Research Article

Secrecy Throughput in Inhomogeneous Wireless Networks with Nonuniform Traffic

Qiuming Liu,1,2 Li Yu,1 Peng Yang,1 and Zuhao Liu3

1 The Department of Electronics and Information Engineering, Huazhong University of Science and Technology (HUST), Wuhan 430074, China
2 Nanchang University of Science and Technology (JXUST), Nanchang 330013, China
3 China Yangtze Power Co., Ltd., Yichang 443002, China

Correspondence should be addressed to Li Yu; hustlyu@hust.edu.cn

Received 2 June 2014; Revised 11 September 2014; Accepted 25 September 2014; Published 27 October 2014

1. Introduction

Security is an important issue in wireless ad hoc networks [1], especially in commercial, government, and military networks. Because of the broadcast nature of wireless channel in multihop wireless networks, it is vulnerable to eavesdroppers and malicious nodes. Traditional methods are based on cryptographic technology such as the well-known RSA public key cryptosystem. However, with the increasing of network size, especially in large-scale wireless networks, cryptosystem encounters some limitation, such as expensive key distribution and improvement on decoding technology, which induces more cost and complicated maintenance. In [2, 3], the authors showed that the capacity of wireless ad hoc networks was \( \Omega(\sqrt{p_f/n \log n}) \) (Given two functions \( f(n) \) and \( g(n) \): \( f(n) = o(g(n)) \) means \( \lim_{n \to \infty} f(n)/g(n) = 0 \); \( f(n) = O(g(n)) \) means \( \lim_{n \to \infty} f(n)/g(n) = c < \infty \); \( f(n) = O(g(n)) \) and \( f(n) = \Omega(g(n)) \) means \( f(n) = \Theta(g(n)) \) when logarithmic terms are ignored.), where \( p_f \) was the probability that a node shared a primary secure association (SAs) with any other nodes and \( n \) was the number of nodes in the network. Hence, to avoid the degradation on the throughput caused by \( p_f \), a method of information theoretic security was proposed by exploiting the difference between channels of legitimate nodes with that of eavesdroppers. In [4], Goel and Negi proposed an artificial noise generation method to suppress eavesdroppers’ receiving signal. Different from [4], Choi II et al. [5] assumed a legitimate node was equipped with three antennas. The noise was generated by the receivers and can be eliminated using the technique of antennas cancelation. Consequently, it is urgent to reveal the effect of this technology on the network performance such as capacity and connectivity. In [6], Vasudevan et al. investigated the trade-off between capacity and security in large-scale wireless networks. To
analyze the cases of independent eavesdropper, eavesdropper with multiple antennas, and colluding eavesdroppers. The authors showed that there exists a critical threshold on the density \( \psi_e \) of malicious node. That was, when \( \psi_e = \Theta(\sqrt{D/n}) \), the per-node secrecy capacity was \( \Theta(\sqrt{D/n}) \), and when \( \psi_e = \Omega(\sqrt{D/n} \text{polylog} n) \), the per-node secrecy capacity was \( \Theta(1/n\psi_e) \), where \( D \) was the delay constraint. Latter on, Çapar et al. [10] considered one-dimensional and two-dimensional ad hoc networks, where the number of eavesdroppers was \( o(n/\log n) \) and the location information of eavesdroppers was unknown. To degrade the signal quality of eavesdroppers, they exploited legitimate information of eavesdroppers, they concluded that the per-node secrecy throughput is \( \Omega(\sqrt{D/n}) \) in one-dimensional and \( \Omega(\sqrt{1/n \log n}) \) in two-dimensional networks, respectively. This result was the same order with the ground-breaking work by Gupta and Kumar [11]. More recently, Zhang et al. [12] constructed a highway system in the network and analyzed the cases of independent eavesdropper, eavesdropper with multiple antennas, and colluding eavesdroppers. The results showed that the secrecy capacity for independent eavesdropper was \( \Omega(1/\sqrt{n}) \), which was the same order with the result [13]. Furthermore, they also obtained that the per-node secrecy capacity can keep the order of \( \Theta(1/\sqrt{n}) \) when the eavesdroppers colluded with each other and the density of eavesdropper was \( o(n^{-\beta}) \).

However, all the works on the scaling law of secrecy capacity were based on homogeneous ad hoc networks; for instance, nodes were distributed uniformly or according to the homogeneous Poisson process, and the destination was randomly selected. In most realistic case, nodes may form into some different clusters and the traffic may be usually occurred at local area, such as the traffic established over heterogeneous wireless networks (Wi-Fi, WLAN, WiMAX, etc.) which is particular inhomogeneous [14]. In [15], the authors considered the capacity property of clustered wireless network, where the node density did not show significant inhomogeneity. Later on, Perevalov et al. [16] used a Matern cluster process to achieve inhomogeneity. The node density inside the cluster was the same, whereas outside the cluster was the sea area. In their work, the bottleneck of the capacity was in the sea area. After that, Alfano et al. [17, 18] considered a more general inhomogeneous node process—SNCP [19], in which the node density was also scaled with the number of nodes. Besides, in [20], Martina et al. extended the inhomogeneous network model to different cluster size and investigated the scaling law of the capacity.

In this paper, we investigate the secrecy throughput capacity of wireless networks with inhomogeneous node density and nonuniform traffic. The node distribution is an inhomogeneous Poisson node process named as shot noise cox process (SNCP). Specifically, we assume \( n \) legitimate nodes uniformly located in \( m = \Theta(n^\epsilon) \) clusters within the area of \( A \) and followed SNCP in each cluster. Meanwhile, the eavesdroppers are uniformly distributed in the network area with density of \( \varphi_e \). We study the independent eavesdropper with single antenna and multiple antennas, respectively. To elaborate the nonuniform traffic, we partition the transmission into two parts: intracluster transmission and intercluster transmission. For intracluster transmission, we construct a novel circular percolation model in each cluster and derive that the per-node secrecy throughput is \( \Omega(\sqrt{1/(1-v)n^{1/2}\log n}) \). For the case of intercluster, we build “information pipelines” among each cluster according to minimum node density \( \Phi \) in the network. Then we achieve a secrecy rate of \( \Omega(\sqrt{n/\log n}) \) for each legitimate node among clusters. As for eavesdropper equipped with \( \Psi(n) \) antennas, the secrecy throughput is \( \Omega\left(\sqrt{1/n^{1-v}(1-v)\log n n^{1/2}\Psi(n)}\right) \) and \( \Omega\left(\sqrt{n/\log n}\Psi^{-1/2}(n)\right) \) for intracluster and intercluster transmission, respectively. Finally, we prove that the bottleneck of secrecy throughput is located in the area with minimum node density.

