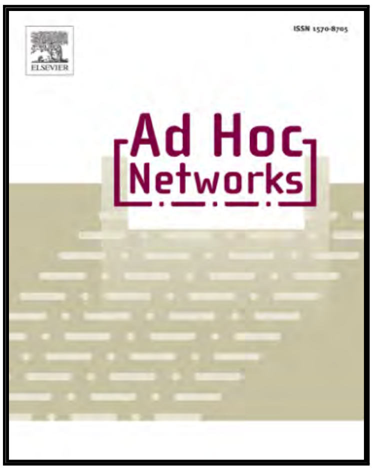


Exact Secrecy Throughput Capacity Study in Mobile Ad Hoc Networks

Xiaochen Li, Shuangrui Zhao, Yuanyu Zhang, Yulong Shen, Xiaohong Jiang

PII:	S1570-8705(18)30028-3
DOI:	10.1016/j.adhoc.2018.01.012
Reference:	ADHOC 1633

To appear in:	*Ad Hoc Networks*

Received date:	6 March 2017
Revised date:	5 January 2018
Accepted date:	30 January 2018

Exact Secrecy Throughput Capacity Study in Mobile Ad Hoc Networks

Xiaochen Li[a,b], Shuangrui Zhao[b], Yuanyu Zhang[c,*], Yulong Shen[b], Xiaohong Jiang[a]

[a]*School of Systems Information Science, Future University Hakodate, 116-2 Kamedanakano-cho, Hakodate, Hokkaido, 041-8655, Japan*
[b]*School of Computer Science and Technology, Xidian University, Xian, Shaanxi, 710071, China*
[c]*Graduate School of Information Science, Nara Institute of Science and Technology, Nara 630-0192, Japan*

Abstract

The secrecy throughput capacity (STC) performance study of mobile ad hoc networks (MANETs) is critical for supporting their applications in security-sensitive scenarios. Despite much work on the scaling law results of MANET STC, the *exact* STC study of such networks remains an open problem. This paper, for the first time, investigates the exact STC of a cell-partitioned MANET with group-based scheduling scheme from the physical layer (PHY) security perspective. We first propose two secure transmission schemes based on the PHY security technology, i.e., secrecy guard zone based and cooperative jamming based schemes. The secrecy guard zone based scheme allows transmissions to be conducted *only if* no eavesdroppers exist in the secrecy guard zone around transmitters. The cooperative jamming based scheme 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. We then derive exact analytical expressions for the STC performance of the concerned network under both secure transmission schemes based on the analysis of two basic secure transmission probabilities. Finally, extensive simulation and nu-

[*]Corresponding author. Tel.: 080-3266-6646
Email addresses: xchenli111@gmail.com (Xiaochen Li), srzhao@stu.xidian.edu.cn (Shuangrui Zhao), yyzhang@is.naist.jp (Yuanyu Zhang), ylshen@mail.xidian.edu.cn (Yulong Shen), jiang@fun.ac.jp (Xiaohong Jiang)

merical results are provided to corroborate our theoretical analysis and also to illustrate the STC performance of the concerned MANET.

Keywords: Mobile ad hoc networks, secrecy throughput capacity, physical layer security.

1. Introduction

As wireless communication technology evolves continuously, mobile ad hoc networks (MANETs) have been highly appealing for supporting lots of critical applications such as military battlefield, emergency rescue, disaster relief, etc. 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.

Traditionally, the security of wireless communications is guaranteed by cryptography, which relies on solving various computationally difficult problems (e.g., RSA problem [1], CDH problem [2], DLP problem [3]). Recently, another promising security approach, called physical layer (PHY) security [4–6], 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 have no enough computing power, they can hardly solve the difficult problems in the cryptography as of today. 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, they can conduct the quantum computing [7]), 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 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 to be a promising security mechanism for MANETs.

This paper focuses on the secrecy throughput capacity (STC) issue in MANETs, which is essentially equivalent to the fundamental and long-standing throughput capacity problem (see [8, 9] 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 STC study of wireless ad hoc network [10–16] (Please refer to Section 2 for related works). It is notable that these works focus on deriving the scaling law results, which are certainly important to characterize how the STC 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 [9], which reveals that exact STC results are more deserved and critical to facilitate the design, development and commercialization of MANETs. Unfortunately, such exact STC study for MANETs remains an open problem in the literature.

As the first step towards the exact study of STC for MANETs, this paper explores the exact STC of a cell-partitioned MANET [17, 18] with the group-based scheduling scheme [19–23]. The results in this paper are envisioned to inspire subsequent theoretical researches continuously devoted to the exact study of the fundamental and important MANET STC issue. 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 first consider a scenario where each transmitter can detect the existence of eavesdroppers in a region around itself, called secrecy guard zone [10, 24–26]. It is notable that the idea of secrecy guard zone has been widely adopted as a security-achieving approach in the study of other security metrics like the secrecy transmission capacity [24, 25] and secure connectivity [26], which differ, to a large extend, from the STC metric considered in this paper. We then consider a new scenario where each transmitter can know the exact locations of eavesdroppers in its transmission range [27]. Note that the above assumptions on the knowledge about the eavesdropper locations are reasonable, as a passive eavesdropper can be detected and located from the local oscillator power leaked from its RF front-end [28, 29]. Notice that this paper extends our previous study in [30] by introducing the second scenario and deriving the exact STC for this scenario. The main contributions of this paper are summarized as follows.

- For the first scenario, we propose a secrecy guard zone based secure transmission scheme, in which the transmission of a selected transmitter will be conducted only if no eavesdroppers exist in its secrecy guard zone. For the second scenario, we propose a cooperative jamming based secure transmission scheme, which 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.

- With the help of the theoretical framework for throughput capacity analysis of MANETs in [31], we derive exact analytical expressions for the STC of the concerned network under both scenarios, 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 and numerical results are provided to corroborate our theoretical analysis and also to illustrate the STC performance of the network.

