sensors

MDPI

*Article*

# Impact of Heterogeneity and Secrecy on theCapacity of Wireless Sensor Networks

**Qiuming Liu [1,2], Li Yu [1,*], Zuhao Liu [3] and Jun Zheng [1]**

Received: 23 September 2015; Accepted: 30 November 2015; Published: 10 December 2015
Academic Editor: Rongxing Lu

1 School of Electronic Information and Communications, Huazhong University of Science and Technology, 1037 Luoyu Road, Wuhan 430074, China; liuqiuming@hust.edu.cn (Q.L.); junzheng@hust.edu.cn (J.Z.)
2 Nanchang of Jiangxi University of Science and Technology, 1180 Shuanggang Road, Nanchang 330013, China
3 China Yangtze Power Co., Ltd., 1 Xibajianshe Road, Yichang 443002, China; liuzuhao@gmail.cn
* Correspondence: hustlyu@hust.edu.cn; Tel.: +86-27-8779-2092; Fax: +86-27-8754-5438

**Abstract:** This paper investigates the achievable secrecy throughput of an inhomogeneous wireless sensor network. We consider the impact of topology heterogeneity and the secrecy constraint on the throughput. For the topology heterogeneity, by virtue of percolation theory, a set of connected highways and information pipelines is established; while for the secrecy constraint, the concept of secrecy zone is adopted to ensure secrecy transmission. The secrecy zone means there is no eavesdropper around the legitimate node. The results demonstrate that, if the eavesdropper's intensity is $\lambda_e = o\left((\log n)^{-\frac{3\delta-4}{\delta-2}}\right)$, a per-node secrecy rate of $\Omega\left(\frac{1}{\sqrt{n^{1-v}(1-v)\log n}}\right)$ can be achieved on the highways, where $\delta$ is the exponent of heterogeneity, $n$ and $n^v$ represent the number of nodes and clusters in the network, respectively. It is also shown that, with the density of the eavesdropper $\lambda_e = o\left((\log(n\underline{\Phi}))^{-2}\right)$, the per-node secrecy rate of $\Omega\left(\sqrt{\frac{\underline{\Phi}}{n}}\right)$ can be obtained in the information pipelines, where $\underline{\Phi}$ denotes the minimum node density in the network.

**Keywords:** secrecy throughput; percolation; heterogeneous topology; wireless sensor networks

## 1. Introduction

Wireless sensor networks are an emerging networking technology, which is widely used in environmental monitoring, emergency and rescue communication, military applications, *etc.* The unique feature of such networks is formed by the huge number of sensor nodes. Each node communicates over a wireless channel without any centralized control [1]. One of the problems in wireless sensor network is efficient data transmission and lifetime. The low-energy adaptive clustering hierarchy (LEACH) protocol presented by Heinzelman *et al.* [2] was a widely known and effective one to reduce and balance the total energy consumption. Later, Tan *et al.* [3] proposed an energy-efficient hybrid cluster-based protocol (HCEP) to prolong the lifetime of the network. To reduce the consumption of energy, Wu *et al.* [4] developed a structure fidelity data collection (SFDC) framework to reduce the number of active sensor nodes, which can not only save energy, but also reserve the data fidelity. Another problem is the throughput capacity, meaning how much traffic the wireless networks can carry. In their groundbreaking work, Gupta and Kumar [5] had shown that, for a static wireless networks consisting of $n$ nodes randomly and uniformly distributed, each node can achieve a rate of order $\Omega\left(\frac{1}{\sqrt{n\log n}}\right)$. 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 $\lim_{n\to\infty} f(n)/g(n) = c < \infty$; if $g(n) = O(f(n))$, $f(n) = \Omega(g(n))$ w.h.p.; if both $f(n) = \Omega(g(n))$ and $f(n) = O(g(n))$,

$f(n) = \Theta(g(n))$; $f(n) = \widetilde{\Theta}(g(n))$ means $f(n) = \Theta(g(n))$ when logarithmic terms are ignored. They also derived an upper bound on the capacity that scaled on the order $O\left(\frac{1}{\sqrt{n}}\right)$. This capacity gap was closed by Franceschetti *et al.* [6]. Inspired by percolation theory, they constructed a series of paths spanning the network both horizontally and vertically. Then, by exploiting the time division multiple access (TDMA) strategy, each node transmitted its information to the nearest horizontal highway. After that, the information was transported in a multi-hop manner toward the vertical paths, which was near the receiver. Finally, the information was sent to the receiver from the existing node on the vertical highway. Based on the "highways scheme", a rate of $\Theta\left(\frac{1}{\sqrt{n}}\right)$ was achieved for each node. Since then, capacity scaling has drawn considerable attention. Hu *et al.* [7] investigated the impact of geometry on the capacity of a wireless network. They constructed highways in a strip network, triangle network and three-dimensional network. Since the infrastructure was an effective way to ease hop-by-hop transmission, Liu *et al.* [8] allocated some infrastructure into the network and proved that the capacity could increase linearly with the number of infrastructures. Tan *et al.* [9] proposed a framework to maximize the total utility of bandwidth allocation for the three traffic types in infrastructure-based wireless networks. Multicast was often used in realistic networks; Li [10] derived the multicast capacity of large-scale wireless networks using a tree-based routing scheme. Later on, Alfano *et al.* [11,12] firstly investigated the capacity of topology inhomogeneous wireless networks. Liu *et al.* [13] constructed a "highway system" in inhomogeneous Poisson networks. Based on the highway system, the lower bound of capacity was obtained, and they found that the bottleneckof the rate was caused by the place of the lowest node density. After that, the scenario of traffic heterogeneity was studied. Kim *et al.* [14] proposed a differentiated channel access scheme to resolve the throughput fairness problem in heterogeneous wireless networks. Recently, Lu and Shen [15] gave a comprehensive overview of the development of capacity and delay in *ad hoc* networks. They also presented the fundamental tradeoffs between capacity and delay under a variety of mobility models.

However, due to the wireless channel being broadcast, it is easily attacked by eavesdroppers and malicious nodes. This motivates considering the secrecy constraint in capacity analysis. With some exceptions, the secrecy capacity under the protection of an RSApublic key cryptosystem was used in [16,17]. They got a pessimistic result that, for a network consisting of $n$ legitimate nodes, a rate of $\Omega\left(\sqrt{\frac{p_f}{n \log n}}\right)$ was obtained, where $p_f$ was the probability that a node shared a primary secure association (SA) with any other node. To avoid the capacity degradation caused by $p_f$ decreasing, an information theoretic security was proposed, which was achieved by using the channel difference between legitimate nodes and eavesdroppers, which required the intended receiver to have a stronger channel than eavesdroppers. To degrade the signal of eavesdropper, Vasudevan *et al.* [18] used other nodes around the transmitters to generate artificial noise. They found that, when a per-node throughput of $\Omega\left(\frac{1}{\sqrt{n \log n}}\right)$ was desired, the network can tolerate up to $\Omega\left((\log n)^c\right)$ independent eavesdroppers or a single eavesdropper with $\Omega\left((\log \log n)^{1-\epsilon}\right)$ antennas, where $c$ and $\epsilon$ were constants. After that, Capar *et al.* [19] investigated the impact of network dimension on the secrecy capacity. They found that the per-node secure throughput was $\Omega\left(\frac{1}{n}\right)$ in one-dimensional and $\Omega\left(\frac{1}{\sqrt{n \log n}}\right)$ in two-dimensional networks, respectively. More recently, Zhang *et al.* [20] considered a homogeneous network with an independent eavesdropper and colluding eavesdroppers. Each node was installed with three antennas, where two of them were used for transmitting and receiving, and the other one was employed to generate artificial noise to degrade the signal of the eavesdropper. By constructing a set of highways in the networks, they derived that the secrecy capacity was $\Theta\left(\frac{1}{\sqrt{n}}\right)$ for the scenario of an independent and colluding eavesdropper. Later on, Cao *et al.* [21] investigated the tradeoff between secrecy capacity and delay in large-scale mobile *ad hoc* networks. They found that, for a given delay constraint $D$, the optimal secrecy throughput capacity was $\widetilde{\Theta}\left(\left(\frac{D}{n}\right)^{\frac{2}{3}}\right)$. In addition to the

method of generating artificial noise to suppress the eavesdroppers' receiving signal, an alternative idea of the secrecy zone was proposed in [22,23], which required neither the channel state information of eavesdroppers, nor extra power to generate artificial noise. Under the protection of the secrecy zone, Koyluoglu *et al.* [22] obtained that, as long as the density of the eavesdropper was $o\left(\frac{1}{(\log n)^2}\right)$, each node can achieve a secure rate of $\Omega\left(\frac{1}{\sqrt{n}}\right)$. Besides the information security issue in wireless networks, privacy security is also concerned. To avoid disclosing the users' interest to others, Luan and Lu *et al.* [24] employed a privacy-preserving mechanism to protect sensitive user information during social communications. Although there existed many works on security issues, all of them focused on homogeneous networks. Therefore, a fundamental question arises: what is the impact of the capacity if both the security constraint and heterogeneity topology are taken into consideration?

