INVESTIGATING MALWARE PROPAGATION IN WIRELESS IOT/CPS USING STOCHASTIC GEOMETRY AND EPIDEMIOLOGY

BY

MUNZIR ELSAIH MOHAMED

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

TELECOMMUNICATION ENGINEERING

March 2023

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **MUNZIR ELSAIH MOHAMED** under the direction of his thesis adviser and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN TELECOMMUNICATION ENGINEERING**.

Thesis Committee

Dr. Wessam Mesbah (Adviser)

Dr. Hesham ElSawy (Co-Adviser)

Dr. Ali Arshad Nasir (Member)

Dr. Suhail Ibrahim Al-Dharrab (Member)

Dr. Maan Kousa (Member)

Dr. Abdallah S. Al-Ahmari
Department Chairman

Prof. Suliman Al-Homidan
Dean of Graduate Studies

12 March, 2023
Date

To my mom

ACKNOWLEDGMENTS

The author would like to express his deep gratitude to Dr. Hesham ElSawy and Dr. Wessam Mesbah for their invaluable patience and feedback throughout the work on this thesis. The completion of my thesis would not have been possible without their guidance and support. I am also grateful to the deanship of scientific research at KFUPM for their generous support through the Project DF191052.

TABLE OF CONTENTS

ACKNOWLEDGMENTS **vi**

LIST OF TABLES **ix**

LIST OF FIGURES **x**

LIST OF SYMBOLS **xii**

LIST OF ABBREVIATIONS **xiii**

ABSTRACT (ENGLISH) **xiv**

ABSTRACT (ARABIC) **xvi**

CHAPTER 1 INTRODUCTION **1**

1.1 Background 2

1.2 Classical models of epidemic spreading 4

1.3 Network Models 6

1.4 Degree-Based Mean-Field Approach 7

CHAPTER 2 LITERATURE REVIEW AND CONTRIBUTION **10**

CHAPTER 3 MALWARE PROPAGATION IN IOT NETWORKS **13**

3.1 Network Model 14

3.2 Analysis 19

3.2.1 Joint distribution of degrees 22

3.2.2 Patching Rate Optimization 24

3.3 Results and discussion 26

CHAPTER 4 SPATIAL FIREWALLS **35**

4.1 Network Model with Firewalls 36

4.2 Analysis 39

4.2.1 Joint and Marginal Degree Distributions in Firewalls Case . . . 41

4.3 Results and Discussion 47

APPENDIX A PROOFS **55**

A.1 Proof of Lemma 1. 55

A.2 Proof of Lemma 2. 56

A.3 Proof of Lemma 3. 57

APPENDIX B SUPPLEMENTARY MATERIAL **58**

B.1 The areas of X, Y, and Z in firewalls case. 58

REFERENCES **65**

VITAE **69**

LIST OF TABLES

3.1 Parameters of network and optimization 29

LIST OF FIGURES

3.1 A realization of the RGG with degrees color coded. 15

3.2 Illustration of the network model, with a typical device, denoted by device i, having communication range r. D2D links are highlighted by blue lines, and three states are possible: healthy, infected, and informed. 18

3.3 Degree-aware MC for state evolution of a typical IoT device if degree k. 20

3.4 Distinct and common neighborhood regions of two connected devices. . 23

3.5 Empirical Joint degree PMF compared to the Theoretical PMFs with and without considering spatial degree correlation. 27

3.6 Kolmogorov–Smirnov statistic D_n as a function of the number of observations n. 28

3.7 The probability of infection $1 - \theta_k^H$ in case of a uniform patching rate across all degrees. 29

3.8 Impact of spatial degree correlation on the optimal patching rates. . . . 30

3.9 Percentage of Healthy devices vs Time: simulating the infection process with different spreading rates 32

3.10 Percentage of Healthy devices vs Time: simulation of the patching process for a completely infected network 33

3.11 Percentage of Healthy devices vs Time: simulation of the equilibrium state when the patching offsets the infection. 34

4.1 Illustration of IoT ad hoc wireless network with firewalls. IoT devices can either be susceptible, Immune or infected (compromised). 38

4.2 Two realizations of the RGG, (a) without firewalls, and (b) with firewalls. Immune devices and firewalls are highlighted in green and red respectively. 40
4.3 IoT device neighbor to a firewall. The degree of device i is determined by the number of devices in the yellow region since only those will be susceptible 43
4.4 The general case for two connected devices i and j separated by distance $d \leq r$ and neighbor to a close firewall k. The coverage areas of both form two overlapping circles with the same radius r. They can be divided into three disjoint areas which are labeled X,Y and Z. 43
4.5 The different cases of overlap between firewall and devices i and j . . . 46
4.6 Validating the theoretical joint distribution of degrees when firewalls are present. 48
4.7 The impact of spatial firewalls on the distribution of degree (a) increasing the intensity of firewalls λ_f, (b) increasing the range of firewalls r_f. 49
4.8 Impact of firewalls on the optimal patching rates ($\tau_H = 0.6$). 50
4.9 Impact of firewalls on the optimal patching rates ($\tau_H = 0.7$). 51
4.10 Impact of firewalls on the optimal patching rates ($\tau_H = 0.8$). 51
4.11 The impact of varying the design parameters r_f and λ_f on the optimal patching rates: (a) increasing the intensity of firewalls, (b) increasing the range of firewalls 52
4.12 Simulation of the patching strategies of different thresholds: start with a completely infected network. 53
4.13 Simulation of the patching strategy of $\tau_H = 0.7$: start near the threshold τ_H. 54

B.1 Visualization of the general case for the overlap between three circles. . 59

LIST OF SYMBOLS

β	The rate of discarding control commands.
k	The connectivity degree of an IoT device.
λ	The intensity of deploying IoT devices in the network.
λ_f	The intensity of deploying firewalls devices in the network.
μ	The patching rate.
r	The communication range of IoT devices.
r_f	The communication range of firewalls.
σ_1	The spreading rate of the malware.
σ_2	The spreading rate of the control commands.
τ_H	The minimum threshold for healthy devices.
$\tau_{\hat{I}}$	The maximum threshold for informed devices.
θ_k^H	The probability a typical neighbor to a degree k device is healthy.
$\theta_k^{\hat{I}}$	The probability a typical neighbor to a degree k device is informed.

LIST OF ABBREVIATIONS

CDF	Cumulative Distribution Function
D2D	Device-to-Device Connectivity
DBMF	Degree-Based Mean-Field Approach
DDoS	Distributed Denial of Service
IoT	Internet of Things
ISG	Infected Susceptible Graph
KPI	Key Performance Indicator
MC	Markov Chain
PDF	Probability Density Function
PMF	Probability Mass Function
PPP	Poisson Point Process
RGG	Random Geometric Graph
SIR	Susceptible-Infected-Recovered Model
SIS	Susceptible-Infected-Susceptible Model
WANET	Wireless Ad hoc Network

THESIS ABSTRACT

NAME: Munzir Elsaih Mohamed

TITLE OF STUDY: Investigating Malware Propagation in Wireless IoT/CPS Using Stochastic Geometry and Epidemiology.

MAJOR FIELD: Telecommunication Engineering

DATE OF DEGREE: March, 2023

Due to cost constraints, security countermeasures are usually overlooked in Internet of Things (IoT) devices, which create several loopholes for malicious software (malware) attacks. Even worse, malware worms can exploit direct device-to-device connectivity to stealthily spread among many IoT devices creating a malware epidemic. Compromising many IoT devices, each denoted as a bot, creates a botnet that can be exploited by adversaries to launch large-scale attacks with cyber (e.g., denial of service and ransomware) and physical (e.g., equipment sabotage and electrical blackout) consequences. Randomized patching is a viable and cost-effective countermeasure to thwart large-scale botnet formation in IoT. However, the optimal patching rate should be sought to balance the trade-off between network operation and security. In this thesis, we aim to account for the intrinsic spatial degree (i.e., number of directly connected neighbors)

correlation among the IoT devices in the patching rate optimization problem. Numerical results show that overlooking the degree correlation deteriorates network security and violates operational constraints. Moreover, spatial firewalls are high-end wireless devices that can be used to immunize groups of devices in proximity to each other. In this thesis, we study the effect of deploying spatial firewalls on the optimal patching rates. The results show that deploying firewalls leads to a general decrease in the optimal patching rates over all degrees and the patching becomes more concentrated on the lower-degree devices.

ملخص الرسالة

الاسم: منذر السائح أبوعبيدة محمد

عنوان الدراسة: دراسة تفشي الفيروسات في شبكة انترنت الأشياء بإستخدام نماذج الجائحة المرضية.

التخصص: هندسة الإتصالات

تاريخ الدرجة العلمية: شعبان، 1444

نظرا لأسباب إقتصادية، قد يهمل المصنعون الإهتمام بالأمان السيبرياني في شبكة إنترنت الأشياء مما قد يؤدي إلى وجود نقاط ضعف في الشبكة تمكن المخترقين من مهاجمة الشبكة وإحداث أضرار جسيمة في البرمجيات و الأجهزة الإلكترونية. ومما يضاعف المشكلة سوءا هو استخدام التواصل اللاسلكي المباشر بين أجهزة الشبكة من غير خادم وسيط، وهذا يمكن الفيروس المستخدم من قبل المخترق من الإنتقال من جهاز لآخر محدثا ما يمكن تشبيهه بالجائحة المرضية في الشبكة. الأجهزة التي يتم إختراقها تكون شبكة فيما بينها وتستطيع مهاجمة الشبكة عن طريق ما يعرف بهجمة "حجب الخدمة" حيث تقوم شبكة الأجهزة المخترقة بإحداث سيل من المعلومات الغير مفيدة في الشبكة مما يسنفد قدرة الخادم ويعطله عن تلقي الطلبات وتلبيتها. يلجئ مشغل الشبكة إلى القيام بإصلاحات دورية للأجهزة لضمان عدم تفشي فيروسات في الشبكة ولكن هذه الإصلاحات الدورية تعطل عمل الشبكة الأساسي لذلك يجب موازنة الأمان في الشبكة مع قدرتها على القيام بوظائفها. إيجاد معدل تكرار الإصلاحات الدورية في الشبكة الذي يوازن بين الأمان و الفعالية تعتبر مشكلة استمثال (تحسين) تتطلب النظر في درجة اتصال الجهاز المتمثلة بعدد الأجهزة المجاورة له، قبل وضع المعدل المناسب له. درجة اتصال الجهاز يمكن تمثيلها بمتغير عشوائي، ,وفي هذه الرسالة قمنا بإيجاد التوزيع (دالة الكثافة الإحتمالية) لهذا المتغير. توصلنا في هذا البحث إلى أن درجات الإتصال للأجهزة المتجاورة تكون مترابطة مع بعضها أي أن الأجهزة ذات الدرجة العالية تكون مجاورة لأجهزة ذات درجة عالية أيضا ،وهذا يجب أخذه في الحسبان عندما نوجد نموذج وديناميكية تفشي الفيروس في الشبكة. المساهمة البحثية الثانية هي أننا درسنا تأثير وضع أجهزة جدار الحماية على ديناميكية تفشي الفيروس و تأثيرها على معدل الإصلاح الدوري للأجهزة الغير محصنة. تقوم أجهزة جدار الحماية بالتواصل مع الأجهزة المجارة لعمل مسح والتحقق من خلوها من البرمجيات الخبيثة، وبهذه الطريقة يمكن تحصين عدة أجهزة

في الشبكة بطريقة اقتصادية وغير مكلفة. وجود أجهزة جدار الحماية في الشبكة يؤدي إلى تقليل معدل الإصلاح الدوري للأجهزة المعرضة للخطر. استنتجنا أيضا أن المعدل الدوري للإصلاح يكون مركزا أكثر على الأجهزة ذات الدرجة الأدنى عندما تكون أجهزة جدار الحماية موجودة في الشبكة وذلك لأن أجهزة جدار الحماية تؤثر على توزيع الدرجات (دالة الكثافة الإحتمالية للدرجات) بجعل الدرجات الأدنى أكثر إحتمالية في الشبكة.

CHAPTER 1

INTRODUCTION

Internet of Things (IoT) describes a network of smart objects with embedded sensors, actuators, microprocessors, and wireless interfaces, which is foreseen to have many applications in our life [1] (e.g., home automation, the industrial revolution, e-health, smart cities, retail, etc.). Usually, IoT devices connect to the internet through access points but they can connect to each other directly via Wi-Fi, ZigBee, or Bluetooth. This creates a huge wireless ad hoc network (WANET) comprising sensors and actuators. Due to the cost and time-to-manufacture constraints, IoT devices might lack many security aspects making them vulnerable to malicious software (malware) attacks. Other vulnerability factors are the lack of security regulations, consumers' malpractices, and unawareness of cyber risks. In the IoT era, the risk of compromised IoT devices, denoted as bots, extends from the cyber domain to the physical world [2]. For instance, compromised robot arms can injure workers, compromised traffic lights can lead to collisions, and compromised switchgears can lead to electrical outages. Exploiting direct device-to-device (D2D) connectivity, the IoT risk becomes more threatening as adversaries can get control over several bots, denoted as a botnet.

In particular, malware worms can stealthily transfer from one IoT device to another creating a malware epidemic in large-scale wireless ad hoc networks [3], which enables adversaries to launch large-scale distributed attacks and terrorist actions that threaten national security.

1.1 Background

The threat from botnets has become increasingly evident in the last decade. A botnet is a network of compromised devices controlled by an external attacker denoted as the botmaster. The main goal of the botnet is to create a disturbance in the network traffic, which leads to disruption of the network operation. From the attacker's point of view, such attacks can also be used to obtain ransom or compromise sensitive data. The Mirai in 2016 and Colonial Pipeline attack in June 2021 have been the most popular botnet attacks in recent history [4], [5]. Newly identified variants of the Mirai botnet (IoTroop, Reaper) have been used to target IoT devices and launch Distributed-Denial-of-Service (DDoS) attacks [6]. For instance, it can compromise vulnerable wireless routers and security cameras. For the case of wireless networks, the botnet formation process starts by infecting some devices, which then act as seeds for the malware propagation in the network [7], [8], [9], [10]. One possible way to accomplish the initial infection is using an unmanned aerial vehicle (UAV). As the malware propagates, more bots join the botnet waiting for commands to launch an attack. The control commands are usually dispatched by the botmaster, and propagate in a similar way to the malware [11]. In wireless networks, the propagation rates of the malware as well as the control commands depend on the density, relative locations, status (i.e., immune, susceptible, or compromised), and communications ranges of the IoT devices [7]. The foreseen massive numbers of IoT devices not only facilitate the propagation of malware and attack-related control commands but also make it hard to identify and localize compromised devices (i.e., bots). Therefore, this necessitates the ongoing prevention of large-scale botnets and the limitation of their ability to launch attacks. An effective way to combat the formation of botnets is to periodically patch devices. Patching is the attempt made by the network defender to bring devices to the healthy state whether they were infected by malware or not. This can be done by power cycling (rebooting), software upgrades, formatting, etc. Sophisticated and stealthy malware can infiltrate the network without being detected, and most IoT devices lack the required resources to detect malware intrusion. Hence, state-oblivious patching is an effective way to mitigate malware propagation in wireless IoT networks. However, patching devices can cause interruption to the regular operations in the network since devices experience downtime when they are being patched. The impact of downtime becomes more severe for devices acting as hubs, i.e. connecting many devices to each other. Hence, the frequency of patching devices needs to be optimized to minimize the disruption to the network operation, while maintaining a minimum security target. Developing a theoretical model that accurately describes the burgeoning dynamical processes (patching, infecting, and sharing control commands) is crucial to the optimization of the patching frequency. In addition, there is also a need to consider a network model that captures the connectivity characteristics in practical networks.

1.2 Classical models of epidemic spreading

Over the past years, modeling the epidemic phenomena has developed into a topic of study that crosses many subfields of biology and other subjects such as malware propagation in computer networks. In this section, we only set the terminology and give some of the fundamental elements and approximations typically employed when modeling epidemic events.

Epidemic models categorize the population into various compartments, such as susceptible (S), infected (I), and recovered (R). Additional compartments may be employed to indicate other potential disease-related states, such as immune. This paradigm can be expanded to take into account disease spreading by interaction with an outside infected individual. Epidemic modeling describes the dynamical evolution of the contagion process within a population. In order to understand the evolution of the number of infected individuals in the population as a function of time we have to define the basic individual-level processes that govern the transition of individuals from one compartment to another.

The simplest epidemic dynamics to be considered is that N individuals make up the system's whole fixed population. The susceptible-infected-susceptible (SIS) paradigm, which has just two potential transitions, is one of the most straightforward two-state classifications. The first transition, marked $S \rightarrow I$, happens when an infected individual transmits the disease to a susceptible one making the latter infected. The second transition, indicated $I \rightarrow S$, takes place when the infected individual regains health and rejoins the group of susceptible individuals. This means that the SIS model assumes the illness does not give immunity and that individuals can become sick repeatedly, going through a cycle $S \to I \to S$ that, in some circumstances, can last forever. The three-state susceptible-infected-recovered (SIR) paradigm is another basic model. The transition IS of the SIS cycle is changed in the SIR model to $I \to R$, which happens when an infected individual recovers and develops a lifetime immunity. When there are no longer any infected people present, the SIR process inevitably comes to an end.

One major difference between the SIS and SIR models is the long-term behavior of the population. The endemic condition in the SIS model is defined by a constant fraction of sick individuals in the long-term regime. Conversely, the number of sick individuals tends to zero in the SIR model. The infection and recovery processes dictate how the epidemic evolves over time. The $I \to R$ and $I \to S$ transitions happen on their own, without the need for any interaction with other members of the population, while the $S \to I$ transition only happens as a result of the susceptible individual coming into contact with an infected one. In this case, the manner in which individuals interact with one another is a defining aspect of disease propagation and must be taken into consideration.

The probability of the $S \to I$ transition is more nuanced and is influenced by the modeling approximations used. The simplest approach takes into account a homogeneous mixing approximation, which implies that all individuals interact randomly and completely. According to this assumption, the probability of infection increases with the number of interactions with infected individuals. In this case, we can define the force of infection (α), which quantifies the probability that a susceptible individual will become infected during a specific time interval. We can define α as a rate in the continuous-time limit and assume that $\alpha = \hat{\beta}\rho$, where $\hat{\beta}$ depends on the specific disease and the patterns of contact in the population, and ρ is the proportion of infected individuals in the population. Therefore, ρ is directly proportional to α. In certain instances, $\hat{\beta}$ is divided into two parts as $k\beta$, where β represents the infection rate per effective contact and k is the total number of contacts. This is consistent with the mass action law, a common tool in the fundamental mean-field analysis of many dynamical processes, where the force of infection is determined by the proportion of infected individuals and decreases for larger populations.

