# Secure Protocol Design for Mobile Ad Hoc Networks

by

Xiaochen Li

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(The School of Systems Information Science)
in Future University Hakodate
September 2020

To my family

# ABSTRACT

Secure Protocol Design for Mobile Ad Hoc Networks

by

Xiaochen Li

As wireless communication technology evolves continuously, mobile ad hoc networks (MANETs) become highly appealing for supporting lots of critical applications in daily life. However, due to the open nature of wireless medium, wireless communication is vulnerable to eavesdropping attacks by unauthorized receivers (eavesdroppers), posing a great threat to the security of MANETs. Recently, a promising security approach, called physical layer (PHY) security, has been proposed to provide a strong security guarantee by exploiting the inherent physical properties of wireless channels, such as noise, interference and time-varying fading. Compared to the cryptography-based methods, the PHY security technology can provide an everlasting security guarantee without the need of costly secret key management/distribution and complex cryptographic protocols. This thesis therefore focuses on the secure protocol design and performance analysis of MANETs based on the typical PHY security techniques (i.e., secrecy guard zone, cooperative jamming, artificial noise).

For cell-partitioned MANETs, we first consider a scenario where each transmitter can detect the existence of eavesdroppers in a region around itself, called secrecy guard zone (SGZ). For this scenario, we propose an SGZ-based secure transmission

protocol, in which the transmission of a selected transmitter will be conducted only if no eavesdroppers exist in its SGZ. To understand the security performance of the SGZ-based secure transmission protocol, we first derive two basic secure transmission probabilities of the network by applying the classical Probability Theory. We then obtain the exact secrecy throughput capacity of the concerned network under the SGZ-based secure transmission protocol based on the analysis of two secure transmission probabilities. Finally, we present extensive simulation and numerical results to validate our theoretical analysis and also to illustrate the impacts of the SGZ-based secure transmission protocol on the secrecy throughput capacity performance.

For cell-partitioned MANETs, we then consider a new scenario where each transmitter can know the exact locations of eavesdroppers in its transmission range. For this scenario, we propose a cooperative jamming (CJ) based secure transmission protocol, which allows non-transmitting legitimate nodes to send artificial noise to suppress eavesdroppers. The transmission of a selected transmitter will be conducted only if all eavesdroppers in the transmission range of the transmitter are suppressed. To understand the security performance of the proposed secure transmission protocol, based on the classical Probability Theory, we first conduct analysis on two basic secure transmission probabilities of the network. We then derive the exact analytical expression for the secrecy throughput capacity of the network under the CJ-based secure transmission protocol. Finally, extensive simulation and numerical results are provided to verify the theoretical analysis also to illustrate the impacts of the CJ-based secure transmission protocol on the secrecy throughput capacity performance.

For continuous MANETs, by combining PHY security techniques and the conventional Aloha protocol, we propose two secure Aloha protocols, i.e., artificial noise (AN)-based Aloha protocol and secrecy guard zone (SGZ)-based Aloha protocol, to ensure secure medium access for legitimate transmitters. In the AN-based Aloha protocol, all potential transmitters (i.e., transmitters scheduled by the conventional

Aloha protocol) are allowed to be active and each active transmitter injects AN into its transmitted signals to confuse eavesdroppers. In the SGZ-based protocol, each potential transmitter has an SGZ, a circle centered at itself, and only the potential transmitters whose SGZ contains no eavesdroppers are allowed to be active. To understand both the security and reliability performance of the proposed secure Aloha protocols, we first apply tools from Stochastic Geometry to derive analytical expressions for the connection outage probability (COP) as well as the upper and lower bounds on the secrecy outage probability (SOP) of the considered network under both the AN-based Aloha protocol and SGZ-based Aloha protocol. Based on the COP and SOP, we then derive the secrecy transmission capacity of the network under both protocols. Finally, we provide simulation/numerical results to validate the theoretical analysis of COP and SOP and also to show the impacts of secure Aloha protocols on the secrecy transmission capacity performance.

# ACKNOWLEDGEMENTS

Upon accomplishing my three-year doctoral study in Future University Hakodate, I would like to express my sincere thanks to all who provide me help, love and encouragement, which certainly make my experience here become one of the most important and wonderful stages that I will never forget in the rest of my life.

First and foremost, I am greatly indebted to my supervisor Professor Xiaohong Jiang, not only for his continuous guidance and support in my academic research, but also for his role as my life mentor to teach me a lot of truth in life. During pursuing my PhD in Hakodate, Professor Jiang guided me to deal with various challenges I encountered such that I can finish this thesis. He and his wife, Mrs Li, always gave me countless care.

I would like to thank Professor Yulong Shen of Xidian University, China, who gave me the opportunity to work together with Professor Xiaohong Jiang and other members in the laboratory when I was a Master student. He opened the door of scientific research for me and showed me the way to be an excellent researcher.

I also want to appreciate my thesis committee members, Professor Yuichi Fujino, Professor Hiroshi Inamura and Professor Masaaki Wada for their constructive comments which help me greatly improve the quality of my thesis. My thanks also go to the research colleagues Yuanyu Zhang, Jia Liu, Pinchang Zhang, Ji He, Wenhao Zhang, Shuangrui Zhao, Ranran Sun, Yeqiu Xiao, Chan Gao, Huihui Wu, Ahmed Salem; my Japanese teachers Katsuko Takahashi, Ritsu Ishikawa and Noriko Watanabe; the university staffs Mr. Igi, Mr. Kikuchi, Mrs Kawagishi and Mrs Arashida. It

is because of them my life in Japan could be so colorful.

Finally, I want to express my great acknowledgments to my parents and other family members. They always give me unconditional love and support such that I hold the courage to face anything. I love them forever.

# TABLE OF CONTENTS

# LIST OF FIGURES

**Figure**

# LIST OF TABLES

**Table**

# LIST OF APPENDICES

**Appendix**

# CHAPTER I

# Introduction

In this chapter, we first introduce the background of mobile ad hoc networks and physical layer security, and then we present the objective and main works of this thesis. Finally, we give the outline and main notations of this thesis.

## 1.1 Research Background

### 1.1.1 Mobile Ad Hoc Networks

A mobile ad hoc network (MANET) is a continuously self-configuring, self-organizing and infrastructure-less network of mobile devices connected without wires [1, 2]. Each device in a MANET can move in any direction freely and independently, so the communication links among devices can be frequently changed. Each device collaborates by forwarding any incoming traffic, therefore, acting as a router. The basic challenge of constructing a MANET is providing each device with the required information needed to route the incoming traffic to the destinations in a fast and reliable manner.

A MANET often appears in scenarios where there is no network infrastructure or it is inconvenient to use the existing network infrastructure. The MANETs find lots of important applications in different areas. First, the well-known mobile conference is created using MANET technology. People use their notebooks to form a

communication network anytime and anywhere, which is convenient for data sharing, information exchange and discussion. Second, MANETs can realize the interconnection of personal area networks (PAN). A PAN only contains devices closely related to one person, and these devices cannot be connected to a wide area network. Bluetooth technology is a typical PAN technology, but it can only achieve indoor short-range communications. Therefore, MANET provides the possibility of establishing a multi-hop interconnection among PANs. Third, MANETs can also be used for disaster recovery. When the network infrastructure fails due to natural disasters or other reasons, it is very important to quickly restore communication. With the help of MANET technology, it is possible to quickly establish a temporary network and extend the network infrastructure, thereby reducing the rescue time and damage caused by disasters. However, due to the open nature of wireless medium, wireless communication is vulnerable to eavesdropping attacks by unauthorized receivers (eavesdroppers), posing a great threat to the security of MANETs.

### 1.1.2 Physical Layer Security

Traditionally, the security of wireless communications is guaranteed by cryptography, which relies on solving various computationally difficult problems (e.g., Rivest-Shamir-Adleman (RSA) problem [3], Computational Diffie-Hellman (CDH) problem [4], Discrete Logarithm (DL) problem [5]). Recently, another promising security approach, called physical layer (PHY) security [6–12], has been proposed to provide a stronger security guarantee by exploiting the inherent physical properties of wireless channels, such as noise, interference and time-varying fading. As adversaries (eavesdroppers) may not have enough computing power, they can hardly solve the difficult problems of the cryptography. Thus, cryptographic approaches are still the main practical and effective security methods for wireless networks nowadays, and in most cases the PHY security technology is regarded as a complement for cryptography

to improve the achieved security. However, as the computing power of eavesdroppers develops (for example, adopting the quantum computing [13]), current cryptographic methods may face the increasingly high risk of being broken. By then, the PHY security technology may be widely applied to provide a strong form of security guarantee for wireless networks. Compared to the cryptography-based methods, the PHY security technology can provide an everlasting security guarantee without the need of costly secret key management/distribution and complex cryptographic protocols. Therefore, although the PHY security technology usually comes with a reduced throughput, it is still envisioned as a promising security mechanism for MANETs.

The PHY security technologies are mainly divided into three categories: secure channel coding technology, PHY security key generation technology and PHY security transmission technology.

The secure channel coding technology achieves the secure communication by designing channel coding schemes. The information theory [14–17] states that as long as the secrecy capacity is greater than 0, there exists a channel coding scheme that allows the probability of error at the receiver to be made arbitrarily small, while the amount of information obtained by eavesdroppers is arbitrarily small. However, it is a challenging task to design a secure channel coding scheme that is suitable for existing communication systems. Previous studies [18–27] have designed a variety of coding schemes based on Wyner's weak and strong security conditions, but these works either have a loss of security or lack of practicality. So secure channel coding schemes need to be further studied.

Based on the randomness and uniqueness of wireless channels in both time and space, the basic idea of the PHY security key generation technology [28–31] is that legitimate nodes may use the common channel between each other to generate the same bit sequence, which can serve as the key. But eavesdroppers cannot generate the same key due to different random fading. This technology can be used as one of the key

generation and deployment schemes to ensure information security by combining with the encryption technology for wireless networks. Existing works have applied different technologies for key generation, such as ultra-wide band pulse, signal strength and differential phase detection. The PHY security key generation technology suffers from the problems of low rates and high complexity.

The basic idea of the PHY security transmission technology is to use the inherent characteristics of the wireless channel, such as randomness, fading, and interference, to realize the transmission of confidential information through the signal processing technology. This technology is easier to deploy in practice, so it has attracted more attention. According to the definition of secrecy capacity, the premise of secure transmission at the physical layer is that the intended recipient's channel is of better quality than that of the eavesdropper. However, due to the fading property of the wireless channel, the intended recipient's channel does not necessarily have an advantage. Fortunately, wireless communication resources and signal processing technologies can be used to create and enhance the advantages of the intended recipient's channel, thereby enabling the secure transmission to be achieved.

## 1.2 Objective and Main Works

This thesis adopts PHY security techniques to ensure the security of wireless communications. Our objective is to design secure protocols, i.e., protocols based on secrecy guard zone (SGZ), cooperative jamming (CJ) or artificial noise (AN), and explore the impacts of secure protocols on network performances. Towards this end, we first propose the SGZ-based secure protocol in cell-partitioned MANETs with group-based scheduling scheme and derive the exact secrecy throughput capacity of the concerned network under the secure protocol. We then design the CJ-based secure protocol in cell-partitioned MANETs with group-based scheduling scheme and also study the exact secrecy throughput capacity under the CJ-based secure protocol.

Finally, we propose secure protocols based on AN and SGZ in continuous MANETs with Aloha protocol and study the secrecy transmission capacity of the concerned MANETs. The main works and contributions of this thesis are summarized in the following subsections.

### 1.2.1 Secrecy Guard Zone based Secure Protocol in Cell-Partitioned MANETs

This work focuses on the secure protocol design and explores the exact secrecy throughput capacity of a cell-partitioned MANET [32, 33] with the group-based scheduling scheme [34–38]. We consider a MANET consisting of multiple legitimate nodes and multiple eavesdroppers moving according to the independent and identically distributed (i.i.d.) mobility model. We consider a scenario where each transmitter can detect the existence of eavesdroppers in a region around itself, called SGZ [39–41] (Please refer to Section 2.1 for related works). It is notable that the idea of SGZ has been widely adopted as a security-achieving approach in the study of other security metrics like the secure connectivity [39] and secrecy transmission capacity [40, 41], which differ, to a large extend, from the secrecy throughput capacity metric considered in this work.

The secrecy throughput capacity issue is essentially equivalent to the fundamental and long-standing throughput capacity problem (see [42, 43] and the references therein) under the consideration of PHY security. This metric characterizes the maximum achievable rate per node at which a source packet can be transmitted to the destination both reliably and securely. Extensive research efforts have been devoted to the secrecy throughput capacity study of wireless ad hoc network [44–50] (Please refer to Section 2.4 for related works). It is notable that these works focus on deriving the scaling law results, which are certainly important to characterize how the secrecy throughput capacity of a MANET scales up as the network size tends to infinity. However, as the above scaling law results are usually functions of only the network

size, they can hardly reflect the impacts of other key parameters of protocols and schemes on network performances. In addition, scaling law results are usually regarded as a retreat when exact results are out of reach [43], which reveals that exact secrecy throughput capacity results are more deserved and critical to facilitate the design, development and commercialization of MANETs. The main contributions of this work can be summarized as follows:

- Based on PHY security technology, we first propose an SGZ-based secure protocol, in which the transmission of a selected transmitter will be conducted only if no eavesdroppers exist in its SGZ.

- With the help of the theoretical framework for throughput capacity analysis of MANETs in [51], we derive exact analytical expression for the secrecy throughput capacity of the concerned network under the secure protocol, based on the analysis of secure (resp. source-destination) transmission probability, i.e., the probability that a secure (resp. source-destination) transmission can be conducted between the nodes in a given active cell and the nodes in the transmission range of this cell.

- Finally, extensive simulation results are provided to validate our theoretical analysis and numerical results are also presented to illustrate the impacts of the SGZ-based secure protocol on the secrecy throughput capacity performance.

### 1.2.2 Cooperative Jamming based Secure Protocol in Cell-Partitioned MANETs

This work focuses on the CJ design of cell-partitioned MANETs. Existing works regarding the CJ scheme design have been reported in [52–55] (Please refer to Section 2.2 for related works). These works indicated that CJ can be used to improve the secrecy rate. Thus, this work focuses on the CJ protocol design to further explore

the exact secrecy throughput capacity of MANETs. The network consists of multiple legitimate nodes and multiple passive and non-colluding eavesdroppers. And each node (both legitimate node and eavesdroppers) moves around in the network according to the i.i.d. mobility model. We consider a scenario where each transmitter can know the exact locations of eavesdroppers in its transmission range [56]. Note that the above assumption on the knowledge about the eavesdropper locations is reasonable, as a passive eavesdropper can be detected and located from the local oscillator power leaked from its RF front-end [57, 58]. The main contributions of this work are summarized as follows.

- This work proposes a CJ-based secure transmission protocol to ensure the PHY security based secure communication between the transmitter and receiver. The CJ-based secure protocol allows non-transmitting legitimate nodes to send artificial noise to suppress eavesdroppers in the same cell. The transmission of a selected transmitter will be conducted only if all eavesdroppers in the transmission range of the transmitter are suppressed.

- The secrecy throughput capacity is adopted to model the security performance of the proposed secure protocol. For the modeling of this performance metric, we first conduct analysis on the secure (resp. source-destination) transmission probability, i.e., the probability that a secure (resp. source-destination) transmission can be conducted between the nodes in a given active cell and the nodes in the transmission range of this cell. With the help of the theoretical framework for throughput capacity analysis of MANETs in [51], we derive exact analytical expression for the secrecy throughput capacity of the concerned network.

- Finally, extensive simulation and numerical results are provided to verify our theoretical analysis and also to illustrate the secrecy throughput capacity performance of the network. Besides, we compare the SGZ-based secure protocol

in our first work with the CJ-based secure protocol in terms of the secrecy throughput capacity.

### 1.2.3 Secure Protocols based on Artificial Noise and Secrecy Guard Zone in Continuous MANETs

For continuous MANETs, the authors in [40] studied the secrecy transmission capacity of MANETs under the conventional Aloha transmission protocol. The secrecy transmission capacity results were derived under the assumption that the distances between transmitters and their receivers are fixed, which is difficult to realize in highly dynamic MANETs. Based on this observation, the authors in [59] considered MANETs with random transmitter-receiver distances and derived the secrecy transmission capacity results as well. Like [59], the authors also adopted Aloha as the transmission protocol, while they ignored the crucial issue of protecting the transmissions from eavesdropping. To address this issue, this work therefore combines two widely-used PHY security schemes, i.e., AN injection [60–63] (Please refer to Section 2.3 for related works)and SGZ [39–41] (Please refer to Section 2.1 for related works), with the Aloha protocol to propose novel secure Aloha transmission protocols and then analyze the secrecy transmission capacity performance of MANETs under the newly proposed protocols.

We consider a continuous MANET consisting of multiple legitimate nodes and multiple eavesdroppers distributed according to two independent and homogeneous Poisson Point Processes (PPP), respectively. We adopt the Aloha protocol to schedule transmissions. To protect the transmissions of the legitimate transmitters, we propose two secure Aloha protocols, which combine commonly-used security schemes and the conventional Aloha protocol. The main contributions of this work are summarized as follows.

- We propose two secure Aloha protocols, i.e., AN-based protocol and SGZ-based

protocol, which implement commonly-used PHY security schemes on top of the conventional Aloha protocol to ensure secure transmissions of transmitters. In the AN-based protocol, all *potential* transmitters (i.e., transmitters scheduled by the conventional Aloha protocol) are allowed to be *active* and each active transmitter injects AN into its transmitted signals to confuse eavesdroppers. In the SGZ-based protocol, each potential transmitter has an SGZ, a circle centered at itself, and only the potential transmitters whose SGZ contains no eavesdroppers are allowed to be active.

- Using the tools from Stochastic Geometry, we derive analytical expressions for the connection outage probability (COP) as well as the upper and lower bounds on the secrecy outage probability (SOP) of the considered network under both the AN-based protocol and SGZ-based protocol. Based on the COP and SOP, we then derive the secrecy transmission capacity of the network under both protocols.

- Finally, extensive simulation and numerical results are provided to validate our theoretical analysis, and also to show the impacts of key network parameters on the COP, SOP and secrecy transmission capacity performances of the network.

## 1.3 Thesis Outline

The remainder of this thesis is outlined as follows. Chapter II introduces the related works of this thesis. In Chapter III, we introduce our work regarding SGZ-based secure protocol in cell-partitioned MANETs with group-based scheduling scheme. Chapter IV presents the work on CJ-based secure protocol in cell-partitioned MANETs with group-based scheduling scheme and Chapter V introduces the work regarding secure protocols based on AN and SGZ in continuous MANETs. Finally, we conclude this thesis in Chapter VI.

## 1.4 Notations

The main notations of this thesis are summarized in Table 1.1.

Table 1.1: Main notations

| Symbol | Definition |
|---|---|
| $n$ | number of legitimate nodes |
| $m$ | number of eavesdroppers |
| $M$ | cell-partitioned parameter |
| $g$ | secrecy guard zone size in the cell-partitioned MANET |
| $\lambda$ | average packet input rate |
| $\mu$ | secrecy throughput capacity |
| $\overline{D}$ | average packet delay |
| $v$ | transmission range of a legitimate node |
| $r$ | spatial multiplexing parameter |
| $\Delta$ | guard factor |
| $\lceil . \rceil$ | ceiling function |
| $S(j,k)$ | Stirling numbers of the second kind |
| $\mathbb{E}[\cdot]$ | expectation operator |
| $\mathbb{P}[\cdot]$ | probability operator |
| $\Psi_L$ | Poisson Point Process (PPP) of legitimate nodes |
| $\Psi_E$ | PPP of eavesdroppers |
| $\Psi_T$, $\Psi_R$ | Sets of transmitter and receiver locations, resp. |
| $\lambda_L$, $\lambda_E$ | density of $\Psi_L$ and $\Psi_E$, resp. |
| $\lambda_T$, $\lambda_R$ | density of $\Psi_T$ and $\Psi_R$, resp. |
| $\lambda_{AT}$ | density of active transmitters |
| $\text{SINR}_j$ | signal-to-interference-plus-noise ratio (SINR) at the receiver $j$ |

| | |
|---|---|
| $\mathrm{SINR}_e$ | SINR at the eavesdropper $e$ |
| $P_{co}$ | connection outage probability (COP) |
| $P_{co}^{AN}$ | COP under the AN-based Aloha protocol |
| $P_{co}^{SGZ}$ | COP under the SGZ-based Aloha protocol |
| $P_{so}$ | secrecy outage probability (SOP) |
| $P_{so}^{AN}$ | SOP under the AN-based Aloha protocol |
| $P_{so}^{SGZ}$ | SOP under the SGZ-based Aloha protocol |
| $\sigma$ | COP constraint |
| $\varepsilon$ | SOP constraint |
| $\beta_t$, $\beta_e$ | SINR thresholds for legitimate nodes and eavesdroppers, resp. |
| $R_t$, $R_s$ | codewords rate and secrecy rate, resp. |
| $R_e$ | rate loss for securing the message against eavesdropping |
| $R_t^{\max}$ | maximum allowable coderate $R_t$ |
| $R_e^{\min}$ | minimum allowable $R_e$ |
| $T_c$ | secrecy transmission capacity |
| $T_c^{\mathrm{AN}}$ | secrecy transmission capacity under the AN-based protocol |
| $T_c^{\mathrm{SGZ}}$ | secrecy transmission capacity under the SGZ-based protocol |
| $p$ | transmission probability |
| $\alpha$ | path-loss exponent |
| $W_r$ | noise power at legitimate receivers |
| $W_e$ | noise power at eavesdroppers |
| $P$ | total transmission power of the transmitter |
| $\tau$ | power allocation parameter |
| $D$ | radius of secrecy guard zone in the continuous MANET |
| $H_{ij}$ | channel fading between nodes $i$ and $j$ |
| $\lvert X_{ij}\rvert$ | distance between nodes $i$ and $j$ |

# CHAPTER II

# Related Works

This section introduces the existing works related to our study in this thesis, including the works on the secrecy guard zone, the works on the cooperative jamming, the works on the artificial noise and the works on the scaling law results of secrecy throughput capacity.