In this paper, we focus on static cluster sparse networks. Our main purpose is solving the secrecy transmission in heterogeneity networks. The transmission is divided into intra-cluster and inter-cluster traffic. For the former transmission, we propose a heterogeneous percolation model. Based on the heterogeneous percolation, we construct a series of "paths" in the radial direction and around the cluster. The information is transported in a multi-hop manner on the paths. While for the latter traffic, some information pipelines have been built among clusters. On the basis of the "highway system" and information pipelines, we employ the secrecy zone to protect the transmission. This is different from the artificial noise generation fashion, where their strategy needs additional power to generate noise.

The main contributions can be concluded as follows:

- We prove the existence of highways in heterogeneous networks. More importantly, it is shown that the networks still percolate in the secrecy constraint model, and many secrecy highway paths can be constructed.
- We first exploit the secrecy zone to protect the transmission in heterogeneous networks. The relationship between the secrecy capacity and the tolerable density of the eavesdropper was established.
- Due to the impact of heterogeneity, we observe that the secrecy throughput of intra-cluster transmission is higher than that in a homogeneous one, and the bottleneck of secrecy throughput is located at the area with the minimum node density.

The rest of this paper is organized as follows. In Section 2, we give the network model. We give the transmission model in Section 3. The construction of the circular percolation model is described in Section 4. Section 5 derives the secrecy throughput in intra-cluster transmission. In Section 6, we investigate the secrecy throughput of inter-cluster transmission. We present the conclusion of this paper in Section 7.

## 2. Network Model

We consider an extended network $A = [0, \sqrt{n}] \times [0, \sqrt{n}]$ with $n$ legitimate nodes randomly distributed, where the distribution of legitimate nodes follows the shot noise Cox process (SNCP) [25]. The main process of SNCP is described as follows: $M$ clusters scattered in $A$ randomly. The expected value of $M$ is $E(M) = m$. We denote the center of the clusters as $C = \{c_j\}_{j=1}^{M}$. For each $c_j$, using the center point $c_j$ as a mother point, a point process centered by $c_j$ with an intensity of $q_j k(c_j, \xi)$ at place $\xi$ is generated. $k(c_j, \xi)$ is a function of density; $q_j$ is the number of nodes of cluster $c_j$. Let each cluster consist of an equal number of legitimate nodes, *i.e.*, $q_j = n/m$. In addition, according to the distribution, the function of density $F$ at place $\xi$ can be expressed as:

$$F(\xi) = \sum_j q_j k(c_j, \xi) \tag{1}$$

where $k\left(c_j,\xi\right) = k(||\xi - c_j||)$ is related to the distance between $\xi$ and $c_j$, and the sum $\int_A k\left(c_j,\xi\right) \mathrm{d}\xi$ on the whole network is finite. For simplicity, we use function $s(\rho)$ to substitute the density function $k\left(c_j,\xi\right)$, where $\rho = ||\xi - c_j||$. To gain finite summation over the whole area, the function $s(\rho)$ is stated as follows:

$$s(\rho) = \min(1, \rho^{-\delta}), \delta > 2 \tag{2}$$

In addition, let $m$ scale as $\Theta(n^v)$; let $\delta$ be a degradation factor; and $v \in (0,1)$. Then, each cluster has a number of nodes $\Theta\left(n^{1-v}\right)$, *i.e.*, $q_j = \Theta\left(n^{1-v}\right)$ for $j = 1, 2, \ldots, M$, since $\int_A k(c_j,\xi)\mathrm{d}\xi$ is finite.

According to the node's distribution, we can obtain the average distance between each cluster center $d_c$ as:

$$d_c = \Theta\left(\sqrt{\frac{A}{m}}\right) = \Theta\left(n^{\frac{1-v}{2}}\right) \tag{3}$$

From Equation (3), we know, when $v < 1$, $d_c \to \infty$ as $n \to \infty$, and the clusters are distributed sparsely. In this work, we only consider the cluster-sparse network, where the $s(\rho)$ is heterogeneous. Let $\overline{\Phi}$ denote the largest density and $\underline{\Phi}$ *vice versa*. Figure 1 is an example of this kind of network topology.

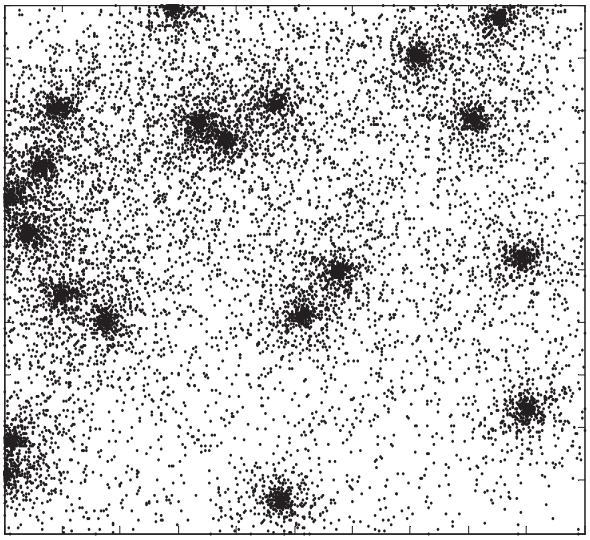

**Figure 1.** Example of a heterogeneous topology network. The parameter of the network is $n = 10{,}000$, $v = 0.3$ and $\delta = 3$.

Different from the legitimate nodes, the eavesdroppers are uniformly and independently distributed in the network with density $\lambda_e$. Let $\varepsilon$ denote the set of eavesdroppers. Since eavesdroppers can be easily detected if they are active, the eavesdroppers are assumed to keep silent. To get insight into the secrecy throughput, the eavesdroppers is also assumed to have a super ability for computing. This means that the traditional method cannot be used here. In addition, let the transmitters know the location of the eavesdropper. Although the assumption seems idealistic, it allows one to gain valuable insight into the problem.

To get the worst case of secrecy throughput, the interference caused by simultaneous transmission is assumed as noise, whereas the eavesdroppers do not have this assumption.

## 3. Transmission Model

For random chosen S-Dpairs, the transmitter $i$ wants to send the information $W_{i,j}$ to a receiver $j$ securely. During time slot $t$, let signals observed at eavesdropper $e$ be $\mathbf{Y}_e \triangleq Y_e(t), \forall t$. In the multi-hop routing, each session in one hop has $N$ channels. Let $R$ be the achievable secrecy rate for the S-D pairs $(i,j)$, if:

- The error decoding the probability of the transmission information at the receiver can be treated arbitrarily low as $N \to \infty$.
- The leakage rate information associated with the transporting information over the whole path, *i.e.*, $\frac{I(W_{i,j};\mathbf{Y}_e)}{N}$, goes to arbitrarily small $\forall e \in \varepsilon$ as $N \to \infty$.

For almost all $(i, j)$, if the message $W_{i,j}$ is transmitted within $H$ hops, we only need to observe the channel of the eavesdropper when considering the security. Hence, the second condition can be satisfied if $\frac{I(W_{i,j};\mathbf{Y}_e(1),,\mathbf{Y}_e(H))}{N}$ can be made arbitrarily small if the block length is sufficiently large, where $\mathbf{Y}_e(h)$ denotes the output vector of length $N$ at eavesdropper $e \in \varepsilon$ during hop $h$.

