Impact of Secrecy on Capacity in Large-Scale Wireless Networks

Jinbei Zhang, Luoyi Fu, Xinbing Wang
Dept. of Electronic Engineering
Shanghai Jiao Tong University, China
Email: {abelchina, yiluofu, xwang8}@sjtu.edu.cn

Abstract—**Since wireless channel is vulnerable to eavesdroppers, the secrecy during message delivery is a major concern in many applications such as commercial, governmental and military networks. This paper investigates information-theoretic secrecy in large-scale networks and studies how capacity is affected by the secrecy constraint where the locations and channel state information (CSI) of eavesdroppers are both unknown. We consider two scenarios: 1) non-colluding case where eavesdroppers can only decode messages individually; and 2) colluding case where eavesdroppers can collude to decode a message. For the non-colluding case, we show that the network secrecy capacity is not affected in order-sense by the presence of eavesdroppers. For the colluding case, the per-node secrecy capacity of $\Theta(\frac{1}{\sqrt{n}})$ can be achieved when the eavesdropper density $\psi_e(n)$ is $O(n^{-\beta})$, for any constant $\beta > 0$ and decreases monotonously as the density of eavesdroppers increases. The upper bounds on network secrecy capacity are derived for both cases and shown to be achievable by our scheme when $\psi_e(n) = O(n^{-\beta})$ or $\psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n)$, where α is the path loss gain. We show that there is a clear tradeoff between the security constraints and the achievable capacity. Furthermore, we also investigate the impact of secrecy constraint on the capacity of dense network, other traffic patterns as well as mobility models in the context.**

I. Introduction

Although facilitating communications through quick deployment and low cost, the broadcast nature of wireless channel makes it vulnerable to attacks such as eavesdropping and jamming, which are important concerns for commercial, governmental and military networks. Traditional solutions are based on cryptographic methods such as the well-known RSA publickey cryptosystem. However, due to the expensive key distribution, the rapid growth of computation power and improvement on decoding technology, cryptographic techniques encounter some limitations, especially as the network size increases. Hence, to avoid such limitations, this paper focuses on information theoretic security where eavesdroppers are assumed to have infinite computational power.

The basis for information theoretic security stems from Shannon's notion of perfect secrecy [1], which is then extended to noisy channels by Wyner [2] and later by Csisz*á*r and K*ö*rner [3]. Information theoretic security is achieved by exploiting the difference between channels of legitimate nodes and that of eavesdroppers, which requires the intended receiver to have a stronger channel than eavesdroppers. Recently, secure wireless communications at the physical layer is intriguing renewed interests among research area. Haenggi [4] and Pinto *et al.* [5] study the in-degree and out-degree distributions under the security constraints. As is shown in both papers, even a small number of eavesdroppers will cause dramatic decreasing in nodes'connectivity. To guarantee the secret transmission, Geol and Negi [6] propose artificial noise generation to suppress eavesdroppers' receiving signal. The independence of fading channels is exploited to generate noise to suppress eavesdroppers' channels taking advantage of cooperative schemes [7] and multiple antennas [8], [9]. Furthermore, Barros *et al.* [10] show that theoretic information secrecy can be achieved by fading alone if channel state information (CSI) is available.

However, so far the research about information theoretic security mainly focuses on distinctive techniques to enhance the security, yet little is known about their impact on network performance such as capacity, delay, etc, especially in large scale wireless networks. As some exceptions, Vasudevan *et al.* [11] study the secrecy capacity issue in a large-scale network. Specifically, they introduce helper nodes around transmitters to generate noise to degrade eavesdroppers' channel and utilize channel fading gain of receivers to enhance secure communications. The impact of secrecy guard zone on capacity is investigated by Koyluoglu *et al.* [12] and Zhou *et al.* [13]. All these works are based on the assumption of either the pre-known CSI information of receivers or some pre-known location information of eavesdroppers which can be used by transmitters to differentiate receivers' channels from eavesdroppers'. However, since in real applications it is difficult to obtain such information a prior, especially in large scale wireless networks, a fundamental question arises: what will be the performance of secrecy capacity, if both the CSI and location information are unknown to legitimate nodes?

We are thus motivated to investigate this issue in static wireless networks. Our main idea to solve the aforementioned problem is to let a receiver distinguish its own channel by adopting self-interference cancelation. More precisely, we assume each receiver is equipped with three antennas, one for message reception and the other two for simultaneous artificial noise generation to suppress eavesdroppers' channels. Since the three antennas are all equipped on one node, the noise generated by the receiver itself can be eliminated through the technique of antenna cancelation proposed in [15]. This differs our noise generation pattern from the work in [6] and [11] and we will show in later part that such difference can dramatically improve network secrecy capacity.

Our main contributions are summarized as follows:

- In the non-colluding case, the optimal per-node secrecy capacity $\Theta(\frac{1}{\sqrt{n}})$ is achievable in the presence of eavesdroppers. This result holds even in the scenario where there are more eavesdroppers than legitimate nodes in the network.
- In the colluding case, we establish the relationship between the secrecy capacity and the tolerable number of eavesdroppers. The corresponding capacity-achieving communication schemes are proposed to meet the upper bound derived.
- We identify the underlying interference model to capture the fundamental impact of secrecy constraints. This model relies weakly on the specific settings such as traffic pattern and mobility models of legitimate nodes. Hence, our study can be flexibly applied to more general cases and shed insights into the design and analysis of future wireless networks.

The rest of this paper is organized as follows. In Section II, we present the system model. Asymptotic analysis on different scenarios is carried out in Section III and IV. We investigate the effect of dense network in Section V. Jamming as a different kind of network attacking is investigated in Section VI. Discussions and concluding remarks are given in Section VII and VIII, respectively.

A. Related Works

Asymptotic analysis can provide fundamental insight on network performance as the network size increases. The ground-breaking work is inspired by Gupta and Kumar [16], who study capacity performance in a network with n randomly distributed nodes. They show that the per-node capacity is lower bounded by $\Omega(\frac{1}{\sqrt{n\log n}})$ and upper bounded by $O(\frac{1}{\sqrt{n}})$. This gap is closed later by Franceschetti *et al.* [18] using percolation theory. The fundamental difference behind these two works is the underlying connectivity. The communication range in [16] should be $\Theta(\sqrt{\frac{\log n}{n}})$ to guarantee full connectivity whereas it only needs to be $\Theta(\sqrt{\frac{1}{n}})$ in [18] to guarantee partial connectivity at the bottleneck. Following that, Grossglauser and Tse [22] further indicate the capacity can be improved to $\Theta(1)$ when mobility is introduced to nodes, at the expense of increased delay [17]. Since then, asymptotic analysis has drawn considerable attention in research area, from the perspective of traffic patterns [23], network architectures [19], [24] and various sophisticated techniques [21], [25], etc.

II. Network Models and Definitions

In this paper, we consider a static ad hoc network in an extended network $\mathscr{B} = [0,\sqrt{n}] \times [0,\sqrt{n}]$.

Legitimate Nodes: Legitimate nodes follow a Poisson distribution with unit intensity over the whole network. And transmitter-receiver pairs are randomly chosen such that each node is the destination of exactly one source. We denote $\mathcal{T}$ and $\mathcal{R}$ as the subsets of nodes simultaneously transmitting and receiving at a given time-slot. We assume that 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 eavesdroppers' channels. The distances between the receive antenna and the two respective transmit antennas should satisfy a difference of half the wavelength. The interference can therefore be eliminated using the technique of self-interference cancelation proposed in [15].

Eavesdroppers: Independently of legitimate nodes, eavesdroppers also follow a Poisson distribution in the network with intensity λ_e. Let $\mathcal{E}$ be the set of eavesdroppers. We assume eavesdroppers always keep silent since they will be easily detected if active. In order to have an insight on the fundamental information theoretical secrecy capacity, we assume eavesdroppers have infinite computation ability which means that traditional cryptography method can not be applied here. We also assume that both CSI and location information of eavesdroppers are unknown to legitimate nodes.

The Physical Model: For simplicity, we denote uniform transmission power as P_t and uniform noise generation power as P_r. The path loss between node i and node j is denoted by $l(x_i,x_j)$, which can be expressed as $l(x_i,x_j)=\min(1,d_{ij}^{-\alpha})$. Here d_{ij} is the transmission distance and the loss exponent $\alpha>2$. When node i is transmitting messages to node j, the signal to interference and noise ratio (SINR) received by node j over a channel of unit bandwidth can be given by:

$$\mathrm{SINR}_{ij} = \frac{P_t l(x_i,x_j)}{N_0 + \sum_{k\in\mathcal{T}\backslash\{i\}} P_t l(x_k,x_j) + \sum_{k\in\mathcal{R}\backslash\{j\}} P_r l(x_k,x_j)},$$

where N_0 denotes the ambient noise power at the receiver. The SINR received by eavesdropper e can be represented by:

$$\mathrm{SINR}_{ie} = \frac{P_t l(x_i,x_e)}{N_0 + \sum_{k\in\mathcal{T}\backslash\{i\}} P_t l(x_k,x_e) + \sum_{k\in\mathcal{R}} P_r l(x_k,x_e)}.$$

Secrecy Throughput Per Hop: As is defined in [3], the secure throughput between any active transmitter-receiver pair is:

$$R_{ij}^s = R_{ij} - \overline{R_{ie}} = \log_2(1+\mathrm{SINR}_{ij}) - \log_2(1+\overline{\mathrm{SINR}_{ie}})$$

where $\overline{\mathrm{SINR}_{ie}} = \max_{e\in\mathcal{E}} \mathrm{SINR}_{ie}$.

