Exact Secrecy Throughput of MANETs with Guard Zone

Xiaochen Li*, Shuangrui Zhao*, Yuanyu Zhang†, Yulong Shen* and Xiaohong Jiang†
*School of Computer Science and Technology, Xidian University, China
†School of Systems Information Science, Future University Hakodate, Japan
Email: Xiaochenli111@163.com, srzhao@stu.xidian.edu.cn, yy90zhang@gmail.com,
ylshen@mail.xidian.edu.cn, jiang@fun.ac.jp

***Abstract*—Different from previous works that mainly focus on deriving the scaling results for secrecy throughput of mobile ad hoc networks (MANETs), this paper studies the exact secrecy throughput of a cell-partitioned MANET with group-based scheduling to eliminate interference from simultaneous transmissions. The concept of secrecy guard zone is introduced to allow each transmitter detect the existence of eavesdroppers in a region around itself. To ensure the transmission security, an on-off transmission scheme is adopted, where the transmission will be conducted (on) if no eavesdroppers exist in the secrecy guard zone around the transmitter, otherwise the transmission will be suspended (off). To derive the exact secrecy throughput, we first compute the probability that a transmission can be securely conducted between a given active cell and the cells in the transmission range of this cell (i.e., coverage cells) and also the probability that a source-destination transmission can be securely conducted between the active cell and its coverage cells. With the help of these two probabilities, we then derive the exact secrecy throughput as well as the upper bound on the delay of the concerned MANET. Finally, extensive simulation and numerical results are provided to corroborate our theoretical analysis and also to illustrate the performances of secrecy throughput and delay.**

Keywords-mobile ad hoc networks, secrecy throughput capacity, delay, physical layer security

I. Introduction

As the wireless communication technology evolves continuously, the 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, posing a great threat to the security of MANET.

Traditionally, the security of wireless communications is guaranteed by cryptography, which uses secret keys to encrypt/decrypt the original information based on various kinds of cryptographic protocols. In cryptography, eavesdroppers are assumed to have limited computing power such that no information can be extracted from the captured ciphertext by eavesdroppers without the secret keys. However, this assumption is now challenged by the rapid advance of computing power of eavesdroppers. In addition, the difficulty of implementing secret key management and distribution without centralized control may limit the application of cryptography-based methods in highly dynamic MANETs. As an alternative, the concept of physical layer (PHY) security has been introduced recently to provide a strong form of security guarantee by exploiting the inherent physical layer properties of the communication system, such as thermal noise, interference, and the time-varying nature of fading channels. Compared to cryptography-based methods, the PHY security can provide an everlasting security guarantee without the need of costly and complex secret key management/distribution. Therefore, the PHY security could be a promising security solution well-suited to MANETs.

By now, most of the previous works on the PHY security performance study of MANETs focused on the metric of secrecy throughput [1]–[3], which represents the maximum achievable rate at which the source packet can be reliably transmitted to the destination, while security can be guaranteed against eavesdroppers. The authors in [1] studied the delay-constrained secrecy throughput of a MANET under passive attack (overhearing the transmission only) and active attack (jamming the transmission in addition to overhearing). The results in [1] showed that the secrecy throughput under passive attack is independent of the number of eavesdroppers m, if m is less than some threshold, while such threshold does not exist for active attack. In addition, the secrecy throughput achieved under active attack is no better than that achieved under passive attack in general. Cao et al. [2] also investigated the delay-constrained secrecy throughput capacity of a MANET with static and passive eavesdroppers and introduced an artificial noise-aided security scheme to improve the secrecy throughput capacity achieved in [1]. The secrecy, throughput and delay were derived for a MANET with passive eavesdroppers under the two-hop routing and other routing policies such as Spray-and-Wait in [3], where the tradeoffs among these three metrics were also examined. It is notable that these works focus on deriving the scaling law results, which are certainly important to characterize how the secrecy throughput of a MANET scales up as the network size tends to infinity. However, they can hardly reflect the exact secrecy throughput of a MANET with finite nodes, which may be more desired to facilitate the design, development and commercialization of MANETs. Actually, some recent works have been reported to study the exact secrecy transmission capacity of MANETs, which, however, characterizes only the local achievable secrecy rate

978-1-4673-9803-9/15 $31.00 © 2015 IEEE
DOI 10.1109/NaNA.2016.41

for one-top transmission.

