Optimal Secrecy Capacity-Delay Tradeoff in Large-Scale Mobile Ad Hoc Networks

Xuanyu Cao, Jinbei Zhang, Luoyi Fu, Weijie Wu, and Xinbing Wang

***Abstract*—In this paper, we investigate the impact of information-theoretic secrecy constraint on the capacity and delay of mobile ad hoc networks (MANETs) with mobile legitimate nodes and static eavesdroppers whose location and channel state information (CSI) are both unknown. We assume n legitimate nodes move according to the fast i.i.d. mobility pattern and each desires to communicate with one randomly selected destination node. There are also n^{ν} static eavesdroppers located uniformly in the network and we assume the number of eavesdroppers is much larger than that of legitimate nodes, i.e., $\nu > 1$. We propose a novel simple secure communication model, i.e., the secure protocol model, and prove its equivalence to the widely accepted secure physical model under a few technical assumptions. Based on the proposed model, a framework of analyzing the secrecy capacity and delay in MANETs is established. Given a delay constraint D, we find that the optimal secrecy throughput capacity is $\widetilde{\Theta}(W((D/n))^{(2/3)})$, where W is the data rate of each link. We observe that: 1) the capacity-delay tradeoff is independent of the number of eavesdroppers, which indicates that adding more eavesdroppers will not degenerate the performance of the legitimate network as long as $\nu > 1$; 2) the capacity-delay tradeoff of our paper outperforms the previous result $\Theta((1/n\psi_e))$ in [11], where $\psi_e = n^{\nu-1} = \omega(1)$ is the density of the eavesdroppers. Throughout this paper, for functions $f(n)$ and $g(n)$, we denote $f(n) = o(g(n))$ if $\lim_{n\to\infty}(f(n)/g(n)) = 0$; $f(n) = \omega(g(n))$ if $g(n) = o(f(n))$; $f(n) = O(g(n))$ if there is a positive constant c such that $f(n) \leq cg(n)$ for sufficiently large n; $f(n) = \Omega(g(n))$ if $g(n) = O(f(n))$; $f(n) = \Theta(g(n))$ if both $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$ hold. Besides, the order notation $\widetilde{\Theta}$ omits the polylogarithmic factors for better readability.**

***Index Terms*—Capacity–delay tradeoff, mobile ad hoc networks (MANETs), secrecy constraint.**

I. Introduction

THOUGH having the advantage of convenience and low cost, wireless networks are vulnerable to attacks such as eavesdropping and jamming due to its broadcast nature. Most of existing solutions are based on cryptographic methods, e.g., RSA public key crypto-system. However, there two major drawbacks of the cryptographic solutions. First, the key distribution can be very costly in terms of both energy consumption and computation/decoding capability because of the rapid growth of the size of today's wireless networks, which makes the traditional cryptographic methods infeasible. Second, the cryptographic schemes essentially guarantee security by imposing hard mathematical problems on the eavesdroppers, whose computational ability are not high enough to solve the problems. But the eavesdroppers do obtain the data information and the enemy will decode the message with enough time and computational power. Therefore, to avoid the limitations of the cryptographic solutions, we focus on information theoretic security in this paper, i.e., safety is ensured even though the eavesdroppers have infinite computational and decoding power.

The study of information-theoretic secrecy originates from the seminal works of Shannon [1], Wyner [2], Csiszar and Korner [3], where the secrecy requires the receiver to have better channel than eavesdroppers. Recently, a few schemes are proposed to guarantee the secret communication. Geol and Negi [4] exploit artificial noise to suppress the SNR at the eavesdroppers so as to ensure security. Independence of wireless fading channels are also used to generate noise with cooperation [5] and multiple antennas [6], [7].

While the above mentioned works all focus on proposing various techniques to ensure information-theoretic security, a few papers also investigate the impact of the secrecy constraint on the network capacity and delay. For example, Vasudevan *et al.* [8] study the secrecy-capacity tradeoff in large-scale wireless networks and introduce helpers around the transmitters to generate noise to suppress the SNR at the eavesdroppers. Capar *et al.* [9] propose a new secrecy communication scheme that can tolerate $o((n/\log n))$ eavesdroppers while keeping the network throughput not affected. To transmit a single bit, the authors proposed to generate multiple bits and transmit all of them to the desired destinations through different paths. The original bit can be decoded if and only if all of the generated bits are obtained and the authors present a routing/scheduling protocol to make sure no eavesdroppers could get all those bits. A very related work is a recent paper by Zhang *et al.* [10]. The authors let every receiver generate artificial noise in order to degrade the SNR at the eavesdroppers and study the impact of secrecy constraints on the capacity scaling in static networks.

However, most existing works such as [9], [10] focus on secrecy capacity scaling in static networks, yet little is known about the secrecy capacity-delay tradeoff in MANETs. As an exception, Liang *et al.* [11] first attempt to study the secrecy-capacity-delay tradeoff in MANETs. But, [11] has its limitation.

Manuscript received February 18, 2014; revised September 15, 2014 and December 27, 2014; accepted February 08, 2015; approved by IEEE/ACM Transactions on Networking Editor L. Ying. Date of publication April 01, 2015; date of current version April 14, 2016. This work was supported in part by NSF China (No. 61325012, 61271219, 61221001, 61428205); China Ministry of Education Doctor Program (No. 20130073110025); Shanghai Basic Research Key Project (No. 11JC1405100, 13510711300, 12JC1405200); and Shanghai International Cooperation Project (No. 13510711300).

X. Cao, J. Zhang, L. Fu, and X. Wang are with the Department of Electronics Engineering, Shanghai Jiao Tong University, Shanghai, Shanghai 200240, China.

W. Wu is with the Department of Electronics, Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, Shanghai 200240, China.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TNET.2015.2405793

The authors do not allow receivers to generate artificial noise so as to degenerate the channel at the eavesdroppers. Instead, they just let each transmitter wait until the intended receiver is sufficiently near. This turns out to be very inefficient compared to the artificial noise methods adopted in [10] and leads to low throughput and high delay. Observing this limitation, we are motivated to investigate the impact of secrecy constraint on the capacity and delay tradeoffs in MANETs with more efficient secrecy scheme. By MANETs, we mean that the legitimate nodes are mobile while the eavesdroppers are static. This is reasonable since the eavesdroppers may be detected easily if they move drastically. To see the impact of the secrecy constraint, we assume that the number of eavesdroppers is larger than that of the legitimate nodes in this paper. The physical layer method that we adopt to achieve information-theoretic security is the same as that of [10]. Specifically, each intended receiver generates artificial noise to suppress the SNR at the eavesdroppers and distinguishes its own channel by adopting the self-interference cancelation techniques proposed in [12]. Thus, each receiver will not be interfered by the noise generated by itself, i.e., the channel at the receiver can be much better than that at the eavesdroppers.

The primary contributions of this work are summarized as follows:

- We propose a novel simple secure communication model, i.e., the secure protocol model, to analyze the performance of wireless networks with secrecy constraint. We show that the secure protocol model is equivalent to the widely accepted secure physical model under a few technical assumptions. Thus, a framework to analyze wireless networks with secrecy constraint is established.
- We apply the secure protocol model to MANETs with mobile legitimate nodes and static eavesdroppers. Given a delay constraint D, we derive upper bound for the secrecy capacity and then present the corresponding capacity achieving scheme. We find that as long as the eavesdropper density $\psi_e = \omega(1)$, the optimal capacity delay tradeoff is always $\widetilde{\Theta}(W((D/n))^{2/3})$, which is independent of the specific value of ψ_e. This significantly improves the previous result in [11] and shows the great advantage of our scheme.

We remark that although the focus of this paper is on networks with i.i.d. mobile legitimate nodes, the secure protocol model we develop is suitable for any wireless networks where the number of eavesdroppers are larger than that of the legitimate nodes. The proposed secure protocol model can be applied to networks with different mobility patterns and traffic patterns (e.g., unicast, multicast, converge-cast) and is thus quite general and extendable.

The rest of this paper is organized as follows. In Section II, we review some related works on the scaling laws of wireless networks. In Section III, we formulate the system model formally while in Section IV, an overview of the solution idea and the main results are presented. In Section V, we propose the secure protocol model and prove its correspondence with the widely accepted secure physical model. In Section VI, we derive an upper bound for the secrecy capacity-delay tradeoff while the corresponding capacity achieving scheme is presented in Section VII. Some discussions are presented in Section VIII and we conclude this work in Section IX.

II. Related Works

In this paper, we provide the asymptotic analysis for the optimal secrecy capacity-delay tradeoffs in MANETs. The fundamental scaling law analysis of wireless networks is initiated by the ground-breaking work of Gupta and Kumar [13]. They show that the per-node unicast capacity for random uniform networks with n nodes is $\Theta((1/\sqrt{n \log n}))$ under the protocol model. Under this framework, multicast traffic pattern [24], heterogeneity in nodes' distribution [25], [26], hybrid networks [27] and MIMO cooperation [28] are also studied in the literature.

Another important trend, which is quite related with this paper, is to introduce mobility to improve the network capacity. Grossglauser and Tse [14] first take the mobility of wireless nodes into consideration and find that capacity can be enhanced significantly by exploiting the nodes' mobility. In their i.i.d. mobility model and two-hop transmission scheme, each source broadcasts the packets to its neighbors which serve as relays, and then the packets are delivered to the destination whenever it is within the transmission range of the one of those relays. However, the major drawback of this scheme is large delay since the destination may not meet with the relays until a long time has passed. Hence, since then, great efforts have been made to improve capacity delay tradeoffs, i.e., to achieve relatively high capacity with acceptable delay [15]–[19]. Particularly, for a variety of mobility models, given a delay constraint D, Ying *et al.* [19] provides matching (except for poly-log terms) upper bounds and lower bounds on the throughput capacity. In addition, various mobility models are also investigated in [20], [21]. Motioncast, i.e., multicast traffic over MANETs, is also studied by Wang *et al.* [22] and Zhang *et al.* [23].

III. System Model

In this paper, we assume that the network area is a square with size $\sqrt{n} \times \sqrt{n}$, where n is the number of legitimate nodes.

A. Legitimate Network

There are n legitimate nodes in total in the network area. Denote X_i the position of legitimate node i. Dividing time into constant duration time slots, we adopt the well known i.i.d. mobility model to characterize the drastic topology change of the MANETs. Specifically, the initial position of each legitimate node is equally likely to be any point in the network area. At the beginning of each time slot, every node randomly and uniformly chooses a point i.i.d. in the network area to be its new position. Throughout this paper, we assume a fast mobility model [19], [23] for the legitimate nodes, i.e., only one-hop transmission is allowed in each time slot. Although the i.i.d. mobility is an oversimplified model to some extent, it is widely adopted in the literature due to its mathematical tractability. In addition, i.i.d. mobility can be viewed as the mobility with very large speed and hence we could use this model to characterize the fundamental impact of mobility on network performance. With the help of mobility, packets could reach the destinations without being relayed for many times, which decreases the traffic load of the network, and larger capacity is expected.