Asymptotic Capacity: Asymptotic per node capacity $\lambda(n)$ is said to be achievable if there is a scheduling and routing scheme such that every node can transmit $\lambda(n)$ bits per second on average to its destination in the long term.

Knuth Notations: Denote $\lambda(n) = O(f(n))$ if there is a positive constant c_1 such that $\lim_{n\to\infty} P(\frac{\lambda(n)}{f(n)} \le c_1) = 1$ and $\lambda(n) = \Omega(f(n))$ if $f(n) = O(\lambda(n))$. $\lambda(n)$ is said to be $\Theta(f(n))$ if both $\lambda(n) = O(f(n))$ and $\lambda(n) = \Omega(f(n))$ hold.

In Table 1, we list the parameters that will be used in later analysis, proofs and discussions.

III. Security Capacity for independent eavesdroppers case

In this section, we investigate secrecy capacity for independent eavesdroppers. We use percolation theory to construct

TABLE I: Notations

Notation	Definition
n	The total number of legitimate nodes in the network.
$\lambda_s(n)$	The per-node secrecy capacity.
$\psi_e(n)$	The expected density of poisson distributed eavesdroppers.
P_t	The power to transmit packets.
P_r	The power to generate noise.
$R(d)$	The rate that a transmitter can transmit to an intended receiver which is located d distance away.
R_e	The rate that an eavesdropper can obtain from a transmitting node.
$R_s(d)$	The rate that a transmitter can securely transmit to an intended receiver which is located d distance away.

the routing scheme which contains three phases, e.g., draining phase, highway transmission and delivery phase. Since our scheme should guarantee the secrecy communication, it seems that the capacity should be degraded. However, we show that regardless of the fact that the capacity will be sacrificed to ensure secrecy in draining phase and delivery phase, the bottleneck still lies in the highway phase where the secrecy capacity remains the same as that in the network without eavesdroppers.

We present the following lemma which will be quoted throughout this paper.

Lemma 1: When a legitimate node t is transmitting to a legitimate receiver r, the maximum rate that an independent eavesdropper e can obtain is upper-bounded by

$$R_e \leq \min\left(\frac{P_t d_{te}^{-\alpha}}{N_0}, \frac{P_t}{P_r}(1+d_{tr})^{\alpha}\right), \tag{1}$$

where d_{tr} is the Euclidean distance between legitimate node t and node r and d_{te} is the distance between legitimate node t and eavesdropper e.

Proof: First we prove the maximum SINR that eavesdroppers can obtain is $\frac{P_t}{P_r}(1+d_{rt})^{\alpha}$. Consider the following four cases.

Case 1: When d_{te} and d_{re} are both greater than 1, then

$$\begin{aligned}\text{SINR}_e &= \frac{P_t l(x_t, x_e)}{N_0 + \sum_{k\in\mathcal{T}\setminus\{t\}} P_t l(x_k, x_e) + \sum_{k\in\mathcal{R}} P_r l(x_k, x_e)} \\ &< \frac{P_t l(x_t, x_e)}{P_r l(x_r, x_e)} = \frac{P_t d_{te}^{-\alpha}}{P_r d_{re}^{-\alpha}} \\ &\leq \frac{P_t d_{te}^{-\alpha}}{P_r (d_{rt}+d_{te})^{-\alpha}} \\ &= \frac{P_t}{P_r}\left(1+\frac{d_{rt}}{d_{te}}\right)^{\alpha} \leq \frac{P_t}{P_r}(1+d_{rt})^{\alpha}.\end{aligned} \tag{2}$$

Case 2: When $d_{te} > 1$ and $d_{re} <= 1$, it is obvious to see that eavesdroppers's interference is more severe than that in case 1 while the signal received is no stronger than that in case 1. So the bound still holds.

Case 3: When $d_{te} <= 1$ and $d_{re} > 1$, we can easily see that the path loss gain of T-E pair is 1 when the bound derived in case 1 holds, which means that the bound cannot be broken by condition $d_{te} <= 1$.

Case 4: When $d_{te} <= 1$ and $d_{re} <= 1$, the SINR at eavesdroppers will not be greater than that in case 3 since eavesdroppers in case 4 suffer more interference. Hence the bound still holds.

Notice that SINR$_e$ is also smaller than $\frac{P_t d_{te}^{-\alpha}}{N_0}$. Hence, since $R_e = \log(1+\max(\text{SINR}_e))$, it is straightforward to conclude this lemma. ■

A. The Highway System

The network is divided into non-overlapping cells with side length of c, where c is a constant .We say that a cell is open if there is at least one node in it. Hence cells are open with probability $p = 1 - e^{-c^2}$ independently.

For ease of exposition, denote m as $\sqrt{n}/\sqrt{2}c$ and we assume m to be an integer, which will not change our results in order sense. As is shown in [18], when the constant c is large enough, there are a lot of crossing paths in the network which behave almost as straight lines. For any $\kappa > 0$, partition the network into rectangles of size $m \times (\kappa \log m - \epsilon_m)$ and choose $\epsilon_m = o(1)$ as the smallest value such that the side length is an integer. Denote R_i as the ith rectangle and C_i as the number of edge-disjoint crossings of R_i. Then the minimal number of disjoint crossing paths $N_p = \min_i C_i$ can be upper bounded by $\delta \log m$ when m goes to infinity and δ is a constant. Further, to make sure that there are at least as many paths as slices inside each rectangle, each rectangle is sliced into horizontal strips with constant $w = \kappa \log m / N_p$.

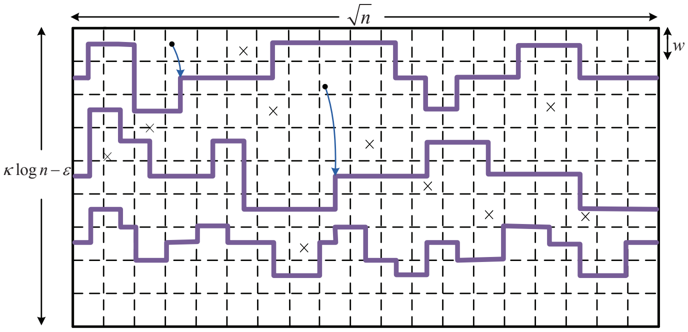

Fig. 1: There are at least $\delta \log m$ disjoint highways in each rectangle. Nodes in i-th slice will transmit to nodes located in the i-th highway and crosses denote eavesdroppers.

Our packet routing scheme includes three steps:

Step 1: Each source in the i-th slice transmits directly to a legitimate relay located on the i-th path. The relay is chosen in a way such that it is closest to the source among all other nodes on the i-th path, as is shown in Fig. 1.

Step 2: Packets are relayed horizontally through the highway and then along a vertical highway until it arrives at an exit point closest to the destination in a multi-hop fashion.

Step 3: Packets are directly delivered from the highway to the destination similar to the first step.

B. Analysis of Secrecy Capacity

Next we present our scheduling scheme and compute the lower bound of the legitimate receiver's rate. Note that our scheduling scheme is different from that proposed in [18], since we should take the issue of secrecy into account. And the basic idea is to space concurrent transmission sufficiently far away so that the interference is tolerable.

Lemma 2: When a legitimate node is transmitting to a legitimate receiver which is located d cells apart, the minimum rate that the legitimate node can receive is lower-bounded by $c_2 P_t d^{-\alpha}$, where c_2 is a constant.

Proof: First we compute the interference at the receiver. Divide the network into disjoint subsquares of $(k+d) \times (k+d)$ cells, where k will be explained later. Every cell in each subsquare takes turn to transmit. Consider a given transmitter-receiver pair, the eight closest transmitters and receivers are located at distance of at least ck and $c(k+d-1)$ from the receiver. The sixteen next closest transmitters and receivers are located at distance at least $c(2k+d)$ and $c(2k+2d-1)$ away from the receiver and so on. Taking into consideration all the interferences in the whole network, the interference at the intended destination can be upper-bounded as follows:

$$\begin{aligned}I(d) &\leq \sum_{i=1}^{\infty} 8i(P_t l(c(i(k+d)-d)) + P_r l(c(i(k+d)-1))) \\ &\leq \sum_{i=1}^{\infty} 8i(P_t + P_r) l(cik) \\ &= (P_t + P_r)(kc)^{-\alpha} \sum_{i=1}^{\infty} 8i(ci)^{-\alpha}.\end{aligned} \tag{3}$$

Note that $\sum_{i=1}^{\infty} 8i(ci)^{-\alpha}$ converges to a constant $c_1^{'}$ when $\alpha \geq 2$.

Since the distance from the transmitter to the designated receiver is at most $c(d+1)$, the receiving signal $S(d)$ can be lower-bounded by

$$\begin{aligned}S(d) &\geq P_t l(c(d+1)) \\ &= P_t (c(d+1))^{-\alpha},\end{aligned} \tag{4}$$

notice that $l(c(d+1)) = (c(d+1))^{-\alpha}$ since d is an integer and c is greater than 1.

Now the minimum rate that the legitimate receiver can achieve can be derived as follows:

$$\begin{aligned}R(d) &= \log\left(1 + \frac{S(d)}{N_0 + I(d)}\right) \\ &\geq \log\left(1 + \frac{P_t (c(d+1))^{-\alpha}}{N_0 + c_1(P_t + P_r)(kc)^{-\alpha}}\right) \\ &\geq c_2^{'} P_t (c(d+1))^{-\alpha} \\ &\geq c_2 P_t d^{-\alpha},\end{aligned} \tag{5}$$

when choosing $k = \Theta(P_r^{\frac{1}{\alpha}})$ and c_2 is a constant. ■

Now we will show that secrecy communication can be assured for any T-R pairs by appropriately spacing for concurrent transmissions.

