x-\ell}{y-\ell}\right) \leq \left(\frac{x}{y}\right)^K \qquad (8.11)$$

since $\frac{x-\ell}{y-\ell}$ decreases as ℓ increases from $\ell = 0$ to $\ell = K-1$.

Moreover, we have

$$1 \pm x \leq e^{\pm x}, \quad 0 \leq x \leq 1 \qquad (8.12)$$

and

$$1 - e^{-x} \geq \frac{x}{2}, \quad 0 \leq x \leq 1 \qquad (8.13)$$

Throughout, we set

$$\binom{x}{y} = 0, \qquad (8.14)$$

whenever $x < y$.

8.4 Connectivity results

We refer to any mapping $\boldsymbol{K} : \mathbb{N}_0 \to \mathbb{N}_0^r$ as a *scaling* provided it satisfies the condition.

$$K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{r,n} < n, \quad n = 2, 3, \ldots. \tag{8.15}$$

Our main technical results, given next, characterize the connectivity of inhomogeneous random K-out graphs. Throughout, it will be convenient to use the notation

$$P(n; \boldsymbol{\mu}, \boldsymbol{K}_n) := \mathbb{P}\left[\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}_n) \text{ is connected}\right]$$

and

$$C(\boldsymbol{\mu}, \boldsymbol{K}_n) = \frac{1}{1 + \frac{2}{\mu_1^2} e^{2K_{\text{avg},n}}} \tag{8.16}$$

and

$$\begin{aligned} \Psi(n, \boldsymbol{\mu}, \boldsymbol{K}_n) = \max\Bigg\{ & \exp\left(-2\left(1 - \tilde{\mu}\right)\left(\frac{K_{r,n} - 1}{4} - \frac{(0.5)^{K_{r,n}-1}}{\tilde{\mu}}\right)\right), \\ & \exp\left(-\left(1 - \tilde{\mu}\right)\frac{n}{2}\left(1 - e^{-1} - \frac{(0.5)^{K_{r,n}-1}}{\tilde{\mu}}\right)\right)\Bigg\} \end{aligned} \tag{8.17}$$

with $0 < \mu_1 < 1$, $K_{\text{avg},n}$ as defined in (8.4), and $\tilde{\mu} = \sum_{i=1}^{r-1} \mu_i$.

The following result establishes an upper bound on the probability of connectivity of the inhomogeneous random K-out graphs when the sequence $K_{r,n}$ is bounded, i.e., $K_{r,n} = O(1)$

8.4.1 An upper bound on the probability of connectivity

Theorem 8.4.1. *Consider a scaling $\boldsymbol{K} : \mathbb{N}_0 \to \mathbb{N}_0^r$ and a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$. If $K_{r,n} = O(1)$, then*

$$\limsup_{n \to \infty} P(n; \boldsymbol{\mu}, \boldsymbol{K}_n) < 1 \tag{8.18}$$

More precisely, we have

$$P(n;\boldsymbol{\mu},\boldsymbol{K}_n) \leq 1 - C(\boldsymbol{\mu},\boldsymbol{K}_n) + o(1) \tag{8.19}$$

The following result establishes a one-law for connectivity for the inhomogeneous random K-out graph.

8.4.2 A one-law for connectivity

Theorem 8.4.2. *Consider a scaling $\boldsymbol{K} : \mathbb{N}_0 \to \mathbb{N}_0^r$ and a probability distribution $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_i > 0$. If $K_{r,n} = \omega(1)$, then*

$$\lim_{n\to\infty} P(n;\boldsymbol{\mu},\boldsymbol{K}_n) = 1$$

More precisely, we have

$$P(n;\boldsymbol{\mu},\boldsymbol{K}_n) \geq 1 - \frac{\tilde{\mu}^2}{1-\tilde{\mu}}\Psi(n,\boldsymbol{\mu},\boldsymbol{K}_n) \tag{8.20}$$

for all $K_{r,n}$ sufficiently large such that $K_{r,n} \geq \left\lceil 4\left(\frac{(0.5)^{K_{r,n}-1}}{\tilde{\mu}}\right)+1\right\rceil$.

8.4.3 Discussion

Theorems 8.4.1 and 8.4.2 state that $\mathbb{H}\left(n;\boldsymbol{\mu},\boldsymbol{K}_n\right)$ is connected with high probability if $K_{r,n}$ is chosen such that $K_{r,n} = \omega(1)$. On the other hand, if $K_{r,n} = O(1)$, then the probability of connectivity of $\mathbb{H}\left(n;\boldsymbol{\mu},\boldsymbol{K}_n\right)$ is strictly less than one in the limit of large network size. In other words, any *bounded* choice for $K_{r,n}$ gives rise to a positive probability of $\mathbb{H}\left(n;\boldsymbol{\mu},\boldsymbol{K}_n\right)$ being *not* connected. Observe that (8.18) follows from (8.19) by virtue of the fact that $K_{\text{avg},n} = O(1)$ when $K_{r,n} = O(1)$.

Connectivity results in the literature of random graphs are usually presented in the form of zero-one laws, where the probability of connectivity (in the limit as $n \to \infty$) exhibits a sharp transition between two different regimes. In the first (respectively, second) regime, the probability tends to zero (respectively, one) as n tends to infinity. One example of such results is given by (8.1) where the probability that $\mathbb{H}(n;K)$ is connected tends to zero when $K=1$ and tends to one when $K\geq 2$. Other examples include the connectivity results on random key graphs [159], Erdős-Rényi graphs [52], and our results appearing in Chapters 6 and 7. Indeed, Theorem 8.4.1 states that the probability of connectivity is strictly less than one whenever $K_{r,n}=O(1)$ but it does not specify whether or not a zero-law exists in this case. In other words, Theorem 8.4.1 does not reveal whether or not $\lim_{n\to\infty} P(n;\boldsymbol{\mu},\boldsymbol{K}_n)=0$ when $K_{r,n}=O(1)$. Such a zero-law, if exists, would complement the one-law given by Theorem 8.4.2.

A careful look at (8.20) reveals that $P(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ exhibits a lower bound that could either be trivial (negative) or non-trivial (positive). As a result, under the conditions that force the bound to be non-trivial, the probability of connectivity is strictly larger than zero, hence a zero-law does not exist in this case. In what follows, we let $K^\star(\tilde{\mu})$ denote the smallest value of $K_{r,n}$ for which

$$\frac{\tilde{\mu}^2}{1-\tilde{\mu}}\Psi(n,\boldsymbol{\mu},\boldsymbol{K}_n)<1.$$

We present a result that utilizes (8.20) to show that under some conditions on $\tilde{\mu}$ and $K_{r,n}$, the probability of connectivity of $\mathbb{H}\left(n;\boldsymbol{\mu},\boldsymbol{K}_n\right)$ is strictly larger than zero, hence, a zero-law does not hold.

Corollary 8.4.3. *Consider a scaling* $\boldsymbol{K}:\mathbb{N}_0\to\mathbb{N}_0^r$ *and a probability distribution* $\boldsymbol{\mu}=\{\mu_1,\mu_2,\ldots,\mu_r\}$ *with* $\mu_i>0$*. For any* $\tilde{\mu}$*, there exists* $K^\star(\tilde{\mu})$ *such that*

$$P(n;\boldsymbol{\mu},\boldsymbol{K}_n)>0$$

whenever $K_{r,n}\geq K^\star(\tilde{\mu})$*.*

In Table 8.1, we provide the values of $K^\star(\tilde{\mu})$ corresponding to some values of $\tilde{\mu}$. Note that whether or not a zero-law holds for the case when $2\leq K_{r,n}<K^\star(\tilde{\mu})$ cannot by established through (8.20) and is beyond the scope of this chapter.

$\tilde{\mu}$	$K^\star(\tilde{\mu})$	$\tilde{\mu}$	$K^\star(\tilde{\mu})$
0.1	5	0.6	3
0.2	4	0.7	5
0.3	4	0.8	13
0.4	4	0.9	43
0.5	3	0.95	117

Table 8.1: The values of $K^\star(\tilde{\mu})$ corresponding to different values for $\tilde{\mu}$. When $K_{r,n} \geq K^\star(\tilde{\mu})$, the probability of connectivity of $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}_n\right)$ is strictly larger than zero by virtue of (8.20), hence a zero-law does not hold in this case.

8.4.4 The effect of heterogeneity

Theorems 8.4.1 and 8.4.2 reveal a striking difference between inhomogeneous random K-out graphs and their homogeneous counterpart. In the context of $\mathbb{H}(n; K)$, we see from (8.1) that it is sufficient to set $K = 2$ to have a connected network with high probability in the limit of large network size. When the network size n is fixed, Yağan and Makowski [152] showed that

$$\mathbb{P}\left[\mathbb{H}(n; 2) \text{ is connected}\right] \geq 1 - \frac{155}{n^3}, \qquad n \geq 16$$

indicating that the probability of connectivity exceeds 0.99 for as little as $n = 50$ nodes (with $K = 2$). As a result, random K-out graphs $\mathbb{H}(n; K)$ can be connected with orders of magnitude fewer links, in total, as compared to most other random graph models such as Erdős-Rényi graphs [52], random key graphs [159], and inhomogeneous random key graphs [157], where the mean degree (respectively, the *minimum* mean degree in inhomogeneous random key graphs) has to be on the order of $\log n$ to ensure connectivity. In contrast, the mean degree of $\mathbb{H}\left(n; K\right)$ is of order $2K$, i.e., a mean degree of 4 is sufficient to ensure connectivity of $\mathbb{H}(n; K)$.

Observe that *inhomogeneous* random K-out graphs (with $K_{1,n} = 1$) require $K_{r,n}$ to grow unboundedly large as $n \to \infty$ so that the probability of connectivity approaches one in the same limit. In other words, the flexibility of arranging nodes into classes comes at the expense of *sparsity*. In particular, the mean degree of $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}\right)$ has to grow unboundedly large as

$n \to \infty$ to ensure the connectivity of the graph. Fortunately, Theorem 8.4.2 does not specify a particular growth rate function for the sequence $K_{r,n}$, other than $K_{r,n} = \omega(1)$. Hence, one can set $K_{r,n} = \log\log\ldots\log n$ to meet the requirements of Theorem 8.4.2. As a result, inhomogeneous random K-out graphs $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K})$ can be connected with orders of magnitude fewer links, in total, as compared to most other random graph models as mentioned above.

8.4.5 Numerical results

The objective of this subsection is to validate the upper bound given by Theorem 8.4.1 in the finite-node regime using computer simulations. In Figure 8.1, we consider an inhomogeneous random K-out graph with three classes. Namely, we set $\boldsymbol{\mu} = \{0.9, 0.06, 0.04\}$ and $\boldsymbol{K} = (1, 2, K_3)$, i.e., each node is classified as class-1 with probability 0.9, class-2 with probability 0.06, and class-3 with probability 0.04. Nodes belonging to class-1 (respectively, class-2) select only one (respectively, two) other node(s) to be paired to. We vary K_3 from 3 to 20 and observe how the empirical probability of connectivity varies in accordance. In particular, for each value of K_3, we run 10^5 independent experiments for each data point and count the number of times (out of 10^5) when the resulting graph is connected. Dividing this number by 10^5 gives the *empirical* probability of connectivity.

Note that as K_3 varies, K_{avg} varies as well according to (8.4). We can then use (8.16) to plot the theoretical upper bound given by $1 - C(\boldsymbol{\mu}, \boldsymbol{K})$. The results given in Figure 8.1 confirm the validity of Theorem 8.4.1 but also reveals its shortcomings. Observe that the bound appears to be loose for small values of K_3, yet it becomes tighter as K_3 increases. The reasoning behind this phenomenon would become apparent in Section 8.5 as we outline our approach in establishing Theorem 8.4.1. At a high level, our approach is based on bounding the probability of connectivity by the probability of *not* observing isolated components of size two, i.e., components formed by two class-1 nodes u and v such that u has selected v, v has selected u, and none of the other $n-2$ nodes has either selected u or v. When K_3 is large, the probability of observing isolated components of sizes larger than two (i.e., three, four, etc.)

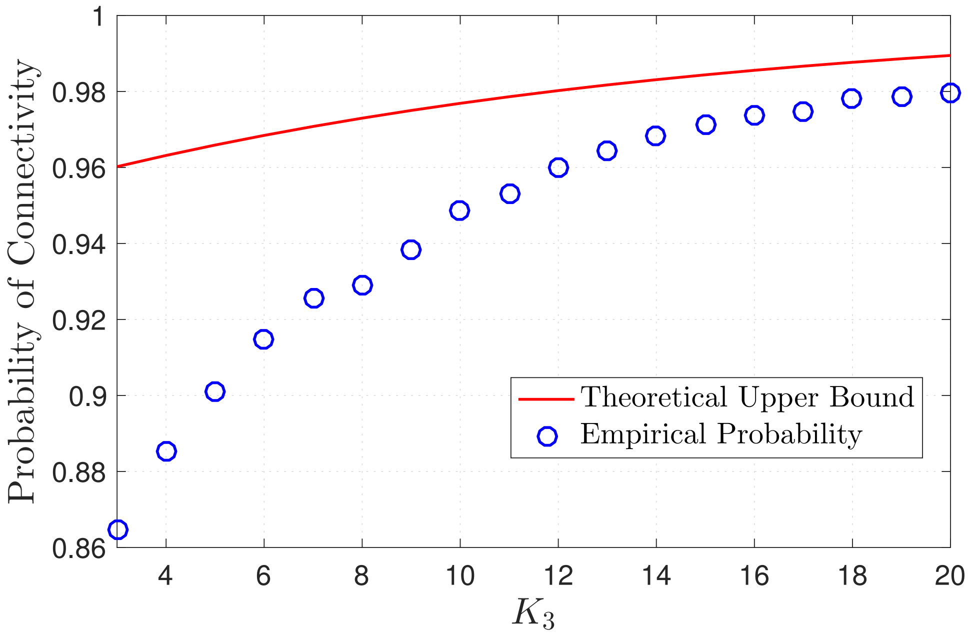


Figure 8.1: *The empirical probability* $P(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ *with* $\boldsymbol{\mu}=\{0.9,0.06,0.04\}$ *and* $\boldsymbol{K}=(1,2,K_3)$ *as a function of* K_3 *for* $n=1000$ *along with the theoretical upper bound given by Theorem 8.4.1. Empirical probabilities approach the upper bound as* K_3 *increases. Empirical probabilities were obtained by averaging over* 10^5 *independent experiments for each data point.*

will be small. Hence, the probability of connectivity in this regime would be tightly bounded by the probability of *not* observing isolated components of size two. However, in the regime where K_3 is small, isolated components of sizes other than two are more likely to be formed, as compared to the case when K_3 is large (see Figure 8.2). Since our approach does not consider such components, our bound becomes slightly loose in this regime.

8.5 A proof of Theorem 8.4.1

In what follows, we establish (8.19) whenever $K_{n,r}=O(1)$. In particular, with each class-1 node selecting only *one* other node, we will show that whenever each class-r node gets paired to a *bounded* number of nodes, there will be a positive probability that the graph is *not* connected. Note that if the sequence $K_{r,n}$ is bounded, then so are the sequences $K_{i,n}$ for $i=2,\ldots,r-1$

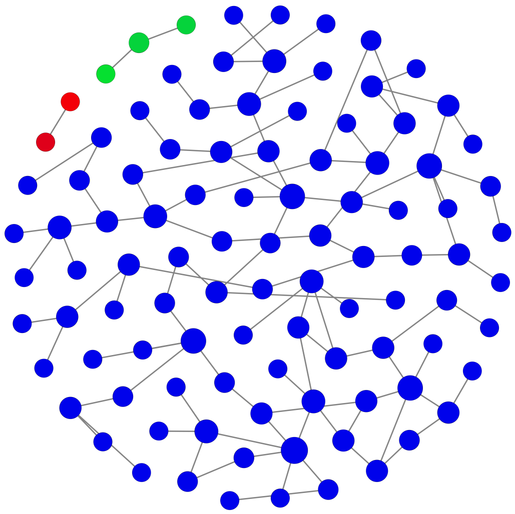


Figure 8.2: *A realization of the inhomogeneous random K-out graph* $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ *with* $r=3$, $\boldsymbol{K}=(1,2,3)$. *The graph is* not *connected as it contains two* isolated *components, highlighted in red and green, respectively. The first isolated component consists of two nodes, while the second isolated component consists of three nodes. We set* $n=100$ *and* $\boldsymbol{\mu}=\{0.9,0.05,0.05\}$. *The size of each node corresponds to its degree.*

by virtue of (8.15). Put differently

$$K_{r,n}=O(1)\Rightarrow K_{i,n}=O(1),\quad i=2,\ldots,r-1$$

Observe that when a positive fraction of the nodes, each, gets paired with only one node, the graph may contain isolated components consisting of two class-1 nodes, say i and j, that were paired with each other, i.e., $\Gamma_{n,i}(\boldsymbol{\mu},\boldsymbol{K}_n)=\{j\}$, $\Gamma_{n,j}(\boldsymbol{\mu},\boldsymbol{K}_n)=\{i\}$, and $\Gamma_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\subseteq\mathcal{N}\setminus\{i,j,\ell\}$ for all $\ell\in\mathcal{N}\setminus\{i,j\}$. Indeed, these isolated components render the graph disconnected. A graphical illustration is given in Figure 8.2. Our approach in establishing Theorem 8.4.1 relies on the method of second moment applied to a variable that counts the number of isolated components that contain two vertices of class-1.

Recall that t_i denotes the class of node i. Let $U_{ij}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ denote the event that nodes i

and j are both class-1 *and* are forming an isolated component, i.e.,

$$\begin{aligned} & U_{ij}(n;\boldsymbol{\mu},\boldsymbol{K}_n) \\ &= \left(\bigcap_{\ell\in\mathcal{N}\setminus\{i,j\}} [\Gamma_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n) \subseteq \mathcal{N}\setminus\{i,j,\ell\}]\right) \cap [\Gamma_{n,i}(\boldsymbol{\mu},\boldsymbol{K}_n) = \{j\}] \\ &\quad \cap [\Gamma_{n,j}(\boldsymbol{\mu},\boldsymbol{K}_n) = \{i\}] \cap [t_1 = 1] \cap [t_2 = 1] \end{aligned} \tag{8.21}$$

Next, let

$$\chi_{ij}(n;\boldsymbol{\mu},\boldsymbol{K}_n) = \mathbf{1}\left[U_{ij}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right]$$

and

$$Y(n;\boldsymbol{\mu},\boldsymbol{K}_n) = \sum_{1\leq i<j\leq n} \chi_{ij}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$$

Clearly, $Y(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ gives the number of isolated components in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ that contain two vertices of class-1. We will show that when $K_{r,n} = O(1)$, we have

$$\mathbb{P}\left[Y(n;\boldsymbol{\mu},\boldsymbol{K}_n) = 0\right] \leq 1 - C(\boldsymbol{\mu},\boldsymbol{K}_n) + o(1)$$

Recall that if $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ is connected, then it does not contain any isolated component. In particular, $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ would consist of a single component of size n. However, the absence of isolated components of size two does not necessarily mean that $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$ is connected, as it may contain isolated components of other sizes (see Figure 8.2). It follows that,

$$P(n;\boldsymbol{\mu},\boldsymbol{K}_n) \leq \mathbb{P}\left[Y(n;\boldsymbol{\mu},\boldsymbol{K}_n) = 0\right]$$

Hence, establishing (8.19) is equivalent to establishing

$$\mathbb{P}\left[Y(n;\boldsymbol{\mu},\boldsymbol{K}_n) = 0\right] \leq 1 - C(\boldsymbol{\mu},\boldsymbol{K}_n) + o(1) \tag{8.22}$$

where $C(\boldsymbol{\mu}, \boldsymbol{K}_n)$ is given by (8.16).

By applying the method of second moments [73, Remark 3.1, p. 55] on $Y(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$, we get

$$\mathbb{P}[Y(n; \boldsymbol{\mu}, \boldsymbol{K}_n) = 0] \leq 1 - \frac{\left(\mathbb{E}[Y(n; \boldsymbol{\mu}, \boldsymbol{K}_n)]\right)^2}{\mathbb{E}[Y^2(n; \boldsymbol{\mu}, \boldsymbol{K}_n)]} \tag{8.23}$$

where

$$\mathbb{E}[Y(n; \boldsymbol{\mu}, \boldsymbol{K}_n)] = \sum_{1 \leq i < j \leq n} \mathbb{E}\left[\chi_{ij}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\right] = \binom{n}{2} \mathbb{E}[\chi_{12}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)] \tag{8.24}$$

and

$$\begin{aligned}
\mathbb{E}[Y^2(n; \boldsymbol{\mu}, \boldsymbol{K}_n)] &= \mathbb{E}\left[\sum_{1 \leq i < j \leq n} \sum_{1 \leq \ell < m \leq n} \chi_{ij}(n; \boldsymbol{\mu}, \boldsymbol{K}_n) \chi_{\ell m}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\right] \\
&= \binom{n}{2} \mathbb{E}\left[\chi_{12}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\right] + 2\binom{n}{2}\binom{n-2}{1} \mathbb{E}\left[\chi_{12}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\chi_{13}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\right] \\
&\quad + \binom{n}{2}\binom{n-2}{2} \mathbb{E}\left[\chi_{12}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\chi_{34}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\right]
\end{aligned}$$

by exchangeability and the binary nature of the random variables $\{\chi_{ij}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\}_{1 \leq i < j \leq n}$. Observe that

$$\mathbb{E}\left[\chi_{12}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\chi_{13}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\right] = 0,$$

since $[U_{12}(n; \boldsymbol{\mu}, \boldsymbol{K}_n) \cap U_{13}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)] = \emptyset$ by definition. Hence,

$$\mathbb{E}[Y^2(n; \boldsymbol{\mu}, \boldsymbol{K}_n)] = \binom{n}{2} \mathbb{E}\left[\chi_{12}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\right] + \binom{n}{2}\binom{n-2}{2} \mathbb{E}\left[\chi_{12}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\chi_{34}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\right] \tag{8.25}$$

Using (8.24) and (8.25), we get

$$\frac{\mathbb{E}[Y^2(n; \boldsymbol{\mu}, \boldsymbol{K}_n)]}{\left(\mathbb{E}[Y(n; \boldsymbol{\mu}, \boldsymbol{K}_n)]\right)^2} = \frac{1}{\binom{n}{2}\mathbb{E}[\chi_{1,2}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)]} + \frac{\binom{n}{2}\binom{n-2}{2}\mathbb{E}[\chi_{1,2}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)\chi_{3,4}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)]}{\left(\binom{n}{2}\mathbb{E}[\chi_{1,2}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)]\right)^2} \tag{8.26}$$

The next two results will help establish (8.22).

Proposition 8.5.1. *Consider a scaling* $\boldsymbol{K} : \mathbb{N}_0 \to \mathbb{N}_0^r$ *and a probability distribution* $\boldsymbol{\mu} = \{\mu_1, \mu_2, \ldots, \mu_r\}$ *with* $\mu_i > 0$. *If* $K_{r,n} = O(1)$, *then*

$$\binom{n}{2}\mathbb{E}\left[\chi_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right] = (1+o(1))\,\frac{\mu_1^2}{2}\exp\left(-2K_{\text{avg},n}\right) \tag{8.27}$$

Proof. Note that under $U_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$, we have

$$\Gamma_{n,1}(\boldsymbol{\mu},\boldsymbol{K}_n) = \{2\} \quad \text{and} \quad \Gamma_{n,2}(\boldsymbol{\mu},\boldsymbol{K}_n) = \{1\}$$

Moreover, we have

$$\Gamma_{n,i}(\boldsymbol{\mu},\boldsymbol{K}_n) \subseteq \mathcal{N} \setminus \{1,2,i\}, \quad i = 3,4,\ldots,n$$

Recall that each of the other $n-2$ nodes is class-i with probability μ_i and that the random variables $\Gamma_{n,1}(\boldsymbol{\mu},\boldsymbol{K}_n), \Gamma_{n,2}(\boldsymbol{\mu},\boldsymbol{K}_n), \ldots, \Gamma_{n,n}(\boldsymbol{\mu},\boldsymbol{K}_n)$ are mutually independent. Hence, we have

$$\mathbb{E}\left[\chi_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right] = \mathbb{P}\left[U_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right] = \mu_1^2\left(\frac{1}{n-1}\right)^2\left(\sum_{i=1}^{r}\mu_i\frac{\binom{n-3}{K_{i,n}}}{\binom{n-1}{K_{i,n}}}\right)^{n-2}$$

Then, we have

$$
\begin{aligned}
\binom{n}{2}\mathbb{E}\left[\chi_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right] &= \frac{\mu_1^2}{2}\left(\frac{n}{n-1}\right)\left(\sum_{i=1}^{r}\mu_i\frac{\binom{n-3}{K_{i,n}}}{\binom{n-1}{K_{i,n}}}\right)^{n-2} \\
&= \frac{\mu_1^2}{2}\left(\frac{n}{n-1}\right)\cdot\left(\sum_{i=1}^{r}\mu_i\left(\frac{(n-1-K_{i,n})}{(n-1)}\frac{(n-2-K_{i,n})}{(n-2)}\right)\right)^{n-2} \\
&= \frac{\mu_1^2}{2}\left(\frac{n}{n-1}\right)\left(\sum_{i=1}^{r}\mu_i\left(1-\frac{K_{i,n}}{n-1}\right)\left(1-\frac{K_{i,n}}{n-2}\right)\right)^{n-2} \\
&= \frac{\mu_1^2}{2}\left(\frac{n}{n-1}\right)\cdot\left(1-\left(\sum_{i=1}^{r}\mu_i\frac{2K_{i,n}(n-1.5)}{(n-1)(n-2)}\right)+\left(\sum_{i=1}^{r}\mu_i\frac{K_{i,n}^2}{(n-1)(n-2)}\right)\right)^{n-2} \\
&= \frac{\mu_1^2}{2}\left(\frac{n}{n-1}\right)\cdot\exp\left(-2\left(\frac{n-1.5}{n-1}\right)\sum_{i=1}^{r}\mu_iK_{i,n}+\frac{1}{n-1}\sum_{i=1}^{r}\mu_iK_{i,n}^2\right) \\
&= (1+o(1))\,\frac{\mu_1^2}{2}e^{-2K_{\mathrm{avg},n}}
\end{aligned}
$$

where the last equality follows since $K_{r,n} = O(1)$. ■

Proposition 8.5.2. *Consider a scaling $\boldsymbol{K}:\mathbb{N}_0\to\mathbb{N}_0^r$ and a probability distribution $\boldsymbol{\mu}=\{\mu_1,\mu_2,\ldots,\mu_r\}$ with $\mu_i>0$. If $K_{r,n}=O(1)$, then*

$$
\frac{\mathbb{E}\left[\chi_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\chi_{34}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right]}{\left(\mathbb{E}\left[\chi_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right]\right)^2} = 1+o(1). \tag{8.28}
$$

Proof. Note that an immediate consequence of Fact 8.3.2 is that

$$
\frac{\binom{n}{2}\binom{n-2}{2}}{\binom{n}{2}^2} = 1+o(1)
$$

Observe that under $[U_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n) \cap U_{34}(n;\boldsymbol{\mu},\boldsymbol{K}_n)]$, we have

$$\Gamma_{n,1}(\boldsymbol{\mu},\boldsymbol{K}_n) = \{2\} \quad \text{and} \quad \Gamma_{n,2}(\boldsymbol{\mu},\boldsymbol{K}_n) = \{1\}$$
$$\Gamma_{n,3}(\boldsymbol{\mu},\boldsymbol{K}_n) = \{4\} \quad \text{and} \quad \Gamma_{n,4}(\boldsymbol{\mu},\boldsymbol{K}_n) = \{3\}$$

Moreover, we have

$$\Gamma_{n,i}(\boldsymbol{\mu},\boldsymbol{K}_n) \subseteq \mathcal{N} \setminus \{1,2,3,4,i\}, \quad i = 5,6,\ldots,n$$

Recall that each of the other $n-4$ nodes is class-i with probability μ_i and that the random variables $\Gamma_{n,1}(\boldsymbol{\mu},\boldsymbol{K}_n), \Gamma_{n,2}(\boldsymbol{\mu},\boldsymbol{K}_n), \ldots, \Gamma_{n,n}(\boldsymbol{\mu},\boldsymbol{K}_n)$ are mutually independent. Hence, we have

$$\mathbb{E}\left[\chi_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\chi_{34}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right] = \mathbb{P}\left[U_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n) \cap U_{34}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right] = \mu_1^4 \left(\frac{1}{n-1}\right)^4 \left(\sum_{i=1}^r \mu_i \frac{\binom{n-5}{K_{i,n}}}{\binom{n-1}{K_{i,n}}}\right)^{n-4}$$

Invoking Fact 8.3.2, we get

$$\begin{aligned}
\frac{\binom{n}{2}\binom{n-2}{2}\mathbb{E}\left[\chi_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\chi_{34}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right]}{\left(\binom{n}{2}\mathbb{E}\left[\chi_{12}(n;\boldsymbol{\mu},\boldsymbol{K}_n)\right]\right)^2} &= (1+o(1)) \frac{\left(\sum_{i=1}^r \mu_i \frac{\binom{n-5}{K_{i,n}}}{\binom{n-1}{K_{i,n}}}\right)^{n-4}}{\left(\sum_{i=1}^r \mu_i \frac{\binom{n-3}{K_{i,n}}}{\binom{n-1}{K_{i,n}}}\right)^{2n-4}} \\
&= (1+o(1)) \cdot \frac{\left(\sum_{i=1}^r \mu_i \left(1 - \frac{4K_{i,n}}{n-1} \pm O\left(\frac{K_{i,n}^4}{n^2}\right)\right)\right)^{n-4}}{\left(\sum_{i=1}^r \mu_i \left(1 - \frac{2K_{i,n}}{n-1} \pm O\left(\frac{K_{i,n}^4}{n^2}\right)\right)\right)^{2n-4}} \\
&= (1+o(1)) \cdot \frac{\left(1 - \frac{4\sum_{i=1}^r \mu_i K_{i,n}}{n-1} \pm O\left(\frac{1}{n^2}\right)\right)^{n-4}}{\left(1 - \frac{2\sum_{i=1}^r \mu_i K_{i,n}}{n-1} \pm O\left(\frac{1}{n^2}\right)\right)^{2n-4}} \\
&= (1+o(1)) \cdot \left(\frac{1 - \frac{4K_{\text{avg},n}}{n-1} \pm O\left(\frac{1}{n^2}\right)}{\left(1 - \frac{2K_{\text{avg},n}}{n-1} \pm O\left(\frac{1}{n^2}\right)\right)^2}\right)^n \\
&= (1+o(1)) \cdot \left(\frac{1 - \frac{4K_{\text{avg},n}}{n-1} \pm O\left(\frac{1}{n^2}\right)}{1 - \frac{4K_{\text{avg},n}}{n-1} \pm O\left(\frac{1}{n^2}\right)}\right)^n \\
&= (1+o(1)) \cdot \left(1 \pm O\left(\frac{1}{n^2}\right)\right)^n = 1 + o(1).
\end{aligned}$$

■

The main result (8.19) now follows by virtue of (8.22) and (8.23) as we combine (8.26), (8.27), and (8.28). Observe that (8.18) follows from (8.19) by virtue of the fact that $K_{\text{avg},n} = O(1)$ when $K_{r,n} = O(1)$.