Since we firstly use percolation theory in inhomogeneous network model and propose a circular percolation model for the SNCP distributed network model, we will give a glance at the percolation theory. Percolation theory [21, 22] is a field of mathematics and statistic physics that provides models of phase transition phenomena. Assume that water is poured on top of a porous stone, will the water be able to make its way from hole to hole and reach the bottom? By modeling the stone as a square grid, each edge can be open and traversed by water with probability \( p \), or closed with probability \( 1-p \), and they are assumed to be independent. For a given \( p \), what is the probability that an open path exists from the top to the bottom? That is, is there a path of connected points of infinite length through the network? In fact, there exists a critical \( p_c \) below which the probability is always \( 0 \) and above which the probability is always \( 1 \). In some cases \( p_c \) may be calculated explicitly; for example, in two dimensions square lattice \( Z^2 \), when \( p > 1/2 \), water percolates through the stone with probability one. One can then ask at what rate the water percolates and how it depends on \( p \). In other words, how rich in disjoint paths are connected component of open edges? To maximize the information flow, we want to operate the network at \( p > 1/2 \), above the percolation threshold, so that we can guarantee the existence of many disjoint paths that traverse the network.

The rest of this paper is organized as follows. In Section 2, we present the network model. We give the transmission model in Section 3. The novel circular percolation model in each cluster is constructed in Section 4. Section 5 derives the secrecy throughput in intracluster transmission. In Section 6, we investigate the secrecy throughput of intercluster transmission. We extend the secrecy throughput to the case of eavesdropper with multiple antennas in Section 7 and conclude the paper in Section 8 with the discussion of some possible future works.
2. Network Model

We consider a network with $n$ legitimate nodes in a two-dimensional torus $\mathbb{N} = [0, \sqrt{A}]$, where $A = \Theta(n)$. All legitimate nodes follow an inhomogeneous Poisson process which is called shot noise cox process (SNCP). The SNCP can be simply described by the following construction. There are $M$ clusters randomly placed in the network and these cluster centers can be denoted by $C = \{c_j\}_{j=1}^M$, where $E(M) = m$. The center point $c_j$ is also called mother point. For each $c_j$, it generates a point process with an intensity of $q_j k(c_j, \xi)$ at point $\xi$, where $k(c_j, \xi)$ is a dispersion density function and the quantity $q_j$ equals the number of nodes generated by cluster center $c_j$. We assume that all cluster centers generate the same number of legitimate nodes; that is, $q_j = n/m$. Moreover, according to SNCP, the density function $F$ at point $\xi$ can be written as follows:

$$F(\xi) = \sum_{j} q_j k(c_j, \xi),$$

where $k(c_j, \xi) = k(||\xi - c_j||)$ depends only on the Euclidean distance $||\xi - c_j||$ between point $\xi$ and the cluster center $c_j$, and the integral $\int_A k(c_j, \xi) \, d\xi$ over the entire network is finite. To simplify the model, we employ function $s(\rho)$ to replace the density function $k(c_j, \xi)$, where $\rho = ||\xi - c_j||$. In order to gain finite integral over increasing network area, the function $s(\rho)$ is given below:

$$s(\rho) = \min(1, \rho^{-\delta}), \quad \delta > 2.$$  \hspace{1cm} (2)

In addition, we define $m$ scales as $\Theta(n^\nu)$, $\delta$ as degradation factor, and $\nu \in (0, 1)$. Then we can get that the number of nodes in each cluster is $\Theta(n^{1-\nu})$, that is, $q_j = \Theta(n^{1-\nu})$ for $j = 1, 2, \ldots, M$, since $\int_A k(c_j, \xi) \, d\xi$ is finite.

Other than legitimate nodes, the eavesdroppers are uniformly and independently distributed in the network with density $\varphi_e$. We assume eavesdroppers always keep silent since they will be easily detected if they are active. In order to have an insight on the fundamental information theoretical secrecy throughput, we also assume eavesdroppers have infinite computation ability which means that traditional cryptography method cannot be applied here. In addition, we assume that both channel state information (CSI) and location of eavesdropper are unknown to legitimate nodes.

Similar to [6, 12], we assume that each legitimate node is equipped with three antennas. When a legitimate node receives packets, one of the antennas is used for message reception, while the other two are applied to generate artificial noise to suppress the eavesdropper’s channel simultaneously. As depicted in [5], the distance between the receiving antenna and the other two artificial noise generation antennas should satisfy a different of half the wavelength. Thus the interference can be eliminated using the technique of self-interference cancelation.

We define $d_c$ as the average distance between neighboring cluster centers. Then we can get

$$d_c = \Theta\left(\frac{\sqrt{A}}{m}\right) = \Theta\left(n^{(1-\nu)/2}\right).$$  \hspace{1cm} (3)

Notice that $\nu < 1$, $d_c \to \infty$ as $n$ tends to infinity, the network is a cluster-sparse network. When $\nu = 1$, the network is transformed to homogeneous model and its secrecy throughput is similar to that in the homogeneous Poisson process (HPP) network [12]. In this paper, we focus on the cluster-sparse network in which the density of the whole network is not identical. We use $\Phi$ to denote the maximum node density and $\Phi$ for the minimum node density in the network.

3. Transmission Model

Let $T$ and $R$ denote the subsets of legitimate nodes simultaneously transmitting and receiving in a given time slot, and $\Gamma$ is the set of eavesdroppers.

We consider the Shannon capacity as the channel capacity between two nodes, and we define SINR$_{ij}$ as the signal to interference and noise ratio (SINR) from legitimate transmission node $i$ to legitimate destination node $j$ over a channel of unit bandwidth, which is given as follows:

$$\text{SINR}_{ij} = \frac{P_{ij} l(i, j)}{N_0 + \sum_{\zeta \notin \Gamma} P_{\zeta} l(\zeta, j) + \sum_{\zeta \in \Gamma} P_{\zeta} l(\zeta, j)},$$  \hspace{1cm} (4)

where $l(i, j) = \min[1, 1/d_{ij}^2]$ with $\alpha > 2$ and represents the path loss in the transmission between the node $i$ and node $j$. $P_{ij}$ and $P_{\zeta}$ denote the power of transmitting node $i$ and artificial noise generation, respectively. $N_0$ stands for noise power of the channel at the receive node $j$, and the $\zeta$ means the set of nodes which can transmit simultaneously with node $i$.

