Secrecy Capacity Scaling of Large-Scale Cognitive Networks

Yitao Chen[†], Jinbei Zhang[†], Xinbing Wang[†], Xiaohua Tian[†], Weijie Wu[‡], Fan Wu[‡], Chee Wei Tan[§]
[†] Dept. of Electronic Engineering, Shanghai Jiao Tong University, China
[‡]Dept. of Computer Science and Engineering, Shanghai Jiao Tong University, China
[§] Dept. of Computer Science, City University of Hong Kong
{albrecht, abelchina, xwang8, xtian, weijiewu, fwu}@sjtu.edu.cn, cheewtan@cityu.edu.hk

ABSTRACT

Increasingly, more spectrum bands are utilized for unlicensed use in wireless cognitive networks. It is important to study how information-theoretic secrecy capacity is affected in large-scale cognitive networks. We consider two scenarios: (1) non-colluding case, where eavesdroppers decode messages individually. In this case, we propose a new secure protocol model to analyze the transmission opportunities of secondary nodes. We show that the secrecy capacity of the primary network is not affected, while the secondary network can achieve the same performance as a standalone network in the order sense. Since our analysis is general as we only make a few relaxed assumptions on both networks, the conclusions hold when both networks are classic static networks, networks with i.i.d mobility, multicast networks etc. (2) colluding case where eavesdroppers can collude to decode a message. In that case, we show that the lower bound of per-node secrecy capacity of the primary network is $\Omega(\frac{1}{\sqrt{n}}\phi_e^{-\frac{2}{\alpha-1}}(n))$ when the eavesdropper density is $\phi_e(n) = \Omega(\log^2 n)$. Interestingly the existence of secondary nodes increases the secrecy capacity of the primary network.

1. INTRODUCTION

The fundamental scaling laws in ad hoc networks have been extensively studied since the seminal work of Gupta and Kumar [1]. They showed that for a network with n static nodes randomly located in a unit area, the per-node capacity is lower bounded by $\Omega(1/\sqrt{n\log n})$ and upper bounded by $O(1/\sqrt{n})$. This gap is later closed by Franceschetti *et al.* [2] using percolation theory. Later on, Grossglauser and Tse [3] further found capacity performance can be significantly improved when nodes are mobile. They showed the mobile network can achieve a per-node capacity of $\Theta(1)$ under the 2-hop relay algorithm. However, the significant improvement of capacity is achieved at the expense of a large delay, which is $\Theta(n)$ as proved by Neely *et al.* [4]. Since then, there have been numerous related works, which cover a wide variety of ad hoc networks with different features, such as multicast networks [5], [6] and hierarchically cooperative networks [7].

As the broadcast nature of the wireless medium allows eavesdroppers and attackers to intercept information transmission and can also degrade transmission quality, the security of wireless ad hoc networks has attracted considerable attention recently. In wireless ad hoc networks, the lack of infrastructure makes the key distribution and management required for traditional symmetric-key cryptographic approaches difficult; energy and computational ability limitations at terminals prohibit the use of asymmetric cryptography. As such, most previous works focus on the information-theoretic security, where eavesdroppers are assumed to have infinite computational power. In the analysis of information-theoretic security, the objective is to keep eavesdroppers from getting enough information. Vasudevan *et al.* [8] studied the secrecy-capacity tradeoff in large-scale wireless networks and introduced helpers around transmitters to generate noises to suppress the SINR at eavesdroppers. Koyluoglu *et al.* [9] showed that if the eavesdropper density is $o(1/(\log n)^2)$ in extended networks, then the secrecy rate scales as $1/\sqrt{n}$. Capar *et al.* [10] proposed a new secrecy communication scheme, which can tolerate $o(n/\log n)$ eavesdroppers, without affecting the network throughput. Zhang *et al.* [11] let the receivers generate artificial noises in order to degrade the SINR at eavesdroppers, and studied the impacts of secrecy constraints on the capacity scaling in static networks.

The aforementioned related work mainly focused on the secrecy capacity and delay scaling for a single network. In recent years, the lack of radio resource has led to the development of *cognitive radio* technology. Coexistent with licensed primary users, *cognitive (secondary)* users need to sense their spectral environment to opportunistically access the spectrum without harming the performance of primary users. Jeon *et al.* [12] showed that the static primary network and secondary network can simultaneously achieve the same capacity as stand-alone networks. Yin *et al.* [13] developed similar results for delay-throughput tradeoff. Huang *et al.* [14] characterized the general conditions for cognitive networks to achieve the same throughput and delay scaling as stand-alone networks. Tan *et al.* [16] propose a optimisation algorithm to the spectrum management in multiuser wireless cognitive networks

MobiHoc'14, August 11–14, 2014, Philadelphia, PA, USA.

Degradation in secrecy capacity is mainly caused by those eavesdroppers that are least affected by the artificial noise from receivers [11]. In cognitive networks, secondary users that are least affected by the interference from primary users get transmission opportunities, which can help to suppress the channel qualities of the eavesdroppers. Therefore, we study in depth the secrecy capacity and delay scaling in cognitive networks.

The main contributions of this paper are summarized as follows.

• In the non-colluding case, we propose a new secure protocol model to analyze the transmission opportunities of the secondary network. We give sufficient conditions under which the secondary network can achieve the same order secrecy performance as a standalone network without degrading the secrecy capacity of the primary network.

• In the non-colluding case, our results are derived without requiring specific constraints on the traffic patterns and the mobility models of primary and secondary networks. Thus, we can apply our results to general cognitive networks, such as classic static networks, networks with i.i.d mobility, multicast networks etc.

• In the colluding case, we prove that introducing the secondary nodes into the network increases the secrecy capacity of the primary network. We show that the lower bound of the secrecy capacity is $\Omega(\frac{1}{\sqrt{n}}\phi_e^{-\frac{2}{\alpha-1}}(n))$.

The rest of this paper is organized as follows. In Section 2, we introduce the system model. In Section 3 and 4, we give asymptotic analysis on secrecy capacity in the non-colluding case and colluding case, respectively. Finally, we conclude our paper in Section 5.

2. SYSTEM MODEL

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

2.1 Legitimate Network

We consider the scenario, in which there are two kinds of legitimate nodes, n primary nodes and m secondary nodes, overlapping in the square $\mathcal{O}$. We assume that both primary nodes and the secondary nodes are independently and identically distributed (i.i.d.) in $\mathcal{O}$ according to the uniform distribution. Their positions are denoted by $\{X_i\}_{i=1}^n$ and $\{Y_j\}_{j=1}^m$, respectively. Let $|X_i - Y_j|$ be the distance between two nodes. For two primary nodes forming a transmitter-receiver pair, they share a primary link denoted by $(X_i, X_{Rx(i)})$, where i is the index of the transmitter and $Rx(\cdot)$ is the index of the corresponding receiver. Similarly, we denote a secondary link by $(Y_j, Y_{Rx(j)})$. We denote $\mathcal{L}^p$ as the set of active primary links, $\mathcal{L}^s$ as the set of active secondary links and $\mathcal{L} = \mathcal{L}^p \cup \mathcal{L}^s$. In addition, $\mathcal{T}^p$ ($\mathcal{T}^s$) and $\mathcal{R}^p$ ($\mathcal{R}^s$) are the sets of active primary (secondary) transmitters and receivers, respectively. For active primary link $(X_i, X_{Rx(i)}) \in \mathcal{L}^p$ and active secondary link $(Y_j, Y_{Rx(j)}) \in \mathcal{L}^s$, we denote their transmission ranges as $R_i = |X_i - X_{Rx(i)}|$ and $r_j = |Y_j - Y_{Rx(j)}|$, respectively. We also use the same artificial noise generation scheme as that in [11] to enable the information-theoretic security in the network. We assume that each legitimate node is equipped with three antennas. When a legitimate node acts as a receiver, one antenna is used for message reception, while the other two simultaneously generate artificial noise to suppress the eavesdroppers' channels. The distances between the receiving antenna and the other two respective transmitting antennas satisfy a difference of half the radio wavelength. The interference can thus be eliminated by invoking the techniques of self-interference cancellation. Thereby, each receiver does not experience the artificial noise generated by the node itself.

2.2 Eavesdropper Network

We consider that there are $n\phi_e(n)$ eavesdroppers located in the same network area, where $\phi_e(n)$ is the density of eavesdroppers. Let $\mathcal{E}$ be the set of eavesdroppers and Z_e be the position of each eavesdropper $e \in \mathcal{E}$. We assume that all the eavesdroppers are silent and static, since they can be easily detected if they are active or move drastically. Hence, instead of jamming the signal, the eavesdroppers only overhear messages. We assume that each eavesdropper independently and identically selects a position in the network area $\mathcal{O}$ according to the uniform distribution. We also assume that the eavesdroppers have two overhearing modes, namely independent mode and colluding mode. In the independent mode, each eavesdropper decodes messages independently. In the colluding mode, all the eavesdroppers can communicate and collaborate to decode the messages. Maximum ratio combining is adopted to maximize the sum of SINR that each eavesdropper obtains. Hence, we can regard all the eavesdroppers as one super-eavesdropper. Moreover, since we consider information-theoretic security in this paper, we assume that the eavesdroppers have infinite computation resources. We also assume that both channel state information (CSI) and location information of the eavesdroppers are unknown to the legitimate nodes.