8.6 A proof of Theorem 8.4.2

In what follows, we establish that

$$\lim_{n\to\infty} P(n; \boldsymbol{\mu}, \boldsymbol{K}_n) = 1 \tag{8.29}$$

whenever $K_{r,n} = \omega(1)$.

Observe that for any non-empty subset S of nodes, i.e., $S \subseteq \mathcal{N}$, we say that S is *isolated* in $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$ if there are no edges in $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$ between the nodes in S and the nodes in the complement $S^c = \mathcal{N} - S$. This is characterized by the event $B_n(\boldsymbol{\mu}, \boldsymbol{K}_n; S)$ given by

$$B_n(\boldsymbol{\mu}, \boldsymbol{K}_n; S) = \bigcap_{i\in S} \bigcap_{j\in S^c} \left([i \notin \Gamma_{n,j}(\boldsymbol{\mu}, \boldsymbol{K}_n)] \cap [j \notin \Gamma_{n,i}(\boldsymbol{\mu}, \boldsymbol{K}_n)] \right).$$

Note that if $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$ is *not* connected, then there must exist a non-empty subset S of nodes which is isolated. Recall that each node in $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$ is class-i with probability μ_i and that $K_{1,n} = 1$. Thus, we may observe isolated sets in $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$ of cardinality[1] $\ell = 2, 3, \ldots, \lfloor \frac{n}{2} \rfloor$. Thus, with $D_n(\boldsymbol{\mu}, \boldsymbol{K}_n)$ denoting the event that $\mathbb{H}(n; \boldsymbol{\mu}, \boldsymbol{K}_n)$ is connected, we have the inclusion

$$D_n(\boldsymbol{\mu}, \boldsymbol{K}_n)^c \subseteq \cup_{S\in\mathcal{P}_n:\ 2\leq|S|\leq\lfloor\frac{n}{2}\rfloor}\ B_n(\boldsymbol{\mu}, \boldsymbol{K}_n; S) \tag{8.30}$$

where $\mathcal{P}_n$ stands for the collection of all non-empty subsets of $\mathcal{N}$. A standard union bound

[1] Note that if vertices S form an isolated set then so do vertices $\mathcal{N} - S$, hence the sum need to be taken only until $\lfloor \frac{n}{2} \rfloor$.

argument immediately gives

$$\mathbb{P}\left[D_n(\boldsymbol{\mu},\boldsymbol{K}_n)^c\right] \leq \sum_{S\in\mathcal{P}_n:2\leq|S|\leq\lfloor\frac{n}{2}\rfloor} \mathbb{P}\left[B_n(\boldsymbol{\mu},\boldsymbol{K}_n;S)\right] = \sum_{\ell=2}^{\lfloor\frac{n}{2}\rfloor}\left(\sum_{S\in\mathcal{P}_{n,\ell}} \mathbb{P}\left[B_n(\boldsymbol{\mu},\boldsymbol{K}_n;S)\right]\right) \tag{8.31}$$

where $\mathcal{P}_{n,\ell}$ denotes the collection of all subsets of $\mathcal{N}$ with exactly ℓ elements.

For each $\ell = 1,\ldots,n$, we simplify the notation by writing $B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n) = B_n(\boldsymbol{\mu},\boldsymbol{K}_n;\{1,\ldots,\ell\})$. Under the enforced assumptions, exchangeability implies

$$\mathbb{P}\left[B_n(\boldsymbol{\mu},\boldsymbol{K}_n;S)\right] = \mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right], \quad S\in\mathcal{P}_{n,\ell}$$

and the expression

$$\sum_{S\in\mathcal{P}_{n,\ell}} \mathbb{P}\left[B_n(\boldsymbol{\mu},\boldsymbol{K}_n;S)\right] = \binom{n}{\ell}\,\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right] \tag{8.32}$$

follows since $|\mathcal{P}_{n,\ell}| = \binom{n}{\ell}$. Substituting into (8.31) we obtain the bounds

$$\mathbb{P}\left[D_n(\boldsymbol{\mu},\boldsymbol{K}_n)^c\right] \leq \sum_{\ell=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{\ell}\,\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right]. \tag{8.33}$$

For each $\ell = 2,\ldots,\lfloor\frac{n}{2}\rfloor$, it is easy to check that

$$\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right] = \left(\sum_{i=1}^{r}\mu_i\frac{\binom{\ell-1}{K_{i,n}}}{\binom{n-1}{K_{i,n}}}\right)^{\ell}\left(\sum_{i=1}^{r}\mu_i\frac{\binom{n-\ell-1}{K_{i,n}}}{\binom{n-1}{K_{i,n}}}\right)^{n-\ell} \tag{8.34}$$

To see why this last relation holds, recall that for nodes $\{1,\ldots,\ell\}$ to be isolated in $\mathbb{H}(n;\boldsymbol{\mu},\boldsymbol{K}_n)$, we need that (i) none of the sets $\Gamma_{n,1}(\boldsymbol{\mu},\boldsymbol{K}_n),\ldots,\Gamma_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)$ contains an element from the set $\{\ell+1,\ldots,n\}$; and (ii) none of the sets $\Gamma_{n,\ell+1}(\boldsymbol{\mu},\boldsymbol{K}_n),\ldots,\Gamma_{n,n}(\boldsymbol{\mu},\boldsymbol{K}_n)$ contains an element from $\{1,\ldots,\ell\}$. More precisely, we must have

$$\Gamma_{n,i}(\boldsymbol{\mu},\boldsymbol{K}_n) \subseteq \{1,\ldots,\ell\}\setminus\{i\}, \quad i=1,\ldots,\ell$$

and

$$\Gamma_{n,j}(\boldsymbol{\mu},\boldsymbol{K}_n) \subseteq \{\ell+1,\ldots,n\} \setminus \{j\}, \quad j=\ell+1,\ldots,n.$$

Hence, the validity of (8.34) is now immediate from (8.2) and the mutual independence of the rvs $\Gamma_{n,1}(\boldsymbol{\mu},\boldsymbol{K}_n),\ldots,\Gamma_{n,n}(\boldsymbol{\mu},\boldsymbol{K}_n)$.

We now establish that under the enforced assumptions of Theorem 8.4.2, we have

$$\lim_{n\to\infty} \sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right] = 0$$

which in turn establishes Theorem 8.4.2 by virtue of (8.33).

Note that the quantities

$$\frac{\binom{\ell-1}{K_{i,n}}}{\binom{n-1}{K_{i,n}}} \quad \text{and} \quad \frac{\binom{n-\ell-1}{K_{i,n}}}{\binom{n-1}{K_{i,n}}}$$

are monotonically decreasing in $K_{i,n}$. We use (8.11) and (8.34) to get

$$\begin{aligned}
&\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right] \\
&= \left(\sum_{i=1}^{r-1} \mu_i \frac{\binom{\ell-1}{K_{i,n}}}{\binom{n-1}{K_{i,n}}} + \mu_r \frac{\binom{\ell-1}{K_{r,n}}}{\binom{n-1}{K_{r,n}}}\right)^{\ell} \cdot \left(\sum_{i=1}^{r-1} \mu_i \frac{\binom{n-\ell-1}{K_{i,n}}}{\binom{n-1}{K_{i,n}}} + \mu_r \frac{\binom{n-\ell-1}{K_{r,n}}}{\binom{n-1}{K_{r,n}}}\right)^{n-\ell} \\
&\leq \left(\frac{\binom{\ell-1}{K_{1,n}}}{\binom{n-1}{K_{1,n}}} \left(\sum_{i=1}^{r-1} \mu_i\right) + \mu_r \frac{\binom{\ell-1}{K_{r,n}}}{\binom{n-1}{K_{r,n}}}\right)^{\ell} \cdot \left(\frac{\binom{n-\ell-1}{K_{1,n}}}{\binom{n-1}{K_{1,n}}} \left(\sum_{i=1}^{r-1} \mu_i\right) + \mu_r \frac{\binom{n-\ell-1}{K_{r,n}}}{\binom{n-1}{K_{r,n}}}\right)^{n-\ell} \\
&\leq \left(\tilde{\mu}\left(\frac{\ell-1}{n-1}\right) + (1-\tilde{\mu})\left(\frac{\ell-1}{n-1}\right)^{K_{r,n}}\right)^{\ell} \cdot \left(\tilde{\mu}\left(\frac{n-\ell-1}{n-1}\right) + (1-\tilde{\mu})\left(\frac{n-\ell-1}{n-1}\right)^{K_{r,n}}\right)^{n-\ell}
\end{aligned} \tag{8.35}$$

where $\tilde{\mu} = \sum_{i=1}^{r-1} \mu_i$ and $1-\tilde{\mu} = \mu_r$.

Observe that the bound appearing in (8.35) resembles the case where each node belongs to one of two classes. Namely, a node could either be class-1 (with probability $\tilde{\mu}$) or class r (with probability $1-\tilde{\mu}$). We further use (8.12) to get

$$\begin{aligned}
&\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right] \\
&\leq \left(\tilde{\mu}\left(\frac{\ell}{n}\right)+(1-\tilde{\mu})\left(\frac{\ell}{n}\right)^{K_{r,n}}\right)^{\ell}\cdot\left(\tilde{\mu}\left(1-\frac{\ell}{n}\right)+(1-\tilde{\mu})\left(1-\frac{\ell}{n}\right)^{K_{r,n}}\right)^{n-\ell} \\
&= \tilde{\mu}^{\ell}\left(\frac{\ell}{n}\right)^{\ell}\left(1+\frac{1-\tilde{\mu}}{\tilde{\mu}}\left(\frac{\ell}{n}\right)^{K_{r,n}-1}\right)^{\ell}\left(1-\frac{\ell}{n}\right)^{n-\ell}\cdot\left(1-(1-\tilde{\mu})\left(1-\left(1-\frac{\ell}{n}\right)^{K_{r,n}-1}\right)\right)^{n-\ell} \\
&\leq \tilde{\mu}^{\ell}\left(\frac{\ell}{n}\right)^{\ell}\left(1-\frac{\ell}{n}\right)^{n-\ell}\left(1+\frac{1-\tilde{\mu}}{\tilde{\mu}}\left(\frac{\ell}{n}\right)^{K_{r,n}-1}\right)^{\ell}\cdot\left(1-(1-\tilde{\mu})\left(1-e^{-\ell\left(\frac{K_{r,n}-1}{n}\right)}\right)\right)^{n-\ell} \\
&\leq \tilde{\mu}^{\ell}\left(\frac{\ell}{n}\right)^{\ell}\left(1-\frac{\ell}{n}\right)^{n-\ell}\exp\left(\frac{1-\tilde{\mu}}{\tilde{\mu}}\ell\left(\frac{\ell}{n}\right)^{K_{r,n}-1}-(1-\tilde{\mu})(n-\ell)\left(1-e^{-\ell\left(\frac{K_{r,n}-1}{n}\right)}\right)\right)
\end{aligned} \tag{8.36}$$

Combining (8.7) with (8.36), we conclude that

$$\mathbb{P}\left[D_n(\boldsymbol{\mu},\boldsymbol{K}_n)^c\right]\leq\sum_{\ell=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{\ell}\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right]\leq\sum_{\ell=2}^{\lfloor\frac{n}{2}\rfloor}\tilde{\mu}^{\ell}A_{n,\ell} \tag{8.37}$$

where we define

$$A_{n,\ell}:=\exp\left(\frac{1-\tilde{\mu}}{\tilde{\mu}}\ell\left(\frac{\ell}{n}\right)^{K_{r,n}-1}-(1-\tilde{\mu})(n-\ell)\left(1-e^{-\ell\left(\frac{K_{r,n}-1}{n}\right)}\right)\right) \tag{8.38}$$

with $2\leq\ell\leq n/2$.

Next, our goal is to derive an upper bound on $A_{n,\ell}$ that is valid for all n sufficiently large and $\ell=2,\ldots,\lfloor\frac{n}{2}\rfloor$, and show that this bound tends to zero as n gets large. Fix $n=2,3,$ sufficiently large. For each $\ell=2,\ldots,\lfloor\frac{n}{2}\rfloor$, either one of the following should hold

$$\frac{\ell(K_{r,n}-1)}{n}\leq 1 \quad\text{and}\quad \frac{\ell(K_{r,n}-1)}{n}>1.$$

If it holds that $\frac{\ell(K_{r,n}-1)}{n}\leq 1$, then we use (8.13) to get $1-e^{-\ell\left(\frac{K_{r,n}-1}{n}\right)}\geq\frac{\ell(K_{r,n}-1)}{2n}$. Using this in (8.38) yields

$$\begin{aligned} A_{n,\ell} &\leq \exp\left(\frac{1-\tilde{\mu}}{\tilde{\mu}}\ell\left(\frac{\ell}{n}\right)^{K_{r,n}-1} - (1-\tilde{\mu})(n-\ell)\frac{\ell(K_{r,n}-1)}{2n}\right) \\ &\leq \exp\left(\frac{1-\tilde{\mu}}{\tilde{\mu}}\ell\left(\frac{1}{2}\right)^{K_{r,n}-1} - (1-\tilde{\mu})\frac{\ell(K_{r,n}-1)}{4}\right) \qquad (8.39) \\ &= \exp\left(-(1-\tilde{\mu})\,\ell\left(\frac{(K_{r,n}-1)}{4} - \frac{(0.5)^{K_{r,n}-1}}{\tilde{\mu}}\right)\right) \\ &\leq \exp\left(-2(1-\tilde{\mu})\left(\frac{(K_{r,n}-1)}{4} - \frac{(0.5)^{K_{r,n}-1}}{\tilde{\mu}}\right)\right) \qquad (8.40) \end{aligned}$$

where (8.39) follows from the facts that $n-\ell \geq n/2$ and $\ell/n \leq 0.5$ on the specified range for ℓ, and (8.40) follows for all $K_{r,n}$ sufficiently large such that $K_{r,n} \geq \left\lceil 4\left(\frac{(0.5)^{K_{r,n}-1}}{\tilde{\mu}}\right)+1\right\rceil$ upon noting that $\ell \geq 2$.

If, on the other hand, it holds that $\frac{\ell(K_{r,n}-1)}{n} > 1$, we see that $1-e^{-\ell\left(\frac{K_{r,n}-1}{n}\right)} \geq 1-e^{-1}$. Reporting this into (8.38) and using $\ell \leq n/2$, we get

$$\begin{aligned} A_{n,\ell} &\leq \exp\left(\frac{1-\tilde{\mu}}{\tilde{\mu}}\ell\left(\frac{\ell}{n}\right)^{K_{r,n}-1} - (1-\tilde{\mu})(n-\ell)\left(1-e^{-1}\right)\right) \\ &\leq \exp\left(\frac{1-\tilde{\mu}}{\tilde{\mu}}\left(\frac{n}{2}\right)(0.5)^{K_{r,n}-1} - (1-\tilde{\mu})\frac{n}{2}\left(1-e^{-1}\right)\right) \\ &= \exp\left(-(1-\tilde{\mu})\frac{n}{2}\left(1-e^{-1}-\frac{(0.5)^{K_{r,n}-1}}{\tilde{\mu}}\right)\right). \qquad (8.41) \end{aligned}$$

Combining (8.40) and (8.41) we see that $A_{n,\ell} \leq \Psi(n,\boldsymbol{\mu},\boldsymbol{K}_n)$ for all n sufficiently large and all $\ell = 2,\ldots,\lfloor\frac{n}{2}\rfloor$, where $\Psi(n,\boldsymbol{\mu},\boldsymbol{K}_n)$ is given by (8.17).

Observing that the bound derived on $A_{n,\ell}$ is independent on ℓ, we get from (8.17) and (8.37)

$$\sum_{\ell=2}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{\ell}\mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu},\boldsymbol{K}_n)\right] \leq \Psi(n,\boldsymbol{\mu},\boldsymbol{K}_n)\sum_{\ell=2}^{\infty}\tilde{\mu}^{\ell} = \frac{\tilde{\mu}^2}{1-\tilde{\mu}}\Psi(n,\boldsymbol{\mu},\boldsymbol{K}_n)$$

Letting n go to infinity, it is now easy to see that

$$\lim_{n\to\infty}\Psi(n,\boldsymbol{\mu},\boldsymbol{K}_n) = 0, \quad 2 \leq \ell \leq n/2$$

under the enforced assumption that $\lim_{n\to\infty} K_{r,n} = \infty$. Hence, the conclusion

$$\lim_{n\to\infty} \sum_{\ell=2}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{\ell} \mathbb{P}\left[B_{n,\ell}(\boldsymbol{\mu}, \boldsymbol{K}_n)\right] = 0$$

immediately follows since $0 < \tilde{\mu} < 1$. This establishes Theorem 8.4.2.

8.7 Conclusion

In this chapter, we have proposed inhomogeneous random K-out graphs $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}_n\right)$ where nodes are arranged into r disjoint classes and the number of selections made by a node is dependent on its class. In particular, we consider the case where each node is classified as class-i with probability $\mu_i > 0$ for $i = 1, \ldots, r$. A class-i node selects $K_{i,n}$ other nodes uniformly at random to be paired to. Two nodes are deemed adjacent if at least one selects the other. Without loss of generality, we assumed that $K_{1,n} \leq K_{2,n} \leq \ldots \leq K_{r,n}$.

Earlier results on homogeneous random K-out graphs (where all nodes select K other nodes) suggest that the graph is connected whp if $K \geq 2$. Hence, $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}_n\right)$ is trivially connected whenever $K_{1,n} \geq 2$. We investigated the connectivity of $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}_n\right)$ in the particular case when $K_{1,n} = 1$. Our results revealed that when $K_{1,n} = 1$, $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}_n\right)$ is connected with high probability if and only if $K_{r,n} = \omega(1)$. Any bounded choice of $K_{r,n}$ is shown to yield a positive probability of $\mathbb{H}\left(n; \boldsymbol{\mu}, \boldsymbol{K}_n\right)$ being *not* connected, and an explicit lower bound on this probability is provided.

Part III

Application Area II: Modeling real-world social networks

Chapter 9

The multiple-strain model on random graphs with arbitrary degree distribution

9.1 Motivation

What causes an outbreak of a disease? How can we predict its emergence and control its progression? Over the past several decades, multidisciplinary research efforts were converging to tackle the above questions, aiming for providing a better understanding of the intricate dynamics of disease propagation and accurate predictions on its course [6, 12, 28, 56, 65, 89, 103, 104, 111, 120, 120, 145, 146]. At the heart of these research efforts is the development of mathematical models that provide insights on predicting, assessing, and controlling potential outbreaks [20, 34, 77, 135]. The early mathematical models relied on the *homogeneous mixing* assumption, meaning that an infected individual is equally likely to infect any other individual in the population, without regard to her location, age, or the people with whom she interacts. Homogeneity allowed writing a set of differential equations that characterize the speed and scale of propagation (in the limit of large population size), providing insights on how the parameters of a disease, e.g., its *basic reproductive number*, indicate whether a disease will die out, or an epidemic will emerge [6, 77].

In real-life, however, the spread of a disease is highly dependent on the contact patterns between individuals. In particular, a person may only infect those with whom she interacts, and the number of contacts people have, varies dramatically between individuals. These basic observations render the homogeneous mixing models inaccurate, as they tend to underestimate the epidemic size in the initial stages of the outbreak and overestimate it towards the end [11]. As a result of the these shortcomings, *network epidemics* has emerged as a mathematical modeling approach that takes the underlying contact network into consideration [12, 76, 98, 111, 119]. Since then, a large body of research has looked into the delicate interplay between the structural properties of the contact network and the dynamics of propagation, leading to accurate predictions of the spatio-temporal progression of disease outbreaks. In addition to diseases, opinions and information also propagate through networks in patterns similar to those of epidemics [39]. Hence, research efforts on *information propagation* draw on the theory of infectious diseases to model the dynamics of propagation [65, 71, 102, 160, 168]. Throughout, we use the term *spreading processes* to denote a general class of processes that propagate in contact networks, such as infectious diseases and information.

A common theme among the proposed models for network epidemics is the assumption that the propagating object, i.e., a virus or a piece of information, is transferred across the nodes without going through any modification or *evolution* [6,10,35,114,124,130,158,160,168]. However, in real-life spreading processes, pathogens often *evolve* in response to changing environments and medical interventions [3, 7, 86, 104, 123], and information is often modified by individuals before being forwarded [1, 163]. In fact, 60% of the (approximately) 400 emerging infectious diseases that have been identified since 1940 are zoonotic [1] [75, 105]. A zoonotic disease is initially poorly adapted, poorly replicated, and inefficiently transmitted [118], hence its ability to go from animal-to-human transmissions to human-to-human transmissions depends on the pathogen *evolving* to a strain that is well-adapted to the human host.

Similar patterns of evolution are observed in the way information propagates among individuals. Needless to say, one observes, on a daily basis, how information mutates unintentionally, or perhaps intentionally by an adversary, on social media platforms [1]. At a high-level, an individual may mutate the information by exaggeration, hoping for her variant to go viral.

[1] A zoonosis is any disease or infection that is naturally transmissible from vertebrate animals to humans [117].

Mutations may also occur unintentionally. In particular, Dawkins [29] argued that ideas and information spread and evolve between individuals with patterns similar to genes, in a sense that they self-replicate, mutate, and respond to selective pressure as they interact with their host. Concluding, if we are to ignore evolution, we underestimate the severity of the epidemic and fail to understand the intricate interplay between the dynamics of propagation and evolution.

In this chapter, we aim to bridge the disconnect between how spreading processes propagate *and evolve* in real-life, and the current mathematical and simulation models that do not capture evolution. In particular, we investigate the *evolution* of spreading processes with the aim of i) revealing the role of evolutionary adaptations on the threshold, probability, and final size of epidemics; and ii) understanding the interplay between the structural properties of the network and the evolutionary adaptations of the process. Throughout, we use the term *epidemics* to denote disease/information outbreaks that result in a positive fraction of infected individuals in the limit of large network size and *self-limited outbreaks* to denote small disease/information outbreaks for which the fraction of infected individuals tends to zero in the limit of large network size. We also use the term *strain* to denote a pathogen strain in the context of infectious disease propagation, or a particular variation of the information in the context of information propagation. At a high level, strains represent homogeneous groups within species [9] and they generally possess unique features such as virulence, infectivity, growth rate, etc.

In modeling the underlying contact network, we utilize *random graphs with arbitrary degree distribution* generated by the configuration model [100,115]. The configuration model generates random graphs with specified degree sequence (sampled from an arbitrary degree distribution), but are otherwise random, by taking a uniformly random matching on the half-edges of the specified degree sequence. The model provides a tractable mathematical framework that allows the investigation of several key properties related to the spreading process and how it interacts with the structure of the underlying graph, as specified by its degree distribution. In addition, since the model could match the degree sequence of real-world social networks, it would essentially generate graphs that resemble such real-world networks to a great extent.

In modeling the evolutionary adaptations of spreading processes, we adopt the (inhomogeneous) multiple-strain model that was introduced by Alexander and Day in [3]. Their model can be briefly outlined as follows (more details are given in Section 9.4). Consider a multiple-strain spreading process that starts with an individual, i.e., the seed, receiving infection (from an external reservoir) with strain-1 of a particular pathogen (respectively, information). The seed infects each of her contacts independently with probability T_1, called the *transmissibility* of strain-1. Once a susceptible individual receives the infection from the seed, the pathogen may evolve within that new host prior to any subsequent infections. In particular, the pathogen may remain as strain-1 with probability μ_{11} or mutate to strain-2 (that has transmissibility T_2) with probability $\mu_{12} = 1 - \mu_{11}$. If the pathogen remains as strain-1 (respectively, mutates to strain-2) within a newly infected host, then that host infects each of her susceptible neighbors in the subsequent stages independently with probability T_1 (respectively, T_2). As the process continues to grow, if any susceptible individual receives strain-1, the pathogen may remain as strain-1 with probability μ_{11} or mutate to strain-2 with probability $\mu_{12} = 1 - \mu_{11}$ prior to subsequent infections. Similarly, if any susceptible individual receives strain-2, the pathogen may remain as strain-2 with probability μ_{22} or mutate to strain-1 with probability $\mu_{21} = 1 - \mu_{22}$ prior to subsequent infections. The process continues to grow until no additional infections are possible. We remark that it is straightforward to extend the model to the general case, where there are m possible strains for some finite integer $m \geq 2$. More details are given in Section 9.5.

Note that as multiple strains propagate throughout the population, a susceptible individual may simultaneously get into infectious contact with neighbors infected with strain-1 as well as neighbors infected with strain-2. This gives rise to the possibility of a susceptible individual becoming *co-infected* with multiple pathogen strains. Indeed, co-infection with multiple pathogen strains is prevalent in disease-causing protozoa, helminths, bacteria, fungi, and viruses and is known to cause significant implications [4,9,25,126,139]. However, from a mathematical standpoint, the possibility of co-infections creates phase discontinuities (see Section 9.8) that render the process mathematically intractable.

We start by considering the case when co-infection is ignored, meaning that a susceptible individual may *only* be infected with a single strain. In particular, a susceptible individual who simultaneously receives x infections of strain-1 and y infections of strain-2 becomes infected by strain-1 (respectively, strain-2) with probability $x/(x+y)$ (respectively, $y/(x+y)$). In this case, we develop a mathematical theory that draws on the tools developed for analyzing the zero-temperature random-field Ising model on Bethe lattices [133] as well as on random graphs [60,61]. Our theory fully characterizes the process and accurately predicts the epidemic threshold, expected epidemic size and the expected fraction of individuals infected by each strain (all at steady state). These metrics are computed as functions of the characteristics of the spreading process (i.e., T_1 and T_2), evolutionary adaptations (i.e., μ_{11} and μ_{22}), and the structure of the underlying contact network (e.g., its degree distribution).

In addition to the mathematical theory, we perform extensive simulations on random graphs with arbitrary degree distributions (generated by the configuration model [18,100,115]) as well as with real-world networks (obtained from SNAP dataset [83] as well as [131] and [141]) to verify our theory and reveal the significant shortcomings of the classical mathematical models that do not capture evolution. In particular, we show that the classical, single-type bond-percolation models [5,96,101,111] may accurately predict the threshold and final size of epidemics, but their predictions on the probability of emergence are *significantly inaccurate* on both random and real-world networks. This inaccuracy sheds the light on a fundamental disconnect between the classical single-type, bond-percolation models and real-life spreading processes that entail evolution.