Theorem 1: For any legitimate transmitter-receiver pair which is spaced at a distance of d cells apart, there exists an $R_s(d) = \Omega(d^{-\alpha-4})$, so that the receiver can receive at a rate of $R_s(d)$ securely from the transmitter.

Proof: According to the definition of secure rate and combining with Lemma 1 and Lemma 2, the secrecy rate $R^s(d)$ each cell can transmit can be denoted as:

$$\begin{aligned}R^s(d) &= \frac{1}{(k+d)^2}(R(d) - R_e) \\ &\geq \frac{1}{(k+d)^2}\left(c_2 P_t d^{-\alpha} - c_3 \frac{P_t}{P_r} d^{\alpha}\right)\end{aligned} \tag{6}$$

where $\frac{1}{(k+d)^2}$ is the time utilization factor, c_2 and c_3 are both constants.

Let $P_r = 2\frac{c_3}{c_2} d^{2\alpha}$. Hence, to bound the interference incurred to the intended receiver, according to Equation (5), $k = \Theta(P_r^{\frac{1}{\alpha}}) = \Theta(d^2)$. Therefore, the secrecy rate each cell can receive is $\Omega(d^{-\alpha-4})$. ■

Theorem 1 indicates positive secrecy rate is achievable even under the worst attack. In order to calculate per-node secrecy capacity, we first compute the number of legitimate nodes in each cell and then derive the traffic load that each node in the highway should relay, as are shown in the following two lemmas.

Lemma 3: There are at most $\log n$ legitimate nodes in each cell of constant size c^2 *w.h.p.*[1].

Proof: Let A_i be the number of legitimate nodes in cell i and A be the maximum number of A_i. Hence, we have

$$\begin{aligned}P(A \geq \log n) &= P(\max A_i \geq \log n) \\ &\leq P(\cup_i (A_i \geq \log n)) \\ &\leq \sum_i P(A_i \geq \log n) \\ &\leq \frac{n}{c^2} e^{-c^2} \left(\frac{c^2 e}{\log n}\right)^{c^2 \log n} \\ &= \frac{1}{c^2} e^{-c^2} \left(\frac{c^2 e^{1+1/c^2}}{\log n}\right)^{c^2 \log n} \rightarrow 0.\end{aligned}$$

Note that the third inequality follows from union bounds and the fourth one follows from Chernoff bounds [27]. ■

Lemma 4: If nodes are poisson distributed with intensity $\psi(n)$ in the network $\mathscr{B}$, partition the network into disjoint regions with same size $f(n)$, let N_i be the number of nodes inside region i. We have

$$P\left(\frac{1}{2} f(n)\psi(n) \leq N_i \leq 2 f(n)\psi(n), \forall i\right) = 1$$

when $f(n)\psi(n) \geq \log_{4/e} n$ and $f(n) = \Omega(1)$.

Proof: The number of nodes inside each region N_i is a poisson variable and denote its expectation as ψ. Hence, we have $\psi = E(N_i) = f(n)\psi(n)$. Letting N be the maximum number of N_i, for all i. Under similar derivation of Lemma

[1] In this paper, *w.h.p* stands for with high probability, which means the probability tends to 1 as n goes to infinity.

3, we can get that

$$\begin{aligned} P(N \geq 2f(n)\psi(n)) &\leq \frac{n}{f(n)} P(N_i \geq 2f(n)\psi(n)) \\ &\leq \frac{n}{f(n)} e^{-\psi} \left(\frac{e\psi}{2\psi}\right)^{2\psi} \\ &= \frac{n}{f(n)} \left(\frac{e}{4}\right)^{f(n)\psi(n)} \\ &\leq \frac{1}{f(n)} \to 0 \end{aligned} \tag{7}$$

when $f(n)\psi(n) \geq \log_{4/e} n$ and $f(n) = \Omega(1)$.

Similarly, we can show that $\min_i N_i$ is greater than $\frac{1}{2}f(n)\psi(n)$ *w.h.p.* when conditions hold. ■

Theorem 2: With n legitimate nodes poisson distributed in $\mathscr{B}$, the achievable per-node secrecy throughput under the existence of independent eavesdroppers is $\Omega(\frac{1}{\sqrt{n}})$.

Proof: As is shown in the routing scheme, the maximum distance between source and relay on the highway is no larger than $\kappa \log m + 2c$ in the first step. Applying Theorem 1, we obtain that one node in the cell can transmit securely at rate $\Omega(\log^{-\alpha-4} n)$ to the relay. Since there may be multiple nodes inside the cell, they should share the transmission chances. The number of nodes inside each cell can be bounded as $O(\log n)$ according to Lemma 3. Hence, the achievable secrecy capacity is $\Omega(\log^{-\alpha-5} n)$ in the draining phase. Note that since the delivery phase is a reverse process of the draining phase, the secrecy capacity of the delivery phase is the same as that of draining phase.

In the highway phase, the transmission range between T-R pairs is at most $2\sqrt{2}c$. Hence each node on the highway can transmit securely at rate $\Omega(1)$ to the next relay by applying Theorem 1. According to the routing scheme, each source in the i-th slice transmit packets to the i-th highway in the same rectangle. Since the density of legitimate nodes is 1 and the size of each slice is $w\sqrt{n}$, which satisfy the conditions given by Lemma 4, we obtain that the maximum number of legitimate nodes inside each slice is no larger than $2w\sqrt{n}$. Hence, the traffic load on each relay node in the highway is at most $2w\sqrt{n}$ nodes. Therefore, the secrecy capacity of the highway phase is $\Omega(\frac{1}{\sqrt{n}})$.

Based on the results above, we conclude that per-node secrecy capacity is $\Omega(\frac{1}{\sqrt{n}})$. ■

C. The Optimality of Our Scheme

We first consider the case where no eavesdropper exists in the network. Due to the broadcast nature of wireless channel, every concurrent transmission will incure interference to other transmissions. The following lemma shows that there is a constraint on the total network throughput underlying this fundamental physical model.

Theorem 3: When n nodes is identically and randomly located in a wireless network and source-destination pairs are randomly chosen, the per-node throughput $\lambda(n)$ is upper bounded by $O(\frac{1}{\sqrt{n}})$.

Proof: Let L be the expected distance between all source-destination pairs. Hence $L = \Theta(\sqrt{n})$ [16]. Denote r and $T(r)$ as the average transmission range and rate of each hop respectively. Let l be the average distance that simultaneous transmissions can occure. Since the expected number of hops that a packet should travel is L/r, the total traffic load the network should carry is $n\lambda(n)L/r$. And the total traffic that the network can carry is $\frac{n}{l^2}T(r)$. Hence, we obtain that $n\lambda(n)L/r \leq \frac{n}{l^2}T(r)$, which means $\lambda(n) \leq \frac{rT(r)}{l^2\sqrt{n}}$. Substituting $T(r)$ into the equation, we have

$$\lambda(n) \leq \frac{rT(r)}{l^2\sqrt{n}} = \frac{P_t \min(1, r^{-\alpha})}{N_0 + \sum_{k \in \mathcal{T}\setminus\{i\}} P_t l(x_k, x_j)} \frac{r}{l^2\sqrt{n}}$$

where $\mathbf{T}$ denotes the set of concurrent transmission nodes and $l(x_k, x_r)$ denotes the path loss gain.

It is easily verified that $\min(r, r^{1-\alpha}) = O(1)$. Next We show that $(N_0 + \sum_{k \in \mathcal{T}\setminus\{i\}} P_t l(x_k, x_r))l^2 = \Omega(1)$. If $l = \Omega(1)$, the result is straightforward. If $l = o(1)$, there would be $\Theta(\frac{1}{l^2})$ concurrent transmission nodes inside unit area around the receiver and the path loss gain between these nodes and the intended receiver is $\Theta(1)$. Therefore, the result holds. ■

Since the per-node throughput without the secrecy constraint is $O(\frac{1}{\sqrt{n}})$, the per-node secrecy capacity can also be bounded by $O(\frac{1}{\sqrt{n}})$ which indicates the optimality of our scheme.

IV. Colluding Eavesdroppers

In previous section, the maximum SINR received by an independent eavesdropper can be suppressed by artificial noise generation. And it has already been shown that the per-node throughput does not entail lost, regardless of how many eavesdroppers are present in the network. However, if eavesdroppers are equipped with multiple antennas or multiple eavesdroppers can collude to decode the messages, is it still possible to ensure secrecy transmission and what is the network secrecy performance? We will focus on these problems in this section.

A. Eavesdroppers with multiple antennas

We start from the special case where every eavesdropper is equipped with $A(n)$ antennas but eavesdroppers do not collaborate with each other.

To get an intuitive insight, we assume that the eavesdropper can employ maximum ratio combining to maximize the SINR which means that the correlation across the antennas is ignored.

Theorem 4: If eavesdroppers are equipped with $A(n)$ antennas, the per-node secrecy capacity $\lambda_s(n)$ is $\Omega(\frac{1}{\sqrt{n}}A(n)^{-\frac{2}{\alpha}})$.