The rest of the paper is organized as follows. In Section 2, we introduce the related work. In Section 3, we introduce the system model and the proposed secure transmission schemes. In Section 4, we study the exact STC for the first scenario. The exact STC for the second scenario is derived in Section 5. Simulation/numerical results and the corresponding discussions are provided in Section 6. Finally, we conclude this paper in Section 7.

2. Related Work

Some scaling law results on the network STC have been reported in [10–13] for static ad hoc networks and in [14–16] for MANETs. For the STC study in static ad hoc networks, the authors in [10] explored the STC 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 secrecy guard zone to guarantee secure transmissions of legitimate transmitters. In addition, the authors also investigated the STC of an arbitrary network with multiple legitimate nodes and eavesdroppers. The STC of a Poisson network was also studied in [11], while, different from [10], the authors assumed that the locations of eavesdroppers are unknown and each receiver has two extra antennas for generating artificial noise to suppress eavesdroppers. This work was later extended in [12] by introducing social relationships among legitimate network nodes. For a stochastic network with eavesdroppers of unknown location, the authors in [13] investigated the trade-off between the network throughput and the maximum number of eavesdroppers that can be tolerated by the network. Similar to [11] and [12], the authors in [13] adopted the artificial noise generation technique to improve security, while the difference is that the noise is generated from other helper nodes instead of extra antennas of receivers.

For the STC study in MANETs, the authors in [14] studied the scaling law results of delay-constrained STC 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 [14] showed that the presence of eavesdroppers has a significant impact on the network STC and in general the STC under active attack is less than the STC under passive attack. In [15], the scaling law result of delay-constrained MANET STC was also investigated, while the authors considered static and passive eavesdroppers, and adopted the artificial noise generation technique in [11] and [12] to suppress the eavesdroppers. The scaling law result of delay-constrained STC in MANETs with passive eavesdroppers under various routing policies such as Spray-and-Wait was examined in [16].

It is notable that the significant difference between the above works and this paper is that this paper derived the exact STC of MANETs while the above works focused on the STC scaling laws of static ad hoc networks [10–13] or MANETs [14–16]. In addition, the above works applied the technique of either secrecy guard zone [10] or artificial noise generation [11–13, 15] to provide security guarantee, while this paper adopted both.

3. System Model and Security Scheme

3.1. System Model

As shown in Figure 1, we consider a torus network with unit area [20, 21, 32], 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

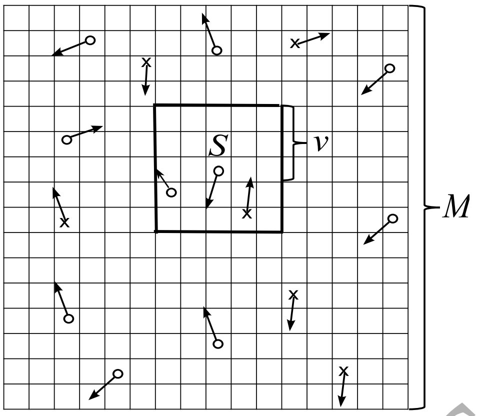


Figure 1: Illustration of a cell partitioned MANET: the circle represents legitimate node, the cross represents eavesdropper and the arrow represents the moving direction of nodes.

eavesdroppers) moves around in the network according to the independent and identically distributed (i.i.d.) mobility model [8, 17, 33]. 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 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 [34, 35], 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 λ (i.e., $E\{A_i(t)\} = \lambda$) and a bounded second moment A^2_{max} (i.e., $E\{A^2_i(t)\} \leq A^2_{max} < \infty$), where $E\{\}$ is the expectation operator. This represents that all source nodes have the same average packet input rate λ packets/slot. To coordinate the simultaneous transmission of source nodes, we adopt the widely-used group-based scheduling scheme [19–23]. This scheme divides all the network cells into α^2 groups with each group consisting of $K = \lfloor M^2/\alpha^2 \rfloor$ cells and becoming active (i.e., allowed to transmit packets) alternately in every α^2 time slots. As shown in Figure

2, the distance between any two horizontally (or vertically) adjacent cells in the same group is of α cells, and α is given by

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

where $\lceil . \rceil$ is the ceiling function and Δ 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 paper.

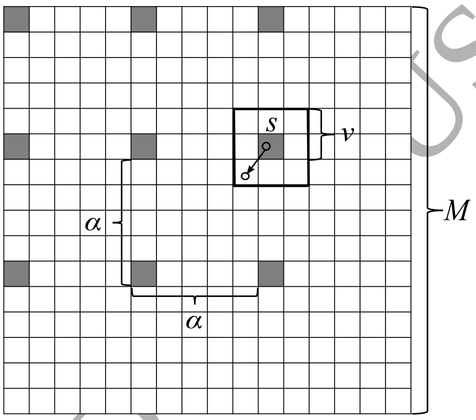
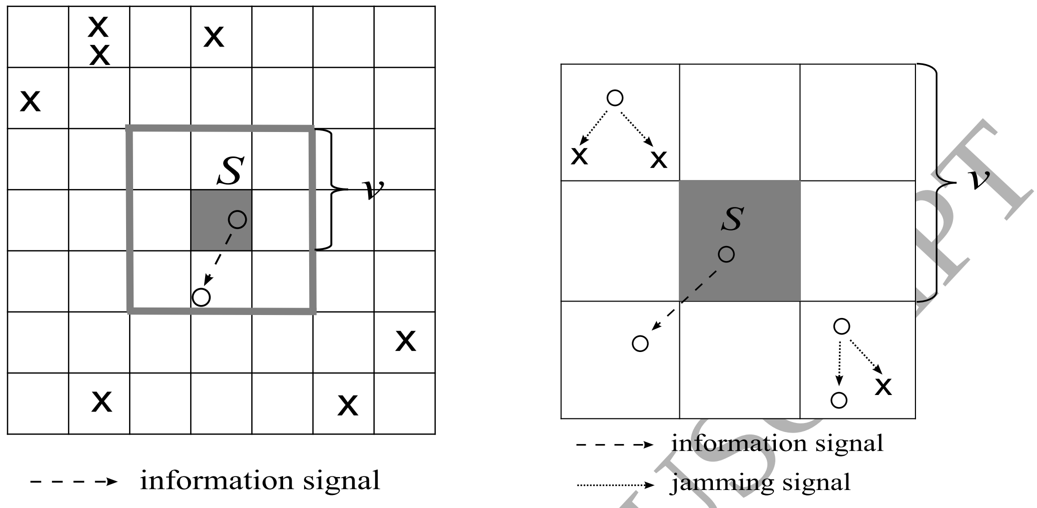


Figure 2: Group-based scheduling.