We then focus on the case where co-infection is possible. Although recent studies have shown that co-infection with multiple pathogen strains is prevalent in nature [4,9,25,126, 139], there has been a lack of models that explain its occurrence, reveal its implications, and investigate its delicate interplay with the underlying contact network. Note that a considerable amount of literature has examined the case where co-infection with multiple *diseases* is possible [8, 21, 27, 66], yet multiple-disease co-infection is fundamentally different from multiple-strain co-infection (see Section 9.3). In this chapter, we use computer simulations to explore the case where multiple-strain co-infection is possible. In particular, a susceptible individual who gets infected with strain-1 and strain-2 *simultaneously* becomes co-infected, and starts to transmit the co-infection, i.e., the mixture of the two strains, with a transmissibility T_{co}.

The transmissibility T_{co} could be larger than the maximum of T_1 and T_2 (e.g., modeling a synergistic cooperation between the two resident strains) or smaller than their minimum (e.g., modeling a negative competition among the two resident strains), and it may also fall anywhere in between. We show that co-infection gives rise to a rich set of dynamics: it can amplify or inhibit the spreading dynamics, and more remarkably *lead the order of phase transition to change from second-order to first-order*. We investigate the interplay between the characteristics of co-infection, the structure of the underlying contact network, and evolutionary adaptations and reveal the cases where such interplay induces a *first-order* phase transition for the expected epidemic size.

9.2 A roadmap

We consider the evolution of spreading processes in complex networks. We start with the case where co-infection is ignored. In this case, we develop a mathematical theory that unravels the relationship between the characteristics of the spreading process, the structure of the underlying contact network, and the process of evolution, thereby, providing accurate predictions on the epidemic threshold, expected epidemic size, and the expected fraction of individuals infected by each strain at steady state. In addition to the mathematical theory, we perform extensive simulations on random and real-world networks to verify our theory and reveal the significant shortcomings of the classical mathematical models that do not capture evolution. Then, we use computer simulations to explore the case where co-infection is possible and show that co-infection could *lead the order of phase transition to change from second-order to first-order.*

We investigate the interplay between the characteristics of co-infection, the structure of the underlying contact network, and evolutionary adaptations and explain how such interplay controls the order of phase transition for the expected epidemic size.

9.3 Related work

9.3.1 Evolution of infectious diseases

A large body of research has investigated the role of evolutionary adaptations in enabling pathogen establishment in human populations [75, 104, 106, 123, 147]. A pronounced example of such evolutionary adaptations is the emergence of zoonoses. In particular, zoonotic diseases are poorly adapted and inefficiently transmitted at first [118], yet they may eventually (through evolutionary adaptations) cross the *species barrier* and start to spread from human to human. In fact, a key event that is thought to have caused the emergence of the 1918 H1N1 pandemic is a *recombination* in the hemagglutinin gene that resulted in a novel virus with increased virulence [79]. Other evolutionary adaptations include genetic changes (e.g., *Salmonella enterica*), recombination or reassortment (e.g., *H5N1 influenza*), and hybridization (e.g., *Phytophthora alni*) [147].

To date, most of the research studies on the evolution of infectious diseases either assume a homogeneous-mixing host population, or focus entirely on the ecological or environmental factors of pathogen evolution. Indeed, the recent advances in *network epidemics* pave the way for exploring new depths and revealing new insights on the delicate interplay between the structural properties of the host contact network and the process of evolution. In what follows, we review the recent progress in creating a modeling framework that captures the spread and evolution of infectious diseases on realistic host contact networks.

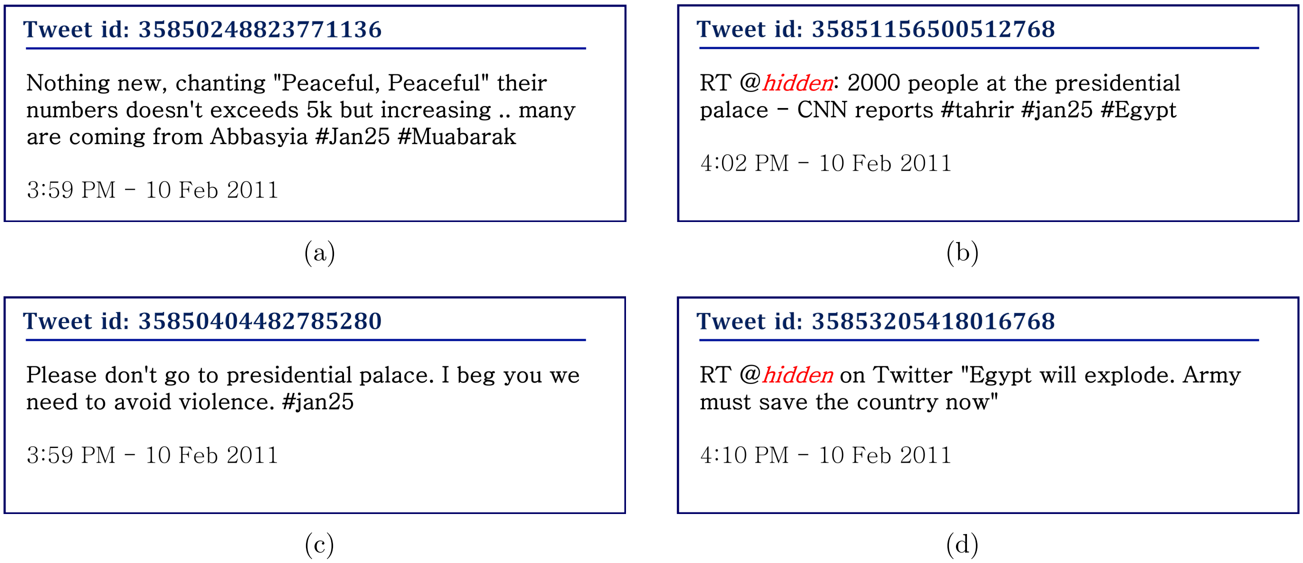
In [3], Alexander and Day proposed a network-based framework that characterizes the spread and evolution of an introduced pathogen on a contact network. Their main objective was to investigate the probability of emergence, and its relation to mutation probabilities, pathogens' transmissibilities, and the structure of the underlying contact network. Using a multi-type branching process [69,99], they derived recursive relations governing the probability of emergence for a given initial strain of the pathogen. The initial strain was assumed to have a poor transmissibility, hence, evolution to a strain with sufficient transmissibility was necessary for emergence. Alexander and Day explored the potential risk factors that could lead to such evolutionary emergence of the pathogen. In particular, they showed that for a given transmissibility, heterogeneity in network structure can significantly increase the risk of emergence. Moreover, certain mutational schemes (e.g., reverse mutation) have limited impact on the probability of emergence, while others (e.g., simultaneous point mutations or recombination) have a dramatic effect on the probability of emergence.

The framework proposed by Alexander and Day in [3] represents a crucial first step towards understanding the role of evolutionary adaptations in driving the emergence of infectious diseases, but it lacks any insights on the expected epidemic size (denoted by S) or, more precisely, the expected fraction of individuals infected by each strain (denoted by S_1 and S_2, respectively). Also, the multi-type branching formalism inherently assumes a tree structure of the underlying graph, hence co-infection (which mainly occurs due to the existence of *cycles*) is essentially ignored in their framework. Finally, the results presented in [3] were neither verified on theoretical, nor real-world contact networks. Our work addresses those limitations by means of i) developing a mathematical theory that characterizes the epidemic threshold, expected epidemic size and the expected fraction of individuals infected by each strain; ii) validating our results (as well as Alexander and Day's results) on theoretical and real-world contact networks; and iii) investigating the case when co-infection is possible.

When the timescale of evolution is much longer than the timescale of propagation, mutations might occur after the original pathogen has invaded the population. In [86], Leventhal et al. considered an SIS process that starts with a pathogen (of single-strain) invading the population. As the disease reaches an endemic equilibrium, a second strain of the disease appears in a random infected individual. Authors assumed that co-infection is not possible, i.e., an infected host carries either strain-1 or strain-2, but not both. Moreover, hosts infected by either strain have perfect immunity against the other strain. Authors investigated the probability that the second strain invades the population and drives the resident strain to extinction, i.e., the *fixation probability*. Results from both theoretical and real-world networks suggested that the heterogeneity in network structure (which facilitated the spread of the resident strain) *lowers* the fixation probability, hence enhancing the resiliency of the resident strain to invasion by new variants.

In contrast to [86], our work considers the case when the epidemiological and evolutionary processes occur on a similar time scale. In particular, each new infection event entails an opportunity for mutation, leading to an entirely different model (with different scope) than the one proposed by Leventhal et al. in [86]. The model considered in our work is reasonable for pathogens with long infectious periods, e.g., HIV, or pathogens with short infectious periods but high mutation rates, large population sizes, and short generation times, e.g., RNA viruses [67]. Furthermore, Leventhal et al. [86] ignore the case where co-infection is possible. However, recent studies revealed the prevalence of multiple-strain co-infection in disease-causing protozoa, bacteria, and viruses [4, 9, 25, 126, 139].

Since humans, animals, plants, and other organisms may become *co-infected* with multiple diseases, a growing body of research has attempted to explore the emergence of this phenomenon and its consequences on complex networks [8, 21, 27, 66]. However, most of the research studies focus on the case where co-infection results from simultaneous exposure to multiple diseases (or pathogen species), rather than multiple-strains of the same pathogen. In [21], Cai et al. considered the case when two diseases are spreading on the same contact network. A susceptible host that has not been exposed to either disease has probability p to get infected by an infective neighbor. Note that the infection probabilities are the same for both diseases. Infected hosts recover after exactly one time step, and gain immunity against the disease that they were infected with, but *not* the other disease. A host that has been infected by one disease (being still active or has already recovered) has a probability q (with $q > p$)



Tweet id: 358502488237711 36

Nothing new, chanting "Peaceful, Peaceful" their numbers doesn't exceeds 5k but increasing .. many are coming from Abbasyia #Jan25 #Muabarak

3:59 PM - 10 Feb 2011

(a)

Tweet id: 358511565005127 68

RT @*hidden*: 2000 people at the presidential palace - CNN reports #tahrir #jan25 #Egypt

4:02 PM - 10 Feb 2011

(b)

Tweet id: 358504044827852 80

Please don't go to presidential palace. I beg you we need to avoid violence. #jan25

3:59 PM - 10 Feb 2011

(c)

Tweet id: 358532054180167 68

RT @*hidden* on Twitter "Egypt will explode. Army must save the country now"

4:10 PM - 10 Feb 2011

(d)

Figure 9.1: **Information mutation on Twitter**. *A collection of four tweets posted within a 10-minute window during the* 2011 *Arab Spring in Cairo, Egypt. The tweets were posted in response to the same underlying event, namely, the marching of protesters towards the presidential palace in order to force the then president, Mubarak, to resign. Information mutation gave rise to several variants with potentially different consequences. Observe that (a) reports peaceful, traditional demonstrations while (d) suggests that the country is on a brink of collapse. User names are hidden for anonymity and tweet ids are given instead.*

to get infected by the other disease, i.e., an infection with one disease weakens the immune system of the infected individual and makes her more susceptible to the second disease. Cai et al. revealed that co-infection dynamics could give rise to a *hybrid* phase transition, where the probability of emergence exhibits a second-order transition, while the fraction of doubly infected nodes exhibits a *first-order* transition.

In Section 9.8, we consider the case where co-infection with multiple strains of the *same* pathogen is possible, giving rise to a different class of epidemiological processes than those considered in [8,21,27,66]. Our model is motivated by the recent research findings that revealed the prevalence of multiple-strain co-infection in disease-causing protozoa, helminths, bacteria, fungi, and viruses [4, 9, 25, 126, 139]. From a modeling standpoint, the key difference between the two processes is that evolution is a *perquisite* for co-infection in our model. In particular, the epidemic process in [21] i) does not entail any mutation events and ii) starts with a *doubly* infected seed, i.e., an infected host that initially carries both diseases. However, our epidemic process starts with a host receiving infection with only one strain of the pathogen, e.g., strain-1, hence the emergence of other strains (which is dictated by the underlying mutational scheme, transmissibility, and network structure) is a perquisite for co-infection. Moreover, our co-infection process differs fundamentally in the way a host becomes co-infected. Unlike the model given in [21], we assume a perfect *cross-immunity*, i.e., a host that has recovered from strain-1 develops immunity against *both* strain-1 and strain-2. Hence, the only pathway for co-infection is when a susceptible host is exposed *simultaneously* to one or more infections of strain-1 and one or more infections of strain-2.

9.3.2 Evolution of information

Evolution and co-infection are two key phenomena of significant relevance to epidemiological processes. However, we are also beginning to observe their emergence and roles in the context of information propagation. We notice on daily basis how news is mutated intentionally, e.g., by adversaries, or unintentionally, e.g., by exaggeration, on social media platforms. A single underlying event could be expressed very differently by different people, creating several variants of information with different implications (see Figure 9.1).

A few research studies have recently explored information evolution on complex networks [1,163]. In [163], Zhang et al. investigated the evolution of rumors on homogeneous and scale-free social networks. In their model, each individual could be in one of three different states, namely, ignorant, spreader, or stifler. These states resemble the susceptible, infected, and recovered states that we have in our model. A fraction F of ignorant individuals are deemed as *forwarders*, i.e., they forward the received rumor to their neighbors without any modifications. The remaining $1 - F$ fraction is deemed as *modifiers*, i.e., they modify the received rumor before forwarding it to their friends. Each modification increments the version number by one. Note that as the process continues to grow, different individuals would receive different versions of the rumor before they turn into stiflers. The main objective of [163] was to determine the average version number of a rumor as a function of time (and degree, for scale-free networks).

Although our work is essentially motivated by the same observation of information evolution in social contexts, our approach and contributions are significantly different from those of [1, 163]. From a modeling perspective, the model presented in [163] is a special case of the multiple-strain model [3] that we utilize in our work. In particular, the model proposed by Zhang et al. essentially assumes that i) $T_i = 1$ for all $i = 1, 2, \ldots$; and ii) the evolutionary pathways are only limited to one-step irreversible mutations. As for the contributions, we focus on the final epidemic size and final fraction of individuals infected by each version of information, in contrast to [163] where authors only focus on the average revision frequency. Another weakness of [163] is that authors made no attempt to provide closed-form expressions for the final epidemic size, the fraction of individuals infected by each version of the rumor, or the average version number of the rumor (only the corresponding differential equations were given). A closed-form expression of the average version number of the rumor at steady state was given only for networks with homogeneous degree distributions.

In [1], Adamic et al. explored the propagation and evolution of memes on Facebook. Authors considered a dataset of Facebook posts which were spread using a copy-and-paste mechanism (prior to the introduction of the *"Share"* functionality in Facebook). The mutation rate of a particular meme was defined as the proportion of copies which introduce new edits as opposed to creating exact replicas. Authors revealed that individuals preferentially transmit a specific variant of a meme that matches their beliefs or culture. Moreover, authors showed that the distribution of variant popularity (the number of copies of that variant posted as Facebook status update) behaves as a power-law distribution for low-mutation rates, yet it deviates from the power-law behavior for high mutation rates. Theoretical predictions based on *Yule* processes [162] (in the limits of very low and very large mutation rates) were shown to have a close resemblance to the empirically observed distributions.

The scope of [1] was limited to one type of propagation, i.e., copy-paste mechanism, and mutations were only characterized by the edit distance [2] between a given variant of the meme

[2] The *edit distance* was defined in [1] as the number of character additions and deletions that must be

and its original version. Indeed, the copy-paste mechanism is no longer sensible in modern social networks where individuals have the option to *"Share"* a post rather than copying and pasting it. In addition, using the edit distance as the sole metric for mutation essentially ignores the *semantic* differences between two different versions of the meme. The theoretical model presented in [1] is technically different than the multiple-strain model [3], yet it resembles a very special case of the latter when i) $T_i = 1$ for all $i = 1, 2, \ldots$; and ii) the evolutionary pathways are only limited to one-step irreversible mutations. Even then, Yule model was considered in [1] only in the limit of very low and very high mutation rates. In contrast to [1], our work attempts to explore information propagation and evolution from a *mathematical modeling* perspective aiming to lay down the foundations for creating a universal model for information propagation and evolution across a wide variety of social media and different possible evolutionary pathways.

9.4 Model definitions

9.4.1 Network model: Random graphs with arbitrary degree distribution

Let $\mathbb{G}$ denote the underlying contact network, defined on the node set $\mathcal{N} = \{1, \ldots, n\}$. We define the structure of $\mathbb{G}$ through its degree distribution $\{p_k\}$. In particular, $\{p_k, k = 0, 1, \ldots\}$ gives the probability that an arbitrary node in $\mathbb{G}$ has degree k. We generate the network $\mathbb{G}$ according to the *configuration model* [18, 100], i.e., the degrees of nodes in $\mathbb{G}$ are all drawn independently from the distribution $\{p_k, k = 0, 1, \ldots\}$. Furthermore, we assume that the degree distribution is well-behaved in the sense that all moments of arbitrary order are finite. Of particular importance in the context of the configuration model is the degree distribution of a randomly chosen neighbor of a randomly chosen vertex, denoted by $\{\hat{p}_k, k = 1, 2, \ldots\}$, and given by

$$\hat{p}_k = \frac{kp_k}{\langle k \rangle}, \quad k = 1, 2, \ldots$$

performed in order to obtain one variant of the meme from another.

where $\langle k \rangle$ denotes the *mean degree*, i.e., $\langle k \rangle = \sum_k k p_k$.

9.4.2 Spreading process model: A multiple-strain model for evolution

In [3], Alexander and Day proposed a *multiple-strain model* that accounts for evolution. Their model is captured by two matrices, namely, the transmissibility matrix $\boldsymbol{T}$ and the mutation matrix $\boldsymbol{\mu}$, both with dimensions $m \times m$ for a finite integer $m \geq 2$ denoting the number of possible strains. The transmissibility matrix $\boldsymbol{T}$ is a $m \times m$ diagonal matrix, with $[T_i]$ representing the transmissibility of strain-i, i.e.,

$$\boldsymbol{T} = \begin{bmatrix} T_1 & 0 & \dots & 0 \\ 0 & T_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & T_m \end{bmatrix}.$$

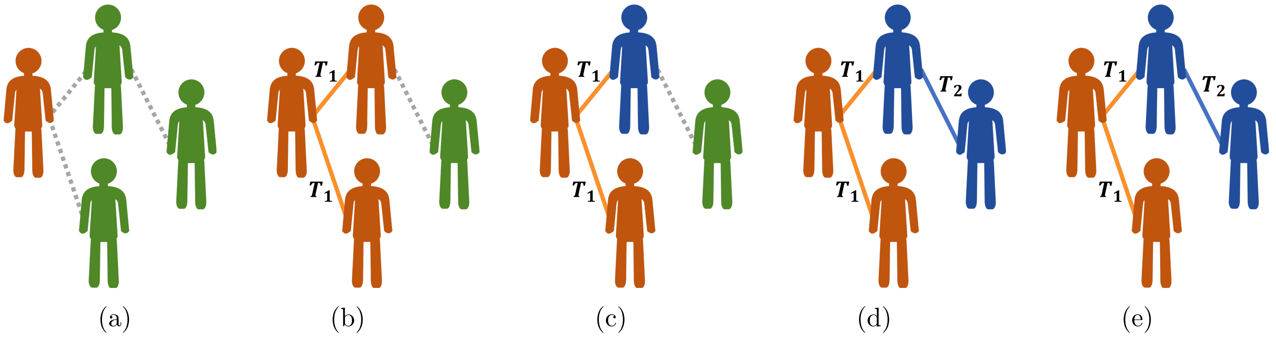
The mutation matrix $\boldsymbol{\mu}$ is a $m \times m$ matrix with μ_{ij} denoting the probability that strain-i mutates to strain-j. Note that $\sum_j \mu_{ij} = 1$, hence $\boldsymbol{\mu}$ is a row-stochastic matrix. One example for the transmissibility and mutation matrices was given by Antia et al. in [7], where the fitness landscape consisted of m strains, with strain-1 through $m-1$ having identical transmissibility such that $R_{0,i} < 1$ for $i = 1, \dots, m-1$, with $R_{0,i}$ denoting the basic reproductive number of strain-i. Strain-m has transmissibility T_m such that $R_{0,m} > 1$, hence the emergence of the pathogen requires evolution from strain-1 to strain-m. Antia et al. considered the the so-called *one-step irreversible mutation* [3,7] where the pathogen must acquire $m-1$ mutations (in order and one at a time) to evolve to strain-m , i.e.,

$$\boldsymbol{T} = \begin{bmatrix} T_1 & 0 & 0 & \dots & 0 \\ 0 & T_1 & 0 & \dots & 0 \\ 0 & 0 & T_1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & T_m \end{bmatrix}$$

and

$$\boldsymbol{\mu} = \begin{bmatrix} 1-\mu & \mu & 0 & \dots & 0 & 0 & 0 \\ 0 & 1-\mu & \mu & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1-\mu & \mu \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{bmatrix}$$

The (inhomogeneous) multiple-strain model proposed by Alexander and Day [3] works as follows. Consider a spreading process that starts with an individual, i.e., the seed, receiving infection with strain-1 from an external reservoir. Since strain-1 has transmissibility T_1, the seed infects each of her contacts independently with probability T_1. Once a susceptible individual receives the infection from the seed, the pathogen may evolve within that new host prior to any subsequent infections. In particular, the pathogen may remain as strain-1 with probability μ_{11} or mutate to strain-i (that has transmissibility T_i) with probability μ_{1i} for $i = 2, \dots, m$. If the pathogen remains as strain-1 (respectively, mutates to strain-i), then the host infects each of her susceptible neighbors in the subsequent stages independently with probability T_1 (respectively, T_i). Observe that as the process continues to grow, multiple strains may coexist in the population as governed by the transmissibility matrix $\boldsymbol{T}$ and the mutation matrix $\boldsymbol{\mu}$. At an intermediate stage, if any susceptible individual receives strain-j, the pathogen may remain as strain-j with probability μ_{jj} or mutate to strain-ℓ with probability $\mu_{j\ell}$ for $\ell \in \{1, 2, \dots, m\} \backslash \{j\}$ prior to subsequent infections. The process terminates when no additional infections are possi-



(a) (b) (c) (d) (e)

Figure 9.2: **The multiple-strain model for evolution**. *(a) The process starts with a single individual, i.e., the seed, receiving infection with strain-*1 *(highlighted in orange) from an external reservoir. (b) The seed infects each of her susceptible neighbors (highlighted in green) independently with probability* T_1*. (c) The pathogen mutates independently within hosts. The pathogen remains as strain-*1 *with probability* μ_{11} *or mutates to strain-*2 *(highlighted in blue) with probability* μ_{12}*. (d) Individuals whose pathogen has mutated to strain-*i *infect their neighbors independently with probability* T_i*. (e) The pathogen mutates independently within hosts. The pathogen remains as strain-*2 *with probability* μ_{22} *or mutates to strain-*1 *with probability* μ_{21}*.*

ble. A graphical illustration for the case when $m = 2$ is given in Figure 9.2. In this chapter, we focus on the case where $m = 2$, however, it is straightforward to extend our theory to handle the general case with m strains. More details are given in Section 9.5.

9.5 Theoretical results

9.5.1 The probability of emergence

The analysis of the probability of emergence was established by Alexander and Day in [3]. Below, we give a brief summary of their results for completeness. Their approach is based on a multi-type branching process [69, 99] that starts with an initial infective of a particular type, e.g., type-1, and then proceeds by infecting each of her neighbors independently with some probability that is characterized by the infecting strain. Each of the infected neighbors mutate independently with a probability that is also characterized by the infecting strain. The process proceeds similarly for subsequent stages. Clearly, the process differs from the standard Single-

Type Branching Process in that individuals of different types may coexist in any generation (other than generation 0), with different offspring distribution per each type, hence the notion Multi-Type [69, 99].

Next, we summarize the results given by Alexander and Day in [3]. Let $\gamma_i\left(s_1, s_2, \ldots, s_m\right)$ be the probability generating function (PGF) for the number of infections of each type transmitted by an *initial* infective of type-i. It holds that

$$\gamma_i\left(s_1, s_2, \ldots, s_m\right) = g\left(1 - T_i + T_i \sum_{j=1}^{m} \mu_{ij} s_j\right),$$

for $i = 1, \ldots, m$ and with $g\left(s\right)$ denoting the PGF of the degree distribution; i.e., $g\left(s\right) = \sum_{k=0}^{\infty} p_k s^k$. Moreover, with $\Gamma_i\left(s_1, s_2, \ldots, s_m\right)$ denoting the PGF for the number of infections of each type transmitted by a *later-generation* infective of type-i (i.e., a typical intermediate host in the process); it holds that

$$\Gamma_i\left(s_1, s_2, \ldots, s_m\right) = G\left(1 - T_i + T_i \sum_{j=1}^{m} \mu_{ij} s_j\right),$$

for $i = 1, \ldots, m$ and with $G\left(s\right)$ denoting the PGF of the *excess degree* distribution; i.e.,

$$G\left(s\right) = \sum_{k=1}^{\infty} \frac{k p_k}{\langle k \rangle} s^{k-1}.$$

We remind that $kp_k/\langle k\rangle$ gives the probability that a randomly chosen neighbor of a randomly chosen vertex has degree k, and note that the excess degree is $k-1$ since one edge is already traversed to reach the node.

The probability of extinction starting from one later-generation infective of type-i, denoted q_i, is the smallest non-negative root of the equation $q_i = \Gamma_i\left(q_1, \ldots, q_m\right)$ solved simultaneously for all $i = 1, \ldots, m$. Finally, the overall extinction probability is given by $g\left(1 - T_i + T_i \sum_{j=1}^{m} \mu_{ij} q_j\right)$ if the whole process starts with an initial infective of type-i. It was shown in [3] that the above process resembles a multi-type branching process with mean matrix [3] given by

$$\boldsymbol{M} = \left(\frac{\langle k^2 \rangle - \langle k \rangle}{\langle k \rangle} \right) \boldsymbol{T\mu} \tag{9.1}$$

The theory of multi-type branching processes states that if the dominant eigenvalue of $\boldsymbol{M}$ is less than or equal to one, then the process goes extinct with probability 1. Otherwise, there is a positive probability of non-extinction. Hence, the phase transition occurs when

$$\rho\left(\boldsymbol{M}\right) > 1, \tag{9.2}$$

where $\rho\left(\boldsymbol{M}\right)$ denotes the *spectral radius*, i.e., the largest eigenvalue (in absolute value) of $\boldsymbol{M}$.

9.5.2 Expected epidemic size and epidemic threshold

Our objective is to derive the expected epidemic size S and the expected fraction of individuals infected by each strain, i.e., $S_1, S_2, \ldots, S_m$ for m possible strains. Note that $S = \sum_{i=1}^{m} S_i$. Below, we provide analysis for the case of two strains, but we later show how to extend our analysis to the general case with m strains, for some finite integer $m \geq 2$. We apply a *tree-based* approach that is based on the work by Gleeson [60, 61]. Their approach draws on the tools developed for analyzing the zero-temperature random-field Ising model on Bethe lattices [133]. Note that as we build our network using the configuration model, the network structure is locally tree-like with the fraction of cycles approaching zero in the limit of large network size [18, 100, 115].

Since $\mathbb{G}$ is locally tree-like, we can replace it by a tree and arrange the vertices in a hierarchical structure, such that at the top level, there is a single node (the *root*) that has degree k with probability p_k. Note that $\{p_k\}$ is a proper degree distribution with $\sum_k p_k = 1$. Each of the k neighbors of the root has degree k' with probability $k' p_{k'} / \langle k \rangle$, where $\langle k \rangle$ denotes the mean degree of the network. Furthermore, we label the levels of the tree from level $\ell = 0$ at

[3] The mean matrix $\boldsymbol{M}$ of a multi-type branching process is defined as $\boldsymbol{M} = [m_{ij}]$, where m_{ij} is the mean number of type-j offspring generated by a type-i parent. Note that $m_{ij} = \left.\frac{\partial \Gamma_i(\boldsymbol{s})}{\partial s_j}\right|_{\boldsymbol{s}=\boldsymbol{1}}$ for the multiple-strain model proposed in [3].

the bottom to level $\ell = \infty$ at the top, i.e., the root.

We assume that nodes update their status starting from the bottom of the tree and proceeding towards the top. This gives rise to a delicate case, where a node at some level ℓ may be exposed to *simultaneous* infections by both strain-1 and strain-2 from her neighbors at level $\ell - 1$. In the remainder of this section, we assume that *co-infection* is not possible, hence a node that receives x infections of strain-1 and y infections of strain-2 becomes infected by strain-1 (respectively, strain-2) with probability $x/(x+y)$ (respectively, $y/(x+y)$). In Section 9.8, we *empirically* consider the case where co-infection is possible, i.e., a node that receives simultaneous infections by both strains becomes co-infected and starts to spread the *co-infection* in the subsequent rounds. In this case, co-infection may be modeled as an additional strain that has transmissibility T_{co} and never mutates back to strain-1 or strain-2.