Proof: Since eavesdroppers is equipped with $A(n)$ antennas, following the same argument of Lemma 1, the maximum rate that eavesdroppers can get is bounded as $R_e \leq c_3 A(n)\frac{P_t}{P_r}(1 + d_{rt})^{\alpha}$. Because eavesdroppers don't transmit any noise so the rate that legitimate receivers can get remains the same as the following

$$R(d) \geq c_2 P_t (c(d+1))^{-\alpha}. \tag{8}$$

Because of $R_s(d) = R(d) - R_e$, it is obvious that there exists a constant c_4, such that when P_r equals $c_4 A(n) d^{2\alpha}$, $R_s(d)$ can be greater than $\frac{1}{2}R(d)$. Hence the secrecy rate is

$\Omega(d^{-\alpha})$. To hold equation (6), k should be in the order of $\Theta(P_r{}^{\frac{1}{\alpha}})$ which is equal to $(A(n)^{\frac{1}{\alpha}}d^2)$. So the secrecy rate in each cell should be $\Omega(d^{-\alpha-4}A(n)^{-\frac{2}{\alpha}})$. When the transmission is on the highway phase, the per-node secrecy capacity is $\Omega(\frac{1}{\sqrt{n}}A(n)^{-\frac{2}{\alpha}})$. When the transmission is on the delivery phase, the per-node secrecy capacity is $\Omega(\log^{-\alpha-5} nA(n)^{-\frac{2}{\alpha}})$. Hence, the per-node secrecy capacity is $\Omega(\frac{1}{\sqrt{n}}A(n)^{-\frac{2}{\alpha}})$. From this result, we can see that there is a tradeoff between the number of a eavesdropper' antennas and the capacity of legitimate nodes. ■

B. Secrecy Capacity for Colluding Eavesdroppers

To get a fundamental insight on how the colluding eavesdroppers will affect the secrecy transmission, we assume that all eavesdroppers in the network can collaborate to decode the messages and maximum ratio combing is adopted to maximize the SINR eavesdroppers obtained. Hence we can regard all eavesdroppers as a super-eavesdropper.

Assume that eavesdroppers are poisson distributed with parameter $\psi_e(n)$ in the network. For a given transmitter-receiver pair, we partition the network into disjoint rings with a same size of $f(n)$. The transmitter is at the center of all these rings. Let r_i be the external diameter of the ith ring. Since $f(n) = \pi r_1^2 = \pi(r_i^2 - r_{i-1}^2)$ for any $i > 1$, we have $r_i = \sqrt{i}r_1$ for any $i \geq 1$. Denote Φ_{ei} as the set of eavesdroppers located inside the i-th ring. Hence the number of eavesdropper N_{ei} in Φ_{ei} is a poisson variable with parameter $\psi_e(n)f(n)$. Recalling Lemma 4, we have

$$P(\frac{1}{2}f(n)\psi_e(n) \leq N_{ei} \leq 2f(n)\psi_e(n), \forall i) = 1,$$

when $f(n)\psi_e(n) \geq \log_{4/e} n$ and $f(n) = \Omega(1)$.

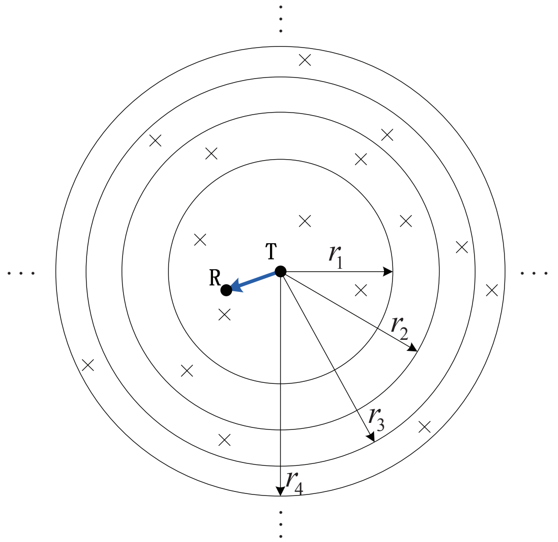

Fig. 2: An illustration of network partition to bound the upper bound of SINR received by eavesdroppers.

Notice that the distance between the transmitter and eavesdroppers is at least r_{i-1}, the signal power received by eavesdroppers in the i-th ring is at most $P_t r_{i-1}^{-\alpha}$ for any $i \geq 2$. For each $\psi_e(n)$, we choose $f(n)$ such that $f(n)\psi_e(n) \geq \log_{4/e} n$ and $f(n) = \Omega(1)$. Denote SINR_{ei} as the SINR received by eavesdroppers in the i-th ring. Taking the summation of the SINR received by the eavesdroppers in all the rings up, we have

$$\begin{aligned}
\text{SINR}_e &\leq \sum_i \text{SINR}_{ei} \\
&= \sum_{j\in\Phi_{e1}} \text{SINR}_{1j} + \sum_{i=2}^{+\infty}\sum_{j\in\Phi_{ei}} \text{SINR}_{ij} \\
&\leq 2f(n)\psi_e(n)\overline{\text{SINR}_{e1}} + \sum_{i=2}^{+\infty} 2f(n)\psi_e(n)\overline{\text{SINR}_{ei}} \qquad (9) \\
&\leq 2f(n)\psi_e(n)\frac{P_t}{P_r}(1+d_{rt})^\alpha + \sum_{i=2}^{+\infty} 2f(n)\psi_e(n)\frac{P_t r_{i-1}^{-\alpha}}{N_0} \\
&= 2\pi\psi_e(n)\left(r_1^2\frac{P_t}{P_r}(1+d_{rt})^\alpha + \frac{P_t}{N_0}r_1^{2-\alpha}\sum_{i=1}^{+\infty} i^{-\frac{\alpha}{2}}\right),
\end{aligned}$$

where the third row of this inequality follows from Lemma 1 and note that $\sum_{i=1}^{+\infty} i^{-\frac{\alpha}{2}}$ converges since $\alpha > 2$.

Case 1: When the transmission is on the highway phase which means $d_{rt} = \Theta(1)$, substituted into Equation (8), it is obvious that there is a constant c_4 satisfying $R_e \leq c_4\psi_e(n)(r_1^2/P_r + r_1^{2-\alpha})$. As is shown in Lemma 2, the rate $R(d)$ received by the intended receiver can be $\Theta(1)$. Note that there are two constraints in the derivation of Equation (9), i.e., $f(n)\psi_e(n) \geq \log_{4/e} n$ and $f(n) = \Omega(1)$. With $r_1 = \max(\Omega(1), \Theta(\psi_e(n)^{\frac{1}{\alpha-2}}))$ and $P_r = \Theta(\psi_e(n)r_1^2)$, the secure transmission can be guaranteed and secure rate each node in the highway can transmit is $\Omega(\frac{1}{k^2})$ where $k = \Theta(P_r^{\frac{1}{\alpha}})$ is the concurrent transmission range.

Hence if $\psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n)$, $P_r = \psi_e(n)r_1^2 = \Theta(\psi_e(n)^{\frac{\alpha}{\alpha-2}})$. The secure rate each node in the highway can transmit is $\Omega(\psi_e(n)^{-\frac{2}{\alpha-2}})$. Since the traffic load at each node in the highway is at most $O(\frac{1}{\sqrt{n}})$, the per-node throughput should be $\Omega(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}})$. If $\psi_e(n) = O(\log^{\frac{\alpha-2}{\alpha}} n)$, with similar argument, the noise generation power can be $\Theta(\log n)$ and we can obtain per-node secrecy capacity of $\Omega(\frac{1}{\sqrt{n}}\log^{-\frac{2}{\alpha}} n)$.

Case 2: When the transmission is on the draining and delivery phases where $d_{rt} = \Theta(\log n)$, there exists a constant c_5 such that $\text{SINR}_e \leq c_5\psi_e(n)(r_1^2\log^\alpha n/P_r + r_1^{2-\alpha})$. Following Lemma 3, the rate allocated at each cell is $\log^{-\alpha} n$. Similar to case 1, choosing $r_1 = \max(\Omega(1), \Theta(\psi_e(n)^{\frac{1}{\alpha-2}}))$ and $P_r = \Theta(\psi_e(n)r_1^2\log^\alpha n)$, the secure transmission could be guaranteed and secure rate R_s allocated at each cell is $\Omega(\frac{1}{k^2\log^\alpha n})$, where $k = \Theta(P_r^{\frac{1}{\alpha}})$. When $\psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n)$, $P_r = \Theta(\psi_e(n)^{\frac{\alpha}{\alpha-2}}\log^\alpha n)$ and $R_s = \Omega(\psi_e(n)^{-\frac{2}{\alpha-2}}\log^{-\alpha-2} n)$. Since there are at most $\log n$ legitimate nodes inside a cell, the per-node secrecy capacity is bounded by $\Omega(\psi_e(n)^{-\frac{2}{\alpha-2}}\log^{-\alpha-3} n)$. When $\psi_e(n) = O(\log^{\frac{\alpha-2}{\alpha}} n)$, using similar technique, we can obtain that the per-node secrecy capacity is $\Omega((\log n)^{-(\alpha+1)(1+\frac{2}{\alpha})})$.

Combining these two cases, we present the following theorem which demonstrates the tradeoff between the secrecy capacity and the tolerable eavesdroppers' density.

Theorem 5: Consider the wireless network $\mathscr{B}$ where legitimate nodes and eavesdroppers are independent poisson distributed with parameter 1 and $\psi_e(n)$ respectively, the per-node secrecy capacity is

$$\lambda_s(n) = \begin{cases} \Omega(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}}), & \psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n) \\ \Omega(\frac{1}{\sqrt{n}}\log^{-\frac{2}{\alpha}} n), & \psi_e(n) = O(\log^{\frac{\alpha-2}{\alpha}} n) \end{cases}. \tag{10}$$

Intuitively, when $\psi_e(n) = o(n^{-1})$, the number of eavesdroppers will be at most 1 *w.h.p.* according to the weak law of large numbers. Hence, the secrecy capacity will be $\Omega(\frac{1}{\sqrt{n}})$ with Theorem 2 which is much higher than the results in Theorem 3. The main reason is that the inequality $f(n)\psi_e(n) \geq \log_{4/e} n$ should be satisfied throughout the proof of Theorem 3. Therefore, the noise generation power should be $\Theta(\log n)$ which will degrade the throughput performance. We re-investigate this problem from another perspective in the following context.