3.2. Secure Transmission Schemes

We consider two scenarios in this paper regarding the knowledge of legitimate nodes about the eavesdroppers. In the first scenario, we assume that each transmitter can detect the existence of eavesdroppers in a region around itself, called secrecy guard zone [10, 24–26]. As shown in Figure 3(a), we model the secrecy guard zone of a transmitter (say S) as a square region with g cells centered at the cell containing S. We refer to this scenario as Scenario 1. In the second scenario, we assume that each transmitter can know the exact location of each eavesdropper in its transmission range. We refer to this scenario as Scenario 2.

To ensure secure transmission in the above two scenarios, we propose two security schemes. For Scenario 1, we propose a secrecy guard zone based secure transmission scheme, in which the transmission of a selected transmitter



(a) Secrecy guard zone based scheme

(b) Cooperative jamming based scheme

Figure 3: Secure transmission schemes.

can be conducted only if no eavesdroppers exist in the secrecy guard zone, and suspended otherwise. For Scenario 2, we propose a cooperative jamming based secure transmission scheme [36, 37], 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. 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. Secrecy Throughput Capacity for Scenario 1

In this section, we derive the exact STC for Scenario 1. Similar to [38, 39] the word exact is used to emphasize that the results derived in this paper 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 STC as follows.

Secrecy Throughput Capacity: Consider a cell-partitioned MANET under the group-based scheduling and the proposed secure transmission schemes, the secrecy throughput capacity (STC) is defined as the maximum input rate λ (packets/slot) that the network can support *stably* and *securely.* The term *stably* means that for a given input rate λ, 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 schemes.

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

4.1. STC Analysis Framework

The STC analysis in this paper is based on the theoretical framework in [31]. Following this framework, we first need to derive an upper bound μ on the STC, 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 μ 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 μ. 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

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

or equivalently

$$\lambda \leq \frac{K\left(p_0+p_1\right)}{2n}+\frac{\epsilon}{n}. \tag{3}$$

When ϵ is arbitrarily small, we can derive the upper bound μ as

$$\mu = \frac{K\left(p_0+p_1\right)}{2n}. \tag{4}$$

Next, we prove that for any input rate $\lambda < \mu$, the average packet delay $\overline{D}$ of the network is bounded. According to [31], with probabilities p_0 and p_1, we can bound the average packet delay $\overline{D}$ as

$$\overline{D} \leq \frac{B_0}{B_1(1-\rho)\lambda\mu}, \tag{5}$$

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

$$B_0 = (nA_{max}^2 + K - 2K\lambda)(p_0^2 - p_1^2) + 2n\mu(p_0 + np_1 - p_1), \tag{6}$$

and

$$B_1 = 4(p_0 + np_1 - p_1)(p_0 - p_1). \tag{7}$$

Therefore, according to the above, the upper bound μ is the exact STC.

4.2. Exact STC Result

We present the following theorem regarding the exact STC result for Scenario 1.

Theorem 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 secrecy guard zone based secure transmission scheme is utilized to ensure secure transmissions, the exact STC μ of the network is given by*

$$\begin{aligned}\mu = \frac{\lfloor M^2/\alpha^2 \rfloor}{2nM^{2n}}\left(1-\frac{g}{M^2}\right)^m \Big[& 2M^{2n} - (M^2-1)^n \\ & - n(M^2-\beta)^{n-1} - (M^4 - 2\beta + 1)^{\frac{n}{2}}\Big],\end{aligned} \tag{8}$$

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

Proof. According to the framework in Section 4.1, we only need to derive p_0 and p_1 to obtain the STC. 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 secrecy guard zone 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 [31], we have

$$\hat{p_0} = \frac{1}{M^{2n}}\Big[M^{2n} - (M^2-1)^n - n(M^2-\beta)^{n-1}\Big]. \tag{9}$$

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

$$p_0 = \frac{1}{M^{2n}}\Big(1-\frac{g}{M^2}\Big)^m\Big[M^{2n} - (M^2-1)^n - n(M^2-\beta)^{n-1}\Big]. \tag{10}$$

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 [31], we have

$$\hat{p_1} = \frac{1}{M^{2n}}\Big[M^{2n} - (M^4-2\beta+1)^{\frac{n}{2}}\Big]. \tag{11}$$

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

$$p_1 = \frac{1}{M^{2n}}\Big(1-\frac{g}{M^2}\Big)^m\Big[M^{2n} - (M^4-2\beta+1)^{\frac{n}{2}}\Big]. \tag{12}$$

After deriving p_0 and p_1, the exact STC in (8) for Scenario 1 then follows according to (4). □

5. Secrecy Throughput Capacity for Scenario 2

In this section, we derive the exact STC for Scenario 2. Similarly, we only need to determine the corresponding probabilities p_0 and p_1, which are given in the following lemma.