Similarly, we denote the SINR received by eavesdropper $e$ as follows:

$$\text{SINR}_{ie} = \frac{P_{ie} l(i, e)}{N_0 + \sum_{\zeta \notin \Gamma} P_{\zeta} l(\zeta, e) + \sum_{\zeta \in \Gamma} P_{\zeta} l(\zeta, e)}.$$  \hspace{1cm} (5)

According to the definition of secrecy throughput in [23], the secure rate between any legitimate nodes can be presented by

$$R_{ij} = R_{ij} - \overline{R}_{ie} = \log_2 (1 + \text{SINR}_{ij}) - \log_2 (1 + \text{SINR}_{ie}),$$  \hspace{1cm} (6)

where $\overline{\text{SINR}}_{ie} = \max_{\zeta \in \Gamma} \text{SINR}_{ie}$.

In our strategy, we employ different power for different nodes. We define rate $\lambda_1(n)$ the secrecy throughput which is the guaranteed rate that can be supported uniformly for source-destination pairs and it is also the average secrecy rate which can simultaneously be achieved by legitimate nodes with high probability (w.h.p.).
4. The Circular Percolation Model for Each Cluster

Following the roadmap of [12], we first construct a routing scheme for the network. As the legitimate nodes are distributed according to SNCP, we divide the transmission into two parts: intracluster traffic and intercluster traffic. For each part of transmission, we use percolation theory to construct the routing scheme. In intracluster traffic, we propose a circular percolation model, which is novel and different from the former percolation model. As for intercluster case, we build information pipelines to connect the clusters.

In our model, based on the idea that transform "inhomogeneous" to "homogeneous," we demonstrate a circular percolation model and build highway system for legitimate nodes in each cluster. Different from the previous highway construction [13], the highways based on our mode are not from bottom to top or left to right, but from inner cluster to external or around the cluster center. In addition, we adopt different transmission range for legitimate nodes while the transmission rate could stay the same.

Lemma 1. Assume that there is a minimum positive separation distance $r_{\text{min}}$ between the center and any nodes for each cluster. Then each cluster can build a highway system within a radius of $r_{\text{max}}$ for $\delta > 2$.

Proof. We first divide a given cluster into $x \times (n/m)/x$ circular lattices, where $x$ denotes the number of radius, and the arc between each neighboring radius is equal, that is, $2\pi/x$. $(n/m)/x$ is the number of concentric circles where the distance between each two neighboring circles is different.

Since SNCP is an inhomogeneous Poisson point process, the intensity at different circular sector area is different, so as to the area of each square. The external circular sectors are larger than the inner ones. From inner circle to external circle, we set the radius of the $i$th concentric circle is as follows:

$$r_i = \left(1 + \frac{2\pi}{x}\right)^{-1} \cdot r_{\text{min}}. \quad (7)$$

Thus, from the circular lattice described above, we can find that small circular area can be viewed as a square when $n$ approaches to infinite.

Lemma 2. To satisfy the cluster-sparse network in our model, the parameter $x$ should meet the condition that $x = \Theta(\sqrt[n]{1-v}/(1-v) \log n)$.

Proof. From Lemma 1, we know the radius of the entire lattice is

$$r_{(n/m)/x+1} = \left(1 + \frac{2\pi}{x}\right)^{n/m}x, \quad n \to \infty. \quad (8)$$

The distance between each two neighboring cluster is $d_c$.

Taking (3) and (8) into consideration together, we can derive the following equation:

$$r_{(n/m)/x+1} = \left(1 + \frac{2\pi}{x}\right)^{n/m}x = e^{2\pi n/m - 1}/x = \frac{d_c}{2}. \quad (9)$$

Finally, we can get $x = \Theta(\sqrt[n]{1-v}/(1-v) \log n)$. \hfill \Box

Lemma 3. Consider a square $s_i$ between the $i$th and $(i + 1)$th concentric circles; let $X_i$ denote the number of nodes distributed in $s_i$; then we can get $P(X_{s_i} \geq 1) > P(X_{s_i} \geq 1)$ for $i < j$.

Proof. Specifically, we say $s_i$ is open if there exists at least one node in square $s_i$, and close otherwise. According to Appendix A in [18], the probability that a square is open can be denoted by

$$p_i = P\left(X_{s_i} \geq 1\right) = 1 - P\left(X_{s_i} = 0\right) \approx 1 - e^{-(n/m)r_i^2(2\pi/x)^2}. \quad (10)$$

From (10), we can get that $p_i$ decreases for increasing values of $i$ on the preconditions of $\delta > 2$.

As the probability $p_i$ is decreased with the parameter $i$, we will calculate the critical value $\rho_{\text{max}}$, within which the probability $p_i$ can satisfy the condition of $p_i > p_c$.

Lemma 4. There exists a critical value $\rho_{\text{max}} = \Theta((1-v) \log n)^{1/(\delta-2)}$, within which each cluster can build a highway system for the degradation factor $\delta > 2$.

Proof. According to percolation theory, there exists a critical probability $p_c$, when $p > p_c$, the probability of the existence of many disjoint paths that traverse the network is going to one. Therefore, we can set the following equation by Lemma 3:

$$p_i = P\left(X_{s_i} \geq 1\right) \approx 1 - e^{-(n/m)r_i^2(2\pi/x)^2} = p_0, \quad (11)$$

where $p_0$ is the probability which denotes the square $s_i$ is open, and $p_c < p_0 < 1$.

Following this equation, we can derive that

$$\frac{n}{m} \cdot \frac{r_i - \delta}{r_i} \left(\frac{2\pi}{x}\right)^2 = c, \quad (12)$$

where $c = \ln(1/(1 - p_c))$. Substituting $x = \Theta((1-v) \log n)$ into (12), we can achieve $\rho_{\text{max}} = \Theta(((1-v) \log n)^{1/(\delta-2)})$.

According to Lemma 4 and (7), we can derive the critical value $\rho_{\text{max}} = \Theta((\log (\log n)/(\delta-2))/\sqrt[n]{1-v}/(1-v) \log n)$. Specifically, we can construct $\Theta((\log (\log n)/(\delta-2))/\sqrt[n]{1-v}/(1-v) \log n)$ concentric circle within the radius $\rho_{\text{max}}$.