Throughout, we say that a node is either *inactive* if it has not received any infection (i.e., still susceptible) or *active and type-i* if it has been infected and then *mutated* to strain-i, for $i = 1, 2$. With a slight abuse of notations, let $q_{\ell+1,i}$ be the probability that a node at level $\ell+1$, say node v, is active *and* type-i. Furthermore, let $q_{\ell+1} = q_{\ell+1,1} + q_{\ell+1,2}$, i.e., $q_{\ell+1}$ is the total probability that a node at level $\ell + 1$ is active. We start by an arbitrary initial distribution for $\{q_{0,1}, q_{0,2}\}$ satisfying $q_{0,1} > 0, q_{0,2} > 0$. Then, we update the distribution properly until we reach the root. Note that if the degree of node v is k, then node v is using one edge to connect to her parent at level $\ell + 2$, and $k - 1$ edges to connect to her neighbors at level ℓ. We can condition on the *excess degree* ($\tilde{d}$) of node v to get

$$q_{\ell+1,i} = \sum_{k=1}^{\infty} \frac{kp_k}{\langle k \rangle} \mathbb{P}\left[\text{node } v \text{ becomes active and type-i} \,\middle|\, \tilde{d} = k-1\right]$$

Next, we further condition on the number of *active* neighbors of type-1 and type-2. Note that we have a Multinomial distribution for the number of active neighbors of both types. In particular, a neighbor at level ℓ may be active and type-1 with probability $q_{\ell,1}$, active and type-2 with probability $q_{\ell,2}$, or inactive with probability $1 - q_\ell = 1 - q_{\ell,1} - q_{\ell,2}$. Let I_i denote the number of active neighbors of type-i. Thus,

$$q_{\ell+1,i} = \sum_{k=1}^{\infty} \frac{kp_k}{\langle k \rangle} \sum_{k_1=0}^{k-1} \sum_{k_2=0}^{k-1-k_1} \binom{k-1}{k_1} \binom{k-1-k_1}{k_2} (q_{\ell,1})^{k_1} (q_{\ell,2})^{k_2} (1 - q_{\ell,1} - q_{\ell,2})^{k-1-k_1-k_2}$$
$$\cdot \mathbb{P}\left[\text{node } v \text{ becomes active and type-i} \,\middle|\, I_1 = k_1, I_2 = k_2\right]$$

Let X and Y denote the number of infections received from type-1 and type-2 neighbors, respectively. Note that conditioned on having k_1 and k_2 active neighbors of type-1 and type-2, respectively, we have

$$X \sim \text{Binomial}(k_1, T_1)$$
$$Y \sim \text{Binomial}(k_2, T_2)$$

where T_i denotes the transmissibility of strain-i. Let

$$A := \mathbb{P}\left[\text{node } v \text{ becomes active and type-i} \,\middle|\, I_1 = k_1, I_2 = k_2\right]$$

Consider a particular realization (x, y) of the random variables (X, Y). Observe that if $x > 0, y = 0$, then node v becomes infected by strain-1 and eventually mutates to type-i with probability μ_{1i}. Similarly, if $x = 0, y > 0$, then node v becomes infected by strain-2 and eventually mutates to type-i with probability μ_{2i}. Finally, if $x > 0, y > 0$, then node v becomes infected by strain-1 (respectively, strain-2) with probability $x/(x + y)$ (respectively, $y/(x + y)$) and eventually mutates to type-i with probability μ_{1i} (respectively, μ_{2i}). Hence, by conditioning on X and Y, we have

$$\begin{aligned}
A &= \sum_{x=0}^{k_1}\sum_{y=0}^{k_2}\binom{k_1}{x}\binom{k_2}{y}T_1^xT_2^y(1-T_1)^{k_1-x}(1-T_2)^{k_2-y}\mathbb{P}\left[A \mid X=x, Y=y\right] \\
&= \sum_{x=0}^{k_1}\sum_{y=0}^{k_2}\binom{k_1}{x}\binom{k_2}{y}T_1^xT_2^y(1-T_1)^{k_1-x}(1-T_2)^{k_2-y}\cdot \\
&\quad \cdot\left(\mu_{1i}\mathbf{1}[x>0,y=0]+\mu_{2i}\mathbf{1}[x=0,y>0]+\left(\frac{x\mu_{1i}}{x+y}+\frac{y\mu_{2i}}{x+y}\right)\mathbf{1}[x>0,y>0]\right)
\end{aligned}$$

Note that

$$\begin{aligned}
&\sum_{x=0}^{k_1}\sum_{y=0}^{k_2}\binom{k_1}{x}\binom{k_2}{y}T_1^xT_2^y(1-T_1)^{k_1-x}(1-T_2)^{k_2-y}\cdot\mu_{1i}\mathbf{1}[x>0,y=0] \\
&= \mu_{1i}(1-T_2)^{k_2}\left(1-\mathbb{P}(X=0)\right) \\
&= \mu_{1i}a_2b_1
\end{aligned}$$

where $a_i = (1-T_i)^{k_i}$ and $b_i = 1-a_i$. Similarly,

$$\sum_{x=0}^{k_1}\sum_{y=0}^{k_2}\binom{k_1}{x}\binom{k_2}{y}T_1^xT_2^y(1-T_1)^{k_1-x}(1-T_2)^{k_2-y}\mu_{2i}\mathbf{1}[x=0,y>0] = \mu_{2i}a_1b_2$$

Thus, we have

$$\begin{aligned}
q_{\ell+1,i} = \sum_{k=1}^{\infty}\frac{kp_k}{\langle k\rangle}\sum_{k_1=0}^{k-1}\sum_{k_2=0}^{k-1-k_1}&\binom{k-1}{k_1}\binom{k-1-k_1}{k_2}\left(q_{\ell,1}\right)^{k_1}\left(q_{\ell,2}\right)^{k_2}\left(1-q_{\ell,1}-q_{\ell,2}\right)^{k-1-k_1-k_2}\cdot \\
&\cdot\left(b_1a_2\mu_{1i}+a_1b_2\mu_{2i}+\sum_{x=0}^{k_1}\sum_{y=0}^{k_2}\binom{k_1}{x}\binom{k_2}{y}T_1^xT_2^y(1-T_1)^{k_1-x}(1-T_2)^{k_2-y}\cdot\right. \\
&\quad\left.\cdot\left(\frac{x\mu_{1i}}{x+y}+\frac{y\mu_{2i}}{x+y}\right)\mathbf{1}[x>0,y>0]\right),
\end{aligned} \tag{9.3}$$

for $\ell = 0, 1, \ldots$ and $i = 1, 2$.

Observe that under the assumption that nodes do not become inactive once they turn active, the quantities $q_{\ell,i}$ appearing in (9.3) are non-decreasing in ℓ, and thus they converge to a limit $q_{\infty,i}$ for $i = 1, 2$. Finally, the final fraction of nodes that are active and type-i is equal (in expected value) to the probability that the root of the tree (at level $\ell \to \infty$) is active and type-i. Note that if the tree root has degree k, then all of these k edges will be utilized to connect with her neighbors at the lower level. Hence,

$$\begin{aligned} Q_i = \sum_{k=0}^{\infty} p_k \sum_{k_1=0}^{k} \sum_{k_2=0}^{k-k_1} \binom{k}{k_1} \binom{k-k_1}{k_2} (q_{\infty,1})^{k_1} (q_{\infty,2})^{k_2} (1 - q_{\infty,1} - q_{\infty,2})^{k-k_1-k_2} \cdot \\ \cdot \left(b_1 a_2 \mu_{1i} + a_1 b_2 \mu_{2i} + \sum_{x=0}^{k_1} \sum_{y=0}^{k_2} \binom{k_1}{x} \binom{k_2}{y} T_1^x T_2^y (1 - T_1)^{k_1-x} (1 - T_2)^{k_2-y} \cdot \right. \\ \left. \cdot \left(\frac{x\mu_{1i}}{x+y} + \frac{y\mu_{2i}}{x+y} \right) \mathbf{1}[x > 0, y > 0] \right) \end{aligned} \tag{9.4}$$

where Q_i for $i = 1, 2$ denotes the probability that the tree root is active and type-i and $q_{\infty,i}$ for $i = 1, 2$ is the steady-state solution of the recursive equations (9.3). Note that $Q = Q_1 + Q_2$ is the total probability that the tree root is active.

Observe that $q_{\infty,1} = q_{\infty,2} = 0$ gives a trivial fixed-point of the recursive equations (9.3). Indeed, this trivial solution leads to $Q = 0$ by virtue of (9.4). Although the trivial fixed point is a valid numerical solution for the recursive equations (9.3), we can show that this trivial solution is *unstable*. Hence, another solution with $q_{\infty,1} > 0$ and $q_{\infty,2} > 0$ may exist. To test whether or not the trivial fixed point is stable, we check the spectral radius of the Jacobian matrix $\boldsymbol{J}(q_{\ell,1}, q_{\ell,2})$ corresponding to the *linearization* of (9.3) at $q_{\ell,1} = q_{\ell,2} = 0$. If the spectral radius of the $\boldsymbol{J}(q_{\ell,1}, q_{\ell,2})$ at $q_{\ell,1} = q_{\ell,2} = 0$ is larger than one, then the trivial fixed-point is unstable, indicating that there exists another solution with $q_{\infty,1} > 0$ and $q_{\infty,2} > 0$ implying the existence of a giant component. The Jacobian matrix is given by

$$\begin{aligned}
\boldsymbol{J}(q_{\ell,1}, q_{\ell,2})|_{q_{\ell,1}=q_{\ell,2}=0} &= \begin{bmatrix} \frac{\partial q_{\ell+1,1}}{\partial q_{\ell,1}} & \frac{\partial q_{\ell+1,1}}{\partial q_{\ell,2}} \\ \frac{\partial q_{\ell+1,2}}{\partial q_{\ell,1}} & \frac{\partial q_{\ell+1,2}}{\partial q_{\ell,2}} \end{bmatrix}_{q_{\ell,1}=q_{\ell,2}=0} \\
&= \left(\frac{\langle k^2\rangle - \langle k\rangle}{\langle k\rangle}\right) \begin{bmatrix} T_1\mu_{11} & T_2\mu_{21} \\ T_1\mu_{12} & T_2\mu_{22} \end{bmatrix} \\
&= \left(\frac{\langle k^2\rangle - \langle k\rangle}{\langle k\rangle}\right) (\boldsymbol{T\mu})^T
\end{aligned}$$

Note that a square matrix and its transpose have the same set of eigenvalues. Hence, the phase transition condition matches the one given in (9.2).

We remark that it is straightforward to extend our analysis to the general case with m strains, for some finite integer $m \geq 2$ as long as the underlying process is *indecomposable* [3, 69, 99]. At a high level, indecomposable processes are those for which each pathogen strain i eventually gives rise to strain-j at some generation $n_{ij} \geq 1$ for $i, j = 1, 2, \ldots, m$. In other words, if an indecomposable process starts with an infection with strain-i, then as the process continues to grow, all other strains will eventually emerge. Such a property is established if, for every pair of strains (i, j), there exists a positive integer n_{ij} such that $\boldsymbol{M}^{n_{ij}}(i, j) > 0$ [3]. If the underlying process is *decomposable*, then there exist classes of strain types such that strain types belonging to the same class can eventually give rise to one another, but not to other strain types. Indeed, the existence of multiple classes leads to multiple solutions for the set of equations (9.4) depending on the initial distribution of $\{q_{0,1}, q_{0,2}, \ldots, q_{0,m}\}$. Hence, to guarantee the uniqueness of the solution of (9.4) and for mathematical tractability, we limit our formalism to the case when the underlying process is indecomposable.

9.6 Numerical results

9.6.1 The structure of the contact network

In this section, we consider synthetic contact networks generated randomly by the configuration model, while real-world networks are considered in Section 9.7. In particular, we consider contact networks with *Poisson* degree distribution as well as *Power-law* degree distribution.

Poisson degree distribution

We start by considering contact networks with Poisson degree distribution. Namely, with λ denoting the mean degree, i.e., $\lambda = \langle k \rangle$, we have

$$p_k = e^{-\lambda} \frac{\lambda^k}{k!}, \qquad k = 0, 1, \ldots$$

In this case, condition (9.2) implies that phase transition occurs when

$$\lambda \times \rho\left(\boldsymbol{T}\boldsymbol{\mu}\right) = 1 \tag{9.5}$$

where $\rho\left(\boldsymbol{T}\boldsymbol{\mu}\right)$ denotes the spectral radius of the matrix multiplication $\boldsymbol{T}\boldsymbol{\mu}$. Observe that condition (9.5) embodies the structure of the contact network (represented by λ for a contact network with Poisson degree distribution), the characteristics of propagation (represented by the matrix $\boldsymbol{T}$) and the process of evolution (represented by $\boldsymbol{\mu}$), hence it unravels how these properties interact together to yield an epidemic.

Power-law degree distribution

Poisson degree distribution provides a formalism for *homogeneous* networks, where the degree sequence of the graph is highly concentrated around the mean degree. However, degree sequences in real-world networks were observed to be heavily skewed to the right [12, 103, 111], meaning that the distribution is *heterogeneous*, or heavy-tailed. We consider Power-law degree distribution with exponential cutoff since they are relevant to a variety of real-world networks [82, 111]. In particular, we set

$$p_k = \begin{cases} 0 & \text{if } k = 0 \\ \left(\mathrm{Li}_\gamma\left(e^{-1/\Gamma}\right)\right)^{-1} k^{-\gamma} e^{-k/\Gamma} & \text{if } k = 1, 2, \ldots . \end{cases}$$

where γ and Γ are positive constants and $\mathrm{Li}_m(z)$ is the mth polylogarithm of z, i.e., $\mathrm{Li}_m(z) = \sum_{k=1}^{\infty} \frac{z^k}{k^m}$. Observe that condition (9.2) now translates to

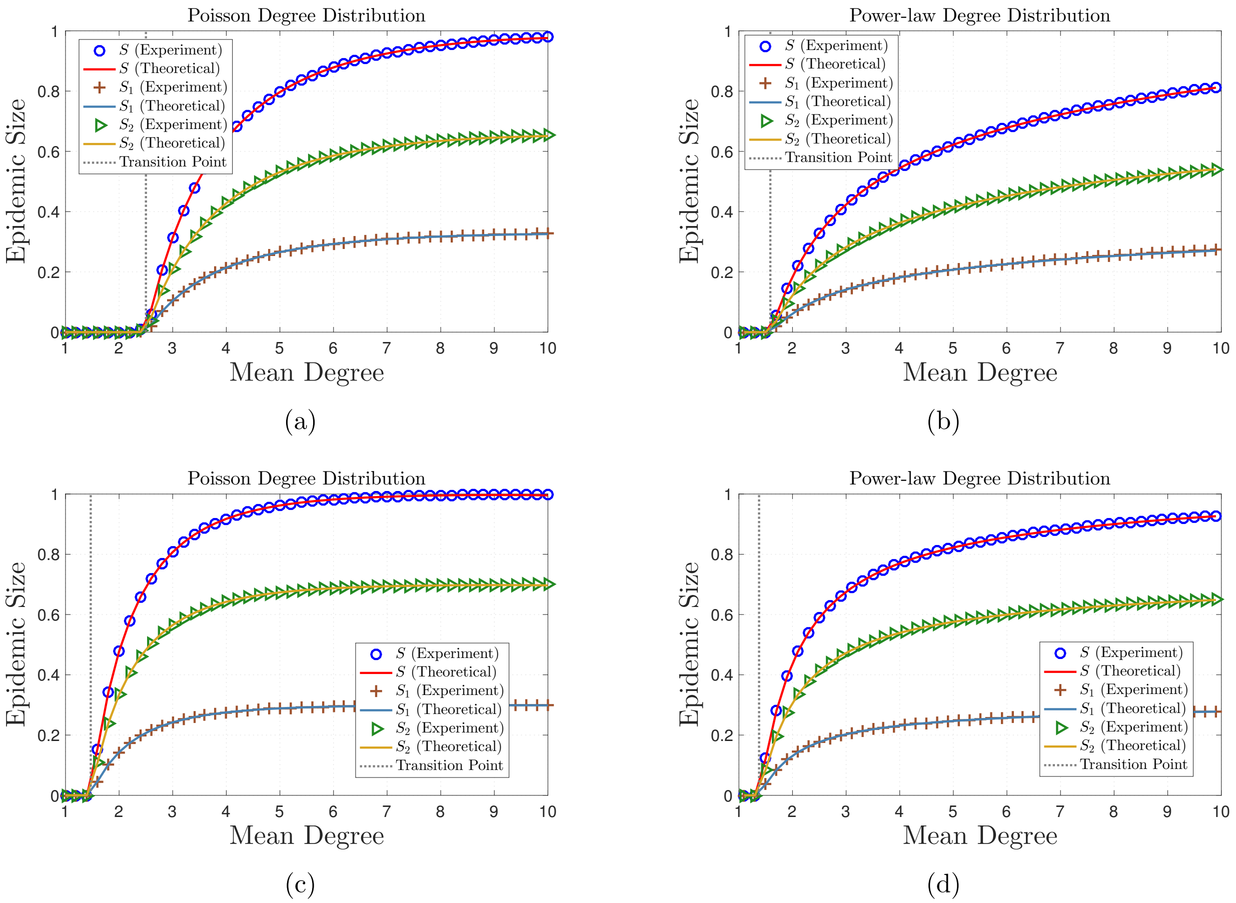
$$\left(\frac{\mathrm{Li}_{\gamma-2}\left(e^{-1/\Gamma}\right) - \mathrm{Li}_{\gamma-1}\left(e^{-1/\Gamma}\right)}{\mathrm{Li}_{\gamma-1}\left(e^{-1/\Gamma}\right)} \right) \times \rho\left(\boldsymbol{T\mu}\right) = 1 \tag{9.6}$$

Similar to (9.5), condition (9.6) indicates how the structure of the underlying network, the characteristics of propagation, and the process of evolution are intertwined together, and under what conditions their relationship would induce an epidemic.

9.6.2 Notations and methods

Notations: In what follows, we use S, S_1 and S_2 to denote the *total* expected epidemic size, the expected fraction of nodes infected with strain-1, and the expected fraction of nodes infected with strain-2, respectively and all at the steady state, i.e., when the process terminates. We use P_1^{BP} and P_2^{BP} to denote the probability of emergence on a single-strain bond-percolated network with T_1 and the probability of emergence on a single-strain bond-percolated network with T_2, respectively.

Methods: We use the configuration model to create random random graphs with particular degree distributions. In particular, we sample a degree sequence from the corresponding distribution, then we use the configuration model to construct a random graph with that degree sequence. We use igraph [26] on both C++ and Python for simulations. Our simulation codes



(a)

(b)

(c)

(d)

Figure 9.3: **Evolution on Poisson and Power-law contact networks**. *The network size n is 2×10^5 and the number of independent experiments for each data point is* 500. *Blue circles, brown plus signs, and green triangles denote the empirical average epidemic size, average fraction of nodes infected with strain-*1*, and average fraction of nodes infected with strain-*2*, respectively. The red, blue, and yellow lines denote the theoretical average total epidemic size, average fraction of nodes infected with strain-*1*, and average fraction of nodes infected with strain-*2*, respectively. Theoretical results are obtained by solving the system of equations (9.4) with the corresponding parameter set. (a)-(b) We set $T_1 = 0.2$, $T_2 = 0.5$, $\mu_{11} = \mu_{22} = 0.75$. (c)-(d) We set $T_1 = 0.4$, $T_2 = 0.8$, and $\mu_{11} = 0.3$, and $\mu_{22} = 0.7$ implying that an infected node, regardless of what type of infection it has, mutates to strain-*1 *(respectively, strain-*2*) with probability* 0.3 *(respectively,* 0.7*), independently. In all cases, we observe good agreement with our theoretical results.*

.

are available online [4]. Unless otherwise stated, we start the process by selecting a node uniformly at random and infecting it with strain-1. The node infects each neighbor independently with probability T_1. Each of the infected neighbors mutate independently to strain-1 with prob-

[4] https://github.com/reletreby/evolution.git

ability μ_{11}, or to strain-2 with probability μ_{12}. As the process continues to grow, both strains might exist in the population. An intermediate node that becomes infected with strain-i would mutate to strain-1 with probability μ_{i1}, or strain-2 with probability μ_{i2}, for $i = 1, 2$. When cycles start to appear, a susceptible node could be exposed to multiple infections at once. If a node is exposed to x infections of strain-1 and y infections of strain-2 simultaneously, the node becomes infected with strain-1 (respectively, strain-2) with probability $x/(x+y)$ (respectively, $y/(x+y)$) for any non-negative constants x and y. A node that receives infection at round i mutate first (by the end of round i) before it attempts to infect her neighbors at round $i+1$. The node is considered *recovered* at round $i+2$, i.e., a node is infective for only one round.

9.6.3 Epidemic size

We start by focusing on the total epidemic size and the expected fraction of nodes that were infected with strain-1 and strain-2. The network size n is set to 2×10^5. We consider two parameter sets that emphasize the correlations between a node's eventual type (after mutation) and the type of infection it has originally received. In particular, we have

- **Parameter set 1:** $T_1 = 0.2$, $T_2 = 0.5$, $\mu_{11} = 0.75$, and $\mu_{22} = 0.75$.
- **Parameter set 2:** $T_1 = 0.4$, $T_2 = 0.8$, $\mu_{11} = 0.3$, and $\mu_{22} = 0.7$.

Observe that we have $\mu_{11} = \mu_{21}$ and $\mu_{22} = \mu_{12}$ for the second parameter set. Hence, an infected node, regardless of what type of infection it has, mutates to strain-1 (respectively, strain-2) with probability 0.3 (respectively, 0.7), independently. This is a special case that can easily be treated by our formalism given in Section 9.5.

In Figure 9.3a and Figure 9.3b, we use the first parameter set and run 500 independent experiments for each data point. We demonstrate our results on contact networks with Poisson degree distribution (Figure 9.3a) and Power-law degree distribution with exponential cutoff (Figure 9.3b). For Figure 9.3b, we set $\Gamma = 15$, and vary γ with the mean degree. In particular, the mean degree λ is given by

$$\lambda = \frac{\mathrm{Li}_{\gamma-1}\left(e^{-1/\Gamma}\right)}{\mathrm{Li}_{\gamma}\left(e^{-1/\Gamma}\right)}. \tag{9.7}$$

Hence, we can numerically solve (9.7) to obtain the particular value of γ corresponding to a given value of λ.

In order to establish the validity of our analytic results given in Section 9.5, we plot the theoretical values of S, S_1, and S_2 obtained by solving the system of equations (9.4) with the corresponding parameter set. We also plot a vertical line at the critical mean degree that corresponds to a phase transition (see (9.5) and (9.6)). Clearly, our experimental results are in perfect agreement with our theoretical results on both contact networks. In Figure 9.3c and Figure 9.3d, we repeat the same procedure, but with the second parameter set. Similarly, we observe perfect agreement with our theoretical results on both contact networks.

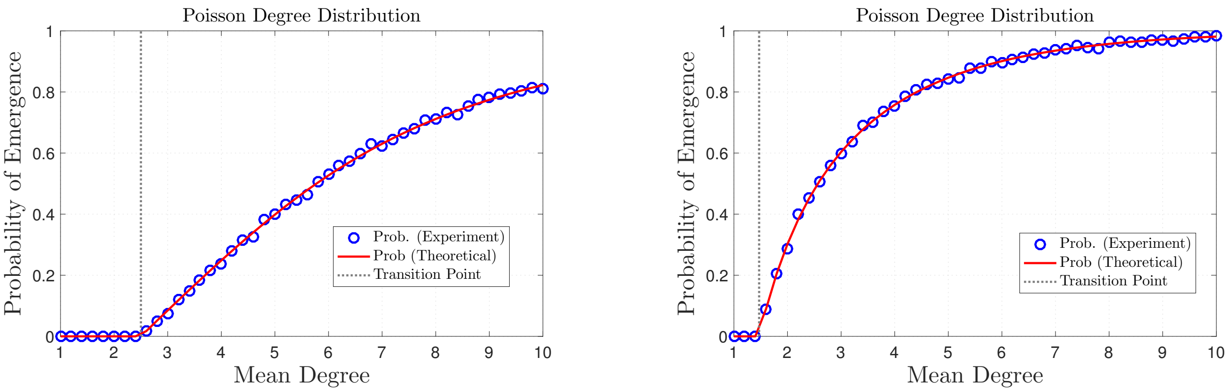
9.6.4 Probability of emergence

In [3], Alexander and Day investigated the probability of emergence for the multiple strain model presented in Section 9.4. However, authors did not provide a comprehensive simulation study to validate their formalism on random or real-world networks. Instead, in [3, Section 3], authors only evaluated their equations *numerically.* In this subsection, we aim to establish the validity of the results presented in [3] on random networks generated by the configuration model. For brevity, we limit our scope to contact networks with Poisson degree distribution. However, similar patterns are observed for contact networks with Power-law degree distribution.

In Figure 9.4, we set the network size $n = 5 \times 10^5$ and run a computer simulation with 10^4 independent experiment for each data point. We use the two parameter sets given in Section 9.5.C. Namely, we set

- $T_1 = 0.2$, $T_2 = 0.5$, and $\mu_{11} = \mu_{22} = 0.75$ for Figure 9.4.a, and

- $T_1 = 0.4$, $T_2 = 0.8$, $\mu_{11} = 0.3$ and $\mu_{22} = 0.7$ for Figure 9.4.b.



(a) (b)

Figure 9.4: **The probability of emergence on contact networks with Poisson degree distribution**. *The network size n is 5×10^5 and the number of independent experiments for data point is 10^4. Blue circles denote the empirical probability of emergence while the red line denotes the theoretical probability of emergence according to [3]. (a) We set $T_1 = 0.2$, $T_2 = 0.5$, $\mu_{11} = \mu_{22} = 0.75$. (b) We set $T_1 = 0.4$, $T_2 = 0.8$, and $\mu_{11} = 0.3$, and $\mu_{22} = 0.7$. Our experimental results prove the validity of the formalism presented by Alexander and Day in [3]*

.

Note that in Figure 9.4, we plot the probability of emergence conditioned on the initial node receiving infection with strain-1 [5]. We observe an agreement between our experimental results and the theoretical results given in [3]. The reasoning behind this is intuitive; the multi-type branching framework assumes that the underlying graph is tree-like, an assumption that works best for networks with vanishingly small clustering coefficient, e.g., networks which are generated by the configuration model.

9.6.5 Reduction to single-type bond-percolation

An important question to ask is whether the classical single-type bond percolation models could predict the threshold, probability, and final size of epidemics that entail *evolution*, i.e., information or diseases that propagate according to the multiple-strain model given in Section 9.4. In pursing an answer to this question, we start by establishing a *matching condition* between single-strain models and multiple-strain models for epidemics.

[5] We remark that the formalism provided by Alexander and Day allows for computing the probability of emergence given any arbitrary initial type.

In [111], Newman proposed a stochastic SIR model for the propagation of a single-strain pathogen on a contact network. Newman showed that, under some conditions, the SIR model is isomorphic to a bond-percolation model on the underlying contact network. Specifically, with the *average transmissibility* of the pathogen (denoted T_{BP}) as the bond-percolation parameter, if we are to occupy each edge of the network with probability T_{BP}, then the probability of emergence as well as the final size of the epidemic are precisely given by the fraction of nodes in the giant component of the *percolated* graph. Finally, it was shown that a phase transition occurs when

$$\left(\frac{\langle k^2\rangle - \langle k\rangle}{\langle k\rangle}\right) T_{\text{BP}} = 1 \tag{9.8}$$

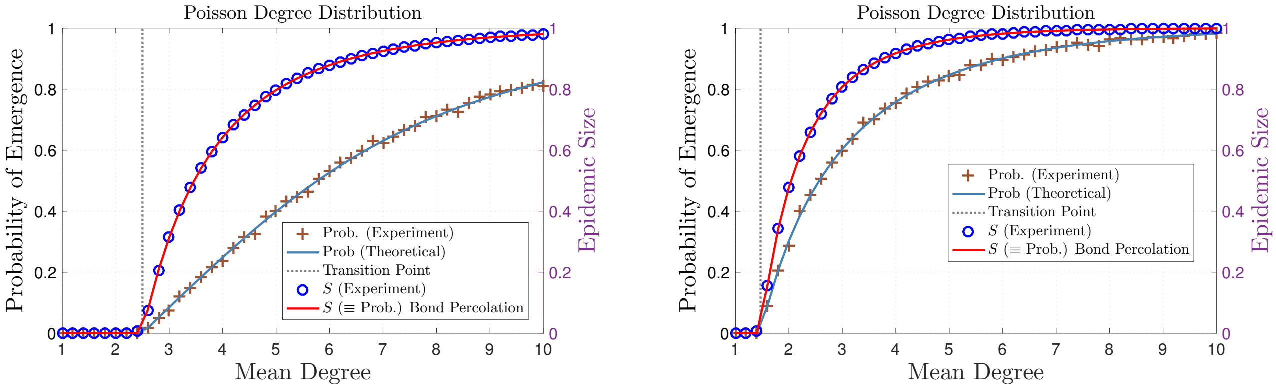
In other words, if the left hand side of (9.8) is strictly larger than 1, a giant component emerges indicating an epidemic. Otherwise, we have self-limited outbreaks.