Lemma 5: When the intensity of the eavesdroppers is $\psi_e(n) = O(n^{-\beta})$ for any constant $\beta > 0$, partitioning the network into disjoint regions with constant size c and denoting by N_{ei} the number of nodes inside region i, we have

$$P(N_{ei} \leq v, \forall i) = 1,$$

where $v = \lceil \frac{1}{\beta} \rceil + 1$.

Proof: Let N_e be the maximum number of N_{ei} and ψ be the expected number of N_{ei}. Hence $\psi = c\psi_e(n)$ and we can further get

$$\begin{aligned} P(N_{ei} \geq v) &= \sum_{i=v}^{\infty} \frac{\psi^i e^{-\psi}}{i!} \\ &\leq \frac{\psi^v e^{-\psi}}{v!}(1 + \psi + \psi^2 + \psi^3 + ...) \\ &\leq \frac{\psi^k e^{-\psi}}{v!}\frac{1}{1-\psi/(v+1)} \to 0. \end{aligned} \tag{11}$$

Using the union bound, we have

$$\begin{aligned} P(N_e \geq v) &\leq \frac{n}{c}\frac{\psi^v e^{-\psi}}{v!}\frac{1}{1-\psi/(v+1)} \\ &\leq \frac{n^{1-v\beta}}{c}\frac{c^v e^{-\psi}}{v!}\frac{1}{1-\psi/(v+1)} \to 0 \end{aligned} \tag{12}$$

as n goes to infinity. ■

Theorem 6: If eavesdroppers are poisson-distributed in the network with intensity $\psi_e(n) = O(n^{-\beta})$ for any constant $\beta > 0$, the per-node secrecy capacity is $\Omega(\frac{1}{\sqrt{n}})$.

Proof: To compute the SINR of the eavesdropper system, we divide the network into two parts. One is the circle which is at most r_1 distance from the transmitter, the other is the rest of the network. There are at most $v\pi r_1^2$ eavesdroppers in the circle where v is a constant as is shown in Lemma 5 and the SINR received by each eavesdropper is upper bounded by the results in Lemma 1. Thus, the cumulative SINR received by eavesdroppers can be calculated as

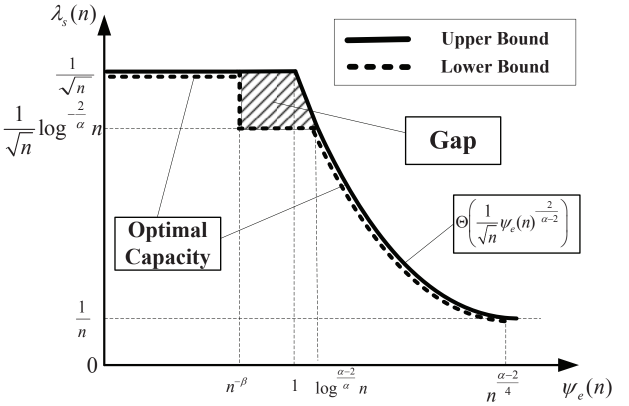

Fig. 3: An illustration of both upper bound and lower bound of secrecy capacity in large-scale networks. The scales of the axes are in terms of the orders in n.

$$\begin{aligned} \text{SINR}_e &\leq v\pi r_1^2 \frac{P_t}{P_r}(1 + d_{rt})^\alpha + \int_{r_1}^{\infty} \frac{P_t r^{-\alpha}}{N_0} 2\pi r v dr \\ &= v\pi r_1^2 \frac{P_t}{P_r}(1 + d_{rt})^\alpha + \frac{P_t 2\pi v r_1^{2-\alpha}}{N_0(\alpha-2)}. \end{aligned} \tag{13}$$

When packets are delivered along the highway, where the distance between T-R pairs is $d_{rt} = \Theta(1)$ and the rate $R(d)$ is a positive constant, there exists constants c_6 and c_7 such that $R_e \leq \text{SINR}_e \leq \frac{1}{2}R(d)$ when $r_1 = c_6$ and $P_r = c_7 r_1^2$. As shown in Equation (6), the concurrent transmission range k is $\Theta(P_r^{\frac{1}{\alpha}})$ and hence is $\Theta(1)$. So the secrecy rate each node on the highway can transmit is $\Theta(1)$. Since the node should relay at most $\Theta(\sqrt{n})$ nodes' traffic, the per-node secrecy capacity is $\Omega(\frac{1}{\sqrt{n}})$.

When the transmission is on the draining and delivery cases where $d_{rt} = \Theta(\log n)$, the rate each cell can transmit is $\Theta(\log^{-\alpha} n)$ as shown in Lemma 3. By choosing $r_1 = c_8 \log^{\frac{\alpha}{\alpha-2}} n$ and $P_r = c_9 r_1^2 \log^\alpha n$ where c_3 and c_4 are both constants, we can obtain $\text{SINR}_e \leq \frac{1}{2}R(d)$. The concurrent transmission range k is $\Theta(P_r^{\frac{1}{\alpha}}) = \Theta(\log^{\frac{3\alpha-2}{\alpha-2}} n)$. Hence the secrecy throughput each cell can transmit is $\Theta(\log^{-\frac{6\alpha-4}{\alpha-2}} n \log^{-\alpha} n)$. Since there are at most $\Theta(\log n)$ nodes in the cell, the per-node secrecy capacity is $\Omega(\log^{-\frac{6\alpha-4}{\alpha-2}} n \log^{-\alpha-1} n)$.

Combining the results above, we conclude this theorem. ■

With Theorem 4 and Theorem 5, the per-node secrecy capacity can be summarized as follows.

$$\lambda_s(n) = \begin{cases} \Omega(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}}) & \psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n) \\ \Omega(\frac{1}{\sqrt{n}}\log^{-\frac{2}{\alpha}} n) & \psi_e(n) = [\Omega(n^{-\beta}), O(\log^{\frac{\alpha-2}{\alpha}} n)] \\ \Omega(\frac{1}{\sqrt{n}}) & \psi_e(n) = O(n^{-\beta}) \end{cases} \tag{14}$$

for any constant $\beta > 0$.

C. The Optimality of Our Scheme

In previous subsection, we have derived the lower bounds of the network secrecy capacity in collaborating case. However, the upper bound of the network secrecy capacity still remains unknown. We will focus on the upper bound in this subsection.

Theorem 7: Consider the wireless network $\mathscr{B}$ where legitimate nodes and eavesdroppers are independent poisson distributed with parameter 1 and $\psi_e(n)$ respectively, the per-node secrecy capacity is

$$\lambda_s(n) = \begin{cases} O(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}}) & \psi_e(n) = \Omega(1) \\ O(\frac{1}{\sqrt{n}}) & \psi_e(n) = O(1) \end{cases} . \quad (15)$$

Proof: When the transmission is on the highway, we assume that the concurrent transmission range is k and partition the network into disjoint subsquares with size $k \times k$. Denote the two squares with length $\frac{3k}{4}$ and length $\frac{k}{4}$ whose centers are both at node i as A_{1i} and A_{2i} respectively. Let the region $A_{1i} - A_{2i}$ be A_i . Denote the number of eavesdroppers located in A_i as N_{ei} where i ranges from 1 to $\frac{n}{k^2}$. Since the expectation of the number of eavesdroppers located in all the regions A_i is $\frac{n}{2}\psi_e(n)$, there are at least $\frac{n}{4}\psi_e(n)$ eavesdroppers in all the regions A_i when $\psi_e(n) \geq \frac{\log_{4/e} n}{n}$ according to Lemma 4. Hence there exists a node i such that N_{ei} will be greater than $\frac{k^2}{4}\psi_e(n)$.

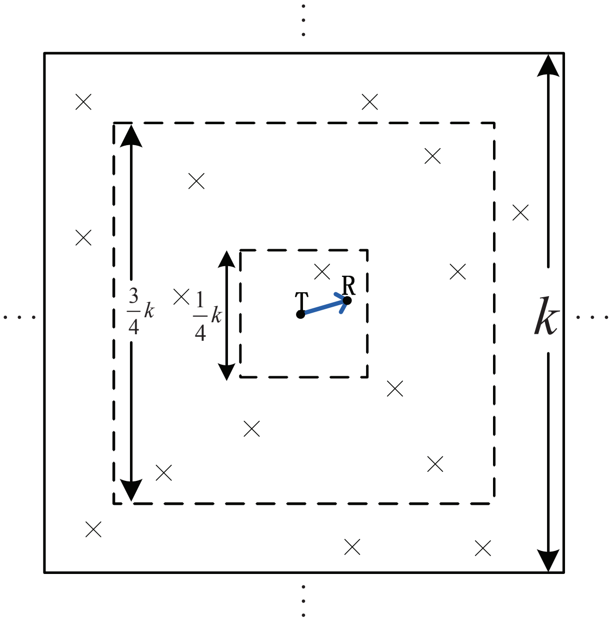

Fig. 4: An illustration of network partition to bound the lower bound of SINR received by eavesdroppers.

Consider a specific eavesdropper j in region i. Since the minimum distance between eavesdropper j and the eight closest concurrent transmission is at least $\frac{k}{4}$ and the next sixteen is at least $\frac{5k}{4}$, the interference eavesdropper j suffers from can be bounded as follows.

$$\begin{aligned} I_j &\leq \sum_{c=1}^{\infty} 8c(P_t + P_r)(\frac{k}{4} + (c-1)k)^{-\alpha} \\ &= (P_t + P_r)(k)^{-\alpha} \sum_{c=1}^{\infty} 8c(c - \frac{3}{4})^{-\alpha} \\ &\leq c_{10} P_r k^{-\alpha} \end{aligned} \quad (16)$$

where c_{10} is a constant.