Till now, we have established a percolation model for the intracluster transmission. The cluster is divided into a $c \times \sqrt[n]{1-v}/(1-v) \log n \times c((\log (\log n)/(\delta-2))/\sqrt[n]{1-v}/(1-v) \log n)$ grid $G_c$. We consider a path of $G_c$ is open if any two adjacent squares are open. Figure 1 is a part of one cluster lattice. Based on Appendix I in [13], we can obtain that there are $[\eta \log m]$ disjoint paths crossing a rectangle of size $m \times (\kappa \log m - \epsilon_m)$. Therefore, within the radius of $\rho_{\text{max}}$, there
exists $\Omega(\sqrt{n^{1-v}/(1-v) \log n})$ disjoint paths from inner circle to external circle, and $\Omega((\log(\log n)/(\delta - 2)) \sqrt{n^{1-v}/\log n})$ disjoint paths around the disk. With these two kinds of paths, the highway system of legitimate nodes is established. Although our model is a circular grid, it can be analyzed similarly as a $c_1 \sqrt{n^{1-v}/(1-v) \log n} \times c_2 ((\log(\log n)/(\delta - 2)) \sqrt{n^{1-v}/\log n})$ rectangle grid, which will be proved in the following section.

As shown in Figure 1, in each cluster, the routing scheme within the area of radius $p_{\text{max}}$ proceeds in four phases.

**Phase 1 (Draining Phase).** Source node $S$ drains the packets to an access point on the highway in the radial direction, using direct transmission and multiple time slots. Note that each highway may not be fully contained in its corresponding sector, but it may deviate from it. However, a highway is never farther than $\kappa \log((n/m)/x) - \epsilon$ from its corresponding sector.

**Phase 2 (Radial Highway Phase).** Information is carried across the cluster along the highway in the radial direction, using multiple hops and multiple time slots, and there exist $\Omega(\sqrt{n^{1-v}/(1-v) \log n})$ disjoint paths from inner circle to external circle.

**Phase 3 (Encircling Highway Phase).** Information is transported clockwise on the highway around the cluster center, and there exist $\Omega((\log(\log n)/(\delta - 2)) \sqrt{n^{1-v}/\log n})$ disjoint paths around the circle.

**Phase 4 (Delivering Phase).** In this phase, information is delivered from the exit point located on the encircling highway to the destination node $D$.

Comparing the rate in each phase, we find that the communication bottleneck is in the radial highway phase.

## 5. The Secrecy Transmission Rate of Intracluster Traffic

The routing protocol of intracluster communication uses four separate phases to deliver the packets and it can be found that the bottleneck occurs on the transmission along the highways. After setting different transmission power for different nodes, we can transform the inhomogeneous circular lattice into homogenous regular square lattice. In this section, we derive the secrecy rate in intracluster transmission via the circular percolation model. In addition, the TDMA scheme is adopted and the packet is delivered hop by hop; then a constant rate along the highway is achieved. However, there are still some differences between circular lattice and the regular one, such as not all the highways sever the same quantity of nodes and the power in each lattice is not equal. Based on these differences, we give the per-node secrecy rate for the circular lattice specifically.

**Lemma 5.** For a given square, to make the interference from the two opposite directions be equal, the transmission and artificial generated noise power of legitimate nodes in square $s_i$ is

$$P_{t_i} = P_{t_0} \cdot \left(\frac{2\pi r_i}{x}\right)^\alpha,$$

$$P_{\alpha_i} = P_{\alpha_0} \cdot \left(\frac{2\pi r_i}{x}\right)^\alpha,$$

where $P_{t_0}$ and $P_{\alpha_0}$ are the unit power for legitimate transmitter and artificial noise generation node, respectively.

**Proof.** For a given square $s_i$, let $I_1$ denote the interference from the direction of outside the square, and $I_2$ for that from the direction of inside the square. if $d$ is the distance between two nodes, which is not Euclidean distance but the number of $d$ squares away, then we can compute the interference from different directions as follows:

$$I_{11}(d) = P_{t(i-d)} \frac{1}{(r_{i+d} - r_i)^\alpha},$$

$$I_{12}(d) = P_{t(i-d)} \frac{1}{(r_i - r_{i-d})^\alpha}.$$

We can also get that

$$I_{11}(d) = \frac{P_{t(i-d)}}{P_{t(d)}} \left(\frac{r_i - r_{i-d}}{r_{i+d} - r_i}\right)^\alpha,$$

$$I_{12}(d) = \left(\frac{r_{i+d} - r_i}{r_i - r_{i-d}}\right)^\alpha \left(1 + \frac{2\pi}{x}\right)^d.$$

**Proof.**
As \( x = \Theta(\sqrt{n^{1/\gamma}(1 - \nu) \log n}) \), when \( d = \alpha(\sqrt{n^{1/\gamma}(1 - \nu) \log n}) \), we can get \( I_{12}(d)/I_{12}(d) \to 1 \).

Similarly, we also can obtain \( I_{11}(d)/I_{12}(d) \to 1 \), if \( P_{\nu} = P_{\nu}(2\pi r_{\nu}/x)^{\alpha} \), where \( I_{11} \) and \( I_{12} \) are the interference caused by artificial generated noise.

Next, we refer to Lemma 1 in [12] and give the upper bound rate that an eavesdropper \( e \) can obtain.

**Lemma 6.** Let \( R_e \) denote the maximum rate that an independent eavesdropper \( e \) can obtain; then we can get that

\[
R_e \leq \min \left( \frac{P_{\mu}t_{e}}{N_0}, \frac{P_{\mu}}{P_{\nu}(1 + d_{ij})^\alpha} \right),
\]

where \( d_{ij} \) is the Euclidean distance between legitimate transmitter \( i \) and receiver \( j \), and \( d_{ie} \) is the Euclidean distance between node \( i \) and eavesdropper \( e \).

**Proof.** The proof is similar to that of Lemma 1 in [12]. In [12], the authors assumed that each legitimate node used identical power for transmission and noise generation, while we assign different power for different nodes, as shown in Lemma 5. Despite difference in the power, the proof goes along the same line as [12]. For concision, we omit details.

**Theorem 7.** In each square, the rate that legitimate source-destination pair can be achieved in the "highway system" is \( R_s(d) = \Omega(d^{-\alpha-4}) \), where \( d \) denotes the transmission range. For special, the distance \( d \) is not Euclidean distance but the number of \( d \) squares away.