## 2.1 Secrecy Guard Zone

The idea of secrecy guard zone (SGZ) has been applied in wireless networks. Pinto *et al.* [39] considered a scenario where each legitimate node can inspect and deactivate the eavesdroppers falling inside its surrounding area, called SGZ. To improve the secure connectivity, they applied an SGZ around each legitimate node and proposed the transmission protocol, in which each legitimate node guarantees the absence of eavesdroppers in its SGZ (e.g., by deactivating such eavesdroppers). To improve the secrecy transmission capacity, Zhou *et al.* [40] applied an SGZ around each legitimate transmitter and proposed the transmission protocol for networks in which each legitimate transmitter is able to detect the existence of eavesdroppers in its SGZ. Transmissions of confidential messages take place only if no eavesdroppers are found inside the SGZ of the corresponding transmitter. The SGZ was also exploited to improve the secrecy transmission capacity in random cognitive radio networks in [41].

It is notable that the idea of SGZ has been widely adopted as a security-achieving approach in the study of other security metrics like the secure connectivity and secrecy transmission capacity, which differ, to a large extend, from the secrecy throughput capacity metric considered in this work.

## 2.2 Cooperative Jamming

For the cooperative jamming (CJ) technology, relay nodes can be used as helper nodes to provide jamming signals to confuse eavesdroppers, thereby improving the security of wireless transmission. CJ schemes have been designed in [52, 53] for the single antenna relay system and in [54, 55] for the multiple antennas relay system. For the CJ scheme study in the case of a single antenna relay, the authors in [52] considered the CJ scheme, where the source is transmitting, and the cooperating nodes transmit weighted noise to confound the eavesdropper. Under the CJ scheme, they investigated the maximization of the achievable secrecy rate subject to a total power constraint and the minimization of the total transmit power under a secrecy rate constraint. In [53], authors used the CJ to achieve the positive secrecy rate for the single antenna relay system by a combination of convex optimization and a one-dimensional search. For the CJ scheme study in the case of a multiple antenna relay, authors in [54] proposed a generalized singular value decomposition (GSVD)-based CJ scheme for the transmission of multiple data streams to improve the secrecy rate. The scenario where the relay is equipped with multiple antennas is also considered in [55]. They designed the CJ protocol for achieving the following two objectives, one is the secrecy rate maximization subject to a total power constraint, and the other is the transmit power minimization subject to a secrecy rate constraint. The difference between the above works and this thesis is that the jamming signals in this thesis interfere with legitimate nodes and eavesdroppers, while the jamming signals in above works interfere only with eavesdroppers.

## 2.3 Artificial Noise

The basic idea of artificial noise (AN) is that the transmitter can use some of the available power to transmit artificial noise. Since this noise is generated by the transmitter, the transmitter can design it such that only the eavesdroppers channel is degraded. Some recent efforts have been devoted to the AN design of wireless networks. Two schemes for generating AN to achieve secrecy were presented in [60]. In the first scheme, the transmitter can use the multiple antennas to generate the AN intelligently such that it degrades only the eavesdroppers channel. For the scenario where transmitter does not have multiple transmit antennas, authors in [60] proposed the second scheme. The helper nodes simulate the effect of multiple antennas and allow the transmitter to generate AN as in the first scheme. The multiple antenna AN scheme was further analyzed in [61, 62], where the MIMO secrecy capacity with the use of AN was explored. In the design of AN scheme, authors in [63] considered the transmit power allocation strategy, which has not been investigated in [61, 62]. The above works considered that there was only one transmitter-receiver pair in the network, while multiple transmitter-receiver pairs were considered in our work.

## 2.4 Scaling Law Results of Secrecy Throughput Capacity

Some scaling law results on the network secrecy throughput capacity have been reported in [44–47] for static ad hoc networks and in [48–50] for MANETs. For the secrecy throughput capacity study in static ad hoc networks, the authors in [44] explored the secrecy throughput capacity of a Poisson network with legitimate nodes and eavesdroppers distributed according to Poisson Point Processes. The authors assumed that the locations of eavesdroppers are known and applied the SGZ to guarantee secure transmissions of legitimate transmitters. In addition, the authors also investigated the secrecy throughput capacity of an arbitrary network with multiple

legitimate nodes and eavesdroppers. The secrecy throughput capacity of a Poisson network was also studied in [45], while, different from [44], the authors assumed that the locations of eavesdroppers are unknown and each receiver has two extra antennas for generating AN to suppress eavesdroppers. This work was later extended in [46] by introducing social relationships among legitimate network nodes. For a stochastic network with eavesdroppers of unknown location, the authors in [47] investigated the trade-off between the network throughput and the maximum number of eavesdroppers that can be tolerated by the network. Similar to [45] and [46], the authors in [47] adopted the AN generation technique to improve security, while the difference is that the AN is generated from other helper nodes instead of extra antennas of receivers.

For the secrecy throughput capacity study in MANETs, the authors in [48] studied the scaling law results of delay-constrained secrecy throughput capacity of a MANET under both passive attack where eavesdroppers only overhear legitimate transmissions without actively sending signals and active attack where eavesdroppers actively attack legitimate transmissions by injecting jamming signals. The results in [48] showed that the presence of eavesdroppers has a significant impact on the network secrecy throughput capacity and in general the secrecy throughput capacity under active attack is less than the secrecy throughput capacity under passive attack. In [49], the scaling law result of delay-constrained MANET secrecy throughput capacity was also investigated, while the authors considered static and passive eavesdroppers, and adopted the AN generation technique in [45] and [46] to suppress the eavesdroppers. The scaling law result of delay-constrained secrecy throughput capacity in MANETs with passive eavesdroppers under various routing policies such as Spray-and-Wait was examined in [50]. The significant difference between the above works and this thesis is that this thesis derived the exact secrecy throughput capacity of MANETs while the above works focused on the secrecy throughput capacity scaling laws.

# CHAPTER III

# Secrecy Guard Zone based Secure Protocol in Cell-Partitioned MANETs

In this chapter, we focus on the secrecy guard zone (SGZ) design in cell-partitioned MANETs, for which we propose an SGZ-based secure protocol to ensure the security of a finite network with multiple legitimate nodes and multiple passive and non-colluding eavesdroppers. To evaluate the performance of the proposed secure protocol, we derive exact analytical expression for the secrecy throughput capacity performance of the concerned network based on the analysis of two basic secure transmission probabilities. Extensive simulation and numerical results are provided to demonstrate the validity of the theoretical analysis as well as to illustrate the performances of the proposed SGZ-based secure protocol.

## 3.1 System Model

As shown in Figure 3.1, we consider a torus network with unit area [35, 36, 64], and the network is evenly partitioned into $M \times M$ cells. The network consists of $n$ legitimate nodes and $m$ passive and non-colluding eavesdroppers. We consider a time-slotted system and each node (both legitimate node and eavesdroppers) moves around in the network according to the independent and identically distributed (i.i.d.)

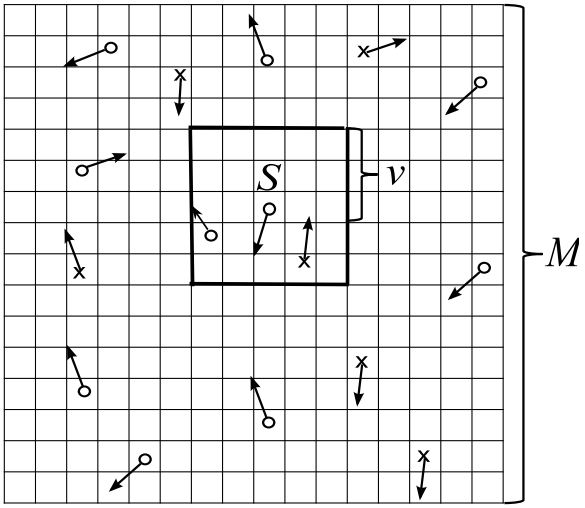



Figure 3.1: Illustration of a cell partitioned MANET: the circle represents legitimate node, the cross represents eavesdropper and the arrow represents the moving direction of nodes.

mobility model [32, 42, 65]. In this model, each node randomly and independently moves into a cell at the beginning of each time slot and stays in this cell during the whole slot. We assume that all legitimate nodes occupy the same wireless channel and have the same transmission range. As illustrated in Figure 3.1, the transmission range of a legitimate node (say $S$) covers a set of cells (called coverage cells) with horizontal or vertical distance of no more than $v-1$ cells away from the cell containing $S$, where $1 \leq v < \lfloor \frac{M+1}{2} \rfloor$ and $\lfloor . \rfloor$ is the floor function. We assume that $n$ is even and the traffic flow follows the permutation model [66, 67], where the source-destination pairs are determined as $1 \leftrightarrow 2, 3 \leftrightarrow 4, \cdots, (n-1) \leftrightarrow n$, i.e., each legitimate node is the source of a traffic flow and at the same time the destination of another traffic flow. Each source node $i$ is assumed to generate local packets according to an i.i.d. process $A_i(t)$, which represents the number of generated packets of source node $i$ at time slot $t$. It is assumed that $A_i(t)$ has a constant mean $\lambda$ (i.e., $\mathbb{E}\{A_i(t)\} = \lambda$) and a bounded second moment $A_{max}^2$ (i.e., $\mathbb{E}\{A_i^2(t)\} \leq A_{max}^2 < \infty$), where $\mathbb{E}\{\}$ is the expectation operator. This represents that all source nodes have the same average packet input rate $\lambda$ packets/slot. To coordinate the simultaneous transmission of source nodes, we

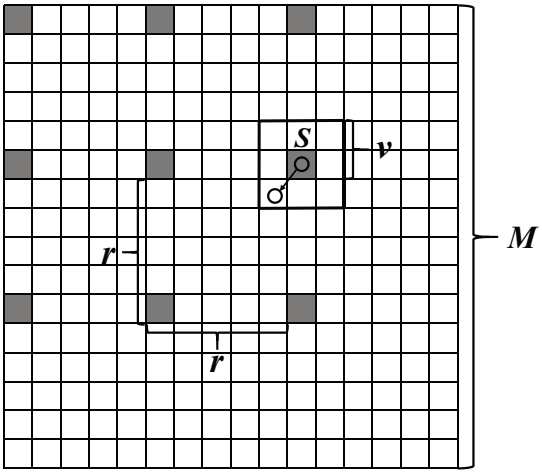



Figure 3.2: Group-based scheduling.

adopt the widely-used group-based scheduling scheme [34–38]. This scheme divides all the network cells into $r^2$ groups with each group consisting of $K = \lfloor M^2/r^2 \rfloor$ cells and becoming active (i.e., allowed to transmit packets) alternately in every $r^2$ time slots. As shown in Figure 3.2, the distance between any two horizontally (or vertically) adjacent cells in the same group is of $r$ cells, and $r$ is given by

$$r = min\{\lceil (1+\Delta)\sqrt{2}v + v \rceil, M\}, \tag{3.1}$$

where $\lceil . \rceil$ is the ceiling function and $\Delta$ is a guard factor to prevent interference from other concurrent transmitters in the same group. We refer to the cells of the active group in the current time slot as active cells throughout this thesis.

## 3.2 Secrecy Guard Zone based Secure Protocol

We consider a scenario in this chapter regarding the knowledge of legitimate nodes about the eavesdroppers. In this scenario, we assume that each transmitter can detect the existence of eavesdroppers in a region around itself, called secrecy guard zone

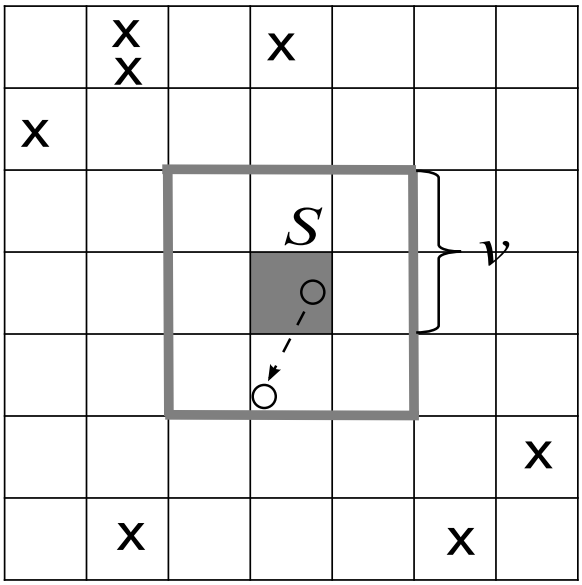



Figure 3.3: SGZ-based secure protocol.

(SGZ) [39–41, 68]. As shown in Figure 3.3, we model the SGZ of a transmitter (say $S$) as a square region with $g$ cells centered at the cell containing $S$. To ensure secure transmission in this scenario, we propose an SGZ-based secure protocol, in which the transmission of a selected transmitter can be conducted only if no eavesdroppers exist in the SGZ, and suspended otherwise.

## 3.3 Exact Secrecy Throughput Capacity Analysis

In this section, we derive the exact secrecy throughput capacity under the SGZ-based secure protocol. Similar to [69, 70] the word exact is used to emphasize that the results derived in this thesis are closed-form expressions rather than order-sense or scaling-law expressions, and that the results are also exact ones rather than upper or lower bounds. We first give the formal definition of secrecy throughput capacity as follows.

**Secrecy Throughput Capacity**: Consider a cell-partitioned MANET under

the group-based scheduling and the proposed secure protocol, the secrecy throughput capacity is defined as the maximum input rate $\lambda$ (packets/slot) that the network can support *stably* and *securely*. The term *stably* means that for a given input rate $\lambda$, we can find a packet delivery algorithm to ensure that the average delay of the network is bounded. The term *securely* means that all transmissions are secure against the eavesdroppers under the proposed secure transmission protocols.

Notice that the secrecy throughput capacity characterizes the fundamental limit on the achievable end-to-end secrecy throughput per source-destination pair of the considered system.

### 3.3.1 Secrecy Throughput Capacity Analysis Framework

The secrecy throughput capacity analysis in this work is based on the theoretical framework in [51]. Following this framework, we first need to derive an upper bound $\mu$ on the secrecy throughput capacity, and then prove this upper bound is achievable, which means that for any input rate $\lambda < \mu$, the network is stable, i.e., the average packet delay $\overline{D}$ is bounded, under a given packet delivery algorithm.

The derivation of the upper bound $\mu$ is based on the fact that the total output rate of packets must be less than the total input rate to stabilize the network. When the total output rate is arbitrarily close to the total input rate, we can obtain $\mu$. Consider a time interval $[0, T]$, it is easy to see that the average number of input packets into the network is $n\lambda T$. To see the average number of output packets, we define $p_0$ ($p_1$) the probability that a (source-destination) transmission can be securely conducted between the nodes in a given active cell $c$ and the nodes in the coverage cells of $c$. According to the group-based scheduling, there are $K$ active cells in each time slot. Thus, during $T$ time slots, the average number of secure (source-destination) transmission opportunities is $Kp_0T$ ($Kp_1T$). In order to deliver as many packets as possible during the $T$ time slots, we use the $Kp_1T$ source-destination

secure transmission opportunities to deliver $Kp_1T$ packets. Since the other packets must traverse at least two hops to reach their destinations, which means that at least two transmission opportunities are consumed for each packet, the remaining $Kp_0T-Kp_1T$ opportunities can be used to deliver at most $(Kp_0T-Kp_1T)/2$ packets. Thus, the total number of output packets during $T$ time slots is no more than $Kp_1T+(Kp_0T-Kp_1T)/2$. To stabilize the network, there should exist sufficiently larger $T$ such that the difference between the total input rate $n\lambda$ and the total output rate $Kp_1+(Kp_0-Kp_1)/2$ should be within an arbitrarily small $\epsilon>0$, that is

$$n\lambda-[Kp_1+(Kp_0-Kp_1)/2]\leq\epsilon, \tag{3.2}$$

or equivalently

$$\lambda\leq\frac{K\left(p_0+p_1\right)}{2n}+\frac{\epsilon}{n}. \tag{3.3}$$

When $\epsilon$ is arbitrarily small, we can derive the upper bound $\mu$ as

$$\mu=\frac{K\left(p_0+p_1\right)}{2n}. \tag{3.4}$$

Next, we prove that for any input rate $\lambda<\mu$, the average packet delay $\overline{D}$ of the network is bounded. According to [51], with probabilities $p_0$ and $p_1$, we can bound the average packet delay $\overline{D}$ as

$$\overline{D}\leq\frac{B_0}{B_1(1-\rho)\lambda\mu}, \tag{3.5}$$

where $\rho=\frac{\lambda}{\mu}$ denotes the system load,

$$B_0=(nA_{max}^2+K-2K\lambda)(p_0^2-p_1^2)+2n\mu(p_0+np_1-p_1), \tag{3.6}$$

and

$$B_1 = 4(p_0 + np_1 - p_1)(p_0 - p_1). \tag{3.7}$$

Therefore, according to the above, the upper bound $\mu$ is the exact secrecy throughput capacity.

### 3.3.2 Exact Secrecy Throughput Capacity Result

We present the following theorem regarding the exact secrecy throughput capacity result.

**Theorem III.1** *Consider a cell-partitioned network with n legitimate nodes, m eavesdroppers and $M^2$ cells, where nodes move according to i.i.d. mobility model, the group-based scheduling is adopted to coordinate simultaneous link transmission and the SGZ-based secure protocol is utilized to ensure secure transmissions, the exact secrecy throughput capacity $\mu$ of the network is given by*

$$\mu = \frac{\lfloor M^2/r^2 \rfloor}{2nM^{2n}} \left(1 - \frac{g}{M^2}\right)^m \Big[2M^{2n} - (M^2-1)^n - n(M^2-\beta)^{n-1} - (M^4 - 2\beta + 1)^{\frac{n}{2}}\Big], \tag{3.8}$$

*where g denotes the size of the SGZ and $\beta = (2v-1)^2$ denotes the size of transmission range.*

**Proof 1** *According to the framework in Section 3.3.1, we only need to derive $p_0$ and $p_1$ to obtain the secrecy throughput capacity. We focus on a given active cell c and derive $p_0$ as the first step. First, we calculate the probability that the transmission is on, which is equivalent to the probability that there are no eavesdroppers in the SGZ of c, i.e., $(1 - \frac{g}{M^2})^m$. Next, we define $\hat{p_0}$ the probability that there are at least two legitimate nodes existing in the coverage cells of c and at least one of those nodes is*

*within c. According to [51], we have*

$$\hat{p_0} = \frac{1}{M^{2n}}\Big[M^{2n} - (M^2-1)^n - n(M^2-\beta)^{n-1}\Big]. \tag{3.9}$$

*Finally, based the probability that transmission is on and* $\hat{p_0}$*, we have*

$$p_0 = \frac{1}{M^{2n}}\left(1-\frac{g}{M^2}\right)^m\Big[M^{2n} - (M^2-1)^n - n(M^2-\beta)^{n-1}\Big]. \tag{3.10}$$

*The second step is to derive* $p_1$*. We define* $\hat{p_1}$ *the probability that there are at least one source-destination pair in the coverage cells of c and at least one node of such pair is in c. According to [51], we have*

$$\hat{p_1} = \frac{1}{M^{2n}}\Big[M^{2n} - (M^4-2\beta+1)^{\frac{n}{2}}\Big]. \tag{3.11}$$

*Finally, based on the probability that transmission is on and* $\hat{p_1}$*, we have*

$$p_1 = \frac{1}{M^{2n}}\left(1-\frac{g}{M^2}\right)^m\Big[M^{2n} - (M^4-2\beta+1)^{\frac{n}{2}}\Big]. \tag{3.12}$$

*After deriving* $p_0$ *and* $p_1$*, the exact secrecy throughput capacity in (3.8) then follows according to (3.4).*

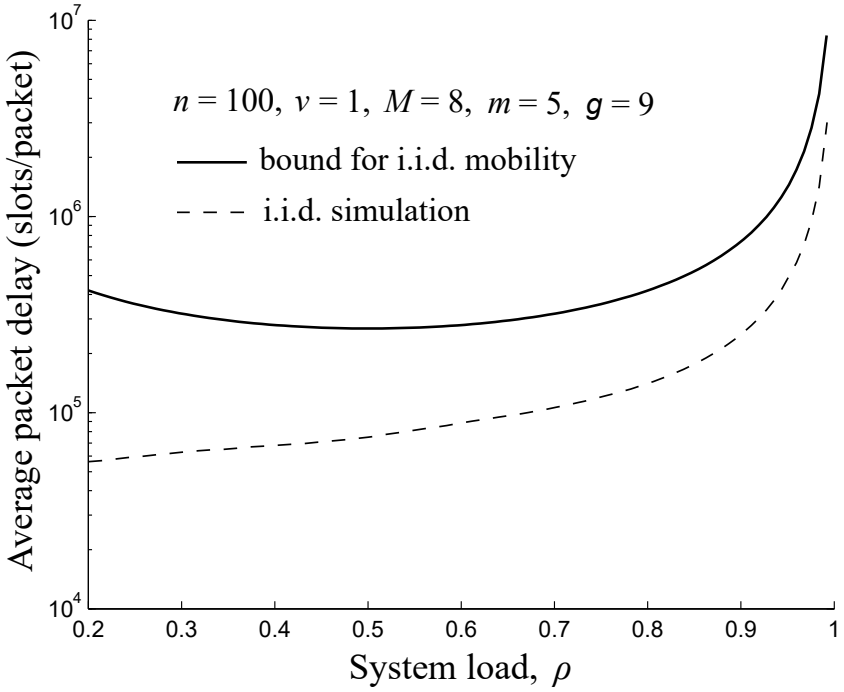
## 3.4 Numerical Results and Discussions

In this section, we first provide simulation results to validate our theoretical analysis for the secrecy throughput capacity performance of the concerned network. We then explore how the secrecy throughput capacity performance varies with the parameters of the proposed SGZ-based secure protocol.