In this paper, we study the exact secrecy throughput capacity for cell-partitioned MANETs [4], [5], where the group-based scheduling [6]–[9] is adopted to coordinate the simultaneous transmission for eliminating interference. Like other PHY security-based studies [10]–[12], we assume each transmitter can detect the existence of eavesdroppers in a region around itself, called secrecy guard zone. The transmission is conducted in an on-off manner such that if no eavesdroppers exist in the secrecy guard zone around the transmitter, the transmission will be conducted (on), otherwise the transmission will be suspended (off). To derive the exact secrecy throughput of the network, we first derive the probability that a transmission can be securely conducted between a given active cell c and the cells in the transmission range of c (i.e., coverage cells) and also the probability that a source-destination transmission can be securely conducted between c and its coverage cells. With the help of these two probabilities and the theoretical framework for throughput analysis of MANETs in [13], we then derive the exact secrecy throughput as well as the upper bound on the delay of the MANET. Finally, extensive simulation and numerical results are provided to corroborate our theoretical analysis and also to illustrate the performances of secrecy throughput and delay.

The rest of the paper is organized as follows. In Section II, we introduce the system model and illustrate the proposed transmission schemes. In Section III, we characterize the exact secrecy throughput capacity and packet delay there. In Section IV, we provide simulation/numerical results to validate our model and also explore the impacts of guard zone size and eavesdroppers density upon throughput capacity and delay. Finally, we conclude this paper in Section V.

II. System Model and Transmission Scheme

As shown in Figure 1, we consider that the wireless network is a square partitioned into $w \times w$ cells. The network consists of n legitimate nodes and m eavesdroppers. We adopt the independent and identically distributed (i.i.d.) mobility model [4], [14], [15], 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 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 $1 \leq v < \lfloor \frac{w+1}{2} \rfloor$ 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 $1 \leftrightarrow 2$, $3 \leftrightarrow 4$, ... , $(n-1) \leftrightarrow n$, 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 λ 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 $E\{A_i(t)\} = \lambda$ and a bounded second moment A_{max}^2 follows $E\{A_i^2(t)\} \leq A_{max}^2 < \infty$, where $E\{\}$ is the expectation operator. We adopt the widely-used group-based scheduling [6]–[9] to coordinate the simultaneous transmission for eliminating interference. In this scheduling, all cells of the network are divided into α^2 groups. Each group consists of $K = \lfloor w^2/\alpha^2 \rfloor$ cells and becomes active to transmit data every α^2 time slots. The cells in the current active group are called active cells throughout the paper. In the same group, the distance between any two horizontally (or vertically) adjacent cells is of α cells, as shown in Figure 1. In addition, α can be determined as

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

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

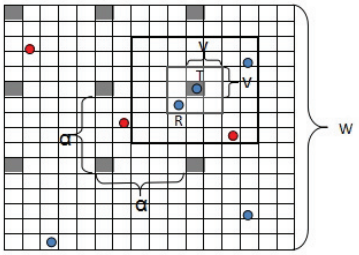


Fig. 1. System Model: T and R respectively stand for the legitimate transmitter and receiver. The red points represent eavesdroppers. All shaded cells mean that they are in the same group. The square with gray bold border means the transmission range. The square with black bold border means the secrecy guard zone. And $w = 16$, $\alpha = 5$ and $v = 2$.

We assume each transmitter can detect the existence of eavesdroppers in a region around itself. We model this region as a square containing g cells and call it the secrecy guard zone as shown in Figure 1. The idea of guard zone has been widely used in [10]–[12]. In [10] and [11], the authors use the guard zone around each legitimate node to study the secure connectivity and secrecy capacity scaling law of ad hoc networks. In [12], the authors use the guard zone around each legitimate receiver to activate or deactivate the receiver on the basis of the existence of eavesdroppers in its guard zone. In this paper, we apply a secrecy guard zone around each legitimate transmitter and consider the following transmission scheme: the transmission is conducted in an on-off manner such that if no eavesdroppers exist in the secrecy guard zone around the transmitters, the transmission will be conducted (on), otherwise the transmission will be suspended (off).