2.3 Communication Model: Physical Model

We describe our communication model in this section. For active primary (secondary) transmitter $i \in \mathcal{T}^p$ ($\mathcal{T}^s$), we use $P_{t,i}^p$ ($P_{t,i}^s$) to denote the transmission power of i, where the subscript t stands for transmitter. For active primary (secondary) receiver $j \in \mathcal{R}^p$ ($\mathcal{R}^s$), we use $P_{r,j}^p$ ($P_{r,j}^s$) to denote the noise generation power of j, where the subscript r stands for receiver. The path loss between node i and node j is denoted by $l(X_i, X_j) = \min\{1, |X_i - X_j|^{-\alpha}\}$. Here, α is the path loss exponent and we assume that $\alpha > 2$, which is a reasonable value range for extended network model. When node i is transmitting messages to node j, the signal to interference and noise ratio (SINR) at the receiver j is given as follows.

For the primary network,

$$\mathrm{SINR}_{ij}^p = \frac{P_{t,i}^p l(X_i, X_j)}{N_0 + I_{pp} + I_{sp}}, \tag{1}$$

where

$$I_{pp} = \sum_{k \in \mathcal{T}^p \setminus \{i\}} P_{t,k}^p l(X_k, X_j) + \sum_{k \in \mathcal{R}^p \setminus \{j\}} P_{r,k}^p l(X_k, X_j),$$

$$I_{sp} = \sum_{k \in \mathcal{T}^s} P_{t,k}^s l(Y_k, X_j) + \sum_{k \in \mathcal{R}^s} P_{r,k}^s l(Y_k, X_j),$$

and N_0 denotes the ambient noise power of the network environment. Note that the transmission power $P_{r,j}^p$ of receiver j causes no interference to itself, since we adopt self-interference cancellation techniques.

Similarly, for the secondary network,

$$\mathrm{SINR}_{ij}^s = \frac{P_{t,i}^s l(Y_i, Y_j)}{N_0 + I_{ps} + I_{ss}}, \tag{2}$$

where

$$I_{ss} = \sum_{k \in \mathcal{T}^s \setminus \{i\}} P_{t,k}^s l(Y_k, Y_j) + \sum_{k \in \mathcal{R}^s \setminus \{j\}} P_{r,k}^s l(Y_k, Y_j),$$

$$I_{ps} = \sum_{k\in\mathcal{T}^p} P^p_{t,k} l(X_k, Y_j) + \sum_{k\in\mathcal{R}^p} P^p_{r,k} l(X_k, Y_j),$$

On the other hand, $P^p_{r,j}$ and $P^s_{r,j}$ do interfere with the eavesdroppers. When node i is transmitting messages, we give the SINR at eavesdropper e for the primary network as follows (the SINR at e for the secondary network can be easily extended from equation (3)),

$$\text{SINR}^p_{ie} = \frac{P^p_{t,i} l(X_i, Z_e)}{N_0 + I_{pe} + I_{se}}, \tag{3}$$

where

$$I_{pe} = \sum_{k\in\mathcal{T}^p\setminus\{i\}} P^p_{t,k} l(X_k, Z_e) + \sum_{k\in\mathcal{R}^p} P^p_{r,k} l(X_k, Z_e),$$
$$I_{se} = \sum_{k\in\mathcal{T}^s} P^s_{t,k} l(Y_k, Z_e) + \sum_{k\in\mathcal{R}^s} P^s_{r,k} l(Y_k, Z_e).$$

2.4 Performance Metrics

Definition 1. Secrecy Throughput Per Hop*: In the non-colluding case, we define the per hop secure throughput between any active transmitter-receiver pair as*

$$G_f = \log(1 + SINR_{ij}) - \log(1 + \max_{e\in\mathcal{E}} SINR_{ie}).$$

In the non-colluding case, we define the per hop secure throughput as

$$G_f = \log(1 + SINR_{ij}) - \log(1 + \sum_{e\in\mathcal{E}} SINR_{ie})$$

Definition 2. Feasible Throughput*: Per-node throughput $g(n)$ of the primary network is said to be feasible if there exists a spatial and temporal scheme for scheduling transmissions, such that every primary source can send $g(n)$ b/s to its destination on average.*

Definition 3. Asymptotic Per-node Capacity $\lambda_p(n)$ *of the primary network is said to be $\Theta(g(n))$ if there exist two positive constants c and c' such that*

$$\lim_{n\to\infty} Pr\{\lambda_p(n) = cg(n) \text{ is feasible}\} = 1$$
$$\lim_{n\to\infty} Pr\{\lambda_p(n) = c'g(n) \text{ is feasible}\} < 1$$

Similarly, we can define the asymptotic per-node capacity $\lambda_s(m)$ for the secondary network.

3. INDEPENDENT EAVESDROPPERS

In this section, we investigate the secrecy capacity and delay scaling of the cognitive network when eavesdroppers work in the independent mode. Since secondary users occupy extra radio resources, it seems that the secrecy capacity and delay of either primary network or secondary network may be degraded. However, we show that the secondary network can achieve the same secrecy performance as a standalone network in the order sense, while the performance of the primary network is not affected at all.

First, we give the definition of secure transmission in this section.

Definition 4. *We define a transmission from i to j to be successful and secret if the following conditions hold, for primary network,*

$$SINR^p_{ij} \geq \gamma_p, \forall e \in \mathcal{E}, SINR^p_{ie} \leq \gamma_e$$

Table 1: Notations

Notations	Definitions
n	The total number of primary nodes
m	The total number of secondary nodes
$n \cdot \phi_e(n)$	The total number of eavesdroppers
α	The path loss exponent, $\alpha > 2$
X_i	The position of primary node i
Y_j	The position of secondary node j
Z_e	The position of eavesdropper e
$Rx(\cdot)$	The index of corresponding receiver
R_i	The transmission range of primary network link
r_i	The transmission range of secondary network link
$\mathcal{SPR}()$	The feasible family of secure protocol model
$\mathcal{PH}()$	The feasible family of secure physical model
$\mathcal{D}()$	The feasible family of Operation Rule 1
$\mathcal{H}()$	The feasible family of secure hybrid protocol model
P^p_t	The transmission power of primary nodes
P^s_t	The transmission power of secondary nodes
P^p_r	The artificial noise power of primary nodes
P^s_r	The artificial noise power of secondary nodes
$\mathcal{L}^p$	The set of active primary links
$\mathcal{L}^s$	The set of active secondary links
$\mathcal{L}$	$\mathcal{L}^p \cup \mathcal{L}^s$
$\mathcal{T}$	The set of active transmitters at a given time slot
$\mathcal{R}$	The set of active receivers at a given time slot
$\mathcal{E}$	The set of eavesdroppers
$\lvert\cdot\rvert$	The Euclidean length or the number of elements of a set
$l(X_i, X_j)$	The path loss function $\min\{1, \lvert X_i - X_j\rvert^{-\alpha}\}$
$D(x, r)$	The disk with radius r centered at x.
λ	The per-node secure throughput of legitimate node
D	The delay constraint imposed on the packets
G_f	The per hop secure throughput

for secondary network,

$$SINR^s_{ij} \geq \gamma_s, \forall e \in \mathcal{E}, SINR^s_{ie} \leq \gamma_e$$

where $\gamma_p, \gamma_s\, \gamma_e$ are constants and $\gamma_e < \min\{\gamma_p, \gamma_s\}$.

The first condition in the definition ensures that the receiver can decode the message successfully. The second condition guarantees none of eavesdroppers can decode the message. Given Definition 4, there is a subset of links can be active such that all transmissions over active links are successful and secret. We call such a subset of links a *feasible state*, and denote the set of all feasible states as *feasible family*. We use $\mathcal{PH}(\gamma_p, \gamma_s, \gamma_e)$ to denote the feasible family of the physical model.

Next, for tractability of calculation, we give some constraints on the transmission power and artificial noise generation power of the cognitive network.

Definition 5. Power Assignment Scheme*: We say the whole network adopts* power assignment scheme $\mathcal{A}(b_1\ , b_2)$, *if $P^p_{t,i} = P^p_t = P, P^p_{r,i} = P^p_r = b_1(1 + R_{\max})^\alpha P, P^s_{t,i} = P^s_t = b_2 P, P^s_{r,i} = P^s_r = b_1 b_2 (1 + r_{\max})^\alpha P$, where $R_{\max} = \max\{R_i\}, r_{\max} = \max\{r_j\}$.*

Since the primary nodes and the secondary nodes have different priorities in accessing the radio spectrum, we give them different operation rules to guarantee their transmission opportunities.

Operation Rule 1. Decision model for the primary network*:*

$$\frac{P^p_t l(X_i, X_j)}{N_0 + I_{pp}} \geq \gamma_p + \epsilon,\ \frac{P^p_t}{P^p_r}(1 + R_{\max})^\alpha \leq \gamma_e \tag{4}$$

The feasible family of the primary decision model is denoted by $\mathcal{D}(\gamma_p + \epsilon, \gamma_e)$.

We do not include any influence of the secondary network in the decision model of the primary network because the primary network needs neither to know the existence of the secondary network nor to adopt to the secondary users. However we put an allowance ϵ in the operation rule to leave some margin to act as buffer against transient interference from the secondary users. The power constraints given by

the second equation are used to guarantee secure transmissions.

The objective of the operation rule for the secondary network is that the whole cognitive network complies with the physical model $\mathcal{PH}(\gamma_p, \gamma_s, \gamma_e)$ when the secondary network joins the primary network. The notation $\mathcal{H}$ in the *Operation Rule 2* will be explained later.