As is shown in Theorem 1, k should be $\Omega(P_r^{\frac{1}{\alpha}})$. Therefore, the interference eavesdropper j suffers from can be bounded by a constant. The maximum distance between eavesdropper j and the closest transmitter is at most $\frac{3k}{4}$. Hence, the SINR received by all the eavesdroppers in region A_i can be lower bounded by

$$\begin{aligned} \text{SINR}_e &\geq \sum_j \frac{S_j}{N_0 + I_j} \\ &\geq N_{ei} \frac{(\frac{3k}{4})^{-\alpha}}{N_0 + \overline{I_j}} \\ &\geq c_{11}\psi_e(n)k^{2-\alpha}, \end{aligned} \quad (17)$$

when c_{11} is a constant.

Since the rate at which each T-R pair can transmit is $\Theta(1)$, we should choose $k = \Omega(\psi_e(n)^{\frac{1}{\alpha-2}})$ to ensure the secrecy of transmission. Note that there are k^2 cells in each subsquare taking turn to transmit and each node in the highway should carry the traffic load of $\Theta(\sqrt{n})$ nodes. Hence the per-node secrecy capacity is at most $O(\frac{1}{k^2\sqrt{n}}) = O(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}})$.

Note that according to Theorem 3, the per-node secrecy capacity is at most $O(\frac{1}{\sqrt{n}})$. Therefore, the upper bound of secrecy capacity is $\min(O(\frac{1}{\sqrt{n}}), O(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}}))$. ■

Compared with Theorem 4, our scheme achieves optimal secrecy capacity when $\psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n)$ and $\psi_e(n) = O(n^{-\beta})$ for any constant $\beta > 0$. And when $\psi_e(n) = O(\log^{\frac{\alpha-2}{\alpha}} n)$, our scheme is close to the optimal one. A more clear picture of such optimality is illustrated in Fig. 3. And we leave it as our future work to further close this gap.

V. Secrecy Capacity in Dense Networks

In previous section, we have considered secrecy transmissions in extended networks. Now we will extend it to dense networks where nodes are poisson distributed in a unit square. On surface, the difference seems to be only a scale factor of $\sqrt{n}$ and all the results can be applied to the dense networks directly. However, we note that this is not the case because the path loss gain in extended networks is bounded while it is unbounded in dense networks. Consider that an eavesdropper is quite close to the transmitter, the SINR at the eavesdropper will be quite large. Hence we should first consider the minimum distance between eavesdroppers and the transmitters which is denoted by c. Let N_e be the number of eavesdroppers in the dense network. When $n\pi c^2 N_e = o(1)$, the region inside the circles centered at transmitters with diameter c will be empty of eavesdroppers.

Conducting similar derivation in Theorem 1, we can obtain that $\text{SINR}_e \le c_1 \frac{P_t}{P_r}(\frac{1}{c\sqrt{n}})^\alpha$ and $\text{SINR}_l \ge c_2 P_t(\sqrt{n})^\alpha$ when the concurrent transmission range k is greater than $P_r^{\frac{1}{\alpha}}$. To assure the transmission is secret, we choose $P_r = \Theta((\frac{1}{cn})^\alpha)$. Hence, the concurrent transmission range is $\Theta(\frac{1}{cn})$ and the per-node secrecy capacity is $\Omega(\frac{1}{\sqrt{n}}(\frac{cn}{\sqrt{n}})^2) = \Omega(\frac{1}{\sqrt{nN_e}})$.

VI. Secrecy Capacity under Active Attacks

We now consider the static ad hoc networks under jamming attacks in which jammers keep sending out radio waves to interrupt the legitimate nodes. This will cause additional interference and hence may degrade the performance of legitimate nodes. For simplicity, we assume the power utilized by all the jammers is the same, denoted by P_m and $P_m = \Theta(1)$.

Assume that jammers are poisson distributed with parameter $\psi_m(n)$ in the network and the set of jammers is denoted by Φ_m. For a given transmitter-receiver pair, we partition the network into disjoint rings with a same size of $f(n)$. The receiver is at the center of all these rings. Let r_i be the external diameter of the ith ring. Since $f(n) = \pi r_1^2 = \pi(r_i^2 - r_{i-1}^2)$ for any $i > 1$, we have $r_i = \sqrt{i} r_1$ for any $i \ge 1$. Denote Φ_{mi} as the sets of eavesdroppers located inside ith ring. Hence the number of eavesdropper N_{mi} in Φ_{mi} is a poisson variable with parameter $\psi_m(n)f(n)$. Recalling Lemma 4, we have

$$P(\frac{1}{2}f(n)\psi_m(n) \le N_m \le 2f(n)\psi_m(n), \forall i) = 1,$$

when $f(n)\psi_m(n) \ge \log_{4/e} n$ and $f(n) = \Omega(1)$.

Notice that the distance between the receiver and jammers is at least r_{i-1}, the interference at the receiver caused by jammers in the i-th ring is at most $P_m r_{i-1}^{-\alpha}$ for any $i \ge 2$. For each $\psi_m(n)$, we choose $f(n)$ such that $f(n)\psi_m(n) \ge \log_{4/e} n$ and $f(n) = \Omega(1)$. Denote I_{mi} as the interference caused by jammers in the i-th ring. Taking the summation of interference caused by jammers in all the rings up, we have

$$\begin{aligned}
\text{I}_m \le& \sum_i \text{I}_{mi} \\
=& \sum_{j\in\Phi_{m1}} \text{I}_{1j} + \sum_{i=2}^{+\infty} \sum_{j\in\Phi_{mi}} \text{I}_{ij} \\
\le& 2f(n)\psi_m(n)\overline{\text{I}_{m1}} + \sum_{i=2}^{+\infty} 2f(n)\psi_m(n)\overline{\text{I}_{mi}} \\
\le& 2f(n)\psi_m(n)P_m + \sum_{i=2}^{+\infty} 2f(n)\psi_m(n)\frac{P_m r_{i-1}^{-\alpha}}{N_0} \\
=& 2P_m f(n)\psi_m(n)\left(1 + \sum_{i=2}^{+\infty}\frac{r_i^{-\alpha}}{N_0}\right) \\
\le& c_1 1 P_m f(n)\psi_m(n),
\end{aligned} \tag{18}$$

where c_{11} is a constant.

Similar to Section III, the highway system is adopted to transmit the messages across the network. Different from Section III, the scheduling scheme will not vary with the density of jammers. Choose the concurrent transmission range k as $2d+1$ where d is the distance between legitimate T-R pairs. According to Lemma 2, the interference $I(d)$ caused by other concurrent transmissions can be bounded as a constant. Hence, the rate that a receiver can obtain is

$$\begin{aligned}
R(d) =& \frac{P_t d^{-\alpha}}{I(d) + I_m} \\
\ge& c_{12}\frac{P_t d^{-\alpha}}{f(n)\psi_m(n)},
\end{aligned} \tag{19}$$

where c_{12} is a constant.

Case 1: When $\psi_m(n) \le \log n$, choosing $f(n)$ to satisfy the conditions in Lemma 4, it is obvious to see that $R(d) = \Omega(\frac{d^{-\alpha}}{\log n})$. When the transmission is on the highway phases which means $d = \Theta(1)$, $R(d) = \Omega(\frac{1}{\log n})$. Since the node on the highway should carry the load of at most $\sqrt{n}$ nodes according to Lemma 4, the per-node capacity is $\Omega(\frac{1}{\sqrt{n}\log n})$. When the transmission is on the draining and delivery phases where $d = \Theta(\log n)$, $R(d) = \Omega(\log^{-\alpha-1} n)$. Since this rate should be shared by at most $\log n$ nodes according to Lemma 3, the per-node capacity is $\Omega(\log^{-\alpha-2} n)$. Combing the results above, the per-node capacity is $\Omega(\frac{1}{\sqrt{n}\log n})$.

Case 2: When $\psi_m(n) \ge \log n$, choosing $f(n) = \Theta(1)$, we can see that $R(d) = \Omega(\frac{d^{-\alpha}}{\psi_m(n)})$ from Equation 19. Similar to the derivation in case 1, the per-node capacity can be obtained which is $\Omega(\frac{1}{\sqrt{n}\psi_m(n)})$ on the highway phase while it is $\Omega(\frac{\log^{-\alpha} n}{\psi_m(n)})$ on the draining and delivery phase. Hence, the per-node throughput is $\Omega(\frac{1}{\sqrt{n}\psi_m(n)})$ when $\psi_m(n) \ge \log n$.

Combining these two cases, we present the following theorem which demonstrates the achievable capacity jamming attacks.

Theorem 8: Consider the wireless network $\mathscr{B}$ where legitimate nodes and jammers are independent poisson distributed with parameter 1 and $\psi_m(n)$ respectively, the per-node capacity is

$$\lambda_m(n) = \left\{ \begin{array}{ll} \Omega(\frac{1}{\sqrt{n}\psi_m(n)}), & \psi_m(n) \ge \log n \\ \Omega(\frac{1}{\sqrt{n}\log n}), & \psi_m(n) < \log n \end{array} \right. . \tag{20}$$

According to Lemma 5, when $\psi_m(n) = o(n^{-\beta})$ for any constant $\beta \ge 0$, the number of jammers will be upper bounded by $\Theta(1)$ *w.h.p.*. However, in previous lemma, the upper bound of the number of jammers is still $\Omega(\log n)$ and hence the result is not tight. Therefore, we re-investigate this problem in the following context.

Theorem 9: If jammers are poisson-distributed in the network with intensity $\psi_m(n) = O(n^{-\beta})$ for any constant $\beta > 0$, the per-node capacity is $\Omega(\frac{1}{\sqrt{n}})$.