Comparing (9.2) to (9.8) suggests the proposal of a matching that results in the same condition for phase transition. More precisely, if we are to set

$$T_{\text{BP}} = \rho\left(\boldsymbol{T\mu}\right) \tag{9.9}$$

then, both (9.2) and (9.8) collapse to the same condition for a given contact network. In what follows, we explore the extent to which classical, single-type bond-percolation models (under the matching condition (9.9)) may predict the threshold, probability, and final size of epidemics that entail evolution, i.e., information or diseases that propagate according to the multiple-strain model given in Section 9.4. We focus on contact networks with Poisson degree distribution, generated by the configuration model, while we devote Section 9.7 for real-world networks.

In Figure 9.5, we extend Figure 9.4 by further adding the experimental results for the final epidemic size as well as the corresponding theoretical values for the probability of emergence on a bond-percolated network under the matching condition (9.9). Note that the probability of emergence is equivalent to the final epidemic size for single-type, bond-percolated networks



(a) (b)

Figure 9.5: **Reduction to single-type bond-percolation**. *The network size n is 5×10^5 and the number of independent experiments for each data point is 10^4. Blue circles and brown plus signs denote the empirical average epidemic size and the probability of emergence, respectively. The navy blue line denotes the theoretical probability of emergence according to [3] while the red line denotes the theoretical average epidemic size (as well as the probability of emergence) predicted by the single-type bond-percolation framework under the matching condition (9.9). (a) We set $T_1 = 0.2$, $T_2 = 0.5$, $\mu_{11} = \mu_{22} = 0.75$. (b) We set $T_1 = 0.4$, $T_2 = 0.8$, and $\mu_{11} = 0.3$, and $\mu_{22} = 0.7$. The classical, single-type bond percolation models may accurately predict the threshold and final size of epidemics, but their predictions on the probability of emergence are clearly inaccurate.*

[111]. Observe that the classical single-type bond-percolation model accurately captures the threshold and final size of epidemic but provides significantly inaccurate predictions when it comes to the probability of emergence. Similar pattern will be observed in Section 9.7 for real-world networks. This inaccuracy sheds the light on a fundamental disconnect between the classical, single-type bond-percolation models and real-life spreading processes that entail evolution. We explain the intuition behind our findings in Section 9.9

9.6.6 Effect of heterogeneity

The results given in Figure 9.5 reveal the significant shortcomings of the bond-percolation model in predicting the probability of emergence for spreading processes governed by the multiple-strain model, but also shed the light on the effect of the embedded heterogeneity of the multiple-strain framework. Observe that a single-type spreading process with $T_{\text{BP}} = \rho\left(\boldsymbol{T}\boldsymbol{\mu}\right)$

is much more likely to cause an epidemic outbreak, i.e., has a higher probability of emergence, as compared to an inhomogeneous spreading process governed by the multiple-strain model, when the initial infective is type-1. The above reasoning implies that one is better off (in terms of maximizing the probability of emergence) allocating $\rho\left(\boldsymbol{T}\boldsymbol{\mu}\right)$ to a single-type spreading process than to allocate $\boldsymbol{T}$ and $\boldsymbol{\mu}$ to an *inhomogeneous* spreading process that starts with the strain that has the lowest transmissibility.

9.6.7 Effect of mutation

When only a single evolutionary pathway is available, mutations have to occur in a particular order [63]. In [7], Antia et al. considered the case where the fitness landscape consists of m strains such that $R_{0,i} < 1$ for $i = 1, \ldots, m-1$, while $R_{0,m} > 1$. Hence, an introduced pathogen (with $R_{0,1} < 1$) must acquire $m - 1$ successive mutations in order for the disease to emerge. Antia et al. derived a set of recursive equations whose solution characterizes the probability of emergence under some conditions; see [7] for more details. To gain further insights on the effect of mutation, Antia et al. proposed a theoretical approximation of the probability of emergence as a product of the probability of mutation, i.e., the probability that the introduced pathogen would eventually mutate to strain-m, and the probability of emergence of strain-m. Indeed, the probability of mutation plays a key role in the overall extinction probability. After all, if the introduced pathogen does not gain $m - 1$ successive mutations, the disease would eventually die out.

Recall that the mathematical theory developed by Alexander and Day [3] defines the probability of emergence as a function of the evolutionary dynamics of the pathogen (i.e., the mutation matrix $\boldsymbol{\mu}$), the characteristics of the spreading process (i.e., the transmissibility matrix $\boldsymbol{T}$), and the structure of the underlying contact network (i.e., the degree distribution $\{p_k, \quad k = 0, 1, \ldots\}$). All of these factors are intertwined together in a way that makes it difficult to predict how the probability of mutation influences the probability of emergence. In what follows, we provide a theoretical approximation to the probability of emergence in a way that clearly distinguishes the role of mutation and shows how it strongly influences the probability of emergence.

Consider the case when the fitness landscape consists of two strains with transmissibility matrix $\boldsymbol{T}$ and mutation matrix $\boldsymbol{\mu}$ given by

$$\boldsymbol{T} = \begin{bmatrix} T_1 & 0 \\ 0 & T_2 \end{bmatrix} \quad \text{and} \quad \boldsymbol{\mu} = \begin{bmatrix} 1-\mu & \mu \\ 0 & 1 \end{bmatrix}.$$

Assume also that $T_1 < T_2$. Note that the process starts by picking a random individual uniformly at random and infecting her with strain-1. Fix the mean degree of the underlying network to λ. Let λ_1 and λ_2 denote the phase transition points (i.e., critical mean degrees) for a single-strain, bond-percolated network with T_1 and T_2, respectively. Observe that $\rho\left(\boldsymbol{T\mu}\right) = T_2$, hence, in view of (9.2), the phase transition is entirely controlled by the parameters of strain-2, i.e., the phase transition occurs at λ_2. Indeed, we can conclude from (9.2) that for $\lambda < \lambda_2$, the probability of emergence is zero (in the limit of large network size). We can write

$$\begin{aligned} &\mathbb{P}\left[\text{emergence}\right] \qquad (9.10) \\ &= \mathbb{P}\left[\text{emergence} \,\middle|\, \text{at least one mutation}\right] \times P_\mu + \mathbb{P}\left[\text{emergence} \,\middle|\, \text{no mutation}\right] \times (1 - P_\mu) \end{aligned}$$

where P_μ denotes the probability that at some point along the chain of infections (starting from the type-1 seed), a node would be infected by strain-1, but then mutate to strain-2. In other words, P_μ captures the probability that at some point during the propagation, a type-2 node would emerge.

Observe that for $\lambda < \lambda_1$, we have $\mathbb{P}\left[\text{emergence} \,\middle|\, \text{no mutation}\right] = 0$ in the limit of large network size (since $P_1^{\text{BP}} = 0$ on this interval), while for $\lambda \geq \lambda_1$, we have $P_\mu = 1$ in the limit of large network size [6]. Hence, the second term in (9.10) is always zero in the limit of large

[6] When $\lambda \geq \lambda_1$, a giant component of type-1 nodes emerges. Now, since $\mu > 0$, and the number of nodes in the giant component tends to infinity in the limit of large network size, the probability that none of the nodes mutate to strain-2 is zero.

network size, leading to

$$\mathbb{P}\left[\text{emergence}\right] = \mathbb{P}\left[\text{emergence} \,\middle|\, \text{at least one mutation}\right] \times P_\mu$$

Note that on the range $\lambda_2 \leq \lambda < \lambda_1$, we have $\mathbb{P}\left[\text{emergence} \,\middle|\, \text{at least one mutation}\right] = P_2^{\text{BP}}$. However, on the range $\lambda \geq \lambda_1$, strain-1 nodes are able to form a giant component on their own. Hence, in the cases where a strain-2 node emerges at some point, but fails to infect any of her neighbors, strain-1 nodes could still trigger the emergence of the disease. It follows that $\mathbb{P}\left[\text{emergence} \,\middle|\, \text{at least one mutation}\right] \geq P_2^{\text{BP}}$ on the range $\lambda \geq \lambda_2$. Note that the bound is tight whenever T_2 is significantly larger than T_1. The reasoning behind this can be explained as follows. Whenever T_2 is significantly larger than T_1, the average number of secondary infections of strain-2 would be much larger than that of strain-1. Hence, infections with strain-2 would propagate much faster and block potential pathways for strain-1 to propagate. In this case, the overall probability of emergence becomes tightly controlled by P_2^{BP}. Next, we turn our attention to deriving P_μ.

Consider a tree of infections that starts with a single node infected with strain-1. Let H be the probability that strain-2 never appears throughout the tree, i.e., H is the probability that the tree of infections starting from the seed does not give rise to strain-2 at any intermediate point. Similarly, let h be the probability that a *subtree* of infections starting from a type-1 host does not give rise to strain-2 at any intermediate point. Recall that $G(.)$ gives the PGF of the excess degree distribution while $g(.)$ gives the PGF of the degree distribution. By conditioning on the *excess* degree as well the number of secondary infections, we get

$$\begin{aligned} h &= \sum_{k=1}^{\infty} \frac{kp_k}{\langle k \rangle} \sum_{x=0}^{k-1} \binom{k-1}{x} \left(T_1 \left(1-\mu\right)\right)^x \left(1-T_1\right)^{k-1-x} h^x \\ &= \sum_{k=1}^{\infty} \frac{kp_k}{\langle k \rangle} \left(1 - T_1 + T_1 \left(1-\mu\right) h\right)^{k-1} \\ &= G\left(1 - T_1 + T_1 \left(1-\mu\right) h\right) \end{aligned} \qquad (9.11)$$

The validity of (9.11) can be explained as follows. Note that the root of any subtree, say node v, has already used an edge to receive an infection with strain-1 from her parent. Hence, if the degree of node v is k, then node v is only using $k-1$ edges to infect her offspring, leading us to use the excess degree distribution. Furthermore, conditioned on the excess degree being $k-1$, the number of secondary infections of each type generated by node v is given by a multinomial distribution characterized by $(k-1, T_1(1-\mu), T_1\mu, 1-T_1)$. In particular, conditioned on node v being type-1 and having an excess degree of $k-1$, the probability of generating x infections of type-1 and y infections of type-2 is given by

$$\binom{k-1}{x}\binom{k-1-x}{y}\left(T_1\left(1-\mu\right)\right)^x\left(T_1\mu\right)^y\left(1-T_1\right)^{k-1-x-y}$$

However, the only relevant term for the computation of h is the one with $y=0$, as all other terms with $y>0$ are contributing with a zero probability to h by definition. Finally, h^x denotes the probability that the subtrees emanating from the current x offspring are themselves free of any strain-2 node.

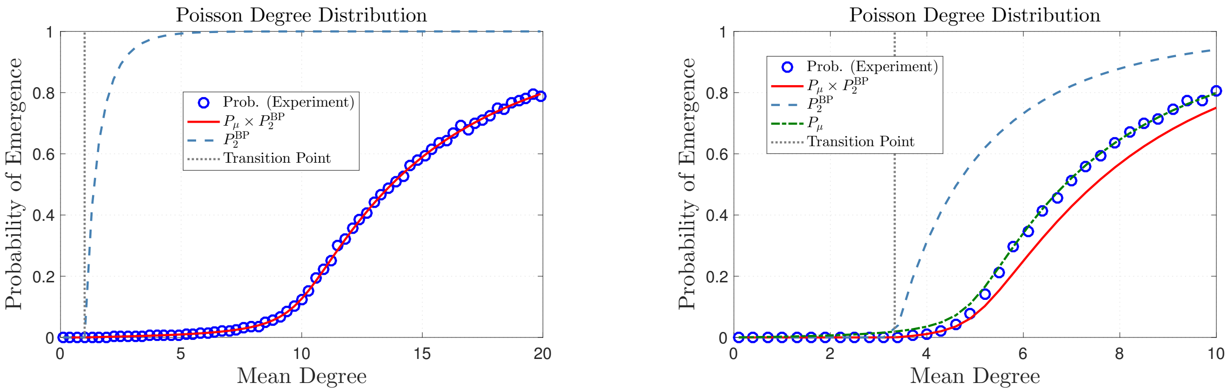
Recall that H denotes the probability that strain-2 never appears throughout the tree (starting from the root) and note that if the tree root has degree k, then all of these k edges will be utilized to connect with her neighbors at the lower level. Hence, in view of (9.11), we can write

$$H = g\left(1-T_1+T_1\left(1-\mu\right)h_\infty\right)$$

where h_∞ denotes the steady-state solution of (9.11). It is now immediate that $P_\mu = 1-H$, leading to

$$\mathbb{P}\left[\text{emergence}\right] \geq \left(1-H\right)P_2^{\text{BP}} \tag{9.12}$$

To confirm the validity of (9.12), we run a computer simulation on random networks generated by the configuration model with Poisson degree distribution. In Figure 9.6, we set the network size $n = 2\times10^5$ and perform 10^4 independent experiments for each data point. In Figure 9.6a, we set $T_1 = 0.1$, $T_2 = 1$, and $\mu = 0.01$. Observe that the bound given by (9.12) is



(a)

(b)

Figure 9.6: **Approximating the probability of emergence:** *The network size n is 2×10^5 and the number of independent experiments for each data point is 10^4. Blue circles denote the empirical probability of emergence while the red line denotes the theoretical approximation of the probability of emergence according to (9.12). The light blue dashed line denotes the probability of emergence for a single-strain, bond-percolated network with T_2. (a) We set $T_1 = 0.1$, $T_2 = 1$, and $\mu = 0.01$. (b) We set $T_1 = 0.2$, $T_2 = 0.3$, and $\mu = 0.01$. We observe good agreement between the experimental results and the theoretical approximation given by (9.12) whenever $\lambda_2 \leq \lambda < \lambda_1$ or whenever T_2 is significantly larger than T_1.*

tight, as T_2 is significantly larger than T_1. In general, we would expect a tight bound whenever $\lambda_2 \leq \lambda < \lambda_1$, where λ_1 and λ_2 denote the phase transition points (i.e., critical mean degrees) for a single-strain, bond-percolated network with T_1 and T_2, respectively, i.e., $1 \leq \lambda < 10$ for the given parameter set. As λ increases beyond λ_1, the tightness of the bound depends on the ratio between T_2 to T_1. This is illustrated in Figure 9.6b for the case when $T_1 = 0.2$ and $T_2 = 0.3$.

The availability of an explicit expression for the probability of mutation allows for exploring the effects of mutation on the overall probability of emergence. Indeed, the way the probability of emergence behaves with respect to changes in the mean degree resembles, to a great extent, the way P_μ behaves, as illustrated in Figure 9.6. Hence, in what follows, we focus on the behavior of P_μ with respect to changes in the mean degree. In Figure 9.7, we set $T_1 = 0.1$ and plot P_μ against the mean degree for a network with Poisson degree distribution. We observe that different values for μ impacts the shape of P_μ (hence, the probability of emergence) in a remarkable way. Firstly, for all values of $\mu \in (0, 1)$, the behavior of P_μ appears to be strikingly different than the universality class of percolation models, e.g., see the shape of the probability of emergence (respectively, P_2^{B}) in Figure 9.4 (respectively, Figure 9.6). Secondly, the effect of mutation probabilities on P_μ appears to be significant as the mean degree increases from small values, reaches its peak right before the critical mean degree corresponding to P_1^{BP}, then decays as the mean degree increases further.

The reasoning behind the aforementioned observation is intuitive. Recall that the process starts with a single infection with strain-1 and note that P_μ is influenced by the structure of the underlying contact network, the transmissibility of strain-1, and the particular value of μ. As the mean degree λ increases towards λ_1, the length of the tree of infections starting from the seed [7] also increases, however, no cycles appear and the epidemic propagates on a finite, tree-like percolated network (since $\lambda < \lambda_1$). Increasing the length of the tree increases the probability that at least one intermediate node would mutate to strain-2, but the fact that the tree is finite makes the particular value of μ very crucial to P_μ. Namely, a small value of μ makes it less likely that a mutant emerges before the chain of infections is terminated, while a relatively larger value could drive the emergence of strain-2 and lead the epidemic to escape extinction. Put differently, the finiteness of the chain of infections when $\lambda < \lambda_1$ creates a limited number of opportunities for mutation, causing the particular value of μ to *bear the burden* of generating a mutant and driving the whole process to emergence. However, as λ increases beyond λ_1, cycles start to appear and a giant component of nodes infected with strain-1 emerges. In this case, the chain of infections is no longer finite, and any positive value of μ results in a mutation almost surely in the limit of large network size. Put differently, when $\lambda \geq \lambda_1$, the structure of the underlying network starts to facilitate the emergence of strain-2, hence reducing the dependence on μ.

[7] The length of the tree of infections can be interpreted as the size of the component (of a bond percolated network with T_1) that contains the seed.

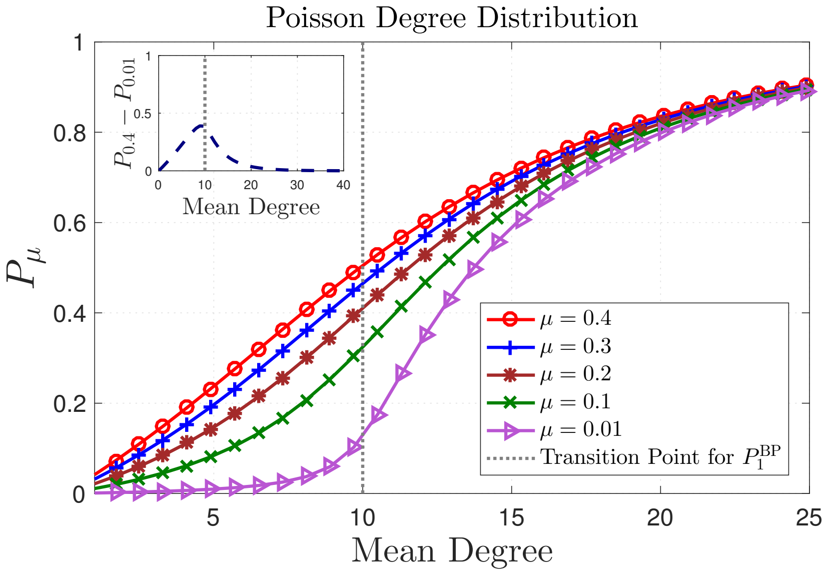


Figure 9.7: **Effect of Mutation:** *We set $T_1 = 0.1$ and plot the behavior of P_μ against the mean degree for a network with Poisson degree distribution. Intuitively, different values of μ have different impact on P_μ. The impact is pronounced before the critical mean degree corresponding to a single-strain, bond-percolated network with T_1. Inset: The difference between the value of P_μ when $\mu = 0.4$ and the value of P_μ when $\mu = 0.01$ as a function of the mean degree of the underlying contact network.*

9.7 Evolution in real-world networks

In Section 9.6.F, we explored the validity of analyzing the multiple-strain model for evolution with the available tools from the classical, single-type bond-percolation framework. We focused on *random* networks generated by the configuration model and demonstrated that a reduction to the classical, single-type bond percolation framework leads to accurate results with respect to the threshold and final size of epidemics, but significantly inaccurate results with respect to the probability of emergence. In this section, we aim to examine the universality of our findings by analyzing the probability of emergence on *real-world* contact networks obtained from SNAP data sets [83]. Our objective is twofold. Firstly, we would like to validate the multi-type branching formalism of Alexander and Day (see Section 9.5.A) on real-world networks. Secondly, we seek to highlight and confirm the limitations of the single-type bond-percolation framework in predicting the probability of emergence on real-world networks.

Network	$\lvert\mathcal{N}\rvert$	$\lvert\mathcal{E}\rvert$	$\lambda_{\text{original}}$	Φ_{original}	$\Phi_{\{\lambda=1\}}$	$\Phi_{\{\lambda=10\}}$	Φ_{random}
Facebook	$4,039$	$88,234$	43.7	0.519	0.011	0.117	0.0107
Twitter	$81,306$	$1,342,296$	33	0.170	0.005	0.051	0.0004
Slashdot	$82,168$	$504,230$	12.3	0.024	0.001	0.019	0.0001
Higgs	$456,626$	$12,508,413$	54.8	0.008	0.0001	0.001	0.0001
School	773	6342	16.4	0.094	0.019	0.059	0.020
Hospital	73	543	14.87	0.446	0.090	0.296	0.183

Figure 9.8: **Real-world contact networks**. *We consider four real-world contact networks in the context of information propagation, namely, Facebook, Twitter, Slashdot, and Higgs networks from SNAP [83] dataset. We also consider two real-world contact networks in the context of infectious disease propagation, namely, a contact network among students, teachers, and staff at a US high school [131] and a contact network among professional staff and patients in a hospital in Lyon, France [141]. For each network, we indicate the number of nodes* $|\mathcal{N}|$*, the number of edges* $|\mathcal{E}|$*, the mean degree of the original network* $\lambda_{\text{original}}$*, and the clustering coefficient of the original network* Φ_{original}. $\Phi_{\{\lambda=1\}}$ *(respectively,* $\Phi_{\{\lambda=10\}}$*) denotes the clustering coefficient of the original network after removing a random subset of edges such that the resulting mean degree is* 1 *(respectively,* 10*).* Φ_{random} *denotes the average clustering coefficient (over* 200 *independent realizations) of a random network generated by the configuration model with Poisson degree distribution. The random network has the same number of nodes and the same (original) mean degree of the corresponding real-world network.*

Dataset: In the context of information propagation, we consider four different contact networks obtained from SNAP [83]. In particular, we consider the following contact networks:

- Facebook [83, 85]: The contact network among the friends of 10 users (including those 10 users).

- Twitter [83, 85]: The contact network among the friends of 1000 users (including those 1000 users).

- Slashdot [83, 84]: The network contains friend/foe links between the users of Slashdot.

- Higgs [30, 83]: The Higgs data set has been collected upon monitoring the spreading processes on Twitter before, during and after the announcement of the discovery of a new particle with the features of the elusive Higgs boson on July 4, 2012. Nodes correspond to the authors of the collected tweets and edges represent the followee/follower relationships between them.

In the context of infectious disease propagation, we consider the following two contact networks:

- High school network [131]: The contact network observed at a US high school during a typical school day. The dataset covers $762,868$ interactions between students, teachers, and staff. Each interaction between two individuals is characterized by their identification numbers as well as the duration of the interaction. Two individuals could have multiple interactions throughout the day, and we sum the durations of these interactions to calculate the total contact time between these two individuals over the whole day. We proceed by sampling a *static* graph out of this dataset, by assigning an edge between nodes u and v with probability $t_{uv}/t_{\max}$ where t_{uv} denotes the total contact time between nodes u and v throughout the day and $t_{\max}$ denotes the maximum total contact time observed in the dataset.

- Hospital network [141]: The contact network observed in a short stay geriatric unit of a university hospital in Lyon, France. The dataset covers five days of interactions between professional staff members and patients. Similar to the high school network, we compute the total contact time between two individuals (over the span of five days), then we sample a static graph out of the dataset, by assigning an edge between nodes u and v with probability $t_{uv}/t_{\max}$.

More details on the networks, including their clustering coefficients are given in Figure 9.8. We assume that all edges are unidirectional.

9.7.1 Methods

To conduct a fair comparison between the formalism given in Section 9.5.A and the single-type bond percolation framework, we fix the parameters of the transmissibility matrix $\boldsymbol{T}$ and the mutation matrix $\boldsymbol{\mu}$, hence fixing $\rho\left(\boldsymbol{T}\boldsymbol{\mu}\right)$ and T_{BP} (according to (9.9)). We vary the mean degree, denoted λ, for each of the contact networks between 1 and 10. For each value of λ, we remove a random subset of edges such that the resulting network is of mean degree λ (approximately). Note that the random removal of edges would indeed lower the clustering coefficient of the network, however, the resulting subgraph would remain highly clustered compared to random networks with the same mean degree (see Figure 9.8). In other words, the sampled networks still exhibit specific structural properties that distinguish them from synthetic contact networks generated randomly by the configuration model (with Poisson degree distribution of the same mean degree). After the mean degree is adjusted, the process proceeds similar to Section 9.6.B.

9.7.2 Results

In Figure 9.9, we plot the probability of emergence for the four contact networks shown in Figure 9.8. We compare the results obtained by computer simulations with those obtained by the multiple-strain formalism (Section 9.5.A) and the single-type bond-percolation framework. We set $T_1 = 0.2$, $T_2 = 0.5$, and $\mu_{11} = \mu_{22} = 0.75$. It follows that $T_{\mathrm{BP}} = 0.4$ according to (9.9).

Similar to our observations on random networks (Section 9.6.E), the single-type, bond-percolation framework provides significantly inaccurate predictions on the probability of emergence, should the underlying process entail evolution. The limitation is universal as it applies to both random and real-world networks. Section 9.9 explains the intuition behind our observations. In contrast, the multiple-strain formalism provides remarkably accurate predictions, especially on contact networks with low clustering coefficient. Note that the multi-type branching framework assumes that the underlying graph is tree-like; an assumption that holds for networks with small clustering coefficient. Hence, one could reasonably argue that the multiple-strain formalism would provide high prediction accuracy on such networks.

9.8 Co-infection controls the order of phase transition

The preceding discussion considers the case when *co-infection* is not possible, hence each infected host either carries strain-1 or strain-2, but not both. However, humans, animals, plants, and other organisms may become *co-infected* with multiple pathogen strains, causing major consequences for both within- and between-host disease dynamics [4,9,25,31,126,139]. For instance, in the case of human malaria, the majority of infected adults are *simultaneously* infected by more than five strains of *Plasmodium falciparum* [4,90]. The competition and interaction patterns between the resident strains trigger significant ramifications of the disease dynamics. Also, the aggregate virulence experienced by the co-infected host could be higher than the most virulent strain, or lower than the least virulent strain, or anywhere in between [4,23,81,140]. Co-infection also applies in the context of information propagation. Observe that with the growing number of news outlets, we may come across various variants of information on social media platforms. Similar to the case of infectious diseases, these variants may reinforce or weaken each other based on whether they share the same bias or not.

In this section, we seek to shed the light on the effects of co-infection on information/disease propagation. In particular, we investigate the extent to which co-infection dynamics could enhance or suppress the scale of epidemics. Of particular interest is whether co-infection could change the order of phase transition from second-order (as it is the case with most epidemic models) to first-order, leading to a phenomenon that is commonly described as *avalanche outbreaks* [21]. To that end, we extend the multiple-strain model given in Section 9.4 to account for co-infection. In particular, a susceptible individual who comes into infectious contacts with type-1 and type-2 hosts *simultaneously* becomes *co-infected* and starts to spread the *co-infection*. Henceforth, we consider the case when the co-infection has its own transmissibility T_{co} and does not mutate back to either strain-1 or strain-2. In other words, a co-infected host infects each of her neighbors independently with probability T_{co}, and infected neighbors are deemed *co-infected* with probability 1.

As with Section 9.6, we consider contact networks with Poisson degree distribution and Power-law degree distribution with exponential cutoff, respectively. For both cases, we set $T_1 = 0.2$, $T_2 = 0.5$, and $\mu_{11} = \mu_{22} = 0.75$. Moreover, we set the network size to 2×10^6 and the number of independent experiments for each data point to 5×10^3. To illustrate how co-infection dynamics control the order of phase transition, we simulate and compare the process for two values of T_{co}, namely $T_{co} = 0.1$ and $T_{co} = 0.8$. Finally, we plot the epidemic size, denoted by s_{co}^{BP}, for a single-strain, bond-percolated network [111].

In all cases, co-infection emerges at the phase transition point that characterizes an epidemic of strain-1 and strain-2, i.e., the mean degree for which $\rho(\boldsymbol{M}) = 1$, where $\boldsymbol{M}$ is given by

$$\boldsymbol{M} = \left(\frac{\langle k^2\rangle - \langle k\rangle}{\langle k\rangle}\right) \begin{bmatrix} T_1 & 0 \\ 0 & T_2 \end{bmatrix} \begin{bmatrix} \mu_{11} & \mu_{12} \\ \mu_{21} & \mu_{22} \end{bmatrix}$$

As seen in Figure 9.10, a *first-order* phase transition is observed on both contact networks when $T_{co} = 0.8$ due to the corresponding first order transition of S_{co}. In particular, the value of S_{co} jumps discontinuously from zero to (approximately) the corresponding value of S_{co}^{BP} for a single-strain, bond-percolated network with $T_{co} = 0.8$. Hence, a first-order phase transition is observed. In general, we conjecture that a first-order phase transition emerges whenever T_{co} is large enough such that $S_{co}^{BP} > 0$ at the critical point $\rho(\boldsymbol{M}) = 1$. If, however, T_{co} is small such that $S_{co}^{BP} = 0$ when $\rho(\boldsymbol{M}) = 1$, then a second-order phase transition is observed. This is confirmed by our simulation results for the case when $T_{co} = 0.1$.