1.3 Network Models

Although the homogeneous mixing approximation is widely employed in the literature to obtain deterministic equations of epidemic processes, it could be insufficient in a number of real-world scenarios where individuals have significant heterogeneity in the contact rate, a particular fixed interaction pattern, or are in contact with a small portion of the population. Depending on the disease or spreading mechanism under consideration, these characteristics may or may not be relevant. Yet, a variety of contagion processes necessitate representing the structure of individual contacts in the mathematical modeling methods. The majority of real-world networks exhibit extremely complex connection patterns that are governed by large-scale heterogeneity that is characterized by heavy-tailed statistical distributions, making this even more pertinent. A general framework for delving into the contact patterns between individuals is provided by network theory. In this thesis, we give a general introduction to the language of graph theory, which is required for a formal analysis of network features, as well as the main concepts and characteristics of networks that are relevant to the spread of epidemics.

1.4 Degree-Based Mean-Field Approach

Several methodologies have been developed to analyze the dynamics of epidemic processes in networks with heterogeneous patterns of connectivity. One of those methodologies is the Degree-Based Mean-Field (DBMF) approach, which is popular due to its applicability to a variety of dynamic processes on complex networks. In this section, we will detail the assumptions in the DBMF approach and its applicability.

Markov theory can be used to define a continuous-time epidemic process on any network where the transitions between compartments occur at constant rates. If we take a general epidemic process with q compartments, then a random variable $X_i(t)$ determines the state of node i at time t. The transitions between compartments are provided by separate Poisson processes with known rates. In this case, a Markov chain (MC) can be used to describe how the epidemic process evolves. The total number of states in a network with N nodes is equal to qN, which includes all potential combinations in which each of the N nodes can take a value between 0 and $q-1$. In theory, all the needed information can be inferred from the state probabilities $\mathbb{P}\{X_1(t) = x_1, \ldots, X_N(t) = x_N\}$ at time t, which can be computed from the $qN \times qN$ generator matrix Q and the initial infection probabilities.

While the Markov approach is exact, applying it to the SIS model has only yielded limited conclusions. A lot of factors make adopting a precise Markov approach difficult. For example, the analysis is restricted to very small graphs due to the linear set of $qN \times qN$ equations that must be solved. Hence, various mean-field theoretical techniques are mostly used in the derivation of explicit results on the behavior of epidemic-spreading processes in complex networks.

The main assumption of the DBMF is that all nodes of degree k are statistically equivalent. This enables us to work with quantities π_k that specify the state of all vertices of degree k which is more desirable than using quantities π_i that just specify the state of vertex i. The assumption further suggests that every vertex of degree k has the same probability $\mathbb{P}\{k'|k\}$ of connecting to a node of degree k'. The method is a practical complexity reduction strategy that involves significantly reducing the system's degrees of freedom. The DBMF approach focuses on the probability an individual of degree k belongs to compartment α, or alternatively the proportion of individuals of degree k in compartment α. These proportions are not independent, and their explicit rate equations are obtained by using the law of mass action.

The implicit assumption of the DBMF is that the network itself is viewed from a mean-field perspective, in which the adjacency matrix is erased and only the degree and the two-vertex correlations of each node are kept. In general, the statistical topological characteristics of the underlying networks, determine the solutions produced by DBMF theory. Although it is clear that the DBMF theory is a strong approximation in the case of dynamical processes occurring on static networks, it is appropriate to capture the behavior of epidemics influenced by interaction patterns changing at a rate faster than the rates at which the spreading process occurs.

CHAPTER 2

LITERATURE REVIEW AND CONTRIBUTION

Malware propagation and botnet formation are long-standing problems in wired IP networks [12], [13], [14], [15], [16], [17], [18], [19]. The work in [13] derives the distribution of the number of individuals infected by a typical host, which gives an insight into its infection ability. The malware propagation process is simulated in [12] based on both epidemic models Susceptible-Infected-Susceptible (SIS) and Susceptible-Infected-Recovered (SIR). The simulation shows that the starting location of the malware affects the time needed to infect a large portion of the network. This information can be used to quarantine specific hosts to delay malware propagation. Despite having significance in IP wired networks, the models and solutions in [12], [13], [14], [15], [16], [17], [18], [19] are not adequate for wireless networks due to the different nature of malware propagation and the limited device resources (e.g., power and computations).

There are several efforts to characterize and understand malware propagation in ad hoc wireless networks [7], [8], [9], [10], [20]. For instance, the work in [7] shows that restricted communication range and channel contention slow down the propagation of malware worms in wireless networks when compared to wired IP networks. The works in [8], [20] propose dynamic malware propagation models based on homogeneous mixing approximation, where devices interact with each other randomly and all devices are statistically equivalent. This may be inadequate in real-life networks where individual devices have large heterogeneity in the contact rate. Hence, there is a need to capture the individuals' contact pattern structure in the mathematical modeling approach. The authors in [10] utilize a stochastic approach to study the effect of mobility on the evolution of botnets in mobile networks. While the models in [7], [8], [9], [10], [20] are essential to characterize malware propagation, none of them propose countermeasures to resolve the problem.

There are also efforts to develop countermeasures to thwart malware propagation in IoT networks [21], [11], [22], [23]. The works in [22], [23] formulate large-population game problems and solve them to achieve desired outcomes of the game. Moreover, the work in [21] proposes a spatial firewall solution to thwart large-scale malware propagation. However, the solution in [21] imposes capital and operational expenditures to deploy and maintain the firewall infrastructure, which might not be always viable for IoT networks. A cost-effective countermeasure to thwart botnets in IoT is the state-oblivious randomized patching of devices [11]. Such random patching enables probabilistic recovery of infected devices at the expense of probabilistic unnecessary interruption for healthy devices. Consequently, the patching rate needs to be set carefully to balance the trade-off between network operation and security. Increasing the patching rate would increase the immunity to malware epidemics at the expense of deteriorating the network performance, and vice versa. The work in [11] derives the optimal patching, which was shown to be a function of the number of directly connected neighbors, which is denoted as the device degree. However, the work in [11] overlooks the intrinsic spatial degree correlation between the IoT devices. At the end of the literature survey, we list the main contributions of this work as follows:

1. We propose an analytical model for malware propagation that takes into account the spatial degree correlation in wireless IoT networks.

2. We use the Degree-Based Mean Field (DBMF) approach to find the equilibrium proportions of healthy, infected, and informed devices.

3. We formulate and solve an optimization problem to minimize the downtime cost of patching devices while maintaining security objectives to prevent the formation of botnets.

4. We incorporate the effect of spatial firewalls on the malware propagation model.

5. We solve the optimization problem to find the optimal patching strategy under firewall deployment, and we show the effectiveness of firewalls in reducing the required patching rates.

6. We develop a simulation tool to validate the effectiveness of the malware propagation models and the acquired optimal patching strategies.

CHAPTER 3

MALWARE PROPAGATION IN IOT NETWORKS

The main goal of this chapter is to provide a rigorous approach for modeling malware propagation and botnet formation in IoT wireless ad hoc networks. We start by first describing the model of the network under consideration and the underlying assumptions. We consider the malware propagation and its mitigation (i.e., dynamic patching) as an epidemic process based on a variation of the Susceptible-Infected-Susceptible (SIS) model. In such a model, susceptible devices may become infected, then infected devices may be patched (cured) to become susceptible once again. Hence no susceptible device can become immune to the malware. We use the Degree-Based Mean Field (DBMF) approach proposed in [24] to analyze the dynamical process of malware propagation in complex networks which have heterogeneous connectivity patterns such as WANET. Based on the proposed model, we formulate and solve a defender optimization problem to minimize the cost associated with patching devices, while maintaining a minimum security target.

3.1 Network Model

The IoT wireless ad hoc network is represented via a Random Geometric Graph (RGG) $\mathbf{G} = \{\mathbf{V}, \mathbf{E}\}$ to account for i) the random spatial location of the IoT devices; and ii) the impact of the wireless communications range on the malware propagation. That is, the vertices in $\mathbf{V} = \{\mathbf{x}_i\}_{i \geq 1}$ with $\mathbf{x}_i \in \mathbb{R}^2$ model the spatial locations of the IoT devices as Poisson Point Process (PPP) with intensity $\lambda \in \mathbb{R}$ devices/km^2. Let r be the wireless communications range between devices, $\|\cdot\|$ denote the Euclidean norm and $|\cdot|$ denote set cardinality. The set of edges $\mathbf{E} = \{\overline{\mathbf{x}_i \mathbf{x}_j} : \|\mathbf{x}_i - \mathbf{x}_j\| \leq r,\ \mathbf{x}_i, \mathbf{x}_j \in \mathbf{V}, \forall i, \forall j \neq i\}$ represent the direct D2D connectivity between vertices (i.e., devices) that are within the wireless communication range of each other. The degree of a typical device $\mathbf{x}_i \in \mathbf{V}$ is defined by the number of edges $K_i = |\mathbf{E}_i|$ connected to it, where $\mathbf{E}_i = \{\overline{\mathbf{x}_i \mathbf{x}_j} : \|\mathbf{x}_i - \mathbf{x}_j\| \leq r,\ \mathbf{x}_i, \mathbf{x}_j \in \mathbf{V}, \forall j \neq i\}$ and $\mathbf{E} = \bigcup_i \mathbf{E}_i$. The degree of a device captures the number of directly connected neighbors, which is a random variable. For RGGs, it is well known that the degrees of the devices have identical but not independent Poisson distributions with mean equal to $\lambda \pi r^2$. Fig 3.1 shows a color-coded realization of the RGG to manifest the intrinsic spatial degree correlations among the devices. For clarity of exposition, the RGG realization is shown without the edges and the devices are categorized into high (red), moderate (blue), and low (green) degrees only. An example of the spatial degree correlation is that high degree nodes are clustered and surrounded by medium degree nodes

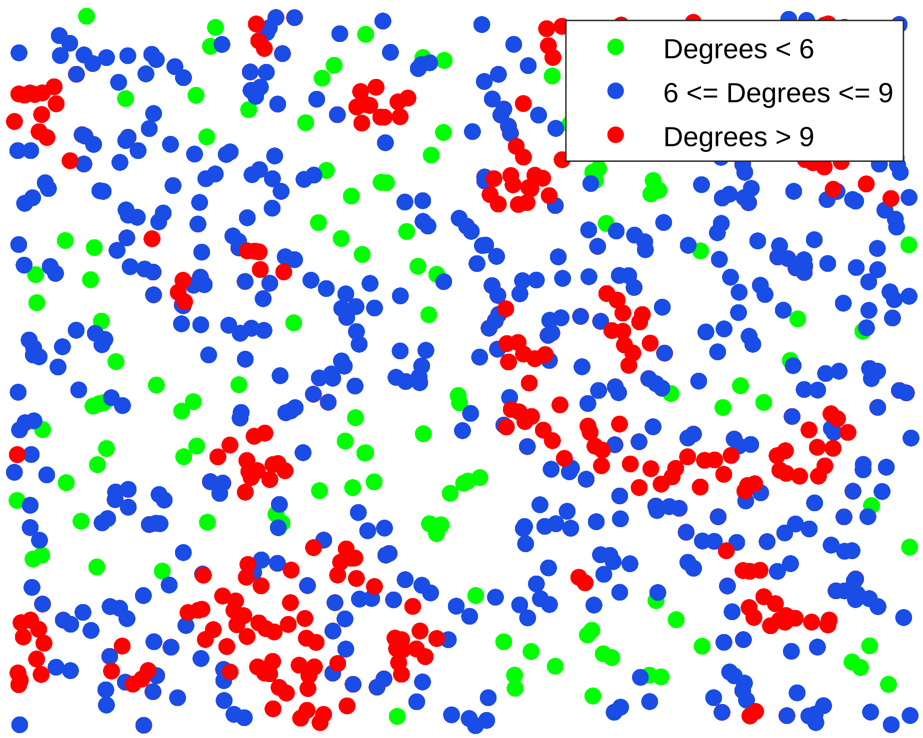


Figure 3.1: A realization of the RGG with degrees color coded.

To simplify modeling the malware propagation, we assume that devices do not coordinate transmission, meaning ALOHA is the medium access control. Considering other medium access control (MAC) protocols is valid, however, it would complicate the malware propagation model since transmission coordination has to be taken into account. The transmission success probability is not the focus of this work, hence it is represented as a constant parameter $\rho \in [0, 1]$. Due to monetary constraints, it is not possible to ensure up-to-date security mechanisms on every device. Hence, it is assumed that a random proportion p of the devices are susceptible to malware infiltration while the rest are immunized by hardware/software security mechanisms. Infected devices can be recovered via a patching process that eliminates the malware. Due to the massive number of IoT devices, it may not be feasible to identify the current state of each IoT device. Hence, state-oblivious random patching is utilized to recover infected and informed devices to the healthy state. We also assume that infected devices can be recruited to attack after they receive control commands from a neighboring informed device. In particular, a susceptible device can be in one of the following three states:

- **Healthy state (H):** the device is not compromised. Upon a successful reception of a malware via the D2D channel, the device goes to state I.
- **Infected state (I):** the device is compromised but not informed about an attack. If patched, the device goes to state H. Upon successful reception of a control command via the D2D channel, an infected device goes state $\hat{I}$.
- **Informed state ($\hat{I}$):** the device is infected and informed to contribute to an

attack. If patched before the attack, the device goes back to state H. Otherwise, it does its role in the attack and goes back to state I.

Malware worms exploit the direct connectivity of the infected and informed devices to infect healthy neighboring devices. Similarly, control commands are transmitted from informed devices to their neighboring infected devices. Governed by the portion of susceptible devices p and wireless transmission success probability ρ, the diffusion rates of malware infection (σ_1) and control command (σ_2) among neighboring devices are given respectively by:

$$\sigma_1 = \rho p \gamma_b, \quad \text{and} \quad \sigma_2 = \rho \gamma_c, \tag{3.1}$$

where γ_b and γ_c are the spreading rates of malware and control commands chosen by the attacker to maintain covert operation. It is also assumed that informed devices do their role in the attack and go back to the infected state at rate β. Moreover, the infected devices weather they are informed or not return to the healthy state based on the patching rate μ that we are aiming to optimize.

In this work, we consider a continuous-time epidemic model which assumes that the transitions between states follow a memoryless continuous-time Markov chain with constant rates. In the definition of a continuous-time Markov chain, the amount of time spent in a state before making a transition into a different state is exponentially distributed [25], and hence the number of devices that transition in a given time interval is Poisson distributed. Since we base our model on a continuous-time Markov chain, the rates (μ, σ_1, σ_2, and β) are the probabilities per unit time of transitioning

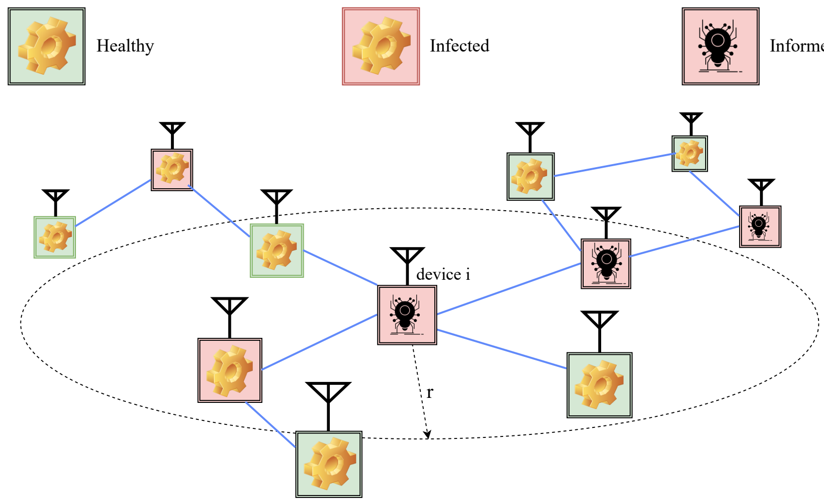


Figure 3.2: Illustration of the network model, with a typical device, denoted by device i, having communication range r. D2D links are highlighted by blue lines, and three states are possible: healthy, infected, and informed.

between different states, and their reciprocals define the amount of time spent in each state before transitioning. For instance, since the rate of discarding control commands is β, the total time τ_i that a given informed device remains informed is exponentially distributed with mean $E[\tau_i] = \frac{1}{\beta}$. The way we implement an optimal patching rate μ^* on devices is by using a back-off timer that generates a random holding time between consecutive patches. For example, if a device is patched at $t = 0$, the next time it is patched is at $t = \tau_r$, where τ_r is an exponential random variable with mean $1/\mu^*$.

An illustration of the wireless network and the states of some IoT devices can be seen in Fig. 3.2. Infected devices can be operating regularly, while attempting to transmit the malware to a neighboring device through D2D links illustrated in blue lines. A group of informed devices can damage the network with a coordinated attack such as DDoS attack.

3.2 Analysis

The degree of a device determines its susceptibility and contribution to malware diffusion. For healthy devices, higher degree implies higher probability of having compromised neighbors, and hence, higher susceptibility to infection. For infected/informed devices, higher degree implies higher opportunities for malware/control command propagation. Following such intuition, we utilize the degree-based mean field (DBMF) approach proposed in [24] to track the status of susceptible IoT devices. However, in contrast to [11], we do not assume that the degrees of neighboring devices are uncorrelated. Instead, we find the two-vertex degree correlations measured by the conditional probability $\mathbb{P}\{k'|k\}$ that a given link from a device of degree k points to a device of degree k' on the other end.