Proof: To compute the interference at the receiver, we divide the network into two parts. One is the circle which is at most r_1 distance from the receiver, the other is the rest of the network. There are at most $v\pi r_1^2$ jammers in the circle where $v = \lceil\frac{1}{\beta}\rceil + 1$ is a constant as is shown in Lemma 5. Thus, the cumulative interference at the receiver can be calculated as

$$\begin{aligned} I_m &\leq v\pi r_1^2 P_m + \int_{r_1}^{\infty} \frac{P_m r^{-\alpha}}{N_0} 2\pi r v dr \\ &= v\pi r_1^2 P_m + \frac{P_m 2\pi v r_1^{2-\alpha}}{N_0(\alpha-2)}. \end{aligned} \tag{21}$$

Hence, choosing $r_1 = \Theta(1)$, I_m can be bounded as a constant. According to Equation 19, $R(d) = \frac{P_t d^{-\alpha}}{I(d)+I_m} = \Omega(d^{-\alpha})$. After similar derivation in the proof of Theorem 8, we conclude this theorem. ■

Now, we can summarize the per-node capacity as follows.

$$\lambda_m(n) = \begin{cases} \Omega(\frac{1}{\sqrt{n}\psi_m(n)}), & \psi_m(n) = \Omega(\log n) \\ \Omega(\frac{1}{\sqrt{n}\log n}), & \psi_m(n) = [\Omega(n^{-\beta}), O(\log n)] \\ \Omega(\frac{1}{\sqrt{n}}) & \psi_e(n) = O(n^{-\beta}) \end{cases} \tag{22}$$

for any constant $\beta > 0$.

Similar to the proof in Part B, Section IV, we can also prove the upper bound of capacity under the presence of jammers.

Theorem 10: Consider the wireless network $\mathscr{B}$ where legitimate nodes and jammers are independent poisson distributed with parameter 1 and $\psi_m(n)$ respectively, the per-node capacity is

$$\lambda_m(n) = \begin{cases} O(\frac{1}{\sqrt{n}\psi_m(n)}) & \psi_e(n) = \Omega(1) \\ O(\frac{1}{\sqrt{n}}) & \psi_e(n) = O(1) \end{cases}. \tag{23}$$

VII. Discussion

A. Relaxation on Some Assumptions

In our model, both CSI and the position information of eavesdroppers are assumed to be unknown to legitimate nodes. It can be seen from Figure 2 that there exists a gap between the lower bound and the upper bound of per-node capacity, when the intensity of eavesdroppers is in the range $[\Theta(n^{-\beta}), \Theta(\log^{\frac{\alpha-2}{\alpha}} n)]$. Thus, it turns out to be a tempting issue whether the secrecy capacity can be improved if some of the information is known.

Note that the gap is caused by the randomness in Poison distribution, since a jump of $\log n$ number of nodes per unit area occurs at the point $\psi_e = 1$. Taking the concurrent transmission range for instance, it has to be set uniform over the whole network to guarantee the transmission secrecy for each T-R pairs in the worst case. However, it can be solved in the case where the information such as the positions of eavesdroppers are known. Because different artificial noise generation powers and different concurrent transmission ranges can be exhibited at different T-R pairs. Hence, it is possible to narrow this gap, by appropriate adjustments on the number of concurrent transmission nodes as well as the corresponding TDMA schemes, which results into capacity improvement. We leave it as our future work for further investigation on the problem.

B. Secrecy Capacity in Random Networks

The difference between Poison distributed network and the random network lies in that with network divided into multiple regions, the numbers of nodes inside a specific region in the former one are mutually independent poisson variables whereas it is not the case in the latter one. Hence it is often computable in poisson networks due to this independence property. In contrast, this does not necessarily hold in random networks since the total number of nodes in the network is given. Thus, the number of nodes inside a given region may affect the distribution probability of that in other regions. However, it is shown in [26] that random networks will converge to Poisson scenarios as n goes to infinity which is also proved in Appendix from another perspective. Hence, our results still hold when applied to random networks.

C. Some Extensions

From the derivations in Section IV, it can be seen that secrecy capacity is strongly related to both the density of eavesdroppers and the distance between the T-R pairs. A larger distance between T-R pairs means that more artificial noise should be generated to decrease the eavesdroppers' SINR. Thus, the concurrent transmission range needs to be enlarged to make sure that legitimate receivers do not interfere with each other. The model presented captures the secrecy constraints by the underlying interference and relies weakly on the specific settings. Hence it can be easily extended to general networks with multicast traffic pattern or mobile nodes such as *i.i.d.* mobility model, one-dimensional mobility model, random walk mobility model and etc. Under the assumption that the legitimate nodes' and eavesdroppers' distribution are both Poison-distributed, the optimality of these models is preserved in secrecy concerned networks. Combined with the artificial noise generation and TDMA scheduling scheme proposed in our paper, the following results are straightforward from [23], [17], [28] and [29].

Denote function $f(\psi_e(n))$ as

$$f(\psi_e(n)) = \begin{cases} \Theta(\psi_e(n)^{-\frac{2}{\alpha-2}}) & \psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n) \\ \Omega(\log^{-\frac{2}{\alpha}} n) & \psi_e(n) = [\Omega(n^{-\beta}), O(\log^{\frac{\alpha-2}{\alpha}} n)] \\ \Theta(1) & \psi_e(n) = O(n^{-\beta}) \end{cases}$$

for any constant $\beta > 0$.

Corollary 1. Assume that legitimate nodes and eavesdroppers are independent poisson distributed in $\mathscr{B}$ with parameter 1 and $\psi_e(n)$ respectively. For each legitimate node, $k-1$ nodes are randomly chosen as its destinations. For independent eavesdroppers case, the aggregated multicast secrecy capacity is $\Theta(\sqrt{\frac{n}{k\log n}} \cdot \log^{-\alpha-4} n)$ when $k = O(\frac{n}{\log n})$ and is $\Theta(\log^{-\alpha-4} n)$ when $k = \Omega(\frac{n}{\log n})$. For colluding eavesdroppers case, the aggregated multicast secrecy capacity is $\Theta(f(\psi_e(n))\sqrt{\frac{n}{k\log n}} \cdot \log^{-\alpha-4} n)$ when $k = O(\frac{n}{\log n})$ and is $\Theta(f(\psi_e(n))\log^{-\alpha-4} n)$ when $k = \Omega(\frac{n}{\log n})$.

Corollary 2. Consider a cell-partitioned network under the two-hop relay algorithm proposed in [17], and assume that nodes change cells i.i.d. and uniformly over each cell every timeslot. For independent eavesdroppers case, the per-node secrecy capacity is $\Theta(1)$ and the corresponding delay is

$\Theta(n)$. For colluding case, the per-node secrecy capacity is $\Theta(f(\psi_e(n))$ and the corresponding delay is $\Theta(\frac{n}{f(\psi_e(n))})$.

Corollary 3. Under random walk mobility model, nodes can only move to adjacent cells every timeslot. For independent eavesdroppers case, the per-node secrecy capacity is $\Theta(1)$ and the corresponding delay is $\Theta(n \log n)$. For colluding case, the per-node secrecy capacity is $\Theta(f(\psi_e(n))$ and the corresponding delay is $\Theta(\frac{n \log n}{f(\psi_e(n))})$.

Corollary 4. Since it is shown by J. Mammen and D. Shah [29] that the capacity and delay under one-dimensional random walk mobility model are the same as that without the 1-D mobility constraint which is also the case in our model. Hence, the secrecy capacity and correspondence delay are the same as that in Corollary 3.

D. Comparison with Previous Work

It is shown in [12] that the per-node secrecy throughput is $\Theta(\frac{1}{\sqrt{n}})$ which means there is no secrecy capacity loss when $\frac{\psi_e}{\psi} = o((\log n)^{-2})$. This result coincides with part of the results presented in our paper. In [12], secrecy guard zone assumed to contain no eavesdroppers existing in a region around the legitimate nodes is adopted to enhance secrecy transmission under the attack of independent eavesdroppers. However, they do not discuss in their paper how to establish a guard zone and what is the secrecy capacity when $\frac{\psi_e}{\psi} = \Omega((\log n)^{-2})$.

Zhang *et al.* [20] show that the per-node secrecy capacity is $\Theta(\frac{1}{\sqrt{n \log n}})$ when $p_f = \Omega(\frac{1}{\log n})$ and $\Theta(\sqrt{\frac{p_f}{n}})$ when $p_f = \left[\Omega(\frac{\log n}{n}), O(\frac{1}{\log n})\right]$. Here p_f represents the probability that neighboring nodes have a common key used to establish security association and is independent with the density of eavesdroppers. To guarantee the connectivity of authenticated nodes, the concurrent transmission range varies as p_f changes. Hence, the relationship between our result and theirs is the underlying concurrent transmission chances, since we focus on the interference model whereas they rely on cryptographic techniques.

Liang *et al.* [14] show that the per-node secrecy capacity in mobile ad hoc network is $\Theta(\sqrt{\frac{D}{n}})$ when $\psi_e = o(\sqrt{\frac{D}{n}})$ and $\Theta(\frac{1}{n\psi_e})$ when $\psi_e = \Omega(\sqrt{\frac{D}{n}}\text{poly}(n))$, with D being the delay constraint. Note that there will be chances that the closest node to the transmitter is the intended receiver when the delay is sufficiently large. Hence, the secrecy is guaranteed by the mobility of legitimate nodes while ours focus on static networks.

To make use of the channel fading gain, it can be seen that the concurrent transmission region in [11] is much larger than that in our paper. Hence more throughput has to be sacrificed to ensure the security. Furthermore, it is not studied in their paper the secrecy capacity when the density of eavesdroppers is larger than 1 while we make such investigation in our work.