We assume that the traffic pattern of between legitimate nodes is unicast. Equivalently speaking, source-destination pairs are randomly chosen such that each node is the destination of exactly one source. We denote $\mathcal{T}(\mathcal{R})$ as the sets of legitimate nodes simultaneously transmitting (receiving) at a given time slot. As in [10], we assume each legitimate node is equipped with three antennas. When a legitimate node acts as a receiver, one antenna is used for message reception while the other two are devoted to simultaneous artificial noise generation to suppress the eavesdroppers' channels. The distances between the receive antenna and the other two respective transmit antennas should satisfy a difference of half of the wavelength. The interference can thus be eliminated by invoking the techniques of self-interference cancelation proposed in [12]. Thus, each receiver will not be interfered by the artificial noise generated by itself.

B. Eavesdropper Network

There are n^{ν} eavesdroppers located in the same network area. Denote $\mathcal{E}$ as the set of all the eavesdroppers and y_e the position of eavesdropper $e \in \mathcal{E}$. We assume that the number of eavesdroppers is much larger than that of legitimate nodes, i.e., $\nu > 1$. Thereby, the density of the eavesdroppers $\psi_e = n^{\nu-1}$ is much larger than 1, i.e., $\psi_e = \omega(1)$. Different from legitimate nodes, the eavesdroppers are assumed to be static, i.e., the position of each eavesdropper does not change with time. This is reasonable since the eavesdroppers may be detected easily if they move drastically. More precisely, each eavesdropper independently and uniformly select a point in the network area as its fixed position. The eavesdroppers always keep silent since they may be detected otherwise. Hence, instead of jamming the signal, the eavesdroppers can only overhear messages in our setup. The eavesdroppers have infinite computational capability and thus information-theoretic security is needed. We also assume that both CSI and location information of eavesdroppers are unknown to the legitimate nodes.

C. Secure Physical Model

The secure physical model is widely accepted in the literature and we describe it in the following. Denote $P_{t,i}$ the transmission power of node i if $i \in \mathcal{T}$. Similarly, denote $P_{r,j}$ the noise generation power of node j if $j \in \mathcal{R}$. The path loss between node i and node j is denoted by $l(X_i, X_j)$ with $l(X_i, X_j) = l(|X_i - X_j|) = \min\{1, |X_i - X_j|^{-\alpha}\}$. Here, X_i is the position of node i while α is the path loss exponent. We assume that $2 < \alpha < 4$, which is a typical value range for outdoor path loss exponent. When node i is transmitting messages to node j, the signal to interference and noise ratio (SINR) at the receiver node j is given by:

$$\mathrm{SINR}_{ij} = \frac{P_{t,i} l(X_i, X_j)}{N_0 + \sum_{k \in \mathcal{T}\backslash\{i\}} P_{t,k} l(X_k, X_j) + \sum_{k \in \mathcal{R}\backslash\{j\}} P_{r,k} l(X_k, X_j)} \tag{1}$$

where N_0 denotes the ambient noise power of the network environment. Note that $P_{r,j}$ is not an interference to the receiver, node j, since we adopt self-interference cancelation techniques.

On the other hand, $P_{r,j}$ do interfere with the eavesdroppers and the SINR at the eavesdropper e cab be represented by:

$$\mathrm{SINR}_{ie} = \frac{P_{t,i} l(X_i, Y_e)}{N_0 + \sum_{k \in \mathcal{T}\backslash\{i\}} P_{t,k} l(X_k, Y_e) + \sum_{k \in \mathcal{R}} P_{r,k} l(X_k, Y_e)}. \tag{2}$$

As in [9], [11], we say a transmission is secret if none of each eavesdropper could decode the messages. Specifically, we define a transmission to be successful and secret if the following two conditions hold.

- $\mathrm{SINR}_{ij} \geq \gamma_r$.
- For each eavesdropper $e \in \mathcal{E}$, $\mathrm{SINR}_{ie} \leq \gamma_e$.

Here γ_r, γ_e are two positive constants indicating the SINR thresholds for successful reception of information. The first condition assures that the receiver, node j, can decode the message successfully while the second condition guarantees that none of each eavesdropper could decode the message. We remark that, in practice, to ensure the transmissions between legitimate nodes are reliable and all the eavesdroppers cannot get any useful information, one may require γ_r to be large and γ_e to be low in the secure physical model.

We assume that the data rate for successful secure transmission is W bit per time slot. We call a couple of nodes a link if they form a transmitter-receiver pair, e.g., (X_i, X_j). Given a communication (interference) model, in general there are a number of subsets of links that can be active simultaneously. We call such subsets of links together with the corresponding power management and node positions a *feasible state*, and define the set of all feasible states as *feasible family* [29]. We use $\mathcal{PH}(\gamma_r, \gamma_e)$ to denote the feasible family of the secure physical model.

D. Definitions of Performance Metrics

We consider hard delay constraints as [19] in this paper. Given a delay constraint D, a packet is said to be successfully delivered if the destination obtains the packet within D time slots after it is sent out from the source.

The asymptotic per-node secure throughput capacity $\lambda(n)$ is said to be achievable if there is a scheduling and routing scheme such that every legitimate node can transmit $\lambda(n)$ bps securely on average to its destination in the long term.

The frequently used parameters are listed in Table I.

IV. Overview of Idea and Main Results

A. Solution Idea

Our system model begins with the widely accepted secure physical model, i.e., the SINR at the receiver should be larger than a threshold to guarantee a successful transmission while the SINR at all the eavesdroppers should be smaller than another threshold to ensure security. Hence, compared to the insecure physical model proposed in [13], the secure physical model

TABLE I
NOTATIONS

Notations	Definitions
n	The total number of legitimate nodes in the network.
n^{ν}	The total number of eavesdroppers in the network, where $\nu > 1$.
ψ_e	The density of eavesdroppers, $\psi_e = n^{\nu-1}$.
α	The path loss exponent, $2 < \alpha < 4$.
$\lambda(n)$	The per-node secure throughput capacity of legitimate nodes.
D	The delay constraint imposed on the packets.
P_t	The common transmission power at a given time.
P_r	The common noise generation power at a given time.
$\mathscr{PH}(\gamma_r, \gamma_e)$	The feasible family of secure physical model.
$\mathscr{PR}(C_t)$	The feasible family of secure protocol model.
$\mathcal{T}$	The set of simultaneously active transmitters at a given time slot.
$\mathcal{R}$	The set of simultaneously active receivers at a given time slot.
$\mathcal{E}$	The set of eavesdroppers.
X_i	The position of legitimate node i.
Y_e	The position of eavesdropper node e.
$\lvert\cdot\rvert$	The Euclidean length or the number of elements of a set.
$D(x, r)$	The disk with radius r centered at x.
$l(X_i, X_j)$ or $l(\lvert X_i - X_j\rvert)$	The path loss function $\min\{1, \lvert X_i - X_j\rvert^{-\alpha}\}$.
W	The data rate for successful secure transmission.

in Section III-C poses another SINR constraint on those eavesdroppers. The key issue that we aim to address is how this secrecy constraint may influence the network capacity and delay.

Though the secure physical model is quite ideal and general for networks with eavesdroppers, it is not convenient from the perspective of analysis because it involves many underlying details such as the network topology, transmission power, noise generation power and SINR judgement for checking the eligibility of a link. Therefore, we propose the *secure protocol model* (Definition 5.2), which has one parameter C_t and is shown to be equivalent to the secure physical model under a few technical assumptions.

The proposed secure protocol model is significantly simpler to analyze because it only relies on the geometry of the nodes' positions and conceals other factors such as power, noise and interference. In Section V, we present the secure protocol model and establish its equivalence to the secure physical model based on a few assumptions formally.

Thanks to the secure protocol model, a framework of analyzing the secrecy capacity-delay tradeoff is formed for MANETs. Under the secure protocol model, we derive an upper bound on the secrecy capacity given a delay constraint. Afterwards, we show a capacity-achieving scheme which could obtain the optimal throughput capacity up to poly-log factors. Since the secure protocol model is equivalent to the secure physical model under several assumptions, our results immediately apply to the secure physical model under those assumptions. Note that the proposed secure protocol model is quite general and is applicable to wireless networks with other traffic patterns and mobility patterns. Indeed, as long as the eavesdropper density $\psi_e = \omega(1)$, the secure protocol model is always effective.

B. Main Results

Supposing the four technical assumptions in Section V hold, we list the main results of this paper as follows.

- **Correspondence between secure protocol model and secure physical model**:
  The secure physical model is shown to be equivalent to the proposed secure protocol model. By equivalence, we mean the capacity-delay scaling law is the same. For any given secure physical model, we can find a secure protocol model such that the feasible family of the secure protocol model is a subset of the feasible family of the given secure physical model (Theorem 5.1). Meanwhile, we can also find a secure protocol model such that the feasible family of the given secure physical model is a subset of the secure protocol model (Theorem 5.2). This equivalence allows us to analyze the secure physical model by transforming it into the proposed secure protocol model without changing the scaling law results.
- **Optimal secrecy-capacity-delay tradeoffs in MANETs**:
  — Under the secure physical model, the secrecy per-node throughput capacity λ with delay constraint D is no more than:
  $$\lambda = O\left(W\left(\frac{D}{n}\right)^{\frac{2}{3}}\log n\right). \tag{3}$$
  — Under the secure physical model, if $D = \Omega(n^{2/5}(\log n)^{21/5})$ and $D = O(n)$, then there exists a feasible scheme achieving a per-node throughput of:
  $$\lambda = \Omega\left(W\left(\frac{D}{n}\right)^{\frac{2}{3}}(\log n)^{-12}\right). \tag{4}$$

V. The Secure Protocol Model

In this section, we propose the secure protocol model formally. Throughout this section, we assume that the eavesdroppers are located uniformly and randomly while the positions of the legitimate nodes are arbitrary. We then establish the equivalence between the proposed secure protocol model and the secure physical model under a few technical assumptions. Thus, a tractable framework of analyzing the secrecy capacity-delay tradeoff is formed. Before introducing these assumptions, we define the parameter d^* of a state as follows.

1) Definition 5.1: For a certain state (with at least two simultaneously active transmitters), we denote d^* the minimum distance between any two simultaneously active transmitters, i.e.,

$$d^* = \min_{i,j}\left\{\lvert X_i - X_j\rvert \middle| i, j \in \mathcal{T}, i \neq j\right\}. \tag{5}$$

Now we list four assumptions of a state in the following.

1) There are at least two simultaneously active transmitters. For any point P in the network area, there is at least one active transmitter within the disk $D(P, 2d^*)$.

2) For any transmitter-receiver pair (X_i, X_j), we have[1] $d^* \geq 8(|X_i - X_j| + 1)$. In addition, for the secure physical model: $d^* \geq ((144\gamma_e \alpha \cdot 2^{2\alpha-1}/\alpha - 2))^{1/\alpha}$.
3) For the secure physical model, all the transmitters utilize the same transmission power, i.e., $P_{t,i} = P_t, \forall i \in \mathcal{T}$ and all the receiver utilize the same noise generation power, i.e., $P_{r,j} = P_r, \forall j \in \mathcal{R}$.
4) For the secure physical model, $\gamma_r > 2^{3\alpha+1}\gamma_e$.