Lemma 1. *For the concerned cell-partitioned MANET with the secure transmission scheme for Scenario 2, 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*

$$p_0 = \Psi_2(0)\Omega_2(0) + \Psi_1(\beta)\Omega_1(\beta) + \sum_{k=1}^{\beta-1}\Big[\Psi_1(k)\Omega_1(k) + \Psi_2(k)\Omega_2(k)\Big]. \tag{13}$$

$$\Psi_1(k) = \sum_{j=k}^{m} \frac{C_{\beta-1}^{k-1} S(j,k)k!}{\beta^j} C_m^j \left(\frac{\beta}{M^2}\right)^j \left(1-\frac{\beta}{M^2}\right)^{m-j}, \tag{14}$$

$$\Omega_1(k) = \sum_{i=k+2}^{n} \sum_{l=k+1}^{i-1} \frac{\left[C_i^l S(l,k)k! - C_i^1 C_{i-1}^{l-1} S(l-1,k-1)(k-1)!\right] \cdot (\beta-k)^{i-l}}{\beta^i} \cdot C_n^i \left(\frac{\beta}{M^2}\right)^i \left(1-\frac{\beta}{M^2}\right)^{n-i}, \tag{15}$$

$$\Psi_2(k) = \sum_{j=k}^{m} \frac{C_{\beta-1}^{k} S(j,k)k!}{\beta^j} C_m^j \left(\frac{\beta}{M^2}\right)^j \left(1-\frac{\beta}{M^2}\right)^{m-j}, \tag{16}$$

$$\Omega_2(k) = \sum_{i=k+2}^{n} \sum_{l=k}^{i-2} \sum_{d=1}^{i-l} \frac{\left[C_i^l S(l,k)k!\right] C_{i-l}^d (\beta-k-1)^{i-l-d}}{\beta^i} \cdot C_n^i \left(\frac{\beta}{M^2}\right)^i \left(1-\frac{\beta}{M^2}\right)^{n-i}. \tag{17}$$

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

$$C_m^j \left(\frac{\beta}{M^2}\right)^j \left(1-\frac{\beta}{M^2}\right)^{m-j}. \tag{18}$$

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

$$\frac{C_{\beta-1}^{k-1} S(j,k)k!}{\beta^j}, \tag{19}$$

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 (14).

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

$$C_n^i \left(\frac{\beta}{M^2}\right)^i \left(1 - \frac{\beta}{M^2}\right)^{n-i}. \tag{20}$$

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

$$\sum_{l=k+1}^{i-1} \frac{\underbrace{\left[C_i^l S(l,k)k! - C_i^1 C_{i-1}^{l-1} S(l-1,k-1)(k-1)!\right]}_{Q} \cdot (\beta - k)^{i-l}}{\beta^i}, \tag{21}$$

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 (15).

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

$$\sum_{k=1}^{\beta} \Psi_1(k)\Omega_1(k). \tag{22}$$

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 (16).

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 (17).

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

$$\sum_{k=0}^{\beta-1} \Psi_2(k)\Omega_2(k). \tag{23}$$

Finally, combining the results in (22) and (23) yields the p_0 in (13). □

Lemma 2. *For the concerned cell-partitioned MANET with the secure transmission scheme for Scenario 2, 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*

$$p_1 = \Psi_2(0)\Phi_2(0) + \Psi_1(\beta)\Phi_1(\beta) + \sum_{k=1}^{\beta-1} \Big[\Psi_1(k)\Phi_1(k) + \Psi_2(k)\Phi_2(k)\Big]. \tag{24}$$

Proof. 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

$$\begin{aligned}\Phi_1(k) = &\sum_{i=k+2}^{n}\sum_{t=1}^{\left\lfloor \frac{i}{2}\right\rfloor}\sum_{l=k+1}^{i-1}\sum_{t_1=1}^{min\{t,l-k+1\}}\sum_{t_2=0}^{\left\lfloor \frac{l-t_1}{2}\right\rfloor}\sum_{t_3=0}^{l-t_1-2t_2}\sum_{s=0,s+t_1\geq 2}^{l-t_1-k+1}\\ &\cdot\frac{C_{l-t_1-t_3}^{s}S\left(l-s-t_1,k-1\right)(k-1)!\left(\beta-k\right)^{i-l}}{\beta^i}C_t^{t_1}2^{t_1}C_{t-t_1}^{t_2}\\ &\cdot C_{t-t_1-t_2}^{t_3}2^{t_3}C_{i-2t}^{l-t_1-2t_2-t_3}C_{\frac{n}{2}}^{t}C_{\frac{n}{2}-t}^{i-2t}2^{i-2t}\left(\frac{\beta}{M^2}\right)^i\left(1-\frac{\beta}{M^2}\right)^{n-i}, \qquad (25)\end{aligned}$$

$$\begin{aligned}\Phi_2(k) = &\sum_{i=k+2}^{n}\sum_{t=1}^{\left\lfloor \frac{i}{2}\right\rfloor}\sum_{l=k}^{i-2}\sum_{t_4=1}^{min\left\{t,\left\lfloor \frac{i-l}{2}\right\rfloor\right\}}\sum_{t_5=0}^{i-l-2t_4}\sum_{t_6=1}^{t_4}\frac{S(l,k)k!C_{t_4}^{t_6}\left[1+2\left(\beta-k-1\right)\right]^{t_6}}{\beta^i}\\ &\cdot\left(\beta-k-1\right)^{2(t_4-t_6)}\left(\beta-k\right)^{i-l-2t_4}C_t^{t_4}C_{t-t_4}^{t_5}2^{t_5}C_{i-2t}^{i-l-2t_4-t_5}\\ &\cdot C_{\frac{n}{2}}^{t}C_{\frac{n}{2}-t}^{i-2t}2^{i-2t}\left(\frac{\beta}{M^2}\right)^i\left(1-\frac{\beta}{M^2}\right)^{n-i}. \qquad (26)\end{aligned}$$

---

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

$$C_{\frac{n}{2}}^{t}C_{\frac{n}{2}-t}^{i-2t}2^{i-2t}\left(\frac{\beta}{M^2}\right)^i\left(1-\frac{\beta}{M^2}\right)^{n-i}. \qquad (27)$$