We consider the Gaussian wiretap channel capacity [26]. Let $SINR_{ij}$ be 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:

$$SINR_{ij} = \frac{P_i l(i,j)}{N_0 + \sum_{\zeta \in T \setminus \{i\}} P_\zeta l(\zeta, j)} \tag{4}$$

where $l(i,j) = \min\{1, 1/d_{ij}^{\alpha}\}$ with $\alpha > 2$ representing the path loss of the channel between node $i$ and node $j$. $P_i$ is the power of transmitting node $i$. $N_0$ denotes the noise power at the receiving node $j$, and $\zeta$ represents the set of nodes that can transmit simultaneously with node $i$.

Similarly, the $SINR$ received at eavesdropper $e$ is as follows:

$$SINR_{ie} = \frac{P_i l(i,e)}{N_0 + \sum_{\zeta \in T} P_\zeta l(\zeta, e)} \tag{5}$$

According to the secrecy throughput defined in [26,27], the secure rate of any legitimate node can be denoted as:

$$R_{ij}^s = R_{ij} - \overline{R_{ie}} = \log_2(1 + SINR_{ij}) - \log_2(1 + \overline{SINR_{ie}}) \tag{6}$$

where $\overline{SINR_{ie}} = \max_{e \in \varepsilon} SINR_{ie}$.

Due to the impact of heterogeneity, we use different powers for different nodes. The secrecy rate is defined as $R_s(n)$, which is also the maximum achievable secrecy capacity.

## 4. Circular Percolation

We first construct a percolation model for the heterogeneous topology. Since the legitimate nodes are distributed heterogeneously, the traffic is divided into two parts: intra-cluster traffic and inter-cluster traffic. For each part of the traffic, we resort to the tools of percolation theory to construct the routing scheme. For the intra-cluster traffic, we establish a circle percolation model, which is different from the previous percolation model; while for the inter-cluster case, we construct a series of information pipelines to link the clusters.

In our model, by virtue of percolation theory, we present a circular percolation model and construct a set of connected highways for legitimate nodes. Different from the the work in [6], the circular highways are from internal to external or encircling the cluster.

**Lemma 1.** *Assume $\rho_{\min}$ is a minimum positive constant that separates the $c_j$ and other nodes. Then, each cluster can build a crossing path within $\rho_{\max}$ for $\delta > 2$.*

**Proof.** Each cluster is tessellated into $x \times \frac{n/m}{x}$ circular squares, where $x$ is the number of sectors and $\frac{n/m}{x}$ is the number of annuli. Note that the arc of each sector is equal, *i.e.*, $\frac{2\pi}{x}$. Due to the heterogeneous node distribution, the distance between every two annuli is not the same, as shown in Figure 2.

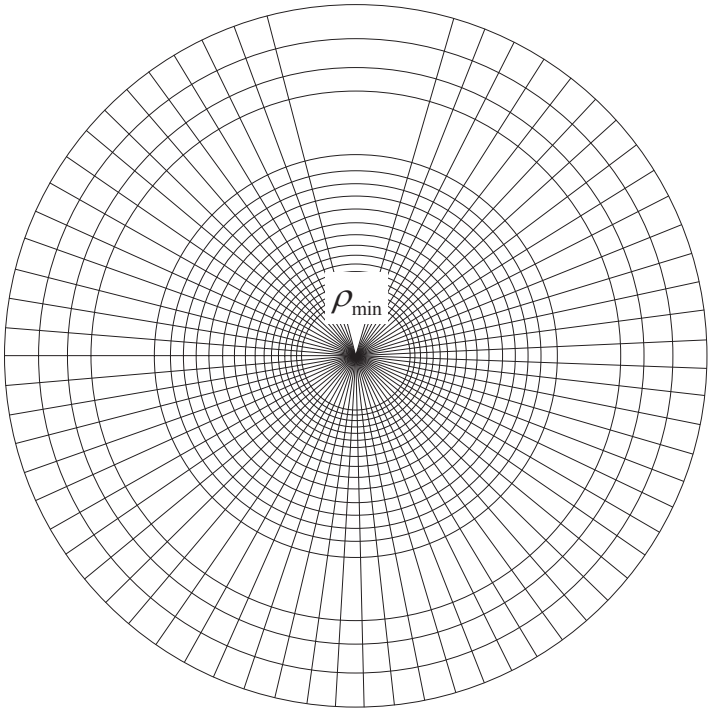


**Figure 2.** A circular square in a cluster. $\rho_{\min}$ is the minimum radius within which there is no node located.

Due to the impact of heterogeneity, the node density at different annulus areas varies. In order to guarantee that each square contains at least one node, the external annuli need to be wider than the inner ones. Correspondingly, we set the radius of the $i$-th annulus to be:

$$r_i = \left(1 + \frac{2\pi}{x}\right)^{i-1} \cdot \rho_{\min} \tag{7}$$

Thus, according to the circular square tessellation above, we can conclude that each cell can be treated as a square when $n \to \infty$. □

**Lemma 2.** *According to the heterogeneous tessellation, we can get that the number of the parameter $x$ is:* $x = \Theta\left(\sqrt{\frac{n^{1-v}}{(1-v)\log n}}\right)$.

**Proof.** From Lemma 1, we know that the radius of one cluster is:

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

Combining Equation (3) and (8), we have:

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

Finally, we obtain $x = \Theta\left(\sqrt{\frac{n^{1-v}}{(1-v)\log n}}\right)$. □

**Lemma 3.** *For a square $s_i$ on the i-th annulus, let $X_{s_i}$ be the number of nodes distributed in $s_i$; then, we can get $P(X_{s_i} \geq 1) > P(X_{s_j} \geq 1)$ for $i < j$.*

**Proof.** According to percolation theory, a square $s_i$ is open if there exists at least one node located in $s_i$, or closed otherwise. From the Appendix A in [12], the open probability of a square is:

$$\begin{aligned} p_i \equiv P\left(X_{s_i} \geq 1\right) &= 1 - P\left(X_{s_i} = 0\right) \\ &\approx 1 - e^{-\frac{n}{m} r_i^{-\delta} \left(r_i \frac{2\pi}{x}\right)^2} \end{aligned} \tag{10}$$

From Equation (10), we can observe that $p_i$ decreases as increasing values of $i$ for $\delta > 2$. □

Since the probability $p_i$ decreases with $i$, we can calculate the critical value $\rho_{\max}$, within which the probability $p_i$ can satisfy the condition of $p_i > p_c$, where $p_c$ is the critical probability in percolation theory.

**Lemma 4.** *There exists a critical value* $\rho_{\max} = \Theta\left(((1-v)\log n)^{\frac{1}{\delta-2}}\right)$, *within which each cluster can construct a set of connected highways if the degradation factor* $\delta > 2$.

**Proof.** From percolation theory, there is a critical probability $p_c$, when $p > p_c$, that there exists many disjoint paths traversing the network, which is going to be one. Thus, we can get the following equation by Lemma 3:

$$p_i \equiv P(X_{s_i} \geq 1) \approx 1 - e^{-r_i^{-\delta}\left(r_i \frac{2\pi}{x}\right)^2} = p_o \tag{11}$$

where $p_o$ is the probability representing that the square $s_i$ is open, and $p_c < p_o < 1$.

Following Equation (11), we can obtain that:

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

where $c = \ln \frac{1}{1-p_o}$. Substituting $x = \Theta\left(\sqrt{\frac{n^{1-v}}{(1-v)\log n}}\right)$ into (12), we can achieve that $\rho_{\max} = \Theta\left(((1-v)\log n)^{\frac{1}{\delta-2}}\right)$. □

Combining Lemma 4 and Equation (7), the critical value $i_{\max} = \Theta\left(\frac{\log(\log n)}{\delta-2}\sqrt{\frac{n^{1-v}}{\log n}}\right)$ is achieved. In particular, we can construct $\Theta\left(\frac{\log(\log n)}{\delta-2}\sqrt{\frac{n^{1-v}}{\log n}}\right)$ annuli within the radius $\rho_{\max}$.