The DBMF implicitly assumes that all devices of the same degree k are statistically equivalent. A degree-aware Markov chain (MC) is utilized to track the status evolution of all devices of a given degree k, which is shown in Fig. 3.3. As shown in the figure, the states and transition probabilities are parameterised with the device degree. Both infected and informed devices may transfer malware infection at the rate σ_1 in (3.1) and there are k neighboring device. Hence, the transition rate between states H_k and I_k is given by $\nu_k = k\sigma_1(1-\theta_k^H)$, where θ_k^H is the probability that a neighboring device is healthy. Only informed devices may transfer control commands at the rate σ_2 in (3.1) and there are k neighboring devices. Hence, the transition rate between states I_k and $\hat{I}_k$ is given by $\omega_k = k\sigma_2\theta_k^{\hat{I}}$, where $\theta_k^{\hat{I}}$ is the probability that a neighboring device is informed. The objective is to find degree-dependent patching rates μ_k, $\forall k$ to balance

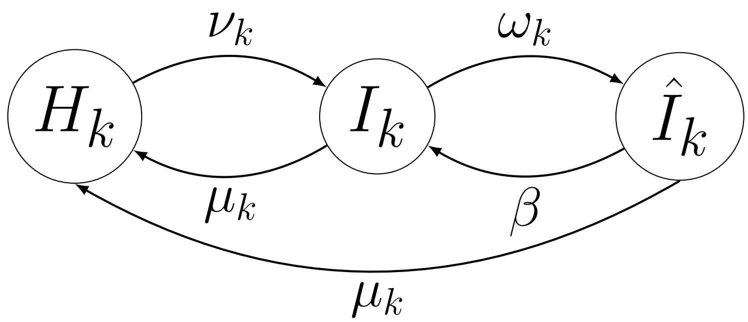


Figure 3.3: Degree-aware MC for state evolution of a typical IoT device if degree k.

the trade-off between network security and operation. To optimize the patching rates at equilibrium, the steady state solution of the MC needs to be expressed in terms of the patching rates μ_k, $\forall k$ and also the network operation Key Performance Indicator (KPI) need to be expressed in terms of the patching rates $\boldsymbol{\mu} = [\mu_k]$, $\forall k$. The solution to the MC in Fig. 3.3 is expressed in terms of the probabilities $\pi_k^H(t)$, $\pi_k^I(t)$, and $\pi_k^{\hat{I}}(t)$ of being in each state at time t. For example, $\pi_k^H(t)$ is the probability that a device of degree k is in the state H at time t.

After defining the states and transition rates, the dynamical equations for the probabilities three states are obtained by applying the law of mass action,

$$\begin{aligned}\frac{d\pi_k^H(t)}{dt} &= \mu_k(\pi_k^I(t) + \pi_k^{\hat{I}}(t)) - k\sigma_1(1 - \theta_k^H(t))\pi_k^H(t) \\ &= \mu_k(1 - \pi_k^H(t)) - k\sigma_1(1 - \theta_k^H(t))\pi_k^H(t) \qquad (3.2)\end{aligned}$$

$$\frac{d\pi_k^I(t)}{dt} = -(\mu_k + k\sigma_2\theta_k^{\hat{I}}(t))\pi_k^I(t) + k\sigma_1(1 - \theta_k^H(t))\pi_k^H(t) + \beta\pi_k^{\hat{I}}(t) \qquad (3.3)$$

$$\frac{d\pi_k^{\hat{I}}(t)}{dt} = k\sigma_2\theta_k^{\hat{I}}(t)\pi_k^I(t) - (\mu_k + \beta)\pi_k^{\hat{I}}(t) \qquad (3.4)$$

The first term in (3.2) accounts for the recovery of infected devices (informed or uninformed), while the second term accounts for the infiltration of healthy devices. Similar statements can be made about (3.3) and (3.4). Using the closure relationship $\pi_k^H(t) + \pi_k^I(t) + \pi_k^{\hat{I}}(t) = 1$, we can get the following independent system of equations:

$$\frac{d\pi_k^H(t)}{dt} = \mu_k - \left[\mu_k + k\sigma_1(1 - \theta_k^H(t))\right] \pi_k^H(t) \tag{3.5}$$

$$\frac{d\pi_k^{\hat{I}}(t)}{dt} = k\sigma_2\theta_k^{\hat{I}}(t) - (\mu_k + \beta + k\sigma_2\theta_k^{\hat{I}}(t))\pi_k^{\hat{I}}(t) - k\sigma_2\theta_k^{\hat{I}}(t)\pi_k^H(t) \tag{3.6}$$

Note the probability θ_k^H depends on time as it decreases when number of infected devices increase. In the steady-state when the ratio of healthy and infected populations are nearly constant ($\frac{d\pi_k^H}{dt} = 0, \frac{d\pi_k^{\hat{I}}(t)}{dt} = 0$), the malware spreading rate is offset by the patching rate. In such case, both π_k^H and $\pi_k^{\hat{I}}$ can be reduced to the following two systems of equations:

$$\pi_k^H = \frac{\mu_k}{\mu_k + k\sigma_1(1 - \theta_k^H)} \tag{3.7}$$

$$\pi_k^{\hat{I}} = \frac{k^2\sigma_1\sigma_2(1 - \theta_k^H)\theta_k^{\hat{I}}}{(\mu_k + k\sigma_1(1 - \theta_k^H))\left(\beta + \mu_k + k\sigma_2\theta_k^{\hat{I}}\right)} \tag{3.8}$$

In this case, all probabilities and proportions become constant and time dependency is removed. The probabilities θ_k^H and $\theta_k^{\hat{I}}$ can be obtained by total probability theorem:

$$\theta_k^H = \sum_{k'} \mathbb{P}\left\{k'|k\right\} \pi_{k'}^H, \tag{3.9}$$

Similarly $\theta_k^{\hat{I}}$ can be described as following:

$$\theta_k^{\hat{I}} = \sum_{k'} \mathbb{P}\left\{k'|k\right\} \pi_{k'}^{\hat{I}}, \tag{3.10}$$

where the conditional probabilities $\mathbb{P}\left\{k'|k\right\}$ can be derived from the joint distribution of degrees for neighboring devices. The joint probability mass function (PMF) of two neighboring devices with degrees k and k', is denoted as $f_{k,k'}(k, k')$. The next subsection describes the derivation of this distribution.

3.2.1 Joint distribution of degrees

Devices are considered neighbors if their separation distance d is less than the D2D communication range (r). In RGGs, the separation distance d between two neighboring devices can be shown to be a random variable with the following Probability Density Function (PDF):

$$f_D\left(d\right) = \frac{2d}{r^2}\ , \quad 0 < d < r. \tag{3.11}$$

Without loss of generality, consider two neighboring devices $\mathbf{x}_i, \mathbf{x}_j \in \mathbf{V}$ that share a common edge $\overline{\mathbf{x}_i\mathbf{x}_j} \in \mathbf{E}$. A pictorial illustration of the two devices is shown in Fig. 4.4, where the overall D2D ranges of the two devices are divided into a common region:

$$Y = \mathbf{B}(\mathbf{x}_i, r) \cap \mathbf{B}(\mathbf{x}_j, r), \tag{3.12}$$

and two disjoint regions

$$X = \mathbf{B}(\mathbf{x}_i, r) \setminus Y, \quad \text{and} \quad Z = \mathbf{B}(\mathbf{x}_j, r) \setminus Y, \tag{3.13}$$

where $\mathbf{B}(\mathbf{a}, b)$ defines a circle centered at $\mathbf{a} \in \mathbb{R}^2$ with radius $b \in \mathbb{R}$. Recalling that the degree of each device is determined by the number of neighbors within the D2D

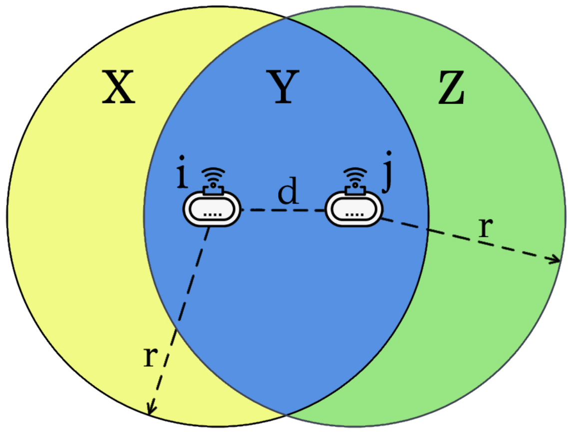


Figure 3.4: Distinct and common neighborhood regions of two connected devices.

range r, the degree correlation of the two devices becomes obvious. In particular, each device has its own independent and distinct set of neighbors in the disjoint regions X and Z. However, the two devices share a set of common neighbors in the overlapping area Y. Accounting for a such common set of neighbors, the joint degree correlation between the two devices is given in the following lemma:

Lemma 3.1 *In RGGs with intensity λ and D2D range of r, the joint degree PMF of neighboring devices is given by:*

$$f_{k,k'}\left(k,k'\right) = \sum_{t=0}^{\min(k,k')-1} \frac{2e^{-2\lambda\pi r^2}}{r^2\ (k-t-1)!\,(k'-t-1)!t!} \times \\ \int_0^r \frac{\left(\lambda A_y\right)^t \zeta e^{\lambda A_y}}{\left(\lambda\pi r^2 - \lambda A_y\right)^{2(t+1)-(k+k')}} d\zeta, \quad k,k' \geq 1, \tag{3.14}$$

where $A_y = 2r^2 \arccos\left(\frac{d}{2r}\right) - \frac{1}{2}\sqrt{d^2(2r-d)(2r+d)}$ is the area of the overlapping region Y.

Proof. *See **Appendix A.1**.* ∎

Utilizing Lemma 3.1, the probabilities θ_k^H and $\theta_k^{\hat{I}}$ in (3.15) and (3.16) can be rewritten as:

$$\theta_k^H = \sum_{k'=1}^{\infty} \frac{f_{k,k'}(k,k')\,\pi_{k'}^H}{\mathbb{P}\{K=k\}}, \tag{3.15}$$

$$\theta_k^{\hat{I}} = \sum_{k'=1}^{\infty} \frac{f_{k,k'}(k,k')\,\pi_{k'}^{\hat{I}}}{\mathbb{P}\{K=k\}}, \tag{3.16}$$

where $\mathbb{P}\{K = k\} = \frac{(\lambda\pi r^2)^k e^{-\lambda\pi r^2}}{k!}$. The steady states π_k^H and $\pi_k^{\hat{I}}$ can be obtained by numerically solving the non-linear system of equations (3.7), (3.8), (3.15), and (3.16) for a given set of patching rates $\boldsymbol{\mu}$. Note that the summations in equations (3.15) and (3.16) needs to be limited to a maximum degree k_{max} for which $\epsilon = \mathbb{P}\{K > k_{max}\}$ is sufficiently small. Such approximation is necessary to optimize the patching rates, where the complexity vs accuracy trade-off is controlled by the parameter ϵ.

3.2.2 Patching Rate Optimization

Due to the massive number of devices, it is infeasible to secure 100% of the devices while maintaining useful network operation. Allowing a slight tolerance to malware infection, the security KPI is to enforce a minimum acceptable percentage of healthy devices and a maximum tolerable percentage of informed (i.e., who contribute to the attack) devices. The network operation KPI can be defined in terms of a cost function that accounts for the downtime due to device patching. For a fair comparison with [11], we utilize the same logistic function ($\phi_k : \mathbb{R}^+ \to \mathbb{R}^+, \forall k \geq 1$) to capture the cost of patching, which is given by:

$$\phi_k(\mu_k) = \frac{{\mu_k}^2}{1 + e^{-a(k-b)}}, a > 0, b > 0. \tag{3.17}$$

Assuming that the infection-informed-patching dynamics of the MC in Fig. 3.3 reaches equilibrium, the steady state solution $\boldsymbol{\pi}_k = [\pi_k^H \; \pi_k^I \; \pi_k^{\hat{I}}]$ gives the probability of being in each of the three states. From the DBMF point of view, the steady state solution $\boldsymbol{\pi}_k$ also gives the percentage of devices of degree k that are in each of the three states. Consequently, the formulation of the patching rates optimization is give by

$$\begin{aligned} \min_{\mu_k, k\geq 1} \quad & \phi(\boldsymbol{\mu}) = \sum_{k=1}^{\infty} \phi_k(\mu_k)\mathbb{P}\{K = k\}, \\ \text{subject to} \quad & \sum_{k=1}^{\infty} \pi_k^H(\boldsymbol{\mu})\mathbb{P}\{K = k\} \geq \tau_H, \\ & \sum_{k=1}^{\infty} \pi_k^{\hat{I}}(\boldsymbol{\mu})\mathbb{P}\{K = k\} \leq \tau_{\hat{I}}, \end{aligned} \tag{3.18}$$

where τ_H and $\tau_{\hat{I}}$ are the target thresholds for the healthy and informed devices, respectively. As mentioned earlier, the degree probabilities $\mathbb{P}\{K = k\}$ follow the Poisson distribution with mean $\lambda\pi r^2$. Equipped by the system of equations (3.7), (3.8), (3.15), and (3.16), we are in a position to optimize the patching rates. Recalling the optimization problem in (3.18), the cost function is a smooth convex and increasing function of the patching rates. Hence, minimizing the cost is equivalent to choosing the minimum patching rates that will satisfy the constraints. The main challenge now is that the constraints do not have closed form expressions in $\boldsymbol{\mu}$, which makes the optimization problem highly nonlinear, and non-convex. Hence, a numerical solution has to be sought. In this context, we refer to the interior point method algorithm introduced in [26], which is widely-accepted for solving such non-linear optimization problems using a barrier approach that employs sequential quadratic programming and trust regions.

Specifically, the logarithmic barrier problem associated with (3.18) is given by:

$$\begin{aligned} \min_{\boldsymbol{\mu},\boldsymbol{s}} \quad & B(\boldsymbol{\mu},\alpha) = \phi(\boldsymbol{\mu}) - \alpha \ln(s_1) - \alpha \ln(s_2), \\ \text{subject to} \quad & \tau_H - \sum_{k=1}^{\infty} \mathbb{P}\{K=k\}\pi_k^H(\boldsymbol{\mu}) + s_1 = 0, \\ & \sum_{k=1}^{\infty} \mathbb{P}\{K=k\}\pi_k^{\hat{I}}(\boldsymbol{\mu}) - \tau_{\hat{I}} + s_2 = 0, \end{aligned} \tag{3.19}$$

where s_1 and s_2 are slack variables restricted to be positive to keep the iterations inside the feasible region. $\alpha > 0$ is the barrier parameter. As α approaches 0, the sequence of solutions to (3.19) will converge to the solution of the nonlinear problem in (3.18). The detailed steps of the algorithm are described in [26].

3.3 Results and discussion

This section shows the impact of the spatial degree correlation on the joint degree distribution as well as on the optimal patching rates. Fig. 3.5 compares three joint degree distributions: the one in (4.7), the distribution used by [11] that assumes independent degrees, and an empirical distribution generated by MATLAB using $n = 10^6$ observations. Clearly, the joint distribution that considers spatial degree correlation matches the empirical distribution, which shows a concentration of probability towards comparable degrees. To better visualize the impact of the spatial degree correlation on the joint PMF, we utilize the Kolmogorov–Smirnov (KS) test which is defined as $D_n = \sup |F_n(i,j) - F(i,j)|$, where F_n is the empirical CDF, F is the theoretical Cumulative Distribution Function (CDF), and sup is the supremum of the

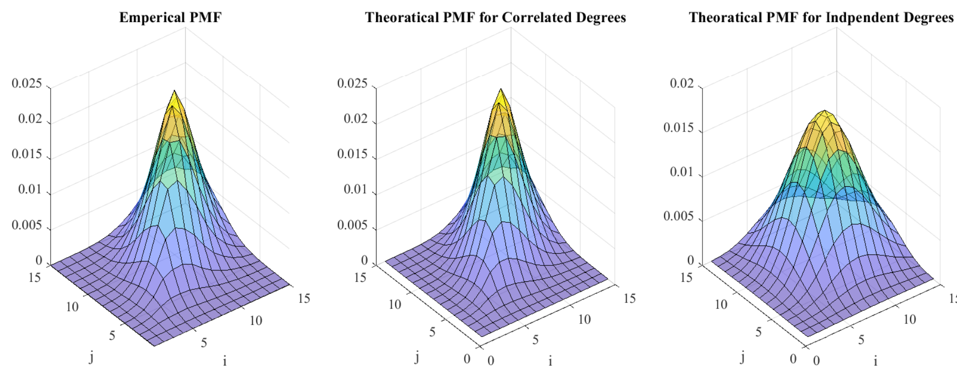


Figure 3.5: Empirical Joint degree PMF compared to the Theoretical PMFs with and without considering spatial degree correlation.

set of distances. In particular, the KS statistic takes the largest absolute difference between the two distribution functions across all i and j values. Fig.3.6 compares D_n for the distribution in (4.7) and the one that ignores correlation as used in [11]. By the Glivenko–Cantelli theorem, if the samples come from the distribution $F(x)$, then D_n converges to zero almost surely in the limit $n \to \infty$. The figure clearly shows that Glivenko–Cantelli theorem only applies to (4.7), which accounts for the intrinsic degree correlation.

To assess the impact of the spatial degree correlation on the susceptibility to infection as well as the optimal patching rates, we will use the same network setup and system parameters in [11] with parameters listed in Table 3.1. Note that $k_{max} = 25$ leads to $\epsilon = \mathbb{P}\{K \geq k_{max}\} \approx 10^{-6}$, which is an acceptable error margin. Fig. 3.7 plots the probability of infection $(1-\theta_k^H)$ for uniform patching rates to emphasize the direct proportionality between the degree and infection probability, which is absent when overlooking the degree correlation. Such different susceptibility to infection between the two models leads to different optimal patching rates as shown in Fig. 3.8. Partic-

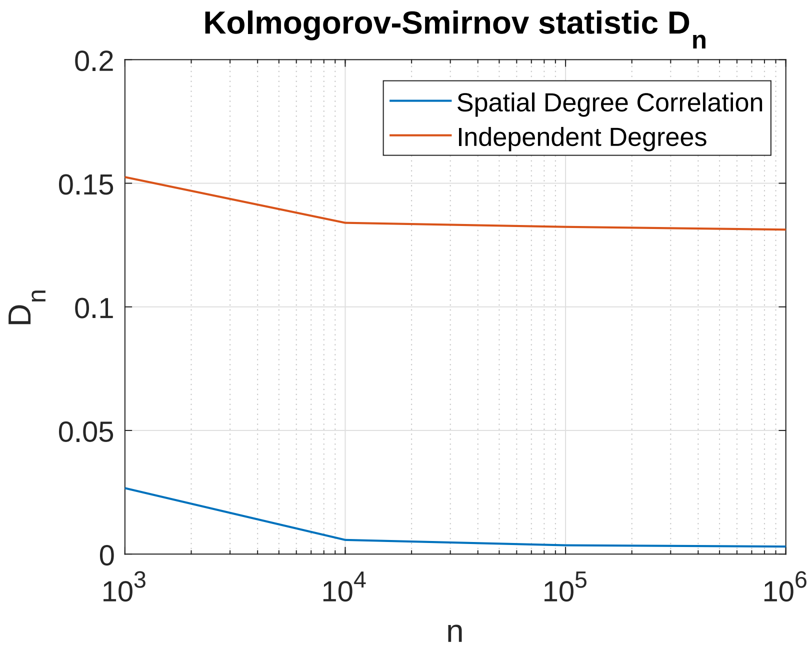


Figure 3.6: Kolmogorov–Smirnov statistic D_n as a function of the number of observations n.

ularly, overlooking the degree correlation leads to the overestimation of the patching rates of lower-degree devices due to the overestimation of their probability of infection. On the other hand, the patching rates of higher-degree devices are underestimated due to the underestimation of their probability of infection. Given the proportional contribution of higher-degree devices in malware spreading, underestimating the patching rates of high-degree devices leads to violating the security KPIs. In particular, The optimal patching rates when overlooking degree correlation (i.e. proposed in [11]) leads to a percentage of healthy devices lower than the desired threshold τ_H. For instance, for $\tau_H = 0.6$, $\tau_H = 0.7$ and $\tau_H = 0.8$, the actual percentages of healthy devices when overlooking the degree correlation are 0.57, 0.66 and 0.73 respectively, which is lower than the required thresholds. Our correlation-aware patching rates satisfy all security KPIs at the cost of an overall 11% higher patching cost.