Operation Rule 2. Decision model for the secondary network: *Let $\mathcal{L}^p$ and $\mathcal{L}^s$ be the sets of active primary links and active secondary links. If $\mathcal{L}^p \in \mathcal{D}(\gamma_p + \epsilon, \gamma_e)$ and $\mathcal{L}^p \cup \mathcal{L}^s \in \mathcal{H}$, then $\mathcal{L}^p \cup \mathcal{L}^s \in \mathcal{PH}(\gamma_p, \gamma_s, \gamma_e)$.*

3.1 Secure Protocol Model: To Bound The Interference

We first prove the physical feasibility of our operation scheme. We propose a new secure protocol model to bound the interference.

3.1.1 Hybrid Secure Protocol Model

Definition 6. Secure Protocol Model *for primary network: A transmission from i to j is feasible if for any $k \in \mathcal{T}^p \backslash \{i\}$ and $l \in \mathcal{R}^p \backslash \{j\}$,*

$$1 + |X_k - X_j| \geq C_{tp}(1 + |X_i - X_j|), \quad (5)$$

$$1 + |X_l - X_j| \geq C_{rp}(1 + |X_i - X_j|)^2, \quad (6)$$

where C_{tp} and C_{rp} define the guard zone for transmitters and receivers in the primary network, respectively. The corresponding feasible family is denoted as $\mathcal{SPR}(C_{tp}, C_{rp})$. Likewise, we define feasible family $\mathcal{SPR}$ (C_{ts}, C_{rs}) for the secondary network.

We prove that the feasible family in the decision model of the primary network is also feasible in the secure protocol model.

Lemma 1. *If $\mathcal{L}^p \in \mathcal{D}(\gamma_p + \epsilon, \gamma_e)$, there exists constant C_{tp} and C_{rp} such that $\mathcal{L}^p \in \mathcal{SPR}(C_{tp}, C_{rp})$.*

Proof. See Appendix A. □

From Lemma 1, we can see that the secure protocol model is much simpler than the secure physical model. We define a new *Hybrid Secure Protocol Model* $\mathcal{H}$ to act as the decision model for the secondary network.

Definition 7. The Hybrid Secure Protocol Model *with feasible family $\mathcal{H}$: $\forall \mathcal{L} \in \mathcal{H}$, let $\mathcal{L}^p \in \mathcal{SPR}(C_{tp}, C_{rp})$, $\mathcal{L}^s \in \mathcal{SPR}(C_{ts}, C_{rs})$. Furthermore, $\forall (X_i, X_j) \in \mathcal{L}^p$*

$$1 + |Y_k - X_j| \geq C_{tsp}(1 + |X_i - X_j|) \quad \forall k \in \mathcal{T}^s \quad (7)$$

$$1 + |Y_l - X_j| \geq C_{rsp}(1 + |X_i - X_j|)^2 \quad \forall l \in \mathcal{R}^s \quad (8)$$

and $\forall (Y_i, Y_j) \in \mathcal{L}^s$

$$1 + |X_k - Y_j| \geq C_{tps}(1 + |Y_i - Y_j|) \quad \forall k \in \mathcal{T}^p \quad (9)$$

$$1 + |X_l - Y_j| \geq C_{rps}(1 + |Y_i - Y_j|)^2 \quad \forall l \in \mathcal{R}^p \quad (10)$$

where constants $C_{tsp}, C_{rsp}, C_{tps}, C_{rps}$ define the inter-network guard zone as illustrated in Figure 1.

3.1.2 Interference at Primary Nodes

We first bound the interference from the secondary network to the primary network. We start this part with a useful property of the hybrid secure protocol model.

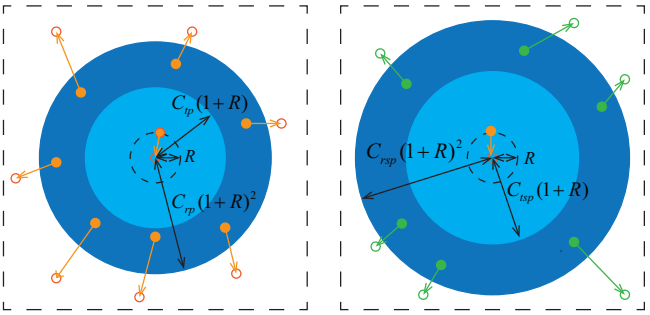

Figure 1: An example of hybrid secure protocol model for a primary transmission pair

Lemma 2. *Given arbitrary $Z_i, Z_j, Z_k, Z_l \in \mathcal{O}$, if (Z_i, Z_j), (Z_k, Z_l) are active links (primary or secondary) and $C_{tx} = 3$, $C_{rx} > 0$ ($x \in \{1, 2\}$ and $C_{tx} \in \{C_{tp}, C_{ts}, C_{tps}, C_{tsp}\}$, $C_{rx} \in \{C_{rp}, C_{rs}, C_{rps}, C_{rsp}\}$), then the $\frac{C_{r1}}{4}(1 + |Z_i - Z_j|)^2$ neighborhood of line segment Z_iZ_j and the $\frac{C_{r2}}{4}(1+|Z_k-Z_l|)^2$ neighborhood of line segment Z_kZ_l are disjoint.*

Proof. See Appendix B. □

From Lemma 2, we know that C_{rx} dominates the representation of the distances between concurrent transmission pairs. Thus we use C_p, C_s, C_{ps}, C_{sp} to represent C_{rp}, C_{rs}, C_{rps}, C_{rsp} for simplicity from now on. We are ready to give the upper bound of interference at primary receivers from the secondary network in Theorem 1 in the following.

Theorem 1. *Under the power assignment $\mathcal{A}(b_1, b_2)$ and the hybrid secure protocol model, if $C_{ps} > C_s$, then for any active primary link $(X_i, X_{Rx(i)})$, the interference at $X_{Rx(i)}$ from the active links of the secondary network is upper-bounded by $b_3(P_t^s + P_r^s)(1 + R_i)^{4-2\alpha}(1 + r_{\min})^{-4}$, where b_3 is a constant.*

Proof. Let $D(X, r)$ be the disk centered at X with radius r. Then, all $D(Y_j, \frac{C_s}{4}(1+r_j)^2), j \in \mathcal{T}^s$ should be mutually disjoint according to Lemma 2. As well, $D(Y_j, \frac{C_{ps}}{4}(1 + r_j)^2), j \in \mathcal{T}^s$ are disjoint with $D(X_{Rx(i)}, \frac{C_{sp}}{4}(1+R_i)^2))$. Because we assume that $C_{ps} > C_s$, then all $D(Y_j, \frac{C_s}{4}(1+r_j)^2)$ and $D(X_{Rx(i)}, \frac{C_{sp}}{4}(1 + R_i)^2))$ are disjoint.
Then we divide the set $\mathcal{T}^s$ into subsets $\mathcal{T}_k^s$, for $1 \leq k \leq \frac{4\sqrt{2n}}{C_{sp}(1+R_i)^2}$ $\mathcal{T}_k^s = \left\{ j \middle| k\frac{C_{sp}(1+R_i)^2}{4} \leq |Y_j - X_{Rx(i)}| \leq (k + 1)\frac{C_{sp}(1+R_i)^2}{4}, j \in \mathcal{T}^s \right\}$.
The radio resource consumed by each transmitter can be bounded by,

$$\frac{1}{3}\pi[\frac{C_s(1 + r_{\min})^2}{4}]^2 \sum_{l=1}^{k} |\mathcal{T}_l^s| \leq \pi[(k + 1)\frac{C_{sp}(1 + R_i)^2}{4}]^2$$

We denote the interference at $X_{Rx(i)}$ that is caused by transmitters in the secondary network as $I_{sp,t}$, and it can be

bounded as follows,

$$
\begin{aligned}
I_{sp,t}(i) &= \sum_{j\in\mathcal{T}^s}\frac{P^s_{t,j}}{(1+|Y_j-X_{Rx(i)}|)^\alpha} \le \sum_k \frac{P^s_t}{|k\frac{C_{sp}(1+R_i)^2}{4}|^\alpha}|\mathcal{T}^s_k| \\
&\le \frac{4^\alpha P^s_t}{C^\alpha_{sp}(1+R_i)^{2\alpha}}\sum_k\frac{1}{k^\alpha}(\sum_{l=1}^{k}|T^s_l|-\sum_{l=1}^{k-1}|T^s_l|) \\
&\le \frac{4^\alpha P^s_t}{C^\alpha_{sp}(1+R_i)^{2\alpha}}\sum_{k=1}^{\infty}[\frac{1}{k^\alpha}-\frac{1}{(k+1)^\alpha}]\sum_{l=1}^{k}|T^s_l| \\
&\le \frac{4^\alpha P^s_t}{C^{\alpha-2}_{sp}C^2_s(1+R_i)^{2\alpha-4}(1+r_{\min})^4}\sum_{k=1}^{\infty}\frac{3\alpha(k+1)^2}{k^{\alpha+1}} \\
&= b_3P^s_t(1+R_i)^{4-2\alpha}(1+r_{\min})^{-4}
\end{aligned}
$$

The interference caused by active receivers can be bounded by similar techniques, $I_{sp,r}(i) = b_3P^s_r(1+R_i)^{4-2\alpha}(1+r_{\min})^{-4}$. And $I_{sp}(i) = I_{sp,t}(i) + I_{sp,r}(i)$. □

3.1.3 Interference at Secondary Nodes

In this part, we bound the interference at secondary receivers from primary nodes and other secondary nodes in Theorem 2 and Theorem 3, respectively.