The percolation model for the intra-cluster traffic has been constructed. Each cluster is partitioned into $c_1\sqrt{\frac{n^{1-v}}{(1-v)\log n}} \times c_2 \frac{\log(\log n)}{\delta-2}\sqrt{\frac{n^{1-v}}{\log n}}$ lattices. Specifically, a path is called open if two adjacent squares are open. Based on Appendix I in [6], we can get that there are $\lceil \mu \log \omega(n) \rceil$ disjoint paths through an area of $\omega(n) \times (\kappa \log \omega(n) - \epsilon)$. Hence, within area of less than $\rho_{\max}$, we can build $\Omega\left(\sqrt{\frac{n^{1-v}}{(1-v)\log n}}\right)$ disjoint paths from the internal to external cluster and $\Omega\left(\frac{\log(\log n)}{\delta-2}\sqrt{\frac{n^{1-v}}{\log n}}\right)$ disjoint paths around each cluster. By the connection of these two paths, the highway system for the legitimate nodes is constructed. Although our model is a heterogeneous lattice, it can be treated similarly as a $c_1\sqrt{\frac{n^{1-v}}{(1-v)\log n}} \times c_2 \frac{\log(\log n)}{\delta-2}\sqrt{\frac{n^{1-v}}{\log n}}$ rectangle lattice.

## 5. The Secrecy Rate of Intra-Cluster Traffic

In this section, as illustrated in Figure 3, we introduce a scheme that ensures the security over the whole path, from the source to a destination. The routing scheme of intra-cluster transmission can be partitioned into four separate phases.

Phase 1 (draining phase): Source node $S$ drains packets to an access node on the radial highway directly. Note that the highway may not be fully contained in its corresponding sector, whereas it may deviate from it. However, according to percolation theory, a highway is never farther than $\kappa \log\left(\frac{n/m}{x} - \epsilon\right)$ from its corresponding sector.

Phase 2 (radial highway phase): Packets are carried across the cluster along the radial highway using multiple hops and multiple time slots.

Phase 3 (encircling highway phase): Similar to Phase 2, packets are transported clockwise on the annulus highway.

Phase 4 (delivering phase): Finally, packets are delivered to the receiver from the exit point on the encircling highway.

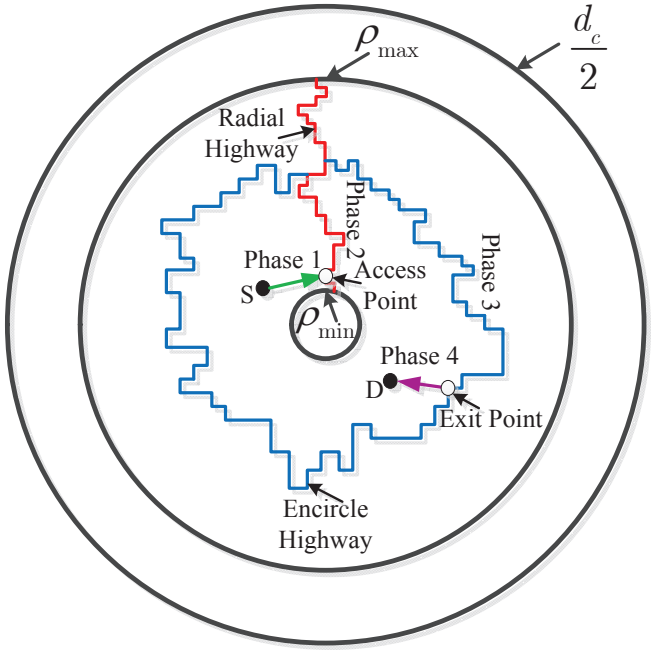


**Figure 3.** A schematic representation of the routing scheme. We omit the eavesdroppers in this figure.

Different nodes are allocated with different power, so that we can transform the heterogeneous circular lattice into a homogenous regular square lattice. In addition, the time division multiple access (TDMA) schedule is employed, and the information is transported hop by hop, then a constant rate on the highway is obtained. However, there are still some differences between our model and the previous one; for example, not all of the highways serve identical nodes, and the power of each node is not equal.

**Lemma 5.** *For a given square, to cancel the interference caused by simultaneous transmission, the power of legitimate nodes in square $s_i$ is:*

$$P_i = P_0 \cdot \left(\frac{2\pi r_i}{x}\right)^{\alpha} \tag{13}$$

*where $P_0$ is the unit power for a legitimate transmitter.*

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

$$I_1(d) = P_{(i+d)} \frac{1}{(r_{i+d} - r_i)^{\alpha}} \tag{14}$$

$$I_2(d) = P_{(i-d)} \frac{1}{(r_i - r_{i-d})^{\alpha}} \tag{15}$$

We can also get that:

$$\begin{aligned}\frac{I_1(d)}{I_2(d)} &= \frac{P_{(i+d)}}{P_{(i-d)}} \cdot \frac{(r_i - r_{i-d})^\alpha}{(r_{i+d} - r_i)^\alpha} \\ &= \left(\frac{r_{i+d}}{r_{i-d}} \cdot \frac{r_i - r_{i-d}}{r_{i+d} - r_i}\right)^\alpha \\ &= \left(1 + \frac{2\pi}{x}\right)^{d\alpha}\end{aligned} \tag{16}$$

As $x = \Theta\left(\sqrt{\frac{n^{1-v}}{(1-v)\log n}}\right)$, when $d = o\left(\sqrt{\frac{n^{1-v}}{(1-v)\log n}}\right)$, we can get $\frac{I_1(d)}{I_2(d)} \to 1$. □

Next, we exploit the idea of the secrecy zone to guarantee the secrecy of the communication over a single hop.

By Lemma 5, for a given square, the interference caused at $d$ squares is equal. Thus, we can make the cluster network as a square network. As shown in Figure 4, we group several squares into a group with edge $k_t d$ squares. Each group contains $(k_t d)^2$ squares. Using the TDMA to schedule the transmission, that is each square takes a turn on the transmission over $(k_t d)^2$ slots, in each slot, a transmitter can send packets to a receiver located at most $d$ squares away. In Figure 4, the larger square around a transmitting square is the secrecy zone, which consists of squares that are at most $k_e d$ squares away. We firstly establish an achievable secure rate on a single hop.

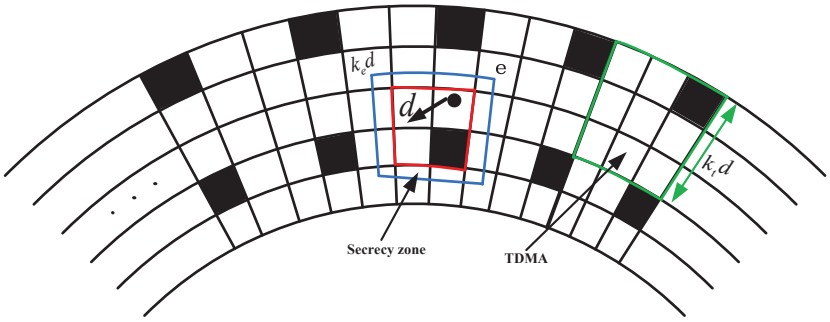


**Figure 4.** An illustration of the TDMA strategy with size $k_t d$. The blue square surrounding the transmitter is the secrecy zone, which is at most $k_e d$ squares away from the transmitter.

**Theorem 6.** *In each square, the secrecy rate that a legitimate source-destination pair can obtain is* $R_s(d) = \Omega\left(d^{-\alpha-2}\right)$, *if:*

$$\frac{(N_0 + c^*)d^{-\alpha}}{N_0(d+1)^{-\alpha}} < k_e^\alpha \tag{17}$$

*where* $c^*$ *is a constant and* $d$ *is the transmission range.*

**Proof.** Assuming that transmitter $i$ in square $s_i$ transmits toward destination $j$ located in square $s_j$ at a distance of $d$ squares away, we obtain the $SINR$ of the legitimate receiver as follows:

$$SINR_{ij} = \frac{P_i d_{ij}^{-\alpha}}{N_0 + \Sigma_{\zeta \in T} P_\zeta d_{\zeta j}^{-\alpha}} \tag{18}$$

where $d_{ij}$ is the distance between source node $i$ and destination node $j$, and $d_{\zeta j}$ is the distance between interferer $\zeta \in T$ and the receiver.