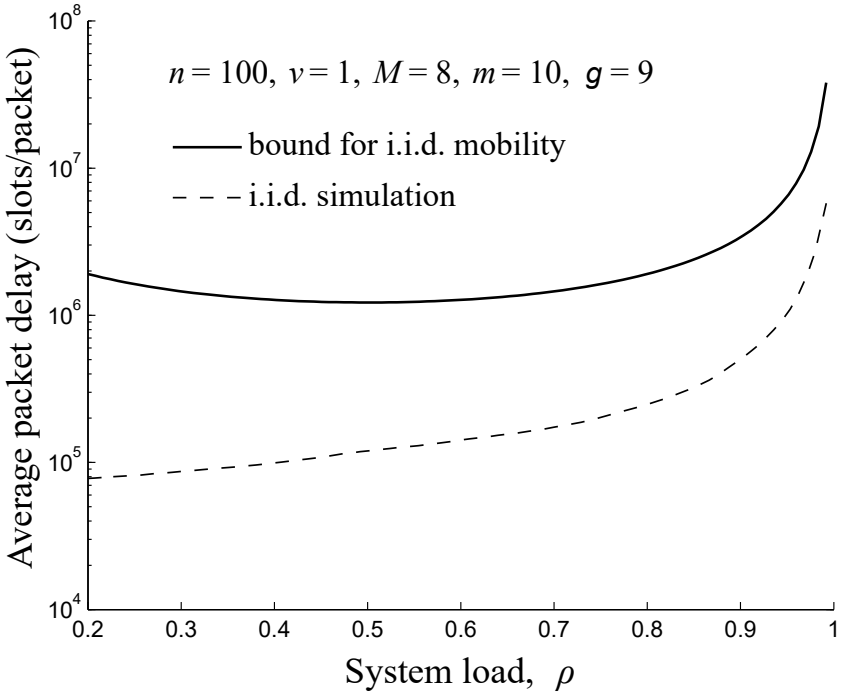
### 3.4.1 Model Validation

To validate our secrecy throughput capacity analysis, a dedicated C++ simulator was developed to simulate the packet delivery process in the concerned MANET under the proposed SGZ-based secure protocol, which is now available at [71]. According to secrecy throughput capacity framework in Section 3.3.1, we conduct extensive simulations to calculate the simulated results of the average packet delay for our secrecy throughput capacity analysis validation. Similar to [71], in the simulation, we fix the guard factor as $\Delta = 1$ and focus the packet delivery process of a given source-destination pair during $10^7$ time slots. The expected packet delay in the simulation is calculated as the ratio of the total delay of all packets delivered to the destination in $10^7$ time slots to the number of these packets.

For the SGZ-based secure protocol, $v$ is fixed as $v = 1$ and hence $r$ is determined as $r = 4$. We conduct simulations under the network scenarios of ($n = 100$, $M = 8$, $m = 5$, $g = 9$) and ($n = 100$, $M = 8$, $m = 10$, $g = 9$), respectively. The simulation results of the average packet delay and the corresponding theoretical ones are summarized in Figure 3.4. We can see from Figure 3.4 that for any input rate $\lambda < \mu$ (i.e., system load $\rho < 1$), the average packet delay $\overline{D}$ of the network can be bounded by our theoretical delay upper bound in (3.5) under both network scenarios, which implies that the network is always stable whenever $\lambda < \mu$. Another observation from Figure 3.4 indicates that when the system load $\rho$ approaches 1, i.e., the input rate $\lambda$ is infinitely close to the secrecy throughput capacity $\mu$, the expected packet delay increases drastically. According to the framework in Section 3.3.1, these two behaviors indicate that our theoretical secrecy throughput capacity result under the SGZ-based secure protocol is efficient to exactly model the network secrecy throughput capacity performance of the concerned network.




(a) Average packet delay vs. system load under network scenario of $n = 100$, $v = 1$, $M = 8$, $m = 5$, $g = 9$.




(b) Average packet delay vs. system load under network scenario of $n = 100$, $v = 1$, $M = 8$, $m = 10$, $g = 9$.

Figure 3.4: Model validation under SGZ-based secure protocol.

### 3.4.2 Performance Discussion

With the help of our theoretical results, we now explore how the secrecy throughput capacity $\mu$ varies with the network parameters. We examine the impacts of the number of eavesdroppers $m$ and the SGZ size $g$ upon the secrecy throughput capacity $\mu$. For the fixed setting of $(n = 100, M = 8, v = 1)$, we show in Figure 3.5 the relationship between $\mu$ and $m$ under three different settings of $g = 1$, $g = 9$ and $g = 25$. We can see from Figure 3.5 that as $m$ increases, the secrecy throughput capacity $\mu$ decreases. This is intuitive since as more eavesdroppers are located in the network, the probability that there exist eavesdroppers within the SGZ of an active transmitter increases, resulting in decreased secure transmission probabilities $p_0$ and $p_1$. It can also be seen from Figure 3.5 that a larger SGZ leads to a decreased secrecy throughput capacity, which is because that as the SGZ size increases, more eavesdroppers will appear in the SGZ and thus the secure transmission probabilities $p_0$ and $p_1$ will decrease.

## 3.5 Summary

This chapter studied the secrecy guard zone (SGZ) design of a cell-partitioned MANET with the group-based scheduling scheme. We first proposed SGZ-based secure protocol, in which the transmission of a selected transmitter will be conducted only if no eavesdroppers exist in its SGZ. We then derived analytical expression for the exact secrecy throughput capacity of the concerned MANET under the secure protocol. Finally, we provide simulation and numerical results to illustrate the efficiency of our secrecy throughput capacity analysis as well the secrecy throughput capacity performance of the network. The results indicated that SGZ is an effective technique to provide security for wireless communications.

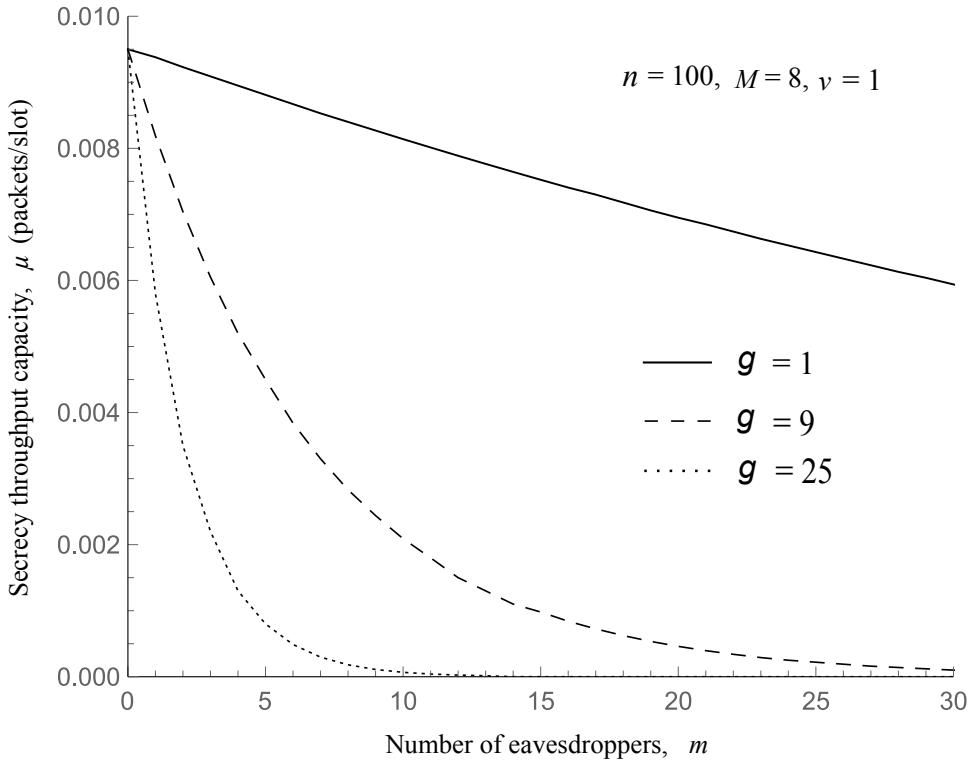



Figure 3.5: Secrecy throughput capacity $\mu$ vs. the number of eavesdroppers $m$ for varying SGZ size $g$.

# CHAPTER IV

# Cooperative Jamming based Secure Protocol in Cell-Partitioned MANETs

This chapter focuses on the cooperative jamming (CJ) design in cell-partitioned MANETs, for which we propose a CJ-based secure protocol to ensure the security of a finite network with multiple legitimate nodes and multiple eavesdroppers moving according to the independent and identically distributed (i.i.d.) mobility model. We then theoretically analyze two secure transmission probabilities and exact secrecy throughput capacity of the network under the CJ-based secure protocol. Finally, extensive simulation and numerical results are presented to validate our theoretical analysis and also to illustrate the impacts of the CJ-based secure protocol on the secrecy throughput capacity performance.

## 4.1 System Model

As illustrated in Figure 4.1, we consider that the wireless network is a square partitioned into $M \times M$ cells. The network consists of $n$ legitimate nodes and $m$ eavesdroppers. We adopt the independent and identically distributed (i.i.d.) mobility model, where each legitimate node or eavesdropper independently moves into a cell at the beginning of each time slot and stays in it during the whole slot. The

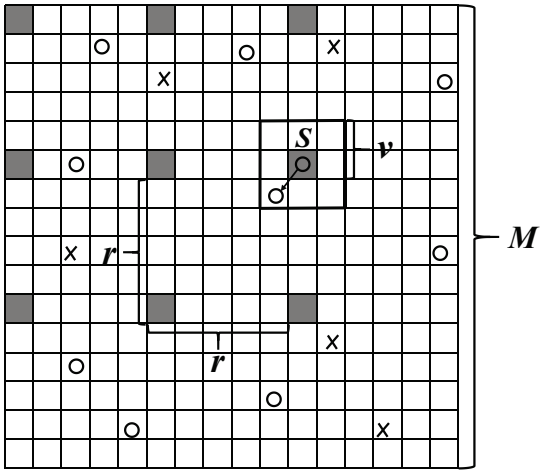



Figure 4.1: System Model: the circle represents legitimate node, the cross represents eavesdropper. All shaded cells mean that they are in the same group.

transmission range of each transmitter can be adjusted to cover a set of cells (called coverage cells) with horizontal and vertical distance of no more than $v-1$ cells away from the cell containing the transmitter, where $1 \leq v < \lfloor \frac{M+1}{2} \rfloor$ and $\lfloor . \rfloor$ is the floor function. We assume that the traffic flow follows the permutation model, where the source-destination pairs are determined as $1 \leftrightarrow 2, 3 \leftrightarrow 4, \cdots, (n-1) \leftrightarrow n$, i.e., each legitimate node is the source of a traffic flow and at the same time the destination of another traffic flow. We first define the $\lambda$ as the average input rate. Then, let $A_i(t)$ represent the number of generating packets for any legitimate transmitter $i$ at time $t$. We assume $\mathbb{E}\{A_i(t)\} = \lambda$ and a bounded second moment $A_{max}^2$ follows $\mathbb{E}\{A_i^2(t)\} \leq A_{max}^2 < \infty$, where $\mathbb{E}\{\}$ is the expectation operator. We adopt the widely-used group-based scheduling to coordinate the simultaneous transmission for eliminating interference. In this scheduling, all cells of the network are divided into $r^2$ groups. Each group consists of $K = \lfloor M^2/r^2 \rfloor$ cells and becomes active to transmit data every $r^2$ time slots. The cells in the current active group are called active cells throughout the thesis. In the same group, the distance between any two horizontally (or vertically) adjacent cells is of $r$ cells, as shown in Figure 4.1. In addition, $r$ can

be determined as

$$r = min\{\lceil(1+\Delta)\sqrt{2}v + v\rceil, M\}, \tag{4.1}$$

where $\lceil . \rceil$ is the ceiling function and $\Delta$ is a guard factor to prevent interference between transmitters and receivers.

## 4.2 Cooperative Jamming based Secure Protocol

We consider a new scenario where each transmitter can know the exact location of each eavesdropper in its transmission range. To ensure secure transmission in this scenario, we propose a cooperative jamming (CJ) based secure protocol [55, 72], in which we use non-transmitting legitimate nodes (say jammers) in the same cell of an eavesdropper to generate artificial noise, such that the eavesdroppers cannot intercept any information, as shown in Figure 4.2. We assume the other legitimate nodes in the same cell cannot correctly receive packets as well due to the heavy interference from jammers. Thus, the transmission of the selected transmitter can be conducted only if each eavesdropper in its transmission range is suppressed by the jammers in the same cell.

## 4.3 Exact Secrecy Throughput Capacity Analysis

In this section, we first need to derive the probability $p_0$ that a transmission can be securely conducted between a given active cell $c$ and the coverage cells of $c$ and also the probability $p_1$ that a source-destination transmission can be securely conducted between $c$ and its coverage cells. We establish the following lemmas regarding the two probabilities.

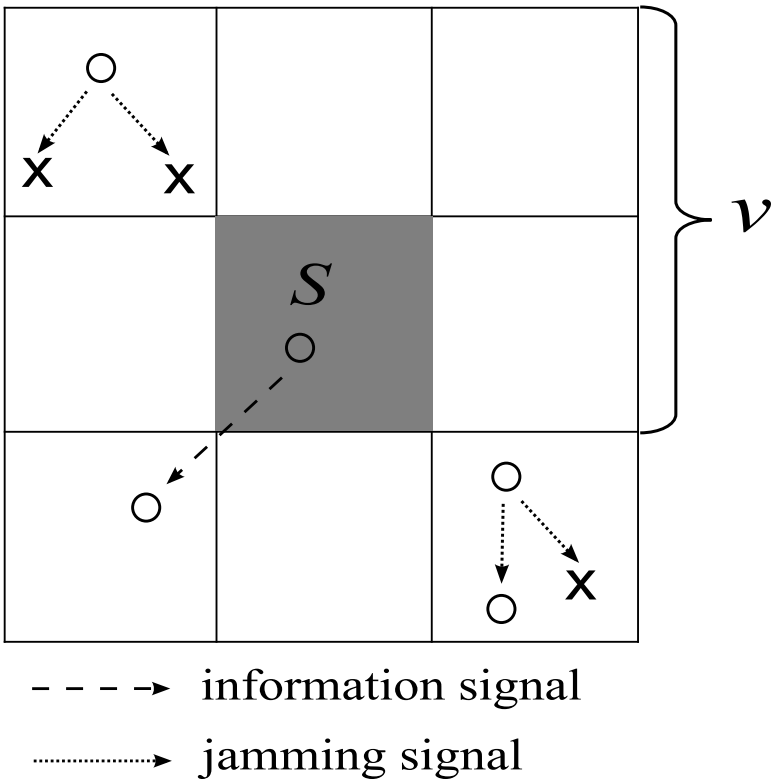



Figure 4.2: CJ-based secure protocol.

**Lemma 1** *For the concerned cell-partitioned MANET with the CJ-based secure protocol, the probability $p_0$ that a transmission can be securely conducted between the nodes in a given active cell $c$ and the nodes in the coverage cells of $c$ is given by*

$$p_0 = \Psi_2(0)\Omega_2(0) + \Psi_1(\beta)\Omega_1(\beta) + \sum_{k=1}^{\beta-1}\Big[\Psi_1(k)\Omega_1(k) + \Psi_2(k)\Omega_2(k)\Big]. \tag{4.2}$$

**Proof 2** *We divide the derivation of $p_0$ into two cases, i.e., the first case where the active cell $c$ contains eavesdroppers and the second case where $c$ does not contain eavesdroppers.*

*For the first case, we first discuss the distribution of eavesdroppers in the transmission range of $c$. We use $A_k$ $(1 \le k \le \beta)$ to denote the event that there are $k$ cells containing eavesdroppers (say eavesdropped cells) in the transmission range. To derive the probability of $A_k$, we first consider the event that there are $j$ eavesdroppers*

$$\Psi_1(k) = \sum_{j=k}^{m} \frac{C_{\beta-1}^{k-1} S(j,k) k!}{\beta^j} C_m^j \left(\frac{\beta}{M^2}\right)^j \left(1 - \frac{\beta}{M^2}\right)^{m-j}, \tag{4.3}$$

$$\Omega_1(k) = \sum_{i=k+2}^{n} \sum_{l=k+1}^{i-1} \frac{\left[C_i^l S(l,k) k! - C_i^1 C_{i-1}^{l-1} S(l-1,k-1)(k-1)!\right] \cdot (\beta - k)^{i-l}}{\beta^i} \cdot C_n^i \left(\frac{\beta}{M^2}\right)^i \left(1 - \frac{\beta}{M^2}\right)^{n-i}, \tag{4.4}$$

$$\Psi_2(k) = \sum_{j=k}^{m} \frac{C_{\beta-1}^{k} S(j,k) k!}{\beta^j} C_m^j \left(\frac{\beta}{M^2}\right)^j \left(1 - \frac{\beta}{M^2}\right)^{m-j}, \tag{4.5}$$

$$\Omega_2(k) = \sum_{i=k+2}^{n} \sum_{l=k}^{i-2} \sum_{d=1}^{i-l} \frac{\left[C_i^l S(l,k) k!\right] C_{i-l}^d (\beta - k - 1)^{i-l-d}}{\beta^i} \cdot C_n^i \left(\frac{\beta}{M^2}\right)^i \left(1 - \frac{\beta}{M^2}\right)^{n-i}. \tag{4.6}$$

---

*in the transmission range of c. It is easy to obtain the probability of this event as*

$$C_m^j \left(\frac{\beta}{M^2}\right)^j \left(1 - \frac{\beta}{M^2}\right)^{m-j}. \tag{4.7}$$

*The probability that these $j$ eavesdroppers are exactly located in the $k$ eavesdropped cells is given by*

$$\frac{C_{\beta-1}^{k-1} S(j,k) k!}{\beta^j}, \tag{4.8}$$

*where $S(j,k)$ is the Stirling numbers of the second kind and the term $C_{\beta-1}^{k-1}$ is due to the fact that we only need to select $k-1$ cells from the $\beta-1$ cells of the transmission range, provided that the active cell c is an eavesdropped cell. Thus, applying the law of total probability, we can determine the probability of $A_k$ as the $\Psi_1(k)$ in (4.3).*

*We then discuss the distribution of legitimate nodes in the transmission range of c such that the transmission can be securely conducted given the event $A_k$. We first consider the event that there are $0 \leq i \leq n$ legitimate nodes in the transmission range*