We note that the above four assumptions are all reasonable and are satisfied by most of the scheduling/routing schemes for homogeneous networks. Assumption 1[2] is satisfied by most TDMA-based schemes to exploit the network radio resources efficiently. It basically states that the distances between different adjacent transmitters are in the same order. The Assumption 2 requires that the distance between two simultaneously active transmitters is larger than both some constant times of the transmission range and another certain constant, in order to avoid interference. Since the network distribution of both the legitimate nodes and the eavesdroppers is homogeneous, it is natural to assume that the transmission power and noise generation power are respectively uniform as in Assumption 3. This assumption is also made in [10]. Assumption 4 keeps a certain gap between the SINR at the receivers and that at the eavesdroppers so as to guarantee reliable (high value for γ_r) and secret (low value for γ_e) transmissions. The four technical assumptions are satisfied by most of the scheduling/routing schemes (such as TDMA) in homogeneous networks in the literature of scaling law analysis. We have not optimized the constants involved in these four assumptions to make the assumptions as weak as possible. Hence, an improvement on these assumptions, though not being the focus of this paper, is possible.

Now, we propose the secure protocol model as follows.

2) Definition 5.2: The **Secure Protocol Model** with feasible family $\mathcal{PR}(C_t)$: for any feasible state, we have:

1) All transmissions are unicast, i.e., one transmitter can only have one intended receiver.
2) For any transmitter-receiver pair (X_i, X_j), and any other simultaneously active transmitter $X_p (p \neq i)$:

$$|X_i - X_p| \geq C_t \left(1 + |X_i - X_j|\right)^2. \tag{6}$$

3) Remark 5.1: Compared with the conventional protocol model in [13], the proposed secure protocol model here is stricter: 1) broadcast is not permitted, i.e., one transmitter can only have one intended receiver; 2) the distance between simultaneously active transmitters is much larger compared to the protocol model in [13], i.e., if the transmission range of a link is d, then loosely speaking, any other simultaneously active transmitters must be d^2 distance away from this transmitter. Conventional protocol model only needs to guarantee successful transmissions between Tx and Rx, while the secure protocol model needs to further suppress the SINR at the eavesdroppers to ensure security, which makes it stricter.

Now, we show in the following theorem that, under Assumption 1, the secure protocol model implies the secure physical model.

4) Theorem 5.1: For any two positive constants γ_r, γ_e, there exists a positive constant C_t such that, provided Assumption 1 holds, if a state is feasible under the secure protocol model $\mathcal{PR}(C_t)$, then it must be feasible under the secure physical model $\mathcal{PH}(\gamma_r, \gamma_e)$ by exploiting some uniform transmission power P_t and some uniform noise generation power P_r i.e., Assumption 3 holds.

Proof: We define two positive constants c_1, c_2 as $c_1 = 2N_0\gamma_r$ and $c_2 = (2^\alpha c_1/\gamma_e)$. Then, there exists a positive constant $C_t > 8$ large enough such that:

$$\frac{192\alpha 2^{\alpha-1} c_1}{(\alpha - 2)C_t^2} \leq \frac{N_0}{2} \tag{7a}$$

$$\frac{12\alpha 2^{4\alpha-1} c_2}{C_t^\alpha (\alpha - 2)} \leq \frac{N_0}{2}. \tag{7b}$$

We denote d largest transmission range, i.e.,

$$d = \max_{i,j} \left\{ |X_i - X_j| \middle| (X_i, X_j) \text{ is a transmitter} - \text{receiver pair} \right\}. \tag{8}$$

Next, we prove that with power assignment $P_t = c_1(1 + d)^\alpha, P_r = c_2(1 + d)^{2\alpha}$, the statement in the theorem holds, i.e., the secure protocol model $\mathcal{PR}(C_t)$ implies the secure physical model $\mathcal{PH}(\gamma_r, \gamma_e)$. We begin from an arbitrary feasible state in $\mathcal{PR}(C_t)$. Let's consider two arbitrary links, (X_i, X_j) and (X_p, X_q). Suppose (X_{i_0}, X_{j_0}) is the link that gives the maximization in the definition of d, i.e., $d = |X_{i_0} - X_{j_0}|$. According to Assumption 1, there is a simultaneously active transmitter X_{i_1} such that $|X_{i_1} - X_{i_0}| \leq 2d^*$. Hence, recalling the definition of d^*, we have:

$$2|X_i - X_p| \geq |X_{i_1} - X_{i_0}| \geq C_t \left(1 + |X_{i_0} - X_{j_0}|\right)^2 = C_t(1 + d)^2. \tag{9}$$

Thus, the disks centered at the transmitters $D(X_i, (C_t/4)(1 + d)^2), i \in \mathcal{T}$ are disjoint. We further have:

$$|X_p - X_j| \geq |X_i - X_p| - |X_i - X_j| \tag{10a}$$

$$\geq \frac{C_t}{2}(1 + d)^2 - d \tag{10b}$$

$$\geq 1 + d. \tag{10c}$$

The reason of (10c) is $C_t > 8$. Then, we divide the set $\mathcal{T}\backslash\{i\}$ into the following subsets $\mathcal{T}_k, 1 \leq k \leq (\sqrt{2n}/1 + d)$.

$$\mathcal{T}_k = \{p | k(1 + d) \leq |X_p - X_j| < (k + 1)(1 + d), p \in \mathcal{T}, p \neq i\} \tag{11a}$$

$$\mathcal{T}\backslash\{i\} = \bigcup_{k=1}^{\frac{\sqrt{2n}}{1+d}} \mathcal{T}_k. \tag{11b}$$

[1] In real-world wireless communications, the typical SINR of a 'relatively good signal condition' is 30 dB, i.e., SNR $= 1000$. Besides, the typical value of outdoor path loss exponent is about 3. Suppose the distance between a transmitter-receive pair is d. Then, the nearest simultaneously active transmitter should be at least $(1000)^{1/3}d = 10d$ away. Thus, the first requirement of the assumption 2 is satisfied.

[2] Throughout this paper, we use Assumption 1, 2, 3, and 4 to denote the above four assumptions respectively.

Noting that each transmitter consumes radio resource of a disk area yields the following upper bound for $|\mathcal{T}_k|$:

$$\frac{1}{3}\pi\left[\frac{C_t}{4}(1+d)^2\right]^2\sum_{l=1}^{k}|\mathcal{T}_l| \le \pi\left[(k+1)(d+1)\right]^2 \tag{12}$$

which is equivalent to the following:

$$\sum_{l=1}^{k}|\mathcal{T}_l| \le \frac{48}{C_t^2}\frac{1}{(d+1)^2}(k+1)^2. \tag{13}$$

Hence, the interference caused by other transmitters at X_j, which we denote as $I_t(X_j)$, can be bounded as follows.

$$I_t(X_j) \le \sum_{k=1}^{\frac{\sqrt{2n}}{d+1}}\frac{2^\alpha P_t}{[k(d+1)]^\alpha}|\mathcal{T}_k| \tag{14a}$$

$$\begin{aligned}&=2^\alpha P_t\sum_k\frac{1}{[k(d+1)]^\alpha}\\&\quad\times\left(\sum_{l=1}^{k}|\mathcal{T}_l|-\sum_{l=1}^{k-1}|\mathcal{T}_l|\right)\end{aligned} \tag{14b}$$

$$=\frac{2^\alpha P_t}{(d+1)^\alpha}\sum_k\left[\frac{1}{k^\alpha}-\frac{1}{(k+1)^\alpha}\right]\sum_{l=1}^{k}|\mathcal{T}_l| \tag{14c}$$

$$\le\frac{2^\alpha P_t}{(d+1)^\alpha}\sum_{k=1}^{\infty}\alpha k^{-\alpha-1}\frac{48}{C_t^2}\frac{1}{(d+1)^2}(k+1)^2 \tag{14d}$$

$$=\frac{192\alpha 2^\alpha P_t}{C_t^2}\frac{1}{(d+1)^{\alpha+2}}\sum_{k=1}^{\infty}k^{1-\alpha} \tag{14e}$$

$$\le\frac{192\alpha 2^{\alpha-1}c_1}{(\alpha-2)C_t^2} \tag{14f}$$

$$\le\frac{N_0}{2}. \tag{14g}$$

(14d) utilizes both (13) and the fact that $(1/k^\alpha)-(1/(k+1)^\alpha) \le \alpha k^{-\alpha-1}$. (14f) utilizes the power management $P_t = c_1(1+d)^\alpha$ while (14g) follows from (7a). Next, we endeavor to bound the interference from other receivers' artificial noise. We have:

$$|X_q-X_j| \ge |X_p-X_i|-2d \ge \frac{C_t}{2}(1+d)^2-2d \ge \frac{C_t}{4}(1+d)^2. \tag{15}$$

Hence, the disks $D(X_j,(C_t/8)(1+d)^2), j \in \mathcal{R}$ are disjoint. Similarly, we also divide the set $\mathcal{R}\backslash\{j\}$ into following subsets $\mathcal{R}_k, 1 \le k \le (8\sqrt{2n}/C_t(1+d)^2)$:

$$\begin{aligned}\mathcal{R}_k = \Big\{q|k\times\frac{C_t}{8}(1+d)^2 &\le |X_p-X_j| < (k+1)\\&\times\frac{C_t}{8}(1+d)^2, q\in\mathcal{R}, q\ne j\Big\}\end{aligned} \tag{16a}$$

$$\mathcal{R}\backslash\{j\} = \bigcup_{k=1}^{\frac{8\sqrt{2n}}{C_t(1+d)^2}}\mathcal{R}_k. \tag{16b}$$

Each receiver consumes a radio resource of a disk area, hence we obtain:

$$\frac{1}{3}\pi\left[\frac{C_t}{8}(1+d)^2\right]^2\sum_{l=1}^{k}|\mathcal{R}_l| \le \pi\left[(k+1)\frac{C_r}{8}(1+d)^2\right]^2 \tag{17}$$

which could be simplified to:

$$\sum_{l=1}^{k}|\mathcal{R}_l| \le 3(k+1)^2. \tag{18}$$

Thus, the interference at the receiver X_j caused by the artificial noise generated by other receivers can be bounded as follows:

$$I_r(X_j) \le \sum_k\frac{P_r}{\left[\frac{kC_t}{8}(1+d)^2\right]^\alpha}|\mathcal{R}_k| \tag{19a}$$

$$\begin{aligned}&\le\frac{8^\alpha}{C_t^\alpha}\frac{P_r}{(1+d)^{2\alpha}}\sum_k\frac{1}{k^\alpha}\\&\quad\times\left(\sum_{l=1}^{k}|\mathcal{R}_l|-\sum_{l=1}^{k-1}|\mathcal{R}_l|\right)\end{aligned} \tag{19b}$$

$$\begin{aligned}&=\frac{8^\alpha}{C_t^\alpha}\frac{P_r}{(1+d)^{2\alpha}}\sum_k\\&\quad\times\left[\frac{1}{k^\alpha}-\frac{1}{(k+1)^\alpha}\right]\sum_{l=1}^{k}|\mathcal{R}_l|\end{aligned} \tag{19c}$$

$$\le\frac{8^\alpha}{C_t^\alpha}\frac{P_r}{(1+d)^{2\alpha}}\sum_{k=1}^{\infty}\alpha k^{-\alpha-1}\cdot 3(k+1)^2 \tag{19d}$$

$$\le\frac{12\alpha 2^{4\alpha-1}}{C_t^\alpha(\alpha-2)}c_2 \le \frac{N_0}{2}. \tag{19e}$$