Parameter	value	Parameter	value	Parameter	value
λ [device/km^2]	300	τ_H	0.7	$\tau_{\hat{I}}$	0.1
r $[km]$	0.1	k_{max}	25	β	0.002
γ_b	0.001	γ_c	0.001	ρ	0.95
p	0.7	a	0.2	b	10

Table 3.1: Parameters of network and optimization

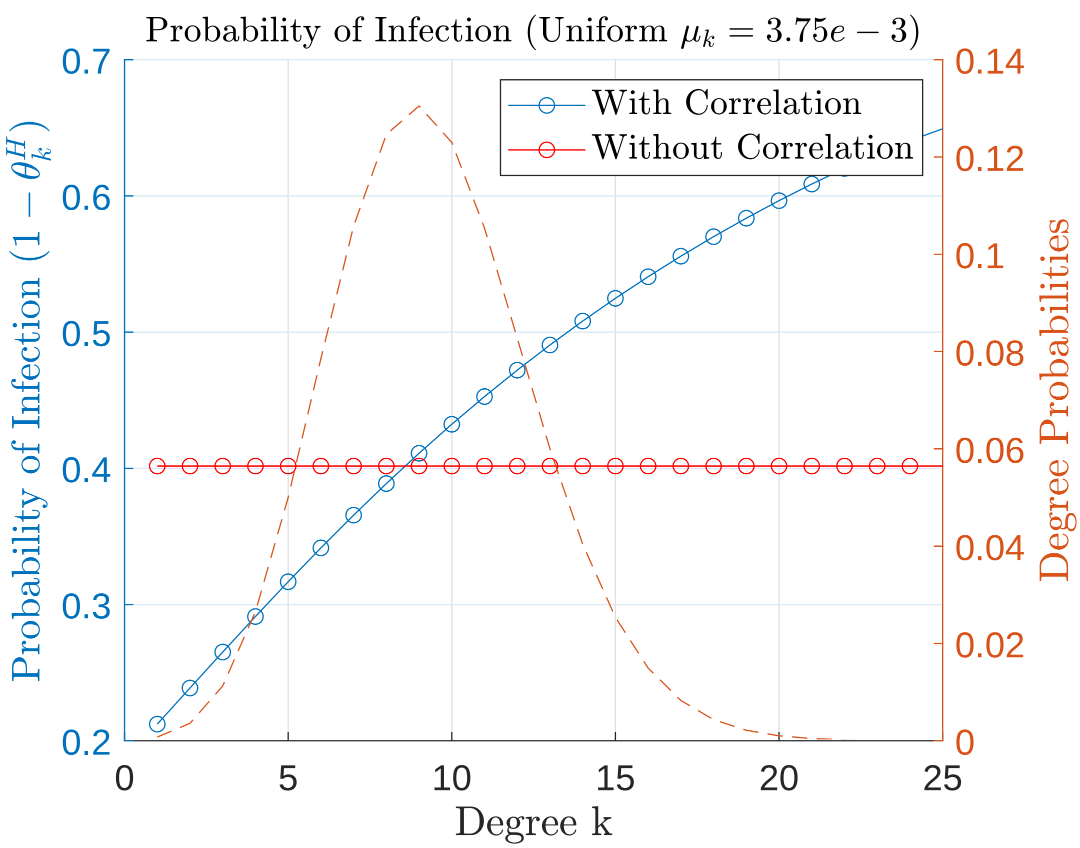


Figure 3.7: The probability of infection $1 - \theta_k^H$ in case of a uniform patching rate across all degrees.

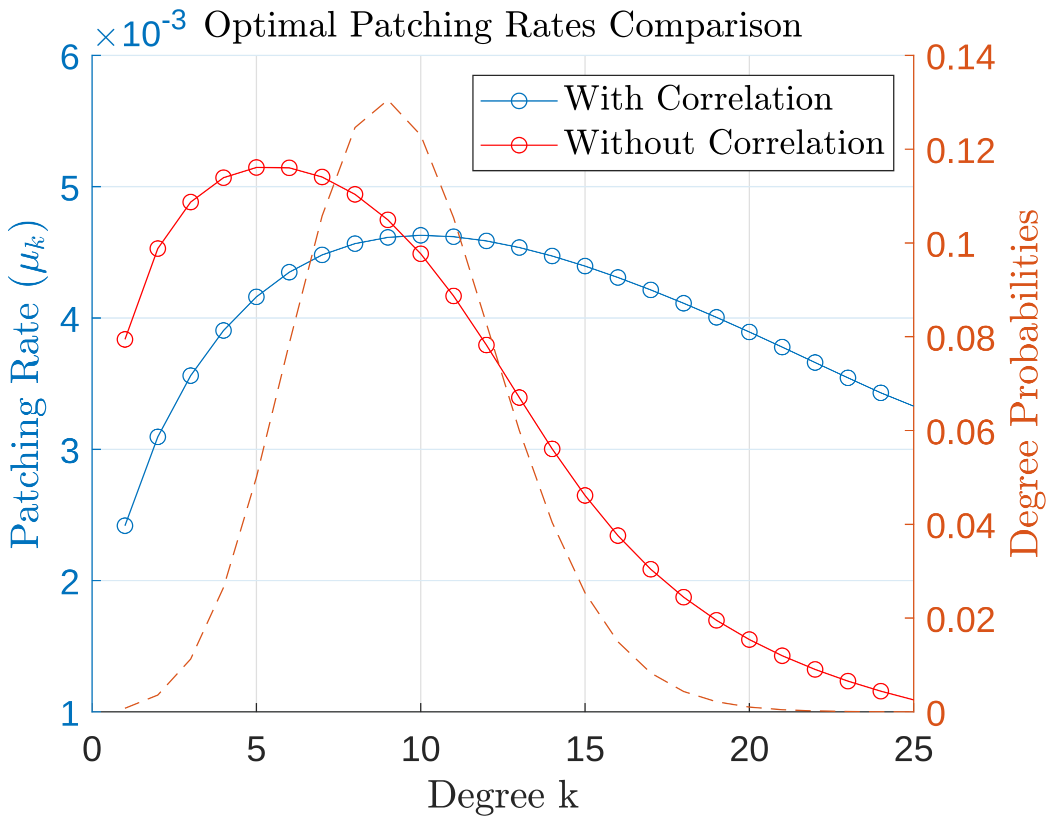


Figure 3.8: Impact of spatial degree correlation on the optimal patching rates.

In order to assess the accuracy of the theoretical model developed, we simulate a PPP network with the same parameters listed in table 3.1, and let the malware propagate through the devices while recording the changes in the percentage of healthy devices. In the first part, we let the malware propagate at different spreading rates γ_b without patching any device. Fig. 3.9 shows the percentage of healthy devices as a function of time. The percentage of healthy devices decreases faster as the spreading rate increases. In the second part, we compare our patching strategy against the patching strategy that does not account for degree correlation. We start at $t = 0$ with all devices infected and apply one patching strategy at a time to see the difference. As shown in Fig. 3.10 our patching rates lead to an equilibrium percentage of healthy devices greater than the minimum required threshold $\tau_H = 0.7$, while ignoring spatial degree correlation leads to deficiency in the percentage of healthy devices as predicted theoretically. This becomes more apparent when we start at $t = 0$ with a percentage of healthy devices close to the threshold $\tau_H = 0.7$, as shown in Fig. 3.11. The uncorrelated case is below the threshold τ_H most of the time while the correlated case is above the threshold most of the time.

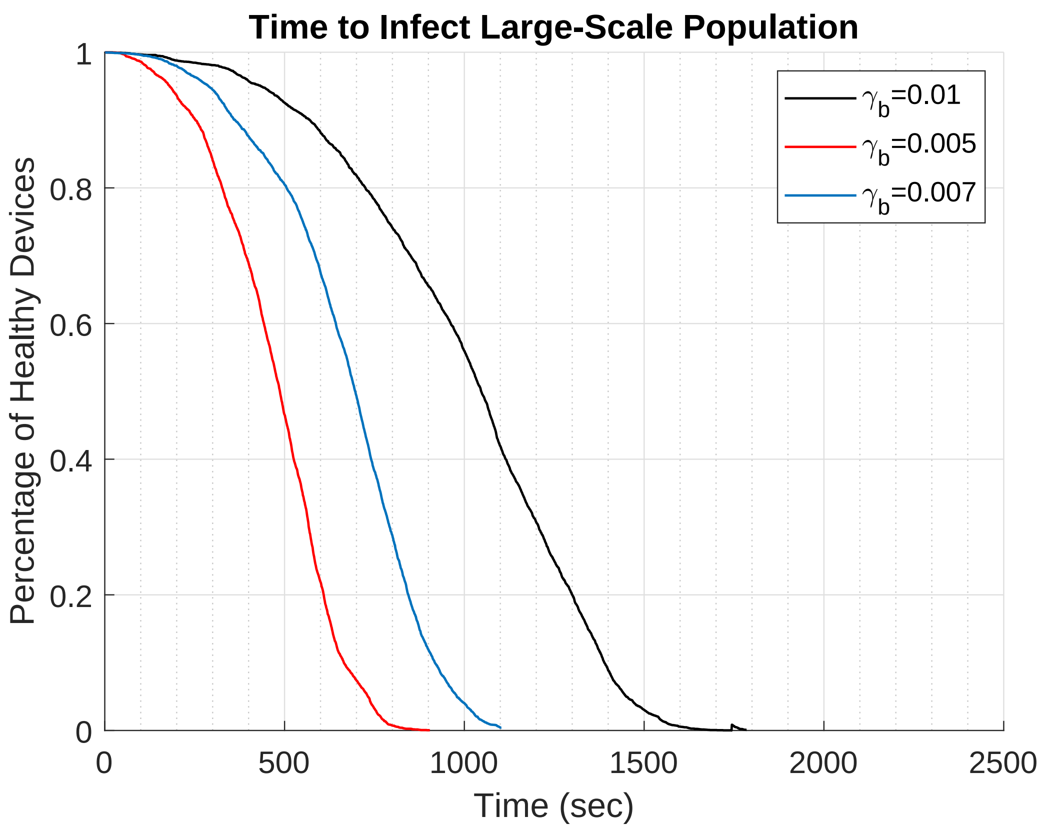


Figure 3.9: Percentage of Healthy devices vs Time: simulating the infection process with different spreading rates

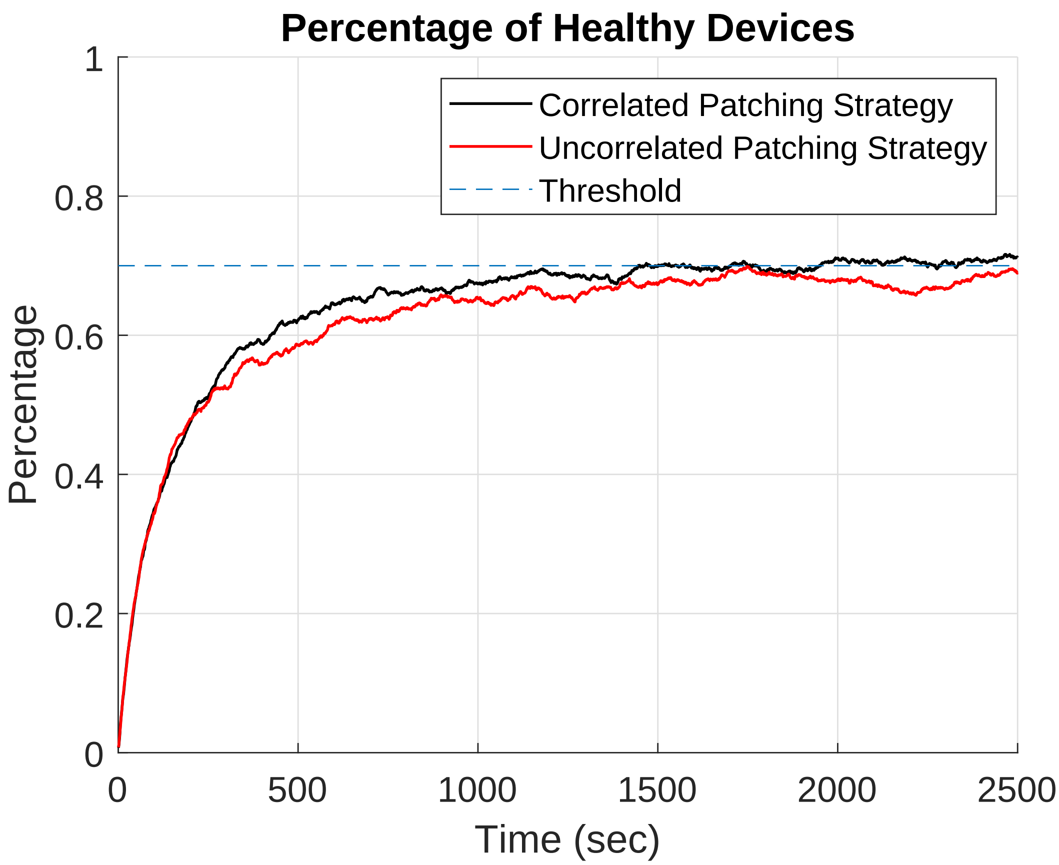


Figure 3.10: Percentage of Healthy devices vs Time: simulation of the patching process for a completely infected network

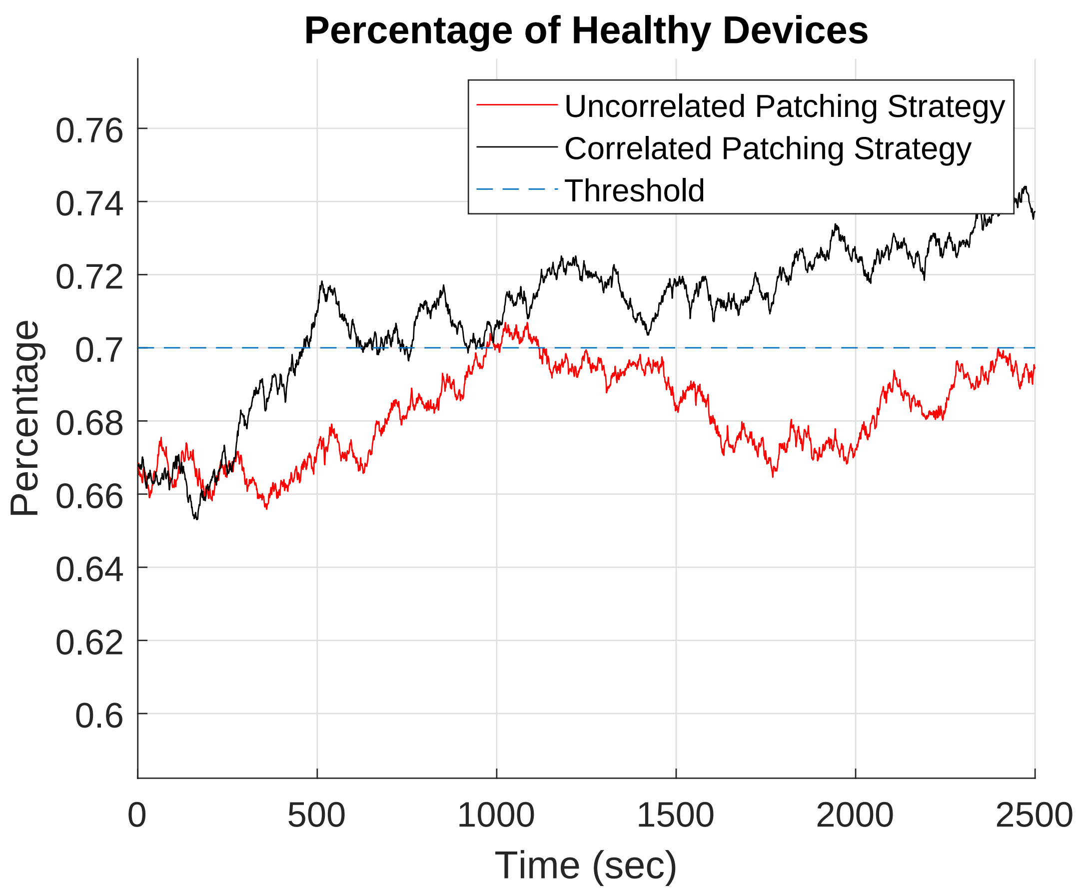


Figure 3.11: Percentage of Healthy devices vs Time: simulation of the equilibrium state when the patching offsets the infection.

CHAPTER 4

SPATIAL FIREWALLS

In this chapter, we introduce another method to thwart malware propagation in IoT ad hoc wireless networks, which is '*Spatial Firewall*'. Spatial firewalls are capable wireless devices scattered around the wireless network. They can store and update anti-virus software and share their protective capability with their neighboring devices. This can be done by communicating with neighboring devices and scanning their software codes before execution. Therefore, devices within the range of a spatial firewall become immune to malware since they do not execute any codes which are flagged by the nearest firewall. The main two design parameters of this scheme are the density of firewall deployment (i.e. average number of firewall devices within a unit area λ_f), and the range of communication of these firewalls r_f. These two parameters are included in the mathematical framework to assess their impact on the effectiveness of the solution.

In the next section, we describe the network model when firewalls are deployed according to a PPP. Then we model the propagation of the malware, outside the range of firewalls, to facilitate finding the optimal patching rates needed to prevent a malware outbreak and wide-range attacks. In the results section, we demonstrate the effectiveness of firewalls in reducing the required patching rates to thwart malware propagation.