In order to validate the order of phase transition when $T_{co} = 0.8$, we conduct an extensive simulation study around the phase transition point on both contact networks. In Figure 9.11, we set the number of nodes n to 15×10^6 (to alleviate finite size effects) and the number of experiments to 10^4 for each data point. We use the same parameters that were used to generate Figure 9.10, i.e., $T_1 = 0.2$, $T_2 = 0.5$, and $\mu_{11} = \mu_{22} = 0.75$. Our results confirm that the phase-transition is indeed first order on both contact networks. In fact, the value of S_{co} jumps discontinuously to (approximately) the corresponding value of S_{co}^{BP} with $T_{co} = 0.8$.

9.9 Correlations of infection events

We have shown that the inability of the single-type bond-percolation framework to predict the probability of emergence is universal; it is observed on both random and real-world contact networks. The universality of the behavior suggests that single-type bond-percolation framework does not properly capture a fundamental property of spreading processes that entail evolution. Below, we argue that this property is stemming from the underlying *correlations* between the infection events of the multiple-strain model. For reasons that will become apparent soon, it is useful to draw parallels between the multiple strain model proposed by Alexandar and Day [3] and the single-strain model proposed by Newman in [111].

In [111], Newman proposed a stochastic SIR model where the probability that an infected node i infects a susceptible node j is given by $T_{ij} = 1 - \exp(-\beta_{ij}\tau_i)$, where β_{ij} denotes the rate of infectious contacts from node i to node j and τ_i denotes the infectious period of node i, i.e., the period of time during which node i remains infective. The infectious period τ_i is a random variable with a Cumulative Distribution Function (CDF) $F_\tau(u)$, and the infectious contact rate β_{ij} is also a random variable with a CDF $F_\beta(v)$. Newman claimed that under the assumptions that i) the infectious contact rates between individuals are independent and identically distributed (i.i.d) and that ii) the infectious periods for all individuals are also i.i.d., the spread of a diseases on a contact network is isomorphic to a bond-percolation model on the contact network with a bond percolation parameter given by

$$T = \langle T_{ij} \rangle = 1 - \int_0^\infty e^{-\beta\tau} dF_\beta(\beta) dF_\tau(\tau)$$

where T was called the *transmissibility* of the disease. The isomorphism to a bond-percolation problem allowed for the use of generating functions to derive the threshold, probability, and final size of epidemics on a contact network with arbitrary degree distributions.

Later on, Kenah and Robins [78] proved that this isomorphism to a bond-percolation problem is valid only when the distribution of the infectious periods is *degenerate*, i.e., $\tau_i = \tau_0$

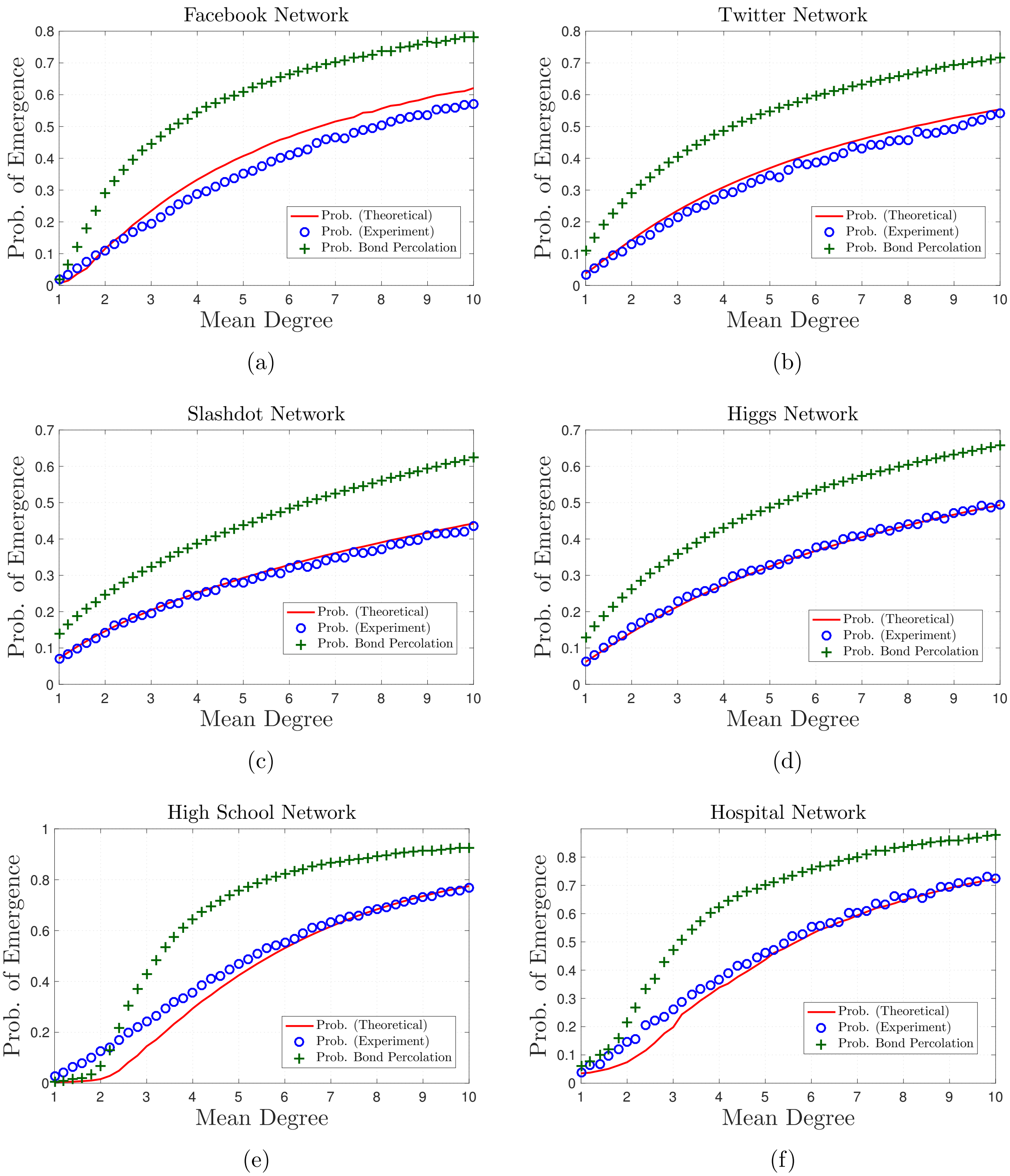
for all $i = 1, 2, \ldots$, where τ_0 is a constant. Kenah and Robins showed that when the distribution of the infectious periods is non-degenerate, there is no bond-percolation probability that will make the bond-percolation model isomorphic to the SIR model. The fundamental reason behind their findings is the fact that the infection events across edges emanating from node i are *conditionally* independent given τ_i, but *marginally* dependent unless $\tau_i = \tau_0$ with probability one. That said, Kenah and Robins showed that even when the distribution of the infectious periods is non-degenerate, the mapping to a bond-percolation process can still be used to accurately predict the epidemic threshold and epidemic size.

The multiple-strain model presented by Alexander and Day exhibits a similar form of correlations between infection events. In particular, infection events are conditionally independent given the type of the infective node. Namely, conditioned on node i being infected with strain-ℓ, node i infects each of her neighbors *independently* with probability T_ℓ. However, infection events are marginally dependent, unless $T_i = T_0$ for all i with probability one; a condition that essentially reduces the dynamics to that of single-strain processes without evolution. To give an example, consider a *regular* network, where each node has exactly 2 neighbors. Let $T_1 = 1$ and $\mu_{11} = \mu_{21} = \mu$. In this case, we have $T_{\text{BP}} = \mu + T_2(1 - \mu)$. Now, we can easily compute the probability that an infection of a randomly selected node results in an outbreak of size *one*. Under the bond percolation framework, this is given by $(1 - T_{\text{BP}})^2 = (1 - \mu - T_2(1 - \mu))^2$. However the multiple-strain formalism predicts a zero probability for this event, should the initial node be infected with strain-1. Indeed, the probability predicted by the bond percolation framework will match the one predicted by the multiple-strain formalism only if $T_2 = 1$ or $\mu = 1$; a condition that diminishes the role of evolution and reduces the dynamics into that of single-strain processes.

9.10 Conclusion

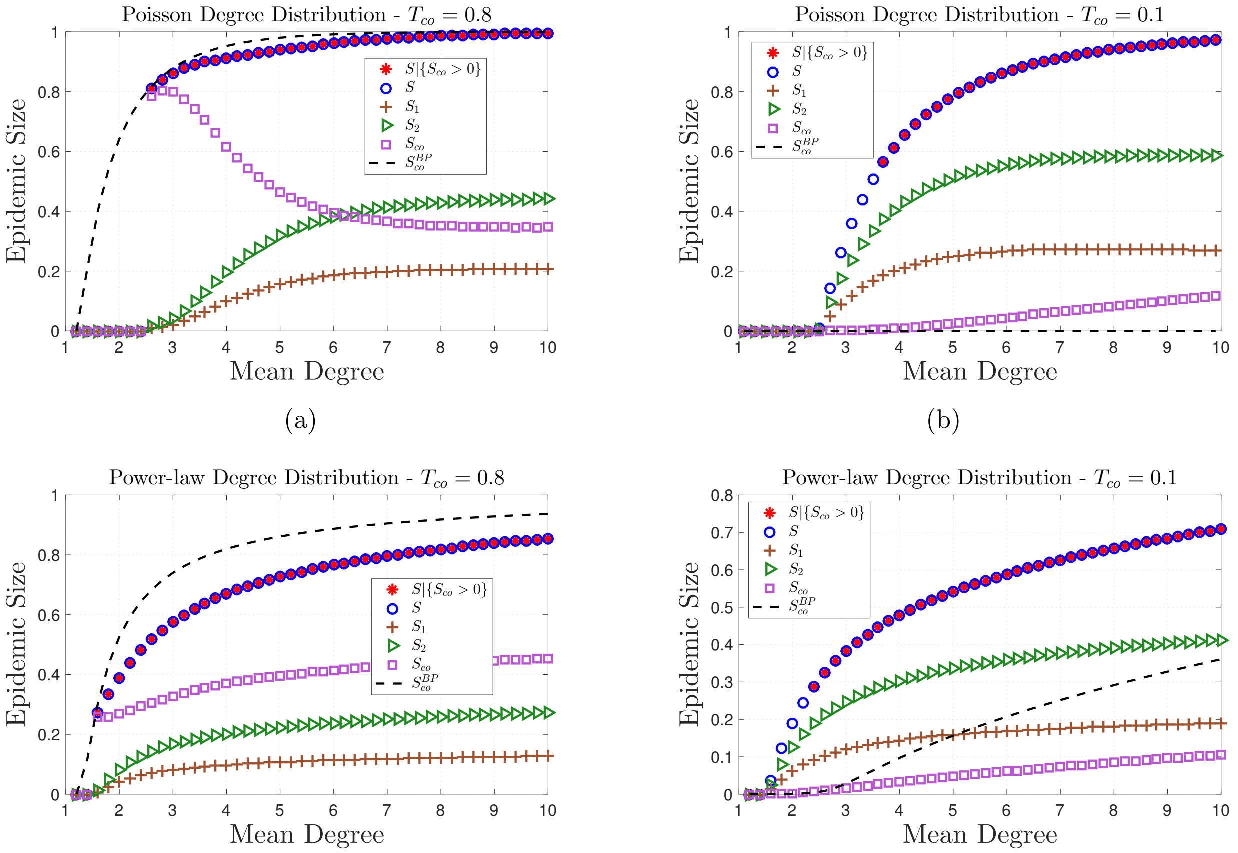
In this chapter, we have investigated the *evolution* of spreading processes on complex networks and developed a mathematical theory that unravels the relationship between the characteristics of the spreading process, evolution, and the structure of the contact network on which the process spreads. Our mathematical theory was complemented by an extensive simulation study on both random and real-world contact networks. The simulation results proved the validity of our theory and revealed the significant shortcomings of the classical mathematical models that do not capture evolution. A matching condition between single- and multiple-strain models was proposed and evaluated in the context of probability of emergence, epidemic size, and epidemic threshold. Under the proposed matching condition, our results revealed that the classical bond-percolation models may accurately predict the threshold and final size of epidemics that entail evolution, but their predictions on the probability of emergence are *significantly inaccurate* on both random and real-world networks. Hence, our formalism is necessary to bridge the disconnect between how spreading processes propagate and evolve on complex networks, and the current mathematical models that do not capture evolution.

We proceeded by deriving a lower bound on the probability of emergence to gain further insights on the effects of mutation. The bound was derived for the special case of one-step irreversible mutation. Our results revealed that the probability of mutation plays a key role in determining the shape and behavior of the probability of emergence. Moreover, the way the particular value of μ influences the probability of mutation varies according to the connectivity of the underlying contact network. Finally, we considered the case when *co-infection* is possible and showed that co-infection dynamics control the order of phase transition in an interesting way. In particular, depending on co-infection dynamics, the order of phase transition of the epidemic size could change from second-order to *first-order*, in contrast to the universality class of percolation models that are typically second-order.



(a) (b) (c) (d) (e) (f)

Figure 9.9: **The probability of emergence on real-world contact networks.** *In the context of information propagation, we consider four contact networks sampled from SNAP data sets [83]: (a) Facebook network, (b) Twitter network, (c) Slashdot network, and (d) Higgs network. In the context of infectious disease propagation, we consider two contact networks: (e) High school contact network and (f) Hospital contact network. We set $T_1 = 0.2$, $T_2 = 0.5$, $\mu_{11} = \mu_{22} = 0.75$ (hence $T_{\text{BP}} = 0.4$) and vary the mean degree, denoted λ, from 1 to 10. For each value of λ, we remove a random subset of edges such that the resulting graph is of mean degree λ (approximately). The sampled networks still exhibit higher clustering coefficient as compared to random networks with the same mean degree. The single-type bond-percolation framework provides inaccurate predictions on the probability of emergence, in contrast to the multiple-strain formalism given by Alexander and Day [3].*



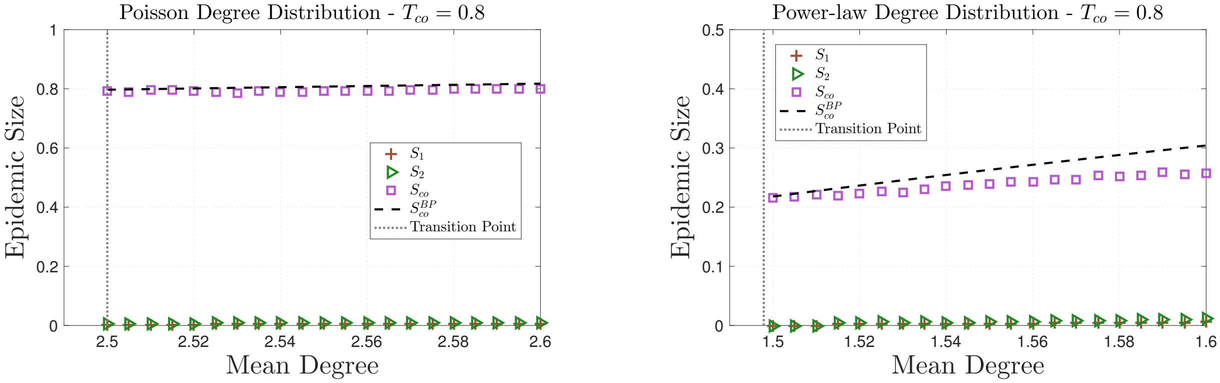
(a)

(b)

(c)

(d)

Figure 9.10: **Co-infection dynamics determine the order of phase transition**. *We set $T_1 = 0.2$, $T_2 = 0.5$, and $\mu_{11} = \mu_{22} = 0.75$ for all subfigures. The network size n is 2×10^6 and the number of independent experiments for each data point is 5×10^3. Blue circles denote the average total epidemic size S and red stars denote the average total epidemic size S conditioned on S_{co} being greater than zero, i.e., conditioned on the existence of a positive fraction of co-infected nodes. Blue plus signs, orange triangles, and yellow squares denote the fraction of nodes infected with strain-1, strain-2, and co-infection, respectively. The black dashed-line denotes the epidemic size for a single-strain, bond-percolated network with T_{co}, i.e., S_{co}^{BP}. (a) and (c): A first order phase transition is observed when $T_{co} = 0.8$ owing to the corresponding first order transition of S_{co}. Co-infection emerges at the phase transition point that characterizes an epidemic of strain-1 and strain-2. At this point, the value of S_{co} jumps discontinuously to (approximately) the corresponding value of S_{co}^{BP} with $T_{co} = 0.8$. Observe that $S_{co}^{BP} > 0$ at the transition point, hence, a first-order phase transition is observed. (b) and (d): Co-infection still emerges right at the phase transition point. However, since T_{co} is small, $S_{co}^{BP} = 0$ at the transition point. Hence, a second-order phase transition is observed.*



(a) (b)

Figure 9.11: **Validating the order of phase transition**. *We set the network size n to 15×10^6, the number of independent experiments for each data point to 10^4, $T_1 = 0.2$, $T_2 = 0.5$, and $\mu_{11} = \mu_{22} = 0.75$. Our results confirm that the phase-transition is indeed first order on both contact networks. The value of S_{co} jumps discontinuously to (approximately) the corresponding value of S_{co}^{BP} with $T_{co} = 0.8$.*

Chapter 10

The multiple-strain model on random graphs with clustering

10.1 Motivation

In Chapter 9, we considered the propagation of spreading processes entailing evolutionary adaptations on contact networks modeled by random graphs with arbitrary degree distribution (generated by the configuration model [100, 115]). We started by considering the case where co-infection with multiple pathogen strains is not possible. In this case, we developed a mathematical theory that predicts the expected epidemic size and epidemic threshold point as functions of the underlying network structure (as given by the degree distributions), the characteristics of the spreading process (the transmissibility matrix), and evolutionary adaptations (the mutation matrix). We then considered the case where co-infection is possible, and showed via computer simulations that co-infection could lead the order of phase transition to change from second-order (as with the universality of percolation models) to first-order.

Although random graphs generated by the configuration model could resemble the degree sequences observed in real-world social networks, they have a vanishingly small clustering coefficient that tends to zero in the limit of large network size. Hence, the random graphs generated by the configuration model can not accurately capture some important aspects of real-world social networks, most notably the property of high clustering [132, 144], which has a significant impact on the behavior of various spreading processes [70, 72].

To better model real-world social networks that are typically clustered, we utilize a model that generates random networks *with clustering* as introduced by Miller [97] and Newman [109], i.e., graphs are generated randomly from given distributions specifying the number of single edges and triangles for any given node. Our objective is to investigate the characteristics of spreading processes that entail evolutionary adaptations on such random graph models with tunable clustering. We focus on the case where co-infection is not possible, and derive a mathematical theory that predicts the epidemic threshold and the probability of emergence as functions of the characteristics of the spreading object, the evolutionary pathways of the pathogen/information, and the structure of the underlying network as given by the *joint* degree distribution of single-edges and triangles.

10.2 A roadmap

We investigate the *evolution* of spreading processes, such as infectious diseases or information, in *clustered* social networks, hence we extend our previous results for the case when the underlying graph had a vanishingly small clustering coefficient. Our objectives are to i) reveal the role of evolutionary adaptations on the threshold and probability of epidemics when the network exhibits a non-vanishing clustering coefficient; as well as ii) identify the interplay between the structural properties of the network (as given by the the joint degree distribution of single-edges and triangles) and evolutionary adaptations. Our results are given in the form of a mathematical theory that accurately predicts the epidemic threshold and the probability of emergence as functions of the characteristics of the spreading process, the evolutionary pathways of the pathogen (respectively, information), and the structure of the underlying contact network (as given by its joint degree distribution of single-edges and triangles). Simulation results on synthetic networks are also provided to verify our theory.

10.3 Model definitions

We consider the propagation of spreading processes characterized by the (inhomogeneous) multiple-strain model (see Chapter 9.4.2) on random graphs with clustering as proposed by Miller [97] and Newman [109]. The model is considered as a generalization to the standard configuration model [100,115] that generates random graphs with arbitrary degree distribution, but a vanishing clustering coefficient. Note that the level of clustering associated with a network could be quantified in different ways, but here we focus on the notion of *global clustering coefficient* as defined in [112]. Namely, the global clustering coefficient is defined as

$$C_{\text{global}} = \frac{3 \times \text{ number of triangles in the network}}{\text{number of connected triples}}$$

where a connected triple means a single vertex connected by edges to two others.

The algorithm used to generate random graphs with clustering is defined as follows. Consider a joint degree distribution $\{p_{st}\}_{s,t=0}^{\infty}$ that specifies the probability that an arbitrary node has s single-edges and is part of t triangles. Note that if a node has s single-edges and is part of t triangles, then its degree is $s + 2t$ since each triangle adds two edges connecting the node to the other end nodes of the triangle. Essentially, in this model, triangles are treated separately from single-edges. Note that we can think of s as the number of single stubs and t as the number of corners of triangles. In order to create the network, we choose pairs of single stubs uniformly at random and join them to make a complete edge between two nodes, and also choose trios of corners of triangles at random and join them to form a triangle. Indeed, the total degree distribution in the network could be obtained through $\{p_{st}\}_{s,t=0}^{\infty}$ as follows.

$$p_k = \sum_{s,t} p_{st}\delta_{k,s+2t}$$

where p_k denotes the probability that an arbitrary node is of degree k and δ_{ij} is the Kronecker delta function. In contrast to the standard configuration model, where C_{global} approaches zero in the limit of large network size, the quantity C_{global} is positive for networks generated according to the above algorithm implying the existence of a non-trivial clustering in the network.

One aspect of particular importance is the joint degree distribution of a node that we arrive at by following a single-edge selected uniformly at random. Note that the joint degree distribution of this node is not simply given by p_{st} since the node under consideration is known to have at least one single-edge that was traversed to reach it. In this case, the joint distribution would be proportional to the number of single-edges assigned to this node (the more single-edges it has, the more likely that we arrive at it when traversing a randomly selected single-edge). Namely, the joint degree distribution in this case would be given by $sp_{s,t}/\langle s\rangle$, where $\langle s\rangle = \sum_{s,t} sp_{s,t}$ ensures proper normalization. Put differently, with probability $sp_{s,t}/\langle s\rangle$, the node has $s-1$ *remaining* single-edges (because one single-edge was already used to reach it) and t triangles. Similarly, we can show that the joint degree distribution of a node that we arrive at by following a triangle selected uniformly at random is given by $tp_{s,t}/\langle t\rangle$, where $\langle t\rangle = \sum_{s,t} tp_{s,t}$.

In the following section, we derive the probability of emergence and epidemic threshold for spreading processes governed by the multiple-strain model on random graphs with clustering. Our mathematical theory reveals the interplay between the structure of the underlying contact network (as given by its joint degree distribution), the characteristics of the spreading process (as given by the transmissibility matrix $\boldsymbol{T}$), and the evolutionary pathways (as given by the mutation matrix $\boldsymbol{\mu}$).

10.4 Theoretical results

We consider a branching process that starts by selecting a node uniformly at random and infecting it with a particular strain, then exploring all the neighbors that are reached and infected due to this node. The process continues recursively until the branching terminates. Our method relies on using the *generating functions* approach to characterize the distribution of the resulting number of nodes that received the infection due to the spreading process. In what follows, we use the term *type-i* node to denote a node that is spreading strain-i, i.e., a node that has received an infection with a strain that has eventually mutated to strain-i prior to subsequent infections. We focus on the case where $m = 2$, i.e., there are only two strains propagating in the population, yet it is straightforward to extend our theory to the general case of m strains.

Let $h_i(x)$ (respectively, $g_i(x)$) denote the probability generating function of the number of *finite* nodes reached and infected by following a randomly selected single-edge (respectively, triangle) emanating from a type-i node. In addition, let $Q_i(x)$ denote the probability generating function of the number of finite nodes reached and infected by selecting a node uniformly at random and making it type-i.

Observe that

$$Q_i(x) = x \sum_{s,t} p_{s,t} h_i(x)^s g_i(t)^t \tag{10.1}$$

where $p_{s,t}$ denotes the joint degree distribution of single-edges and triangles. The validity of (10.1) could be seen as follows. The term x stands for the node that is selected randomly and given the infection as the seed of the process. Note that this node has a joint degree (s,t) with probability $p_{s,t}$. Since this node is type-i, the number of nodes reached and infected by each of its s single-edges (respectively, each of the t triangles) has a generating function $h_i(x)$ (respectively, $g_i(x)$). From the *powers property* of generating functions [115], the total number of nodes reached and infected in this process when the initial node is type-i and has joint degree (s,t) has a generating function $h_i(x)^s g_i(x)^t$. As we average over all possible joint degrees (s,t), we obtain (10.1). In what follows, we obtain expressions for the terms $h_1(x)$, $h_2(x)$, $g_1(x)$, and $g_2(x)$.

10.4.1 Deriving $h_1(x)$ and $h_2(x)$

We start by deriving an expression for $h_1(x)$. Note that $h_1(x)$ denotes the probability generating function of the number of finite nodes reached and infected by following a randomly selected single edge emanating from a type-1 node. Observe that if this edge is not occupied (an event which happens with probability $1 - T_1$), then no node whatsoever would receive the infection following this edge (leading to a term $(1 - T_1)x^0$ in the generating function for $h_1(x)$). If this edge is occupied (an event that happens with probability T_1), then the current node must have received an infection with strain-1, and it would either become type-1 if the pathogen does not mutate (an event that happens with probability μ_{11}) or type-2 if the pathogen mutates to strain-2 (an event that happens with probability μ_{12}). Averaging over all possible mutation outcomes, we get

$$h_1(x) = 1 - T_1 + T_1 x \left(\mu_{11} \sum_{s,t} \frac{s p_{s,t}}{\langle s \rangle} h_1(x)^{s-1} g_1(x)^t + \mu_{12} \sum_{s,t} \frac{s p_{s,t}}{\langle s \rangle} h_2(x)^{s-1} g_2(x)^t \right) \qquad (10.2)$$

The validity of (10.2) could be seen as follows. When the node under consideration receives the infection (which happens when the edge is occupied), the number of nodes reached and infected will be one *plus* all the nodes reached and infected due to the particular node under consideration. This node could be type-1 with probability μ_{11} or type-2 with probability μ_{12}. In either case, the probability that this node has a joint degree (s, t) would be given by $s p_{s,t}/\langle s \rangle$ since it is already known that this node has at least one single-edge. Since this node has already utilized one of its single-edges to connect to its parent, it has $s - 1$ remaining single-edges and t triangles that it could utilize to spread the infection. When the node is type-1 (respectively, type-2), the powers property of generating functions readily implies that the number of nodes reached and infected due to this node has a generating function $h_1(x)^{s-1} g_1(x)^t$ (respectively, $h_2(x)^{s-1} g_2(x)^t$). Averaging over all possible joint degrees and node types gives (10.2). Similarly, we derive an expression for $h_2(x)$ as follows.

$$h_2(x) = 1 - T_2 + T_2 x \left(\mu_{21} \sum_{s,t} \frac{s p_{s,t}}{\langle s \rangle} h_1(x)^{s-1} g_1(x)^t + \mu_{22} \sum_{s,t} \frac{s p_{s,t}}{\langle s \rangle} h_2(x)^{s-1} g_2(x)^t \right) \tag{10.3}$$

10.4.2 Deriving $g_1(x)$ and $g_2(x)$

The situation becomes more challenging as we consider triangles since we need to jointly consider the status of the two end nodes of a triangle. Note that a triangle emanating from a type-i node could have several possible configurations. A graphical illustration of these different configurations is given in Figure 10.1 for the case when the triangle is emanating from a type-1 node. In general (when the parent node is of type-i), we have

1. **C1 - Both end nodes were not infected.** This configuration occurs when the parent node fails to infect both end nodes, i.e., when both edges are not occupied, an event happening with probability $(1 - T_i)^2$.
2. **C2 - One end node was infected and has become type-**1. This configuration occurs when i) the parent node infects one of the end nodes which later becomes type-1, *and* ii) neither the parent node nor the infected end node succeed in infecting the other end node. Hence we have $2T_i\mu_{i1}(1 - T_i)(1 - T_1)$ as the associated probability, where the multiplication by 2 is due to symmetry, i.e., either of the two end nodes could be the infected node.
3. **C3 - Both end node were infected and have become type-**1. The configuration occurs when i) the parent node infects both end nodes and they later become type-1, *or* the parent node infects one of the two end node (say the left node) but fails to infect the other end node (say the right node) which later gets infected due to the left node. Hence, the probability for this configuration is $(T_i\mu_{i1})^2 + 2T_i\mu_{i1}(1 - T_i)T_1\mu_{11}$. Note that the multiplication by 2 is due to symmetry.
4. **C4 - One end node was infected and has become type-**2. Similar to C2, the probability of this configuration is $2T_i\mu_{i2}(1 - T_i)(1 - T_2)$.