**Proof.** First we compute the interference at a given destination node. We can prove that the interference from different directions is equal with the same interference distance \( d \). Then we will treat the cluster network as a square network. In addition, we adopt TDMA scheme and divide time into \((k + d)^2\) successive time slots, where \( k \) is an important parameter. Every square in each subsquare takes turn to transmit, and in one given time slot, squares can transmit simultaneously in accordance with Kumar’s interference region [11]. Assuming that the transmitter in a square \( s_i \) transmits toward a destination located in a square at distance of \( d \) squares away, the eight closest transmitters and receivers are located at distance at least \( k \) and \( k - d \) from the receiver. The sixteen next closest transmitters and receivers are at distance at least \( 2k + d \) and \( 2k \) away from the receivers and so on. Considering the interference in the network, the upper bound of the interference \( I(d) \) caused by simultaneous transmitter nodes and artificial noise could be given as follows:

\[
I(d) \leq \sum_{j=1}^{\infty} 8j \\
	imes \left( \frac{P_{t}(i+j(k+\alpha)-d)}{N_0} \times \left( r_{(i+j)(k+d) - d} - r_{i} \right)^{-\alpha} \right) \\
+ \frac{P_{t}(i+j(k+\alpha)-2d)}{r_{(i+j)(k+d) - 2d}} \times \left( r_{(i+j)(k+d) - 2d} - r_{i} \right)^{-\alpha}
\]

\[
\leq \sum_{j=1}^{\infty} 8j \\
\times \left( \frac{P_{t}(i+j(k+\alpha)-d)}{r_{e}} \times \left( \frac{1}{r_{e}(2\pi/x)} \left( j(k+\alpha)-d \right)^{-\alpha} \right) \right)
\times \left( \frac{1}{r_{e}(2\pi/x)} \left( j(k+\alpha)-2d \right)^{-\alpha} \right)
\]

\[
\leq \sum_{j=1}^{\infty} 8j \\
\times \left( \frac{P_{t} \times \left( 1 + 2\pi/x \right)^{j(k+\alpha)-d}}{j(k+\alpha)-d} \right)^{-\alpha}
\times \left( \frac{1}{r_{e}(2\pi/x)} \left( j(k+\alpha)-2d \right)^{-\alpha} \right)
\]

\[
\leq (P_{t} + P_{\nu}) k^{-\alpha \sum_{j=1}^{\infty} 8j} \left( 1 + \frac{2\pi}{x} \right)^{j(k+\alpha)}.
\]

Notice that this sum will converge if \( \alpha > 2 \) and the proof is shown in Appendix A.

According to the interference model, we will derive a lower bound of received power of legitimate node. We notice that the distance between the transmitter and the receiver is at most \((2\pi r_{\nu}/x)(d + 1)\). Then the signal at the receiver can be bounded by

\[
S(d) \geq P_{t} \left( \frac{2\pi r_{\nu}/x d}{N_0 + 1} \right)^{-\alpha} = P_{t} \theta d^{-\alpha}.
\]

Finally, combining (17) and (18), we can obtain an asymptotic lower bound of the rate for \( d \to \infty \):

\[
R(d) = \log \left( 1 + \frac{S(d)}{N_0 + 1} \right)
\geq \log \left( 1 + \frac{P_{t} \theta d^{-\alpha}}{N_0 + c (P_{t} + P_{\nu}) k^{-\alpha}} \right)
\geq c' P_{t} (d + 1)^{-\alpha} \geq c'' P_{t} d^{-\alpha},
\]

when choosing \( k = \Theta(P_{t}^{1/\alpha}) \), \( c'' \) and \( c' \) are constants.

As shown in Lemma 6 and according to (6), the secrecy rate \( R_s(d) \) which each square can obtain is as follows:

\[
R_s(d) = \frac{1}{(k + \alpha)^2} (R(d) - R_e)
\geq \frac{1}{(k + \alpha)^2} \left( \frac{c'' P_{t} d^{-\alpha} - P_{t} d^{-\alpha}}{P_{\nu} d^{-\alpha}} \right),
\]

where \( 1/(k + \alpha)^2 \) is the time utilization factor.

Let \( P_{t} = 2/c'' \) and \( d^{-\alpha} \). To bound the interference incurred to intended receiver, we can get \( k = \Theta(P_{t}^{1/\alpha}) = \Theta(d^2) \) according to (19). Therefore, the secrecy rate which each square can obtain is \( \Omega(d^{-\alpha-4}) \).
Theorem 7 shows that the secrecy rate is achievable even under the worst attack. In order to calculate the secrecy rate per-node, we will derive the rate in each phase.

**Lemma 8.** If one divides a given cluster into \( w \) sectors with arc of \( 2\pi/w \), then there are no more than \((2n/m)/w\) legitimate nodes located in each sector \( S_{R_i} \).

**Proof.** Let \( P_w \) denote the probability that there exists a sector having more than \((2n/m)/w\) nodes. As the number of nodes in each sector according to Poisson distribution of \((2n/m)/w\), following the Chernoff bound (see Appendix C), when \( n \to \infty \), then

\[
P_w \leq wP \left( |S_{R_i}| > \frac{2n/m}{w} \right) \\
\leq we^{-\left(\frac{\log \left( \frac{2n/m}{w} \right)}{(2n/m)/w} \right)} \tag{21}
\]

\[
= we^{-\left(\frac{\log \left( \frac{n/m}{w} \right)}{(2n/m)/w} \right)} \to 0.
\]

Therefore, we can conclude that there is no sector containing more than \((2n/m)/w\) nodes.

**Lemma 9.** Each legitimate node within the radius of \( \rho_{\text{max}} \) can obtain a secrecy access rate \( R_1 = \Omega(\sqrt{\log((1-v)n^{1-v}\log n)}) \) with a node on the highway of radial direction.

**Proof.** According to Theorem 5 in [13], by choosing \( \epsilon \) and \( \kappa \) appropriately, there are at least \( \Omega((\log((n/m)/x)) \) highways in the direction of radial within a given sector of \((2\pi/x)[\kappa \log((n/m)/x) - \epsilon] \). Note that each highway may not be fully contained in its corresponding sector; it may deviate it. However, it never deviates an arc of \((2\pi/x)[\kappa \log((n/m)/x)] - \epsilon \) from its corresponding sector; that is, it will not father than \( \kappa \log((n/m)/x) - \epsilon \) squares, as it is shown in Figure 1.

Then, according to Theorem 7, let \( d = \kappa \log((n/m)/x) - \epsilon \); we can obtain that the transmission rate between a legitimate node in a square and an access node on the radial highway is

\[
R \left( \kappa \log \left( \frac{n/m}{x} - \epsilon \right) \right) \\
= \Omega \left( \left( \frac{\log((1-v)n^{1-v}\log n)}{\log((1-v)n^{1-v}\log n)} \right)^{-\alpha} \right). \tag{22}
\]

As there are many nodes in a square, they need to share the bandwidth. According to Lemma 8, we conclude that the rate of legitimate nodes in the first phase is

\[
R_1 = \Omega \left( \left( \frac{\log((1-v)n^{1-v}\log n)}{\log((1-v)n^{1-v}\log n)} \right)^{-\alpha} \right). \tag{23}
\]

**Lemma 10.** Every legitimate node in the radial direction highway can achieve a per-node secrecy rate \( R_2 = \Omega(\sqrt{1/(n^{1-v}(1-v)\log n)}) \) w.h.p.