4.1 Network Model with Firewalls

Firewalls are edge computing and immune devices capable of maintaining and sharing anti-malware features with their neighboring devices. In this work, we assume that the locations of the firewall devices follow an independent PPP $\Psi \equiv \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_k, \ldots\} \subset \mathbb{R}^2$ with intensity λ_f. All firewalls are assumed to have the same communication range r_f. We assume that firewalls can have a larger communication range than normal IoT devices (i.e. $r_f \geq r$) because firewalls can transmit at higher power and detect the received signal better than IoT devices. IoT devices located within the range of a firewall take permission from the closest firewall before executing any files received from a neighboring device. The inquired firewall scans the files and only approves the safe executable files, and the suspicious files are disapproved. Consequently, firewalls form secured zones around them and any IoT device in that zone is considered immune from malware infection, and hence does not participate in malware propagation. On the other hand, devices outside the secured zones are forced to directly execute files without scanning, which makes them susceptible to malware intrusion. Therefore, only susceptible devices participate in the malware propagation process. It is important to note that firewalls immunize devices that are spatially close to each other. Therefore, it is different from installing anti-malware software in randomly located IoT devices around the network, which is the case we considered in the previous chapter. Immunizing devices by firewalls is a more cost-effective way than installing anti-malware software on randomly located devices. Fig. 4.1 illustrates the network model and the states of some devices at a particular time.

In the previous chapter, the IoT network was modeled via the RGG $\mathbf{G} = \{\mathbf{V}, \mathbf{E}\}$. To include firewalls in the network model, the set of vertices in $\mathbf{V}$ are divided into a set of susceptible devices $\Xi \subseteq \mathbf{V}$ and a set of immune devices $\Theta \subseteq \mathbf{V}$. The immune set is defined as $\Theta = \{\mathbf{x}_i \in \mathbf{V} : \min_{\mathbf{a}_j \in \Psi} \|\mathbf{x}_i - \mathbf{a}_j\| \leq r_f\}$, where $\min_{\mathbf{a}_j \in \Psi} \|\mathbf{x}_i - \mathbf{a}_j\|$ is the minimum of the distances between $\mathbf{x}_i$ and all firewalls in Ψ. Hence, all the devices that are located in range (r_f) of any firewall are contained in the set Θ. On the other hand, the susceptible set $\Xi = \{\mathbf{x}_i \in \mathbf{V} \ : \ \min_{\mathbf{a}_j \in \Psi} \|\mathbf{x}_i - \mathbf{a}_j\| > r_f\}$ contains all the devices that are not located in any secured zone. Fig. 4.2 shows a realization of the RGG $\mathbf{G} = \{\mathbf{V}, \mathbf{E}\}$ with and without the firewalls.

Moreover, we isolate the susceptible devices and the links between them by defining the infection susceptible graph (ISG) $\mathcal{I} = \{\Xi, \mathcal{E}\}$, where Ξ is the set of susceptible devices and $\mathcal{E}$ is the set of links connecting them. The edges in $\mathcal{E}$ are D2D links that can be exploited for malware propagation between devices. The set $\mathcal{E}$ is defined as:

$$\mathcal{E} = \{\overline{\mathbf{x}_i \mathbf{x}_j} \ : \ \|\mathbf{x}_i - \mathbf{x}_j\| \leq r, \ \mathbf{x}_i, \mathbf{x}_j \in \Xi\} \,. \tag{4.1}$$

Fig. 4.2(b) highlights the ISG including all susceptible devices and links. It is important to note that infection cannot propagate from a device in Ξ to a device in Θ , or vice versa, due to the firewall protection for all devices in Θ. Hence, the definition in (4.1) for the edges in $\mathbf{E}$ is restricted to the ones between susceptible devices only.

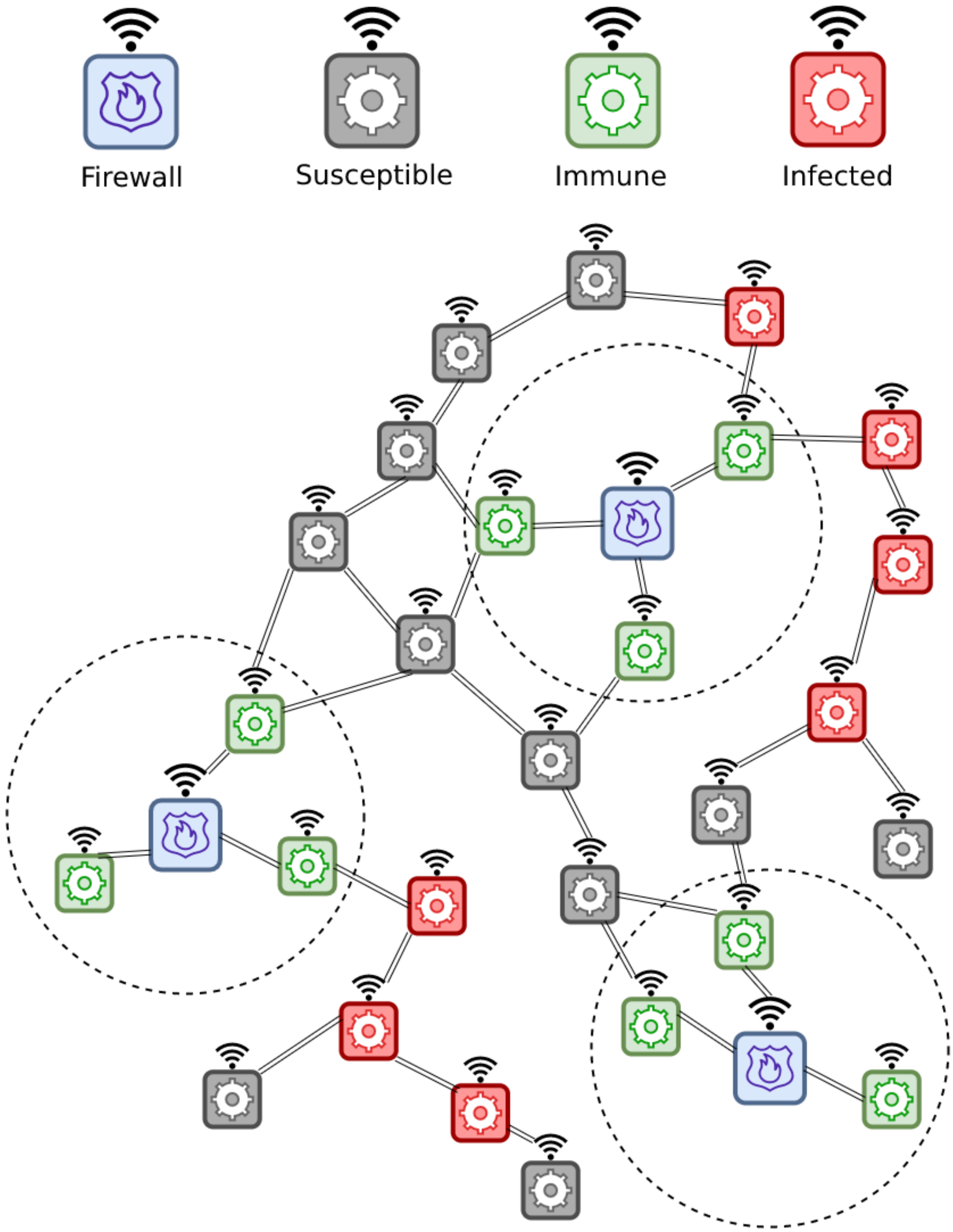


Figure 4.1: Illustration of IoT ad hoc wireless network with firewalls. IoT devices can either be susceptible, Immune or infected (compromised).

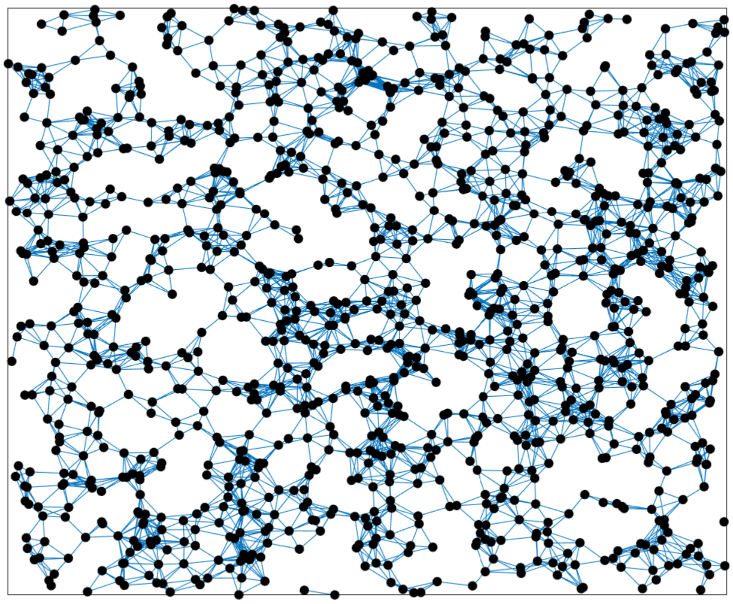
It can be seen that the ISG $\mathcal{I}$ is a subset of the network graph $\mathcal{I} \subseteq \mathbf{G}$. When there are no firewalls deployed (i.e., $\lambda_f = 0$), all the devices are susceptible, and the ISG converges to the network graph $\mathcal{I} = \mathbf{G}(\mathbf{V}, \mathbf{E})$. Moreover, the ISG $\mathcal{I}$ can be constructed by removing the vertices in Θ and their associated edges from $\mathbf{G}(\mathbf{V}, \mathbf{E})$.

In the previous chapter, we defined the degree of a device as the number of devices connected to it. In the context of firewalls, the existence of immune devices necessitates changing the definition. In particular, we redefine the degree of a device as the number of susceptible devices connected to it. Hence, the degree of a typical susceptible device $\mathbf{x}_i \in \Xi$ is the number of incident edges $K_i = |\mathcal{E}_i|$, where $\mathcal{E}_i = \{\overline{\mathbf{x}_i\mathbf{x}_j} : \|\mathbf{x}_i - \mathbf{x}_j\| \leq r,\ \mathbf{x}_j \in \Xi\}$.

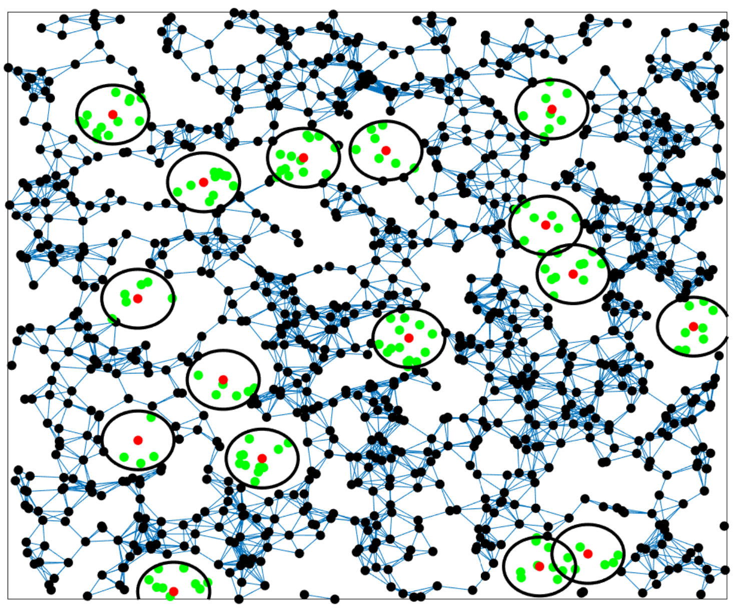
4.2 Analysis

In the previous chapter, we formed a malware propagation model based on the DBMF approach. In the derivation of the model, we utilized the conditional probability $\mathbb{P}\{k'|k\}$ which defines the degree correlation between neighboring vertices. This conditional probability will be different in the case of firewall deployment due to the fact that immune neighbors are not counted towards the degree of a device. The conditional probability is defined as the following:

$$\mathbb{P}\{k'|k\} = \frac{f_{k,k'}(k, k')}{\mathbb{P}\{K = k\}}, \tag{4.2}$$



(a) Before firewalls.



(b) After firewalls.

Figure 4.2: Two realizations of the RGG, (a) without firewalls, and (b) with firewalls. Immune devices and firewalls are highlighted in green and red respectively.

where $f_{k,k'}(k,k')$ is the joint degree distribution of neighboring devices, and $\mathbb{P}\{K=k\}$ is the marginal distribution of degrees in the network. In the next subsection, we derive both of these distributions, which will enable us to find the conditional distribution $\mathbb{P}\{k'|k\}$. Since the malware can only propagate through susceptible devices, these distributions are derived for susceptible devices only (on the ISG). Utilizing the same propagation model from the previous chapter but evaluating the conditional probability $\mathbb{P}\{k'|k\}$ under firewall deployment gives the malware and control commands propagation model outside the secured zones.

4.2.1 Joint and Marginal Degree Distributions in Firewalls Case

In the RGG $\mathbf{G}$, susceptible devices must lie outside the secured zones which means that their distance d_f to the closest firewall must be greater than the communication range of firewalls r_f. The distribution of the distance d_f from a random point to the closest firewall is given by the following CDF and PDF respectively:

$$F_{D_f}(d_f) = \mathbb{P}\{D_f < d_f\} = 1 - e^{-\pi\lambda_f d_f^2}, \qquad 0 < d_f < \infty \tag{4.3}$$

$$f_{D_f}(d_f) = 2\pi\lambda_f d_f \; e^{-\pi\lambda_f d_f^2}, \qquad 0 < d_f < \infty \tag{4.4}$$

where λ_f is the intensity of firewall deployment measured in (firewall/unit area). This distribution can be used to find the percentage of immune devices in the network. In particular, $F_{D_f}(r_f)$ is the percentage of devices lying inside the secured zones. Without loss of generality consider the case depicted in Fig. 4.3, which shows a susceptible device $\mathbf{x}_i \in \Xi$ with the closest firewall $\mathbf{x}_k \in \Psi$ distant by d_f. The D2D coverage area of the device is defined as $\mathbf{B}(\mathbf{x}_i, r)$ which is a circle of radius r and centered at $\mathbf{x}_i$. Similarly, the D2D coverage area of the firewall is defined by the set $\mathbf{B}(\mathbf{x}_k, r_f)$. The overall D2D area of the device overlaps with the area of the firewall, and the region X lying outside the firewall range is obtained by set subtraction $X = \mathbf{B}(\mathbf{x}_i, r) \setminus \mathbf{B}(\mathbf{x}_k, r_f)$. The degree of the device $\mathbf{x}_i$ is defined by the number of devices in region X, and the area of region X can be expressed in terms of d_f as the following:

$$A_x(d_f) = \pi r^2 - r^2 \cos^{-1}\left(\frac{d_f^2 + r^2 - r_f^2}{2\ d_f\ r}\right) + r_f^2 \cos^{-1}\left(\frac{d_f^2 - r^2 + r_f^2}{2\ d_f\ r_f}\right) - \frac{1}{2}\sqrt{-d_f^4 + 2d_f^2 r^2 + 2d_f^2 r_f^2 - r^4 + 2r^2 r_f^2 - r_f^4}, \quad d_f \leq r_f + r \quad (4.5)$$

Note that when $d_f > r_f + r$ there will be no overlap between the circles and the area A_x will be simply πr^2. Hence, we can derive the distribution of the degree of susceptible devices, which is given by the following lemma:

Lemma 4.1 *In GD-RGGs with firewalls intensity λ_f, range r_f, and intensity of IoT devices λ, the distribution of the degree of a typical susceptible device is given by the following PMF:*

$$\mathbb{P}\{K = k\} = \frac{2\pi\lambda_f}{e^{-\pi\lambda_f {r_f}^2}} \int_{r_f}^{\infty} \frac{\zeta\big(\lambda A_x(\zeta)\big)^k}{k!} e^{-\left(\lambda A_x(\zeta) + \pi\lambda_f \zeta^2\right)}\, d\zeta,\ \ k \geq 0. \quad (4.6)$$

Proof. *See **Appendix A.2**.* ∎

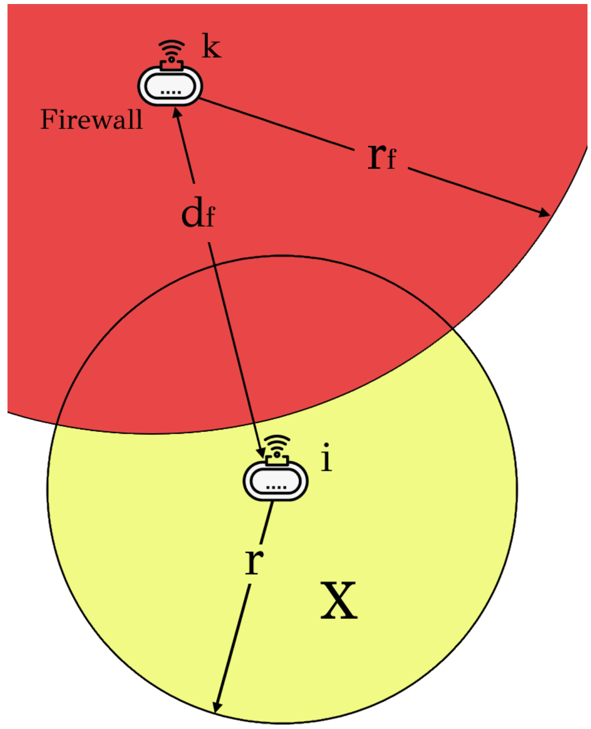


Figure 4.3: IoT device neighbor to a firewall. The degree of device i is determined by the number of devices in the yellow region since only those will be susceptible

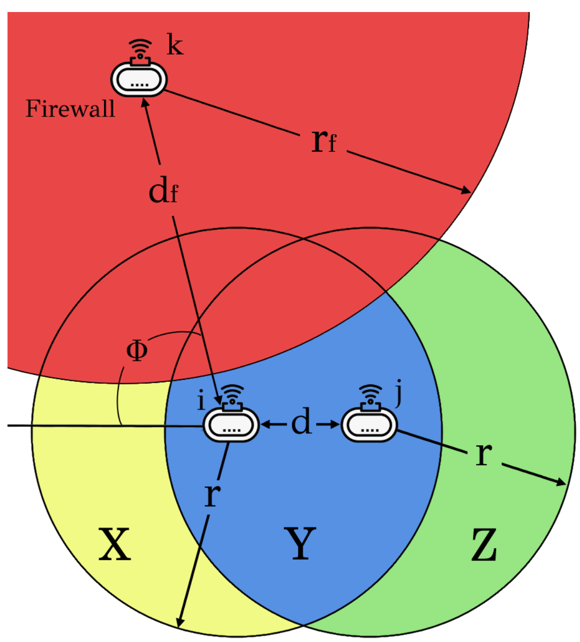


Figure 4.4: The general case for two connected devices i and j separated by distance $d \leq r$ and neighbor to a close firewall k. The coverage areas of both form two overlapping circles with the same radius r. They can be divided into three disjoint areas which are labeled X,Y and Z.