Theorem 2. *Under the power assignment $\mathcal{A}(b_1,b_2)$ and the hybrid secure protocol model, if $C_{sp} > C_p$ for any active link $(Y_i, Y_{Rx(i)})$, the interference at $Y_{Rx(i)}$ from the active primary links is upper-bounded by $b_4(P^p_t+P^p_r)(1+R_{\min})^{-2\alpha}$, where b_4 is a constant.*

Theorem 3. *Under the power assignment $\mathcal{A}(b_1,b_2)$ and the hybrid secure protocol model, for any active link $(Y_i, Y_{Rx(i)})$, the interference at $Y_{Rx(i)}$ from all other simultaneously active secondary links is upper-bounded by $b_5(P^s_t+P^s_r)(1+r_i)^{4-2\alpha}(1+r_{\min})^{-4}$, where b_5 is a constant.*

The techniques used in the proofs of Theorems 2 and 3 are similar to those in Theorem 1. Thus, we omit the proofs here to avoid redundancy.

3.2 Physical Feasibility of the Hybrid Secure Protocol Model

In this subsection, we show that there exists a power assignment $\mathcal{A}(b_1,b_2)$, making the feasible links under the hybrid secure protocol model also feasible under secure physical model. First, we consider the security of the cognitive network.

Lemma 3. *Under power assignment $\mathcal{A}(b_1,b_2)$, $\mathcal{L}^p \in \mathcal{D}(\gamma_p+\epsilon,\gamma_e)$ and $\mathcal{L}\in\mathcal{H}$, if $b_1 = 1/\gamma_e$, all active links are secure.*

Proof. See Appendix C. □

Lemma 3 tells us that in the independent case, the existence of the secondary network neither relaxes nor tightens the condition for secure transmissions in the primary network. Actually the condition $b_1 \ge 1/\gamma_e$ is implicitly contained in the decision model for the primary network.

Lemma 4. *If $C_{ps} > C_s, \mathcal{L}^p \in \mathcal{D}(\gamma_p+\epsilon,\gamma_e)$ and $\mathcal{L}\in\mathcal{H}$, with the power assignment $\mathcal{A}(1/\gamma_e,b_2)$ such that $b_2 \le b'_3(1+r_{\min})^4(1+r_{\max})^{-\alpha}(1+R_{\min})^{\alpha-4}$ (b'_3 is a constant), all primary links are possible under physical model $\mathcal{PH}(\gamma_p,\gamma_s,\gamma_e)$.*

Proof. See Appendix D. □

Next, we turn to the secondary network.

Lemma 5. *Under power assignment $\mathcal{A}(1/\gamma_e,b_2)$ with $b_2 \ge \max\{b'_4\frac{(1+r_{\max})^\alpha(1+R_{\max})^\alpha}{(1+R_{\min})^{2\alpha}}, b'_5(1+r_{\max})^\alpha\}$ (b'_4, b'_5 are constants), if $\mathcal{L}^p\in\mathcal{D}(\gamma_p+\epsilon,\gamma_e), \mathcal{L}\in\mathcal{H}$ and $C_{sp} > C_p$, all secondary links are feasible under physical model $\mathcal{PH}(\gamma_p,\gamma_s,\gamma_e)$.*

Proof. See Appendix E. □

Then, we are ready to prove the final result.

Theorem 4. *If $\alpha > 4$, $(1+r_{\max})^{2\alpha}(1+R_{\max})^\alpha \le (1+R_{\min})^{3\alpha-4}(1+r_{\min})^4$, there exists a power assignment $\mathcal{A}(b_1,b_2)$, such that if $\mathcal{L}^p\in\mathcal{D}(\gamma_p+\epsilon,\gamma_e)$ and $\mathcal{L}\in\mathcal{H}$, then $\mathcal{L}\in\mathcal{PH}(\gamma_p,\gamma_s,\gamma_e)$.*

Proof. From Lemma 3, we know $b_1 = \frac{1}{\gamma_e}$ is sufficient to ensure the secure transmissions. If we choose $\alpha > 4$, $(1+r_{\max})^{2\alpha}(1+R_{\max})^\alpha \le (1+R_{\min})^{3\alpha-4}(1+r_{\min})^4$ and $C_{ps} > C_s, C_{sp} > C_p$, from Lemma 4 and Lemma 5, there exists a range $[b'_4(1+r_{\max})^\alpha(1+R_{\max})^\alpha(1+R_{\min})^{-2\alpha}, b'_3(1+r_{\min})^4(1+r_{\max})^{-\alpha}(1+R_{\min})^{\alpha-4}]$ for b_2. Hence, we prove that there exists a power assignment scheme $\mathcal{A}(b_1,b_2)$ that if $\mathcal{L}^p\in\mathcal{D}(\gamma_p+\epsilon,\gamma_e)$ and $\mathcal{L}\in\mathcal{H}$, $\mathcal{L}\in\mathcal{PH}(\gamma_p,\gamma_s,\gamma_e)$. □

Theorem 4 is explained and discussed as below. First, the condition $\alpha > 4$, resulting from the blend of extended network model and the secure constraints, means a faster attenuation is needed in our model. Second, we represent the result of Theorem 4 in order forms, i.e., $(1+r_{\max})^{2\alpha}(1+r_{\min})^{-4} = O((1+R_{\min})^{3\alpha-4}(1+R_{\max})^{-\alpha})$. Please recall the strict result if you note the order from result is not sufficient to prove Theorem 4 unless proper constants are chosen. We use the order forms to represent our result just for simplicity. In addition, if the transmission ranges of the cognitive network are homogeneous, i.e., $r = r_{\min} = r_{\max}$ and $R = R_{\min} = R_{\max}$, we only need to consider the condition $(1+r) = O((1+R))$.

3.3 Identifying Transmission Opportunities

The previous subsection proves the physical feasibility of our operation scheme. In this section, we construct a scheduling scheme whose configuration complies with our operation scheme to figure out the transmission opportunities of the secondary nodes.

We say a secondary link is *unconstrained*, if it were in a standalone network.

Definition 8. *Given arbitrary $\mathcal{L}^s_{s.a.}\in\mathcal{SPR}(C_s)$ and arbitrary $\mathcal{L}^p\in\mathcal{SPR}(C_p)$, there exists a unique maximal $\mathcal{L}^s\subset\mathcal{L}^s_{s.a.}$ such that $\mathcal{L}^p\cup\mathcal{L}^s\in\mathcal{H}$. We say a link $(Y_i,Y_{Rx(i)})\in\mathcal{L}^s_{s.a.}$ is* unconstrained *if $(Y_i,Y_{Rx(i)})\in\mathcal{L}^s$.*

The definition of a TDMA scheme is as follows.

Definition 9. *A TDMA scheduling scheme. First, we tessellate the networks into cells such that each cell is contained in a disk of diameter $\rho(n)$ and we denote cell i as V_i. Second, we assign color to each cell, such that cells with the same color can be active simultaneously and transmit to neighbor cells, where two cells V_i, V_j have the same color if $\inf\{|X-Y| : X\in V_i, Y\in V_j\} \ge 4C_p(4\rho^2(n)+6\rho(n)+1)$. Third, we activate different groups of cells with the same constant fraction of time b_6 in a round-robin fashion ($\rho(n) = O(1)$).*

Next, we prove that in the proposed TDMA scheme, the cognitive network complies with our operation scheme. Thus every secondary link could be unconstrained for a constant fraction of time.

Lemma 6. *Using our TDMA scheduling scheme, if* $1 < C_{ps} < C_p < C_{sp} < 2C_p$, $m > n$, $\alpha > 4$, $R = R_{\max} = R_{\min}$, $r = r_{\max} = r_{\min}$ *and* $(1+r) = O((1+R))$, *every secondary node has* b_6 *fraction of time to be unconstrained.*

Proof. See Appendix F. □

3.4 Optimal Performance Scaling

In this subsection, we first present our result on secrecy throughput and delay scaling. Then, we apply our result to various situations.

