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.**

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]. 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 [2] and Pinto *et al.* [3] 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 [4] 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 [5]. Furthermore, Barros *et al.* [6] 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.* [7] 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 or mobility on capacity is investigated by Koyluoglu *et al.* [8] , Zhou *et al.* [9] and [10]. 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 [11]. This differs our noise generation pattern from the work in [4] and [7] 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. Concluding remarks are given in the end.

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 [11].

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:

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

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

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

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

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

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

Asymptotic Capacity: Similar to [14], 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.

III. Security Capacity for independent eavesdroppers case

In this section, we investigate secrecy capacity for independent eavesdroppers. Since our scheme should guarantee the secrecy communication, it seems that the capacity should be degraded. However, we show that the secrecy capacity remains the same as that in the network without eavesdroppers at least in order sense. We first 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: Notice that $R_e = \log(1 + \max(\text{SINR}_e))$ and SINR_e is smaller than $\frac{P_t d_{te}^{-\alpha}}{N_0}$, we now prove the maximum SINR that eavesdroppers can obtain is $\frac{P_t}{P_r}(1 + d_{rt})^{\alpha}$. First consider the case when d_{te} and d_{re} are both greater than 1,

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

Under similar derivation, we can show that this lemma is also hold when d_{te} or d_{re} is smaller than 1.

■

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 [13], 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 $w = \kappa \log m / N_p$.

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.

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 [13], 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 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:

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

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

And the receiving signal $S(d)$ can be lower-bounded by

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

.

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

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

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

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:

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

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. To calculate per-node secrecy capacity, we first give two lemmas which can be proved using Chernoff bounds and union bounds.

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

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

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

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

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 is no larger than

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

$\kappa \log m + 2c$ 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.

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.By Lemma 4, we obtain that the maximum number of legitimate nodes inside each slice is no larger than $2w\sqrt{n}$. Therefore, the secrecy capacity of the highway phase is $\Omega(\frac{1}{\sqrt{n}})$.

■

Since the per-node throughput without the secrecy constraint is $O(\frac{1}{\sqrt{n}})$ [12], the per-node secrecy capacity is also bounded by $O(\frac{1}{\sqrt{n}})$ which indicates the optimality of our scheme.

IV. Colluding Eavesdroppers

A. Analysis of Secrecy Capacity

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 $\psi_e(n) f(n)$.

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 all the summation up, we have

$$\begin{aligned}
\text{SINR}_e &\leq \sum_i \text{SINR}_{ei} \\
&= \sum_{j \in \Phi_{e1}} \text{SINR}_{1j} + \sum_{i=2}^{+\infty} \sum_{j \in \Phi_{ei}} \text{SINR}_{ij} \\
&\leq 2f(n)\psi_e(n) \frac{P_t}{P_r}(1 + d_{rt})^\alpha + \sum_{i=2}^{+\infty} 2f(n)\psi_e(n) \frac{P_t r_{i-1}^{-\alpha}}{N_0} \\
&= 2\pi\psi_e(n) \left(r_1^2 \frac{P_t}{P_r}(1 + d_{rt})^\alpha + \frac{P_t}{N_0} r_1^{2-\alpha} \sum_{i=1}^{+\infty} i^{-\frac{\alpha}{2}} \right),
\end{aligned} \tag{7}$$

where the third row of this inequality follows from Lemma 1.

Case 1: When the transmission is on the highway phase where $d_{rt} = \Theta(1)$, 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 (7), 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 $O(\sqrt{n})$, the per-node throughput should be $\Omega(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}})$. If $\psi_e(n) = O(\log^{\frac{\alpha-2}{\alpha}} n)$, 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 $\log^{-\alpha} n$. 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 $\psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n)$, the per-node secrecy capacity is bounded by $\Omega(\psi_e(n)^{-\frac{2}{\alpha-2}} \log^{-\alpha-3} n)$. When $\psi_e(n) = O(\log^{\frac{\alpha-2}{\alpha}} n)$, 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 3: 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

$$\lambda_s(n) = \begin{cases} \Omega(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}}), & \psi_e(n) = \Omega(\log^{\frac{\alpha-2}{\alpha}} n) \\ \Omega(\frac{1}{\sqrt{n}}\log^{-\frac{2}{\alpha}} n), & \psi_e(n) = O(\log^{\frac{\alpha-2}{\alpha}} n) \end{cases}. \tag{8}$$