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

$$\frac{\displaystyle\sum_{l=k+1}^{i-1} \sum_{t_1=1}^{min\{t,l-k+1\}} \sum_{t_2=0}^{\left\lfloor \frac{l-t_1}{2} \right\rfloor} \sum_{t_3=0}^{l-t_1-2t_2} \sum_{s=0,s+t_1\geq 2}^{l-t_1-k+1} C_{l-t_1-t_3}^{s} \underbrace{S\left(l-s-t_1, k-1\right)\left(k-1\right)!}_{Y} \left(\beta-k\right)^{i-l}}{\beta^i} \cdot C_t^{t_1} 2^{t_1} C_{t-t_1}^{t_2} C_{t-t_1-t_2}^{t_3} 2^{t_3} C_{i-2t}^{l-t_1-2t_2-t_3}, \tag{28}$$

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 (25). We then apply the law of total probability in terms of A_k to determine the probability p_1 in the first case as

$$\sum_{k=1}^{\beta} \Psi_1(k)\Phi_1(k). \tag{29}$$

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 (26). Applying the law of total probability in terms of A_k, we determine the probability p_1 in the second case as

$$\sum_{k=0}^{\beta-1} \Psi_2(k)\Phi_2(k). \tag{30}$$

Finally, combining the results in (29) and (30) yields the p_1 in (24). □

Based on p_0 and p_1, we can give the exact STC for the concerned network under Scenario 2 in the following theorem.

Theorem 2. *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 cooperative jamming security scheme is utilized to ensure secure transmissions, the exact STC μ of the concerned MANET under Scenario 2 is given by*

$$\begin{aligned}\mu =& \frac{\lfloor M^2/\alpha^2 \rfloor}{2n}\Bigg\{\Psi_2(0)\Omega_2(0) + \Psi_1(\beta)\Omega_1(\beta) + \Psi_2(0)\Phi_2(0) + \Psi_1(\beta)\Phi_1(\beta) \\ &+ \sum_{k=1}^{\beta-1}\Big[\Psi_1(k)\Omega_1(k) + \Psi_2(k)\Omega_2(k) + \Psi_1(k)\Phi_1(k) + \Psi_2(k)\Phi_2(k)\Big]\Bigg\},\end{aligned} \tag{31}$$

where Ψ_1, Ψ_2 are given by (14) and (16), Ω_1, Ω_2 are given by (15) and (17), and Φ_1, Φ_2 are given by (25) and (26), respectively.

Proof. The theorem directly follows from (4) and Lemma 1 and 2. □

Remark 1. The results in this paper are computed for relatively non-practical models, which makes them not of significant practical values. Although these results fail to reflect the actual STC performances of networks in the real world, they may still be able to provide us some insights on the fundamental trends of system STC 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 [40, 41] for network throughput study, [14–16, 24] for network secrecy throughput study.

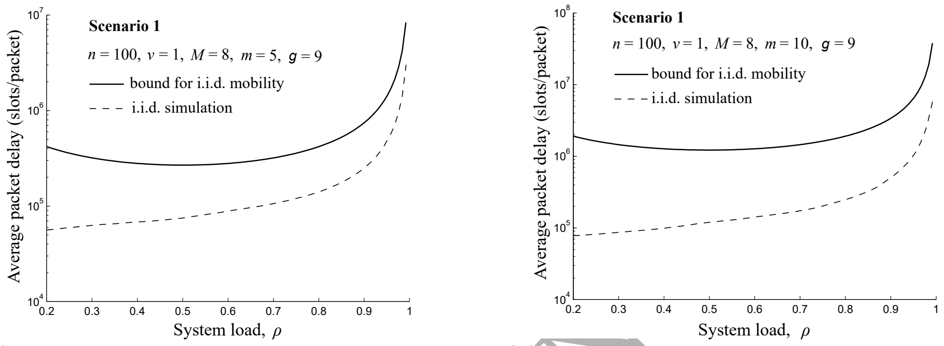
6. Numerical Results and Discussions

In this section, we first provide simulation results to validate our theoretical analysis for the STC performance of the concerned network under both scenarios. We then explore how the STC performance varies with the parameters of the proposed secrecy guard zone and cooperative jamming based secure transmission schemes.

6.1. Model Validation

To validate our STC analysis, a dedicated C++ simulator was developed to simulate the packet delivery process in the concerned MANET under the proposed secure transmission schemes, which is now available at [42]. According to STC framework in Section 4.1, we conduct extensive simulations to calculate the simulated results of the average packet delay for our STC analysis validation. Similar to [42], in each 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 each 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 Scenario 1, v is fixed as $v = 1$ and hence α is determined as $\alpha = 4$. 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 4. We can see from Figure 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 (5) under both network scenarios, which implies that the network is always stable whenever $\lambda < \mu$. Another observation from Figure 4 indicates that when the system load ρ approaches 1, i.e., the input rate λ is infinitely close to the STC μ, the expected packet delay increases drastically. According to the framework in Section 4.1, these two behaviors indicate that our theoretical STC result for Scenario 1 is efficient to exactly model the network STC performance of the concerned network.



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

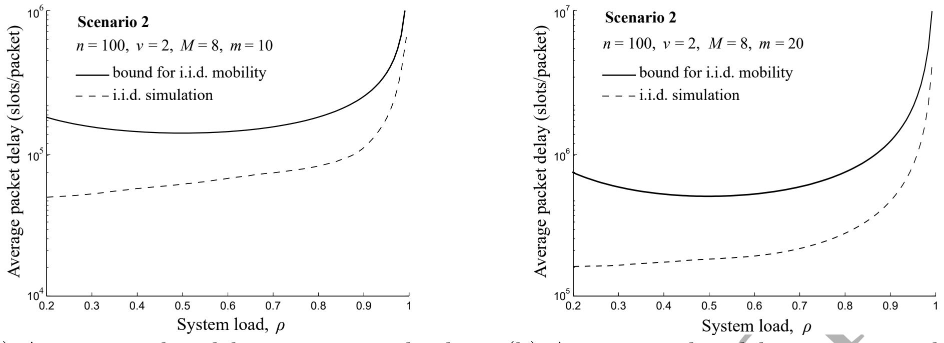
(b) Average packet delay vs. system load under network scenario of $n = 100$, $v = 1$, $M = 8$, $m = 10$, $g = 9$.