*of c, the probability of which is given by*

$$C_n^i \left(\frac{\beta}{M^2}\right)^i \left(1 - \frac{\beta}{M^2}\right)^{n-i}. \tag{4.9}$$

*Next, we assume that l out of the i nodes are located in the k eavesdropped cells. To ensure secure transmission, the distribution of legitimate nodes in the transmission range must satisfy the following conditions:*

*a)* $i \geq k + 2$*;*

*b) the active cell c contains at least two legitimate nodes, one for jamming eavesdroppers and the other for sending packets;*

*c) each of the other* $k - 1$ *eavesdropped cells must contain at least one legitimate node for jamming eavesdroppers;*

*d) there exists at least one legitimate node in the other* $\beta - k$ *cells for receiving packets (i.e.,* $l \leq i - 1$*).*

*Base on conditions b) and c), we have* $l \geq k + 1$*. Thus, the probability of secure transmission can be given by*

$$\sum_{l=k+1}^{i-1} \frac{\underbrace{\left[C_i^l S(l,k)k! - C_i^1 C_{i-1}^{l-1} S(l-1,k-1)(k-1)!\right]}_{Q} \cdot (\beta - k)^{i-l}}{\beta^i}, \tag{4.10}$$

*where the term Q is for ensuring condition b) and c). Thus, applying the law of total probability, the secure transmission probability under the event* $A_k$ *is the* $\Omega_1(k)$ *in (4.4).*

*Applying the law of total probability in terms of* $A_k$*, we determine the probability* $p_0$ *in the first case as*

$$\sum_{k=1}^{\beta} \Psi_1(k)\Omega_1(k). \tag{4.11}$$

*Now, we consider the case where the active cell c does not contain eavesdroppers, i.e., c is not an eavesdropped cell. Thus, we need to select k ($0 \leq k \leq \beta - 1$) cells from the $\beta - 1$ cells of the transmission range as the eavesdropped cells. Thus, the probability of $A_k$ can be determined as the $\Psi_2(k)$ in (4.5).*

*Given that there are $0 \leq i \leq n$ legitimate nodes in the transmission range, in this case, the conditions for secure transmission become as follows:*

*i)* $i \geq k + 2$;

*ii) each of the k eavesdropped cell must contain at least one legitimate node;*

*iii) there exist at least two legitimate nodes in the other $\beta - k$ cells and at least one of these nodes is in the active cell c.*

*Thus, assuming l out of the i nodes are located in the k eavesdropped cells and defining d the number of legitimate nodes in the active cell, the secure transmission probability under event $A_k$ is the $\Omega_2(k)$ in (4.6).*

*Applying the law of total probability in terms of $A_k$, we determine the probability $p_0$ in the second case as*

$$\sum_{k=0}^{\beta-1} \Psi_2(k)\Omega_2(k). \tag{4.12}$$

*Finally, combining the results in (4.11) and (4.12) yields the $p_0$ in (4.2).*

**Lemma 2** *For the concerned cell-partitioned MANET with the CJ-based secure protocol, the probability $p_1$ that a source-destination transmission can be securely conducted between the nodes in a given active cell c and the nodes in the coverage cells of c is given by*

$$p_1 = \Psi_2(0)\Phi_2(0) + \Psi_1(\beta)\Phi_1(\beta) + \sum_{k=1}^{\beta-1} \Big[\Psi_1(k)\Phi_1(k) + \Psi_2(k)\Phi_2(k)\Big]. \tag{4.13}$$

$$\Phi_1(k) = \sum_{i=k+2}^{n} \sum_{t=1}^{\lfloor \frac{i}{2} \rfloor} \sum_{l=k+1}^{i-1} \sum_{t_1=1}^{min\{t,l-k+1\}} \sum_{t_2=0}^{\lfloor \frac{l-t_1}{2} \rfloor} \sum_{t_3=0}^{l-t_1-2t_2} \sum_{s=0,s+t_1\geq 2}^{l-t_1-k+1}$$
$$\cdot \frac{C_{l-t_1-t_3}^{s} S\left(l-s-t_1, k-1\right)(k-1)!\left(\beta-k\right)^{i-l}}{\beta^i} C_t^{t_1} 2^{t_1} C_{t-t_1}^{t_2}$$
$$\cdot C_{t-t_1-t_2}^{t_3} 2^{t_3} C_{i-2t}^{l-t_1-2t_2-t_3} C_{\frac{n}{2}}^{t} C_{\frac{n}{2}-t}^{i-2t} 2^{i-2t} \left(\frac{\beta}{M^2}\right)^i \left(1-\frac{\beta}{M^2}\right)^{n-i}, \tag{4.14}$$

$$\Phi_2(k) = \sum_{i=k+2}^{n} \sum_{t=1}^{\lfloor \frac{i}{2} \rfloor} \sum_{l=k}^{i-2} \sum_{t_4=1}^{min\left\{t,\lfloor \frac{i-l}{2} \rfloor\right\}} \sum_{t_5=0}^{i-l-2t_4} \sum_{t_6=1}^{t_4} \frac{S(l,k)k!C_{t_4}^{t_6}\left[1+2\left(\beta-k-1\right)\right]^{t_6}}{\beta^i}$$
$$\cdot \left(\beta-k-1\right)^{2(t_4-t_6)} \left(\beta-k\right)^{i-l-2t_4} C_t^{t_4} C_{t-t_4}^{t_5} 2^{t_5} C_{i-2t}^{i-l-2t_4-t_5}$$
$$\cdot C_{\frac{n}{2}}^{t} C_{\frac{n}{2}-t}^{i-2t} 2^{i-2t} \left(\frac{\beta}{M^2}\right)^i \left(1-\frac{\beta}{M^2}\right)^{n-i}. \tag{4.15}$$

---

**Proof 3** *Similar to the proof of $p_0$, the proof of $p_1$ is also divided into two cases depending on whether $c$ is an eavesdropped cell or not. Notice that, for both cases, the distributions of eavesdroppers in the transmission range of $c$ (i.e., $\Psi_1(k)$ and $\Psi_2(k)$) are same to those in the derivation of $p_0$. Thus, we only discuss the distribution of legitimate nodes such that the source-destination transmission can be securely conducted for a given number of eavesdropped cells (i.e., the event $A_k$).*

*For the first case where $c$ is an eavesdropped cell, we consider an event that there are $0 \leq i \leq n$ legitimate nodes in the transmission range of $c$ and these $i$ nodes contain $t$ source-destination pairs, where $0 \leq t \leq \lfloor i/2 \rfloor$. The probability of this event can be given by*

$$C_{\frac{n}{2}}^{t} C_{\frac{n}{2}-t}^{i-2t} 2^{i-2t} \left(\frac{\beta}{M^2}\right)^i \left(1-\frac{\beta}{M^2}\right)^{n-i}. \tag{4.16}$$

*Under this event, we calculate the secure source-destination transmission probability. In addition to the conditions a) – d) for a secure communication in the derivation of $p_0$, another critical condition for a secure* source-destination *transmission is that the transmission must be conducted between one of the $t$ source-destination pairs, which*

*makes the calculation of $p_1$ highly complex.*

*We still assume $l$ out of the $i$ nodes are located in the $k$ eavesdropped cells. According to the locations of the two nodes in a source-destination pair, we classify the $t$ source-destination pairs into four categories: 1) one node is located in the active cell and the other is located in the $\beta - k$ non-eavesdropped cells; 2) both nodes are located in the $k$ eavesdropped cells; 3) one node is located in the other $k-1$ eavesdropped cells except for the active cell $c$ and the other is located in the $\beta - k$ non-eavesdropped cells; and 4) both nodes are located in the $\beta - k$ non-eavesdropped cells. We use $t_1$, $t_2$ and $t_3$ to denote the number of source-destination pairs of the categories 1), 2) and 3), respectively. Obviously, $t_1 + t_2 + t_3 \leq t$ and $l \geq t_1 + 2t_2 + t_3$. Notice that the remaining $l - (t_1 + 2t_2 + t_3)$ nodes in the $k$ eavesdropped cells are selected from the other $i - 2t$ unpaired nodes in the transmission range. Next, we use $s$ to denote the number of nodes in the active cell except for the $t_1$ nodes. Notice that these $s$ nodes are selected from the $l - t_1 - t_3$ nodes. Now, we have $s + t_1$ nodes in the active cell, $l - (s + t_1)$ nodes in the other $k - 1$ eavesdropped cells and $i - l$ in the $\beta - k$ non-eavesdropped cells. Based on these definitions and assumptions, in order to ensure a secure source-destination transmission, we must have $s + t_1 \geq 2$ (condition b)), $l - (s + t_1) \geq k - 1$ (condition c)), $l \leq i - 1$ (condition d)) and an additional condition $t_1 \geq 1$. Thus, the probability of a secure source-destination transmission can be given by*

$$\frac{\sum_{l=k+1}^{i-1} \sum_{t_1=1}^{min\{t,l-k+1\}} \sum_{t_2=0}^{\lfloor \frac{l-t_1}{2} \rfloor} \sum_{t_3=0}^{l-t_1-2t_2} \sum_{s=0,s+t_1\geq 2}^{l-t_1-k+1} C_{l-t_1-t_3}^{s} \underbrace{S\left(l-s-t_1, k-1\right)(k-1)!}_{Y} (\beta-k)^{i-l}}{\beta^i} \cdot C_t^{t_1} 2^{t_1} C_{t-t_1}^{t_2} C_{t-t_1-t_2}^{t_3} 2^{t_3} C_{i-2t}^{l-t_1-2t_2-t_3}, \tag{4.17}$$

*where the term $Y$ is to satisfy the condition c). Thus, applying the law of total*

*probability, the probability $p_1$ in the first case under the event $A_k$ is the $\Phi_1(k)$ in (4.14). We then apply the law of total probability in terms of $A_k$ to determine the probability $p_1$ in the first case as*

$$\sum_{k=1}^{\beta} \Psi_1(k)\Phi_1(k). \tag{4.18}$$

*Now, we consider the second case where the active cell $c$ does not contain eavesdroppers, i.e., $c$ is not an eavesdropped cell. We use $t_4$ and $t_5$ to denote the number of source-destination pairs where both nodes are in the $\beta - k$ non-eavesdropped cells (i.e., category 4) ) and the number of source-destination pairs where one node is in the $k$ eavesdropped cells and the other is in the $\beta - k$ non-eavesdropped cells (i.e., categories 1) and 3) ), respectively. In addition, we use $t_6$ to denote the number of source-destination pairs where one node is in the active cell and the other is in the $\beta - k$ non-eavesdropped cells. Notice that these $t_6$ pairs can be used for secure source-destination transmissions. Obviously, $t_6 \leq t_4$ and there are $1 + 2(\beta - k - 1)$ (resp. $(\beta - k - 1)^2$) kinds of distributions for each of the $t_6$ (resp. $t_4 - t_6$) pairs. Again, we assume $i$ nodes are located in the transmission range of the active cell $c$ and $l$ out of the $i$ nodes are located in the $k$ eavesdropped cells. Based on the conditions i)—iii) in the derivation of $p_0$ under the second case and an additional condition $t_6 \geq 1$, the probability $p_1$ under the event $A_k$ in the second case is given by the $\Phi_2(k)$ in (4.15). Applying the law of total probability in terms of $A_k$, we determine the probability $p_1$ in the second case as*

$$\sum_{k=0}^{\beta-1} \Psi_2(k)\Phi_2(k). \tag{4.19}$$

*Finally, combining the results in (4.18) and (4.19) yields the $p_1$ in (4.13).*

Based on $p_0$ and $p_1$, we can give the exact secrecy throughput capacity for the concerned network under the CJ-based secure protocol in the following theorem.

**Theorem IV.1** *Consider a cell-partitioned network with n legitimate nodes, m eavesdroppers and $M^2$ cells, where nodes move according to i.i.d. mobility model, the group-based scheduling is adopted to coordinate simultaneous link transmission and the CJ-based secure protocol is utilized to ensure secure transmissions, the exact secrecy throughput capacity $\mu$ of the concerned MANET is given by*

$$\mu = \frac{\lfloor M^2/r^2 \rfloor}{2n} \Bigg\{ \Psi_2(0)\Omega_2(0) + \Psi_1(\beta)\Omega_1(\beta) + \Psi_2(0)\Phi_2(0) + \Psi_1(\beta)\Phi_1(\beta) + \sum_{k=1}^{\beta-1} \Big[ \Psi_1(k)\Omega_1(k) + \Psi_2(k)\Omega_2(k) + \Psi_1(k)\Phi_1(k) + \Psi_2(k)\Phi_2(k) \Big] \Bigg\}, \tag{4.20}$$

*where $\Psi_1$, $\Psi_2$ are given by (4.3) and (4.5), $\Omega_1$, $\Omega_2$ are given by (4.4) and (4.6), and $\Phi_1$, $\Phi_2$ are given by (4.14) and (4.15), respectively.*

**Proof 4** *The theorem follows from the proof in Chapter III. The basic idea of the proof is as follows: first, we prove $\mu$ in (4.20) is an upper bound on the secrecy throughput capacity. Based on $p_0$, $p_1$, during the time slot T, we can get the overall transmission opportunities $Kp_0T$ and the source-destination transmission opportunities $Kp_1T$. Because the $Kp_1T$ opportunities can reach their destinations in only one top, and the $Kp_0T - Kp_1T$ opportunities can deliver at most $(Kp_0T - Kp_1T)/2$ packets. For arbitrarily small $\epsilon > 0$, the difference between the total input rate $n\lambda$ and the total output rate $Kp_1 + (Kp_0 - Kp_1)/2$ should be within $\epsilon$, thus, we derive the upper bound $\mu$. Second, we prove $\mu$ is the achievable upper bound. For any input rate $\lambda < \mu$, the concerned MANET is stable under the two-hop relay algorithm. Therefore, the upper bound $\mu$ is the exact secrecy throughput capacity. For the details of the proof, please refer to the secrecy throughput capacity analysis framework in Chapter III.*

**Remark 1** *The results in this work are computed for relatively non-practical models, which makes them not of significant practical values. Although these results fail to reflect the actual secrecy throughput capacity performances of networks in the real*

*world, they may still be able to provide us some insights on the fundamental trends of system secrecy throughput capacity performances as some key system parameters change. Notice that assuming highly academic non-practical models has been one of the basic research methodologies for network performance evaluation in the literature, like [73, 74] for network throughput study, [40, 48–50] for network secrecy throughput study.*

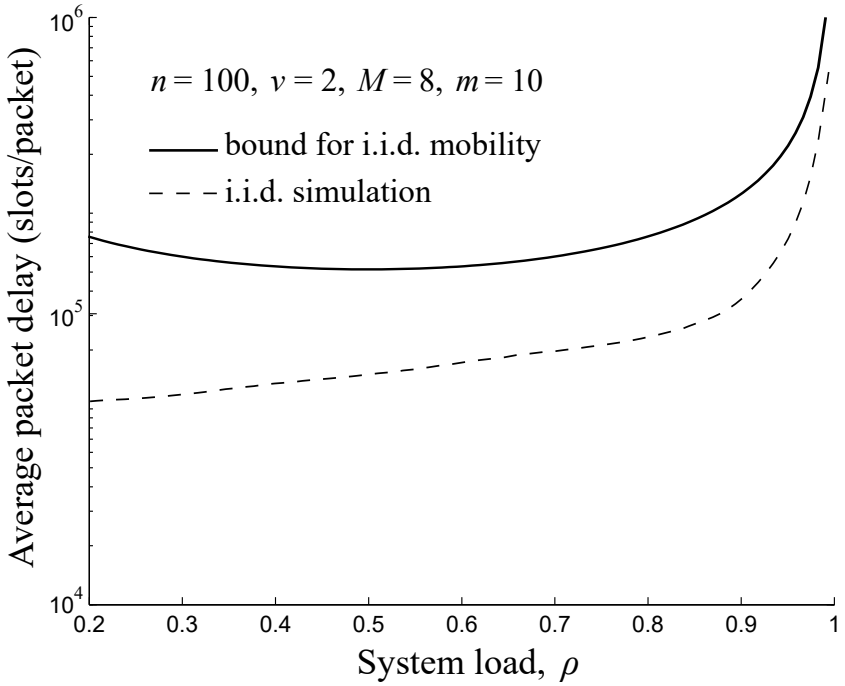
## 4.4 Numerical Results and Discussions

In this section, we first provide simulation results to validate our theoretical analysis for the secrecy throughput capacity performance of the concerned network. We then explore how the secrecy throughput capacity performance varies with the network parameters under the proposed CJ-based secure protocol.

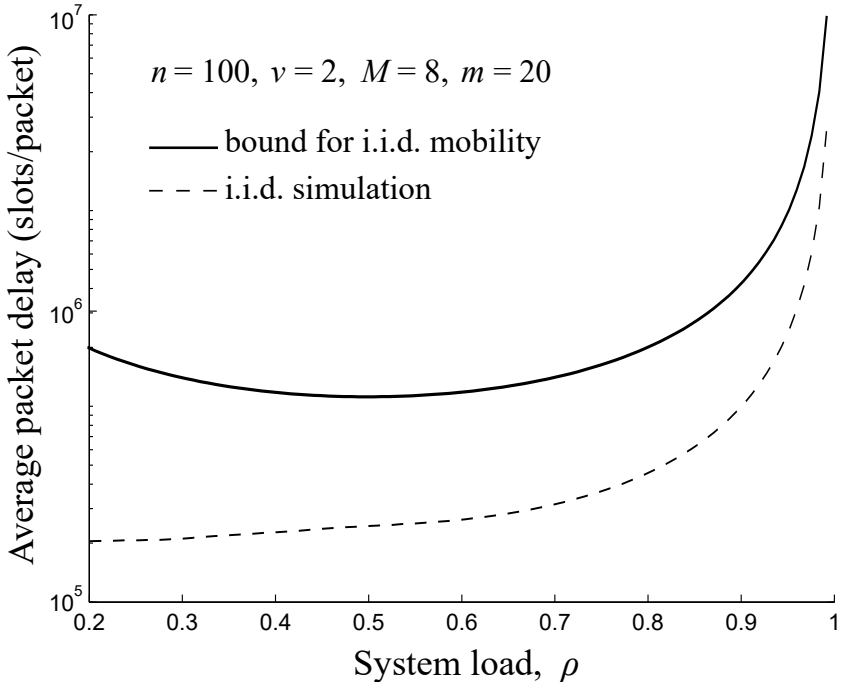
### 4.4.1 Model Validation

We developed a dedicated C++ simulator to simulate the packet delivery process in the concerned network under the CJ-based secure protocol, which is now available at [71]. In the simulation, we fix the guard factor as $\Delta = 1$ and focus the packet delivery process of a given source-destination pair during $10^7$ time slots.

For the CJ-based secure protocol, we set $v = 2$ (hence $r = 8$) and conduct extensive simulations under the network scenarios of ($n = 100$, $M = 8$, $m = 10$) and ($n = 100$, $M = 8$, $m = 20$), respectively. We provide plots of the simulated average packet delay and the theoretical delay bound in Figure 4.3. Similar behaviors of the average packet delay versus the system load $\rho$ can be observed from Figure 4.3, which indicates that our theoretical secrecy throughput capacity result under the CJ-based secure protocol is also efficient to exactly model the network secrecy throughput capacity performance of the concerned network.




(a) Average packet delay vs. system load under network scenario of $n = 100$, $v = 2$, $M = 8$, $m = 10$.




(b) Average packet delay vs. system load under network scenario of $n = 100$, $v = 2$, $M = 8$, $m = 20$.

Figure 4.3: Model validation under CJ-based secure protocol.

### 4.4.2 Performance Discussion

We investigate the impacts of the number of eavesdroppers $m$ and the side-length of transmission range $v$ on the secrecy throughput capacity $\mu$. For the fixed setting of $n = 100$ and $M = 8$, Figure 4.4 illustrates how $\mu$ varies with $m$ under three different sizes of transmission range, i.e., $v = 2$, $v = 3$ and $v = 4$. We can observe from Figure 4.4 that the secrecy throughput capacity decreases as $m$ increases, due to the reason that more eavesdroppers result in more eavesdropped cells in the transmission range of an active cell and thus more nodes will be sacrificed for suppressing these eavesdroppers, reducing the chances for an active cell to schedule two nodes to do packet (or source-destination packet) transmissions. Another observation from Figure 4.4 shows that, $\mu$ decreases as $v$ increases. This can be explained as follows: as $v$ increases, the size of transmission range increases, which leads to an increase in the number of eavesdropped cells. Thus, more legitimate nodes are required for secure transmission, resulting in a decrease in the secure transmission probabilities.