III. Secrecy Throughput Capacity and Delay

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

Lemma 1: For a given time slot and a given active cell c, let p_0 denote the probability that a transmission can be securely conducted between a given active cell c and its coverage cells, and let p_1 denote the probability that a source-destination transmission can be securely conducted between c and its coverage cells, then we have

$$p_0 = \frac{1}{w^{2n}}(1-\frac{g}{w^2})^m\{w^{2n}-(w^2-1)^n- \\ n(w^2-(2v-1)^2)^{n-1}\}, \tag{2}$$

$$p_1 = \frac{1}{w^{2n}}(1-\frac{g}{w^2})^m\{w^{2n}-(w^4-2(2v- \\ 1)^2+1)^{\frac{n}{2}}\}. \tag{3}$$

Proof. First, we need to 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. We derive the probability that there are j $(j \geq 1)$ eavesdroppers in the secrecy guard zone centered at c is

$$\binom{m}{j}(\frac{g}{w^2})^j(\frac{w^2-g}{w^2})^{m-j}. \tag{4}$$

Thus, the probability that the transmission can be on is determined as

$$(1-\frac{g}{w^2})^m. \tag{5}$$

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 [13], we have

$$\hat{p_0} = \frac{1}{w^{2n}}\{w^{2n}-(w^2-1)^n-n(w^2-(2v-1)^2)^{n-1}\}. \tag{6}$$

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

$$p_0 = \frac{1}{w^{2n}}(1-\frac{g}{w^2})^m\{w^{2n}-(w^2-1)^n- \\ n(w^2-(2v-1)^2)^{n-1}\}. \tag{7}$$

We then 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 [13], we have

$$\hat{p_1} = \frac{1}{w^{2n}}\{w^{2n}-(w^4-2(2v-1)^2+1)^{\frac{n}{2}}\}. \tag{8}$$

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

$$p_1 = \frac{1}{w^{2n}}(1-\frac{g}{w^2})^m\{w^{2n}-(w^4-2(2v- \\ 1)^2+1)^{\frac{n}{2}}\}. \tag{9}$$

Based on p_0 and p_1, we get the exact secrecy throughput capacity as well as the upper bound on the delay for the concerned network, which can hold for any feasible packet delivery algorithm.

Theorem 1: Consider a cell-partitioned network with n legitimate nodes, m eavesdroppers and w^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 on-off transmission scheme is utilized to ensure secure transmissions, the exact secrecy throughput capacity μ of the concerned MANET is given by

$$\mu = \frac{\lfloor w^2/\alpha^2 \rfloor}{2nw^{2n}}(1-\frac{g}{w^2})^m\{2w^{2n}-(w^2-1)^n- \\ n(w^2-(2v-1)^2)^{n-1}-(w^4-2(2v-1)^2+1)^{\frac{n}{2}}\}. \tag{10}$$

The expected packet delay $\overline{D}$ of the concerned MANET is given by

$$\overline{D} \leq \frac{B_0}{B_1(1-\rho)\lambda\mu}, \tag{11}$$

where

$$B_0 = (nA_{max}^2+K-2K\lambda)(p_0^2-p_1^2)+2n\mu(p_0+ \\ np_1-p_1), \tag{12}$$