Figure 4: Model Validation for Scenario 1.

For Scenario 2, we set $v = 2$ (hence $\alpha = 8$) 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 5. Similar behaviors of the average packet delay versus the system load ρ can be observed from Figure 5, which indicates that our theoretical STC result for Scenario 2 is also efficient to exactly model the network STC performance of the concerned network.

6.2. Performance Discussion

With the help of our theoretical results, we now explore how the STC μ varies with the network parameters. We first focus on Scenario 1 and examine the impacts of the number of eavesdroppers m and the secrecy guard zone size g upon the STC μ. For the fixed setting of $(n = 100, M = 8, v = 1)$, we show in Figure 6 the relationship between μ and m under three different settings of $g = 1$, $g = 9$ and $g = 25$. We can see from Figure 6 that as m increases, the STC μ decreases in Scenario 1. This is intuitive since as



(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 5: Model Validation for Scenario 2.

more eavesdroppers are located in the network, the probability that there exist eavesdroppers within the secrecy guard zone of an active transmitter increases, resulting in decreased secure transmission probabilities p_0 and p_1. It can also be seen from Figure 6 that a larger secrecy guard zone leads to a decreased STC, which is because that as the secrecy guard zone size increases, more eavesdroppers will appear in the secrecy guard zone and thus the secure transmission probabilities p_0 and p_1 will decrease.

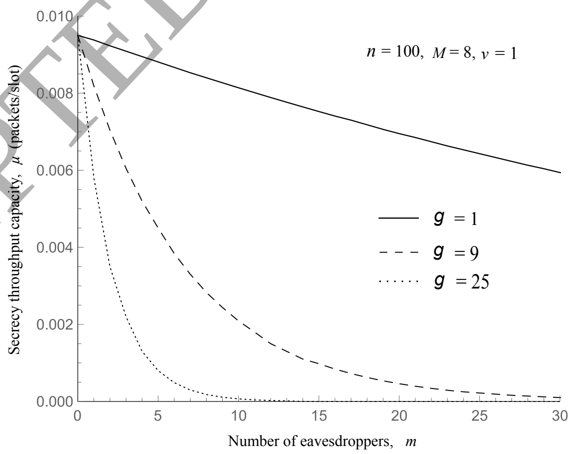


Figure 6: Secrecy throughput capacity μ vs. the number of eavesdroppers m for varying secrecy guard zone size g under Scenario 1.

We then focus on Scenario 2 and investigate the impacts of the number of eavesdroppers m and the side-length of transmission range v on the STC μ. For the fixed setting of $n = 100$ and $M = 8$, Figure 7 illustrates how μ varies with m under three different sizes of transmission range, i.e., $v = 2$, $v = 3$ and $v = 4$. We can observe from Figure 7 that the STC 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 7 shows that, μ 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.

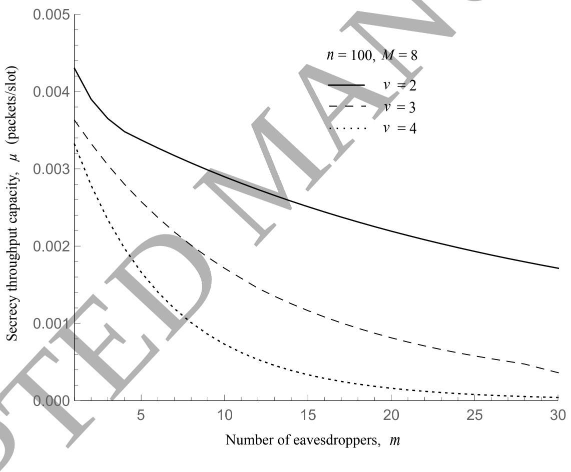


Figure 7: Secrecy throughput capacity μ vs. the number of eavesdroppers m for varying v under Scenario 2.

Finally, we compare the secrecy guard zone based security scheme for Scenario 1 with the cooperative jamming based security scheme for Scenario 2 in terms of the STC μ. To make these two schemes comparable, we set the size of secrecy guard zone in Scenario 1 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 8 how the μ varies with m under both schemes. We can see from Figure 8 that under the setting of $g = (2v-1)^2$, the cooperative jamming based security scheme can achieve a larger STC μ than the secrecy guard zone based security scheme. This is because that for $g = (2v-1)^2$ if there exists eavesdroppers in the secrecy guard zone (i.e., transmission range), the secrecy guard zone based scheme cannot provide secure transmission opportunities, while the cooperative jamming based scheme may still be able to ensure secure transmissions by suppressing these eavesdroppers.

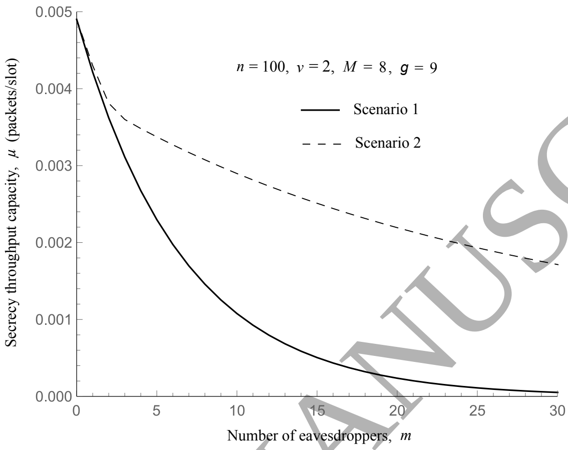


Figure 8: Secrecy guard zone based security scheme vs. cooperative jamming based security scheme with guard zone size $g = (2v-1)^2$.