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

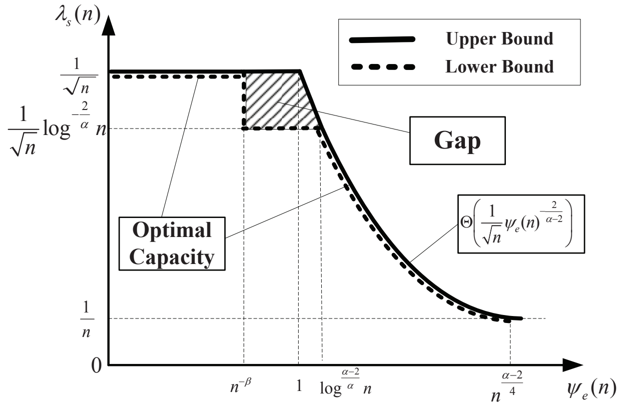

Fig. 1: An illustration of both upper bound and lower bound of secrecy capacity in large-scale networks. The scales of the axes are in terms of the orders in n.

by N_{ei} the number of nodes inside region i, we have

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

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

Theorem 4: 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 $\Omega(\frac{1}{\sqrt{n}})$.

Remark: Due to the space limit, we only present the basic idea behind this theorem. There are not enough eavesdroppers near the receiver according to Lemma 5. And the eavesdroppers far away can not affect the scaling law of secrecy capacity.

B. The Optimality of Our Scheme

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

$$\lambda_s(n) = \begin{cases} O(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}}) & \psi_e(n) = \Omega(1) \\ O(\frac{1}{\sqrt{n}}) & \psi_e(n) = O(1) \end{cases} . \tag{9}$$

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 $\frac{k^2}{4}\psi_e(n)$.

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 $I_j \leq c_6 P_r k^{-\alpha}$ where c_6 is a constant.

As is shown in Theorem 1, k should be $\Omega(P_r^{\frac{1}{\alpha}})$. 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

$$\begin{aligned} \text{SINR}_e &\geq \sum_j \frac{S_j}{N_0 + I_j} \\ &\geq N_{ei}\frac{(\frac{3k}{4})^{-\alpha}}{N_0 + I_j} \\ &\geq c_7 \psi_e(n) k^{2-\alpha}, \end{aligned} \tag{10}$$

when c_7 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 $O(\frac{1}{k^2\sqrt{n}}) = O(\frac{1}{\sqrt{n}}\psi_e(n)^{-\frac{2}{\alpha-2}})$. ■

V. Acknowledgment

This work is supported by National Fundamental research grant (2011CB302701), NSF China (No. 60832005); China Ministry of Education New Century Excellent Talent (No. NCET-10-0580); China Ministry of Education Fok Ying Tung Fund (No. 122002); Qualcomm Research Grant; Shanghai Basic Research Key Project (No.11JC1405100); National Key Project of China (2010ZX03003-001-01).

References

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

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

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

[4] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise", in *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", in *Proc. IEEE INFOCOM*, Rio de Janeiro, Brazil, Apri. 2009.

[6] 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.

[7] S. Vasudevan, D. Goeckel and D. Towsley, "Security-capacity Tradeoff in Large Wireless Networks using Keyless Secrecy", in *Proc. ACM MobiHoc*, Chicago, Illinois, USA, Sept. 2010.

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

[9] 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*.

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

[11] 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.

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

[13] 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.

[14] X. Wang, W. Huang, S. Wang, J. Zhang, C. Hu, "Delay and Capacity Tradeoff Analysis for MotionCast," in IEEE/ACM Transactions on Networking, Vol. 19, no. 5, pp. 1354-1367, Oct 2011.