$$B_1 = 4(p_0+np_1-p_1)(p_0-p_1), \tag{13}$$

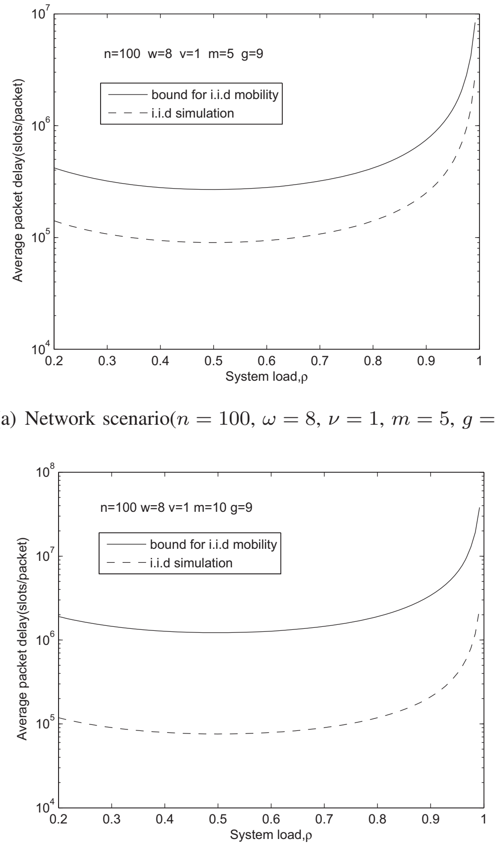
and

$$\rho = \frac{\lambda}{\mu} \text{ denotes the system load.} \tag{14}$$

Proof. The theorem follows from the proof in [13]. The basic idea of the proof is as follows: first, we prove μ in (10) 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 ϵ, thus, we derive the upper bound μ. Second, we prove μ 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 μ is the exact secrecy throughput capacity. For the details of the proof, please refer to [13].

IV. Numerical Results and Discussions

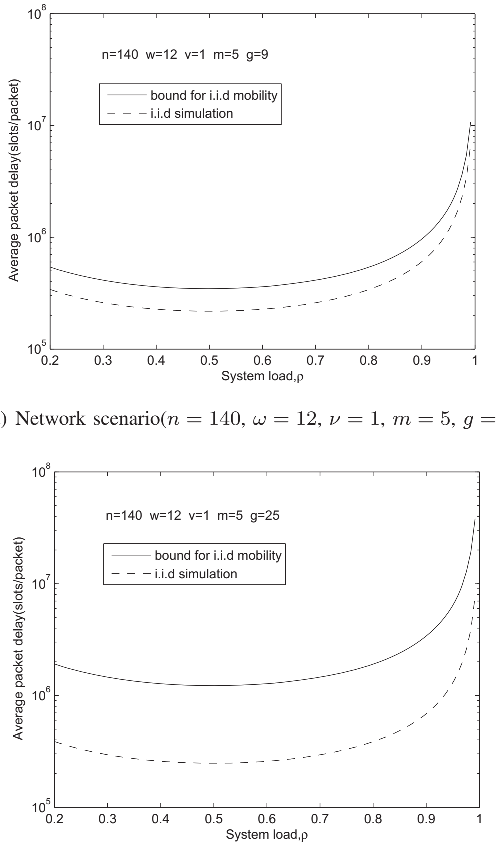
In this section, we provide simulation/numerical results to validate our model and also to explore the impacts of guard zone size and the number of eavesdroppers upon the secrecy throughput capacity and the expected packet delay.



(a) Network scenario($n = 100$, $\omega = 8$, $\nu = 1$, $m = 5$, $g = 9$)

(b) Network scenario($n = 100$, $\omega = 8$, $\nu = 1$, $m = 10$, $g = 9$)

Fig. 2. Average packet delay for network scenarios with $n = 100$, $\omega = 8$



(a) Network scenario($n = 140$, $\omega = 12$, $\nu = 1$, $m = 5$, $g = 9$)

(b) Network scenario($n = 140$, $\omega = 12$, $\nu = 1$, $m = 5$, $g = 25$)