Theorem 5. *When the cognitive network uses the TDMA scheduling scheme and satisfies the conditions in Lemma 6, and if we assume that the standalone secondary network can achieve per-node secrecy throughput* $\lambda_s^{s.a.}$ *and delay* $D_s^{s.a.}$, *then the secondary network can also achieve per-node secrecy throughput* $\lambda_s^{c.r.} = \Theta(\lambda_s^{s.a.})$ *and delay* $D_s^{c.r.} = \Theta(D_s^{s.a.})$ *in the cognitive network.*

Proof. If the secondary network is standalone, we denote the throughput rate of link (Y_i, Y_j) by $c_{ij}^{s.a.}$ which is determined by the scheduling scheme. If we assume a slotted time, then a deterministic scheduling scheme is characterized by a sequence $(\mathcal{L}_t^{s.a.})_{t=1}^T, \mathcal{L}_t^{s.a.} \in \mathcal{SPR}(C_s)$,

$$c_{ij}^{s.a.} = \lim_{T\to\infty} \frac{W}{T} \sum_{t=1}^{T} 1((Y_i, Y_j) \in \mathcal{L}_t^{s.a.}(t)),$$

where the function $1(\cdot)$ returns 1, if the variable is true; 0, otherwise. We use a random matrix $[\lambda_{sd}]$ to describe the traffic pattern ($\lambda_{sd} = 1$, if s and d is a source-destination pair, and $\lambda_{sd} = 0$ otherwise). We use f_{sd}^{ij}, the average fraction of traffic from s to d that is routed through link (Y_i, Y_j), to describe the routing scheme. Then, for the per-node secrecy throughput $\lambda_s^{s.a.}$, it holds that

$$\lambda_s^{s.a.} \sum_s \sum_d \lambda_{sd} f_{sd}^{ij} \le c_{ij}^{s.a.} \quad 1 \le i, j \le m.$$

Next, we consider the cognitive network. In that situation, the change is that we only allow the unconstraint secondary links to be active. Denote the corresponding throughput rate of link (Y_i, Y_j) as $c_{ij}^{c.r.}$, and according to Lemma 6, $c_{ij}^{c.r.} = b_6 c_{ij}^{s.a.}$. Letting $\lambda_s^{c.r.} = b_6 \lambda_s^{s.a.} = \Theta(\lambda_s^{s.a.})$, it follows that

$$\lambda_s^{c.r.} \sum_s \sum_d \lambda_{sd} f_{sd}^{ij} \le c_{ij}^{c.r.} \quad 1 \le i, j \le m.$$

Therefore, no edge is overloaded and the secrecy throughput $\lambda_s^{c.r.}$ is feasible.

Next, we consider the delay. In the cognitive network, an extra delay is incurred for the secondary network since at each time a secondary node wants to transmit, it may wait until the link is unconstrained. We can easily figure out that the upper-bound of this waiting time is one round of the TDMA scheduler. Thus the delay $D_s = \frac{1}{b_6} D_s^{s.a.} = \Theta(D_s^{s.a.})$. □

With Theorem 5, we can apply the optimal schemes and results from standalone secure networks to secure cognitive networks. The following corollaries are straightforward from [11]. Other results that use centralized TDMA scheduling scheme can also be derived from our conclusion. We do not list them here due to limited space. Note the degradation factor $\log^{-1} n$ in the secrecy capacity of the secondary network in Corollary 2 is caused by the transmission range of the primary network $R = \Theta(\sqrt{\log n}) \neq O(1)$ and can be eliminated by using percolation theory.

Corollary 1. *Assume there are* n *primary nodes,* m *secondary nodes* ($m > n$) *and* $n\phi_e(n)$ *eavesdroppers in the network area with size* $\sqrt{n} \times \sqrt{n}$. *All of them are static and i.i.d according to the uniform distribution. If the traffic pattern is unicast and the eavesdroppers work in the independent mode, the secrecy capacity is* $\lambda_p = \Theta(1/\sqrt{n})$ *for the primary network and* $\Theta(n\lambda_p/m) \le \lambda_s \le \Theta(\sqrt{n}/m)$ *for the secondary network, independent of the density of eavesdroppers.*

Corollary 2. *Assume there are* n *primary nodes,* m *secondary nodes* ($m > n$) *and* $n\phi_e(n)$ *eavesdroppers in the network area with size* $\sqrt{n} \times \sqrt{n}$. *All of them are static and i.i.d according to the uniform distribution. For each primary node,* $n_d - 1$ *nodes are randomly chosen as its destinations and for each secondary node,* $m_d - 1$ *nodes are randomly chosen as its destination. If the eavesdroppers work in the independent mode and* $(1 + \sqrt{\frac{n \log m}{m}}) = o((1 + \sqrt{\log n}))$, *the aggregated multicast secrecy capacity is* $\lambda_p = \Theta(\sqrt{\frac{n}{n_d \log n}} \log^{-\frac{\alpha+4}{2}} n)$ *when* $n_d = O(\frac{n}{\log n})$ *for the primary network and is* $\lambda_s = \Theta(\sqrt{\frac{m}{m_d \log m}}(1+\sqrt{\frac{n \log m}{m}})^{-\alpha-4} \log^{-1} n)$ *for the secondary network when* $m_d = O(\frac{m}{\log m})$.

4. COLLUDING EAVESDROPPERS

In this section, we focus on the secrecy capacity scaling problem in the case where eavesdroppers can collude to decode the message.

Before we begin to calculate the secrecy capacity of cognitive networks in the colluding case, we give some explanations to the differences in assumptions between two cases. The first difference is that in colluding case, we assume the network is a Poisson-distributed random network for that mathematical tractability instead of a uniform distributed random network. It is shown in [15] that random networks converge to Poisson scenarios as n goes to infinity, so the two network models are equivalent in asymptotic analysis.

The second difference is that unlike the general analysis of secure cognitive networks in the previous section, in order to calculate the detailed secrecy capacity, we need to specify a routining scheme for wireless transmission. In the colluding case, we use the *Highway System*.

Definition 10. Highway System*: For the primary network, we divide the network into non-overlapping cells with side length c, where c is a constant. We say a cell is open if there is at least one node in it. Hence, a cell is open with probability* $p = 1 - e^{-c^2}$ *independently based on the Poisson distribution. Denote the number of edges composing the side length of the network area by* $h_p = \frac{\sqrt{n}}{\sqrt{2}c}$ *where c is rounded up such that* h_p *is an integer. According to the Theorem 5 in [2], we can choose c large enough such that there are w.h.p* $\Omega(h_p)$ *paths crossing the network area from left to right, and these can be grouped into disjoint sets of* $\lceil \delta \log h_p \rceil$ *paths, each group crossing a rectangle of size* $h_p \times (\kappa \log h_p - \epsilon_m)$, *for all* $\kappa > 0$, δ *small enough, and a vanishingly small* ϵ_m *so that the side length of each rectangle is an integer. The same is true for vertical paths. We call these backbone paths the Highway System.*

Based on the *Highway System*, we give our packet routing scheme.

Definition 11. A Routing Scheme*: The scheme consists of three phases. The first phase is used to drain information*

to the highway. The second phase is to transport information on the highways. The third phase is to deliver information from the highway to the destination.

Next, based on the routing scheme, we compute the lower bound of the primary transmission rate. First, we give a lemma which is useful throughout this section.

Lemma 7. *If nodes are Poisson-distributed with intensity $\phi(n)$ in the network $\mathcal{O}$, partition the network into disjoint regions with same size $f(n)$, let N_i be the number of nodes in the region i. We have*

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

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

Proof. See Appendix G. □

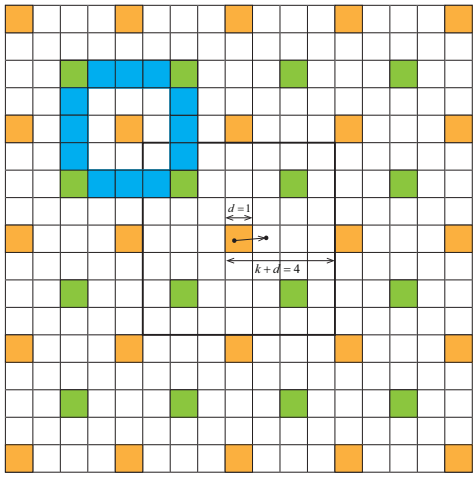

Figure 2: Illustration of network configuration according to the TDMA scheduling scheme. Orange cells contains active primary transmitters. Green cells contains active secondary links.

Lemma 8. *When a primary node is transmitting to a legitimate receiver that is located d cells apart, the minimum rate that the primary node can receive is lower-bounded by $b_7 P_t^p d^{-\alpha}$, where b_7 is a constant.*

Proof. See Appendix H. □

Now, we get the per-hop transmission rate of primary nodes in the cognitive network. Recall Definition 1, if we want to know the per-hop secrecy transmission rate, the total SINR of all the eavesdroppers needs to be calculated.

By the definition of SINR_{ie}^p, there are three parts of the interference at each eavesdropper, namely N_0, I_{pe}, I_{se}, where N_0 is constant. In order to bound I_{pe} and I_{se}, we partition the network into disjoint rings with a same size of $f(n)$. The eavesdropper is at the center of all the rings. Let r_i be the external diameter of the ith ring. Since $f(n) = \pi r_1^2 = \pi(r_i^2 - r_{i-1}^2)$ for any $i > 1$, we have $r_i = \sqrt{i} r_1$ for any $i \ge 1$. We know the primary nodes, secondary nodes and eavesdroppers are Poisson-distributed with parameter $\phi_p(n) = 1, \phi_s(n) = \frac{m}{n}$ and $\phi_e(n)$, respectively. Denote the number of secondary nodes and eavesdroppers in the ith ring as N_{si} and N_{ei}, respectively. By Lemma 7, if $f(n) > 1$ and $\phi_s(n)f(n) = \omega(\log_{e/4} n)$, $\phi_e(n)f(n) = \omega(\log_{e/4} n)$, we can conclude $\frac{1}{2}f(n)\phi_s(n) \le N_{si} \le 2f(n)\phi_s(n)$ and $\frac{1}{2}f(n)\phi_e(n) \le N_{ei} \le 2f(n)\phi_e(n)$.