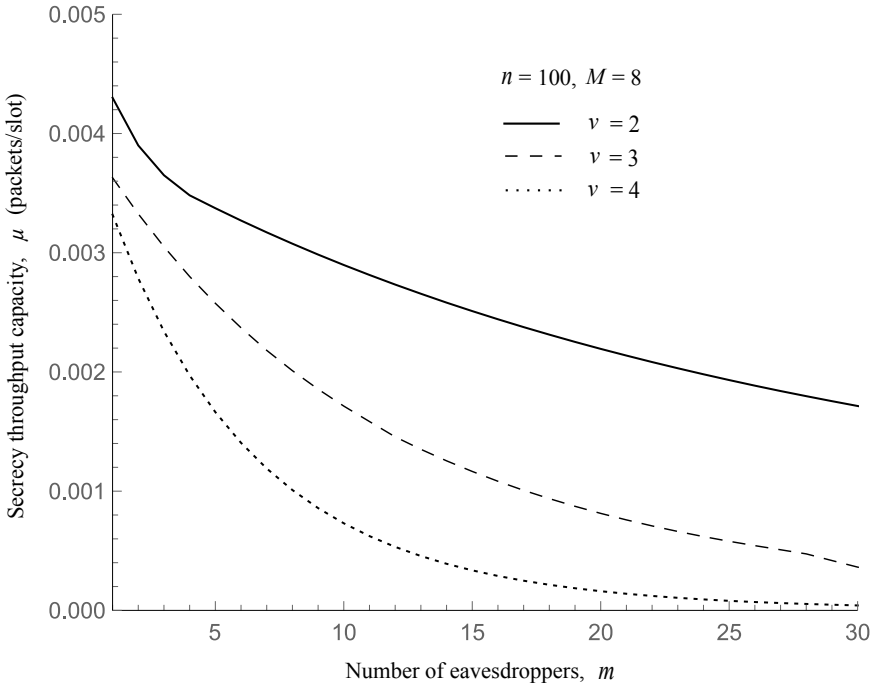
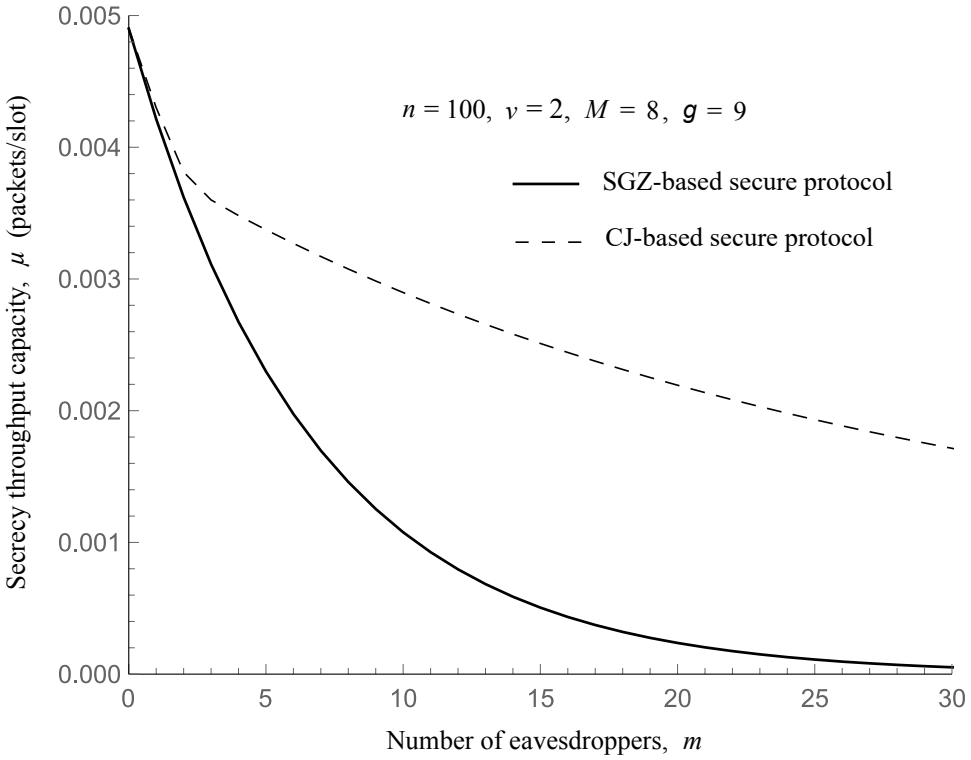


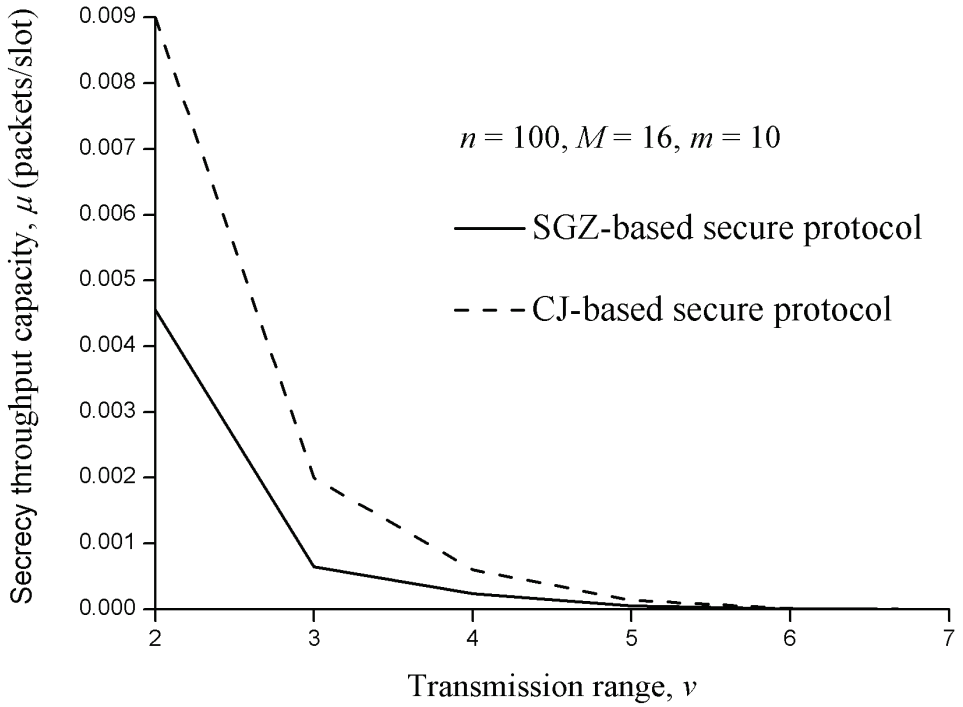

Figure 4.4: Secrecy throughput capacity $\mu$ vs. the number of eavesdroppers $m$ for varying $v$ under CJ-based secure protocol.

Finally, we compare the SGZ-based secure protocol in Chapter III with the CJ-based secure protocol in terms of the secrecy throughput capacity $\mu$. To make these two protocols comparable, we set the size of SGZ in Chapter III equal to the size of transmission range, i.e., $g = (2v-1)^2$. Under the setting of $n = 100, v = 2, M = 8$ and $g = 9$, we illustrate in Figure 4.5(a) how the $\mu$ varies with $m$ under both protocols. Under the setting of $n = 100, M = 16$ and $m = 10$, we illustrate in Figure 4.5(b) how the $\mu$ varies with $v$ under both protocols. We can see from Figure 4.5 that under the setting of $g = (2v - 1)^2$, the CJ-based secure protocol can achieve a larger secrecy throughput capacity $\mu$ than the SGZ-based secure protocol. This is because that for $g = (2v - 1)^2$ if there exists eavesdroppers in the SGZ (i.e., transmission range), the SGZ-based protocol cannot provide secure transmission opportunities, while the CJ-based protocol may still be able to ensure secure transmissions by suppressing these eavesdroppers.

Besides, we explore the impacts of the number of legitimate nodes $n$ on the secrecy throughput capacity $\mu$ under both protocols. As we can see from Figure 4.6, there exists an optimal number of legitimate nodes to maximize secrecy throughput capacity. This can be explained as follows: on the one hand, a greater number of legitimate nodes will result in more chances for an active cell to schedule two nodes to do packet transmissions and thus an increase in transmission rates of source nodes, but on the other hand, a greater number of legitimate nodes will introduce more significant medium contentions among source nodes and thus a decrease in their transmission rates. When the former (resp. the latter) factor dominates, secrecy throughput capacity increases (resp. decreases) as the number of legitimate nodes increases.




(a) Secrecy throughput capacity $\mu$ vs. the number of eavesdroppers $m$.




(b) Secrecy throughput capacity $\mu$ vs. transmission range $v$.

Figure 4.5: SGZ-based secure protocol vs. CJ-based secure protocol with guard zone size $g = (2v-1)^2$.

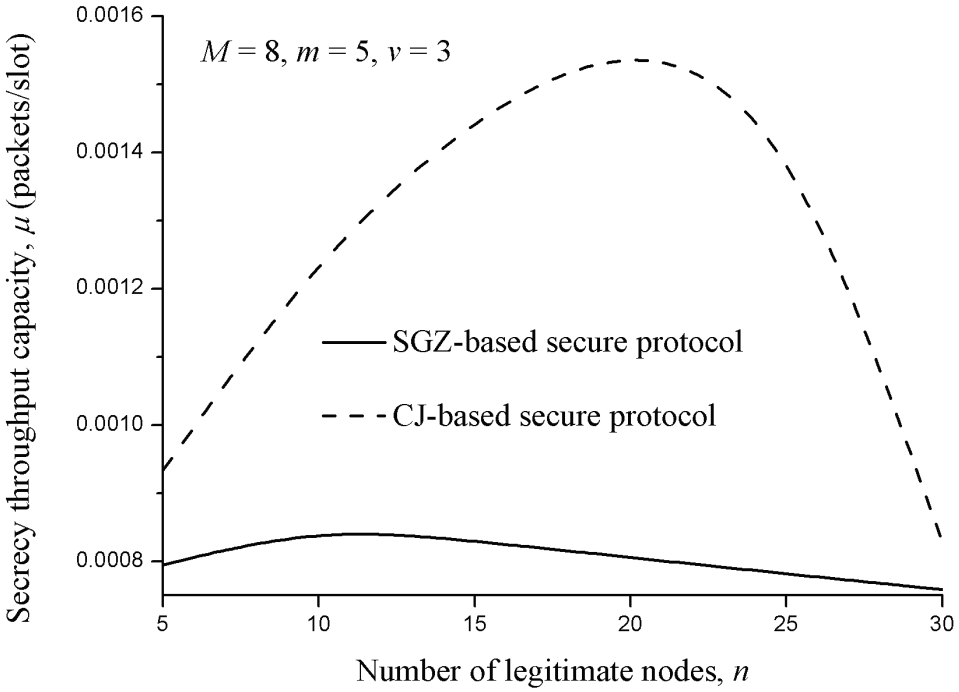



Figure 4.6: Secrecy throughput capacity $\mu$ vs. the number of legitimate nodes $n$ under both secure protocols.

## 4.5 Summary

This chapter explored the physical layer security-based secure communications in a finite cell-partitioned MANETs, for which a cooperative jamming (CJ) based secure protocol is proposed. The CJ-based protocol utilizes non-transmitting nodes to generate artificial noise to suppress eavesdroppers in the same cell, such that transmissions can be conducted only if all eavesdroppers in the transmission range are suppressed. To understand the security performance of the proposed secure protocol, we derived the exact secrecy throughput capacity result based on the analysis of two basic secure transmission probabilities. We also compared the SGZ-based secure protocol with the CJ-based secure protocol in terms of the secrecy throughput capacity. The results indicated that the CJ-based protocol outperforms the SGZ-based protocol with respect to the secrecy throughput capacity performance when the SGZ is equivalent to the transmission range.

# CHAPTER V

# Secure Protocols based on Artificial Noise and Secrecy Guard Zone in Continuous MANETs

In this chapter, by combining PHY security techniques (e.g., artificial noise injection and secrecy guard zone) and the conventional Aloha protocol, we first propose an artificial noise (AN)-based Aloha protocol and a secrecy guard zone (SGZ)-based Aloha protocol to ensure secure medium access for legitimate transmitters in continuous MANETs. To understand the security performances of the proposed secure Aloha protocols, we then apply tools from Stochastic Geometry to analyze the secrecy transmission capacity performance of MANETs under both protocols. Finally, we provide simulation/numerical results to validate our theoretical analysis and also to show the impacts of network parameters on the secrecy transmission capacity performance of the concerned network.

## 5.1 Preliminaries and Secure Protocols

### 5.1.1 Network Model

We consider a MANET, where the locations of legitimate nodes and eavesdroppers are modeled by independent and homogeneous Poisson Point Processes (PPPs) $\Psi_L$ and $\Psi_E$ with densities $\lambda_L$ and $\lambda_E$, respectively. We adopt the Aloha protocol

to schedule transmissions, where each legitimate node becomes a transmitter (resp. receiver) with probability $p$ (resp. $1-p$) in each time slot. Thus, due to the independent thinning, the locations of legitimate transmitters can be modeled by a PPP $\Psi_T$ with density $\lambda_T = p\lambda_L$ and those of the legitimate receivers by another independent PPP $\Psi_R$ with density $\lambda_R = (1-p)\lambda_L$.

To characterize the propagation effects, we consider the quasi-static Rayleigh fading model, where all channel gains remain constant in one time slot and vary randomly and independently from slot to slot. Thus, the fading coefficient $H_{ij}$ between nodes $i$ and $j$ follows the exponential distribution with unit mean. In addition to fading, all channels are also impaired by path loss and noise. We use $\alpha$ to denote the path loss exponent and use $W_r$ (resp. $W_e$) to denote the noise power at legitimate receivers (resp. eavesdroppers).

To transmit messages, each transmitter selects the nearest legitimate receiver as its *destination* receiver. Regarding the eavesdropping attack, we assume that information signals from the transmitters will not interfere with the eavesdroppers, which can be considered as the worst case.

### 5.1.2 Secure Aloha Protocols

To protect the transmissions of the legitimate transmitters, we propose two secure Aloha protocols, which combine commonly-used security schemes and the conventional Aloha protocol as described in Section 5.1.1. The first one is based on AN injection and thus called AN-based protocol. In this protocol, all transmitters become active and each transmits confidential messages and AN simultaneously to its destination receiver, as shown in Figure 5.1. We assume both the transmitter and receiver of a transmission pair know the channel state information (CSI) between them such that the receiver can eliminate the AN, while either the eavesdroppers or the other receivers cannot. The second one is based on SGZ and thus named SGZ-based

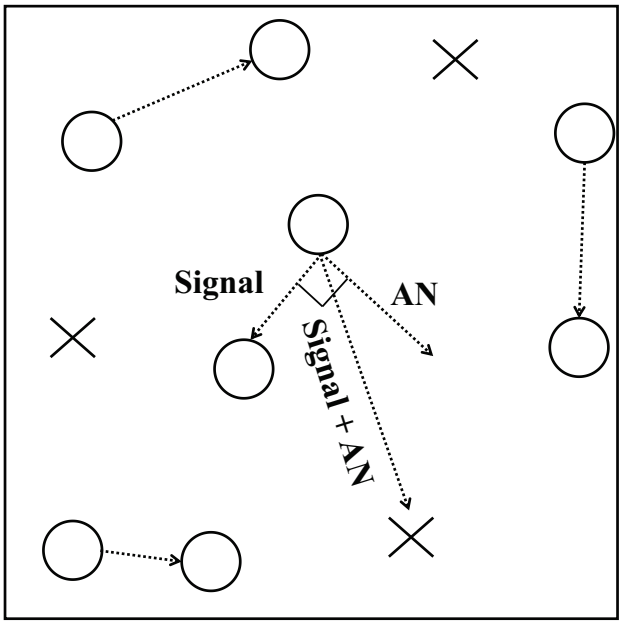



Figure 5.1: AN-based secure Aloha protocol: the circle represents legitimate node and the cross represents eavesdropper.

protocol. In this scheme, we assume that each transmitter can detect the existence of eavesdroppers inside a circle with radius $D$ around it, i.e., the SGZ as shown in Figure 5.2. Different from the AN-based protocol, in the SGZ-based protocol, only the transmitters whose SGZ contains no eavesdroppers become active, i.e., transmit messages.

### 5.1.3 Performance Metrics

In this chapter, we assume the transmitters adopt the Wyner encoding scheme [17] when transmitting confidential messages. In this scheme, each confidential message is associated with multiple symbols, and encoded to one of them at random during the transmission. Two rates are chosen for each transmission, i.e., one rate $R_t$ to encode the symbol and one rate $R_s$ to encode the confidential message. The difference $R_e = R_t - R_s$ reflects the cost to confuse the eavesdroppers.

The main performance metric considered in this work is the secrecy transmission

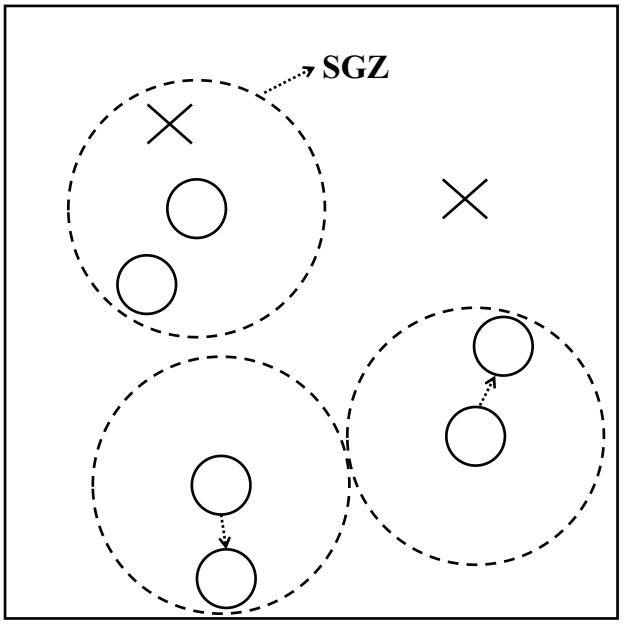



Figure 5.2: SGZ-based secure Aloha protocol.

capacity, which characterizes the average maximum achievable rate of secure and reliable transmissions per unit area. To characterize the reliability of a certain transmission, the connection outage probability (COP) is adopted, which is the probability that the intended receiver fails to decode the transmitted message, i.e., the channel capacity is less than rate $R_t$. Denoting the receiver by $j$, we can formulate the COP as

$$\begin{aligned} p_{co} &= \mathbb{P}\left(\log(1+\mathrm{SINR}_j) < R_t\right) \\ &= \mathbb{P}\left(\mathrm{SINR}_j < 2^{R_t} - 1\right), \end{aligned} \tag{5.1}$$

where $\mathrm{SINR}_j$ denotes the Signal-to-Interference-plus-Noise Ratio (SINR) at the receiver and log is to the base of 2. We can see that the COP is a monotonically increasing function of $R_t$.

To characterize the security of the transmission, we adopt the secrecy outage probability (SOP) metric, which represents the probability that eavesdroppers succeed in decoding the transmitted messages and can be formulated as

$$
\begin{aligned}
p_{so} &= 1 - \mathbb{P}\Big( \bigcap_{e \in \Psi_E} \log(1 + \mathrm{SINR}_e) \leq R_e \Big) \\
&= 1 - \mathbb{P}\Big( \bigcap_{e \in \Psi_E} \mathrm{SINR}_e \leq 2^{R_e} - 1 \Big),
\end{aligned} \tag{5.2}
$$

where $\mathrm{SINR}_e$ denotes the SINR at eavesdropper $e$. This definition implies that the transmission suffers from secrecy outage, i.e, is not secure, if at least one eavesdropper can decode the transmitted messages. We can see that the SOP is a monotonically decreasing function of $R_e$.

According to [40], given a COP constraint $\sigma$ and an SOP constraint $\varepsilon$, i.e., $p_{co}(R_t) \leq \sigma$ and $p_{so}(R_e) \leq \varepsilon$, we can formulate the secrecy transmission capacity $T_c$ as

$$
T_c = (1 - \sigma)\lambda_{AT}(R_t^{\max} - R_e^{\min}), \tag{5.3}
$$

where $\lambda_{AT}$ denotes the density of active transmitters, $R_t^{\max}$ denotes the maximum allowable coderate $R_t$ and $R_e^{\min}$ denotes the minimum allowable $R_e$. Due to the monotonicity of $p_{co}$ in terms of $R_t$, $R_t^{\max}$ can be given by

$$
R_t^{\max} = \log(1 + p_{co}^{-1}(\sigma)). \tag{5.4}
$$

Similarly, $R_e^{\min}$ can be given by

$$
R_e^{\min} = \log(1 + p_{so}^{-1}(\varepsilon)). \tag{5.5}
$$

## 5.2 Secrecy Transmission Capacity for Artificial Noise based Aloha Protocol

This section presents the secrecy transmission capacity analysis for the network under the AN-based protocol, for which the COP and SOP are derived in Subsections

5.2.1 and 5.2.2, respectively. Based on the COP and SOP, the secrecy transmission capacity is given in Subsection 5.2.3.