Fig. 3. Average packet delay for network scenarios with $n = 140, \omega = 12$

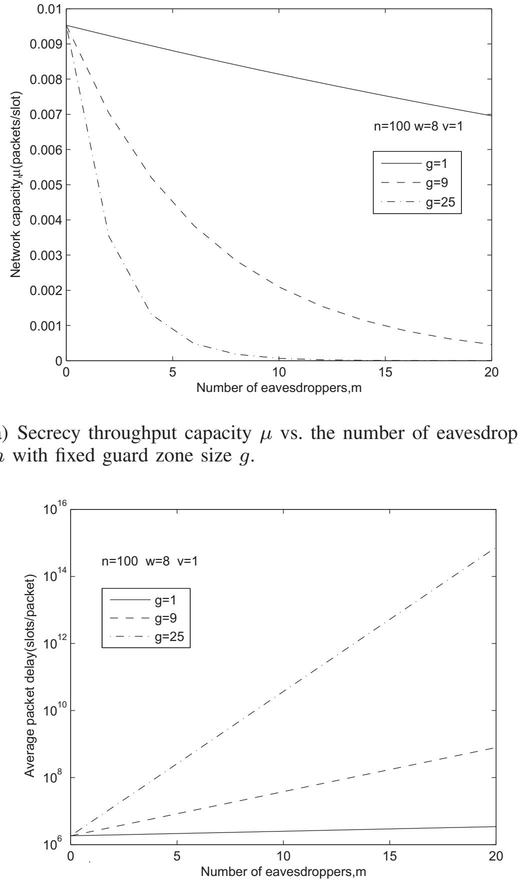
A. Model Validation

We developed a dedicated C++ simulator to simulate the packet delivery process in the concerned network with i.i.d n-ode mobility, group-based scheduling, secrecy guard zone and general transmission range. Assume that the system generates local packets with average input rate λ (packets/slot).

Numerous simulations have validated the secrecy throughput capacity and the delay upper bound. Figure 2 and 3 indicate clearly the relationship between the system load and the expected packet delay. When ρ approaches 1, namely, the input rate λ is infinitely close to the secrecy throughput μ, the expected packet delay increases drastically. When $\lambda < \mu$, the theoretical delay upper bound in (11) can always bound the expected packet delay, implying that the network is always stable. Therefore, our theoretical model can be used to effectively explore the secrecy throughput capacity as well as the upper bound on the delay.

B. Impacts of Guard Zone Size and the Number of Eavesdroppers on Secrecy Throughput and Delay

With the help of new secrecy throughput capacity result, we explore the impacts of secrecy guard zone size and the number of eavesdroppers upon the secrecy throughput capacity and the expected packet delay. Figure 4 shows how secrecy throughout capacity and delay upper bound vary with secrecy guard zone size g. We considered three different network scenarios of $g = 1$, 9 and 25, which correspond to low security, moderate security and high security. We can see that as g increases, the secrecy throughput capacity decreases, while the expected packet delay increases. This is because that as the secrecy guard zone size becomes larger, more eavesdroppers appear in the secrecy guard zone and the probability that the transmission is on will become smaller. In Figure 5, we also



(a) Secrecy throughput capacity μ vs. the number of eavesdroppers m with fixed guard zone size g.

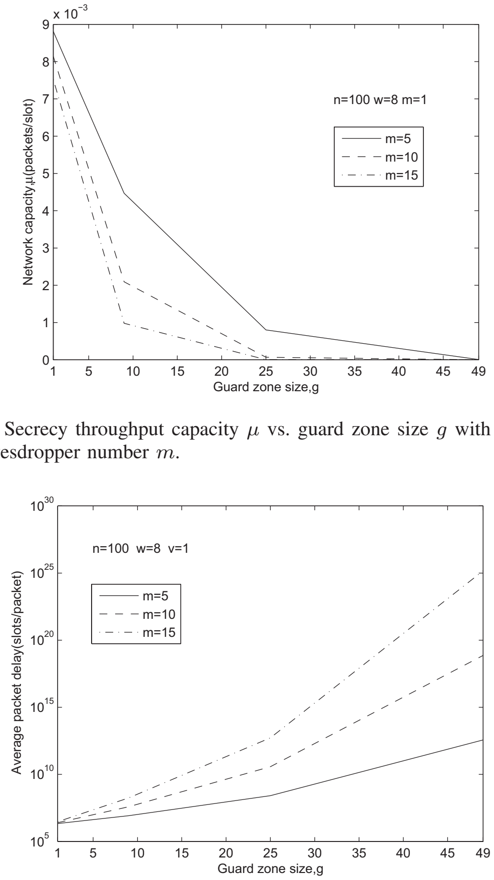
(b) Packet delay $\overline{D}$ vs. the number of eavesdroppers m with fixed guard zone size g.