The last step (19e) utilizes the power management $P_r = c_2(1+d)^{2\alpha}$ and (7b). Thereby, the SINR at X_j can be bounded as:

$$\mathrm{SINR}(X_j) \ge \frac{c_1}{N_0+\frac{N_0}{2}+\frac{N_0}{2}} = \gamma_r. \tag{20}$$

For any eavesdropper e, whose position is denoted as Y_e, the interference at it is at least:

$$I_e \ge \frac{P_r}{(|X_j-Y_e|+1)^\alpha} \ge \frac{P_r}{(1+d+|Y_e-X_i|)^\alpha}. \tag{21}$$

Hence, the SINR at e is at most:

$$\mathrm{SINR}(Y_e) \le, \frac{\frac{2^\alpha P_t}{(1+|Y_e-X_i|)^\alpha}}{\frac{P_r}{(1+d+|Y_e-X_i|)^\alpha}} \tag{22a}$$

$$=\frac{2^\alpha P_t}{P_r}\left(1+\frac{d}{1+|Y_e-X_i|}\right)^\alpha \tag{22b}$$

$$\le\frac{2^\alpha P_t}{P_r}(1+d)^\alpha \tag{22c}$$

$$=\frac{2^\alpha c_1}{c_2} = \gamma_e. \tag{22d}$$

Thus, SINR constraint at receivers and eavesdroppers are both satisfied, indicating that the state is feasible under the secure physical model $\mathcal{PH}(\gamma_r,\gamma_e)$.

We further assert in the next theorem that, under the previously presented four assumptions, the secure physical model implies the secure protocol model, which is converse to Theorem 5.1.

5) Theorem 5.2: For any two positive constants γ_r, γ_e satisfying Assumption 4, there exists a positive constant C_t such that, provided Assumption 1, 2, and 3 all hold, if a state is feasible under the secure physical model $\mathcal{PH}(\gamma_r, \gamma_e)$, then it must be feasible under the secure protocol model $\mathcal{PR}(C_t)$, a.a.s.[3].

Proof: Given a state satisfying $\mathcal{PH}(\gamma_r, \gamma_e)$ and the four assumptions, we first show that all its links are unicast, i.e., one transmitter has only one receiver.

Consider an arbitrary active transmitter X_i. Suppose it has multiple receivers $X_{j_1}, X_{j_2}, \ldots, X_{j_m}$ where $m \geq 2$. Without loss of generality, we let $|X_{j_1} - X_{j_2}|$ be the minimum distance between any two receivers of X_i, i.e., $\forall 1 \leq k, l \leq m, k \neq l$, we have $|X_{j_k} - X_{j_l}| \geq |X_{j_1} - X_{j_2}|$. We further assume that X_{j_2} is nearer to X_i than X_{j_1} does, i.e., $|X_{j_2} - X_i| \leq |X_{j_1} - X_i|$. Then, for any other receiver of X_i, say X_{j_3}, we have:

$$|X_{j_3} - X_{j_1}| \geq |X_{j_2} - X_{j_1}| = 2\left|X_{j_1} - \frac{X_{j_1} + X_{j_2}}{2}\right|. \tag{23}$$

Hence,

$$\begin{aligned} &\left|X_{j_3} - \frac{X_{j_1} + X_{j_2}}{2}\right| \\ &\quad \geq |X_{j_3} - X_{j_1}| - \left|X_{j_1} - \frac{X_{j_1} + X_{j_2}}{2}\right| && \text{(24a)} \\ &\quad \geq \left|X_{j_1} - \frac{X_{j_1} + X_{j_2}}{2}\right|. && \text{(24b)} \end{aligned}$$

Furthermore,

$$\begin{aligned} &2\left|X_{j_3} - \frac{X_{j_1} + X_{j_2}}{2}\right| \\ &\quad \geq \left|X_{j_1} - \frac{X_{j_1} + X_{j_2}}{2}\right| + \left|X_{j_3} - \frac{X_{j_1} + X_{j_2}}{2}\right| && \text{(25a)} \\ &\quad \geq |X_{j_1} - X_{j_3}|. && \text{(25b)} \end{aligned}$$

Recall that the density of the eavesdroppers is $n^{\nu - 1}$, where $\nu > 1$. So, asymptotically almost surely, for every point in the network area, there is an eavesdropper within a distance of $o(1)$. Hence, there exists an eavesdropper e such that $|Y_e - (X_{j_1} + X_{j_2}/2)| \leq 1$. Recalling the definition of the path loss function $l(\cdot)$, we have:

$$\begin{aligned} l(|X_{j_1} - X_{j_3}|) &\geq l\left(2\left|X_{j_3} - \frac{X_{j_1} + X_{j_2}}{2}\right|\right) && \text{(26a)} \\ &\geq 2^{-\alpha} l\left(\left|X_{j_3} - \frac{X_{j_1} + X_{j_2}}{2}\right|\right) && \text{(26b)} \\ &\geq 2^{-\alpha} l(|X_{j_3} - Y_e| + 1) && \text{(26c)} \\ &\geq 4^{-\alpha} l(|X_{j_3} - Y_e|). && \text{(26d)} \end{aligned}$$

Due to the arbitrariness of X_{j_3}, we actually have:

$$\sum_{k=3}^{m} l(|X_{j_k} - Y_e|) \leq 4^{\alpha} \sum_{k=3}^{m} l(|X_{j_k} - X_{j_1}|). \tag{27}$$

Besides, we can easily show that $l(|X_{j_2} - Y_e|) \leq 4^{\alpha} l(|X_{j_1} - X_{j_2}|)$. Adding it onto (27) yields:

$$\sum_{k=2}^{m} l(|X_{j_k} - Y_e|) \leq 4^{\alpha} \sum_{k=2}^{m} l(|X_{j_k} - X_{j_1}|). \tag{28}$$

Because $l(|X_{j_1} - Y_e|) \leq 4^{\alpha} l(|X_{j_1} - X_{j_2}|)$, we have:

$$\sum_{k=1}^{m} l(|X_{j_k} - Y_e|) \leq 2 \cdot 4^{\alpha} \sum_{k=2}^{m} l(|X_{j_k} - X_{j_1}|). \tag{29}$$

According to Assumption 2, other simultaneous transmitters and their intended receivers are far away from X_i and $X_{j_k}, 1 \leq k \leq m$, i.e., for eavesdroppers Y_e and the receivers of X_i, the interference caused by X_i's receivers dominates. So, we just ignore the interference from other nodes. A rigorous proof of the above argument is nothing more than some tedious bounding using Assumption 2 and is omitted here. From the above analysis and (29), we obtain $I(Y_e) \leq 2 \cdot 4^{\alpha} I(X_{j_1})$. Furthermore,

$$\begin{aligned} |Y_e - X_i| \leq &\left|Y_e - \frac{X_{j_1} + X_{j_2}}{2}\right| \\ &+ \left|\frac{X_{j_1} + X_{j_2}}{2} - X_i\right| && \text{(30a)} \\ \leq &\, 1 + \frac{1}{2}|X_{j_1} - X_i| + \frac{1}{2}|X_{j_2} - X_i| && \text{(30b)} \\ \leq &\, 1 + |X_{j_1} - X_i|. && \text{(30c)} \end{aligned}$$

Hence, $l(|Y_e - X_i|) \geq 2^{-\alpha} l(|X_{j_1} - X_i|)$. So, we have:

$$\gamma_e \geq \mathrm{SINR}(Y_e) \geq 2^{-3\alpha - 1}\mathrm{SINR}(X_{j_1}) \geq 2^{-3\alpha - 1}\gamma_r. \tag{31}$$

This contradicts to Assumption 4, indicating that every X_i cannot have more than 1 receiver, i.e., every link should be unicast.

Now, we start to prove (6) in the definition of the secure protocol model. Consider one arbitrary unicast link pair (X_i, X_j). Let X_p be the nearest simultaneously active transmitter to X_i and X_q be the intended receiver of X_p. According to Assumption 1, we know $|X_p - X_i| \leq 2d^*$. As previously mentioned, there should be an eavesdropper $Y_{e'}$ such that $|Y_{e'} - X_i| \leq 1$, a.a.s.. Hence,

$$|X_p - Y_{e'}| \geq |X_p - X_i| - |X_i - Y_{e'}| \geq d^* - 1 \geq \frac{1}{2}d^* \tag{32}$$

i.e., every transmitter other than X_i is at least $(1/2)d^*$ away from eavesdropper $Y_{e'}$. We also know that the distance between any two transmitters is at least d^*. Hence, the interference at eavesdropper $Y_{e'}$ from other simultaneously active transmitters is at most $I_t(Y_{e'}) \leq O((P_t/(d^*)^{\alpha}))$. The strict proof of this statement is similar to that of Theorem 5.1 and is omitted here. To bound the interference from receivers other than X_j, we have:

$$|X_q - Y_{e'}| \geq |X_i - X_p| - |X_p - X_q| - 1 \geq \frac{1}{2}d^* \tag{33a}$$

$$|X_q - X_j| \geq |X_p - X_i| - |X_p - X_q| - |X_i - X_j| \geq \frac{1}{2}d^* \tag{33b}$$

where we utilize Assumption 2. Hence, the interference at eavesdropper $Y_{e'}$ from receivers other than X_j is at most $O((P_r/(d^*)^{\alpha}))$ while the interference from X_j is at most $O((P_r/(|X_i - X_j| + 1)^{\alpha}))$. Thus, the total interference at eavesdropper e is at most:

$$I(Y_{e'}) \leq O\left(\frac{P_t}{(d^*)^{\alpha}} + \frac{P_r}{(|X_i - X_j| + 1)^{\alpha}}\right). \tag{34}$$

[3] a.a.s. stands for “asymptotically almost surely.” We say an event series A_n happens asymptotically almost surely if $\lim_{n \to \infty} \Pr(A_n) = 1$.