Lemma 9. *The upper bound of the SINR all eavesdroppers get from a given transmission is $\Theta(\frac{k\phi_e(n)P_t^p}{\phi_s(n)P_r^s} d^{2\alpha})$.*

Proof. See Appendix I. □

Theorem 6. *Considering the cognitive network where primary nodes, secondary nodes and eavesdroppers are independently Poisson-distributed with parameter $\phi_p(n) = 1, \phi_s(n) = \frac{m}{n}$ and $\phi_e(n)$, respectively, the per-node secrecy capacity for the primary network is,*

$$\lambda_f(n) = \begin{cases} \Omega(\frac{1}{\sqrt{n}} \phi_e^{-\frac{2}{\alpha-1}}(n)) & \phi_e(n) = \Omega(\log^2 n) \\ \Omega(\frac{1}{\sqrt{n}} \log^{-\frac{4}{\alpha-1}} n) & \phi_e(n) = O(\log^2 n) \end{cases} \quad (11)$$

Proof. Substituting the results of Lemma 8 and Lemma 9 into Definition 1, the secrecy rate $G_f(d)$ that each cell transmits is

$$\begin{aligned} G_f(d) =& \frac{1}{(k+d)^2}(G(d) - G_e) \\ \ge& \frac{1}{(k+d)^2}(b_7 P_t^p d^{-\alpha} - b_8 P_t^p \frac{k\phi_e(n)}{\phi_s(n)P_r^s} d^{2\alpha}). \end{aligned} \quad (12)$$

In order to get positive secrecy rate, let $\phi_s(n)P_r^s = 2\frac{b_8}{b_7} k\phi_e(n) d^{3\alpha}$. According to Lemma 8, $k^\alpha = \Theta(\phi_s(n)P_r^s)$. Therefore, the secrecy transmission rate that each cell can achieve is $\Omega((\phi_e^{\frac{1}{\alpha-1}}(n) d^{\frac{3\alpha}{\alpha-1}} + d)^{-2} d^{-\alpha})$. In the following, we compute the secrecy capacity for draining/delivery phase and highway phase, respectively.

Draining/Delivery Phase: According to the highway system, the distance between sources and relay on the highway is never larger than $\kappa \log h_p + \sqrt{2}c$. Thus $d = \Theta(\log n), r_1 = \Theta(\log^2 n)$. We assume $\phi_e(n)f(n) = \Omega(\log^2 n) = \omega(\log n)$, which requires $\phi_e(n) = \Omega(\log^{-2} n)$. Under the condition $\phi_e(n) = \Omega(\log^{-2} n)$, we have $\phi_e^{\frac{1}{\alpha-1}}(n)\, d^{\frac{3\alpha}{\alpha-1}} = \omega(d)$, when $\alpha > 2$. Hence, $G_f(d) = \Omega(\phi_e^{-\frac{2}{\alpha-1}}\, d^{-(\alpha+\frac{6\alpha}{\alpha-1})}) = \Omega(\phi_e^{-\frac{2}{\alpha-1}}(n) \log^{-(\alpha+\frac{6\alpha}{\alpha-1})} n)$. Since there are at most $\log n$ primary nodes inside a cell, the per-node secrecy capacity is $\Omega(\phi_e^{-\frac{2}{\alpha-1}}(n) \log^{-(\alpha+\frac{7\alpha-1}{\alpha-1})} n)$.

Highway Phases: In the highway phase, the transmission range between T-R pairs is at most $2\sqrt{2}c$. Hence, $d = \Theta(1), r_1 = \Theta(1)$. Similar to the analysis in draining and delivery phase, we have $\phi_e(n) = \Omega(\log^2 n)$ and $G_f(d) = \Omega(\phi_e^{-\frac{2}{\alpha-1}}(n))$. According to the definition of highway system, each source in the ith slice transmit packets to the ith highway in the same rectangle. Since the density of primary nodes is $\phi_p(n) = 1$ and the size of each slice is $w\sqrt{n}$, which satisfies the conditions given by Lemma 7, we deduce that the maximum number of primary nodes inside each slice is no larger than $2w\sqrt{n}$. Hence a node on a highway must relay traffic for at most $2w\sqrt{n}$ nodes. Therefore, the secrecy capacity of the highway phase is $\Omega(\phi_e^{-\frac{2}{\alpha-1}}(n)\frac{1}{\sqrt{n}})$. If $\phi_e(n) = O(\log^2 n)$, the term R_e will be smaller than in the $\phi_e(n) = \Omega(\log^2 n)$ case, when we keep the other parameters the same, and we can obtain per-node secrecy capacity of $\Omega(\frac{1}{\sqrt{n}} \log^{-\frac{4}{\alpha-1}} n)$.

To summarize the above two cases, we find that the bottleneck of the secrecy capacity is in the highway phase and the per-node secrecy capacity is $\Omega(\phi_e^{-\frac{2}{\alpha-1}}(n)\frac{1}{\sqrt{n}})$. □

Last but not least, we compare our results with the results in single networks [11], as illustrated in Figure 3. *Cooperation* in the legend means that legitimate nodes cooperate to generate artificial noise.

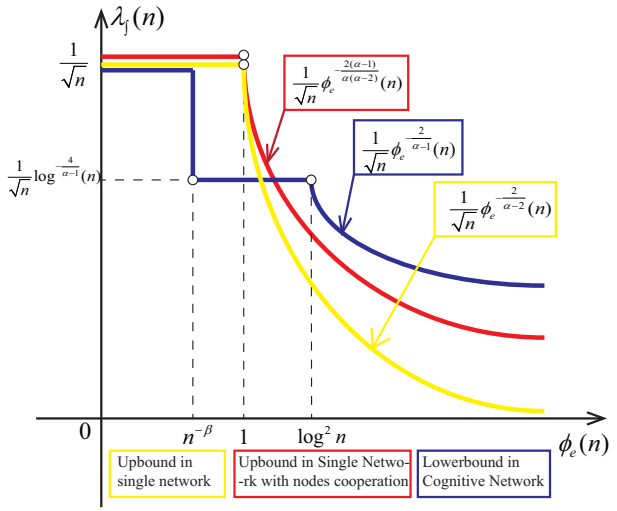

Figure 3: Comparison of our result and the results in single networks

5. CONCLUSION

In this paper, we investigate the impact of introducing secondary users to the network on the secrecy capacity of the primary network. We divide our analysis into two parts according to the two overhearing models of eavesdroppers. In the non-colluding case, we prove that the secondary network can achieve the same performance as standalone networks without adversely affecting the secrecy capacity of the primary network. We also apply our results to various scenarios. In the colluding eavesdroppers case, we calculate the lower bound of the secrecy capacity of the primary network and reveal that the existence of secondary users increases the secrecy capacity of the primary network. Our results may shed insight into the future design of wireless networks, i.e., if we want to enforce the security of primary network, allowing secondary users to co-exist with spectrum sharing is a good security solution. Finally, the secrecy capacity of the secondary network in the colluding case will be studied in a future work.

Acknowledgement

This work is partially supported by NSF China (No. 61325012, 61271219); China Ministry of Education Doctor Program (No. 20130073110025); Shanghai Basic Research Key Project (No.11JC1405100); Shanghai International Cooperation Project: (No. 13510711300)

6. REFERENCES

[1] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," in *IEEE Trans. on Inform. Theory*, vol. 46, no. 2, pp. 388-404, Mar. 2000.

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

[3] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 4, pp. 477-486, Aug. 2002.

[4] M. J. Neely and E. Modiano, "Capacity and Delay Tradeoffs for Ad-Hoc Mobile Networks," *IEEE Trans. Inform. Theory*, vol. 51, no. 6, pp. 1917-1937, 2005.

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

[6] X.-Y. Li, Y. Liu, S. Li, and S. Tang, "Multicast capacity of wireless ad hoc networks under Gaussian channel model," *IEEE/ACM Trans. Netw.*, vol. 18, no. 4, pp. 1145-1157, Jun. 2010.

[7] A. Ozgur, O. Leveque, and D. N. C. Tse, "Hierarchical cooperation achieves optimal capacity scaling in ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3549-3572, Oct. 2007.

[8] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. ACM MobiHoc,* Chicago, IL, USA, Sep. 2010, pp. 21-30.

[9] O. Koyluoglu, E. Koksal and E. Gammel, "On Secrecy Capacity Scaling in Wireless Networks", in *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 3000-3015, 2012.

[10] C. Capar, D. Goeckel, B. Liu, D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. INFOCOM*, pp. 1152-1160, 2012.

[11] J. Zhang, L. Fu, X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," to appear in *IEEE/ACM Trans. Netw.*, 2013.

[12] S.-W. Jeon, N. Devroye, M. Vu, S.-Y. Chung, and V. Tarokh, "Cognitive networks achieve throughput scaling of a homogeneous network," *IEEE Trans. Inf. Theory,* vol. 57, no. 8, pp. 5103-5115, Aug. 2011.

[13] C. Yin, L. Gao, and S. Cui, "Scaling laws for overlaid wireless networks: A cognitive radio network versus a primary network," *IEEE/ACM Trans. Netw.*, vol. 18, no. 4, pp. 1317-1329, Aug. 2010.

[14] W. Huang and X. Wang, "Throughput and Delay Scaling of General Cognitive Networks," in *Proceedings of IEEE INFOCOM*, 2011.

[15] M. Penrose, "Random Geometric Graphs", *Oxford Univ. Press*, Oxford, U.K., 2003.

[16] C. W. Tan, S. Friedland and S. H. Low, "Spectrum Management in Multiuser Cognitive Wireless Networks: Optimality and Algorithm", *IEEE Journal on Selected Areas in Communications*, Vol. 29, No. 2, pp. 421-430, 2011.