**Proof.** According to the construction of highway system, the delivering strategy is hop-by-hop and information is transmitted from one square to a neighboring square. Therefore, by applying Theorem 7, we can obtain that the rate in the highway phase is \( \Omega(1) \). Since \( x \gg \log(n/mx) \), there will be \( \Omega(x) \) distinct highways which span from inner circle to external circle. According to Chernoff bound, there are at most \( 2n/mx \) nodes w.h.p. in the arc of \( 2\pi/x \). It follows that each node can transmit at a rate of order \( \Omega(\sqrt{1/(n^{1-v}(1-v)\log n)}) \) in the radial direction.

**Lemma 11.** The legitimate nodes in the highway which are around the cluster can achieve w.h.p. a per-node secrecy rate \( R_3 = \Omega(\sqrt{(1-v)\log n/n^{1-v} \cdot f(\delta)}) \), where \( f(\delta) \) is the “inhomogeneous factor” which is only decided by the inhomogeneous characteristic of the node distribution.

**Proof.** Compared with the highway in the radial direction, the condition in which data is transmitted around the cluster becomes more complicated since the number of nodes in different highways is not equal. If each highway around the cluster is identical, we can get a corresponding rate of order \( \Omega(\sqrt{(1-v)\log n/n^{1-v}}) \). Nevertheless, for the effect of inhomogeneous, the achievable rate can be written as

\[
R_3 = \Omega(\sqrt{(1-v)\log n/n^{1-v} \cdot f(\delta)}) \tag{24}
\]

where \( f(\delta) \) is an inhomogeneous factor, and will be discussed in detail in Appendix B.

The delivery phase is a reverse process of the first phase. Therefore, we can get the secrecy rate directly, which is the same order with the draining phase.

**Lemma 12.** Every legitimate node can receive information from the highway at rate \( R_4 = \Omega((\log(\sqrt{(1-v)n\log n})^{-\alpha}) \) w.h.p.

Comparing the secrecy rate in each phase, we can conclude that the secrecy rate of intracluster transmission is as follows.

**Theorem 13.** For the intracluster traffic in each independent cluster, the legitimate nodes which are within the area of radius \( \rho_{\text{max}} \) can achieve w.h.p. a per-node secrecy rate of \( R_{\text{max}} = \Omega(\sqrt{1/(n^{1-v}(1-v)\log n)}) \).

**Proof.** The routing strategy based on percolation theory has been deeply researched. The data transmission within the area of radius \( \rho_{\text{max}} \) can be divided into four phases: draining information to the highway; transporting information on the highway of the radial direction; transporting information on the highway around the cluster; and delivering the
Figure 2: An illustration of information pipelines among cluster. As the minimum legitimate node density is \( \Phi \), we can build \( \Omega(\sqrt{A \Phi}) \) pipelines among these clusters.

information to the destination. We can find that the communication bottleneck is in the highway phase. In addition, for \( 0 < v < 1 \), we can get that w.h.p. \( R_2 < R_3 \) (the proof is in Appendix B). Then the per-node secrecy rate in the intracluster transmission can be achieved as \( R_y^{\text{intra}} = \Omega(\sqrt{1/(n^{1-v}(1-v) \log n)}) \).

6. The Secrecy Transmission of Intercluster Traffic

As we consider cluster-sparse network, the node density between two neighboring clusters is much lower. These areas may be disjoint sets that we cannot utilize the highway system mentioned in the previous section. Using the properties of Poisson point process, we extract part of nodes which are distributed like homogeneous Poisson point process with the density of \( \phi \), which is smaller than \( \Phi \). Then we can build information pipelines constructed by these nodes among clusters; see Figure 2 for details.

The network is divided into a regular lattice and the area of each small square is \( c_0/\Phi \), where \( c_0 \) is a constant. Our strategy of delivering data among clusters is easy to understand and implement. For some special large value \( c_0 \), we can extract part of nodes to form “information pipelines,” which is similar to the highways in the homogeneous network. However, due to the inhomogeneous distribution, the number of node in each square is not equal.

In the previous section, we have already derived the secrecy throughput in the cluster area through a circular highway system. In these cluster areas, data is transmitted according to strategy of circular highway system. Only if the information needs to be forwarded to the nodes located in different clusters, the data will be transmitted through the “information pipelines.” In light of this scheme, we can obtain the achievable secrecy rate of these pipelines in the network.

According to the percolation theory in [13], we can build \( \Omega(\sqrt{A \Phi}) \) pipelines among these clusters. All these pipelines need to serve \( \Theta(m) \) clusters. Similar to Lemma 2 in [12], we can also obtain that the interference caused by intercluster transmission is converged, in which the square length is not \( c \), but \( \sqrt{c_0/\Phi} \). Since we have computed the interference of intracluster transmission which is converged, we can conclude that the effect caused by interference will not change our results in order sense. Therefore, each cluster can be served by \( \Omega(\sqrt{A \Phi}/n) \) pipelines w.h.p. Under the analysis of secrecy capacity of homogeneous wireless network in [12], we can get that the rate between legitimate nodes on these pipelines is \( \Omega(\sqrt{A \Phi}/n) \). Based on the analysis above, we can obtain the following theorem directly.

**Theorem 14.** For the intercluster traffic, one can get that the achievable secrecy rate for legitimate node is \( R_y^{\text{inter}} = \Omega(\sqrt{A \Phi}/n) = \Omega(\sqrt{\Phi}/\sqrt{n}) \), where \( \Phi \) is the minimum node density in the network area.

Specially, for the homogeneous network, we can get that \( \Phi = \Theta(1) \) and \( R_y^{\text{inter}} = \Omega(1/\sqrt{n}) \), which is the secrecy capacity in homogeneous wireless networks under the case of independent eavesdropper [12].

Comparing the results of intracluster and intercluster transmission, we can find that the bottleneck of the secrecy throughput is in the area with minimum node density. However, the communication traffic in real world always occurs in the local region which may communicate with the node in the same cluster. In other words, the traffic may be inhomogeneous. To deal with such situation, a remarkable contribution of our model is that we set independent transmission models in distinct clusters. Furthermore, the computing for the throughput may be convenient when the traffic is inhomogeneous. As to the inhomogeneous traffic, we can derive the following theorem.