VIII. Conclusion and Future Work

Secrecy of message delivery is a major concern in a lot of real applications. This paper studies the asymptotic behavior of secrecy capacity in an ad hoc network where both the channel state information and locations of eavesdroppers are unknown. With interference cancelation, we propose a novel construction which enhances network security greatly. Relationships of secrecy capacity and the density of eavesdroppers are investigated for both independent eavesdroppers and colluding case. Extensions to dense networks and the effect of other eavesdropping models and mobility models are also discussed. Jamming as a different kind of network attacking is also investigated. The most interesting insight in our paper perhaps is the shift on the pattern how legitimate nodes generate noises which may shed insight into the future design of wireless networks.

The secrecy issue in large-scale networks are strongly correlated with the node distributions of both legitimate nodes and eavesdroppers, also depends on how the packets is delivered across the network. Hence, it is an interesting future work to study the relationship between the secrecy capacity and the heterogeneity distributions of nodes. Finally, as social network is more and more important in our daily life, how to ensure the secrecy transmission is also of great interest.

References

[1] C. E. Shanon, “Communication Theory of Secrecy Systems”, in *J. Bell Syst. Tech.*, Vol.28, pp.656-715, 1948.

[2] A. D. Wyner, “The Wire-Tap Channel”, in *J. Bell Sys. Tech.*, Vol. 54, No. 8, pp. 1355-1367, Oct. 1975.

[3] I. Csiszár and J. Körner, “Broadcast Channels with Confidential Messages”, in *IEEE Trans. Inform. Theory*, Vol. 24, No. 3, pp. 339-348, July 1978.

[4] M. Haenggi, “The Secrecy Graph and Some of Its Properties”, in *Proc. IEEE ISIT*, Toronto, Canada, July 2008.

[5] P. C. Pinto, J. Barros, M. Z. Win, “Wireless Secrecy in Large-Scale Networks.” in *Proc. IEEE ITA’11*, California, USA, Feb. 2011.

[6] S. Goel and R. Negi, “Guaranteeing Secrecy using Artificial Noise”, in *IEEE Trans. Wireless Commun.*, Vol. 7, No. 6, pp. 2180-2189, 2008.

[7] E. Perron, S. Diggavi, and E. Telatar, “On Cooperative Wireless Network Secrecy”, in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, Apri. 2009.

[8] T. Liu and S. Shamai, “A Note on the Secrecy Capacity of the Multiple Antenna Wiretap Channel”, in *IEEE Trans. Inform. Theory*, Vol. 55, No. 6, pp. 2547-2553, June 2009.

[9] A. Khist and G. W. Wornell, “Secure Transmission with Multiple Antennas–Part II: The MIMOME Wiretap Channel”, in I*EEE Trans. Inform. Theory*, Vol. 56, No. 11, pp. 5515-5532, 2010.

[10] M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, “Wireless Information-theoretic Security”, in *IEEE Trans. Inform. Theory*, Vol. 54, No. 6, pp. 2515-2534, 2008.

[11] S. Vasudevan, D. Goeckel and D. Towsley, “Security-capacity Trade-off in Large Wireless Networks using Keyless Secrecy”, in *Proc. ACM MobiHoc*, Chicago, Illinois, USA, Sept. 2010.

[12] O. Koyluoglu, E. Koksal, E. Gammel, “On Secrecy Capacity Scaling in Wireless Networks”, submitted to *IEEE Trans. Inform. Theory*, Apr. 2010.

[13] X. Zhou, R. K. Ganti, J. G. Andrews and A. Hjorungnes, “The Throughput Cost of Information-Theoretic Security in Decentralized Wireless Networks”, *Arxiv preprint arXiv: 1012.4552*.

[14] Y. Liang, H. V. Poor and L. Ying, “Secrecy Throughput of MANETs under Passive and Active Attacks”, to appear in *IEEE Trans. Inform. Theory*.

[15] J. I. Choiy, M. Jainy, K. Srinivasany, P. Levis and S. Katti, “Achieving Single Channel, Full Duplex Wireless Communication”, in *ACM Mobicom’10*, Chicago, USA, Sept. 2010.

[16] P. Gupta and P. Kumar, “The Capacity of Wireless Networks”, in *IEEE Trans. Inform. Theory*, Vol. 46, No. 2, pp. 388-404, Mar. 2000.

[17] M. J. Neely and E. Modiano, “Capacity and Delay Tradeoffs for Ad Hoc Mobile Networks”, in *IEEE Trans. Inform. Theory*, Vol. 51, No. 6, pp. 1917-1937, 2005.

[18] M. Franceschetti, O. Dousse, D. N. Tse and P. Thiran, “Closing the Gap in the Capacity of Wireless Networks via Percolation Theory”, in *IEEE Trans. Inform. Theory*, Vol. 53, No. 3, pp. 1009-1018, 2007.

[19] M. Garetto, P. Giaccone, and E. Leonardi, “Capacity Scaling in Ad Hoc Networks with Heterogeneous Mobile Nodes: The Super-Critical Regime, in *IEEE/ACM Trans. Networking*, Vol. 17, No. 5, pp. 1522-1535, 2009.

[20] C. Zhang, Y. Song, Y. Fang and Y. Zhang, “On the Price of Security in Large-Scale Wireless Ad Hoc Networks”, in *IEEE/ACM Trans. Networking*, Vol. 99, Issue 2, pp. 319-332, Apri. 2011.

[21] L. Ying, S. Yang and R. Srikant, “Optimal Delay-Throughput Tradeoffs in Mobile Ad Hoc Networks”, in *IEEE Trans. Inform. Theory*, Vol. 54, No. 9, Sep. 2008.

[22] M. Grossglauser and D. N. C. Tse, “Mobility Increases the Capacity of Ad Hoc Wireless Networks”, in *IEEE/ACM Trans. Networking*, Vol. 10, No. 4, pp. 477-486, 2002.

[23] X. Li, “Multicast Capacity of Wireless Ad Hoc Networks”, in *IEEE/ACM Trans. Networking*, Vol. 17, No. 3, pp. 950-961, 2009.

[24] B. Liu, P. Thiran and D. Towsley, “Capacity of a Wireless Ad Hoc Network with Infrastructure”, in *ACM MobiHoc’07*, New York, NY, USA, 2007.

[25] A. Özgür and O. Lévêque, “Throughput-Delay Trade-Off for Hierarchical Cooperation in Ad Hoc Wireless Networks”, in *Proc. Int. Conf. Telecom.*, Jun. 2008.

[26] M. Penrose, “Random Geometric Graphs”, *Oxford Univ. Press*, Oxford, U.K., 2003.

[27] T. Hagerup and C. R$\ddot{u}$b, “A guided tour of Chernoff bounds”, in *Inf. Process. Lett.*, Vol. 33, No. 6, pp. 305-308, Feb. 1990.

[28] A. Gamal, J. Mammen, B. Prabhakar, and D. Shah, “Throughput-delay trade-off in wireless networks”, In *Proceeding of IEEE INFOCOM*, Hong Kong, China, Mar. 2004.

[29] J. Mammen and D. Shah, “Throughput and Delay in Random Wireless Networks With Restricted Mobility”, in *IEEE Trans. Inform. Theory*, Vol. 53, No. 3, pp. 1108-1116, 2007.

IX. Appendix

Lemma 6: Partition the network into disjoint cells with equal size 1, if there are k nodes randomly distributed in the network, then the probability each cell has i nodes is

$$C_k^i(\frac{1}{n})^i(1-\frac{1}{n})^{k-i}. \tag{24}$$

Proof: Denote the number of cells that has i nodes in it as $T^{'}_{k}(i)$ and the expectation of $T^{'}_{k}(i)$ as $T_k(i)$. Consider there are k nodes in the network and a new node joins in. If the new node joins in a cell with i nodes, $T^{'}_{k+1}(i)$ should be $T^{'}_{k}(i)-1$ and $T^{'}_{k+1}(i+1)$ should be $T^{'}_{k}(i+1)+1$. Hence, we have

$$T^{'}_{k+1}(0)=\begin{cases} T^{'}_{k}(0) & \frac{n-T^{'}_{k}(0)}{n} \\ T^{'}_{k}(0)-1 & \frac{T^{'}_{k}(0)}{n} \end{cases}. \tag{25}$$

$$T^{'}_{k+1}(i)=\begin{cases} T^{'}_{k}(i)-1 & \frac{T^{'}_{k}(i)}{n} \\ T^{'}_{k}(i) & \frac{n-T^{'}_{k}(i)-T^{'}_{k}(i-1)}{n} \\ T^{'}_{k}(i)+1 & \frac{T^{'}_{k}(i-1)}{n} \end{cases} \tag{26}$$

for all $i \geq 2$ and $i \leq k$.

$$T^{'}_{k+1}(k+1)=\begin{cases} 0 & \frac{n-T^{'}_{k}(k)}{n} \\ 1 & \frac{T^{'}_{k}(k)}{n} \end{cases}. \tag{27}$$

Taking expectation of both sides, we have

$$\begin{cases} T_{k+1}(0)=T_k(0)(1-\frac{1}{n}) \\ T_{k+1}(i)=(1-\frac{1}{n})T_k(i)+\frac{1}{n}T_k(i-1) \\ T_{k+1}(k+1)=\frac{1}{n}T_k(k) \end{cases}. \tag{28}$$

Note that $T_0(0)=n$, $T_1(0)=n-1$ and $T_1(1)=1$, using mathematical induction, we have

$$T_k(i)=nC_k^i(\frac{1}{n})^i(1-\frac{1}{n})^{k-i}.$$

Since n cells are the same, we conclude this lemma. When n and k both goes to infinity, the probability converges to a poisson variable with parameter $\frac{k}{n}$.

■