For the case of eavesdropper $e \in \varepsilon$, the upper bound $SINR$ at the eavesdropper is:

$$SINR_e \leq \frac{P_i d_{ie}^{-\alpha}}{N_0} \tag{19}$$

where $d_{ie}$ is the distance between the transmitter and eavesdropper $e$, where the upper bound of $SINR_e$ is obtained by getting rid of the interference at the eavesdropper. Note that the distance between the $i$ and $j$ is at most $\frac{2\pi r_i}{x}(d+1)$, *i.e.*,

$$d_{ij} \leq (d+1)\frac{2\pi r_i}{x} \tag{20}$$

and:

$$d_{ie} \leq k_e d\frac{2\pi r_i}{x} \tag{21}$$

Let $I(d)$ denote the upper bound of the interference caused by simultaneous transmitter nodes. Then,

$$\begin{aligned} I(d) &\leq \sum_{\zeta=1}^{\infty} 8\zeta P_{i+\zeta k_t d}\left(\frac{1}{\sqrt{2}r_{i+\zeta k_t d} - r_i}\right)^{\alpha} \\ &\leq \sum_{\zeta=1}^{\infty} 8\zeta P_{i+\zeta k_t d}\left(\frac{1}{\sqrt{2}\zeta k_t d r_i \frac{2\pi}{x}}\right)^{\alpha} \\ &= \sum_{\zeta=1}^{\infty} 8\zeta P_0\left(\frac{1}{\sqrt{2}\zeta k_t d}\left(1+\frac{2\pi}{x}\right)^{k_t\zeta d}\right)^{\alpha} \\ &= P_0(\sqrt{2}k_t d)^{-\alpha}\sum_{\zeta=1}^{\infty} 8\zeta^{1-\alpha}\left(1+\frac{2\pi}{x}\right)^{k_t\zeta d\alpha} \end{aligned} \tag{22}$$

notice that this sum will converge to a constant $c^*$, if $\alpha > 2$, and the proof is shown in Appendix A.

Substitute Equations (20)–(22) in Equations (18) and (19); we obtain that:

$$SINR_{ij} \geq \underline{SINR_{ij}} \triangleq \frac{P_i\left((d+1)\frac{2\pi r_i}{x}\right)^{-\alpha}}{N_0 + c^*} \tag{23}$$

and:

$$SINR_e \leq \overline{SINR_{e^*}} \triangleq \frac{P_i\left(k_e d\frac{2\pi r_i}{x}\right)^{-\alpha}}{N_0} \tag{24}$$

Hence, $SINR_{ij} > SINR_e$ for every eavesdropper $e$, if we choose $k_e$ such that:

$$\frac{(N_0 + c^*)d^{-\alpha}}{N_0(d+1)^{-\alpha}} < k_e^{\alpha} \tag{25}$$

According to the Gaussian wiretap channel capacity [27], the secrecy rate $R_s(d)$ in each square is:

$$R_s(d) = \frac{1}{(k_t d)^2}\left[\log(1+\underline{SINR_{ij}}) - \log(1+\overline{SINR_{e^*}})\right] = \Omega\left(d^{-\alpha-2}\right) \tag{26}$$

where $\frac{1}{(k_t d)^2}$ is the time utilization factor. □

Now, similar to Lemma 2 in [22], we adopt the multi-hop randomization strategy, which guarantees the security over the entire path, from source to destination, at each eavesdropper listening to all transmissions. In [22], the authors assumed that each legitimate node used identical power for transmission, while we assign different powers for different nodes, as shown in Lemma 5. Despite the difference in the power, the proof goes along the same line as [22]. For conciseness, we omit details.

**Lemma 7.** *(Lemma 2 in [22]) If we can secure each hop from an eavesdropper, then we can ensure secure for all hops from any eavesdropper located on the edge of the secrecy zone.*

In Section 4, we have described the circular percolation model and constructed highways without the constraint of security. If taking the secrecy constraint into consideration, a square is open if the square contains at least one legitimate node and there is no eavesdropper within the secrecy zone of the square. The following result gives the existence of a sufficient number of secure highways in intra-cluster transmission.

**Lemma 8.** *We can construct a number of* $\Theta\left(\sqrt{\frac{n^{1-v}}{(1-v)\log n}}\right)$ *radial secrecy highways and* $\Theta\left(\frac{\log(\log n)}{\delta-2}\sqrt{\frac{n^{1-v}}{\log n}}\right)$ *encircling highways within the radius* $\rho_{\max}$, *if* $\lambda_e = o\left((\log n)^{-\frac{\delta}{\delta-2}}\right)$.

**Proof.** For a given square, let $q_i$ be the probability of $s_i$ contained in a secrecy zone without eavesdroppers. According to a Poisson random distribution, the average number of eavesdroppers located in a secrecy zone is $\lambda_e(2k_ed+1)^2\left(\frac{2\pi}{x}r_i\right)^2$, and $q_i$ can be denoted as:

$$q_i = e^{-\lambda_e(2k_ed+1)^2\frac{n}{m}\left(\frac{2\pi}{x}r_i\right)^2} \tag{27}$$

Since $r_i < \rho_{\max} = \Theta\left(((1-v)\log n)^{\frac{1}{\delta-2}}\right)$, $n \to \infty$, we have that $q_i$ trends to one if $\lambda_e = o\left((\log n)^{-\frac{\delta}{\delta-2}}\right)$.

Note that the status of edges in squares is not statistically independent due to the intersection of the associated secrecy zone. If both secrecy zones did not cross, the states of two squares would be independent. This occurs when the squares are at a distance of at least $2k_ed$ squares away. Thus, we can conclude that the dependent model is related to a finite dependence model, as $k_e$ and $d$ are constants. According to Theorem 7.65 in [28], this dependent model stochastically dominates an independent model. Let $p_i'$ be the probability that squares are independently open. If $p_iq_i$ can be made arbitrarily high, $p_i'$ will be close to one. Therefore, under the assumption of the finite dependence model and some desirable properties, we can prove that the network will still percolate with the same properties, since both $p_i$ and $q_i$ can be set sufficiently large.

Under the independent square model, by Theorem 5 in [6], with a square openness probability of $p_i'$, we can obtain that there are $\Theta\left(\sqrt{\frac{n^{1-v}}{(1-v)\log n}}\right)$ radial secrecy highways and $\Theta\left(\frac{\log(\log n)}{\delta-2}\sqrt{\frac{n^{1-v}}{\log n}}\right)$ annuli highways. □

Till now, we have established the existence of a sufficient number of secure highways using the circular percolation model. Since there are four phases for packet transmission, we will derive the secrecy rate in each phase to find the rate bottleneck.

**Lemma 9.** *If a cluster is divided into* $w$ *sectors with an arc of* $2\pi/w$, *then for each sector* $SR_i$, *there are no more than* $\frac{2n/m}{w}$ *legitimate nodes located.*

**Proof.** Let $|SR_i|$ represent the number of legitimate nodes located in $SR_i$ and $P_w$ be the probability that there exists a sector containing more than $\frac{2n/m}{w}$ nodes. For each sector, the number of nodes follows a Poisson distribution of $\frac{2n/m}{w}$. According to the Chernoff bound, when $n \to \infty$, then:

$$\begin{aligned} P_w &\leq wP\left(|SR_i| > \frac{2n/m}{w}\right) \\ &\leq we^{-\frac{n/m}{w}}\left(\frac{e^{\frac{n/m}{w}}}{\frac{2n/m}{w}}\right)^{\frac{2n/m}{w}} \\ &= we^{-\frac{n/m}{w}}\left(\frac{e}{2}\right)^{\frac{2n/m}{w}} \to 0 \end{aligned} \tag{28}$$

Therefore, we can get that there is no sector existing with more than $\frac{2n/m}{w}$ nodes. □

**Lemma 10.** *In Phase 1, if the density of the eavesdropper is* $\lambda_e = o\left((\log n)^{-\frac{3\delta-4}{\delta-2}}\right)$, *each legitimate node can achieve a secrecy access rate* $R_1 = \Omega\left(\left(\log\left(\sqrt{(1-v)n^{1-v}\log n}\right)\right)^{-3-\alpha}\right)$ *with a node on the radial highway.*

**Proof.** According to Theorem 5 in [6], if we choose $\epsilon$ and $\kappa$ appropriately, there exist at least $\Omega(\log(\frac{n/m}{x}))$ radial highways within a sector of arc $\frac{2\pi}{x}[\kappa\log(\frac{n/m}{x})-\epsilon]$. From percolation theory, we know that each highway may not be fully contained in its corresponding sector, and it may deviate from it. However, it never deviate by an arc of $\frac{2\pi}{x}[\kappa\log(\frac{n/m}{x})-\epsilon]$ from its corresponding sector, *i.e.*, it will not be father than $\kappa\log\left(\frac{n/m}{x}-\epsilon\right)$ squares.