**Theorem 15.** If one considers the nonuniform traffic in the network, the per-node secrecy rate is in the interval of

\[
\lambda_s^y(n) = \left[ \Omega \left( \frac{\sqrt{\Phi}}{\sqrt{n}} \right), \Omega \left( \frac{1}{n^{1-v}(1-v) \log n} \right) \right].
\]

7. Case of Eavesdroppers with Multiple Antennas

In the previous section, we have derived the secrecy throughput in the case of independent eavesdroppers suppressed by artificial noise generation. Regardless of the number and location of eavesdroppers, the results show that there is no loss in the throughput. However, if eavesdroppers are equipped with multiple antennas, what is the secrecy throughput between legitimate nodes?

Without loss of generality, we assume eavesdroppers do not collaborate with each other and the correlation across the antennas is ignored, so that the eavesdroppers can employ maximum ratio combining to maximize the SINR.

**Theorem 16.** If eavesdropper is equipped with \( \mathcal{V}(n) \) antennas, the per-node secrecy throughput of intracluster transmission is...
Ω(√1/n1−v(1 − v) log nΨ−2/α(n)) and Ω((√D/√n)Ψ−2/α(n)) for intercluster transmission.

Proof. According to Lemma 6, the maximum rate that eavesdroppers can get is bounded as \( R_e \leq c_b \Psi(n)P_{\epsilon_0}/P_{\alpha_0}(1 + d_r)^{k_r} \). As eavesdroppers are always silent, the rate that legitimate can obtain remains the same; that is, \( R_l(d) = \omega(d) = c_b \Psi(n)d^{k_r} \). Since \( R_l(d) = R_l(d) - R_e \), we can find a constant \( c' \), such that when \( P_{\epsilon_0} = c' \Psi(n) d^{2\alpha} \), \( R_l(d) \) can be greater than \( (1/2)R(d) \), and the secrecy rate is \( \Omega(d^{-\alpha}) \). In addition, we need to choose \( k = \Theta(P_{\alpha_0}(d + 1)^{-\alpha}) \), that is, \( k = \Theta(\Psi^{-\alpha}(n)d^2) \), such that (20) can hold. Therefore, the secrecy throughput in each square is \( \Omega((d - 4 - 2\alpha)\Psi^{-2/\alpha}(n)) \). Hence, when the transmission is occurred in the intracluster, the per-node secrecy throughput is \( \Omega(\sqrt{1/n1−\gamma(1 − v) log n}\Psi^{-2/\alpha}(n)) \). Similarly, for the intercluster transmission, according to Theorem 14, we can get the per-node secrecy throughput which is \( \Omega((\sqrt{D}/\sqrt{n})\Psi^{-2/\alpha}(n)) \).

Comparing to the case of eavesdropper equipped with single antenna, there exists a degradation factor for secrecy throughput, which is \( \Psi^{-2/\alpha}(n) \). Moreover, when the traffic is nonuniform, the secrecy throughput \( \lambda_s^I(n) \) is fallen into an interval, which can be denoted as follows:

\[
\lambda_s^M(n) \in \left[ \Omega\left(\frac{\sqrt{D}}{\sqrt{n}}\Psi^{-2/\alpha}(n)\right), \Omega\left(\frac{1}{n^{1-\gamma}(1 - v) \log n}\Psi^{-2/\alpha}(n)\right) \right].
\]

8. Conclusion

In this paper, we analyze the secrecy throughput capacity of cluster-sparse network where the legitimate nodes are distributed according to the SNCP. In order to get the secrecy throughput capacity under the independent eavesdroppers with single antenna, the transmission is divided into two parts: the intracluster transmission and the intercluster transmission. For the first part, we novelty establish a circular percolation model and find the bottleneck of secrecy throughput capacity is in the highway phase, where per-node secrecy rate of order \( \Omega(\sqrt{1/n^{1-\gamma}(1 − v) \log n}) \) is achieved. For the second part, we employ the idea of “information pipelines” to obtain a per-node secrecy rate of \( \Omega((\sqrt{D}/\sqrt{n})\Psi^{-2/\alpha}(n)) \). Taking both transmissions into consideration, the secrecy rate \( \lambda_s^I(n) \) is fallen into an interval of \( \left[ \Omega(\sqrt{D}/\sqrt{n}), \Omega(\sqrt{1/n^{1-\gamma}(1 − v) \log n}) \right] \). In Figure 3, we depict the order sense of secrecy rate of intracluster and intercluster transmission. Unexpectedly, we find the secrecy throughput in intracluster transmission is greater than that of homogeneous networks.

We also investigate the scenario where eavesdropper is equipped with multiple antennas. If the eavesdropper is equipped with \( \Psi(n) \) antennas and do not collaborate with each other, the secrecy throughput of intracluster transmission is \( \Omega((\sqrt{D}/\sqrt{n})\Psi^{-2/\alpha}(n)) \) and \( \Omega((\sqrt{D}/\sqrt{n})\Psi^{-2/\alpha}(n)) \) for intercluster transmission. Similarly, when the traffic is nonuniform, the secrecy throughput \( \lambda_s^M(n) \) is fallen into an interval, which can be denoted as follows:

\[
\lambda_s^M(n) \in \left[ \Omega\left(\frac{\sqrt{D}}{\sqrt{n}}\Psi^{-2/\alpha}(n)\right), \Omega\left(\frac{1}{n^{1-\gamma}(1 - v) \log n}\Psi^{-2/\alpha}(n)\right) \right].
\]

Finally, we do not consider the case of eavesdroppers collaborating with each other. What is more is that the secrecy throughput is strongly correlated to the distribution of nodes. Therefore, it is an interesting future work to study the scenario of colluding eavesdroppers, where the distribution of legitimate nodes and eavesdroppers will impact the secrecy throughput greatly.

Appendices

A. The Proof of Theorem 7

Proof. We show the convergence of the summation of (17). As we consider the asymptotic situation, we can simply this summation and just need to prove the convergence of summation \( \sum_{j=1}^{\infty} \frac{1}{j\alpha(d+k)} \). Firstly, we analyze \( (1 + 2\pi/x)^{2j\alpha(d+k)} \), and \( x \) is presented in Lemma 2. Thus we can get the following:

\[
(1 + \frac{2\pi}{x})^{2j\alpha(d+k)} = \left(1 + \frac{2\pi}{\sqrt{n^{1-\gamma}/(1 - v) \log n}}\right)^{2j\alpha(d+k)} \approx e^{(2\pi/\sqrt{n^{1-\gamma}/(1 - v) \log n})2 j\alpha(d+k)}.
\]
\[
\Omega \left( 1/\sqrt{(1 - \nu)n^{1-\nu}\log n} \right) \Omega(n^{1/2}) \Omega (\sqrt{\Theta / \sqrt{n}})
\]

\[+\infty \]

Figure 3: An illustration of secrecy throughput of intracluster transmission and intercluster transmission when the eavesdropper is equipped with single antenna, and we also give a comparison with that in [12]. The scales of the axes are in terms of the order in \( n \).

when \((k + d) = o(\sqrt{n^{1-\nu}/(1 - \nu) \log n})\) and \(n \to \infty\), Then
\[
(1 + 2\pi/x)^{ja(k+d)} = e^{(2\pi/x)/(n^{1-\nu}/(1 - \nu) \log n) - 2\pi ja (k+d)} \to \Theta(1).
\]

For \(\alpha > 2\), we can prove that the summation (17) is convergence.