Fig. 4. The performances of secrecy throughput and delay vary with guard zone size g.

considered three different network scenarios of $m = 5$, 10 and 15, which correspond to sparse eavesdroppers, general eavesdroppers and dense eavesdroppers. We can observe that as the number of eavesdroppers increases, the secrecy throughput capacity decreases, while the expected packet delay increases. This is because that as the number of eavesdroppers increases, the probability that there are at least one eavesdropper appearing in the secrecy guard zone becomes larger, that is, the probability that transmission is on will become smaller.

V. Conclusion

This paper derived the exact secrecy throughput capacity of a cell-partitioned MANET with the group-based scheduling to eliminate interference from simultaneous transmissions, adopted the secrecy guard zone to allow each transmitter to detect the existence of eavesdroppers in a region around itself, and used an on-off transmission scheme to ensure the transmission security. First, we compute the probabilities of overall transmissions and source-destination transmissions. With the help of the two probabilities, we then derive the exact secrecy throughput as well as the upper bound on the delay of the concerned network. Numerical results validate our theoretical analysis and illustrate the performances of secrecy throughput and delay.



(a) Secrecy throughput capacity μ vs. guard zone size g with fixed eavesdropper number m.

(b) Packet delay $\overline{D}$ vs. guard zone size g with fixed eavesdropper number m.

Fig. 5. The performances of secrecy throughput and delay vary with eavesdropper number m.

References

[1] Y. Liang, H. V. Poor, and L. Ying. Secrecy throughput of manets under passive and active attacks. *IEEE Trans. Inf. Theory*, 57(10):6692–6702, 2011.

[2] 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 Trans. Network*, 2015.

[3] S. Shintre, L. Sassatelli, and J. Barros. Generalized delay-secrecy-throughput trade-offs in mobile ad-hoc networks. In *Antennas and Propagation in Wireless Communications (APWC), 2011 IEEE-APS Topical Conference on*, pages 1424–1427, 2011.

[4] M. J. Neely and E. Modiano. Capacity and delay tradeoffs for ad hoc mobile networks. *IEEE Trans. Inf. Theory*, 51(6):1917–1937, 2005.

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

[6] J. Liu, X. Jiang, H. Nishiyama, and N. Kato. Delay and capacity in ad hoc mobile networks with f-cast relay algorithms. *IEEE Trans. Wireless Communications*, 10(8):2738–2751, 2011.

[7] D. Ciullo, V. Martina, M. Garetto, and E. Leonardi. Impact of correlated mobility on delaycthroughput performance in mobile ad hoc networks. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9, 2010.

[8] P. Li, Y. Fang, J. Li, and X. Huang. Smooth trade-offs between throughput and delay in mobile ad hoc networks. *IEEE Trans. Mobile Compute*, 11(3):427–438, 2012.

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

[10] P. C. Pinto, J. Barros, and M. Z. Win. Secure communication in stochastic wireless networksłpart ii: Maximum rate and collusion. *IEEE Trans. Inf. Forensics and Security*, 7(1):139–147, 2012.

[11] O. Koyluoglu, C. Kaksal, and H. El Gamal. On secrecy capacity scaling in wireless networks. In *Information Theory and Applications Workshop (ITA), 2010*, pages 1–4, 2010.

[12] A. Hasan and Andrews J. G. The guard zone in wireless ad hoc networks. *IEEE Trans. Wireless Communications*, 6(3):897–906, 2007.

[13] J. Gao, J. Liu, and X. Jiang. Throughput capacity of manets with group-based scheduling and general transmission range. *Ieice Trans Commun*, 2013.

[14] M. Grossglauser and D. Tse. Mobility increases the capacity of ad hoc wireless networks. In *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1360–1369, 2001.

[15] S. Toumpis and A. J. Goldsmith. Large wireless networks under fading, mobility, and delay constraints. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 1, page 619, 2004.