To derive the joint distribution of degrees between two connected susceptible devices, we consider the general case as shown in Fig.4.4. Two connected devices centered at $\mathbf{x}_i$ and $\mathbf{x}_j$ separated by distance d. A neighboring firewall is centered at $\mathbf{x}_k$ and is located at a distance d_f from the closest of the two IoT devices (device i). The firewall coverage area $\mathbf{B}(\mathbf{x}_k, r_f)$ may overlap with the coverage area of the two devices depending on d, d_f, and the angle of rotation ϕ. The three regions X, Y and Z are given by:

$$X = \mathbf{B}(\mathbf{x}_i, r) \setminus \mathbf{B}(\mathbf{x}_j, r) \setminus \mathbf{B}(\mathbf{x}_k, r_f)$$

$$Z = \mathbf{B}(\mathbf{x}_j, r) \setminus \mathbf{B}(\mathbf{x}_i, r) \setminus \mathbf{B}(\mathbf{x}_k, r_f)$$

$$Y = (\mathbf{B}(\mathbf{x}_i, r) \cap \mathbf{B}(\mathbf{x}_j, r)) \setminus \mathbf{B}(\mathbf{x}_k, r_f)$$

Fig. 4.4 shows one case for the overlap of these three circles. Depending on the values of d, d_f, and ϕ, we have one of the following four cases for the overlap of the three circles:

- Case 1: The overlap of the three circles forms a circular triangle in the middle as illustrated by Fig.4.5 (a).
- Case 2: There is an overlap between the three circles but it is not a circular triangle as illustrated by Fig.4.5 (b).
- Case 3: There is only an overlap between the firewall and device i as shown in Fig.4.5 (c).
- Case 4: The firewall does not overlap with any of the circles, as shown in Fig.4.5

(d).

The areas of X, Y and Z are denoted by A_x, A_y, and A_z respectively. Appendix.B.1 is dedicated to finding these areas in closed form as a function of d, d_f, and ϕ, for the four cases. Once the areas are derived we can proceed in deriving the joint degree distribution. The following lemma provides the PMF of joint degrees with firewalls deployment:

Lemma 4.2 *In GD-RGGs with firewalls deployment intensity λ_f and range r_f, the joint degree PMF of neighboring vertices is given by:*

$$f_{k,k'}(k,k') = \int_0^r \int_{r_f}^{\infty} \int_0^{\phi_{max}} f_{k,k'|d,d_f,\phi}(k,k') \frac{f_{D_f}(\psi)\ f_D(\zeta)}{[1-F_{D_f}(r_f)]\ \phi_{max}}\, d\phi\, d\psi\, d\zeta, \quad (4.7)$$

where $\phi_{max} = \pi - \cos^{-1}\frac{d}{2d_f}$, and the conditional distribution $f_{k,k'|d,d_f,\phi}(k,k')$ is given by:

$$f_{k,k'|d,d_f,\phi}(k,k') = \sum_{t=0}^{\min(k,k')-1} \frac{(\lambda A_x)^{k-t-1}(\lambda A_z)^{k'-t-1}(\lambda A_y)^{t}}{(k-t-1)!\ (k'-t-1)!\ t!} \exp\left(-\lambda\left(A_x+A_z+A_y\right)\right) \quad (4.8)$$

Proof. *See **Appendix A.3**.* ▌

Since we have both $f_{k,k'}(k,k')$ and $\mathbb{P}\{K=k\}$, we can find the conditional probability $\mathbb{P}\{k'|k\}$. Therefore, the propagation model outside the secured zones is defined by the following system of equations:

$$\pi_k^H = \frac{\mu_k}{\mu_k + k\sigma_1(1-\theta_k^H)} \quad (4.9)$$

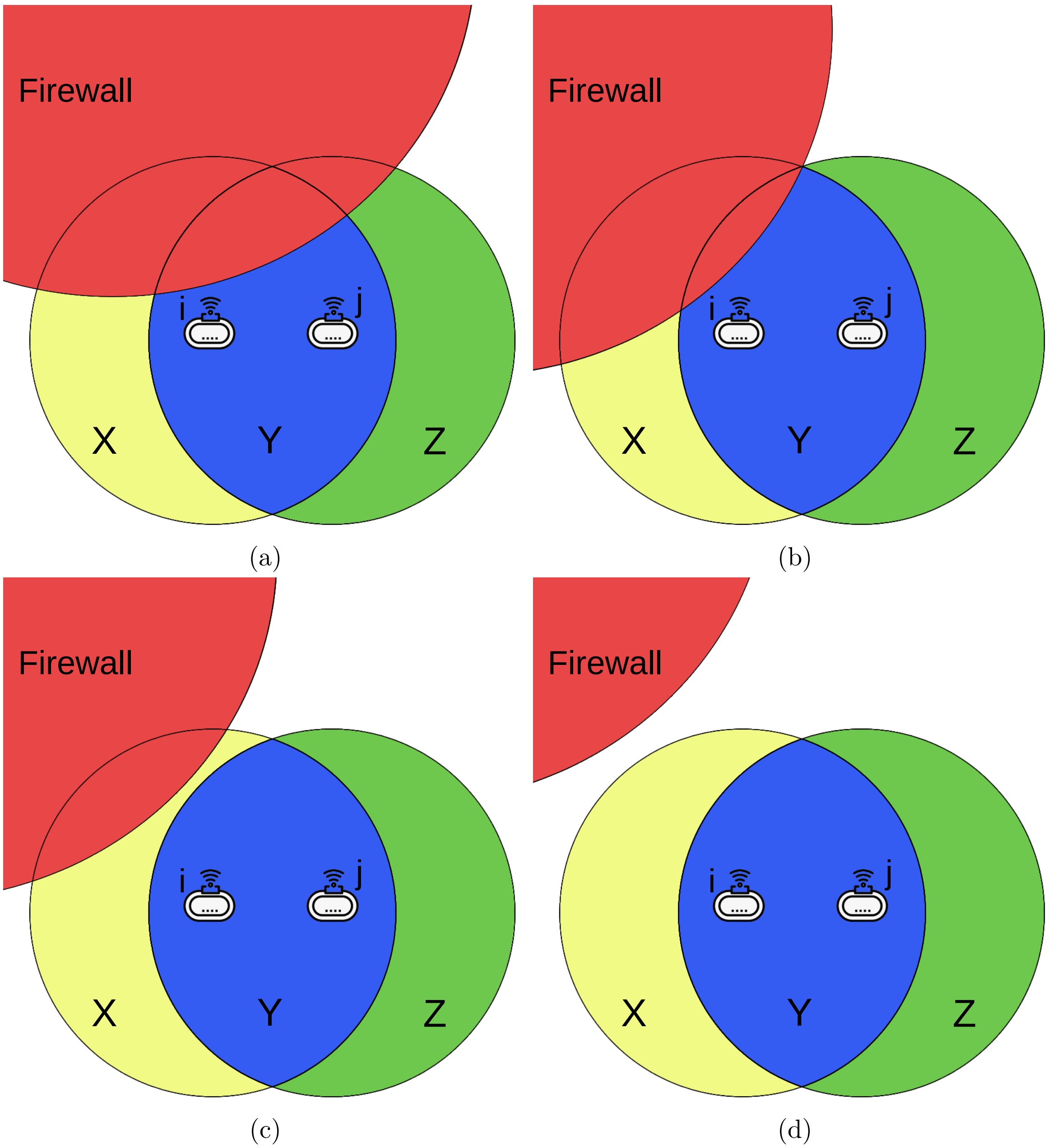


Figure 4.5: The different cases of overlap between firewall and devices i and j

$$\pi_k^{\hat{I}} = \frac{k^2\sigma_1\sigma_2(1-\theta_k^H)\theta_k^{\hat{I}}}{\left(\mu_k + k\sigma_1(1-\theta_k^H)\right)\left(\beta+\mu_k+k\sigma_2\theta_k^{\hat{I}}\right)} \tag{4.10}$$

$$\theta_k^H = \sum_{k'=1}^{\infty} \frac{f_{k,k'}\left(k,k'\right)\pi_{k'}^H}{\mathbb{P}\{K=k\}}, \tag{4.11}$$

$$\theta_k^{\hat{I}} = \sum_{k'=1}^{\infty} \frac{f_{k,k'}\left(k,k'\right)\pi_{k'}^{\hat{I}}}{\mathbb{P}\{K=k\}}, \tag{4.12}$$

This is the same model as the previous chapter but the only difference is the joint and marginal degree distributions $f_{k,k'}(k,k')$ and $\mathbb{P}\{K=k\}$ will be evaluated from equations (4.7) and (4.6).

4.3 Results and Discussion

In this section, we present the results of including spatial firewalls along with dynamic patching to thwart the malware propagation in IoT wireless networks. The theoretical distribution provided in eqs. (4.7) is compared with an empirical distribution generated by MATLAB for $n = 10^6$ observations, and the result is shown in Fig. 4.6. The figure validates the theoretical distribution since it matches the empirical distribution. The effect of firewalls on the degree distribution is illustrated in Fig. 4.7. As shown, firewalls deployment causes the degree distribution to be more concentrated on the lower-degree devices, and as we increase the range or intensity of firewalls the concentration increases.

The same optimization problem in 3.18 was solved using the interior point algorithm in the case of firewalls presence. We compare the optimal patching rates before

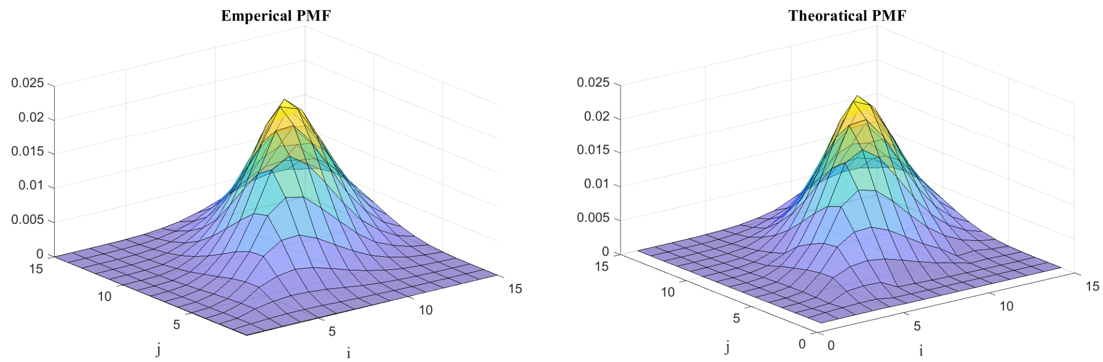
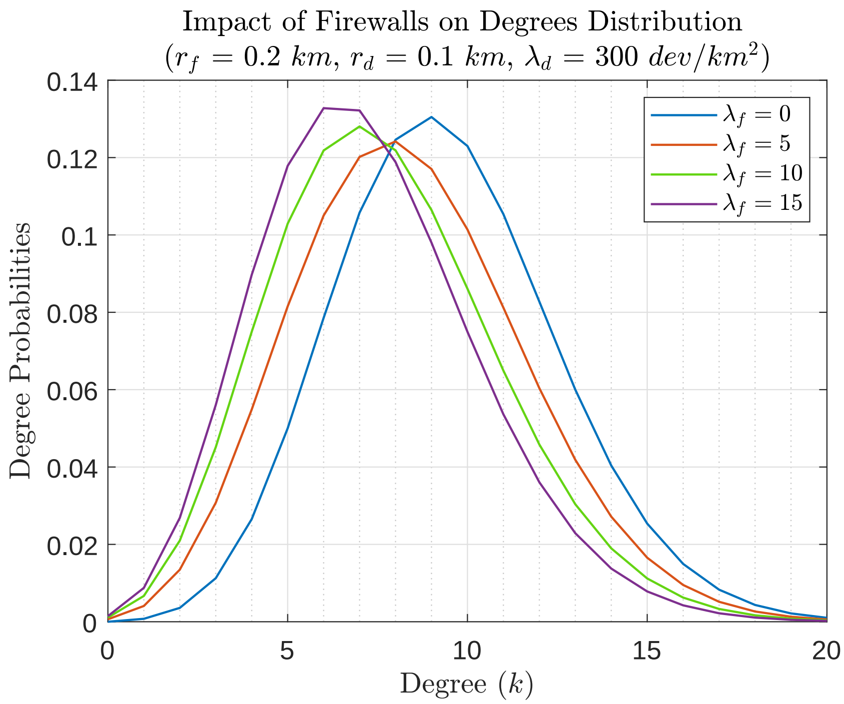
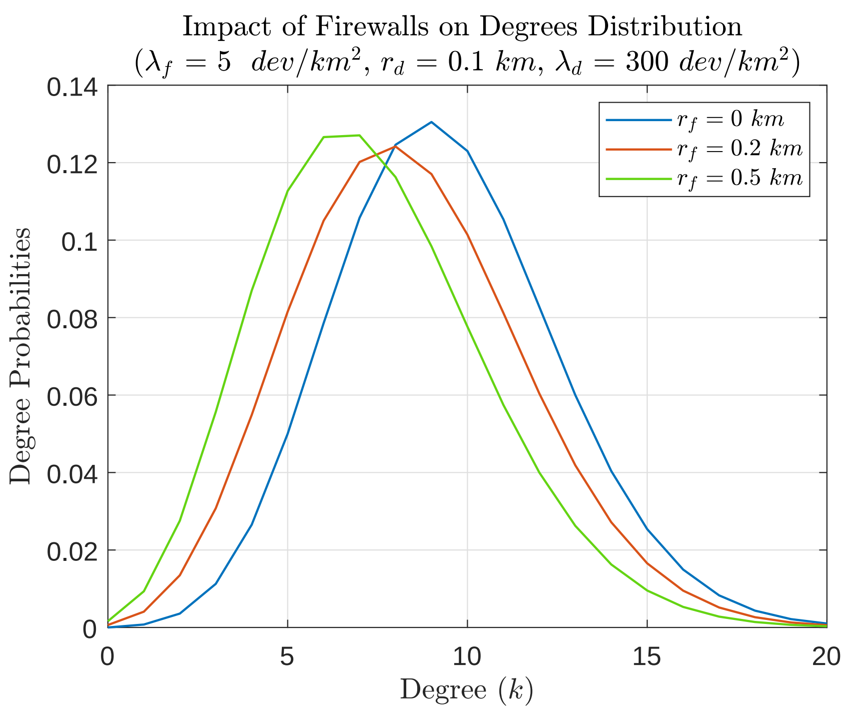


Figure 4.6: Validating the theoretical joint distribution of degrees when firewalls are present.

and after the deployment of firewalls for different minimum thresholds of healthy devices τ_H. The intensity and range of firewalls are chosen to be $\lambda_f = 2.85\ device/km^2$ and $r_f = 0.2\ km$ respectively. In this case, 30% of the devices are immunized since we have $\int_0^{0.2} f_{D_f}(\psi)d\psi = 0.3$. The results of the comparison are shown in the figures 4.8, 4.9, and 4.10 for $\tau_H = 0.6$, $\tau_H = 0.7$, and $\tau_H = 0.8$ respectively. As shown, most of the degrees in the network experienced a decrease in the patching rate when firewalls are deployed which is expected due to the immunization of 30% of the devices hence the required number of susceptible devices to be protected by patching is less. As an exception, few lower degrees have higher optimal patching rates after firewalls deployment. The reason is that firewalls cause the distribution of degrees to be shifted towards the left and become more concentrated on the lower degrees as shown in Fig. 4.7. Therefore, lower-degree devices become more popular in the network and patching them at a higher rate contributes more towards high percentage of healthy devices. In other words, despite having a bit higher patching rates for lower degree devices, the overall cost $\phi(\boldsymbol{\mu})$ of the patching strategy after firewalls deployment is



(a) Increasing firewalls intensity.



(b) Increasing firewalls range.

Figure 4.7: The impact of spatial firewalls on the distribution of degree (a) increasing the intensity of firewalls λ_f, (b) increasing the range of firewalls r_f.

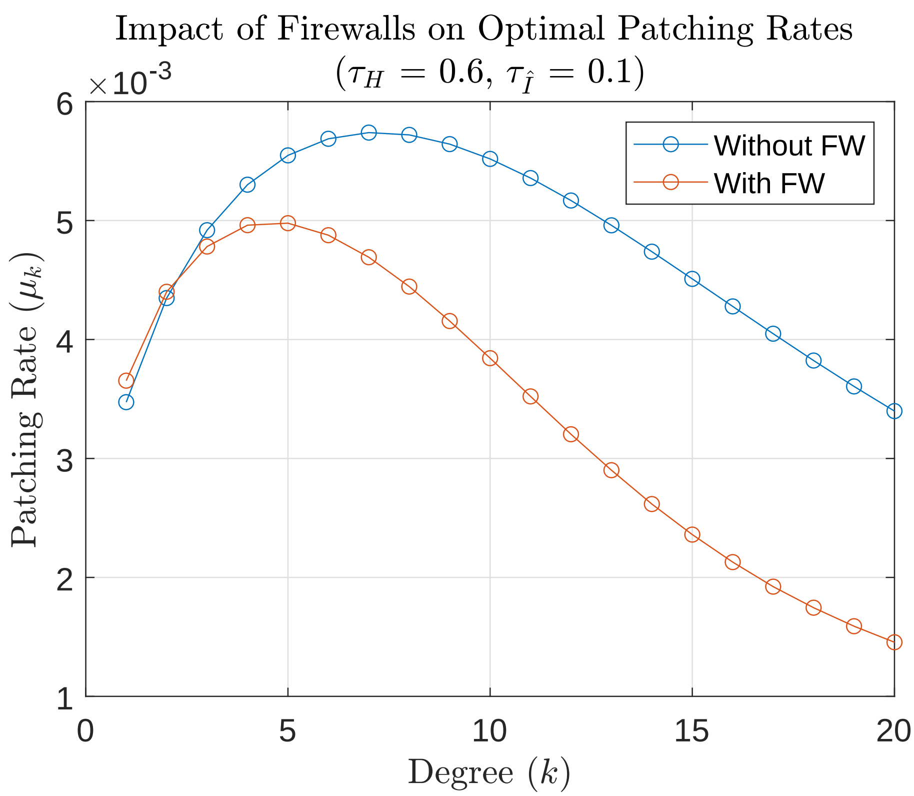


Figure 4.8: Impact of firewalls on the optimal patching rates ($\tau_H = 0.6$).

much lower than the non-firewalls case. The impact of the design parameters λ_f and r_f on the optimal patching rates is demonstrated in Fig. 4.11. Increasing the range or intensity of firewalls causes the optimal patching rates to be decreased at all degrees, however the intensity of the firewalls has more effect on the optimal patching rates.