APPENDIX

Appendix A: Proof to Lemma 1

Proof. For any active link $(X_i, X_j), (X_k, X_l) \in \mathcal{L}^p$ and $i, k \in \mathcal{T}^p, j, l \in \mathcal{R}^p$, according to the Operation Rule 1,

$$\frac{P_t^p(1+|X_i-X_j|)^{-\alpha}}{P_t^p(1+|X_k-X_j|)^{-\alpha}} \geq \frac{P_t^p l(X_i,X_j)}{N_0+I_{pp}} \geq \gamma_p+\epsilon.$$

Therefore, $1+|X_k-X_j| \geq (\gamma_p+\epsilon)^{\frac{1}{\alpha}}(1+|X_i-X_j|)$ and we can set $C_{tp} \leq (\gamma_p+\epsilon)^{\frac{1}{\alpha}}$. For the second equation of the secure protocol model,

$$\frac{P_t^p(1+|X_i-X_j|)^{-\alpha}}{P_r^p(1+|X_l-X_j|)^{-\alpha}} \geq \frac{P_t^p l(X_i,X_j)}{N_0+I_{pp}} \geq \gamma_p+\epsilon,$$
$$\frac{P_t^p}{P_r^p}(1+|X_i-X_j|)^{\alpha} \leq \frac{P_t^p}{P_r^p}(1+R_{\max})^{\alpha} \leq \gamma_e.$$

Therefore, $1+|X_l-X_j| \geq (\frac{\gamma_p+\epsilon}{\gamma_e})^{\frac{1}{\alpha}}(1+|X_i-X_j|)^2$ and we can set $C_{rp} \leq (\frac{\gamma_p+\epsilon}{\gamma_e})^{\frac{1}{\alpha}}$. □

Appendix B: Proof to Lemma 2

Proof. Let P and Q be two arbitrary points on line segment Z_iZ_j and Z_kZ_l, by applying the triangle inequality and the fact Z_i, P, Z_j and Z_k, Q, Z_l are are collinear, respectively, we have

$$\begin{aligned}&|Z_i-Z_j|+|Z_k-Z_l|+2|P-Q|\\ =&|Z_i-P|+|P-Q|+|Q-Z_l|\\ +&|Z_k-Q|+|P-Q|+|P-Z_j|\\ \geq&|Z_i-Z_l|+|Z_k-Z_j|.\end{aligned}$$

Consider the two following cases.
Case 1: $i,k \in \{\mathcal{T}^p, \mathcal{T}^s\}$ and $j,l \in \{\mathcal{R}^p, \mathcal{R}^s\}$, by the definition of hybrid secure protocol model and the above equation, we have,

$$\begin{aligned}&1+|Z_i-Z_j|+1+|Z_k-Z_l|+2|P-Q|\\ \geq&1+|Z_i-Z_l|+1+|Z_k-Z_j|\\ \geq&C_{t1}(1+|Z_k-Z_l|)+C_{t2}(1+|Z_i-Z_j|)\end{aligned}$$

Simplifying the above equation, we can get $|P-Q| \geq \frac{C_{t1}-1}{2}(1+|Z_k-Z_l|)+\frac{C_{t2}-1}{2}(1+|Z_i-Z_j|)$ which means the first equation of the secure protocol model requires the distance between any two point of a active link is at least $\frac{C_{t1}-1}{2}(1+|Z_k-Z_l|)+\frac{C_{t2}-1}{2}(1+|Z_i-Z_j|)$.
Case 2: $j,k \in \{\mathcal{T}^p, \mathcal{T}^s\}$ and $i,l \in \{\mathcal{R}^p, \mathcal{R}^s\}$, using the conclusion of Case 1 and the second equation of the definition of the secure protocol model, we have,

$$\begin{aligned}&2(1+|Z_i-Z_j|)+2(1+|Z_k-Z_l|)+4|P-Q|\\ \geq&2(1+|Z_k-Z_j|)+1+|Z_i-Z_l|+1+|Z_l-Z_i|\\ \geq&(C_{t1}-1)(1+|Z_i-Z_j|)+(C_{t2}-1)(1+|Z_k-Z_l|)\\ +&1+|Z_i-Z_l|+1+|Z_l-Z_i|\\ \geq&C_{r1}(1+|Z_k-Z_l|)^2+C_{r2}(1+|Z_i-Z_j|)^2+(C_{t1}\\ -&1)(1+|Z_i-Z_j|)+(C_{t2}-1)(1+|Z_k-Z_l|).\end{aligned}$$

By the condition $C_{tx}=3$, we can conclude $|P-Q| \geq \frac{C_{r1}}{4}(1+|Z_k-Z_l|)^2+\frac{C_{r2}}{4}(1+|Z_i-Z_j|)^2$. □

Appendix C: Proof to Lemma 3

Proof. For the primary network, by the definition of SINR_{ie}^p and the condition $b_1=1/\gamma_e$, $\forall e \in \mathcal{E}$, we have

$$\begin{aligned}\mathrm{SINR}_{ie}^p \leq&\frac{P_t^p(1+|X_i-Z_e|)^{-\alpha}}{P_r^p(1+|X_i-X_{Rx(i)}|+|X_i-Z_e|)^{-\alpha}}\\ \leq&\frac{P_t^p}{P_r^p}(1+\frac{R_{\max}}{1+|X_i-Z_e|})^{\alpha} \leq \gamma_e.\end{aligned}$$

Using a similar process, we can prove the security of the secondary links under the condition $b_1=1/\gamma_e$. □

Appendix D: Proof to Lemma 4

Proof. $\mathcal{L}^p \in \mathcal{D}(\gamma_p+\epsilon)$ implies that for any $(X_i, X_{Rx(i)}) \in \mathcal{L}^p$,

$$\frac{P_t^p(1+R_i)^{-\alpha}}{N_0+I_{pp}(i)} \geq \gamma_p+\epsilon. \tag{13}$$

From Theorem 1, we know the upper bound of $I_{sp}(i)$. Combining the upper bound of $I_{sp}(i)$ with the condition $b_2 \leq b_3'(1+r_{\min})^4(1+r_{\max})^{-\alpha}(1+R_{\min})^{\alpha-4}$ and $b_3'=2\gamma_e\epsilon/b_3\gamma_p(\gamma_p+\epsilon)$, we have

$$\begin{aligned}&\frac{P_t^p(1+R_i)^{-\alpha}}{I_{sp}(i)}\\ \geq&\frac{P_t^p(1+R_i)^{-\alpha}}{b_3(P_t^s+P_r^s)(1+R_i)^{4-2\alpha}(1+r_{\min})^{-4}}\\ \geq&\frac{(1+R_i)^{\alpha-4}(1+r_{\max})^{\alpha}}{b_3b_3'[1+b_1(1+r_{\max})^{\alpha}](1+R_{\min})^{\alpha-4}}\\ \geq&\frac{2}{b_1b_3b_3'} \geq \frac{\gamma_p(\gamma_p+\epsilon)}{\epsilon}.\end{aligned} \tag{14}$$

Then, from the equation (13) and (14), we have the assertion. □

Appendix E: Proof to Lemma 5

Proof. From Theorem 2 we know for any $(Y_i, Y_{Rx(i)}) \in \mathcal{H}$, $I_{ps}(i) \leq b_4(P_t^p+P_r^p)(1+R_{\min})^{-2\alpha}$. With $b_2 \geq b_4'(1+r_{\max})^{\alpha}(1+R_{\max})^{\alpha}(1+R_{\min})^{-2\alpha}$ and $b_4'=4b_4\gamma_s/\gamma_e$, it follows that

$$\begin{aligned}\frac{P_t^s(1+r_i)^{-\alpha}}{I_{ps}(i)} \geq&\frac{P_t^s(1+r_i)^{-\alpha}}{b_4(P_t^p+P_r^p)(1+R_{\min})^{-2\alpha}}\\ \geq&\frac{b_2(1+R_{\min})^{2\alpha}}{b_4[1+b_1(1+R_{\max})^{\alpha}](1+r_i)^{\alpha}}\\ \geq&\frac{b_4'(1+r_{\max})^{\alpha}(1+R_{\max})^{\alpha}}{b_4[1+b_1(1+R_{\max})^{\alpha}](1+r_i)^{\alpha}}\\ \geq&\frac{b_4'}{2b_1b_4} \geq 2\gamma_s.\end{aligned} \tag{15}$$

Similarly, from Theorem 3, we know $I_{ss}(i) \leq b_5(P_t^s+P_r^s)(1+r_i)^{4-2\alpha}(1+r_{\min})^{-4}$. In the two cases, $I_{ss}(i) \geq N_0$ and $I_{ss}(i) < N_0$, if $b_2 \geq b_5'(1+r_{\max})^{\alpha}$, we can prove

$$\frac{P_t^s(1+r_i)^{-\alpha}}{N_0+I_{ss}(i)} \geq 2\gamma_s. \tag{16}$$

Case 1: If $I_{ss}(i) \geq N_0$, we have,

$$\begin{aligned}\frac{P_t^s(1+r_i)^{-\alpha}}{N_0+I_{ss}(i)} \geq&\frac{P_t^s(1+r_i)^{-\alpha}}{2I_{ss}(i)}\\ \geq&\frac{P_t^s(1+r_i)^{\alpha-4}(1+r_{\min})^4}{2b_5(P_t^s+P_r^s)}\\ \geq&\frac{(1+r_i)^{\alpha-4}(1+r_{\min})^4}{2b_5[1+b_1(1+r_{\max})^{\alpha}]}\\ \geq&\frac{(1+r_{\min})^{\alpha}}{4b_1b_5(1+r_{\max})^{\alpha}} \geq 2\gamma_s\end{aligned}$$