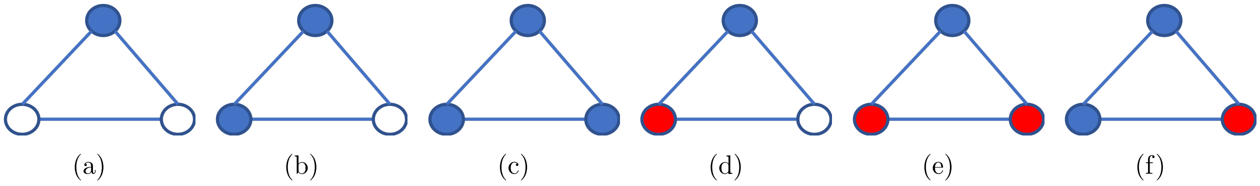


Figure 10.1: **Different possible configurations for a triangle emanating from a type-1 node**. *Type-1 nodes are highlighted in blue, while type-2 nodes are highlighted in red. The two ends nodes could be in one of several configurations. Namely, (a) both end nodes are not infected, (b) one end node is type-1, (c) both end nodes are type-1, (d) one end node is type-2, (e) both end nodes are type-2, and (f) one end node is type-1 while the other end node is type-2.*

5. **C5 - Both end node were infected and have become type-2**. Similar to C3, the probability of this configuration is $(T_i\mu_{i2})^2 + 2T_i\mu_{i2}(1-T_i)T_2\mu_{22}$.
6. **C6 - Both end node were infected, one of them has become type-1, and the other has become type-2**. This configuration occurs when i) the parent node infects both end nodes, then one of them becomes type-1 and the other becomes type-2, *or* ii) the parent node infects *only* one node that later becomes type-1 (or type-2) and infects the other. Hence, the probability of this configuration is given by

$$2\left(T_i^2\mu_{i1}\mu_{i2} + T_i\mu_{i1}(1-T_i)T_1\mu_{12} + T_i\mu_{i2}(1-T_i)T_2\mu_{21}\right)$$

where the multiplication by 2 is again due to symmetry.

Let c_{ij} denotes the probability of the jth configuration when the parent node is type-i for $i = 1, 2$ and $j = 1, \ldots, 6$. We then have

$$\begin{aligned} g_i(x) = c_{i1} + c_{i2}x\sum_{s,t}\frac{tp_{st}}{\langle t\rangle}h_1(x)^s g_1(x)^{t-1} + c_{i3}\left(x\sum_{s,t}\frac{tp_{st}}{\langle t\rangle}h_1(x)^s g_1(x)^{t-1}\right)^2 + \\ c_{i4}x\sum_{s,t}\frac{tp_{st}}{\langle t\rangle}h_2(x)^s g_2(x)^{t-1} + c_{i5}\left(x\sum_{s,t}\frac{tp_{st}}{\langle t\rangle}h_2(x)^s g_2(x)^{t-1}\right)^2 + \\ c_{i6}\left(x\sum_{s,t}\frac{tp_{st}}{\langle t\rangle}h_1(x)^s g_1(x)^{t-1}\right)\left(x\sum_{s,t}\frac{tp_{st}}{\langle t\rangle}h_2(x)^s g_2(x)^{t-1}\right) \end{aligned} \quad (10.4)$$

for $i = 1, 2$, where the validity of (10.4) could be seen as follows. With probability c_{i1}, the triangle is in configuration C1, hence, both end nodes are not spreading any infection. This leads to a term $c_{i1}x^0$ in the generating function. Next, with probability c_{i2} (respectively, c_{i4}), the triangle is in configuration C2 (respectively, C4), in which case the degree distribution of the infected node would be given by $tp_{st}/\langle t \rangle$ since it is already known that this node has at least one triangle. Since this node has already utilized one triangle to connect to its parent, it can only utilize the remaining $t - 1$ triangles and s single-edges to infect its neighbors. Using the powers property of the generating functions, along with the fact that in this configuration the node under consideration is type-1 (respectively, type-2), the generating function for the number of subsequent infections would be given by $h_1(x)^s g_1(x)^{t-1}$ (respectively, $h_2(x)^s g_2(x)^{t-1}$). For configuration C3, C5, and C6, the two end nodes are spreading the infection, yet to two independent sets of other nodes, hence we could utilize the powers property of generating functions to get the corresponding terms.

10.4.3 Threshold and probability of epidemics

Recall that $Q_i(x)$ gives the probability generating function for the number of *finite* nodes reached and infected by selecting a node uniformly at random and making it type-i. By conservation of probability and the definition of generating functions, we know that $Q_i(1) = 1$ only if the final number of infected nodes is finite with probability one. Hence, when the process starts with a type-i node, an outbreak would emerge only if $Q_i(1) < 1$. Put differently, the term $1 - Q_i(1)$ gives the probability of emergence, i.e., the probability that the process (starting with a type-i node) leads to an infinite component of infected nodes.

Note that in order to compute $1 - Q_i(1)$, we need to obtain the fixed point of the recursive equations (10.2 - 10.4) at $x = 1$, then report the resulting values of $h_1(1)$, $h_2(1)$, $g_1(1)$, and $g_2(1)$ back into (10.1). For notational simplicity, define $h_1 := h_1(1)$, $h_2 := h_2(1)$, $g_1 := g_1(1)$, and $g_2 := g_2(1)$. Clearly, the set of equations (10.2 - 10.4) admit a trivial fixed point $h_1 = h_2 = g_1 = g_2 = 1$. Substituting back into (10.1) gives $1 - Q_i(1) = 0$, i.e., all infected components are of finite size and no outbreak emerges. In order to check the stability of this trivial solution, we linearize the set of equations (10.2 - 10.4) around $x = 1$, and compute the corresponding Jacobian matrix $\boldsymbol{J} = [J_{ij}]$. If the largest eigenvalue of the Jacobian matrix (in absolute value), denoted $\sigma(\boldsymbol{J})$, is less than one, then the trivial solution is stable, leading to a zero probability of emergence. However, if $\sigma(\boldsymbol{J}) > 1$, then there exists another stable solution with $h_1, h_2, g_1, g_2 < 1$, leading to a positive probability of emergence, i.e., $1 - Q_i(1) > 0$. Put differently, a phase transition occurs if

$$\sigma(\boldsymbol{J}) > 1$$

In what follows, we show the form of the Jacobian matrix $\boldsymbol{J}$. For notational simplicity, let

$$\begin{aligned}
f_1(h_1, h_2, g_1, g_2) &:= 1 - T_1 + T_1 x \left(\mu_{11} \sum_{s,t} \frac{s p_{s,t}}{\langle s \rangle} h_1^{s-1} g_1^t + \mu_{12} \sum_{s,t} \frac{s p_{s,t}}{\langle s \rangle} h_2^{s-1} g_2^t \right) \\
f_2(h_1, h_2, g_1, g_2) &:= 1 - T_2 + T_2 x \left(\mu_{21} \sum_{s,t} \frac{s p_{s,t}}{\langle s \rangle} h_1^{s-1} g_1^t + \mu_{22} \sum_{s,t} \frac{s p_{s,t}}{\langle s \rangle} h_2^{s-1} g_2^t \right) \\
f_3(h_1, h_2, g_1, g_2) &:= c_{11} + c_{12} x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_1^s g_1^{t-1} + c_{13} \left(x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_1^s g_1^{t-1} \right)^2 + \\
&\quad c_{14} x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_2^s g_2^{t-1} + c_{15} \left(x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_2^s g_2^{t-1} \right)^2 + \\
&\quad c_{16} \left(x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_1^s g_1^{t-1} \right) \left(x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_2^s g_2^{t-1} \right) \\
f_4(h_1, h_2, g_1, g_2) &:= c_{21} + c_{22} x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_1^s g_1^{t-1} + c_{23} \left(x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_1^s g_1^{t-1} \right)^2 + \\
&\quad c_{24} x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_2^s g_2^{t-1} + c_{25} \left(x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_2^s g_2^{t-1} \right)^2 + \\
&\quad c_{26} \left(x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_1^s g_1^{t-1} \right) \left(x \sum_{s,t} \frac{t p_{st}}{\langle t \rangle} h_2^s g_2^{t-1} \right)
\end{aligned}$$

We have

$$\begin{aligned}
J_{i1} &= \frac{\partial}{\partial h_1} f_i(h_1, h_2, g_1, g_2)\Big|_{h_1=h_2=g_1=g_2=1} \\
J_{i2} &= \frac{\partial}{\partial h_2} f_i(h_1, h_2, g_1, g_2)\Big|_{h_1=h_2=g_1=g_2=1} \\
J_{i3} &= \frac{\partial}{\partial g_1} f_i(h_1, h_2, g_1, g_2)\Big|_{h_1=h_2=g_1=g_2=1} \\
J_{i4} &= \frac{\partial}{\partial g_2} f_i(h_1, h_2, g_1, g_2)\Big|_{h_1=h_2=g_1=g_2=1}
\end{aligned}$$

for $i = 1, 2, 3, 4$. It follows that

$$\boldsymbol{J} = \begin{bmatrix}
T_1\mu_{11}\frac{\langle s^2\rangle-\langle s\rangle}{\langle s\rangle} & T_1\mu_{12}\frac{\langle s^2\rangle-\langle s\rangle}{\langle s\rangle} & T_1\mu_{11}\frac{\langle st\rangle}{\langle s\rangle} & T_1\mu_{12}\frac{\langle st\rangle}{\langle s\rangle} \\
T_2\mu_{21}\frac{\langle s^2\rangle-\langle s\rangle}{\langle s\rangle} & T_2\mu_{22}\frac{\langle s^2\rangle-\langle s\rangle}{\langle s\rangle} & T_2\mu_{21}\frac{\langle st\rangle}{\langle s\rangle} & T_2\mu_{22}\frac{\langle st\rangle}{\langle s\rangle} \\
d_1\frac{\langle st\rangle}{\langle t\rangle} & d_2\frac{\langle st\rangle}{\langle t\rangle} & d_1\frac{\langle t^2\rangle-\langle t\rangle}{\langle t\rangle} & d_2\frac{\langle t^2\rangle-\langle t\rangle}{\langle t\rangle} \\
d_3\frac{\langle st\rangle}{\langle t\rangle} & d_4\frac{\langle st\rangle}{\langle t\rangle} & d_3\frac{\langle t^2\rangle-\langle t\rangle}{\langle t\rangle} & d_4\frac{\langle t^2\rangle-\langle t\rangle}{\langle t\rangle}
\end{bmatrix}$$

with

$$d_1 = c_{12} + 2c_{13} + c_{16}$$

$$d_2 = c_{14} + 2c_{15} + c_{16}$$

$$d_3 = c_{22} + 2c_{23} + c_{26}$$

$$d_4 = c_{24} + 2c_{25} + c_{26}$$

10.5 Numerical results

In this section, we aim to validate our theoretical results using computer simulations. We focus on the case where $m = 2$, i.e., there are only two strains propagating in the population and consider the following parameters for the multiple-strain model:

$$\boldsymbol{T} = \begin{bmatrix} 0.2 & 0 \\ 0 & 0.5 \end{bmatrix} \qquad \text{and} \qquad \boldsymbol{\mu} = \begin{bmatrix} 0.75 & 0.25 \\ 0.25 & 0.75 \end{bmatrix}$$

Unless otherwise stated, we start the process by selecting a node uniformly at random and infecting it with strain-1. The node infects each neighbor independently with probability T_1. Each of the infected neighbors mutate independently to strain-1 with probability μ_{11}, or to strain-2 with probability μ_{12}. As the process continues to grow, both strains might exist in the population. An intermediate node that becomes infected with strain-i would mutate to strain-1 with probability μ_{i1}, or strain-2 with probability μ_{i2}, for $i = 1, 2$. When cycles start to appear, a susceptible node could be exposed to multiple infections at once. If a node is exposed to x infections of strain-1 and y infections of strain-2 simultaneously, the node becomes infected with strain-1 (respectively, strain-2) with probability $x/(x+y)$ (respectively, $y/(x+y)$) for any non-negative constants x and y. A node that receives infection at round i mutate first (by the end of round i) before it attempts to infect her neighbors at round $i+1$. The node is considered *recovered* at round $i+2$, i.e., a node is infective for only one round.

The underlying contact network is modeled by random graphs with clustering, where the joint degree sequence $p_{s,t}$ is given by the *doubly Poisson distribution*, i.e., the number of single-edges and triangles are independent and they follow a Poisson distribution. Namely, we set

$$p_{st} = e^{-\lambda_s} \frac{(\lambda_s)^s}{s!} \cdot e^{-\lambda_t} \frac{(\lambda_t)^t}{t!}, \quad s, t = 1, \ldots$$

with λ_s and λ_t denoting the mean number of single-edges and triangles, respectively. Note that in this case, the Jacobian matrix is given by

$$\boldsymbol{J} = \begin{bmatrix} T_1\mu_{11}\lambda_s & T_1\mu_{12}\lambda_s & T_1\mu_{11}\lambda_t & T_1\mu_{12}\lambda_t \\ T_2\mu_{21}\lambda_s & T_2\mu_{22}\lambda_s & T_2\mu_{21}\lambda_t & T_2\mu_{22}\lambda_t \\ d_1\lambda_s & d_2\lambda_s & d_1\lambda_t & d_2\lambda_t \\ d_3\lambda_s & d_4\lambda_s & d_3\lambda_t & d_4\lambda_t \end{bmatrix} \tag{10.5}$$

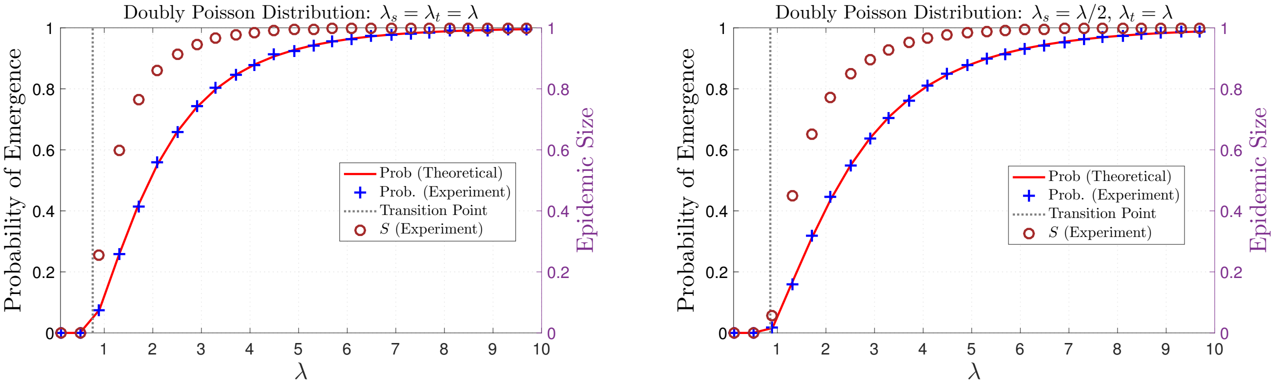
10.5.1 Threshold and probability of epidemics

In Figure 10.2, we consider the cases when i) $\lambda_s = \lambda_t = \lambda$ while λ varies from 1 to 10 and ii) $\lambda_s = \lambda/2$, $\lambda_t = \lambda$ while λ varies from 1 to 10 . For each value of λ, we obtain the empirical probability of emergence. In particular, we set the network size n to 2×10^5 and perform $15,000$ independent experiment per each data point. The empirical probability of emergence is given by the fraction of experiments for which an outbreak emerges. In addition, we compute the critical value of λ for which (10.5) has a spectral radius of one, i.e., $\sigma(\boldsymbol{J}) = 1$, to mark the phase transition point. Our theoretical results on the probability of emergence and phase transition point are in excellent agreement with simulation results. We also show the expected epidemic size S obtained by the simulations.

10.5.2 Impact of clustering

In order to better understand the impact of clustering, we consider a joint degree distribution that allows us to control the level of clustering, while keeping the mean total degree fixed. In particular, we set the distribution of the number of single-edges as 2 Poi $\left(\frac{4-c}{2}\lambda\right)$ and the distribution of the number of triangles to Poi $\left(\frac{c}{2}\lambda\right)$ where $c \in [0, 4]$. Note that in this case, the degree distribution (singles-edges plus triangle-edges) is given by 2 Poi $\left(\frac{4-c}{2}\lambda\right)$ + 2 Poi $\left(\frac{c}{2}\lambda\right)$. This ensures that as c varies, both the mean and the variance of the degree distribution remains constant, allowing us to focus only on the effect of clustering.

Observe that when $c = 0$, there will be no triangles in the network and its clustering



(a) (b)

Figure 10.2: **The probability of emergence on contact networks with doubly Poisson distribution**. *The network size* n *is* 2×10^5 *and the number of independent experiments for data point is* $15,000$. *Blue plus signs denote the empirical probability of emergence while the red line denotes the theoretical probability of emergence according to our analysis. The brown circles denote the expected epidemic size. (a) We set* $\lambda_s = \lambda_t = \lambda$ *and vary* λ *from* 1 *to* 10. *(b) We set* $\lambda_2 = \lambda/2$ *and* $\lambda_t = \lambda$ *and vary* λ *from* 1 *to* 10. *Our experimental results are in excellent agreement with our theoretical results.*

coefficient will be close to zero, however, when $c = 4$, there will be no single-edges in the network, hence it would consist only of triangles with a clustering coefficient close to one. Put differently, the parameter c controls the level of clustering, as c increases, the clustering coefficient of the network also increases. In Figure 10.3, we consider three different values for the parameter c, namely, $c = 0.01$, $c = 2.00$, and $c = 3.99$, respectively to illustrate the impact of the clustering coefficient on the probability of emergence and the epidemic threshold. Our results reveal that high clustering i) increases the threshold of epidemics and ii) reduces the probability of emergence around the transition point. These conclusions are in the same vein with the ones given in [168] for clustered networks.

10.6 Conclusion

In this chapter, we investigated the propagation of spreading processes governed by the multiple-strain model on random graphs with clustering. We presented a mathematical theory that ac-

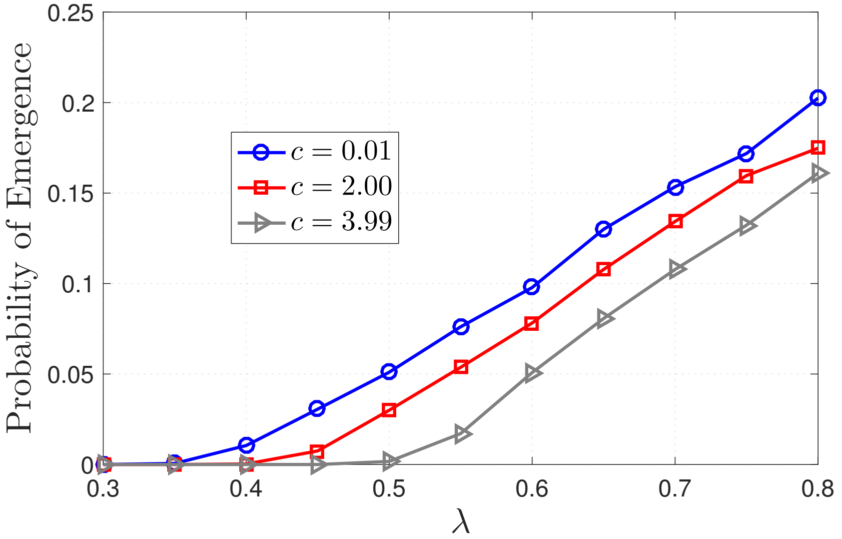


Figure 10.3: **The impact of clustering**. *The network size* n *is* 2×10^5 *and the number of independent experiments for data point is* 10^4*. Blue circles, red squares, and gray triangles denote the empirical probability of emergence when* $c = 0.01$*,* $c = 2.00$*, and* $c = 3.99$*, respectively. Our experimental results show that high clustering increases the threshold of epidemics and reduces the probability of emergence around the transition point.*

curately predicts the threshold and probability of epidemics as functions of i) the structure of the underlying network (as given by the joint degree distribution of single edges and triangles), the characteristics of the spreading process (as given by the matrix $\boldsymbol{T}$), and the evolutionary pathways of the underlying pathogen/information (as given by $\boldsymbol{\mu}$). Our theoretical results were complemented with numerical results on synthetic networks to confirm their validity and reveal the impact of clustering on the threshold and probability of epidemics. It was shown that high clustering increases the epidemic threshold and lowers the probability of emergence around the phase transition point.

Part IV

Concluding Remarks and Future Work

Chapter 11

Concluding Remarks

In this thesis, we have focused on two specific application areas of random graph theory, namely, i) modeling secure connectivity of large-scale wireless sensor networks utilizing random predistribution of cryptographic keys, and ii) modeling real-world social networks. Since each application area poses its unique research problems, we tackled each of them separately. In the first part of the thesis, we focused on the former area and proposed several inhomogeneous random graphs to model the secure connectivity of large-scale wireless sensor networks. In particular, we proposed a novel composite random graph obtained by the intersection of *inhomogeneous* random key graphs with Erdős-Rényi graphs as a model for a large scale wireless sensor network secured by the heterogeneous random key predistribution scheme under a *uniform* on-off channel model. We derived scaling conditions on the model parameters so that with high probability i) the network has no isolated nodes, ii) is connected, iii) the minimum node degree is no less than k, and iv) the network is k-connected. We then proceeded by considering a more realistic channel model, namely, the *heterogeneous* on-off channel model where the wireless link availability between two nodes is determined based on their respective classes. This led to a novel composite random graph model formed by the intersection of *inhomogeneous* random key graphs with *inhomogeneous* Erdős-Rényi graphs. We derived scaling conditions on the model parameters such that with high probability i) the network has no isolated nodes, and ii) is connected. Finally, we proposed *inhomogeneous* random K-out graphs as a novel modeling framework for secure connectivity of large-scale wireless sensor networks secured by a heterogeneous variant of the *random pairwise key predistribution scheme.* We investigated the connectivity of the model and presented the conditions needed to make the graph connected.

In the second part of the thesis, we looked at random graphs as models for real-world social networks. We utilized existing random graph models of social networks in order to investigate the propagation of spreading processes that entail evolutionary adaptations in social contexts. We considered the propagation of *inhomogeneous* spreading processes, governed by the multiple-strain model, on contact networks modeled by i) random graphs with arbitrary degree distributions (generated by the configuration model) and ii) random graphs with clustering. In the context of the former model, we proposed a mathematical theory that characterized the expected epidemic size and the epidemic threshold as functions of the structure of the underlying contact network, the properties of the spreading process, and the evolutionary pathways of the propagating object. Extensive simulation results on synthetic and real-world contact networks were performed to validate our theory and reveal the significant shortcomings of the classical epidemic models that do not capture evolutionary adaptations. In the context of the latter model, we proposed a mathematical theory that accurately captures the probability of emergence (the probability that the spreading process would eventually reach a positive fraction of the nodes) and the epidemic threshold as functions of the structure of the underlying contact network (which takes clustering into consideration), the properties of the spreading process, and the evolutionary pathways of the propagating object. Our theoretical results were validated by a simulation study that also revealed the impact of clustering on the probability of emergence and the epidemic threshold.

A common takeaway from both parts of the thesis is that **homogeneous models are more resource-efficient than their inhomogeneous counterparts**, despite the fact that the latter facilitate a broader modeling framework that accurately captures real-world networks and spreading processes.

Chapter 12

Future Work

There are many open directions for future work. In the context of the first application area, namely, modeling secure connectivity of large-scale wireless sensor networks, it would be interesting to analyze the minimum node degree and k-connectivity properties of inhomogeneous random key graphs intersecting inhomogeneous Erdős-Rényi graphs. The k-connectivity property provides reliability guarantees against the failure of some nodes and links and it also implies that any $k-1$ sensors are free to move around without causing the network to be disconnected. Indeed, such results would provide guidelines on how to dimension the parameters of the heterogeneous random key predistribution scheme such that the resulting wireless sensor networks is connected and reliable in the presence of the heterogeneous on-off channel model.

We have investigated the connectivity of inhomogeneous random K-out graphs under full-visibility, yet the full-visibility assumption is too optimistic and is not likely to hold in real-world where the wireless media is often unreliable. Hence, it would be interesting to investigate the connectivity of inhomogeneous random K-out graphs under the uniform and heterogeneous on-off channel models. The former would amount to the intersection of inhomogeneous random K-out graphs with Erdős-Rényi graphs, while the latter would amount to the intersection of inhomogeneous random K-out graphs with inhomogeneous Erdős-Rényi graphs. The overall model would then provide accurate guidelines on how to design the parameters of the underlying random pairwise scheme to achieve secure connectivity in the presence of unreliable wireless media.

Another future direction is to investigate the minimum node degree and k-connectivity properties of inhomogeneous random K-out graphs. This would be essential in order to design secure wireless sensor networks (in the context of random pairwise scheme) that are not only connected but also reliable against the failure of some nodes and links. In fact, such a study has already been carried out in [137]. Finally, it would be interesting to propose a variant of inhomogeneous random K-out graphs where two nodes u and v are adjacent if u selects v *and* v selects u. This model would be more realistic in social contexts where two individuals are considered friends if they *both* choose to befriend one another.

In the context of the second application area, namely, the role of random graphs in modeling real-world social networks, it would be interesting to obtain real-world data that captures the actual progression of a pathogen/information and the evolutionary adaptations that have occurred throughout the propagation. Such a dataset would allow us to investigate how far off the predictions of the multiple- strain model are from the actual spreading phenomenon.

In order to accurately model real-world social networks, it would be useful to consider the propagation of spreading processes governed by the multiple-strain model in *clustered, multi-layer* networks. Since people interact with each other in multiple contexts, e.g., work, school, neighborhood, etc., we could model each context as a layer in a multi-layer network that captures the contact patterns among individuals in multiple contexts. Since social networks are known to be highly clustered, we could also generate the layers in such a way that some (or all) of the layers are clustered. Such a network model is indeed more realistic than the single-layer model presented in this thesis. Hence, it would better resemble real-world social networks.

Bibliography

[1] Lada A. Adamic, Thomas M. Lento, Eytan Adar, and Pauline C. Ng. Information evolution in social networks. In *ACM WSDM 2016*, pages 473–482.

[2] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114, Aug 2002.

[3] HK Alexander and T Day. Risk factors for the evolutionary emergence of pathogens. *Journal of The Royal Society Interface*, 7(51):1455–1474, 2010.

[4] Samuel Alizon, Jacobus C de Roode, and Yannis Michalakis. Multiple infections and the evolution of virulence. *Ecology letters*, 16(4):556–567, 2013.

[5] Linda JS Allen, Fred Brauer, Pauline Van den Driessche, and Jianhong Wu. *Mathematical epidemiology*, volume 1945. Springer, 2008.

[6] Roy M Anderson, Robert M May, and B Anderson. *Infectious diseases of humans: dynamics and control*, volume 28. Wiley Online Library, 1992.

[7] Rustom Antia, Roland R Regoes, Jacob C Koella, and Carl T Bergstrom. The role of evolution in the emergence of infectious diseases. *Nature*, 426(6967):658, 2003.

[8] N. Azimi-Tafreshi. Cooperative epidemics on multiplex networks. *Phys. Rev. E*, 93:042303, Apr 2016.

[9] Oliver Balmer and Marcel Tanner. Prevalence and implications of multiple-strain infections. *The Lancet infectious diseases*, 11(11):868–878, 2011.

[10] Justin Balthrop, Stephanie Forrest, Mark EJ Newman, and Matthew M Williamson. Technological networks and the spread of computer viruses. *Science*, 304(5670):527–529, 2004.

[11] Shweta Bansal, Bryan T Grenfell, and Lauren Ancel Meyers. When individual behaviour matters: homogeneous and network models in epidemiology. *Journal of the Royal Society Interface*, 4(16):879–891, 2007.

[12] Albert-László Barabási. *Network science*. Cambridge university press, 2016.

[13] Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *science*, 286(5439):509–512, 1999.

[14] Albert-László Barabási and Eric Bonabeau. Scale-free networks. *Scientific american*, 288(5):60–69, 2003.

[15] Simon R Blackburn and Stefanie Gerke. Connectivity of the uniform random intersection graph. *Discrete Mathematics*, 309(16):5130–5140, 2009.

[16] M. Bloznelis, J. Jaworski, and K. Rybarczyk. Component evolution in a secure wireless sensor network. *Netw.*, 53:19–26, 2009.

[17] Stefano Boccaletti, Vito Latora, Yamir Moreno, Martin Chavez, and D-U Hwang. Complex networks: Structure and dynamics. *Physics reports*, 424(4-5):175–308, 2006.

[18] Béla Bollobás. *Random graphs*, volume 73. Cambridge university press, 2001.