7. Conclusion

This paper studied the exact secrecy throughput capacity (STC) of a cell-partitioned MANET with the group-based scheduling scheme. We first proposed two secure transmission schemes based on the physical layer security technology, i.e., secrecy guard zone and cooperative jamming based schemes, respectively and then provided analytical expressions for the exact STC of the concerned MANET under both secure transmission schemes. Finally, we provide simulation and numerical results to illustrate the efficiency of our STC analysis as well the STC performance of the network. The results in this paper showed that the cooperative jamming based scheme outperforms the secrecy guard zone based scheme with respect to the STC performance when the secrecy guard zone is equivalent to the transmission range. The theoretical framework (exact capacity) in this paper is developed for the group-based scheduling schemes, so one possible future work is to study the STC under more flexible time sharing schemes. Since this paper considered a non-practical model, another interesting and also important research direction is to study the exact STC under some relatively practical network models. Also, performing experiments or simulations in real-world networks or on testbeds will be a possible research direction to obtain STC results of practical significance.

References

[1] D. Aggarwal, U. Maurer, Breaking RSA Generically Is Equivalent to Factoring, IEEE Trans. Inf. Theory 62 (11) (2016) 6251–6259.

[2] F. Bao, R. Deng, H. Zhu, Variations of Diffie-Hellman Problem, in: ICICS, 2003, pp. 301–312.

[3] D. Adrian, K. Bhargavan, Z. Durumeric, et al., Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, in: ACM CCS, 2015, pp. 5–17.

[4] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, H.-H. Chen, Physical layer security in wireless networks: A tutorial, IEEE Wireless Commun. 18 (2) (2011) 66–74.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, A. L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surveys Tuts. 16 (3) (2014) 1550–1573.

[6] Y.-W. P. Hong, P.-C. Lan, C.-C. J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Proc. Mag. 30 (5) (2013) 29–40.

[7] C. Cheng, R. Lu, A. Petzoldt, T. Takagi, Securing the Internet of Things in a Quantum World, IEEE Commun. Mag. 55 (2) (2017) 116–120.

[8] M. Grossglauser, D. N. C. Tse, Mobility increases the capacity of ad-hoc wireless networks, IEEE/ACM Trans. Netw. 10 (4) (2002) 477–486.

[9] N. Lu, X. S. Shen, Scaling laws for throughput capacity and delay in wireless networks - A survey, IEEE Commun. Surveys Tuts. 16 (2) (2014) 642–657.

[10] O. O. Koyluoglu, C. E. Kaksal, H. E. Gamal, On Secrecy Capacity Scaling in Wireless Networks, IEEE Trans. Inf. Theory 58 (5) (2012) 3000–3015.

[11] J. Zhang, L. Fu, X. Wang, Asymptotic analysis on secrecy capacity in large-scale wireless networks, IEEE/ACM Trans. Netw. 22 (1) (2014) 66–79.

[12] K. Zheng, J. Zhang, X. Liu, L. Fu, X. Wang, X. Jiang, W. Zhang, Secrecy Capacity Scaling of Large-Scale Networks With Social Relationships, IEEE Trans. Veh. Technol. 66 (3) (2017) 2688–2702.

[13] S. Vasudevan, D. Goeckel, D. F. Towsley, Security-capacity trade-off in large wireless networks using keyless secrecy, in: Proc. ACM Int. Symp. Mobile Ad Hoc Networking and Computing, 2010, pp. 21–30.

[14] Y. Liang, H. V. Poor, L. Ying, Secrecy Throughput of MANETs Under Passive and Active Attacks, IEEE Trans. Inf. Theory 57 (10) (2011) 6692–6702.

[15] X. Cao, J. Zhang, L. Fu, W. Wu, X. Wang, Optimal Secrecy Capacity-Delay Tradeoff in Large-Scale Mobile Ad Hoc Networks, IEEE/ACM Trans. Netw. 24 (2) (2016) 1139–1152.

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

[17] M. J. Neely, E. Modiano, Capacity and Delay Tradeoffs for Ad Hoc Mobile Networks, IEEE Trans. Inf. Theory 51 (6) (2005) 1917–1937.

[18] R. Urgaonkar, M. J. Neely, Network capacity region and minimum energy function for a delay-tolerant mobile ad hoc network, IEEE/ACM Trans. Netw. 19 (4) (2011) 1137–1150.

[19] J. Liu, X. Jiang, H. Nishiyama, N. Kato, Delay and Capacity in Ad Hoc Mobile Networks with f-cast Relay Algorithms, IEEE Trans. Wirel. Commun. 10 (8) (2011) 2738–2751.

[20] D. Ciullo, V. Martina, M. Garetto, E. Leonardi, Impact of correlated mobility on delay-throughput performance in mobile ad hoc networks, IEEE/ACM Trans. Netw. 19 (6) (2011) 1745–1758.

[21] P. Li, Y. Fang, J. Li, X. Huang, Smooth Trade-Offs between Throughput and Delay in Mobile Ad Hoc Networks, IEEE Trans. Mob. Comput. 11 (3) (2012) 427–438.

[22] S. R. Kulkarni, P. Viswanath, A deterministic approach to throughput scaling in wireless networks, IEEE Trans. Inf. Theory 50 (6) (2004) 1041–1049.

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

[24] X. Zhou, R. K. Ganti, J. G. Andrews, A. Hjorungnes, On the throughput cost of physical layer security in decentralized wireless networks, IEEE Trans. Wireless Commun. 10 (8) (2011) 2764–2775.

[25] Y. Cai, X. Xu, W. Yang, Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise, IET Commun. 10 (15) (2016) 1904–1913.