By Theorem 6, let $d = \kappa\log\left(\frac{n/m}{x}-\epsilon\right)$; we can get that the secrecy rate between a legitimate node and an access node is:

$$R\left(\kappa\log\left(\frac{n/m}{x}-\epsilon\right)\right) = \Omega\left(\left(\sqrt{\log((1-v)n^{1-v}\log n)}\right)^{-2-\alpha}\right) \tag{29}$$

Since there is an amount of nodes in a square, they need to share the bandwidth. From Lemma 9, we have that, if the associated secrecy zone contains no eavesdropper, the secrecy rate for Phase 1 is $\Omega\left(\left(\sqrt{\log((1-v)n^{1-v}\log n)}\right)^{-3-\alpha}\right)$. Next, we elaborate that this will happen if $\lambda_e = o\left((\log n)^{-\frac{3\delta-4}{\delta-2}}\right)$ as $n$ goes to infinity.

For the $i$-th annulus, the area of the guard zone is $A_i = (2k_ed+1)^2\left(\frac{2\pi}{x}r_i\right)^2$, which is the area to eliminate the eavesdroppers. Let $|\varepsilon|$ be the number of eavesdroppers in a cluster (Poisson with parameter $\frac{\lambda_e n}{m}$) and $|L|$ as the total amount of legitimate nodes in a cluster. In addition, we denote the total area that the eavesdroppers make it impossible for a legitimate user to arrive at a highway as $A_\varepsilon$. Clearly, $A_\varepsilon \le A_{\max}|\varepsilon|$, where $A_{\max} = (2k_ed+1)^2\left(\frac{2\pi}{x}\rho_{\max}\right)^2$. For each $A_i$, let the amount of legitimate nodes in this region be $L_i$. According to the heterogeneity of node distribution, we have $L_i \le \frac{n}{m}r_i^{-\delta}A_i$. Thus, for each cluster, by the Chebyshev inequality, we have:

$$\begin{aligned} |\varepsilon| &\le (1+\epsilon)\lambda_e\frac{n}{m} \\ |L| &\ge (1-\epsilon)\frac{n}{m} \\ L_{A_{\max}|\varepsilon|} &\le (1+\epsilon)\frac{n}{m}A_{\max}|\varepsilon| \end{aligned} \tag{30}$$

for any $\epsilon \in (0,1)$ with high probability as $n \to \infty$. Let $F$ be the fraction of legitimate nodes that cannot transmit to highways due to the eavesdropper, and we can obtain the upper bound of $F$ as:

$$F \le \frac{L_{A_{\max}|\varepsilon|}}{L} \le \frac{(1+\epsilon)^2(2k_ed+1)^2\frac{n}{m}\left(\frac{2\pi}{x}\rho_{\max}\right)^2\lambda_e\frac{n}{m}}{(1-\epsilon)\frac{n}{m}} \to 0 \tag{31}$$

with the probability going to one as $n \to \infty$. The first inequality is deduced from the intersecting secrecy zones caused by eavesdroppers, and the second inequality derives from Equation (30), while the limit holds as $d = \kappa\log\left(\frac{n/m}{x}-\epsilon\right)$ and $\lambda_e = o\left((\log n)^{-\frac{3\delta-4}{\delta-2}}\right)$. Under this condition, we can conclude that almost all of the legitimate nodes are securely connected to the highways as $n \to \infty$. □

Phase 4 is the opposite process of Phase 1. Therefore, a similar conclusion can be made for this phase.

**Lemma 11.** *In Phase 4, if the density of eavesdropper* $\lambda_e = o\left((\log n)^{-\frac{3\delta-4}{\delta-2}}\right)$*, then a legitimate node can receive information securely from the highway at a rate of* $R_4 = \Omega((\log(\sqrt{(1-v)n^{1-v}\log n}))^{-3-\alpha})$.

In the highway phase, the information is transmitted hop by hop. Let $d = 1$ in Theorem 6; we obtain the secrecy rate in Phase 2.

**Lemma 12.** *In Phase 2, if the density of eavesdropper* $\lambda_e = o\left((\log n)^{-\frac{\delta}{\delta-2}}\right)$*, then a legitimate node on the radial highway can achieve a secrecy rate* $R_2 = \Omega\left(\frac{1}{\sqrt{n^{1-v}(1-v)\log n}}\right)$.

**Proof.** According to the highway system, the transmission is occurring from one square to a neighboring square, where within the secrecy zone, there are no eavesdroppers. Thus, using Theorem 6 and letting $d = 1$, the secrecy rate in Phase 2 is $\Omega(1)$. Since $x >> \log\frac{n}{mx}$, there are $\Omega(x)$ radial paths extended from internal to external. By Lemma 9, we have that there are at most $\frac{2n}{mx}$ users w.h.p. in the sector of $\frac{2\pi}{x}$. That is, each node can enjoy a rate of order $\Omega\left(\frac{1}{\sqrt{n^{1-v}(1-v)\log n}}\right)$ in the radial highway. □

In this way, the following lemma gives the secrecy rate of Phase 3.

**Lemma 13.** *The legitimate nodes on the annulus highway can enjoy a per-node secrecy rate* $R_3 = \Omega\left(\sqrt{\frac{(1-v)\log n}{n^{1-v}}} \cdot f(\delta)\right)$*, where* $f(\delta)$ *is a "heterogeneous factor", which is only decided by* $\delta$.

**Proof.** Compared to the radial highways, it is more complicated for data delivered around the cluster, since the number of nodes served by the annulus paths is not identical. Assume each annulus highway is identical, similar to Lemma 12; the secrecy rate of order $\Omega\left(\sqrt{\frac{(1-v)\log n}{n^{1-v}}}\right)$. Nevertheless, due to the impact of heterogeneity, we denote the achievable secrecy rate as $\Omega\left(\sqrt{\frac{(1-v)\log n}{n^{1-v}}} \cdot f(\delta)\right)$, where $f(\delta)$ is a function of heterogeneous factor $\delta$, which will be discussed in detail in Appendix B. □

Comparing the secrecy rate and the tolerable density of eavesdroppers in each phase, the secrecy rate of intra-cluster transmission can be concluded as follows.

**Theorem 14.** *For the intra-cluster traffic, if the density of eavesdropper* $\lambda_e = o\left((\log n)^{-\frac{3\delta-4}{\delta-2}}\right)$*, then each legitimate node located within* $\rho_{\max}$ *can achieve a secrecy rate of* $R_s^{intra} = \Omega\left(\frac{1}{\sqrt{n^{1-v}(1-v)\log n}}\right)$,

**Proof.** Comparing the achievable secrecy rate in each phase, the rate bottleneck occurs in Phase 2. Since the information is transmitted hop by hop, we need to guarantee security in each phase. Thus, comparing the density of eavesdroppers in each phase, we can get that, if the density of eavesdroppers $\lambda_e = o\left((\log n)^{-\frac{3\delta-4}{\delta-2}}\right)$, the secrecy rate of intra-cluster transmission is $R_s^{intra} = \Omega\left(\frac{1}{\sqrt{n^{1-v}(1-v)\log n}}\right)$ (the proof is in Appendix B). □

## 6. The Secrecy Transmission of Inter-Cluster Traffic

Since we focus on the cluster-sparse network, the node density outside the circular square is much lower. Thus, we cannot use the highway system constructed in Section 5. However, according to the distribution of PPP, we can extract part of nodes with a density of $\phi$ to build "information

pipelines", where $\phi$ is smaller than $\underline{\Phi}$ and is selected randomly and uniformly. As shown in Figure 5, we use these "information pipelines" to connect the clusters.