[19] Béla Bollobás, Svante Janson, and Oliver Riordan. The phase transition in inhomogeneous random graphs. *Random Structures & Algorithms*, 31(1):3–122, 2007.

[20] Fred Brauer, Carlos Castillo-Chavez, and Carlos Castillo-Chavez. *Mathematical models in population biology and epidemiology*, volume 1. Springer, 2012.

[21] Weiran Cai, Li Chen, Fakhteh Ghanbarnejad, and Peter Grassberger. Avalanche outbreaks emerging in cooperative contagions. *Nature physics*, 11(11):936, 2015.

[22] Seyit A Çamtepe and Bülent Yener. Key distribution mechanisms for wireless sensor networks: a survey. *Rensselaer Polytechnic Institute, Troy, New York, Technical Report*, pages 05–07, 2005.

[23] Frank Cézilly, Marie-Jeanne Perrot-Minnot, and Thierry Rigaud. Cooperation and conflict in host manipulation: interactions among macro-parasites and micro-organisms. *Frontiers in microbiology*, 5:248, 2014.

[24] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In *Proc. of IEEE S&P 2003*.

[25] Ted Cohen, Paul D van Helden, Douglas Wilson, Caroline Colijn, Megan M McLaughlin, Ibrahim Abubakar, and Robin M Warren. Mixed-strain mycobacterium tuberculosis infections and the implications for tuberculosis treatment and control. *Clinical microbiology reviews*, 25(4):708–719, 2012.

[26] Gabor Csardi and Tamas Nepusz. The igraph software package for complex network research. *InterJournal*, Complex Systems:1695, 2006.

[27] Peng-Bi Cui, Francesca Colaiori, and Claudio Castellano. Mutually cooperative epidemics on power-law networks. *Phys. Rev. E*, 96:022301, Aug 2017.

[28] Peter Daszak, Lee Berger, Andrew A Cunningham, Alex D Hyatt, D Earl Green, and Rick Speare. Emerging infectious diseases and amphibian population declines. *Emerging infectious diseases*, 5(6):735, 1999.

[29] Richard Dawkins. *The selfish gene.* Oxford university press, 2016.

[30] Manlio De Domenico, Antonio Lima, Paul Mougel, and Mirco Musolesi. The anatomy of a scientific rumor. *Scientific reports*, 3:2980, 2013.

[31] Jacobus C de Roode, Michelle EH Helinski, M Ali Anwar, and Andrew F Read. Dynamics of multiple infection and within-host competition in genetically diverse malaria infections. *The American Naturalist*, 166(5):531–542, 2005.

[32] Luc Devroye and Nicolas Fraiman. Connectivity of inhomogeneous random graphs. *Random Structures & Algorithms*, 45(3):408–420, 2014.

[33] Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei, Alessandro Panconesi, and Jaikumar Radhakrishnan. Redoubtable sensor networks. *ACM Trans. Inf. Syst. Secur.*, 11(3), Mar 2008.

[34] Odo Diekmann and Johan Andre Peter Heesterbeek. *Mathematical epidemiology of infectious diseases: model building, analysis and interpretation*, volume 5. John Wiley & Sons, 2000.

[35] Peter Sheridan Dodds and Duncan J Watts. Universal behavior in a generalized model of contagion. *Phys. Rev. Letters*, 92(21):218701, 2004.

[36] Danny Dolev. The byzantine generals strike again. 1981.

[37] Wenliang Du, Jing Deng, Yunghsiang S Han, Shigang Chen, and Pramod K Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In *IEEE INFOCOM 2004*, volume 1. IEEE, 2004.

[38] Xiaojiang Du, Yang Xiao, Mohsen Guizani, and Hsiao-Hwa Chen. An effective key management scheme for heterogeneous sensor networks. *Ad Hoc Networks*, 5(1):24 – 34, 2007.

[39] Rick Durrett. Some features of the spread of epidemics and information on a random graph. *Proceedings of the National Academy of Sciences*, 107(10):4491–4498, 2010.

[40] Holger Ebel, Lutz-Ingo Mielsch, and Stefan Bornholdt. Scale-free topology of e-mail networks. *Physical review E*, 66(3):035103, 2002.

[41] R. Eletreby and O. Yağan. Connectivity of inhomogeneous random key graphs intersecting inhomogeneous Erdős-Rényi graphs. In *Proc. of IEEE ISIT 2017*, June.

[42] R. Eletreby and O. Yağan. k-connectivity of inhomogeneous random key graphs with unreliable links. *IEEE Transactions on Information Theory*, pages 1–1, 2019.

[43] R. Eletreby and O. Yağan. k-connectivity of inhomogeneous random key graphs with unreliable links. *IEEE Transactions on Information Theory*, pages 1–1, 2019.

[44] Rashad Eletreby and Osman Yağan. Minimum node degree in inhomogeneous random key graphs with unreliable links. In *Information Theory (ISIT), 2016 IEEE International Symposium on*, pages 2464–2468. IEEE, 2016.

[45] Rashad Eletreby and Osman Yağan. Secure and reliable connectivity in heterogeneous wireless sensor networks. In *Information Theory (ISIT), 2017 IEEE International Symposium on*, pages 2880–2884. IEEE, 2017.

[46] Rashad Eletreby and Osman Yağan. On the connectivity of inhomogeneous random k-out graphs. Full version available online at `https://www.andrew.cmu.edu/user/reletreb/papers/isit2019full.pdf`.

[47] Rashad Eletreby and Osman Yağan. On the network reliability problem of the heterogeneous key predistribution scheme. In *Proc. of IEEE CDC 2016*, pages 13–18, Dec.

[48] Rashad Eletreby and Osman Yağan. Node isolation of secure wireless sensor networks under a heterogeneous channel model. In *54th Annual Allerton Conference on Communications, Control and Computing*, October 2016.

[49] Rashad Eletreby and Osman Yağan. Connectivity of inhomogeneous random K-out graphs. *ArXiv e-prints*, June 2018.

[50] Rashad Eletreby and Osman Yağan. Connectivity of wireless sensor networks secured by heterogeneous key predistribution under an on/off channel model. *IEEE Transactions on Control of Network Systems*, 2018.

[51] Rashad Eletreby and Osman Yağan. Connectivity of wireless sensor networks secured by the heterogeneous random pairwise key predistribution scheme. In *Proc. of IEEE CDC 2018*, Dec 2018.

[52] P. Erdős and A. Rényi. On random graphs, I. *Publicationes Mathematicae (Debrecen)*, 6:290–297, 1959.

[53] Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In *Proc. of ACM CCS 2002*, pages 41–47.

[54] Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bhargava, Andrew Miller, and Pramod Viswanath. Dandelion++: Lightweight cryptocurrency networking with formal anonymity guarantees. *Proc. ACM Meas. Anal. Comput. Syst.*, 2(2):29:1–29:35, June 2018.

[55] T. I. Fenner and A. M. Frieze. On the connectivity of randomm-orientable graphs and digraphs. *Combinatorica*, 2(4):347–359, Dec 1982.

[56] Christophe Fraser, Steven Riley, Roy M Anderson, and Neil M Ferguson. Factors that make an infectious disease outbreak controllable. *Proceedings of the National Academy of Sciences of the United States of America*, 101(16):6146–6151, 2004.

[57] Linton C Freeman. Some antecedents of social network analysis. *Connections*, 19(1):39–42, 1996.

[58] Deepak Ganesan, Ramesh Govindan, Scott Shenker, and Deborah Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5:11–25, October 2001.

[59] E. N. Gilbert. Random graphs. *Ann. Math. Statist.*, 30(4):1141–1144, 12 1959.

[60] James P. Gleeson. Cascades on correlated and modular random networks. *Phys. Rev. E*, 77:046117, Apr 2008.

[61] James P. Gleeson and Diarmuid J. Cahalane. Seed size strongly affects cascades on random networks. *Phys. Rev. E*, 75:056103, May 2007.

[62] E Godehardt and J Jaworski. Two models of random intersection graphs for classification. In *Exploratory data analysis in empirical research*, pages 67–81. Springer, 2003.

[63] Chaitanya S Gokhale, Yoh Iwasa, Martin A Nowak, and Arne Traulsen. The pace of evolution across fitness valleys. *Journal of Theoretical Biology*, 259(3):613–620, 2009.

[64] Anna Goldenberg, Alice X Zheng, Stephen E Fienberg, Edoardo M Airoldi, et al. A survey of statistical network models. *Foundations and Trends in Machine Learning*, 2(2):129–233, 2010.

[65] Clara Granell, Sergio Gómez, and Alex Arenas. Competing spreading processes on multiplex networks: awareness and epidemics. *Phys. Rev. E*, 90(1):012808, 2014.

[66] Peter Grassberger, Li Chen, Fakhteh Ghanbarnejad, and Weiran Cai. Phase transitions in cooperative coinfections: Simulation results for networks and lattices. *Phys. Rev. E*, 93:042316, Apr 2016.

[67] Bryan T Grenfell, Oliver G Pybus, Julia R Gog, James LN Wood, Janet M Daly, Jenny A Mumford, and Edward C Holmes. Unifying the epidemiological and evolutionary dynamics of pathogens. *science*, 303(5656):327–332, 2004.

[68] Piyush Gupta and Panganamala R Kumar. Critical power for asymptotic connectivity in wireless networks. In *Stochastic analysis, control, optimization and applications*, pages 547–566. Springer, 1999.

[69] Patsy Haccou, Patricia Haccou, Peter Jagers, Vladimir A Vatutin, and Vladimir A Vatutin. *Branching processes: variation, growth, and extinction of populations*. Number 5. Cambridge university press, 2005.

[70] Adam Hackett, Sergey Melnik, and James P Gleeson. Cascades on a class of clustered random networks. *Physical Review E*, 83(5):056107, 2011.

[71] Liang Huang, Kwangho Park, and Ying-Cheng Lai. Information propagation on modular networks. *Phys. Rev. E*, 73(3):035103, 2006.

[72] Xuqing Huang, Shuai Shao, Huijuan Wang, Sergey V Buldyrev, H Eugene Stanley, and Shlomo Havlin. The robustness of interdependent clustered networks. *EPL (Europhysics Letters)*, 101(1):18002, 2013.

[73] Svante Janson, Tomasz Łuczak, and Andrzej Ruciński. Random graphs. *Wiley–Intersci. Ser. Discrete Math. Optim*, 2000.

[74] Shane Tyler Jensen. *The Laguerre-Samuelson inequality with extensions and applications in statistics and matrix theory*. PhD thesis, Department of Mathematics and Statistics, McGill University, 1999.

[75] Kate E Jones, Nikkita G Patel, Marc A Levy, Adam Storeygard, Deborah Balk, John L Gittleman, and Peter Daszak. Global trends in emerging infectious diseases. *Nature*, 451(7181):990, 2008.

[76] Matt J Keeling and Ken TD Eames. Networks and epidemic models. *Journal of the Royal Society Interface*, 2(4):295–307, 2005.

[77] Matt J Keeling and Pejman Rohani. *Modeling infectious diseases in humans and animals*. Princeton University Press, 2011.

[78] Eben Kenah and James M Robins. Second look at the spread of epidemics on networks. *Phys. Rev. E*, 76(3):036113, 2007.

[79] Mark S Klempner and Daniel S Shapiro. Crossing the species barrier–one small step to man, one giant leap to mankind. *New England Journal of Medicine*, 350(12):1171–1172, 2004.

[80] R. J. La and E. Seo. Network connectivity with a family of group mobility models. *IEEE Transactions on Mobile Computing*, 11(3):504–517, March 2012.

[81] Sandra Lass, Peter J Hudson, Juilee Thakar, Jasmina Saric, Eric Harvill, Réka Albert, and Sarah E Perkins. Generating super-shedders: co-infection increases bacterial load and egg production of a gastrointestinal helminth. *Journal of the Royal Society Interface*, 10(80):20120588, 2013.

[82] EA Leicht and Raissa M D'Souza. Percolation on interacting networks. *arXiv preprint arXiv:0907.0894*, 2009.

[83] Jure Leskovec and Andrej Krevl. SNAP Datasets: Stanford large network dataset collection. `http://snap.stanford.edu/data`, June 2014.

[84] Jure Leskovec, Kevin J Lang, Anirban Dasgupta, and Michael W Mahoney. Community structure in large networks: Natural cluster sizes and the absence of large well-defined clusters. *Internet Mathematics*, 6(1):29–123, 2009.

[85] Jure Leskovec and Julian J Mcauley. Learning to discover social circles in ego networks. In *Advances in neural information processing systems*, pages 539–547, 2012.

[86] Gabriel E Leventhal, Alison L Hill, Martin A Nowak, and Sebastian Bonhoeffer. Evolution and emergence of infectious diseases in theoretical and real-world networks. *Nature communications*, 6:6101, 2015.

[87] X. Li, P. Wan, Y. Wang, and C. Yi. Fault tolerant deployment and topology control in wireless networks. In *Proc. of ACM MobiHoc*, 2003.

[88] Donggang Liu, Peng Ning, and Rongfang Li. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(1):41–77, 2005.

[89] James O Lloyd-Smith, Sebastian J Schreiber, P Ekkehard Kopp, and Wayne M Getz. Superspreading and the effect of individual variation on disease emergence. *Nature*, 438(7066):355, 2005.

[90] CC Lord, B Barnard, K Day, JW Hargrove, JJ McNamara, REL Paul, K Trenholme, and MEJ Woolhouse. Aggregation and distribution of strains in microparasites. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 354(1384):799–807, 1999.

[91] K. Lu, Y. Qian, M. Guizani, and H. Chen. A framework for a distributed key management scheme in heterogeneous wireless sensor networks. *IEEE Transactions on Wireless Communications*, 7(2):639–647, February 2008.

[92] Alan Mainwaring, David Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 88–97. ACM, 2002.

[93] George E Martin. *Counting: The art of enumerative combinatorics*. Springer Science & Business Media, 2013.

[94] Miller McPherson, Lynn Smith-Lovin, and James M Cook. Birds of a feather: Homophily in social networks. *Annual review of sociology*, 27(1):415–444, 2001.

[95] Alessandro Mei, Alessandro Panconesi, and Jaikumar Radhakrishnan. Unassailable sensor networks. In *Proc. of SecureComm 2008*, New York, NY, USA, 2008. ACM.

[96] Lauren Meyers. Contact network epidemiology: Bond percolation applied to infectious disease prediction and control. *Bulletin of the American Mathematical Society*, 44(1):63–86, 2007.

[97] Joel C Miller. Percolation and epidemics in random clustered networks. *Physical Review E*, 80(2):020901, 2009.

[98] Joel C Miller and Istvan Z Kiss. Epidemic spread in networks: Existing methods and current challenges. *Mathematical modelling of natural phenomena*, 9(2):4–42, 2014.

[99] Charles J Mode. *Multitype branching processes: theory and applications*, volume 34. American Elsevier Pub. Co., 1971.

[100] Michael Molloy and Bruce Reed. A critical point for random graphs with a given degree sequence. *Random Structures & Algorithms*, 6(2-3):161–180, 1995.

[101] Cristopher Moore and Mark EJ Newman. Exact solution of site and bond percolation on small-world networks. *Phys. Rev. E*, 62(5):7059, 2000.

[102] Yamir Moreno, Maziar Nekovee, and Amalio F Pacheco. Dynamics of rumor spreading in complex networks. *Phys. Rev. E*, 69(6):066130, 2004.

[103] Yamir Moreno, Romualdo Pastor-Satorras, and Alessandro Vespignani. Epidemic outbreaks in complex heterogeneous networks. *The European Physical Journal B-Condensed Matter and Complex Systems*, 26(4):521–529, 2002.

[104] David M Morens, Gregory K Folkers, and Anthony S Fauci. The challenge of emerging and re-emerging infectious diseases. *Nature*, 430(6996):242, 2004.

[105] Stephen S Morse, Jonna AK Mazet, Mark Woolhouse, Colin R Parrish, Dennis Carroll, William B Karesh, Carlos Zambrana-Torrelio, W Ian Lipkin, and Peter Daszak. Prediction and prevention of the next pandemic zoonosis. *The Lancet*, 380(9857):1956 – 1965, 2012.

[106] Stephen S Morse, Jonna AK Mazet, Mark Woolhouse, Colin R Parrish, Dennis Carroll, William B Karesh, Carlos Zambrana-Torrelio, W Ian Lipkin, and Peter Daszak. Predic-

tion and prevention of the next pandemic zoonosis. *The Lancet*, 380(9857):1956–1965, 2012.

[107] Lenore Newman and Ann Dale. Homophily and agency: creating effective sustainable development networks. *Environment, development and sustainability*, 9(1):79–90, 2007.

[108] M. E. J. Newman. Spread of epidemic disease on networks. *Phys. Rev. E*, 66:016128, Jul 2002.

[109] M. E. J. Newman. Random graphs with clustering. *Phys. Rev. Lett.*, 103:058701, Jul 2009.

[110] Mark EJ Newman. The structure of scientific collaboration networks. *Proceedings of the national academy of sciences*, 98(2):404–409, 2001.

[111] Mark EJ Newman. Spread of epidemic disease on networks. *Phys. Rev. E*, 66(1):016128, 2002.

[112] Mark EJ Newman. The structure and function of complex networks. *SIAM review*, 45(2):167–256, 2003.

[113] Mark EJ Newman. Mathematics of networks. *The new Palgrave dictionary of economics*, pages 1–8, 2016.

[114] Mark EJ Newman, Stephanie Forrest, and Justin Balthrop. Email networks and the spread of computer viruses. *Phys. Rev. E*, 66(3):035101, 2002.

[115] Mark EJ Newman, Steven H Strogatz, and Duncan J Watts. Random graphs with arbitrary degree distributions and their applications. *Phys. Rev. E*, 64(2):026118, 2001.

[116] Mark EJ Newman, Duncan J Watts, and Steven H Strogatz. Random graph models of social networks. *Proceedings of the National Academy of Sciences*, 99(suppl 1):2566–2572, 2002.

[117] World Health Organization. `http://www.who.int/topics/zoonoses/en/`.

[118] Colin R Parrish, Edward C Holmes, David M Morens, Eun-Chung Park, Donald S Burke, Charles H Calisher, Catherine A Laughlin, Linda J Saif, and Peter Daszak. Cross-species virus transmission and the emergence of new epidemic diseases. *Microbiology and Molecular Biology Reviews*, 72(3):457–470, 2008.

[119] Romualdo Pastor-Satorras, Claudio Castellano, Piet Van Mieghem, and Alessandro Vespignani. Epidemic processes in complex networks. *Reviews of modern physics*, 87(3):925, 2015.

[120] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic dynamics and endemic states in complex networks. *Phys. Rev. E*, 63(6):066117, 2001.

[121] M. D. Penrose. *Random Geometric Graphs*. Oxford University Press, July 2003.

[122] Mathew D Penrose et al. Connectivity of soft random geometric graphs. *The Annals of Applied Probability*, 26(2):986–1028, 2016.

[123] Karin S Pfennig. Evolution of pathogen virulence: the role of variation in host phenotype. *Proceedings of the Royal Society of London B: Biological Sciences*, 268(1468):755–760, 2001.

[124] Dajun Qian, Osman Yağan, Lei Yang, and Junshan Zhang. Diffusion of real-time information in social-physical networks. In *IEEE GLOBECOM 2012*, pages 2072–2077.

[125] C. S. Raghavendra, Krishna M. Sivalingam, and Taieb Znati, editors. *Wireless Sensor Networks*. Kluwer Academic Publishers, 2004.

[126] Andrew F Read and Louise H Taylor. The ecology of genetically diverse infections. *Science*, 292(5519):1099–1102, 2001.

[127] Herbert Robbins. A remark on stirling's formula. *The American mathematical monthly*, 62(1):26–29, 1955.

[128] Katarzyna Rybarczyk. Diameter, connectivity, and phase transition of the uniform random intersection graph. *Discrete Mathematics*, 311(17):1998–2019, 2011.

[129] Katarzyna Rybarczyk. Sharp threshold functions for random intersection graphs via a coupling method. *the electronic journal of combinatorics*, 18(1):P36, 2011.

[130] Faryad Darabi Sahneh, Caterina Scoglio, and Piet Van Mieghem. Generalized epidemic mean-field model for spreading processes over multilayer complex networks. *IEEE/ACM Transactions on Networking*, 21(5):1609–1620, 2013.

[131] Marcel Salathé, Maria Kazandjieva, Jung Woo Lee, Philip Levis, Marcus W. Feldman, and James H. Jones. A high-resolution human contact network for infectious disease transmission. *Proceedings of the National Academy of Sciences*, 107(51):22020–22025, 2010.

[132] M Ángeles Serrano and Marian Boguna. Clustering in complex networks. i. general formalism. *Physical Review E*, 74(5):056114, 2006.

[133] James P. Sethna, Karin Dahmen, Sivan Kartha, James A. Krumhansl, Bruce W. Roberts, and Joel D. Shore. Hysteresis and hierarchies: Dynamics of disorder-driven first-order phase transformations. *Phys. Rev. Lett.*, 70:3347–3350, May 1993.

[134] Elaine Shi and Adrian Perrig. Designing secure sensor networks. *IEEE Wireless Communications*, 11(6):38–43, 2004.

[135] Constantinos I Siettos and Lucia Russo. Mathematical modeling of infectious disease dynamics. *Virulence*, 4(4):295–306, 2013.

[136] Huai-Dong Song, Chang-Chun Tu, Guo-Wei Zhang, Sheng-Yue Wang, Kui Zheng, Lian-Cheng Lei, Qiu-Xia Chen, Yu-Wei Gao, Hui-Qiong Zhou, Hua Xiang, Hua-Jun Zheng, Shur-Wern Wang Chern, Feng Cheng, Chun-Ming Pan, Hua Xuan, Sai-Juan Chen, Hui-Ming Luo, Duan-Hua Zhou, Yu-Fei Liu, Jian-Feng He, Peng-Zhe Qin, Ling-Hui Li, Yu-Qi

Ren, Wen-Jia Liang, Ye-Dong Yu, Larry Anderson, Ming Wang, Rui-Heng Xu, Xin-Wei Wu, Huan-Ying Zheng, Jin-Ding Chen, Guodong Liang, Yang Gao, Ming Liao, Ling Fang, Li-Yun Jiang, Hui Li, Fang Chen, Biao Di, Li-Juan He, Jin-Yan Lin, Suxiang Tong, Xiangang Kong, Lin Du, Pei Hao, Hua Tang, Andrea Bernini, Xiao-Jing Yu, Ottavia Spiga, Zong-Ming Guo, Hai-Yan Pan, Wei-Zhong He, Jean-Claude Manuguerra, Arnaud Fontanet, Antoine Danchin, Neri Niccolai, Yi-Xue Li, Chung-I Wu, and Guo-Ping Zhao. Cross-host evolution of severe acute respiratory syndrome coronavirus in palm civet and human. *Proceedings of the National Academy of Sciences*, 102(7):2430–2435, 2005.

[137] Mansi Sood and Osman Yağan. Towards k-connectivity in heterogeneous sensor networks under pairwise key predistribution. *arXiv preprint arXiv:1907.08049*, 2019.

[138] Frank Stajano and Ross J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proc. of the 7th International Workshop on Security Protocols*, pages 172–194, 2000.

[139] Hanna Susi, Benoit Barrès, Pedro F Vale, and Anna-Liisa Laine. Co-infection alters population dynamics of infectious disease. *Nature communications*, 6:5975, 2015.

[140] Charlotte Tollenaere, Hanna Susi, and Anna-Liisa Laine. Evolutionary and epidemiological implications of multiple infection in plants. *Trends in plant science*, 21(1):80–90, 2016.

[141] Philippe Vanhems, Alain Barrat, Ciro Cattuto, Jean-François Pinton, Nagham Khanafer, Corinne Régis, Byeul-a Kim, Brigitte Comte, and Nicolas Voirin. Estimating potential infection transmission routes in hospital wards using wearable proximity sensors. *PLOS ONE*, 8(9):1–9, 09 2013.

[142] Yong Wang, G. Attebury, and B. Ramamurthy. A survey of security issues in wireless sensor networks. *IEEE Communications Surveys Tutorials*, 8(2):2–23, Second 2006.

[143] Stanley Wasserman, Katherine Faust, et al. *Social network analysis: Methods and applications*, volume 8. Cambridge university press, 1994.

[144] Duncan J Watts and Steven H Strogatz. Collective dynamics of'small-world'networks. *nature*, 393(6684):440, 1998.

[145] Xiping Wei, Sajal K Ghosh, Maria E Taylor, Victoria A Johnson, Emilio A Emini, Paul Deutsch, Jeffrey D Lifson, Sebastian Bonhoeffer, Martin A Nowak, Beatrice H Hahn, et al. Viral dynamics in human immunodeficiency virus type 1 infection. *Nature*, 373(6510):117, 1995.

[146] Nathan D Wolfe, Claire Panosian Dunavan, and Jared Diamond. Origins of major human infectious diseases. *Nature*, 447(7142):279, 2007.

[147] Mark EJ Woolhouse, Daniel T Haydon, and Rustom Antia. Emerging pathogens: the epidemiology and evolution of species jumps. *Trends in ecology & evolution*, 20(5):238–244, 2005.

[148] Chun-Hsien Wu and Yeh-Ching Chung. Heterogeneous wireless sensor network deployment and topology control based on irregular sensor model. In Christophe Cérin and Kuan-Ching Li, editors, *Advances in Grid and Pervasive Computing*, pages 78–88, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[149] Osman Yağan and Virgil Gligor. Analysis of complex contagions in random multiplex networks. *Phys. Rev. E*, 86:036103, Sep 2012.

[150] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh. Exploiting heterogeneity in sensor networks. In *Proc. of IEEE INFOCOM 2005.*

[151] O. Yağan and A. M. Makowski. On the gradual deployment of random pairwise key distribution schemes. In *Proc. of WiOpt 2011*, pages 257–264, May 2011.

[152] O. Yağan and A. M. Makowski. On the connectivity of sensor networks under random pairwise key predistribution. *IEEE Transactions on Information Theory*, 59(9):5754–5762, Sept 2013.

[153] O. Yağan and A. M. Makowski. Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings? *IEEE/ACM Transactions on Networking*, PP(99):1–14, 2016.

[154] O. Yağan and A.M. Makowski. Modeling the pairwise key predistribution scheme in the presence of unreliable links. *Information Theory, IEEE Transactions on*, 59(3):1740–1760, March 2013.

[155] Osman Yağan. *Random Graph Modeling of Key Distribution Scheme in Wireless Sensor Networks.* PhD thesis, University of Maryland, College Park (MD), 2011.

[156] Osman Yağan. Performance of the Eschenauer-Gligor key distribution scheme under an ON/OFF channel. *IEEE Transactions on Information Theory*, 58(6):3821–3835, June 2012.

[157] Osman Yağan. Zero-one laws for connectivity in inhomogeneous random key graphs. *IEEE Transactions on Information Theory*, 62(8):4559–4574, Aug 2016.

[158] Osman Yağan and Virgil Gligor. Analysis of complex contagions in random multiplex networks. *Phys. Rev. E*, 86:036103, Sep 2012.

[159] Osman Yağan and Armand M Makowski. Zero–one laws for connectivity in random key graphs. *IEEE Transactions on Information Theory*, 58(5):2983–2999, 2012.

[160] Osman Yağan, Dajun Qian, Junshan Zhang, and Douglas Cochran. Conjoining speeds up information diffusion in overlaying social-physical networks. *IEEE Journal on Selected Areas in Communications*, 31(6):1038–1048, 2013.

[161] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer networks*, 52(12):2292–2330, 2008.

[162] G Udny Yule et al. Ii.—a mathematical theory of evolution, based on the conclusions of dr. jc willis, fr s. *Phil. Trans. R. Soc. Lond. B*, 213(402-410):21–87, 1925.

[163] Yichao Zhang, Shi Zhou, Zhongzhi Zhang, Jihong Guan, and Shuigeng Zhou. Rumor evolution in social networks. *Phys. Rev. E*, 87(3):032133, 2013.

[164] J. Zhao. Analyzing connectivity of heterogeneous secure sensor networks. *IEEE Transactions on Control of Network Systems*, PP(99):1–1, 2016.

[165] J. Zhao, O. Yağan, and V. Gligor. On connectivity and robustness in random intersection graphs. *IEEE Transactions on Automatic Control*, 62(5):2121–2136, May 2017.

[166] Jun Zhao, O. Yağan, and V. Gligor. k-connectivity in random key graphs with unreliable links. *IEEE Transactions on Information Theory*, 61(7):3810–3836, July 2015.

[167] Jun Zhao, Osman Yağan, and Virgil Gligor. On the strengths of connectivity and robustness in general random intersection graphs. In *Proc. of IEEE CDC 2014*, pages 3661–3668.

[168] Yong Zhuang and Osman Yağan. Information propagation in clustered multilayer networks. *IEEE Transactions on Network Science and Engineering*, 3(4):211–224, 2016.