### 5.2.1 COP Analysis

To facilitate the analysis, we focus on a typical transmitter-receiver pair and define $i$ and $j$ the transmitter and receiver, respectively. The total transmission power of the transmitter is $P$, of which a fraction $\tau$ $(0 < \tau < 1)$ is allocated to message transmission and the remaining $1-\tau$ fraction is to AN transmission. From the Slivnyak's theorem [75], given the location of the typical transmitter, the locations of other transmitters still follow the PPP with density $p\lambda_L$. Since $j$ receives interference from the other concurrent transmitters in $\Psi_T \backslash \{i\}$, the SINR of $j$ can be given by

$$\mathrm{SINR}_j = \frac{\tau P H_{ij} \left|X_{ij}\right|^{-\alpha}}{\sum_{k \in \Psi_T \backslash \{i\}} P H_{kj} \left|X_{kj}\right|^{-\alpha} + W_r}, \tag{5.6}$$

where $H_{aj}$ and $|X_{aj}|$ represent the channel fading and the distance between nodes $a$ $(a \in \{i, k\})$ and $j$, respectively. $W_r$ denotes the background noise power at the receiver $j$. Based on the formulation in (5.1), we now derive the COP in the following lemma.

**Lemma 3** *The COP of any link in the considered MANET under the AN-based Aloha protocol is*

$$p_{co}^{\mathrm{AN}} = 1 - 2(1-p)\lambda_L \pi \int_0^{\infty} e^{-\theta(\frac{\beta_t}{\tau})^{\frac{2}{\alpha}} r^2 - (1-p)\lambda_L \pi r^2 - \frac{\beta_t}{\tau P} W_r r^{\alpha}} r \mathrm{d}r, \tag{5.7}$$

where $\beta_t = 2^{R_t} - 1$, $\theta = \pi p \lambda_L \Gamma(1 - 2/\alpha)\Gamma(1 + 2/\alpha)$.

**Proof 5** *Based on the definition in (5.1), we have*

$$\begin{aligned}
p_{co}^{\mathrm{AN}} &= \mathbb{P}\left(\mathrm{SINR}_j < \beta_t\right) \\
&= 1 - \mathbb{P}\left(\mathrm{SINR}_j \geq \beta_t\right) \\
&= 1 - \mathbb{P}\left(\frac{\tau P H_{ij} \left|X_{ij}\right|^{-\alpha}}{\sum_{k\in\Psi_T\setminus\{i\}} P H_{kj} \left|X_{kj}\right|^{-\alpha} + W_r} \geq \beta_t\right) \\
&= 1 - \mathbb{P}\left[H_{ij} \geq \frac{\beta_t}{\tau}\left|X_{ij}\right|^{\alpha}\left(I_0 + \frac{W_r}{P}\right)\right] \\
&\overset{(a)}{=} 1 - \mathbb{E}\left[e^{-\frac{\beta_t}{\tau}\left|X_{ij}\right|^{\alpha}\left(I_0+\frac{W_r}{P}\right)}\right] \\
&= 1 - \mathbb{E}_{I_0}\left(e^{-\frac{\beta_t}{\tau}\left|X_{ij}\right|^{\alpha} I_0}\right)\mathbb{E}_{W_r}\left(e^{-\frac{\beta_t}{\tau P}\left|X_{ij}\right|^{\alpha} W_r}\right) \\
&\overset{(b)}{=} 1 - \exp\left[-\theta\left(\frac{\beta_t}{\tau}\right)^{\frac{2}{\alpha}}\left|X_{ij}\right|^2\right]\exp\left(-\frac{\beta_t}{\tau P} W_r \left|X_{ij}\right|^{\alpha}\right)
\end{aligned} \tag{5.8}$$

where $I_0 = \sum_{k\in\Psi_T\setminus\{i\}} H_{kj}\left|X_{kj}\right|^{-\alpha}$ is a shot noise process, $(a)$ follows since $H_{ij}$ is an exponential random variable with unit mean, and $(b)$ follows from the Laplace transform of $I_0$ in [76].

Since each transmitter chooses the nearest legitimate receiver as the destination receiver. The distance $|X_{ij}|$ between the typical transmitter $i$ and destination receiver $j$ is a random variable, whose probability density function (PDF) is given by [77]

$$f_{|X_{ij}|}(r) = \mathrm{e}^{-(1-p)\lambda_L \pi r^2} 2(1-p)\lambda_L \pi r. \tag{5.9}$$

Taking the expectation of the last step in (5.8) in terms of $|X_{ij}|$ completes the proof.

### 5.2.2 SOP Analysis

For the analysis of the SOP, we focus on the typical transmission link $i \to j$ again. Any eavesdropper $e$ targeting this link receives interference from only the AN of the

transmitters in $\Psi_T$. Hence, the SINR at the eavesdropper $e$ is given by

$$\mathrm{SINR}_e = \frac{\tau P H_{ie} \left|X_{ie}\right|^{-\alpha}}{I_{ie} + I_{\tilde{i}e} + W_e}, \tag{5.10}$$

where $H_{ie}$ and $|X_{ie}|$ represent the channel fading and the distance between the transmitter $i$ and the eavesdropper $e$,

$$I_{ie} = (1-\tau) P H_{ie} \left|X_{ie}\right|^{-\alpha}$$

denotes the interference from the transmitter $i$ and the eavesdropper $e$,

$$I_{\tilde{i}e} = \sum_{k \in \Psi_T \setminus \{i\}} (1-\tau) P H_{ke} \left|X_{ke}\right|^{-\alpha}$$

denotes the interference at $e$ from the other concurrent transmitters, and $W_e$ denotes the background noise power at $e$. Based on the formulation in (5.2), we derive the upper bound on the SOP in the following lemma.

**Lemma 4** *The upper bound on the SOP of any link in the considered MANET under the AN-based Aloha protocol is*

$$p_{so}^{\mathrm{AN,UB}} = 1 - \exp\Bigg[ - \frac{2\pi\lambda_E \tau}{\beta_e - \tau\beta_e + \tau} \int_0^\infty e^{-\theta\left(\frac{(1-\tau)\beta_e}{\tau}\right)^{\frac{2}{\alpha}} r^2 - \frac{\beta_e}{\tau P} W_e r^\alpha} r \mathrm{d}r \Bigg] \tag{5.11}$$

*where* $\beta_e = 2^{R_e} - 1$, $\theta = \pi p \lambda_L \Gamma(1-2/\alpha)\Gamma(1+2/\alpha)$.

**Proof 6** *See Appendix A.1.*

Next, we derive the lower bound on the SOP in the following lemma.

**Lemma 5** *The lower bound on the SOP of any link in the considered MANET under*

*the AN-based Aloha protocol is*

$$p_{so}^{\mathrm{AN,LB}} = \frac{2\lambda_E \pi \tau}{\beta_e - \tau\beta_e + \tau} \int_0^\infty e^{-\theta\left(\frac{(1-\tau)\beta_e}{\tau}\right)^{\frac{2}{\alpha}} r^2 - \lambda_E \pi r^2 - \frac{\beta_e}{\tau P} W_e r^\alpha} r \mathrm{d}r. \tag{5.12}$$

*where* $\beta_e = 2^{R_e} - 1$, $\theta = \pi p \lambda_L \Gamma(1 - 2/\alpha)\Gamma(1 + 2/\alpha)$.

**Proof 7** *To derive the lower bound, we only consider the eavesdropper nearest to the transmitter. We define* $|X_{ie^*}|$ *the distance between the typical transmitter* $i$ *and the nearest eavesdropper* $e^*$. *The probability density function* $f_{|X_{ie^*}|}(r)$ *of the* $|X_{ie^*}|$ *is*

$$f_{|X_{ie^*}|}(r) = e^{-\lambda_E \pi r^2} 2\lambda_E \pi r. \tag{5.13}$$

*Thus, we have*

$$\begin{aligned} p_{so}^{\mathrm{AN}} &\geq \mathbb{P}\left(\mathrm{SINR}_{e^*} \geq \beta_e\right) \\ &= \frac{\tau}{\beta_e - \tau\beta_e + \tau} \exp\left[-\theta\left(\frac{(1-\tau)\beta_e}{\tau}\right)^{\frac{2}{\alpha}} |X_{ie^*}|^2\right] \exp\left(-\frac{\beta_e}{\tau P} W_e |X_{ie^*}|^\alpha\right). \end{aligned} \tag{5.14}$$

*Computing the expectation of (5.14) in terms of* $|X_{ie^*}|$ *completes the proof.*

### 5.2.3 Secrecy Transmission Capacity Analysis

Finally, we obtain the lower bound on the secrecy transmission capacity based on the COP in Lemma 3 and the upper bound on the SOP in Lemma 4. The result is summarized in the following theorem.

**Theorem V.1** *Given a COP constraint* $\sigma$ *and an SOP constraint* $\varepsilon$, *the secrecy transmission capacity of the considered MANET under the AN-based Aloha protocol can be lower bounded by*

$$T_c^{\mathrm{AN}} \geq p\lambda_L(1-\sigma)(R_t^{\max,\mathrm{AN}} - R_e^{\min,\mathrm{AN}}), \tag{5.15}$$

*where* $R_t^{\max,\mathrm{AN}}$ *is given by*

$$R_t^{\max,\mathrm{AN}} = \log(1 + (p_{co}^{\mathrm{AN}})^{-1}(\sigma)), \tag{5.16}$$

*and* $R_e^{\min,\mathrm{AN}}$ *is given by*

$$R_e^{\min,\mathrm{AN}} = \log(1 + (p_{so}^{\mathrm{AN,UB}})^{-1}(\varepsilon)). \tag{5.17}$$

**Proof 8** *The proof directly follows the definition in (5.3) with* $\lambda_{AT} = p\lambda_L$, $p_{co}$ *replaced by* $p_{co}^{\mathrm{AN}}$ *and* $p_{so}$ *replaced by* $p_{so}^{\mathrm{AN,UB}}$.

## 5.3 Secrecy Transmission Capacity for Secrecy Guard Zone based Aloha Protocol

This section focuses on the secrecy transmission capacity analysis for the SGZ-based protocol. We drive the COP and SOP in Subsections 5.3.1 and 5.3.2, respectively, based on which the secrecy transmission capacity is derived in Subsection 5.3.3.

### 5.3.1 COP Analysis

According to the SGZ-based protocol, each transmitter becomes active if and only if there exist no eavesdroppers in its SGZ, which is a circle with radius $D$ centered at itself. In other words, each eavesdropper silents the transmitters in a circle with radius $D$ centered at itself. As a result, the locations of active transmitters follow the Poisson Hole Process (PHP) [78], which is formed by the baseline PPP $\Psi_L$ and hole PPP $\Psi_E$ in the way that each eavesdropper $e \in \Psi_E$ carves out a hole with radius $D$ from the PPP $\Psi_L$. Since exact modeling of the PHP is challenging in general, we resort to a good approximation, which approximates the PHP by a homogeneous

PPP $\Psi_{AT}$ with density

$$\lambda_{AT} = p\lambda_L \exp(-\pi D^2 \lambda_E), \tag{5.18}$$

where $\exp(-\pi D^2 \lambda_E)$ is the probability that there are no eavesdroppers in the SGZ of a transmitter.

Based on this approximation, we proceed to derive the COP, for which we focus on a typical link $i \to j$ again. Since $j$ receives interference from simultaneous transmitters, the SINR of $j$ can be given by

$$\mathrm{SINR}_j = \frac{PH_{ij} |X_{ij}|^{-\alpha}}{\sum_{k \in \Psi_{AT} \setminus \{i\}} PH_{kj} |X_{kj}|^{-\alpha} + W_r}, \tag{5.19}$$

The COP can be easily obtained based on Lemma 3, which is given in the following lemma.

**Lemma 6** *The COP of any link in the considered MANET under the SGZ-based Aloha protocol is*

$$\mathrm{p}_{\mathrm{co}}^{\mathrm{SGZ}} = 1 - 2(1-p)\lambda_L \pi \int_0^\infty e^{-\vartheta(\beta_t)^{\frac{2}{\alpha}} r^2 - \pi(1-p)\lambda_L r^2 - \frac{\beta_t}{P} W_r r^\alpha} r \mathrm{d}r, \tag{5.20}$$

*where* $\beta_t = 2^{R_t} - 1$, $\vartheta = \pi\lambda_{AT}\Gamma(1-2/\alpha)\Gamma(1+2/\alpha)$.

**Proof 9** *See Appendix A.2*

### 5.3.2 SOP Analysis

Since we consider the worst case where information signals form concurrent transmitters will not interfere with eavesdroppers, the received signals of an eavesdropper $e$ are only impaired by the background noise. Thus, the $\mathrm{SINR}_{\mathrm{e}}$ at the eavesdropper $e$ is

$$\mathrm{SINR}_e = \frac{PH_{ie} |X_{ie}|^{-\alpha}}{W_e}, \tag{5.21}$$

Following the derivations in Lemmas 4 and 5, the bounds on the SOP can be easily derived in the following lemmas.

**Lemma 7** *The upper bound on the SOP of any link in the considered MANET under the SGZ-based Aloha protocol can be given by*

$$p_{so}^{\mathrm{SGZ,UB}} = 1 - \exp\left[-2\pi\lambda_E \int_D^{\infty} e^{-\frac{\beta_e}{P}W_e r^{\alpha}} r \mathrm{d}r\right], \tag{5.22}$$

*where* $\beta_e = 2^{R_e} - 1$.

**Proof 10** *See Appendix A.3.*

Next, we derive the lower bound on the SOP in the following lemma.

**Lemma 8** *The lower bound on the SOP of any link in the considered MANET under the SGZ-based Aloha protocol is*

$$p_{so}^{\mathrm{SGZ,LB}} = 2\pi\lambda_E \int_D^{\infty} e^{-\frac{\beta_e}{P}W_e r^{\alpha} - \lambda_E \pi r^2} r \mathrm{d}r, \tag{5.23}$$

**Proof 11** *To derive the lower bound, we only consider the eavesdropper nearest to the transmitter. We define* $|X_{ie^*}|$ *the distance between the typical transmitter* $i$ *and the nearest eavesdropper* $e^*$*. Based on the probability density function* $f_{|X_{ie^*}|}(r)$ *of the* $|X_{ie^*}|$ *in (5.13), we have*

$$\begin{aligned} p_{so}^{\mathrm{SGZ}} &\geq \mathbb{P}\left(\mathrm{SINR}_{e^*} \geq \beta_e\right) \\ &= \exp\left(-\frac{\beta_e}{P} W_e \left|X_{ie}\right|^{\alpha}\right) \end{aligned} \tag{5.24}$$

*Computing the expectation of (5.24) in terms of* $|X_{ie^*}|$ *completes the proof.*

### 5.3.3 Secrecy Transmission Capacity Analysis

We obtain the secrecy transmission capacity based on the COP in Lemma 6 and the upper bound on the SOP in Lemma 7. The result is summarized in the following

theorem.

**Theorem V.2** *Given a COP constraint $\sigma$ and an SOP constraint $\varepsilon$, the secrecy transmission capacity of the considered MANET under the SGZ-based Aloha protocol can be lower bounded by*

$$T_c^{\mathrm{SGZ}} \geq p\lambda_L e^{-\pi D^2 \lambda_E}(1-\sigma)(R_t^{\max,\mathrm{SGZ}} - R_e^{\min,\mathrm{SGZ}}), \tag{5.25}$$

*where $R_t^{\max,\mathrm{SGZ}}$ is given by*

$$R_t^{\max,\mathrm{SGZ}} = \log(1 + (p_{co}^{\mathrm{SGZ}})^{-1}(\sigma)), \tag{5.26}$$

*and $R_e^{\min,\mathrm{SGZ}}$ is given by*

$$R_e^{\min,\mathrm{SGZ}} = \log(1 + (p_{so}^{\mathrm{SGZ,UB}})^{-1}(\varepsilon)). \tag{5.27}$$

**Proof 12** *The proof directly follows the definition in (5.3) with $\lambda_{AT} = p\lambda_L \exp(-\pi D^2 \lambda_E)$, $p_{co}$ replaced by $p_{co}^{\mathrm{SGZ}}$ and $p_{so}$ replaced by $p_{so}^{\mathrm{SGZ,UB}}$.*

## 5.4 Numerical Results and Discussions

This section provides numerical results to validate the theoretical analysis of COP and SOP under both secure Aloha protocols, and also to show the impacts of network parameters on the secrecy transmission capacity performance.

### 5.4.1 COP Validation

We develop a Java simulator [79] that simulates the COP for both secure Aloha protocols. The network parameters are set as follows: $\lambda_L = 0.015$, $\alpha = 4$, $P = 1$, $\beta_t = 0.4$.

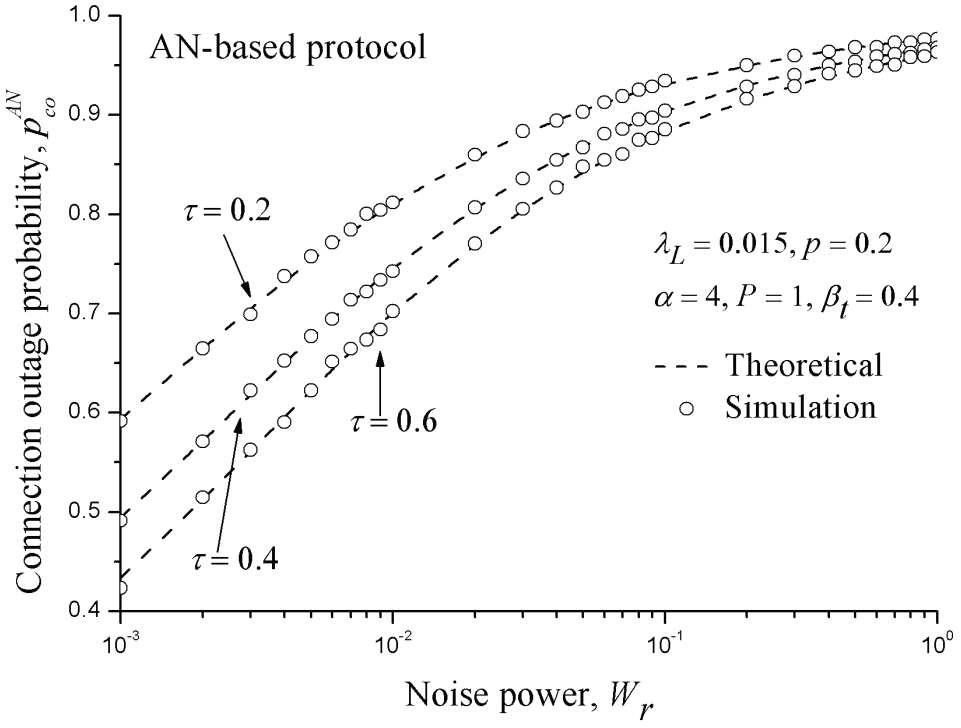



Figure 5.3: COP vs. noise power $W_r$ under AN-based protocol.

Figure 5.3 plots the theoretical and simulation results versus noise power $W_r$ under the AN-based Aloha protocol. In Figure 5.3, we set transmission probability $p = 0.2$ and consider three settings of transmission power ratio $\tau$, i.e., $\tau = 0.2, 0.4, 0.6$. Figure 5.3 shows that the theoretical COP results match nicely with the simulation ones, implying the correctness of the derived COP result. We can see from Figure 5.3 that as the noise power $W_r$ increases, the COP increases. This is because as the noise power increases, the total interference at a receiver increases, leading to a smaller SINR and thus a larger COP. From Figure 5.3 we can also see that as the power allocation ratio $\tau$ increases, the COP decreases. This is because as $\tau$ increases, the power for confidential information transmission increases, and so does the SINR of the destination receiver, resulting in a smaller COP.