Since the current state is feasible under the secure physical model $\mathcal{PH}(\gamma_r, \gamma_e)$, at the eavesdropper $Y_{e'}$, we have:

$$\frac{P_t}{N_0 + O\left(\frac{P_t}{(d^*)^\alpha} + \frac{P_r}{(|X_i - X_j| + 1)^\alpha}\right)} \leq \gamma_e. \tag{35}$$

We also know that $P_t \geq N_0 \gamma_r$. Note that the notation $O(\cdot)$ only contains some constants terms related to α. Hence, under Assumption 2 and Assumption 4, the third (last) term of the denominator must dominate the value of the denominator in (35). Thereby, (35) can be simplified to:

$$\frac{P_t}{P_r} \leq O\left(\frac{1}{(|X_i - X_j| + 1)^\alpha}\right) \tag{36}$$

where we absorb the term γ_e into the notation $O(\cdot)$.

Next, we turn to the interference at the receiver X_j. We have:

$$|X_q - X_j| \leq |X_p - X_i| + |X_p - X_q| + |X_i - X_j| \leq 3d^*. \tag{37}$$

Thus, the interference at the receiver X_j is at least $I(X_j) \geq (P_r/(3d^*)^\alpha)$. Hence,

$$\frac{\frac{2^\alpha P_t}{(|X_i - X_j| + 1)^\alpha}}{\frac{P_r}{(3d^*)^\alpha}} \geq \gamma_r \tag{38}$$

which is equivalent to:

$$\frac{P_t}{P_r} \geq \Omega\left(\left(\frac{|X_i - X_j| + 1}{d^*}\right)^\alpha\right). \tag{39}$$

Combining (36) and (39), we obtain:

$$d^* \geq \Omega\left((|X_i - X_j| + 1)^2\right). \tag{40}$$

Recall that d^* is the smallest distance between any two transmitters. By choosing the positive constant C_t small enough, we have:

$$|X_p - X_i| \geq C_t(|X_i - X_j| + 1)^2. \tag{41}$$

Thus, we conclude that the current state is feasible under the secure protocol model $\mathcal{PR}(C_t)$.

6) Remark 5.2: Theorem 5.1 together with Theorem 5.2 establishes equivalence between the secure physical model and the proposed secure protocol model under the four technical assumptions. By equivalence, we mean that the capacity delay scaling law results under the two models are the same. Actually, by using Theorems 5.1 and 5.2, we can easily convert the capacity scaling results obtained under the secure protocol model into results under the secure physical model. This works as follows. Suppose under any secure protocol model $\mathcal{PR}(C_t)$, we could always find a feasible scheduling scheme such that the per-node throughput is λ (this is exactly what we will do in Section VII). According to Theorem 5.1, for any given secure physical model $\mathcal{PH}(\gamma_r, \gamma_e)$ we can find C_t large enough such that $\mathcal{PR}(C_t) \subseteq \mathcal{PH}(\gamma_r, \gamma_e)$. Then the aforementioned λ-throughput scheduling scheme feasible under $\mathcal{PR}(C_t)$ turns out to be also feasible under $\mathcal{PH}(\gamma_r, \gamma_e)$. So, we can conclude that any secure physical model could reach a throughput of λ. Similarly, if we have got an upper bound for the throughput capacity under the secure protocol model (Section VI), by using Theorem 5.2, we could assert that the upper bound also holds for the secure physical model.

7) Remark 5.3: We can see from the secure protocol model that the secrecy constraint does have great impacts on network behaviors. Compared to the insecure protocol model presented in [13], the secure protocol model is clearly stricter. This will definitely degenerate the network performance such as capacity and delay, which we will discuss quantitatively in Section VI and Section VII. An interesting thing is that the secure protocol model is independent of the eavesdropper density $\psi_e = n^{\nu-1}$, as long as it is much larger than one, i.e., $\psi_e = \omega(1)$ or $\nu > 1$. This indicates that adding more eavesdroppers into the network will not further degenerate the network capacity.

VI. An Upper Bound on the Secrecy Capacity-Delay Tradeoff

In this section, we derive the upper bound for the network capacity under certain secrecy and delay constraints in MANETs, by using the proposed secure protocol model $\mathcal{PR}(C_t)$. Since the secure protocol model is shown to be equivalent to the secure physical model if the four technical assumptions hold, the derived upper bound in this section is also suitable for a majority of feasible schemes (or more precisely, schemes satisfying the four technical assumptions) under the secure physical model. In Section VII, we present a capacity achieving (except for poly-log gap) scheme satisfying those assumptions. This indicates that the upper bound derived in this section is essentially tight.

Denote D_b the delay of bit b, i.e., the number of time slots it takes for bit b to reach its destination after it enters into the network system. Denote L_b the capture range of bit b, i.e., the distance between the last mobile relay of bit b and the final destination in the final time slot of bit b[4]. Denote R_b the number of duplicates of bit b, i.e., the number of mobile relays holding bit b before it reaches the destination. Since the legitimate nodes move according to an i.i.d. pattern, there is a tradeoff between D_b, L_b and R_b, which is stated as the following lemma. This lemma has been proved in [16].

1) Lemma 6.1: The following inequality holds for any causal scheduling policy:

$$\tilde{c}\mathsf{E}(D_b)\log n \geq \frac{1}{\left(\frac{\mathsf{E}(L_b)}{\sqrt{n}} + \frac{1}{n^2}\right)^2 \mathsf{E}(R_b)} \tag{42}$$

where $\tilde{c}$ is a positive constant.

Under the secure protocol model $\mathcal{PR}(C_t)$, every transmission is unicast. Hence, to make R_b duplicates in the network, we need R_b transmissions. According to (6), every transmission will consume at least $\Omega(1)$ area of radio resource. Thus, in a long period of time, say T time slots, the total area of radio resource consumed by duplication is at least $\Omega(\sum_{b=1}^{\lambda nT} R_b)$, where λ is the per-node throughput. On the other hand, because the capture range is L_b and only one-hop transmission is allowed in a

[4] By final time slot, we mean the time slot when the desired destination gets bit b.

time slot (fast mobility), the capture phase of bit b will consume $\Omega(L_b^4)$ area of radio resource. The reason is that, according to (6), disks centered at simultaneously active transmitters with radius $\Theta(L_b^2)$ must be disjoint. Meanwhile, the total radio resource of T time slots is an area of nWT. From the above analysis, we obtain the following lemma.

2) Lemma 6.2: The following inequality holds for any causal scheduling policy:

$$\Omega\left(\sum_{b=1}^{\lambda nT} R_b\right) + \Omega\left(\sum_{b=1}^{\lambda nT} L_b^4\right) \leq O(nWT). \tag{43}$$

Now, we are ready to derive the upper bound of the secure capacity for MANETs. We assume that $D = O(n)$ since a delay constraint of $\Theta(n)$ is already sufficient to ensure a constant per-node throughput, as we will see later. Hence, a weaker delay constraint $D = \Omega(n)$ cannot improve the capacity any more and is ignored.

3) Theorem 6.1: Under the secure protocol model, if $D = O(n)$, the following upper bound holds for any causal scheduling policy:

$$\lambda = O\left(W\left(\frac{D}{n}\right)^{\frac{2}{3}} \log n\right). \tag{44}$$

Proof: (42) in Lemma 6.1 can be rewritten as:

$$\mathsf{E}(R_b) \geq \frac{1}{\log n} \frac{1}{\left(\frac{\mathsf{E}(L_b)}{\sqrt{n}} + \frac{1}{n^2}\right)^2} \frac{1}{\mathsf{E}(D_b)} \tag{45}$$

where we omit the constant c_1 since this will not change our result in order sense. Summing over all the bits and invoking Cauchy–Schwartz inequality twice yields:

$$\sum_{b=1}^{\lambda nT} \mathsf{E}(R_b) \geq \frac{1}{\log n} \sum_{b=1}^{\lambda nT} \frac{1}{\left(\frac{\mathsf{E}(L_b)}{\sqrt{n}} + \frac{1}{n^2}\right)^2} \frac{1}{\mathsf{E}(D_b)} \tag{46a}$$

$$\geq \frac{1}{\log n} \frac{\left(\sum_{b=1}^{\lambda nT} \frac{1}{\frac{\mathsf{E}(L_b)}{\sqrt{n}} + \frac{1}{n^2}}\right)^2}{\sum_{b=1}^{\lambda nT} \mathsf{E}(D_b)} \tag{46b}$$

$$\geq \frac{\lambda^4 n^4 T^4}{\log n} \frac{1}{\sum_{b=1}^{\lambda nT} \mathsf{E}(D_b)} \times \left[\frac{1}{\sum_{b=1}^{\lambda nT} \left(\frac{\mathsf{E}(L_b)}{\sqrt{n}} + \frac{1}{n^2}\right)}\right]^2. \tag{46c}$$

From (43) in Lemma 6.2, we obtain:

$$\sum_{b=1}^{\lambda nT} \mathsf{E}(R_b) + \sum_{b=1}^{\lambda nT} \mathsf{E}\left(L_b^4\right) \leq O(nWT). \tag{47}$$

Bringing (46c) into (47) yields:

$$\frac{\lambda^4 n^4 T^4}{\log n} \frac{1}{\sum_{b=1}^{\lambda nT} \mathsf{E}(D_b)} \frac{1}{\left[\sum_{b=1}^{\lambda nT} \left(\frac{\mathsf{E}(L_b)}{\sqrt{n}} + \frac{1}{n^2}\right)\right]^2} + \sum_{b=1}^{\lambda nT} \mathsf{E}\left(L_b^4\right) \leq O(nWT). \tag{48}$$

Now, there are two cases we need to consider.

4) Case I: If $\sum_{b=1}^{\lambda nT} \geq (\lambda T/\sqrt{n})$, then (48) can be rewritten as:

$$\frac{\lambda^4 n^4 T^4}{\log n} \frac{1}{\sum_{b=1}^{\lambda nT} \mathsf{E}(D_b)} \frac{n}{\left[\sum_{b=1}^{\lambda nT} \mathsf{E}(L_b)\right]^2} + \sum_{b=1}^{\lambda nT} \mathsf{E}\left(L_b^4\right) \leq O(nWT). \tag{49}$$

Since $f(x) = x^4$ is a convex function on $\mathbb{R}_+$, by applying Jenson's inequality, we have:

$$\sum_{b=1}^{\lambda nT} \mathsf{E}\left(L_b^4\right) \geq \sum_{b=1}^{\lambda nT} \left[\mathsf{E}(L_b)\right]^4. \tag{50}$$

Invoking Holder's inequality yields:

$$\left\{\sum_{b=1}^{\lambda nT} \left[\mathsf{E}(L_b)\right]^4\right\}^{\frac{1}{4}} \left(\sum_{b=1}^{\lambda nT} 1\right)^{\frac{3}{4}} \geq \sum_{b=1}^{\lambda nT} \mathsf{E}(L_b) \tag{51}$$

which could be simplified to:

$$\sum_{b=1}^{\lambda nT} [\mathsf{E}(L_b)]^4 \geq (\lambda nT)^{-3} \left[\sum_{b=1}^{\lambda nT} \mathsf{E}(L_b)\right]^4. \tag{52}$$