Similarly, by virtue of percolation theory, we can divide the area into regular squares with a side length of $\sqrt{c_0/\overline{\Phi}}$, where $c_0$ is a constant. For some special large value $c_0$, we can extract part of nodes to form "information pipelines", which is similar to the highways constructed in the homogeneous network. However, due to the heterogeneity, each square contains difference nodes.

In the previous section, we have already achieved the secrecy rate in the cluster area through a highway system. Within the dense areas, information is transmitted by the routes formed by the highway system. Only if the destination is located in different clusters, the information will be delivered through the "information pipelines". Similar to the derivation of intra-cluster transmission, the achievable secrecy rate of inter-cluster traffic can be obtained easily.

Borrowing the tools from percolation theory in [6], we can construct $\Omega(\sqrt{A\underline{\Phi}})$ pipelines among clusters. All of these pipelines need to serve $\Theta(m)$ clusters. Similar to Lemma 1 in [22], a secrecy zone is employed to protect the secrecy transmission over a single hop, where the edge of the secrecy zone is not $c$, but $\sqrt{\frac{c_0}{\underline{\Phi}}}$. Correspondingly, we can build $\Omega\left(\frac{\sqrt{A\underline{\Phi}}}{m}\right)$ pipelines between two neighboring clusters, *i.e.*, each cluster can enjoy $\Omega\left(\frac{\sqrt{A\underline{\Phi}}}{m}\right)$ pipelines. By Theorem 6 in [22], we can conclude that, if $\lambda_e = o\left(\left(\log\left(n\underline{\Phi}\right)\right)^{-2}\right)$, the secrecy rate of inter-cluster transmission is $\Omega\left(\frac{\sqrt{A\underline{\Phi}}}{n}\right)$.

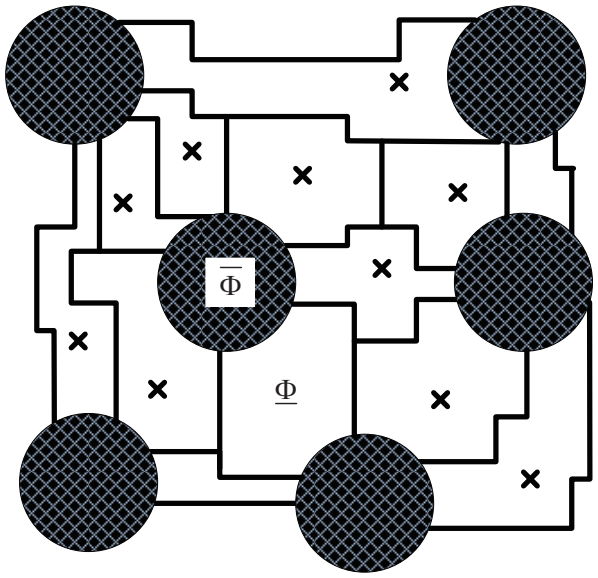


**Figure 5.** An illustration of information pipelines among clusters. Since the minimum node density is $\underline{\Phi}$, we can construct $\Omega(\sqrt{A\underline{\Phi}})$ pipelines among clusters. The crosses denote the eavesdroppers.

**Theorem 15.** *For the inter-cluster transmission, the achievable secrecy rate is* $R_s^{inter} = \Omega\left(\frac{\sqrt{A\underline{\Phi}}}{n}\right) = \Omega\left(\sqrt{\frac{\underline{\Phi}}{n}}\right)$, *if the density of the eavesdropper* $\lambda_e = o\left(\left(\log\left(n\underline{\Phi}\right)\right)^{-2}\right)$.

Figure 6 compares the throughput under homogeneous networks and heterogeneous networks. By observing the secrecy rate of intra-cluster and inter-cluster transmission, we find that the secrecy rate of intra-cluster transmission is higher than that of homogeneous networks; therefore, the bottleneck occurs in the inter-cluster transmission. This is due to the reduction of the number of highways caused by the lower density and, thereby, the amount of relaying traffic increasing. Particularly, when the network is transferred to a homogeneous network, *i.e.*, $\underline{\Phi} = \Theta(\overline{\Phi}) = \Theta(1)$, the secrecy rate is $R_s^{inter} = \Omega(\frac{1}{\sqrt{n}})$, and the tolerable density of the eavesdropper is $\lambda_e = o\left(\left(\log n\right)^{-2}\right)$, which is the same result as that in homogeneous wireless networks [22].

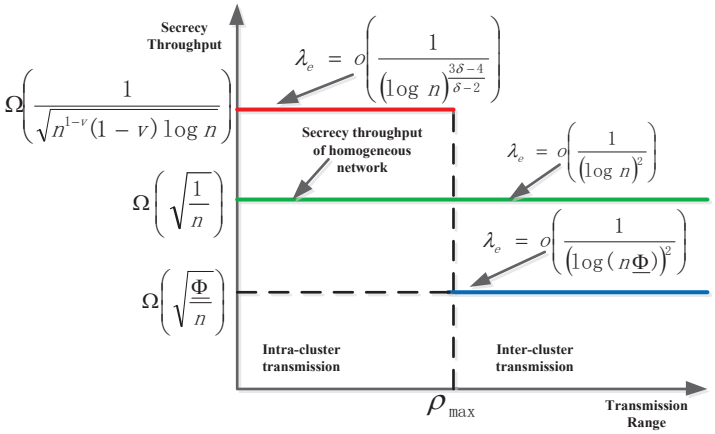


**Figure 6.** An illustration of secrecy throughput. We also give a comparison with that in a homogeneous networks [22].

## 7. Conclusions

In this work, we study the impact of heterogeneity and the secrecy constraint on the capacity of wireless networks. Borrowing the tools from percolation theory, we first constructed a secrecy highway system for intra-cluster and inter-cluster transmission, respectively. With the protection of the secrecy zone, the relationship between secrecy capacity and the tolerable density of the eavesdropper is studied. It is shown that the intra-cluster transmission not only can achieve a higher secrecy capacity, but also can tolerate more eavesdroppers. Moreover, the highway system we constructed is suitable for non-uniform traffic networks, typically, such as social networks. Thus, this work provides an insight model to analyze social networks. Finally, we do not consider the case of eavesdroppers collaborating with each other. Thus, it is a valuable future work to study the scenario of colluding eavesdroppers, where the distribution of legitimate nodes and eavesdroppers will influence the secrecy throughput greatly.

**Acknowledgments:** This work was supported in part by the Key project of the National Natural Science Foundation of China (NSFC) (Grant No. 61231010), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20120142110015), the 863 project of China (Grant No. 2014AA01A701) and the National Natural Science Foundation of China (NSFC) (Grant No. 61471408).

**Author Contributions:** Qiuming Liu proposed the idea, derived the results and wrote the paper. Li Yu supervised the work and reviewed the article in the initial and revised versions. Zuhao Liu proposed the circular percolation model. Jun Zheng assisted in revising the paper.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix

### A. The Proof of Theorem 1

Proof: We prove the summation of Equation (22) to converge to some constant. Since we consider the scenario of $n \to \infty$, Equation (22) can be simplified as $\sum_{\zeta=1}^{\infty} \zeta^{1-\alpha}(1+2\pi/x)^{k_t\zeta d\alpha}$. Firstly, we solve $(1+2\pi/x)^{k_t\zeta d\alpha}$, where $x$ is given in Lemma 2. Thus, we obtain:

$$\begin{aligned}(1+2\pi/x)^{k_t\zeta d\alpha} &= (1+\frac{2\pi}{\sqrt{\frac{n^{1-v}}{(1-v)\log n}}})^{\frac{\sqrt{\frac{n^{1-v}}{(1-v)\log n}}}{2\pi}\cdot\frac{2\pi}{\sqrt{\frac{n^{1-v}}{(1-v)\log n}}}\cdot k_t\zeta d\alpha} \\ &= e^{\frac{2\pi}{\sqrt{\frac{n^{1-v}}{(1-v)\log n}}}\cdot k_t\zeta d\alpha}\end{aligned} \tag{A1}$$

when $d = o(\sqrt{\frac{n^{1-v}}{(1-v)\log n}})$ and $n \to \infty$. Then, $(1+2\pi/x)^{k_t\zeta d\alpha} = e^{\frac{2\pi}{\sqrt{\frac{n^{1-v}}{(1-v)\log n}}}\cdot k_t\zeta d\alpha} \to \Theta(1)$. Since $\alpha > 2$, the summation Equation (22) converges to a constant.