For the validation of the COP under the SGZ-based Aloha protocol, we plot in Figure 5.4 the theoretical and simulation COP results versus noise power under different settings of transmission probability $p$, i.e., $p = 0.2, 0.4, 0.6$. We set the radius

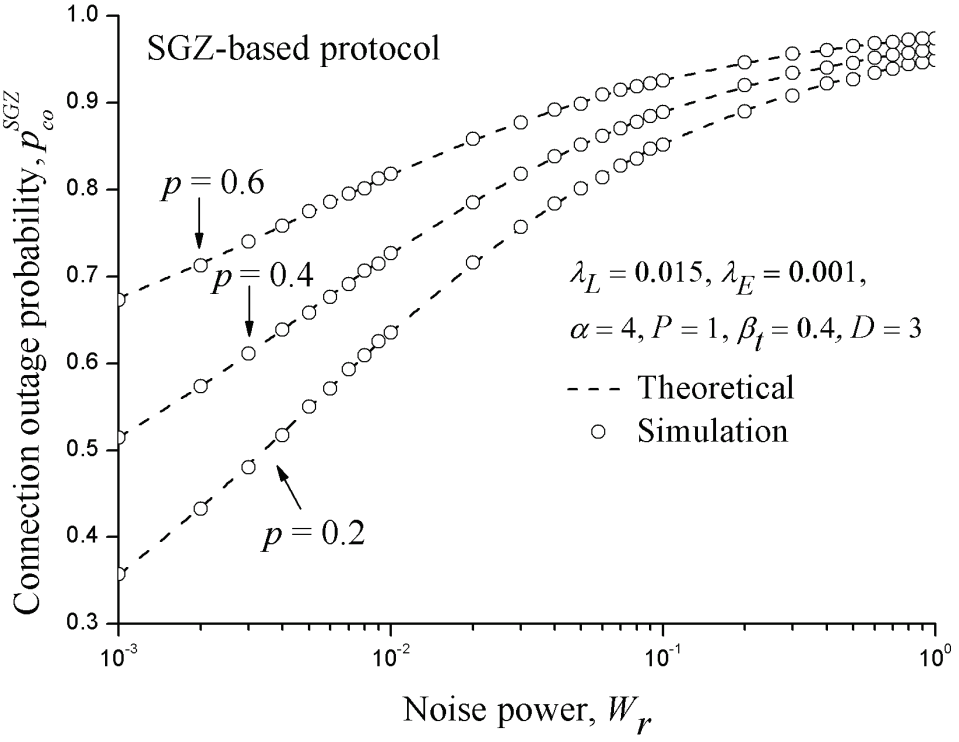



Figure 5.4: COP vs. noise power $W_r$ under SGZ-based protocol.

of the SGZ to $D = 3$ and the eavesdropper density to $\lambda_E = 0.001$. Figure 5.4 shows that the theoretical COP results under the SGZ-based Aloha protocol match nicely with the simulation ones, implying the correctness of the derived COP result. We can see from Figure 5.4 that as the noise power increases, the COP increases due to the same reason as in Figure 5.3. We can also observe that as the transmission probability $p$ increases, the COP also increases. The reason is that as $p$ increases, there will be more transmitters in the network, causing more interference at a receiver and thus leading to an increased COP.

### 5.4.2 SOP Validation

The Java simulator [79] is also used to simulate the SOP for both secure Aloha protocols. The parameters are set as follows: $\lambda_E = 0.001$, $\alpha = 4$, $P = 1$, $\beta_e = 0.01$.

For the validation of the SOP under the AN-based Aloha protocol, we set $\lambda_L =$

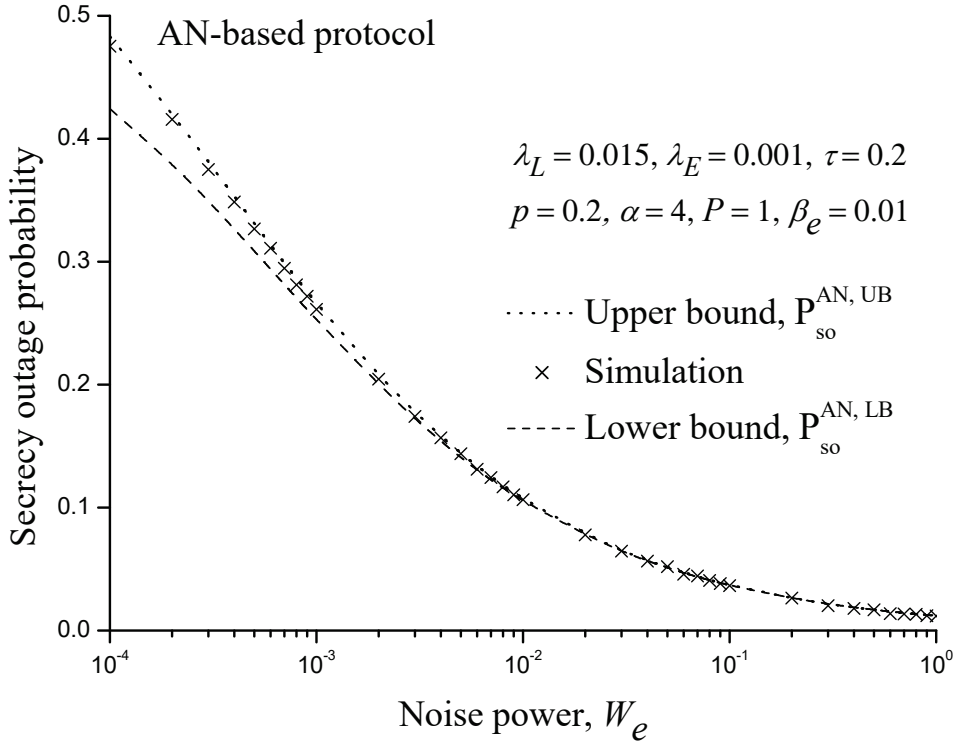



Figure 5.5: SOP vs. noise power $W_e$ under AN-based protocol.

0.015, $\tau = 0.2$, $p = 0.2$ and summarize the theoretical results (upper bound and lower bound results) and simulation results versus noise power $W_e$ at eavesdroppers in Figure 5.5. We can see from Figure 5.5 that the upper bound matches nicely with the simulation results, while the lower bound does not, implying that the upper bound is effective to model the SOP performance of the network. Figure 5.5 shows that as noise power $W_e$ increases, the SOP decreases. This is because as $W_e$ increases, the SINR at an eavesdropper becomes smaller, leading to a smaller SOP.

For the validation of the SOP under the SGZ-based Aloha protocol, Figure 5.6 shows the theoretical and simulation results of SOP versus noise power $W_e$ under different settings of $D$, i.e., $D = 3, 6$. Similarly, Figure 5.6 shows that the upper bound is tight enough to depict the SOP performance of the network under the SGZ-based Aloha protocol. We can see from Figure 5.6 that as the noise power increases, the SOP decreases due to the same reason as in Figure 5.5. Figure 5.6 also shows

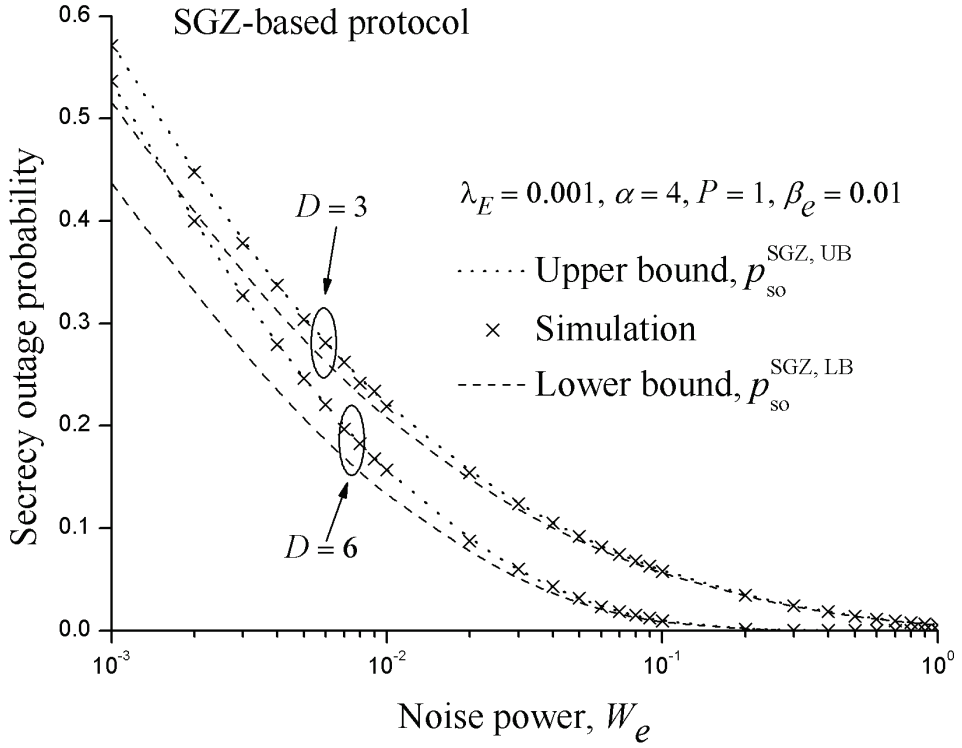



Figure 5.6: SOP vs. noise power $W_e$ under SGZ-based protocol.

that as the radius of SGZ $D$ increases, the SOP decreases. The reason is that as $D$ increases, the distances between eavesdroppers and the typical transmitter become larger. Thus, the signal power received by the eavesdroppers will decrease, and so does the SOP.

### 5.4.3 Secrecy Transmission Capacity vs. Transmitter Density

This part explores the impacts of the transmitter density $\lambda_T$ on the secrecy transmission capacity performance in MANETs under both secure Aloha protocols. We assume that the legitimate receiver density is fixed. The network parameters are set as follows: $\lambda_R = 0.01$, $\lambda_E = 0.001$, $\alpha = 4$, $P = 1$, $W_r = W_e = 0.001$, $\sigma = 0.4$. For the AN-based Aloha protocol, in Figure 5.7, we set the power allocation ratio $\tau = 0.4$ and consider three settings of $\varepsilon$, i.e., $\varepsilon = 0.3, 0.5, 1$. Figure 5.7 shows that, the secrecy transmission capacity first increases and then decreases as the transmitter

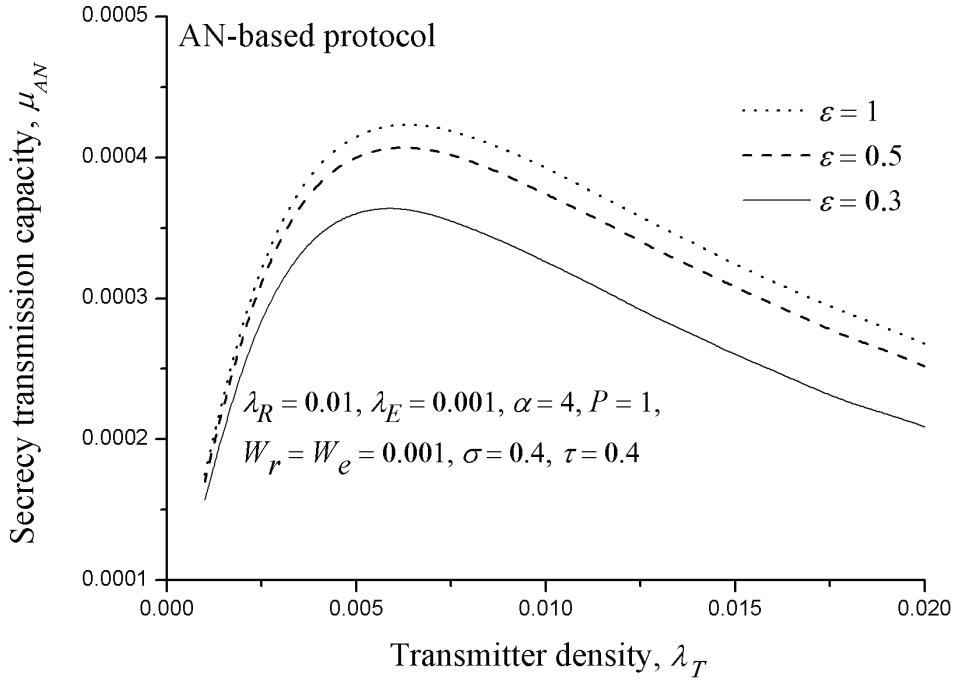



Figure 5.7: Secrecy transmission capacity vs. transmitter density $\lambda_T$ under AN-based protocol.

density $\lambda_T$ increases, and thus there exists an optimal $\lambda_T$ that maximizes the secrecy transmission capacity. We can also observe that the secrecy transmission capacity increases as the SOP constraint $\varepsilon$ increases. This is because as $\varepsilon$ becomes larger, the security requirement becomes lower, allowing a smaller minimum required rate $R_e$. As a result, the secrecy transmission capacity increases.

For the secrecy transmission capacity performance under the SGZ-based Aloha protocol, Figure 5.8 depicts the secrecy transmission capacity vs. $\lambda_T$ under different settings of $\varepsilon$ for $D = 3$. We can see that, similar to Figure 5.7, there also exists an optimal $\lambda_T$ for each value of $\varepsilon$, and the secrecy transmission capacity also increases as the SOP constraint $\varepsilon$ increases.

### 5.4.4 Secrecy Transmission Capacity vs. Power Allocation

This part explores the impact of the power allocation ratio $\tau$ on the secrecy transmission capacity performance in MANETs under the AN-based Aloha protocol. Fig-

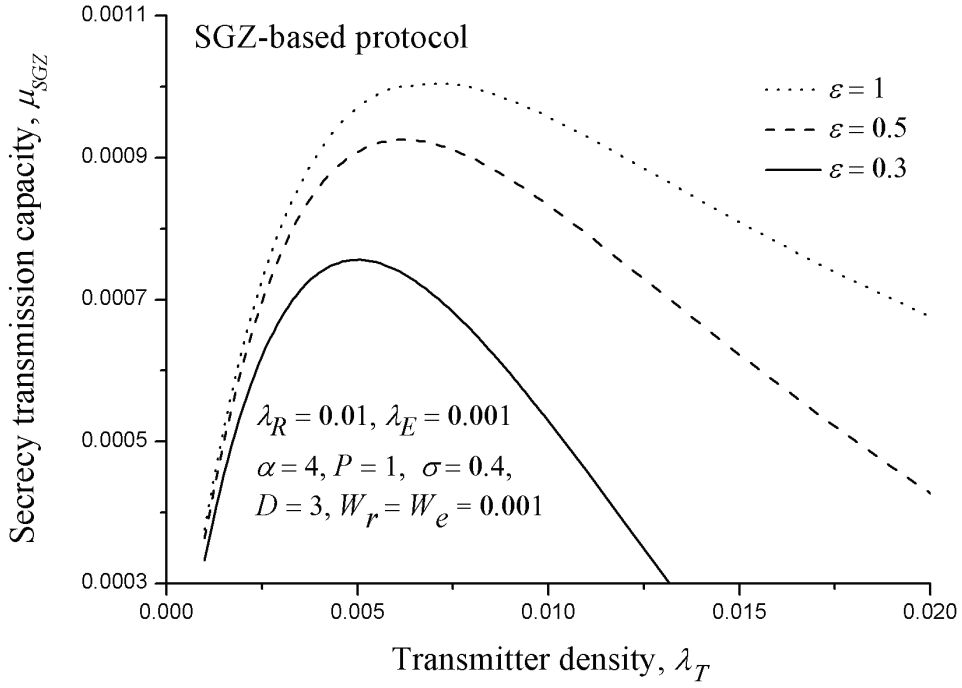



Figure 5.8: Secrecy transmission capacity vs. transmitter density $\lambda_T$ under SGZ-based protocol.

ure 5.9 plots secrecy transmission capacity versus $\tau$ for different $\lambda_E$ under the settings of $\lambda_L = 0.015$, $p = 0.2$, $\alpha = 4$, $P = 1$, $W_r = W_e = 0.001$, $\sigma = 0.4$, $\varepsilon = 0.3$. We can observe from Figure 5.9 that as the power allocation increases, the secrecy transmission capacity of the network first increases and then decreases. Thus, there exists an optimal power allocation ratio $\tau$ that maximizes the secrecy transmission capacity. A careful observation indicates that the optimal $\tau$ increases as $\lambda_E$ decreases. This is because as $\lambda_E$ decreases, the security requirement becomes lower, allowing the smaller AN transmission power $(1 - \tau)P$. As a result, the $\tau$ increases.

## 5.5 Summary

This chapter explored the physical layer security-based secure communications in a infinite Poisson MANET. We proposed an artificial noise (AN)-based Aloha protocol and a secrecy guard zone (SGZ)-based Aloha protocol for the network. To

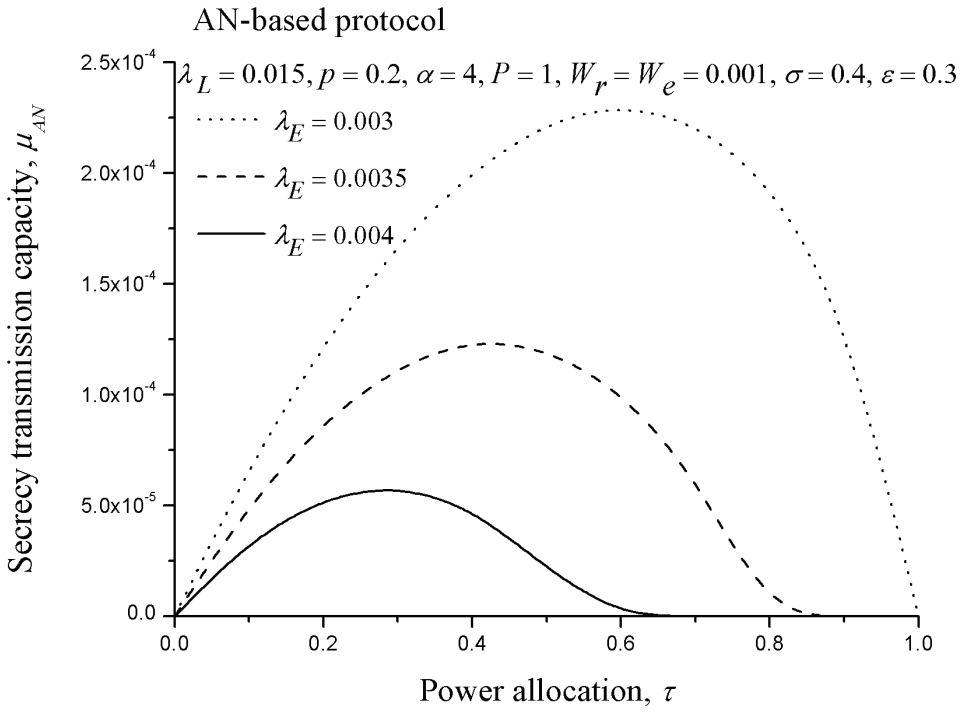



Figure 5.9: Secrecy transmission capacity vs. power allocation ratio $\tau$ under AN-based protocol.

understand the security and reliability performances of the proposed secure Aloha protocols, we analyzed the COP as well as the upper and lower bounds on the SOP of the considered network. Based on the COP and SOP, we then derived the secrecy transmission capacity of the network under both protocols. Numerical results in this work showed that the proposed secure Aloha protocols can significantly improve the secrecy transmission capacity of networks for the worst case where information signals from the transmitter will not interfere with the eavesdroppers. For a network with the AN-based Aloha protocol, our theoretical analysis can serve as a guideline on the proper setting of power allocation ratio such that the optimal secrecy transmission capacity in the network can be achieved.

# CHAPTER VI

# Conclusion

In this thesis, we studied the secure protocol design in MANETs, where the typical PHY security techniques, such as secrecy guard zone (SGZ), cooperative jamming (CJ) and artificial noise (AN), are adopted to ensure secure communications. We first explored the SGZ-based secure protocol in cell-partitioned MANETs, and then investigated the CJ-based secure protocol in cell-partitioned MANETs. Finally, we examined the secure protocols based on AN and SGZ in continuous MANETs.

For the secure protocol design of wireless networks, we studied in Chapter III the SGZ-based protocol in a cell-partitioned MANET with multiple legitimate nodes and multiple eavesdroppers. We considered a scenario where each transmitter can detect the existence of eavesdroppers in a region around itself, called SGZ. For this scenario, we proposed an SGZ-based secure protocol, in which the transmission of a selected transmitter will be conducted only if no eavesdroppers exist in its SGZ. We then derived exact analytical expression for the secrecy throughput capacity performance of the concerned network under the proposed secure protocol based on the analysis of two basic secure transmission probabilities. The main results in Chapter III showed that SGZ is an effective technique to provide security for wireless communications.

In Chapter IV, we addressed the CJ design issue in large-scale wireless networks, for which proposed a CJ-based secure protocol to ensure the secure transmission of

a finite cell-partitioned MANET with multiple legitimate nodes and multiple eavesdroppers. The CJ-based secure protocol utilizes non-transmitting nodes to generate artificial noise to suppress eavesdroppers in the same cell, such that transmissions can be conducted only if all eavesdroppers in the transmission range are suppressed. The exact analytical expression for the secrecy throughput capacity was also derived to evaluate the performances of the proposed protocol. The results in this thesis indicated that the CJ-based protocol outperforms the SGZ-based protocol with respect to the secrecy throughput capacity performance when the SGZ is equivalent to the transmission range.