A simulation of the malware propagation is carried out and the percentage of healthy devices is plotted versus time. In the first experiment, we start with all devices infected and apply different patching strategies for the thresholds of healthy devices, $\tau_H = 0.6$, $\tau_H = 0.7$, and $\tau_H = 0.8$. As shown in Fig 4.12, the patching strategies lead to constant percentage of healthy devices, which satisfy their respective threshold. This is also true for the second experiment where we start at $t = 0$ with a percentage of healthy devices close to the required threshold as shown in Fig. 4.13.

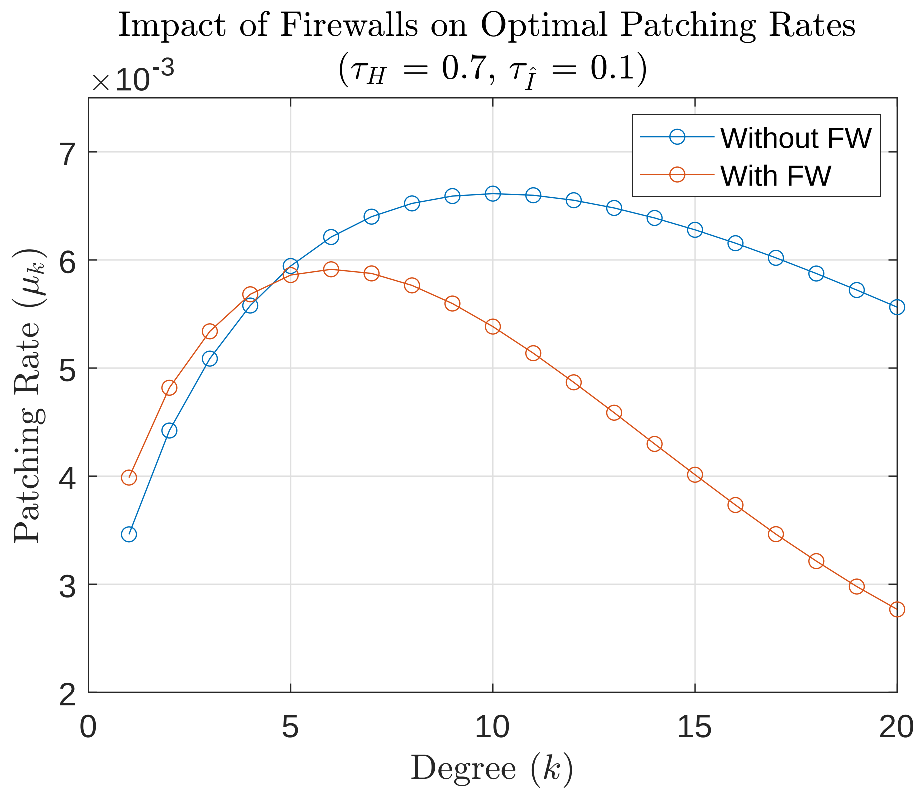


Figure 4.9: Impact of firewalls on the optimal patching rates ($\tau_H = 0.7$).

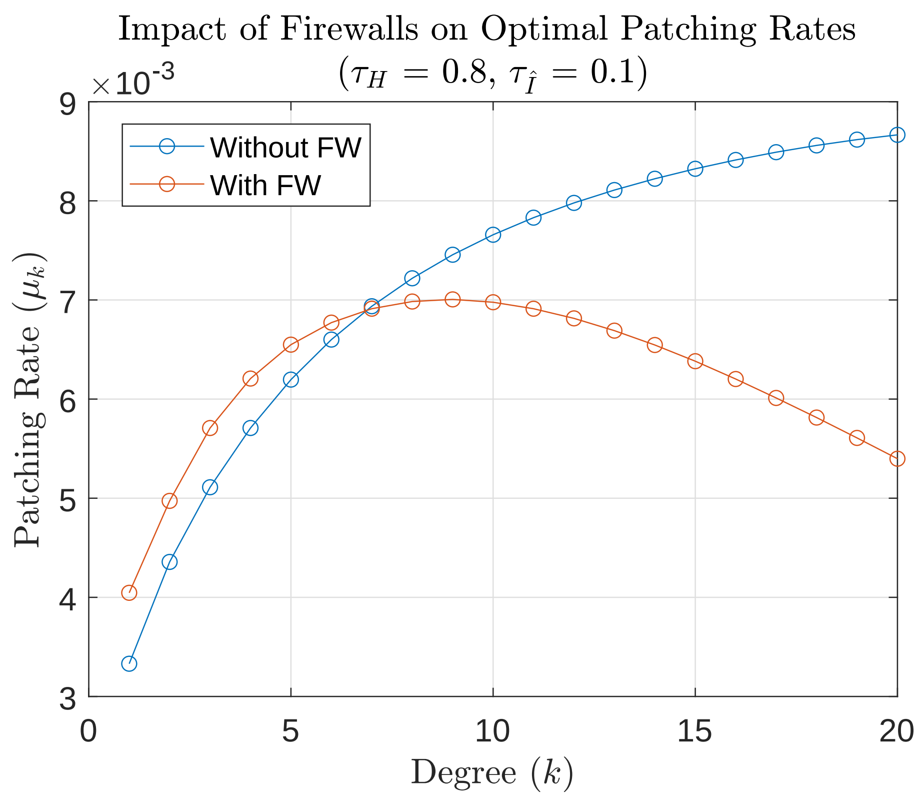
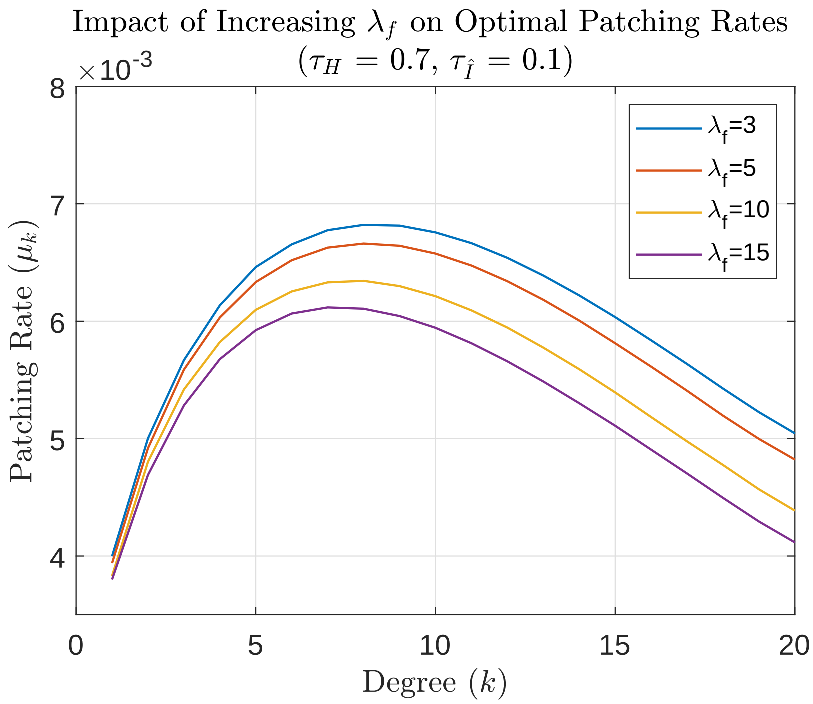
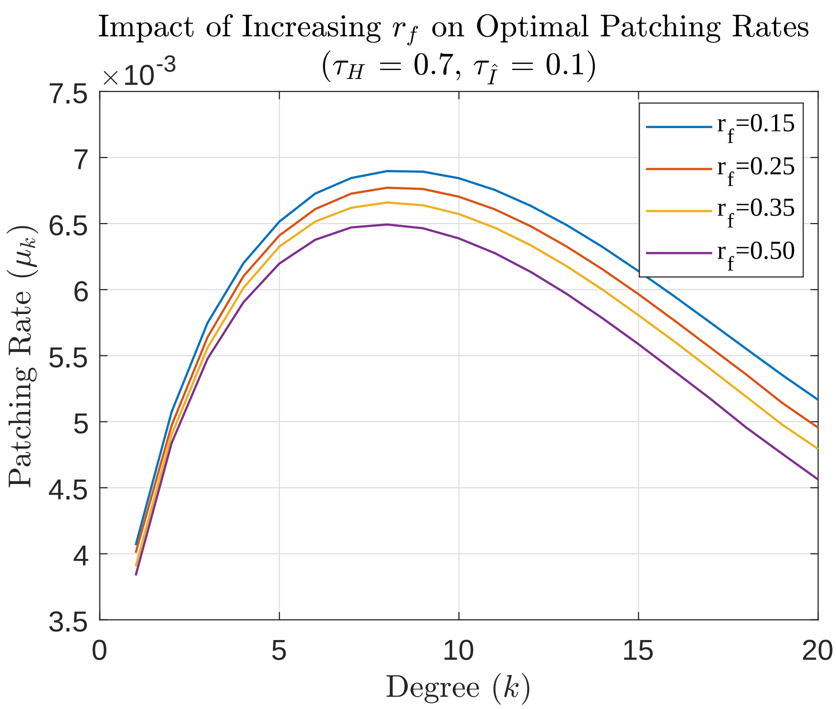


Figure 4.10: Impact of firewalls on the optimal patching rates ($\tau_H = 0.8$).



(a) Increasing firewalls intensity.



(b) Increasing firewalls range.

Figure 4.11: The impact of varying the design parameters r_f and λ_f on the optimal patching rates: (a) increasing the intensity of firewalls, (b) increasing the range of firewalls

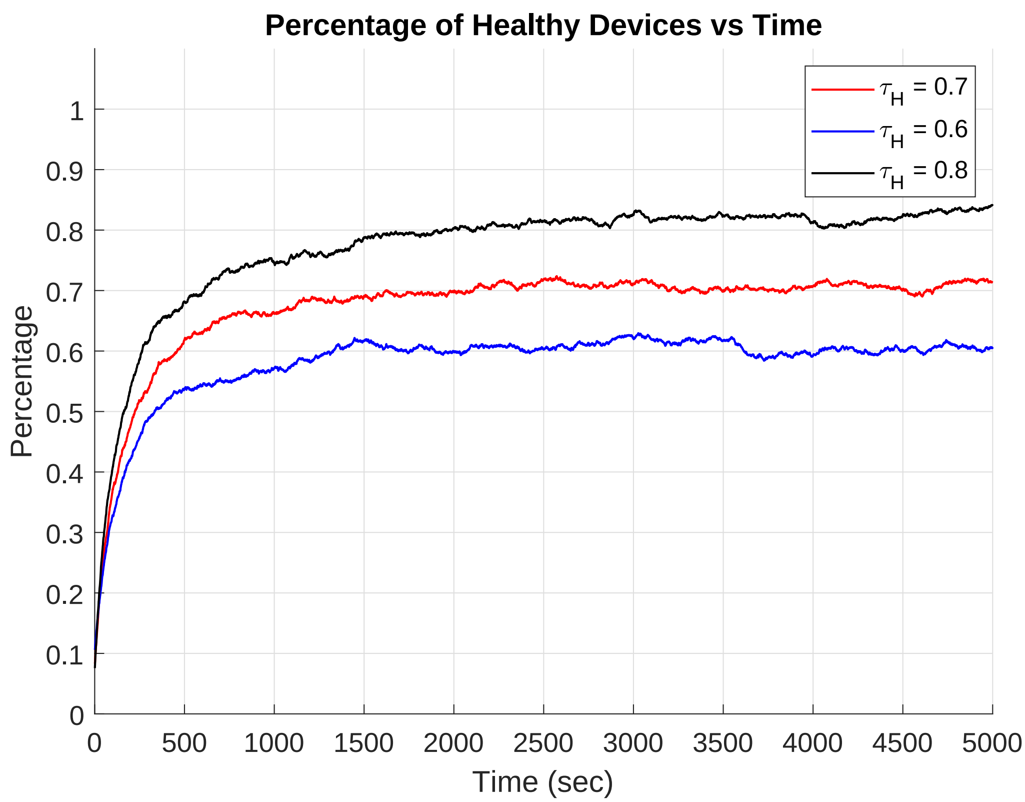


Figure 4.12: Simulation of the patching strategies of different thresholds: start with a completely infected network.

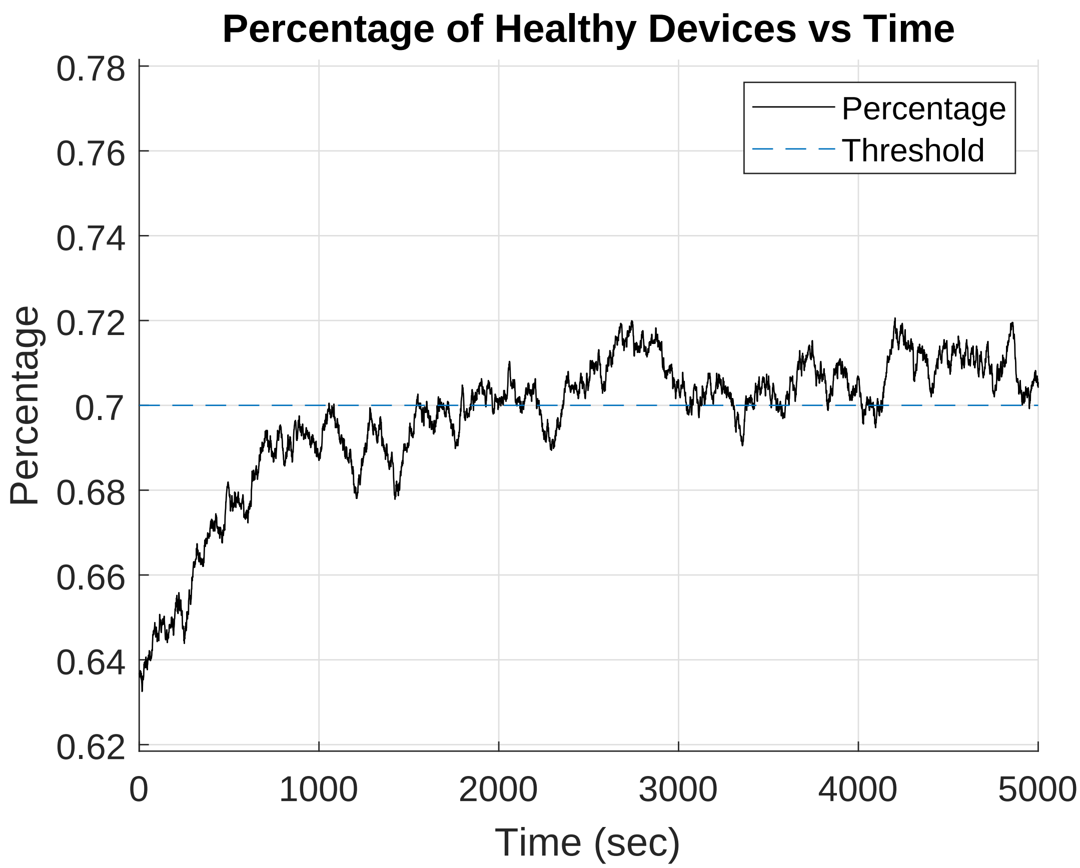


Figure 4.13: Simulation of the patching strategy of $\tau_H = 0.7$: start near the threshold τ_H.

APPENDIX A

PROOFS

A.1 Proof of Lemma 1.

In RGGs, the numbers of devices in disjoint regions have independent Poisson distributions. Exploiting such property, we first condition on the separation distance d and the number of devices $t = |\mathbf{V} \cap Y|$ in the common region Y. Conditioned on d and t, the joint degree distribution $\mathbb{P}\{k, k'|d, t\}$ can be expressed as following:

$$\mathbb{P}\{k, k'|d, t\} = \mathbb{P}\{|\mathbf{V} \cap X| = k - t - 1\} \times \mathbb{P}\{|\mathbf{V} \cap Z| = k' - t - 1\}, \tag{A.1}$$

where $|\mathbf{V} \cap X|$ refers to the number of devices in region X. By averaging over all values of t from 0 to $min(k, k') - 1$ we obtain the following:

$$\mathbb{P}\{k, k'|d\} = \sum_{t=0}^{\min(k,k')-1} \mathbb{P}\{k, k'|d, t\} \times \mathbb{P}\{|\mathbf{V} \cap Y| = t\}. \tag{A.2}$$

The number of devices in the regions X, Y, and Z are given respectively by the following:

$$\mathbb{P}\{|\mathbf{V} \cap X| = k-t-1\} = \frac{(\lambda A_x)^{k-t-1} e^{-\lambda A_x}}{(k-t-1)!}, \tag{A.3}$$

$$\mathbb{P}\{|\mathbf{V} \cap Z| = k'-t-1\} = \frac{(\lambda A_z)^{k'-t-1} e^{-\lambda A_z}}{(k'-t-1)!}, \tag{A.4}$$

$$\mathbb{P}\{|\mathbf{V} \cap Y| = t\} = \frac{(\lambda A_y)^{t} e^{-\lambda A_y}}{t!}, \tag{A.5}$$

where A_x and A_z are the areas of X and Z respectively, and are both equal $A_x = A_z = \pi r^2 - A_y$. Finally, By averaging over all values of d from 0 to r we obtain the result in Lemma 3.1:

$$f_{k,k'}\left(k, k'\right) = \int_0^r \mathbb{P}\{k, k'|\zeta\} \times f_D\left(\zeta\right) \, d\zeta. \tag{A.6}$$

A.2 Proof of Lemma 2.