### B. The Proof of Theorem 2

Proof: The achievable rate of the annulus highway in the intra-cluster phase is derived as follows: According to four phases of the routing scheme, we give a comparison of the secrecy rate on the radial highway and the annulus highway. The secrecy rate on the radial highway can be obtained easily (Lemma 12). Hence, We only need to derive the secrecy rate of the annulus highway. Due to the number of nodes on different annuli not being identical, the derivation of the annulus highway is more complicated than the case of the radial highway. According to the distribution of legitimate nodes, let $E(N_i)$ be the average number of nodes in annulus $i$. Then, the expectation of $E(N_i)$ is:

$$E(N_i) = \frac{n}{m}\left(r_i\frac{2\pi}{x}\right)^2\frac{1}{r_i^{\delta}}x \tag{B1}$$

Using Equation (7) to substitute $r_i$, we can get:

$$\begin{aligned} E(N_i) &= \frac{n}{m}\left(r_i\frac{2\pi}{x}\right)^2\frac{1}{r_i^{\delta}}x \\ &= 4\pi^2\frac{n}{m}x^{-1}r_i^{2-\delta} \\ &= 4\pi^2\frac{n}{m}x^{-1}\left(1+\frac{2\pi}{x}\right)^{i(2-\delta)} \\ &= 4\pi^2\frac{n}{m}\sqrt{\frac{(1-v)\log n}{n^{1-v}}}\left(1+\frac{2\pi}{\sqrt{\frac{n^{1-v}}{(1-v)\log n}}}\right)^{i(2-\delta)} \end{aligned} \tag{B2}$$

Since $\delta > 2$, $E(N_i)$ is decreased with the increasing of $i$. Therefore, the annulus highway near the center will service the most nodes. As a consequence, the achievable secrecy rate on the annulus highway is:

$$R_3 > R_r(i=1) = \Theta\left(\sqrt{\frac{1}{(1-v)n^{1-v}\log n}}\left(1+\frac{2\pi}{\sqrt{\frac{n^{1-v}}{(1-v)\log n}}}\right)^{(\delta-2)}\right) \tag{B3}$$

By comparing the rate $R_2$ and $R_3$, we can find that $R_2 < R_3$, for $\delta > 2$, *i.e.*, the secrecy rate bottleneck is in the phase of the radial highway.

### References


1. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. *IEEE Commun. Mag.* **2002**, *40*, 102–114.
2. Heinzelman, W.B.; Chandrakasan, A.P.; Balakrishnan, H. An application-specific protocol architecture for wireless microsensor networks. *IEEE Trans. Wirel. Commun.* **2015**, *45*, 1018–1034.
3. Tan, L.; Ge, F.; Li, J.; Kato, J. HCEP: A hybrid cluster-based energy-efficient protocol for wireless sensor networks. *Int. J. Sensor Netw.* **2009**, *5*, 67–78.
4. Wu, M.; Tan, L.; Xiong, N. A structure fidelity approach for big data collection in wireless sensor networks. *Sensors* **2014**, *14*, 248–273.
5. Gupta, P.; Kumar, P.R. The capacity of wireless networks. *IEEE Trans. Inf. Theory* **2000**, *46*, 388–404.
6. Franceschetti, M.; Dousse, O.; Tse, D.N.; Thiran, P. Closing the gap in the capacity of wireless networks via percolation theory. *IEEE Trans. Inf. Theory* **2007**, *53*, 1009–1018.

7. Hu, C.; Wang, X.; Yang, Z.; Zhang, J.; Xu, Y.; Gao, X. A geometry study on the capacity of wireless networks via percolation. *IEEE Trans. Commun.* **2010**, *58*, 2916–2925.
8. Liu, B.; Thiran, P.; Towsley, D. Capacity of a wireless ad hoc network with infrastructure. In Proceedings of the 8th ACM International Symposium on Mobile ad hoc Networking and Computing, Montreal, QC, Canada, 9–14 September 2007; pp. 229–237.
9. Tan, L.; Zhu, Z.; Ge, F.; Xiong, N. Utility Maximization Resource Allocation in Wireless Networks: Methods and Algorithms. *IEEE Trans. Syst. Man Cybernetics: Syst.* **2015**, *45*, 1018–1034.
10. Xiangyang, L. Multicast capacity of wireless Ad Hoc networks. *IEEE/ACM Trans. Netw.* **2009**, *17*, 950–962.
11. Alfano, G.; Garetto, M.; Leonardi, E. Capacity scaling of wireless networks with inhomogeneous node density: Upper bounds. *IEEE J. Selected Areas Commun.* **2009**, *27*, 1147–1157.
12. Alfano, G.; Garetto, M.; Leonardi, E.; Martina, V. Capacity scaling of wireless networks with inhomogeneous node density: Lower bounds. *IEEE/ACM Trans. Netw.* **2010**, *18*, 1624–1636.
13. Liu, Z.; Yu, L.; Gao, Y.; Hu, S.; Samb, D. A Constructive Capacity Lower Bound of the Inhomogeneous Wireless Networks. *Wirel. Personal commun.* **2013**, *71*, 2333–2348.
14. Kim, E.J.; Shon, T.; Park, J.J.H.; Jeong, Y.S. Throughput Fairness Enhancement Using Differentiated Channel Access in Heterogeneous Sensor Networks. *Sensors* **2011**, *11*, 6629.
15. Lu, N.; Shen, X.S. Scaling laws for throughput capacity and delay in wireless networks—A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 642–657.
16. Zhang, C.; Song, Y.; Fang, Y.; Zhang, Y. On the price of security in large-scale wireless ad hoc networks. *IEEE/ACM Trans. Netw.***2011**, *19*, 319–332.
17. Bhandari, V.; Vaidya, N. Secure capacity of multi-hop wireless networks with random key pre-distribution. In Proceedings of the IEEE INFOCOM Workshops, Phoenix, AZ, USA, 13–18 April 2008; pp. 1–6.
18. Vasudevan, S.; Goeckel, D.; Towsley, D.F. Security-capacity trade-off in large wireless networks using keyless secrecy. In Proceedings of the Eleventh ACM International Symposium on Mobile Ad Hoc Networking and Computing, Chicago, IL, USA, 20–24 September 2010; pp. 21–30.
19. Capar, C.; Goeckel, D.; Liu, B.; Towsley, D. Secret communication in large wireless networks without eavesdropper location information. In Proceedings of the IEEE INFOCOM, Orlando, FL, USA, 25–30 March 2012; pp. 1152–1160.
20. Zhang, J.; Fu, L.; Wang, X. Asymptotic Analysis on Secrecy Capacity in Large-Scale Wireless Networks. *IEEE/ACM Trans. Netw.* **2014**, *22*, 66–79.
21. Cao, X.; Zhang, J.; Fu, L.; Wu, W.; Wang, X. Optimal Secrecy Capacity-Delay Tradeoff in Large-Scale Mobile Ad Hoc Networks. *IEEE/ACM Trans. Netw.***2015**, doi:10.1109/TNET.2015.2405793.
22. Koyluoglu, O.O.; Koksal, C.E.; Gamal, H.E. On secrecy capacity scaling in wireless networks. *IEEE Trans. Inf. Theory* **2012**, *58*, 3000–3015.
23. Zhou, X.; Ganti, R.K.; Andrews, J.G.; Hjorungnes, A. On the throughput cost of physical layer security in decentralized wireless networks. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 2764–2775.
24. Luan, T.; Lu, R.; Shen, X.; Bai, F. Social on the road: Enabling secure and efficient social networking on highways. *IEEE Wirel. Commun.* **2015**, *22*, 44–51.
25. Møller, J. Shot noise Cox processes. *Advances Appl. Probab.* **2003**, *35*, 614–640.
26. Wyner, A.D. The Wire-Tap Channel. *BELL LABS TECH J.* **1975**, *54*, 1355–1387.
27. Csiszár, I.; Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inform. Theory* **1978**, *24*, 339–348.
28. Grimmett, G. Inequalities and entanglements for percolation and random-cluster models. In *Perplexing Problems in Probability*; Birkhäuser: Basel, Switzerland, 1999; pp. 91–105.


© 2015 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons by Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).