In Chapter V, we studied the secure protocol design in continuous MANETs with multiple legitimate nodes and multiple eavesdroppers, whose locations are modeled by two independent and homogeneous Poisson Point Processes, respectively. We first proposed two secure Aloha protocols, i.e., AN-based protocol and SGZ-based protocol, which implement commonly-used PHY security schemes on top of the conventional Aloha protocol to ensure secure transmissions of transmitters. We then theoretically analyzed the COP, the upper and lower bounds on the SOP of the network under two secure Aloha protocols. Based on the COP and SOP results, we then determined the secrecy transmission capacity of both protocols. The results in this chapter showed that the proposed secure Aloha protocols can significantly improve the secrecy transmission capacity of networks for the worst case where information signals from the transmitter will not interfere with the eavesdroppers. For a network with the AN-based Aloha protocol, our theoretical analysis can serve as a guideline on the proper setting of power allocation ratio such that the optimal secrecy transmission capacity in the network can be achieved.

The secure protocols in this thesis are proposed under the permutation traffic model, so one possible future work is to explore the performance of the proposed secure protocols under the spanning tree traffic model. Since this thesis derived the

exact secrecy throughput capacity for a two-hop network, another interesting and also important research direction is to study the performance in multi-hop MANETs with the proposed secure protocols.

# APPENDICES

# APPENDIX A

# Proofs in Chapter V

## A.1 Proof of Lemma 4

The SOP is the probability that the SINR of at least one eavesdropper is greater than the given threshold $\beta_e$. We use $v(e)$ to indicate whether the secrecy outage caused by eavesdropper $e$ occurs. If the secrecy outage happens, $v(e) = 1$. Otherwise, $v(e) = 0$. Thus, the SOP can be calculated as follows.

$$\begin{aligned} p_{so}^{\mathrm{AN}} &= 1 - \mathbb{E}_{\Psi_T, H_{ie}, \{H_{ke}\}} \left\{ \mathbb{E}_{\Psi_E} \left\{ \prod_{e \in \Psi_E} \Big[ 1 - v(e) \Big] \right\} \right\} \\ &= 1 - \mathbb{E}_{\Psi_T, H_{ie}, \{H_{ke}\}} \left\{ \mathbb{E}_{\Psi_E} \left\{ \prod_{e \in \Psi_E} \Big[ 1 - \mathbb{P}\Big( \mathrm{SINR}_e \geq \beta_e \Big) \Big] \right\} \right\} \\ &= 1 - \mathbb{E}_{\Psi_T, H_{ie}, \{H_{ke}\}} \left\{ \mathbb{E}_{\Psi_E} \left\{ \prod_{e \in \Psi_E} \Big[ 1 - \mathbb{P}\Big( \frac{\tau P H_{ie} \left| X_{ie} \right|^{-\alpha}}{I_{ie} + I_{\bar{ie}} + W_e} \geq \beta_e \Big) \Big] \right\} \right\}. \end{aligned} \tag{A.1}$$

According to [75], applying the probability generating functional of the PPP $\Psi_E$

and then changing to the polar coordinate system gives

$$p_{so}^{\mathrm{AN}} = 1 - \mathbb{E}_{\Psi_T, H_{ie}, \{H_{ke}\}} \Bigg\{ \exp\Big[ -2\pi\lambda_E \int_0^{\infty} \mathbb{P}\Big( \frac{\tau P H_{ie} r^{-\alpha}}{I_{ie} + I_{\bar{i}e} + W_e} \geq \beta_e \Big) r \mathrm{d}r \Big] \Bigg\}. \tag{A.2}$$

Next, applying the Jensen's Inequality, we have

$$\begin{aligned} p_{so}^{\mathrm{AN}} &\leq 1 - \exp\Big[ -2\pi\lambda_E \int_0^{\infty} \mathbb{E}_{\Psi_T, H_{ie}, \{H_{ke}\}} \Big\{ \mathbb{P}\Big( \frac{\tau P H_{ie} r^{-\alpha}}{I_{ie} + I_{\bar{i}e} + W_e} \geq \beta_e \Big) \Big\} r \mathrm{d}r \Big] \\ &= 1 - \exp\Big[ -2\pi\lambda_E \int_0^{\infty} \mathbb{E}_{\Psi_T, H_{ie}, \{H_{ke}\}} \Big\{ \exp\Big[ -\frac{\beta_e r^{\alpha} (I_{ie} + I_{\bar{i}e} + W_e)}{\tau P} \Big] \Big\} r \mathrm{d}r \Big] \\ &= 1 - \exp\Big[ -2\pi\lambda_E \int_0^{\infty} \mathcal{L}_{I_{ie}}\Big( \frac{\beta_e r^{\alpha}}{\tau P} \Big) \mathcal{L}_{I_{\bar{i}e}}\Big( \frac{\beta_e r^{\alpha}}{\tau P} \Big) \exp\Big( -\frac{\beta_e r^{\alpha} W_e}{\tau P} \Big) r \mathrm{d}r \Big]. \end{aligned} \tag{A.3}$$

The Laplace transform of $I_{ie}$ is easy to derive, since $H_{ie}$ follows the exponential distribution with unit mean, and the Laplace transform of $I_{\bar{i}e}$ follows from that of $I_0$ since $I_{\bar{i}e}$ is also a shot noise process. After calculating the Laplace transforms, we complete the proof.

## A.2 Proof of Lemma 6

Based on the definition in (5.1), we have

$$\begin{aligned} p_{co}^{\mathrm{SGZ}} &= \mathbb{P}\left(\mathrm{SINR}_j < \beta_t\right) \\ &= 1 - \mathbb{P}\left(\mathrm{SINR}_j \geq \beta_t\right) \\ &= 1 - \mathbb{P}\left(\frac{PH_{ij}\left|X_{ij}\right|^{-\alpha}}{\sum_{k\in\Psi_{AT}\setminus\{i\}} PH_{kj}\left|X_{kj}\right|^{-\alpha} + W_r} \geq \beta_t\right) \\ &= 1 - \mathbb{P}\left[H_{ij} \geq \beta_t \left|X_{ij}\right|^{\alpha}\left(I_0^{'} + \frac{W_r}{P}\right)\right] \\ &\overset{(c)}{=} 1 - \mathbb{E}\left[e^{-\beta_t|X_{ij}|^{\alpha}\left(I_0^{'}+\frac{W_r}{P}\right)}\right] \\ &= 1 - \mathbb{E}_{I_0^{'}}\left(e^{-\beta_t|X_{ij}|^{\alpha}I_0^{'}}\right)\mathbb{E}_{W_r}\left(e^{-\frac{\beta_t}{P}|X_{ij}|^{\alpha}W_r}\right) \\ &\overset{(d)}{=} 1 - \exp\left[-\vartheta(\beta_t)^{\frac{2}{\alpha}}\left|X_{ij}\right|^2\right]\exp\left(-\frac{\beta_t}{P}W_r\left|X_{ij}\right|^{\alpha}\right) \end{aligned} \tag{A.4}$$

where $I_0^{'} = \sum_{k\in\Psi_{AT}\setminus\{i\}} H_{kj}\left|X_{kj}\right|^{-\alpha}$ is a shot noise process, $(c)$ follows since $H_{ij}$ is an exponential random variable with unit mean, and $(d)$ follows from the Laplace transform of $I_0^{'}$ in [76].

Since each transmitter chooses the nearest legitimate receiver as the destination receiver. The distance $|X_{ij}|$ between the typical transmitter $i$ and destination receiver $j$ is a random variable, whose probability density function (PDF) is given by [77]

$$f_{|X_{ij}|}(r) = \mathrm{e}^{-(1-p)\lambda_L\pi r^2}2(1-p)\lambda_L\pi r. \tag{A.5}$$

Taking the expectation of the last step in (A.4) in terms of $|X_{ij}|$ completes the proof.

## A.3 Proof of Lemma 7

We also use $v(e)$ to indicate whether the secrecy outage caused by eavesdropper $e$ occurs. If the secrecy outage happens, $v(e) = 1$. Otherwise, $v(e) = 0$. Thus, the

SOP can be calculated as follows.

$$\begin{aligned} p_{so}^{\mathrm{SGZ}} &= 1 - \mathbb{E}_{H_{ie}}\left\{\mathbb{E}_{\Psi_E}\left\{\prod_{e\in\Psi_E}\Big[1 - v(e)\Big]\right\}\right\} \\ &= 1 - \mathbb{E}_{H_{ie}}\left\{\mathbb{E}_{\Psi_E}\left\{\prod_{e\in\Psi_E}\Big[1 - \mathbb{P}\Big(\mathrm{SINR}_e \geq \beta_e\Big)\Big]\right\}\right\} \\ &= 1 - \mathbb{E}_{H_{ie}}\left\{\mathbb{E}_{\Psi_E}\left\{\prod_{e\in\Psi_E}\Big[1 - \mathbb{P}\Big(\frac{PH_{ie}\,|X_{ie}|^{-\alpha}}{W_e} \geq \beta_e\Big)\Big]\right\}\right\}. \end{aligned} \tag{A.6}$$

According to [75], applying the probability generating functional of the PPP $\Psi_E$ and then changing to the polar coordinate system gives

$$p_{so}^{\mathrm{SGZ}} = 1 - \mathbb{E}_{H_{ie}}\left\{\exp\Big[-2\pi\lambda_E\int_D^{\infty}\mathbb{P}\Big(\frac{PH_{ie}r^{-\alpha}}{W_e} \geq \beta_e\Big)r\mathrm{d}r\Big]\right\}. \tag{A.7}$$

Next, applying the Jensen's Inequality, we have

$$\begin{aligned} p_{so}^{\mathrm{SGZ}} &\leq 1 - \exp\Big[-2\pi\lambda_E\int_D^{\infty}\mathbb{E}_{H_{ie}}\Big\{\mathbb{P}\Big(\frac{PH_{ie}r^{-\alpha}}{W_e} \geq \beta_e\Big)\Big\}r\mathrm{d}r\Big] \\ &= 1 - \exp\Big[-2\pi\lambda_E\int_D^{\infty}\mathbb{E}_{H_{ie}}\Big\{\exp\Big[-\frac{\beta_e r^{\alpha}W_e}{P}\Big]\Big\}r\mathrm{d}r\Big] \\ &= 1 - \exp\Big[-2\pi\lambda_E\int_D^{\infty}\exp\Big(-\frac{\beta_e r^{\alpha}W_e}{P}\Big)\,r\mathrm{d}r\Big]. \end{aligned} \tag{A.8}$$

# BIBLIOGRAPHY

# BIBLIOGRAPHY


[1] C. K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems.* Prentice-Hall, Englewood Cliffs, NJ, 2002.

[2] C. S. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols.* Upper Saddle River, NJ: Prentice-Hall, 2004.

[3] D. Aggarwal and U. Maurer, "Breaking RSA Generically Is Equivalent to Factoring," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6251–6259, 2016.

[4] F. Bao, R. Deng, and H. Zhu, "Variations of Diffie-Hellman Problem," in *International conference on information and communications security*, 2003, pp. 301–312.

[5] D. Adrian, K. Bhargavan, Z. Durumeric *et al.*, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 5–17.

[6] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[7] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[8] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2019.

[9] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[10] H.-M. Wang, X. Zhang, and J.-C. Jiang, "UAV-involved wireless physical-layer secure communications: Overview and research directions," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 32–39, 2019.

[11] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and Opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, 2019.

[12] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical layer security in space information networks: A survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2020.

[13] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a Quantum World," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 116–120, 2017.

[14] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[15] P. R. Geffe, "Secrecy systems approximating perfect and ideal secrecy," *Proceedings of the IEEE*, vol. 53, no. 9, pp. 1229–1230, 1965.

[16] M. Hellman, "An extension of the shannon theory approach to cryptography," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 289–294, 1977.

[17] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[18] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41–50, 2013.

[19] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type ldpc codes for the bec wiretap channel," *IEEE transactions on information theory*, vol. 59, no. 2, pp. 1048–1064, 2013.

[20] V. Rathi, R. Urbanke, M. Andersson, and M. Skoglund, "Rate-equivocation optimal spatially coupled ldpc codes for the bec wiretap channel," in *IEEE International Symposium on Information Theory Proceedings*, 2011, pp. 2393–2397.

[21] C. W. Wong, T. F. Wong, and J. M. Shea, "Secret-sharing ldpc codes for the bpsk-constrained gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 551–564, 2011.

[22] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[23] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.

[24] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of ldpc codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[25] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," in *IEEE International Symposium on Information Theory*. IEEE, 2010, pp. 2538–2542.

[26] M. Cheraghchi, F. Didier, and A. Shokrollahi, "Invertible extractors and wiretap protocols," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1254–1274, 2012.

[27] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Annual Cryptology Conference*. Springer, 2012, pp. 294–311.

[28] U. Maurer and S. Wolf, "Secret key agreement over a nonauthenticated channel-parts I-III: Definitions and bounds," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 822–831, 2003.

[29] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[30] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 205–215, 2011.

[31] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[32] M. J. Neely and E. Modiano, "Capacity and Delay Tradeoffs for Ad Hoc Mobile Networks," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1917–1937, 2005.

[33] R. Urgaonkar and M. J. Neely, "Network capacity region and minimum energy function for a delay-tolerant mobile ad hoc network," *IEEE/ACM Transactions on Networking*, vol. 19, no. 4, pp. 1137–1150, 2011.

[34] J. Liu, X. Jiang, H. Nishiyama, and N. Kato, "Delay and Capacity in Ad Hoc Mobile Networks with f-cast Relay Algorithms," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2738–2751, 2011.

[35] D. Ciullo, V. Martina, M. Garetto, and E. Leonardi, "Impact of correlated mobility on delay-throughput performance in mobile ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 6, pp. 1745–1758, 2011.

[36] P. Li, Y. Fang, J. Li, and X. Huang, "Smooth Trade-Offs between Throughput and Delay in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 3, pp. 427–438, 2012.

[37] S. R. Kulkarni and P. Viswanath, "A deterministic approach to throughput scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 50, no. 6, pp. 1041–1049, 2004.

[38] C. Zhang, Y. Fang, and X. Zhu, "Throughput-Delay Tradeoffs in Large-scale MANETs with Network Coding," in *IEEE INFOCOM*, 2009, pp. 199–207.

[39] P. C. Pinto, J. Barros, and M. Z. Win, "Secure Communication in Stochastic Wireless Networks - Part I: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125–138, 2012.

[40] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2764–2775, 2011.

[41] Y. Cai, X. Xu, and W. Yang, "Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise," *IET Communications*, vol. 10, no. 15, pp. 1904–1913, 2016.

[42] M. Grossglauser and D. N. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM transactions on networking*, vol. 10, no. 4, pp. 477–486, 2002.

[43] N. Lu and X. S. Shen, "Scaling laws for throughput capacity and delay in wireless networks - A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 2, pp. 642–657, 2014.

[44] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.

[45] J. Zhang, L. Fu, and X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," *IEEE/ACM Transactions on Networking*, vol. 22, no. 1, pp. 66–79, 2014.

[46] K. Zheng, J. Zhang, X. Liu, L. Fu, X. Wang, X. Jiang, and W. Zhang, "Secrecy Capacity Scaling of Large-Scale Networks With Social Relationships," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2688–2702, 2017.

[47] S. Vasudevan, D. Goeckel, and D. F. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proceedings of the eleventh ACM international symposium on Mobile ad hoc networking and computing*, 2010, pp. 21–30.

[48] Y. Liang, H. V. Poor, and L. Ying, "Secrecy Throughput of MANETs Under Passive and Active Attacks," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6692–6702, 2011.

[49] X. Cao, J. Zhang, L. Fu, W. Wu, and X. Wang, "Optimal Secrecy Capacity-Delay Tradeoff in Large-Scale Mobile Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, pp. 1139–1152, 2016.

[50] S. Shintre, L. Sassatelli, and J. Barros, "Generalized delay-secrecy-throughput trade-offs in mobile ad-hoc networks," in *APWC, IEEE-APS*, 2011, pp. 1424–1427.

[51] J. Gao, J. Liu, X. Jiang, O. Takahashi, and N. Shiratori, "Throughput Capacity of MANETs with Group-Based Scheduling and General Transmission Range," *IEICE Transactions on Communications*, vol. 96, no. 7, pp. 1791–1802, 2013.

[52] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.

[53] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2010.

[54] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

[55] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Workshop on Statistical Signal Processing*. IEEE, 2009, pp. 417–420.

[56] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 11, pp. 3980–3991, 2012.

[57] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in *IEEE International Symposium on Dynamic Spectrum Access Networks*, 2005, pp. 124–130.

[58] S. Park, L. E. Larson, and L. B. Milstein, "An RF receiver detection technique for cognitive radio coexistence," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 8, pp. 652–656, 2010.

[59] J. Zhu, Y. Chen, Y. Shen, O. Takahashi, X. Jiang, and N. Shiratori, "Secrecy transmission capacity in noisy wireless ad hoc networks," *Ad Hoc Networks*, vol. 21, pp. 123–133, 2014.

[60] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 62, no. 3, 2005, pp. 1906–1910.

[61] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Military Communications Conference*. IEEE, 2005, pp. 1501–1506.

[62] ——, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[63] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.

[64] A. El Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Optimal throughput-delay scaling in wireless networks: part I: the fluid model," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2568–2592, 2006.

[65] S. Toumpis and A. J. Goldsmith, "Large wireless networks under fading, mobility, and delay constraints," in *Proceedings of IEEE INFOCOM*, 2004.

[66] P. Li, Y. Fang, and J. Li, "Throughput, Delay, and Mobility in Wireless Ad Hoc Networks," in *Proceedings of IEEE INFOCOM*, 2010, pp. 1–9.

[67] M. Garetto, P. Giaccone, and E. Leonardi, "Capacity Scaling in Ad Hoc Networks With Heterogeneous Mobile Nodes: The Subcritical Regime," *IEEE/ACM Transactions on Networking*, vol. 17, no. 6, pp. 1888–1901, 2009.

[68] O. O. Koyluoglu, C. E. Kaksal, and H. E. Gamal, "On Secrecy Capacity Scaling in Wireless Networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.

[69] Y. Chen, Y. Shen, J. Zhu, X. Jiang, and H. Tokuda, "On the Throughput Capacity Study for Aloha Mobile Ad Hoc Networks," *IEEE Transactions on Communications*, vol. 64, no. 4, pp. 1646–1659, 2016.

[70] J. Liu, M. Sheng, Y. Xu, J. Li, and X. Jiang, "On throughput capacity for a class of buffer-limited MANETs," *Ad Hoc Networks*, vol. 37, pp. 354–367, 2016.

[71] X. Li, "C++ simulator for the exact secrecy throughput capacity study of MANETs," [Online]. Available: https://hyqc.blogspot.jp/, 2018.

[72] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.

[73] J. Mammen and D. Shah, "Throughput and delay in random wireless networks with restricted mobility," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1108–1116, 2007.

[74] X. Wang, W. Huang, S. Wang, J. Zhang, and C. Hu, "Delay and capacity tradeoff analysis for MotionCast," *IEEE/ACM Transactions on Networking*, vol. 19, no. 5, pp. 1354–1367, 2011.

[75] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*. John Wiley & Sons, 2013.

[76] M. Haenggi, R. K. Ganti *et al.*, "Interference in large wireless networks," *Foundations and Trends® in Networking*, vol. 3, no. 2, pp. 127–248, 2009.

[77] M. Haenggi, "On distances in uniformly random networks," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3584–3586, 2005.

[78] Z. Yazdanshenasan, H. S. Dhillon, M. Afshang, and P. H. Chong, "Poisson hole process: Theory and applications to wireless networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7531–7546, 2016.

[79] X. Li, "Java simulator for secrecy transmission capacity study of MANETs with secure aloha protocols," [Online]. Available: http://bit.ly/2HFe6D5, 2020.

# Publications

## Journal Articles

[1] Xiaochen Li, Shuangrui Zhao, Yuanyu Zhang, Yulong Shen and Xiaohong Jiang. Exact Secrecy Throughput Capacity Study in Mobile Ad Hoc Networks. *Ad Hoc Networks (Elsevier)*, 72: 105–114, 2018.

[2] Xiaochen Li, Yuanyu Zhang, Yulong Shen and Xiaohong Jiang. Secrecy Transmission Capacity in Mobile Ad Hoc Networks with Security-Aware Aloha Protocol. *IET Communications*. (In peer review)

## Conference Papers

[3] Xiaochen Li, Shuangrui Zhao, Yuanyu Zhang, Yulong Shen and Xiaohong Jiang. Exact Secrecy Throughput of MANETs with Guard Zone. International Conference on Networking and Network Applications (NaNA), Hakodate, Japan, July 2016.

[4] Shuangrui Zhao, Jia Liu, Xiaochen Li, Yulong Shen and Xiaohong Jiang. Secure Beamforming for Full-Duplex MIMO Two-Way Communication via Untrusted Relaying. IEEE Globecom Workshops (GC Workshops), Singapore, December 2017.

[5] Jiao Quan, Xiaochen Li, Yeqiu Xiao, Yulong Shen and Fenghua Li. Secure Transmission with Limited Feedback in MISOME Wiretap Channels. International Conference on Networking and Network Applications (NaNA), Kathmandu, Nepal, October 2017.