Bringing (50) and (52) into (49), we obtain:

$$\frac{\lambda^4 n^4 T^4}{\log n} \frac{1}{\sum_{b=1}^{\lambda nT} \mathsf{E}(D_b)} \frac{n}{\left[\sum_{b=1}^{\lambda nT} \mathsf{E}(L_b)\right]^2} + (\lambda nT)^{-3} \left[\sum_{b=1}^{\lambda nT} \mathsf{E}(L_b)\right]^4 \leq O(nWT) \tag{53}$$

which could be rewritten as:

$$\left\{\left[\frac{\lambda^4 n^4 T^4}{\log n} \frac{n}{\sum_{b=1}^{\lambda nT} \mathsf{E}(D_b)}\right]^{\frac{2}{3}} \frac{1}{\left[\sum_{b=1}^{\lambda nT} \mathsf{E}(L_b)\right]^{\frac{4}{3}}}\right\}^{\frac{3}{2}} + \left\{(\lambda nT)^{-1} \left[\sum_{b=1}^{\lambda nT} \mathsf{E}(L_b)\right]^{\frac{4}{3}}\right\}^3 \leq O(nWT). \tag{54}$$

Exploiting Young's inequality in (54) yields:

$$\frac{(\lambda nT)^{\frac{5}{3}}}{(\log n)^{\frac{2}{3}}} \frac{n^{\frac{2}{3}}}{\left[\sum_{b=1}^{\lambda nT} \mathsf{E}(D_b)\right]^{\frac{2}{3}}} \leq O(nWT). \tag{55}$$

Noting that $D \geq \mathsf{E}(D_b)$, we could simplify (55) as follows:

$$\lambda \leq O\left(W\left(\frac{D \log n}{n}\right)^{\frac{2}{3}}\right). \tag{56}$$

5) Case II: If $\sum_{b=1}^{\lambda nT} \mathsf{E}(L_b) < (\lambda T/\sqrt{n})$, then (48) can be rewritten as:

$$\frac{\lambda^4 n^4 T^4}{\log n} \frac{1}{\lambda nTD} \frac{1}{\left(\frac{1}{n^2} \cdot \lambda nT\right)^2} \leq O(nWT) \tag{57}$$

which is further simplified to:

$$\lambda \leq O(WDn^{-4} \log n). \tag{58}$$

Combining (56)(58) and noticing that $D = O(n)$, we always have:

$$\lambda \leq O\left(W\left(\frac{D}{n}\right)^{\frac{2}{3}} \log n\right). \tag{59}$$

We thus conclude the proof.

6) Remark 6.1: Because, under the four assumptions, the secure protocol model is equivalent to the secure physical model, the result in Theorem 6.1 applies to the latter immediately under the four assumptions. This is exactly a major result we have mentioned in (3) in Section IV. From the theorem, we observe that the upper bound is independent of the eavesdropper density ψ_e. This is not surprising since the secure protocol model is also independent of ψ_e.

VII. Capacity Achieving Scheme

In this section, under the secure protocol model, assuming that $D = \Omega(n^{2/5}(\log n)^{21/5})$ and $D = O(n)$, we present and analyze an efficient scheme which can obtain the capacity upper bound derived in Theorem 6.1 up to poly-log factors.

A. Scheme

In this subsection, we present the capacity-achieving scheme explicitly. In order to achieve the upper bound, we require that the inequalities involved in the derivation of Theorem 6.1 all hold with equality. This gives the best choice for R_b and L_b. Specifically, we choose a common number of duplications R and common capture range L for all the bits as follows:

$$R = \Theta\left(\left(\frac{n}{D}\right)^{\frac{2}{3}}\right), \ L = \Theta\left(\left(\frac{n}{D}\right)^{\frac{1}{6}} \log n\right). \tag{60}$$

In (60), we add log factor so as to ensure that the proposed scheme is successful asymptotically almost surely. The scheme consists of two phases: duplication phase and capture phase. In duplication phase, we schedule source-to-relay transmissions to guarantee that each bit is duplicated $\Theta(R)$ times. In capture phase, we arrange relay-to-destination transmissions to guarantee that each bit generated in the previous duplication phase can be delivered to its desired destination successfully asymptotically almost surely. The duplication phase consists of $\Theta((D/(\log n)^7))$ time slots while the capture phase consists of $\Theta(D)$ time slots. Thus, if we can schedule each bit generated in the duplication phase to reach its destination in the next capture phase, the delay of each bit is upper bounded by $O(D)$. Now, we present the detailed scheme as follows.

1) **Duplication Phase**: Tessellate the network area into small squares with area $7 \log n$. We call those small squares *duplication cells*. Then, asymptotically almost surely, there are $\Theta(\log n)$ legitimate nodes in each duplication cell. Under the secure protocol model, in order to avoid interference, we invoke traditional TDMA scheme: simultaneously active duplication cells are at least $\Theta((\log n)^2)$ away as (6) indicates. Hence, each duplication cell could be active for $(1/(\log n)^4)$ amount of time in each slot. In each time slot, when a duplication cell is scheduled to be active, every node[5] within that duplication cell takes turns to transmit bits generated by it to a relay node inside this duplication cell. Thus, every node could transmit data for $(1/(\log n)^5)$ amount of time in each slot. So, each node could send out $\Theta((W/(\log n)^5))$ bits in each time slot. We call such $\Theta((W/(\log n)^5))$ bits a packet in the following. We could guarantee that, during the duplication phase, at different time slot, each source node can transmit packets to different relays, i.e., after the duplication phase, each source has $\Theta((D/(\log n)^7))$ relays. We will formally prove this in the next subsection. In every R slots, each node keeps transmitting the same packet to its relays. And in the next R slots, it transmits another packet. Hence, every node transmits $\Theta((D/(\log n)^7/R)) = \Theta(D^{5/3}n^{-(2/3)}(\log n)^{-7})$ packets in the duplication phase. In all, after the duplication phase, each source node[6] has successfully sent out $\Theta(D^{5/3}n^{-(2/3)}(\log n)^{-7})$ packets with each packet owned by $\Theta(R)$ relays. Then, the network moves to the capture phase.

2) **Capture Phase**: This phase is illustrated in Fig. 1 and described as follows. Tessellate the network area into squares with side length L^2. We call these squares super-cells. Further tessellate each super-cell into small squares with side length L. We call these small squares cells. In the capture phase, we only allow transmission inside each cell, i.e., the transmitter and receiver must lie in the same cell. We regularly select $\Theta(1)$ percent of the super-cells as *feasible super-cells* such that different feasible super-cells are separated for at least $\Theta(L^2)$ away. Hence, under the secure protocol model, transmissions at different feasible super-cells will not interfere with each other. Throughout the capture phase, we only allow transmissions inside those feasible super-cells and in each super-cell, we only allow one transmitter-receiver pair. Thereby, the scheme accords with the secure protocol model. Inside each cell, if a node has a packet destined to another node, we call this packet a *deliverable packet*. In each time slot, for each feasible super-cell: 1) if there are one or two deliverable packets inside the super-cell, then the packets are delivered; 2) if there are at least three deliverable packets inside the super-cell, randomly choose one to be delivered; 3) if no deliverable packet exists in the super-cell, we still schedule one meaningless transmission[7] inside an arbitrary cell in that super-cell (we do this so as to assure that Assumption 1 always holds). Keep doing so until the D-slot-long capture phase ends.

B. Analysis

In this subsection, we analyze the feasibility and the throughput of the proposed scheme. Denote A an arbitrary legitimate node. We have claimed that in different time slots

[5] In the following, we use the notation “node” to denote legitimate node.

[6] Since we consider unicast, each legitimate node is a source node.

[7] The transmission does not carry any information and its only goal is to suppress other eavesdroppers' channels.

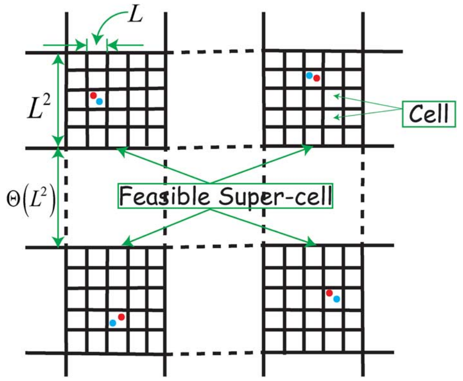


Fig. 1. An illustration of the capture phase in the proposed capacity achieving scheme. The small squares with side length L are called cells while the big squares with side length L^2 are called super-cells. $\Theta(1)$ percent of the super-cells are feasible super-cells, which are located regularly in the network. Each pair of red circle and blue circle depicted in the cell is an active link. In the capture phase, as the figure indicates, we only allow transmissions inside the feasible super-cell and in a single feasible super-cell, only one transmission can occur. The transmitter-receiver pair must reside in the same cell.

of the duplication phase, node A is able to transmit packets to different relay nodes. Now we formally prove that node A does have this opportunity. Denote the starting time slot of the duplication phase as time slot 0. At the beginning of time slot k, if node A has already transmitted packets to k different relay nodes, where $0 \leq k \leq \Theta(D/(\log n)^7)$, then the probability that none of the remaining $n - k - 1$ nodes is located in the same cell as node A is $(1 - (7\log n/n))^{n-k-1}$. Hence, the probability that node A can always find a new relay in each time slot throughout the entire duplication phase is[8]

$$\prod_{k=1}^{\Theta\left(\frac{D}{(\log n)^7}\right)} \left[1 - \left(1 - \frac{7\log n}{n}\right)^{n-k-1}\right] \tag{61a}$$

$$\geq \prod_{k=1}^{\frac{D}{(\log n)^7}} \left[1 - \exp\left(-\frac{7(n-k)\log n}{n}\right)\right] \tag{61b}$$

$$\geq \prod_{k=1}^{\frac{D}{(\log n)^7}} \left[1 - n^{-7\left(1-\frac{k}{n}\right)}\right] \tag{61c}$$

$$\geq \left[1 - n^{-7\left(1-\frac{D}{n(\log n)^7}\right)}\right]^{\frac{D}{(\log n)^7}}. \tag{61d}$$

Therefore, the probability that node A fails to find a new relay in some time slot in the duplication phase is no more than:

$$1 - \left[1 - n^{-7\left(1-\frac{D}{n(\log n)^7}\right)}\right]^{\frac{D}{(\log n)^7}} \tag{62a}$$

$$\leq \frac{D}{(\log n)^7} n^{-7\left(1-\frac{D}{n(\log n)^7}\right)} \tag{62b}$$

$$\leq n^{-2.5}. \tag{62c}$$

Thereby, the probability that there exists a node such that it fails to find a new relay in some time slot in the duplication phase is no more than $n \times n^{-2.5} = n^{-1.5} \to 0$, i.e., every node is able to transmit to different relay nodes in different time slots in the duplication phase a.a.s.. Thus, the duplication phase is successfully a.a.s. and every source node sends out $\Theta(D^{5/3}n^{-(2/3)}(\log n)^{-7})$ packets with each packet owned by $\Theta(R)$ relays. There are in total $\Theta(D/(\log n)^7)$ relays associated with one source node and these relays are different from each other.