### B. The Proof of Theorem 13

**Proof.** Here we give a rigorous deduction of the achievable rate during the highway phase in the intracluster transmission. According to the circular percolation theory, we need to compare the rates on the highway of radial direction and around the cluster. The rate on radial direction is easy to get and has been proved in Lemma 10. We will calculate the rate of the highway around the cluster. As the number of nodes on different paths is not in the same level, the condition along the circular ring is more sophisticated with respect to the radial direction. According to the analysis above, we use \(E(N_i)\) which denotes the mathematical expectation number of nodes in each circular ring. Then we can achieve the expectation from our model and simplify it as follows:

\[
E(N_i) = \frac{n}{m} \left( \frac{2\pi}{x} \right)^2 \frac{1}{r_i^{\delta}} x.
\]

Using (7) to substitute \(r_i\), we can get

\[
E(N_i) = \frac{n}{m} \left( \frac{2\pi}{x} \right)^2 \frac{1}{r_i^{\delta}} x = 4\pi^2 \frac{n}{m} x^{-1} \left( 1 + \frac{2\pi}{x} \right)^{(2-\delta)}.
\]

As for \(\delta > 2\), we can find that \(E(N_i)\) decreases as increasing of parameter \(i\). Thus the circular highways near the cluster center need to service more nodes. Then we can get the achievable rate on the circular highway:

\[
R_3 > R_r (i = 1)
\]

\[
= \Theta \left( \frac{1}{\sqrt{(1 - \nu)n^{1-\nu}\log n}} \right)
\]

\[
\times \left( 1 + \frac{2\pi}{\sqrt{n^{1-\nu}/(1 - \nu) \log n}} \right)^{(\delta-2)}.
\]

In the end, comparing the \(R_2\) and \(R_3\), we can find that \(R_2 < R_3\), for \(\delta > 2\); that is, the secrecy rate bottleneck is on the highway phase of radial direction.

### C. Chernoff Bound

**Theorem 17.** Chernoff bound: Let \(X\) be a Poisson random variable of parameter \(\lambda\). One has

\[
Pr [X \geq \xi] \leq e^{-\lambda (\epsilon \lambda)^\xi / \xi}, \quad \text{for } \xi > \lambda,
\]

\[
Pr [X \leq \xi] \leq e^{-\lambda (\epsilon \lambda)^\xi / \xi}, \quad \text{for } \xi < \lambda.
\]

For \(0 < \delta < 1\), Chernoff bounds given in (C.1) can be combined and simplified to

\[
Pr [|X - \lambda| \geq \delta \lambda] \leq 2e^{-\delta^2 \lambda/2}.
\]

### Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

### Acknowledgments

This work was supported in part by the Key project of National Natural Science Foundation of China (NSFC) (Grant no. 61231010) and the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant no. 20120142110015).
**References**

[1] J. Ponniah, Y.-C. Hu, and P. Kumar, “A system-theoretic clean slate approach to provably secure ad hoc wireless networking,” http://arxiv.org/abs/1309.2904.

[2] C. Zhang, Y. Song, Y. Fang, and Y. Zhang, “On the price of security in large-scale wireless ad hoc networks,” IEEE/ACM Transactions on Networking, vol. 19, no. 2, pp. 319–332, 2011.

[3] V. Bhandari and N. H. Vaidya, “Secure capacity of multi-hop wireless networks with random key pre-distribution,” in Proceedings of the IEEE INFOCOM Workshops, pp. 1–6, Phoenix, Ariz, USA, April 2008.

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

[5] J. Choi II, M. Jain, K. Srinivasan, P. Levis, and S. Katti, “Achieving single channel, full duplex wireless communication,” in Proceedings of the 16th Annual Conference on Mobile Computing and Networking (MobiCom ’10), pp. 1–12, ACM, September 2010.

[6] S. Vasudevan, D. Goeckel, and D. F. Towsley, “Security-capacity trade-off in large wireless networks using keyless secrecy,” in Proceedings of the 11th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc ’10), pp. 21–30, ACM, September 2010.

[7] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, “On secrecy capacity scaling in wireless networks,” IEEE Transactions on Information Theory, vol. 58, no. 5, pp. 3000–3015, 2012.

[8] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, “On the throughput cost of physical layer security in decentralized wireless networks,” IEEE Transactions on Wireless Communications, vol. 10, no. 8, pp. 2764–2775, 2011.

[9] Y. Liang, H. V. Poor, and L. Ying, “Secrecy throughput of MANETs under passive and active attacks,” IEEE Transactions on Information Theory, vol. 57, no. 10, pp. 6692–6702, 2011.

[10] Ç. Çapar, D. Goeckel, B. Liu, and D. Towsley, “Secret communication in large wireless networks without eavesdropper location information,” in Proceedings of the IEEE Conference on Computer Communications (INFOCOM ’12), pp. 1152–1160, IEEE, March 2012.

[11] P. Gupta and P. R. Kumar, “The capacity of wireless networks,” IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 388–404, 2000.

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

[13] M. Franceschetti, O. Dousse, D. N. Tse, and P. Thiran, “Closing the gap in the capacity of wireless networks via percolation theory,” IEEE Transactions on Information Theory, vol. 53, no. 3, pp. 1009–1018, 2007.

[14] H. Venkataraman, P. Kalyampudi, and G.-M. Muntean, “CASHeW: cluster-based adaptive scheme for multimedia delivery in heterogeneous wireless networks,” Wireless Personal Communications, vol. 62, no. 3, pp. 517–536, 2012.

[15] S. Toumpis, “Capacity bounds for three classes of wireless networks: asymmetric, cluster, and hybrid,” in Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MoBiHoc ’04), pp. 133–144, ACM, May 2004.

[16] E. Perevalov, R. S. Blum, and D. Safi, “Capacity of clustered ad hoc networks: how large is “large”?” IEEE Transactions on Communications, vol. 54, no. 9, pp. 1672–1681, 2006.