Given d_f, then the conditional probability $\mathbb{P}\{K = k|d_f\}$ can be obtained as:

$$\mathbb{P}\{K = k|d_f\} = \mathbb{P}\left\{|\mathbf{V} \cap X| = k\right\} = \frac{\left(\lambda A_x\right)^k}{k!} e^{-\lambda A_x} \tag{A.7}$$

Then we average the conditional probability over $d_f > r_f$, since we are seeking the distribution for susceptible devices only.

$$\mathbb{P}\{K = k\} = \int_{r_f}^{\infty} \mathbb{P}\{K = k|d_f\} \times \frac{f_{D_f}\left(\zeta\right)}{1 - F_{D_f}(r_f)} d\zeta, \;\; k \geq 0 \tag{A.8}$$

Utilizing the distribution of d_f in (4.4) and (4.3), we reach at the result in Lemma 4.1. This concludes the proof.

A.3 Proof of Lemma 3.

To prove lemma 3 we start by finding the conditional distribution $f_{k,k'|d,d_f,\phi}(k,k')$. In the same manner as the proof of lemma 1, we can reach at the expression in (4.8). Then we need to average over the three random variables d, d_f and ϕ. we start averaging over the rotation angle ϕ, which has a uniform distribution from 0 to ($\phi_{max} = \pi - \cos^{-1}\frac{d}{2d_f}$). We stop at ϕ_{max} because we assumed without loss of generality that device $\mathbf{x}_i$ is closer to the firewall than device $\mathbf{x}_j$, hence ϕ_{max} is the maximum allowable angle.

$$f_{k,k'|d,d_f}(k,k') = \int_0^{\phi_{max}} \frac{f_{k,k'|d,d_f,\phi}(k,k')}{\phi_{max}} d\phi. \tag{A.9}$$

Then we average over d_f, but only on the interval from r_f to ∞. This is done because we want to find the distribution for susceptible devices only.

$$f_{k,k'|d}(k,k') = \int_{r_f}^{\infty} f_{k,k'|d,d_f}(k,k') \times \frac{f_{D_f}(\psi)}{1 - F_{D_f}(r_f)} d\psi. \tag{A.10}$$

Finally we average over d on the interval from 0 to r, to reach to the result in lemma 3.

$$f_{k,k'}(k,k') = \int_0^{r} f_{k,k'|d}(k,k')\, f_D(\zeta)\, d\zeta. \tag{A.11}$$

APPENDIX B

SUPPLEMENTARY MATERIAL

B.1 The areas of X, Y, and Z in firewalls case.

In this appendix we define the areas A_x, A_y and A_z as functions of d, d_f and ϕ. To make the derivation easier to follow, we will refer to the three circles of device i, device j, and the firewall as circle 1, circle 2 and circle 3 respectively, and their radii are denoted as r_1, r_2 and r_3. We also denote the distances between their centers appropriately (e.g. d_{ij} refers to the distance between center i and center j). We will also denote the point of intersection between circle i and circle j as (x_{ij}, y_{ij}). The notations can be visualized in Fig. B.1.

As illustrated in Fig. 4.5, there are four cases for the overlap between the three circles. The first case can be seen in Fig. 4.5 (a) where there is a circular triangle formed by the overlap. This case is investigated in [27], and the area of the circular triangle is derived in terms of the radii and distances between the circles. The following

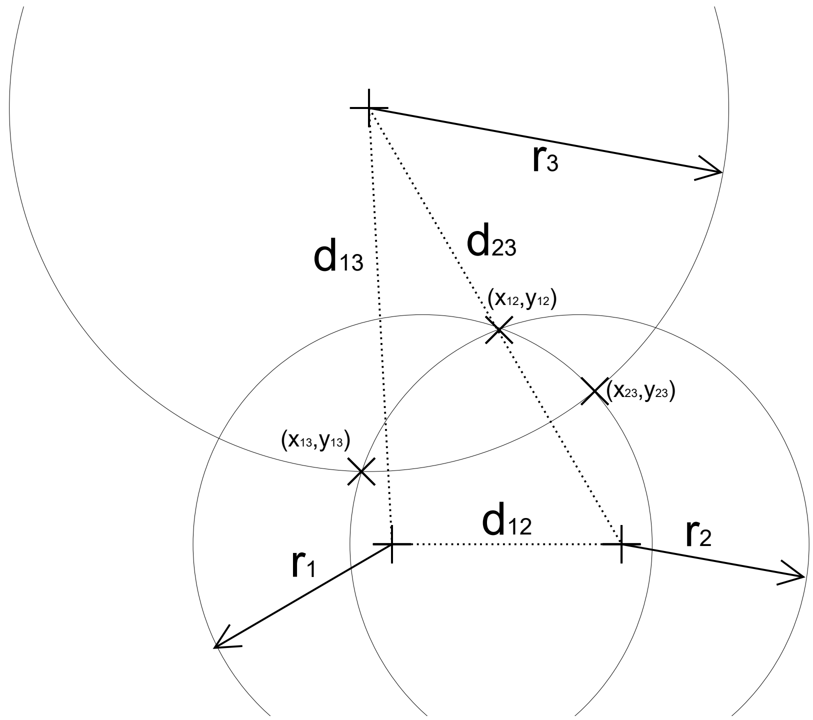


Figure B.1: Visualization of the general case for the overlap between three circles.

condition grantees the existence of the circular triangle:

$$(x_{12} - d_{13}\cos\theta)^2 + (y_{12} - d_{13}\sin\theta)^2 < r_3^2 \tag{B.1}$$

where

$$x_{12} = \frac{d_{12}}{2}, \quad y_{12} = \frac{1}{2}\sqrt{4r_1^2 - d_{12}^2},$$

$$\cos\theta = (d_{12}^2 + d_{13}^2 - d_{23}^2)/2d_{13}d_{12}, \quad \sin\theta = \sqrt{1-\cos^2\theta},$$

The areas A_x, A_y and A_z in this case have the following form:

$$A_x = \pi r_1^2 - O_{12} - (O_{13} - T_c),$$

$$A_y = O_{12} - T_c,$$

$$A_z = \pi r_2^2 - O_{12} - (O_{23} - T_c),$$

where T_c is the area of the circular triangle, and O_{ij} is the overlap area between circle i and circle j. All the overlap areas O_{ij} between a pair of circles can be found by the following expression:

$$\begin{aligned} O_{ij} = {r_i}^2 \cos^{-1}\left(\frac{d_{ij}^2 + {r_i}^2 - r_j^2}{2\ d_{ij}\ r_i}\right) + r_j^2 \cos^{-1}\left(\frac{d_{ij}^2 - {r_i}^2 + r_j^2}{2\ d_{ij}\ r_j}\right) \\ - \frac{1}{2}\sqrt{-d_{ij}^4 + 2d_{ij}^2 {r_i}^2 + 2d_{ij}^2 r_j^2 + 2{r_i}^2 r_j^2 - {r_i}^4 - r_j^4} \end{aligned} \tag{B.2}$$

The area of the circular triangle T_c is given in terms of the cords lengths c_1, c_2 and c_3 as:

$$\begin{aligned} T_c = \frac{1}{4}\sqrt{(c_1 + c_2 + c_3)(c_2 + c_3 - c_1)(c_1 + c_3 - c_2)(c_1 + c_2 - c_3)} \\ + \sum_{k=1}^{3} {r_k}^2 \sin^{-1}\left(\frac{c_k}{2r_k}\right) - \frac{c_k}{4}\sqrt{4{r_k}^2 - c_k} \end{aligned} \tag{B.3}$$

where,

$$\begin{aligned} {c_1}^2 &= (x_{12} - x_{13})^2 + (y_{12} - y_{13})^2, \\ {c_2}^2 &= (x_{12} - x_{23})^2 + (y_{12} - y_{23})^2, \\ {c_3}^2 &= (x_{13} - x_{23})^2 + (y_{13} - y_{23})^2, \end{aligned} \tag{B.4}$$

where (x_{ij}, y_{ij}) is the coordinates of the point of intersection between circle i and circle

j. The first coordinates of intersection (x_{12}, y_{12}) are given by:

$$x_{12} = \frac{d_{12}}{2}, \quad y_{12} = \frac{1}{2}\sqrt{4r_1^2 - d_{12}^2},$$

The point of intersection (x_{13}, y_{13}) can be obtained by first finding the coordinates (x'_{13}, y'_{13}) of the translated coordinate system (x', y') that has its origin at the center of circle 1 and the x' axis passes through the center of circle 3. Hence the point (x'_{13}, y'_{13}) is given by:

$$x'_{13} = \frac{{r_1}^2 - {r_3}^2 + {d_{13}}^2}{2d_{13}}, y'_{13} = \frac{-1}{2d_{13}}\sqrt{2{d_{13}}^2\left({r_1}^2 + {r_3}^2\right) - \left({r_1}^2 - {r_3}^2\right)^2 - {d_{13}}^4}. \quad \text{(B.5)}$$

Then the translation to the coordinate system (x, y) is made by the the following transformation:

$$x_{13} = x'_{13}\cos\theta' - y'_{13}\sin\theta', \quad y_{13} = x'_{13}\sin\theta' + y'_{13}\cos\theta', \quad \text{(B.6)}$$

$$\cos\theta' = \frac{{d_{12}}^2 + {d_{13}}^2 - {d_{23}}^2}{2d_{12}d_{13}}, \quad \sin\theta' = \sqrt{1 - \cos^2\theta'}. \quad \text{(B.7)}$$

The point of intersection (x_{23}, y_{23}) can be obtained by first finding the coordinates (x''_{23}, y''_{23}) of the translated coordinate system (x'', y'') that has its origin at the center of circle 2 and the x'' axis passes through the center of circle 3. Hence the point (x''_{23}, y''_{23}) is given by:

$$x''_{23} = \frac{{r_2}^2 - {r_3}^2 + {d_{23}}^2}{2d_{23}}, y''_{23} = \frac{1}{2d_{23}}\sqrt{2{d_{23}}^2\left({r_2}^2 + {r_3}^2\right) - \left({r_2}^2 - {r_3}^2\right)^2 - {d_{23}}^4}. \quad \text{(B.8)}$$

Then the transformation to the (x, y) coordinate system is made by the following:

$$x_{23} = x''_{23} \cos\theta'' - y''_{23} \sin\theta'' + d_{12}, \quad y_{23} = x''_{23} \sin\theta'' + y''_{23} \cos\theta'', \tag{B.9}$$

$$\cos\theta'' = \frac{{d_{12}}^2 + {d_{23}}^2 - {d_{13}}^2}{2d_{12}d_{23}}, \quad \sin\theta'' = \sqrt{1 - \cos^2\theta''}. \tag{B.10}$$

The second case is when there is an overlap between the three circles, but it is not a circular triangle. This case of overlap occurs when the condition in (B.1) is not satisfied, and the following conditions are satisfied:

$$d_{23} < r_3 + r_2 \tag{B.11}$$

$$d_{13} < r_3 + r_1 \tag{B.12}$$

In this case the areas are given by:

$$A_x = \pi r_1^2 - O_{12} - (O_{13} - O_{23})$$

$$A_y = O_{12} - O_{23}$$

$$A_z = \pi r_2^2 - O_{12}$$

The third case is where there is no overlap between circle 3 and circle 2, but there is an overlap between circle 3 and circle 1. This case occurs when the condition (B.12) is satisfied, and (B.11) is not. In this case, only A_x and A_y change to the following:

$$A_x = \pi r_1^2 - O_{12} - O_{13}$$

$$A_y = O_{12}$$

$$A_z = \pi r_2^2 - O_{12}$$

In the last case, circle 3 does not overlap with any of the other circles. This case requires condition (B.12) to be false. In this case the areas are given by:

$$A_x = \pi r_1^2 - O_{12}$$

$$A_y = O_{12}$$

$$A_z = \pi r_2^2 - O_{12}$$

Hence, we can put the areas A_x, A_y and A_z in the following definition:

$$A_x = \begin{cases} \pi r_1^2 - O_{12} - (O_{13} - T_c) & \text{, case 1} \\ \pi r_1^2 - O_{12} - (O_{13} - O_{23}) & \text{, case 2} \\ \pi r_1^2 - O_{12} - O_{13} & \text{, case 3} \\ \pi r_1^2 - O_{12} & \text{, otherwise} \end{cases} \tag{B.13}$$

$$A_y = \begin{cases} O_{12} - T_c & \text{, case 1} \\ O_{12} - O_{23} & \text{, case 2} \\ O_{12} & \text{, otherwise} \end{cases} \tag{B.14}$$

$$A_z = \begin{cases} \pi r_2^2 - O_{12} - (O_{23} - T_c) & \text{, case 1} \\ \pi r_2^2 - O_{12} & \text{, otherwise} \end{cases} \tag{B.15}$$

Finally, we make the following substitutions to put the areas as functions of d, d_f and ϕ:

$$d_{12} = d,\ d_{13} = d_f,\ d_{23} = \sqrt{d^2 + d_f^2 - 2dd_f\cos(\pi - \phi)},\ r_1 = r_2 = r,\ r_3 = r_f. \tag{B.16}$$

REFERENCES

[1] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, “6g internet of things: A comprehensive survey,” *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 359–383, 2022.

[2] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-physical systems security—a survey,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[3] J. Kleinberg, “The wireless epidemic,” *Nature*, vol. 449, no. 7160, pp. 287–288, 2007.

[4] D. C. Smith, “Cybersecurity in the energy sector: are we really prepared?” pp. 265–270, 2021.

[5] L. E. S. Jaramillo, “Malware detection and mitigation techniques: lessons learned from mirai ddos attack,” *Journal of Information Systems Engineering & Management*, vol. 3, no. 3, p. 19, 2018.

[6] P. Moriuchi and S. Chohan, “Mirai-variant iot botnet used to target financial sector in january 2018,” *Recorded Future Cyber Threat Analysis Report*, pp. 118–140, 2018.

[7] M. Nekovee, "Worm epidemics in wireless ad hoc networks," *New Journal of Physics*, vol. 9, no. 6, p. 189, 2007.

[8] B. Liu, W. Zhou, L. Gao, H. Zhou, T. H. Luan, and S. Wen, "Malware propagations in wireless ad hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 1016–1026, 2018.

[9] G. Yan and S. Eidenbenz, "Modeling propagation dynamics of bluetooth worms (extended version)," *IEEE Transactions on Mobile Computing*, vol. 8, no. 3, pp. 353–368, 2009.

[10] Z. Lu, W. Wang, and C. Wang, "On the evolution and impact of mobile botnets in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 15, 2016.

[11] M. J. Farooq and Q. Zhu, "Modeling, analysis, and mitigation of dynamic botnet formation in wireless iot networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, 2019.

[12] J. Kim, S. Radhakrishnan, and S. K. Dhall, "Measurement and analysis of worm propagation on internet network topology," in *Proceedings. 13th International Conference on Computer Communications and Networks (IEEE Cat. No. 04EX969).* IEEE, 2004, pp. 495–500.

[13] Q. Wang, Z. Chen, and C. Chen, "On the characteristics of the worm infection family tree," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1614–1627, 2012.

[14] M. Vojnovic and A. J. Ganesh, "On the race of worms, alerts, and patches," *IEEE/ACM Transactions on Networking*, vol. 16, no. 5, pp. 1066–1079, 2008.

[15] Z. Chen, L. Gao, and K. Kwiat, "Modeling the spread of active worms," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, vol. 3, 2003, pp. 1890–1900 vol.3.

[16] B. K. Mishra and S. K. Pandey, "Dynamic model of worm propagation in computer network," *Applied Mathematical Modelling*, vol. 38, no. 7, pp. 2173–2179, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0307904X13006586

[17] D. Dagon, C. C. Zou, and W. Lee, "Modeling botnet propagation using time zones." in *NDSS*, vol. 6, 2006, pp. 2–13.

[18] H. Okamura, H. Kobayashi, and T. Dohi, "Markovian modeling and analysis of internet worm propagation," in *16th IEEE International Symposium on Software Reliability Engineering (ISSRE'05)*, 2005, pp. 10 pp.–158.

[19] Y. Yao, L. Guo, H. Guo, G. Yu, F.-x. Gao, and X.-j. Tong, "Pulse quarantine strategy of internet worm propagation: modeling and analysis," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1047–1061, 2012.

[20] L. Li, J. Cui, R. Zhang, H. Xia, and X. Cheng, "Dynamics of complex networks: Malware propagation modeling and analysis in industrial internet of things," *IEEE Access*, vol. 8, pp. 64 184–64 192, 2020.

[21] A. Zhaikhan, M. A. Kishk, H. Elsawy, and M. S. Alouini, “Safeguarding the iot from malware epidemics: A percolation theory approach,” *IEEE Internet of Things Journal*, vol. 8, 2021.

[22] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao, “Differential game-based strategies for preventing malware propagation in wireless sensor networks,” *IEEE Transactions on Information Forensics and Security*, vol. 9, 2014.

[23] Y. Hayel and Q. Zhu, “Epidemic protection over heterogeneous networks using evolutionary poisson games,” *IEEE Transactions on Information Forensics and Security*, vol. 12, 2017.

[24] R. Pastor-Satorras, C. Castellano, P. V. Mieghem, and A. Vespignani, “Epidemic processes in complex networks,” *Reviews of Modern Physics*, vol. 87, 2015.

[25] W. J. Anderson, “Continuous-time markov chains,” 1991.

[26] R. H. Byrd, M. E. Hribar, and J. Nocedal, “An interior point algorithm for large-scale nonlinear programming,” *SIAM Journal on Optimization*, vol. 9, no. 4, pp. 877–900, 1999.

[27] M. Fewell, “Area of common overlap of three circles,” *DSTO Defence Science and Technology Organisation*, 2006.

VITAE

Information

- Name: Munzir Elsaih Mohamed.
- Nationality: Sudan.
- Date of Birth: January 1, 1997.
- Email: *munzirahmed035@gmail.com*
- Permenant Address: Elradmia Street, El- Haj Yousif, Khartoum 12216, Sudan.

Education

- (January, 2020) King Fahd University of Petroleum and Minerals: Bachelor of Science in Electrical Engineering.
- (May, 2023) King Fahd University of Petroleum and Minerals: Master of Science in Telecommunication Engineering.

Publications

- M. Mohamed, H. ElSawy and W. Mesbah, ”Optimized Degree-Aware Random Patching for Thwarting IoT Botnets,” in IEEE Networking Letters, vol. 5, no. 1, pp. 59-63, March 2023, doi: 10.1109/LNET.2023.3241867.
- M. Ahmed, S. Kuriry, M. D. Shafiullah and M. A. Abido, ”DC Microgrid Energy Management with Hybrid Energy Storage Systems,” 2019 23rd International Conference on Mechatronics Technology (ICMT), Salerno, Italy, 2019, pp. 1-6, doi: 10.1109/ICMECT.2019.8932147.