Now we turn to the capture phase. Denote the $\Theta(D^{5/3}n^{-(2/3)}(\log n)^{-7})$ packets sent out by node i as $\{(i,1),(i,2),\ldots,(i,D^{5/3}n^{-(2/3)}(\log n)^{-7})\}$. Without loss of generality, we assume that the destination node of source node i is node $i+1$. Denote the super-cell with node $i+1$ located in super-cell $\mathcal{S}$. Denote the cell with node $i+1$ located in cell $\mathcal{C}$. Consider one arbitrary packet of node i, say (i,k), where $1 \leq k \leq D^{5/3}n^{-(2/3)}(\log n)^{-7}$. Consider an arbitrary fixed time slot t in the capture phase. Denote $\mathcal{D}_{(i,k)}[t]$ the event that the packet (i,k) is delivered at time slot t. Then, $\mathcal{D}_{(i,k)}[t]$ must occur if the following two conditions hold.

1) One duplicate packet of (i,k) is a deliverable packet. None of Other duplicate packets of (i,s), $1 \leq s \leq D^{5/3}n^{-(2/3)}(\log n)^{-7}$, is deliverable. Denote $\mathcal{D}^1_{(i,k)}[t]$ this event. Assume the mentioned deliverable duplicate packet is (i,k,j), i.e., node j is the relay node which contains the duplicate packet.
2) Except one deliverable packet from node j to node $i+1$ and one possible deliverable packet from node $i+1$ to node j, there is no other deliverable packet inside the super-cell $\mathcal{S}$. Let $\mathcal{D}^2_{(i,k)}[t]$ denote this event.

Note that a duplicate packet of (i,k) is deliverable if and only if it is located in the cell $\mathcal{C}$. Since there are in total R duplicate packet of (i,k) and $(D/(\log n)^7)$ duplicate packets sent out from node i, we have:

$$\mathsf{Pr}\left(\mathcal{D}^1_{(i,k)}[t]\right) = \frac{RL^2}{n}\left(1 - \frac{L^2}{n}\right)^{D(\log n)^{-7}} \tag{63a}$$

$$= \frac{(\log n)^2}{D}\left(1 - n^{-\frac{2}{3}}D^{-\frac{1}{3}}(\log n)^2\right)^{D(\log n)^{-7}} \tag{63b}$$

$$= \frac{(\log n)^2}{D}. \tag{63c}$$

In the derivation, we omit the constant terms since they will not influence our scaling results. The number of duplicate packets which are destined to node j is $(D/(\log n)^7)$. Denote $\mathcal{E}_1$ the event that besides the possible duplicate packet owned by node $i+1$, at least one duplicate packet destined to j is deliverable. We have:

$$\mathsf{Pr}(\mathcal{E}_1) = 1 - \left(1 - \frac{L^2}{n}\right)^{\frac{D}{(\log n)^7}} \tag{64a}$$

$$= D^{\frac{2}{3}}n^{-\frac{2}{3}}(\log n)^{-5} \to 0. \tag{64b}$$

Consider one arbitrary node p, where $1 \leq p \leq n, p \neq i+1, p \neq j$. Denote $\mathcal{E}^p_2$ the event that node p is within the super-cell $\mathcal{S}$. Then,

$$\mathsf{Pr}\left(\mathcal{E}^p_2\right) = \Theta\left(\frac{L^4}{n}\right) = \Theta\left(n^{-\frac{1}{3}}D^{-\frac{2}{3}}(\log n)^4\right). \tag{65}$$

[8] In the derivation, we may omit some constant factors which do not affect the scaling results

Denote $\mathcal{E}_3^p$ the event that there is at least one deliverable packet destined to node p. Thus,

$$\mathsf{Pr}\left(\mathcal{E}_3^p|\mathcal{E}_2^p\right) = 1 - \left(1 - \frac{L^2}{n}\right)^{\frac{D}{(\log n)^7}} = D^{\frac{2}{3}} n^{-\frac{2}{3}} (\log n)^{-5}. \tag{66}$$

Hence, combining (65) and (66) yields:

$$\mathsf{Pr}\left(\mathcal{E}_2^p \bigcap \mathcal{E}_3^p\right) = n^{-1}(\log n)^{-1}. \tag{67}$$

Thus, the probability that there exists a node p such that $\mathcal{E}_2^p \bigcap \mathcal{E}_3^p$ occurs is no more than:

$$n\mathsf{Pr}\left(\mathcal{E}_2^p \bigcap \mathcal{E}_3^p\right) = \frac{1}{\log n} \to 0. \tag{68}$$

Combing (64b) and (68), we obtain $\mathsf{Pr}(\mathcal{D}^2_{(i,k)}[t]|\mathcal{D}^1_{(i,k)}[t]) \to 1$. Hence, from (63c), we have:

$$\mathsf{Pr}\big(\mathcal{D}_{(i,k)}[t]\big) \geq \mathsf{Pr}\Big(\mathcal{D}^2_{(i,k)}[t] \bigcap \mathcal{D}^1_{(i,k)}[t]\Big) \geq \Omega\bigg(\frac{(\log n)^2}{D}\bigg). \tag{69}$$

Thereby, the probability that the packet (i,k) cannot be delivered successfully to its destination node $i+1$ is no more than:

$$\prod_{t=1}^{D}\left[1 - \mathsf{Pr}\left(\mathcal{D}_{(i,k)}[t]\right)\right] \leq \left[1 - \frac{(\log n)^2}{D}\right]^D \tag{70a}$$

$$\leq \exp\left[-(\log n)^2\right] \tag{70b}$$

$$\leq n^{-\log n}. \tag{70c}$$

We notice that the number of packets in the network is no more than $n \times D^{5/3} n^{-(2/3)} = O(n^2)$. Hence, the probability that at least one packet cannot be delivered successfully to its destination node is no more than: $n^2 \times n^{-\log n} \to 0$. In other words, every packet generated in the previous duplication phase can be successfully delivered to its destination in the capture phase a.a.s.. Thus, the proposed scheme achieves a per-node throughput of:

$$\lambda = \Omega\left(\frac{1}{D}\frac{W}{(\log n)^5} D^{\frac{5}{3}} n^{-\frac{2}{3}} (\log n)^{-7}\right) \tag{71a}$$

$$= \Omega\left(W\left(\frac{D}{n}\right)^{\frac{2}{3}} (\log n)^{-12}\right). \tag{71b}$$

1) Remark 7.1: Note that the proposed scheme is subject to the secure protocol model and satisfies Assumption 1. Thus, according to Theorem 5.1, it is also feasible under the secure physical model. So, a throughput of $\lambda = \Omega(W(D/n)^{2/3}(\log n)^{-12})$ is also achievable under the secure physical model. By choosing the involved constants properly, we could further assure that Assumption 1, 2, and 3 are all satisfied by our proposed scheme. Hence, combining Theorem 6.1 and the proposed scheme, we claim that under the four assumptions, the optimal secrecy capacity-delay tradeoff is $\lambda = \widetilde{\Theta}(W(D/n)^{2/3})$.

VIII. Discussion

For wireless networks without eavesdroppers, the optimal capacity-delay tradeoff under the i.i.d. fast mobility model is shown to be $\lambda = \Theta(W\sqrt{D/n})$ by Ying *et al.* [19]. In contrast, our results indicate that as long as the number of eavesdroppers are sufficiently large, i.e., $\psi_e = \omega(1)$, under a few technical assumptions, the optimal secure capacity-delay tradeoff is $\lambda = \widetilde{\Theta}(W(D/n)^{2/3})$. Thus, we have the following three observations:

1) The secrecy constraint has a great impact on the optimal capacity-delay tradeoff. Specifically, given a delay constraint, it degrades the throughput capacity compared with networks without eavesdroppers, which is illustrated by the red line and blue line in Fig. 2. An intuitive explanation of this degradation is as follows. So as to degrade the channels at the eavesdroppers, the active receivers should generate sufficiently large artificial noise. However, the noise generated by a receiver also increases the interference at the other receivers and hence suppresses the SINR at them. In order to control this kind of interference to be small enough, we should guarantee that the distance between simultaneous transmissions is large enough. The quantitative expression of this thought is just the proposed secure protocol model, which is stricter than the insecure protocol model and naturally leads to network performance degradation.
2) It is shown in [10] that secrecy constraint will not influence the capacity of static networks[9]. However, according to our results, the optimal capacity-delay tradeoff is significantly influenced by the secrecy constraint in MANETs. The main reason of this difference is discussed as follows. As can be seen from the secure protocol model, the secrecy constraint has significant punishment on long-distance transmissions: in insecure networks, a transmission of distance r consumes $\Theta(r^2)$ radio resource while in secure networks, a transmission of distance r consumes $\Theta(r^4)$ radio resource. Hence, if the transmission range is very small, i.e., $r = \widetilde{\Theta}(1)$, the secrecy constraint does not impact the network capacity significantly, as is the case for the capacity achieving scheme in static networks [10]. However, if the transmission range is large, the secrecy constraint will degrade the network performance heavily. In MANETs, in order to satisfy the delay constraint D, we need to schedule long-distance transmissions in the capture phase. Compared with the insecure case, these long-distance transmissions will consume more radio resource in the secure case, which is the essential reason of the network capacity degradation. The above argument also explains an interesting phenomenon in Fig. 2: the gap between the insecure result in [19] and the secure result in this paper decreases as the delay constraint D increases and vanishes when $D = \Theta(n)$. The reason is that as D increases, we are able to schedule transmissions with smaller transmission range, which reduces the impact of the secrecy constraint.
3) As can be seen from our results, the density of the eavesdroppers does not affect the capacity-delay tradeoff as long as it is much larger than 1, i.e., $\psi_e = \omega(1)$. This indicates that adding more eavesdroppers into the network will not

[9] Our system model corresponds to the non-colluding model in [10]. For static networks, it is shown in [10] that in non-colluding case, the per-node capacity is always $1/\sqrt{n}$, which is not affected by the secrecy constraint.

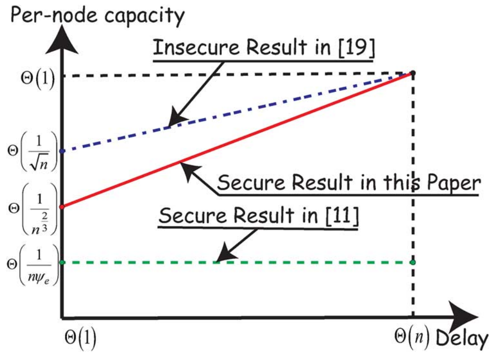


Fig. 2. A comparison between the capacity-delay tradeoff result of this paper and that of [11] and [19] (we assume that the link data rate is $W = 1$). The red line represents the optimal secure capacity-delay tradeoff in this paper. The blue line corresponds to the optimal insecure capacity-delay tradeoff presented in [19], and the green one is the secure capacity-delay tradeoff achieved in [11] when the number of eavesdroppers is larger than that of the legitimate nodes, i.e., $\psi_e = \omega(1)$.

further degrade the network performance. Actually, this is not surprising. As long as $\psi_e = \omega(1)$, we can already ensure that, for every active transmitter, there is an eavesdropper near enough, i.e., within a distance of 1, to it a.a.s.. This eavesdropper is the critical one since it has the highest SINR for signals sent by the transmitter. To guarantee secrecy, we essentially need to guarantee that the SINR at this eavesdropper is small enough. It is meaningless to set eavesdroppers even nearer due to the path loss model. Hence, adding more eavesdroppers will not help degrade the network performance any more.