Case2: If $I_{ss}(i) < N_0$, we have

$$\frac{P_t^s(1+r_i)^{-\alpha}}{N_0+I_{ss}(i)} \geq \frac{P_t^s(1+r_i)^{-\alpha}}{2N_0} \geq \gamma_s$$

Combing equation (15) and (16), we have the assertion. □

Appendix F: Proof to Lemma 6

Proof. For a generic secondary link $(Y_i, Y_{Rx(i)})$. Pick the point X that $|X-Y_i|=2C_p(4\rho^2(n)+6\rho(n)+1)$ and denote the cell X belongs to is V. We claim whenever V is chosen to be active, the link $(Y_i, Y_{Rx(i)})$ is unconstrained. First, we prove that the primary network will not be interfered by Y_i. For any point P belongs to V, we have $|P-X| <$

$\rho(n)$. For any point Q belongs to a neighbor cell of V, we have$|Q-X|<2\rho(n)$, then

$$|Y_i-Q|\geq 2C_p(4\rho^2(n)+6\rho(n)+1)-2\rho(n)$$
$$>C_{sp}(1+2\rho(n))^2\geq C_{sp}(1+|P-Q|)^2.$$

For other simultaneous active cell V'. Similarly, $X'\in V'$ is $|X'-X|>4C_p(4\rho^2(n)+6\rho(n)+1)$, then $|X'-Y_i|\geq |X'-X|-|X-Y_i|>2C_p(4\rho^2(n)+6\rho(n)+1)$ which means that other simultaneous active cells are also not interfered by Y_i. Second, since $(1+r)=O((1+R))$, if $m>n$ and $2C_p>C_{ps}$, $|Q-Y_{Rx(i)}|\geq C_{ps}(1+|Y_i-Y_{Rx(i)}|)^2$ always holds. Thus we have proved our deployment in the scheduling scheme complies with our operation scheme and complete the proof. □

Appendix G: Proof to Lemma 7

Proof. N_i is a Poisson variable, and we denote its expectation as $\lambda=f(n)\phi(n)$. Let $N=\max_i\{N_i\}$, $\forall i$. According to the union bounds and Chernoff bounds, we can get

$$P(N\geq 2\lambda)\leq P(\cup_i(N_i\geq 2\lambda))\leq\sum_i P(N_i\geq 2\lambda)$$
$$\leq\frac{n}{f(n)}e^{-\lambda}(\frac{e\lambda}{2\lambda})^{2\lambda}=\frac{n}{f(n)}(\frac{e}{4})^{f(n)\phi(n)}\to 0,$$

when $f(n)\phi(n)=\omega(\log_{4/e}n)$ and $f(n)=\Omega(1)$.
Similarly, we can show that $\min_i N_i$ is greater than $\frac{1}{2}f(n)\phi(n)$ *w.h.p.* when conditions hold. □

Appendix H: Proof to Lemma 8

Proof. First we compute the interference at the receiver. Different from the situation when there is only one kind of nodes, in cognitive network, the primary nodes will get additional noise from active secondary links. We divide the network into disjoint squares of $(k+d)\times(k+d)$, where k and d together define the concurrent range. We use $(k+d)^2$ TDMA scheduling scheme as in Figure 2. Every cell in each sub-square takes a turn to transmit. Consider a given transmitter-receiver pair, the 8 closest primary transmitters and receivers are located in at distance of at least ck and $c(k+d-1)$ from the receiver. The 16 next closest transmitters and receivers are located in the distance at least $c(2k+d)$ and $c(2k+2d-1)$ away from the receiver and so on. The 4 closest cells which contains active secondary links are at least $\sqrt{2}(\frac{k+d}{2}-1)$, and the 12 next closest cells are at least $\sqrt{2}(\frac{3}{2}(k+d)-1)$ and so on. By extending the sum of the interferences to the whole plane, this can then be bounded as follows (b_7', b_7'' are constants):

$$I(d)\leq\sum_{i=1}^{\infty}8i(P_t^p l(c(i(k+d)-d))+P_r^p l(c(i(k+d)-1)))$$
$$+\sum_{i=1}^{\infty}(8i-4)\phi_s(n)c^2(P_t^s+P_r^s)l(\sqrt{2}c((k+d)(i-\frac{1}{2})$$
$$-1))=b_7'(P_t^p+P_r^p)(kc)^{-\alpha}+b_7''(P_t^s+P_r^s)\phi_s(n)(kc)^{-\alpha}.$$

Next, we want to bound the signal received from the transmitter. We observe first that the distance between the transmitter and the receiver is at most $\sqrt{2}c(d+1)$. Hence, the signal $S(d)$ at the receiver can be bounded by

$$S(d)\geq P_t^p l(\sqrt{2}c(d+1))\geq P_t^p(1+\sqrt{2}c(d+1))^{-\alpha}.$$

Finally, by combing $S(d)$ and $I(d)$, the lower bound of the rate that a primary transmission pair can achieve can be derived as follows (b_7''' is a constant):

$$G(d)=\log\left(1+\frac{S(d)}{N_0+I(d)}\right)$$
$$\geq\log\left(1+\frac{P_t^p(1+\sqrt{2}c(d+1))^{-\alpha}}{N_0+I(d)}\right)$$
$$\geq b_7'''P_t^p(1+\sqrt{2}c(d+1))^{-\alpha}\geq b_7P_t^p d^{-\alpha},$$

when choosing $k=\Theta((P_r^s\phi_s(n))^{\frac{1}{\alpha}})$. □

Appendix I: Proof to Lemma 9

Proof. For a given eavesdropper which is intended to overhear the communication between transmitter u ($u\in\mathcal{T}^p$) and receiver v ($v\in\mathcal{R}^p$), the previous work [11] mainly utilizes the artificial noise generated by the receiver v to suppress the SINR at the eavesdropper. In that case, an active T-R pair mutes other transmissions in the vicinity of size $\Theta(d^4)$, where d is the transmission range. In this paper, we mainly focus on utilizing the artificial noise generated by secondary nodes to suppress the SINR of eavesdroppers. Lemma 8 tells us that in the scheduling configuration as Figure 2, the transmission of secondary nodes does not affect that of the primary nodes. We assume there is also no active secondary transmission pairs in the $\Theta(d^4)$ neighborhood of an active primary transmission pair. Again, we partition the network area into disjoint rings with size $f(n)$ where $r_1=\Theta(d^2)$ and in this time the transmitter u is at the center of all the rings. And we categorize all eavesdroppers into two sets. The first set contains the eavesdroppers which are in the first ring. The second set contains others. Denote SINR_{eij} as the SINR received by eavesdropper j in the ith ring, and $\mathcal{E}_i$ as the set of eavesdroppers located in the ith ring. Taking the summation of the SINR received by all the eavesdroppers, we have, $\mathrm{SINR}_e\leq\sum_{j\in\mathcal{E}_1}\mathrm{SINR}_{e1j}+\sum_{i=2}^{+\infty}\sum_{j\in\mathcal{E}_i}\mathrm{SINR}_{eij}$. We denote $\mathcal{R}^{s*}=\{v|\ X_v\in D(X_u,r_2)-D(X_u,r_1), v\in\mathcal{R}^s\}$. For $v,v*\in\mathcal{R}^{s*}, e\in\mathcal{E}_1$, $l(X_{v*},X_e)=\min\{l(X_v,X_e)\}$, we have

$$\mathrm{SINR}_{e1j}\leq\frac{P_t^p l(X_u,X_e)}{\sum_{v\in\mathcal{R}^{s*}}P_r^s l(X_v,X_e)}\leq\frac{2b_8'P_t^p l(X_u,X_e)}{\phi_s(n)f(n)P_r^s l(X_{v*},X_e)}$$
$$\leq\frac{2b_8'P_t^p}{\phi_s(n)f(n)P_r^s}(1+|X_{v*}-X_u|)^{\alpha}$$
$$\leq\frac{2b_8'P_t^p}{\phi_s(n)f(n)P_r^s}(1+\sqrt{2}r_1)^{\alpha},$$

where $b_8'=\Theta(k+d)=\Theta(k)$ is the reciprocal of the ratio of active secondary regions and represents the effect of mute regions of other transmitters. The the second term suffers the same affection,

$$\mathrm{SINR}_{eij}\leq\frac{b_8'P_t^p r_{i-1}^{-\alpha}}{\frac{1}{2}\phi_s(n)f(n)P_r^s r_1^{-\alpha}}\leq\frac{2b_8'P_t^p}{\phi_s(n)f(n)P_r^s}(i-1)^{-\frac{\alpha}{2}}.$$

So the total SINR can be bounded by,

$$\mathrm{SINR}_e\leq 2f(n)\phi_e(n)\frac{2b_8'P_t^p}{\phi_s(n)f(n)P_r^s}(1+\sqrt{2}r_1)^{\alpha}$$
$$+\sum_{i=2}^{+\infty}2f(n)\phi_e(n)\frac{2b_8'P_t^p}{\phi_s(n)f(n)P_r^s}(i-1)^{-\frac{\alpha}{2}}$$
$$=\frac{4b_8'\phi_e(n)P_t^p}{\phi_s(n)P_r^s}((1+\sqrt{2}r_1)^{\alpha}+\sum_{i=1}^{+\infty}i^{-\frac{\alpha}{2}}).$$

□