[26] P. C. Pinto, J. Barros, M. Z. Win, Secure Communication in Stochastic Wireless Networks - Part I: Connectivity, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 125–138.

[27] W. Saad, X. Zhou, B. Maham, T. Basar, H. V. Poor, Tree formation with physical layer security considerations in wireless multi-hop networks, IEEE Trans. Wireless Commun. 11 (11) (2012) 3980–3991.

[28] B. Wild, K. Ramchandran, Detecting primary receivers for cognitive radio applications, in: Proc. IEEE Int. Symp. DySPAN, 2005, pp. 124–130.

[29] S. Park, L. E. Larson, L. B. Milstein, An RF receiver detection technique for cognitive radio coexistence, IEEE Trans. Circuits Syst. II Express Briefs 57 (8) (2010) 652–656.

[30] X. Li, S. Zhao, Y. Zhang, Y. Shen, X. Jiang, Exact Secrecy Throughput of MANETs with Guard Zone, in: International Conference on Networking and Network Applications, 2016, pp. 167–172.

[31] J. Gao, J. Liu, X. Jiang, O. Takahashi, N. Shiratori, Throughput Capacity of MANETs with Group-Based Scheduling and General Transmission Range, IEICE Trans. Commun. 96 (7) (2013) 1791–1802.

[32] A. El Gamal, J. Mammen, B. Prabhakar, D. Shah, Optimal throughput-delay scaling in wireless networks: part I: the fluid model, IEEE/ACM Trans. Netw. 14 (SI) (2006) 2568–2592.

[33] S. Toumpis, A. J. Goldsmith, Large wireless networks under fading, mobility, and delay constraints, in: IEEE Proc. INFOCOM, 2004.

[34] P. Li, Y. Fang, J. Li, Throughput, Delay, and Mobility in Wireless Ad Hoc Networks, in: IEEE Proc. INFOCOM, 2010, pp. 1–9.

[35] M. Garetto, P. Giaccone, E. Leonardi, Capacity Scaling in Ad Hoc Networks With Heterogeneous Mobile Nodes: The Subcritical Regime, IEEE/ACM Trans. Netw. 17 (6) (2009) 1888–1901.

[36] G. Zheng, L. Choo, K. Wong, Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays, IEEE Trans. Signal Process. 59 (3) (2011) 1317–1322.

[37] L. Dong, Z. Han, A. Petropulu, H. Poor, Cooperative jamming for wireless physical layer security, in: Proc. 15th IEEE Workshop on Statistical Signal Processing, 2009, pp. 417–420.

[38] Y. Chen, Y. Shen, J. Zhu, X. Jiang, H. Tokuda, On the Throughput Capacity Study for Aloha Mobile Ad Hoc Networks, IEEE Trans. Commun. 64 (4) (2016) 1646–1659.

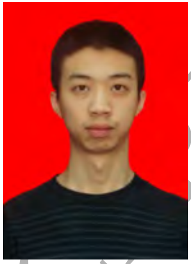
[39] J. Liu, M. Sheng, Y. Xu, J. Li, X. Jiang, On throughput capacity for a class of buffer-limited MANETs, Ad Hoc Networks 37 (2016) 354–367.

[40] J. Mammen, D. Shah, Throughput and delay in random wireless networks with restricted mobility, IEEE Trans. Inf. Theory 53 (3) (2007) 1108–1116.

[41] X. Wang, W. Huang, S. Wang, J. Zhang, C. Hu, Delay and capacity tradeoff analysis for MotionCast, IEEE/ACM Trans. Netw. 19 (5) (2011) 1354–1367.

[42] C++ simulator for the exact STC study of MANETs, [Online]. Available: https://hyqc.blogspot.jp/.

Xiaochen Li received her B.S. degree in Computer Science from Henan University of Science and Technology in 2015. She is currently working towards a M.S. degree at the school of Computer Science and Technology, Xidian University. Her research interests include wireless network security and MANET performance modeling.



Shuangrui Zhao received his B.S. degree in Mathematics from Xidian University in 2015. He is currently working towards a Ph.D. degree at the school of Computer Science and Technology, Xidian University. His research interests include physical layer security and performance evaluation of MIMO systems.

Yuanyu Zhang received his B.S. degree in Software Engineering from Xidian University in 2011 and M.S. degrees in Computer Science from Xidian University in 2014. He is currently working towards a Ph.D. degree at the School of Systems Information Science at Future University Hakodate. His research interests include the physical layer security of wireless communications, and performance modeling and evaluation of wireless networks.

Yulong Shen received the B.S. and M.S. degrees in Computer Science and Ph.D. degree in Cryptography from Xidian University, Xian, China, in 2002, 2005, and 2008, respectively. He is currently a Professor at the School of Computer Science and Technology, Xidian University, China. He is also an associate director of the Shaanxi Key Laboratory of Network and System Security and a member of the State Key Laboratory of Integrated Services networks Xidian University, China. He has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS and SOWN. His research interests include Wireless network security and cloud computing security.

Dr.Xiaohong Jiang received his B.S., M.S. and Ph.D degrees in 1989, 1992, and 1999 respectively, all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. Before joining Future University, Dr. Jiang was an Associate professor, Tohoku University, from Feb.2005 to Mar.2010. Dr. Jiangs research interests include computer communications networks, mainly wireless networks and optical networks, network security, routers/switches design, etc. He has published over 260 technical papers at premium international journals and conferences, which include over 50 papers published in top IEEE journals and top IEEE conferences, like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, IEEE Transactions on Parallel and Distributed Systems, IEEE INFOCOM. Dr. Jiang was the winner of the Best Paper Award of IEEE HPCC 2014, IEEE WCNC 2012, IEEE WCNC 2008, IEEE ICC 2005-Optical Networking Symposium, and IEEE/IEICE HPSR 2002. He is a Senior Member of IEEE, a Member of ACM and IEICE.