4) If unlike the scenario considered here, the number of eavesdroppers is less than that of the legitimate nodes, the capacity-delay tradeoff still remains unknown. But, we observe that the capacity-delay tradeoff must lie between that in paper [19] (no eavesdroppers) and that in this paper (large number of eavesdroppers). In other words, if we plot the capacity-delay tradeoff curve in Fig. 2, it must lie between the blue line and the red line.

A closely related work of this paper is [11]. Compared with this paper, a major difference is that the authors of [11] do not allow active receivers to generate artificial noise. Rather, they only let each transmitter wait until the intended receiver is sufficiently near and then transmit messages securely. Under this secrecy scheme, when the number of eavesdroppers is larger than that of legitimate nodes n, i.e., $\psi_e = \omega(1)$, the optimal per-node throughput capacity is $\lambda = \Theta(W/n\psi_e)$ for whatever delay constraint D. This corresponds to the green line in Fig. 2. Our result evidently enhances this result to be $\lambda = \widetilde{\Theta}(W(D/n)^{2/3})$, which corresponds to the red line in Fig. 2. This shows the great benefit we could obtain from letting active receivers generate artificial noise.

IX. Conclusion and Future Work

Secrecy is a major concern when designing wireless networks. This paper studies the optimal secrecy capacity-delay tradeoff in MANETs. We propose the secure protocol model to assist analysis, which is also applicable to not only our system model but also many other network models. We prove the equivalence between the proposed secure protocol model and the widely accepted secure physical model under a few technical assumptions. Based on the secure protocol model, a tractable framework of analyzing the secrecy capacity-delay tradeoff is established. We derive an upper bound on the capacity-delay tradeoff and then present a capacity-achieving scheme, which justifies the optimality of our result. By allowing receivers to generate artificial noise, our result outperforms that of [11].

There are several directions for future work. First, real world wireless networks are usually heterogeneous to some extent, which has great impact on the network capacity and delay [25], [26]. Hence, it is interesting to know the impact of the network heterogeneity on the mobile or static secrecy networks. Second, instead of the i.i.d. mobility model, people may want to know the secrecy capacity-delay tradeoff with more realistic mobility model, e.g., random walk mobility. Third, in some practical applications, the traffic pattern is multicast or converge-cast instead of the unicast considered in this paper. The impact of secrecy constraint on the network performance under those traffic patterns needs to be further investigated. We remark that the proposed secure protocol model is still applicable for the situations mentioned above and extensions to various network models are tractable under our framework.

References

[1] C. Shannon, “Communication theory of secrecy system,” *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1948.

[2] A. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[3] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, Jul. 1978.

[4] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[5] E. Perron, S. Diggavi, and E. Telatar, “On cooperative wireless network secrecy,” presented at the IEEE INFOCOM, Rio de Janeiro, Brazil, Apr. 2009.

[6] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple antenna wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[7] A. Khist and G. Wornell, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[8] S. Vasudevan, D. Goeckel, and D. Towsley, “Security-capacity trade-off in large wireless networks using keyless secrecy,” presented at the ACM MobiHoc 2010, Chicago, IL, USA, Sep. 2010.

[9] C. Capar, D. Goeckel, B. Liu, and D. Towsley, “Secret communication in large wireless networks without eavesdropper location information,” in *Proc. IEEE INFOCOM*, 2012, pp. 1152–1160.

[10] J. Zhang, L. Fu, and X. Wang, “Asymptotic analysis on secrecy capacity in large-scale wireless networks,” *IEEE/ACM Trans. Netw.*, vol. 22, no. 1, pp. 66–79, Feb. 2014.

[11] Y. Liang, H. Poor, and L. Ying, “Secrecy throughput of MANETs under passive and active attacks,” *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6692–6702, 2011.

[12] J. Choiy, M. Jainy, K. Srinivasany, P. Levis, and S. Katti, “Achieving single channel, full duplex wireless communication,” presented at the ACM Mobicom 2010, Chicago, IL, USA, Sep. 2010.

[13] P. Gupta and P. R. Kumar, “The capacity of wireless networks,” *IEEE Trans. Inf. Theory*, vol. 46, pp. 388–404, Mar. 2000.

[14] M. Grossglauser and D. Tse, “Mobility increases the capacity of ad hoc wireless networks,” *IEEE/ACM Trans. Netw.*, vol. 10, pp. 477–486, 2002.

[15] M. J. Neely and E. Modiano, “Capacity and delay tradeoffs for ad-hoc mobile networks,” *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1917–1937, Jun. 2005.

[16] X. Lin and N. Shroff, “The fundamental capacity-delay tradeoff in large mobile ad hoc networks,” presented at the 3rd Annu. Mediterranean Ad Hoc Networking Workshop, Bodrum, Turkey, 2004.

[17] A. EI Gammal, J. Mammen, B. Prabhakar, and D. Shah, “Optimal throughput-delay scaling in wireless networks—Part I: The fluid model,” *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2568–2592, Jun. 2006.

[18] A. EI Gammal, J. Mammen, B. Prabhakar, and D. Shah, “Optimal throughput-delay scaling in wireless networks—Part II: Constant-size packets,” *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5111–5116, Nov. 2006.

[19] L. Ying, S. Yang, and R. Srikant, “Optimal delay-throughput tradeoffs in mobile ad hoc networks,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4119–4143, Sep. 2008.

[20] J. Mammen and D. Shah, “Throughput and delay in random wireless networks with restricted mobility,” *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1108–1116, Mar. 2007.

[21] P. Li, Y. Fang, and J. Li, “Throughput, delay, mobility in wireless ad hoc networks,” presented at the IEEE INFOCOM, San Diego, CA, USA, Mar. 2010.

[22] X. Wang, W. Huang, S. Wang, J. Zhang, and C. Hu, “Delay and capacity tradeoff analysis for motioncast,” *IEEE/ACM Trans. Netw.*, vol. 19, no. 5, pp. 1354–1367, Oct. 2011.

[23] J. Zhang, X. Wang, X. Tian, Y. Wang, X. Chu, and Y. Cheng, “Optimal multicast capacity and delay tradeoffs in MANETs,” *IEEE Trans. Mobile Comput.*, vol. 13, no. 5, pp. 1104–1117, May 2014.

[24] X.-Y. Li, “Multicast capacity of wireless ad hoc networks,” *IEEE/ACM Trans. Netw.*, vol. 17, no. 3, pp. 950–961, Jun. 2009.

[25] G. Alfano, M. Garetto, and E. Leonardi, “Capacity scaling of wireless networks with inhomogeneous node density: Upper bounds,” *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1147–1157, Sep. 2009.

[26] G. Alfano, M. Garetto, and E. Leonardi", “Capacity scaling of wireless networks with inhomogeneous node density: Lower bounds,” in *Proc. IEEE INFOCOM*, , 2009, pp. 1890–1898.

[27] B. Liu, P. Thiran, and D. Towsley, “Capacity of a wireless ad hoc network with infrastruture,” presented at the ACM MobiHoc'07, New York, NY, USA, 2007.

[28] A. Ozgur, O. Leveque, and D. Tse, “Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks,” *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3549–3572, 2007.

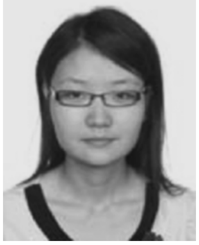
[29] W. Huang and X. Wang, “Capacity scaling of general cognitive networks,” *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1501–1513, Oct. 2012.

Xuanyu Cao received the B.E. degree in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, in 2013. He won the first prizes in Chinese National Mathematics Contest in 2007 and 2008. He received the Jimmy Lin scholarship from the Department of Electrical and Computer Engineering at the University of Maryland, College Park, MD, USA, where he is now pursuing the Ph.D. degree.

His current research interests are in the area of data science, network science, social networking and social media.

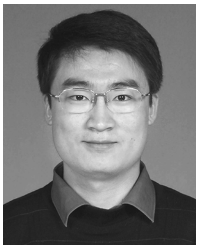
Jinbei Zhang received the B. E. degree in electronic engineering from Xidian University, Xi'an, China, in 2010, and is currently pursuing the Ph.D. degree in electronic engineering at Shanghai Jiao Tong University, Shanghai, China.

His current research interests include network security, capacity scaling law, and mobility models in wireless networks.



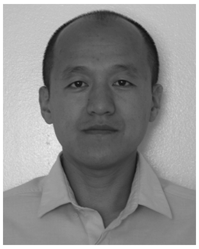
Luoyi Fu received the B.E. degree in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, in 2009, and is currently pursuing the Ph.D. degree in electronic engineering under the supervision of Prof. Xinbing Wang at Shanghai Jiao Tong University.

Her research of interests are in the area of scaling laws analysis in wireless networks and performance evaluation in social networks.



Weijie Wu received the Ph.D. degree in computer science from The Chinese University of Hong Kong in August 2012, and Bachelor degree in electronic and information science and technology from Peking University, Beijing, China, in July 2008. When he was a Ph.D. student, he spent two months at National University of Singapore working as a research intern.

He is an Assistant Professor in School of Electronic, Information and Electrical Engineering, Shanghai Jiao Tong University. Before that, he was a research fellow working with Dr. Richard T. B. Ma in National University of Singapore, and a postdoctoral fellow working with Prof. John C. S. Lui at The Chinese University of Hong Kong. His current research interests are in computer networks from mathematical modelling, data analytics, and economic perspectives. In particular, he is recently interested in network science (e.g., online social networks, large scale network with data implications, etc.), network economics (e.g., game theoretic analysis on communication networks, pricing and incentive design in network applications, etc.), and network optimization (e.g., resource allocation and pricing in cloud computing, information centric networks, etc.). His personal interests include table-tennis, badminton and hiking.



Xinbing Wang received the B.S. degree (with hons.) from the Department of Automation, Shanghai Jiaotong University, Shanghai, China, in 1998, and the M.S. degree from the Department of Computer Science and Technology, Tsinghua University, Beijing, China, in 2001. He received the Ph.D. degree, major in electrical and computer engineering, minor in mathematics, from North Carolina State University, Raleigh, NC, USA, in 2006.

Currently, he is a Professor in the Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai, China.

Dr. Wang has been an associate editor for IEEE/ACM TRANSACTIONS ON NETWORKING and IEEE TRANSACTIONS ON MOBILE COMPUTING, and a member of the Technical Program Committees of several conferences including ACM MobiCom 2012, ACM MobiHoc 2012–2014, and IEEE INFOCOM 2009–2014.