Optimal Secrecy Capacity-Delay Tradeoff in Large-Scale Mobile Cognitive Networks

Yitao Chen[*]

Shanghai Jiao Tong University
albrechtdirac@gmail.com

Abstract

In this paper, we study the impact of information-theoretic secrecy constraint on the capacity delay tradeoff of mobile cognitive ad hoc networks with overlapping n primary nodes, m secondary nodes and n^v static eavesdroppers in a $\sqrt{n} \times \sqrt{n}$ network area. We first propose a simple and extendable decision model, i.e., the hybrid secrecy protocol model, for the secondary nodes to exploit spatial gap among primary transmissions for frequency reuse. Then, a framework for general secrecy cognitive networks is established based on the secrecy hybrid protocol model to analyze the occurrence of transmission opportunities for secondary nodes. We show that if the primary network operates in a generalized TDMA fashion, or employs a routing scheme such that traffic flows choose relays independently, then the hybrid secrecy protocol model suffice to guide the secondary network to achieve the same throughput and delay scaling as a standalone network without harming the performance of the primary network.

I. Introduction

Though having the advantage of convenience and low cost, wireless networks are vulnerable to attacks such as eavesdropping and jamming due to their broadcast nature. Most of existing solutions are based on cryptographic methods, e.g., RSA public key crypto-system. However, there two major drawbacks of the cryptographic solutions. First, the key distribution can be very costly in terms of both energy consumption and computation/decoding capability because of the rapid growth of the size of today's wireless networks, which makes the traditional cryptographic methods infeasible. Second, the cryptographic schemes essentially guarantees security by imposing hard mathematical problems on the eavesdroppers, whose computational ability are not high enough to solve the problems efficiently. But the eavesdroppers do obtain the data information and the enemy will decode the message with enough time and computational power. Therefore, to avoid the limitations of the cryptographic solutions, we focus on information-theoretic security in this paper, i.e., safety is ensured even though the eavesdroppers have infinite computational and decoding power.

The study of information-theoretic secrecy originates from the seminal works of Shannon [1],Wyner [2], Csiszar and Korner [3], where the secrecy requires the receiver to have better channel than eavesdroppers. Recently, a few schemes are proposed to guarantee the secret communication. Geol and Negi [4] exploit artificial noise to suppress the SNR at the eavesdroppers so as to ensure security. Independence of wireless fading channels are also used to generate noise with cooperation [5] and multiple antennas [6, 7]. While the above mentioned works all focus on proposing various techniques to ensure information-theoretic security, a few papers also investigate the impact of the secrecy constraint on the network capacity and delay. For example, Vasudevan et al.

[*]Student No:5100309877

[8] study the secrecy-capacity tradeoff in large-scale wireless networks and introduce helpers around the transmitters to generate noise to suppress the SNR at the eavesdroppers. Capar et al. [9] propose a new secrecy communication scheme which can tolerate $o(\frac{n}{log\ n})$ eavesdroppers while keeping the network throughput not affected. To transmit a single bit, the authors propose to generate multiple bits and transmit all of them to the desired destinations through different paths. The original bit can be decoded if and only if all of the generated bits are obtained and the authors present a routing/scheduling protocol to make sure that no eavesdropper could get all those bits. A very related work is a recent paper by Zhang et al. [10]. The authors let every receiver generate artificial noise in order to degrade the SNR at the eavesdroppers and study the impact of secrecy constraints on the capacity scaling in static networks. The most related work to us is by Cao et al. [11] in which the capacity and delay tradeoff in MANETS is studied. However, most existing work listed above focus on networks with one kind of node, no work studies the capacity delay tradeoff in cognitive networks. Observing this limitations, we are motivated to investigate the impact of secrecy contraint on the capacity and delay tradeoff in MANETS in cognitive networks.

II. System Model

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

II.1 Legitimate Network

There are two kinds of legitimate node, primary node and secondary node. There are n primary nodes and m secondary nodes in total in the network area. Denote X_i and Y_i the position of primary node and secondary node respectively. Dividing time into constant duration time slots, we adopt the well known i.i.d. mobility model to characterize the drastic topology change of the MANETs. Specifically, the initial position of each legitimate node is equally likely to be any point in the network area. At the beginning of each time slot, every node randomly and uniformly chooses a point i.i.d. in the network area to be its new position. Throughout this paper, we assume a fast mobility model for the legitimate nodes, i.e., only one-hop transmission is allowed in each time slot. Although the i.i.d. mobility is a somewhat oversimplified model, it is widely adopted in the literature due to its mathematical tractability. In addition, i.i.d. mobility can be viewed as the mobility with very large speed and hence we could use this model to see the fundamental impact of mobility on network performance. With the help of mobility, packets could reach the destinations without being relayed for many times, which decreases the traffic load of the network, and larger capacity is thus expected.

We assume that the traffic pattern between legitimate nodes is unicast. Equivalently speaking, source-destination pairs are randomly chosen such that each node is the destination of exactly one source. We denote $\mathcal{T}_p(\mathcal{R}_p)$ and $\mathcal{T}_s(\mathcal{R}_s)$ as the sets of primary nodes and secondary nodes simultaneously transmitting(receiving) at a given time slot. As in [10], we assume each legitimate node is equipped with three antennas. When a legitimate node acts as a receiver, one antenna is used for message reception while the other two are devoted to simultaneous artificial noise generation to suppress the eavesdroppersąŕchannels. The distances between the receive antenna and the other two respective transmit antennas should satisfy a difference of half of the wavelength. The interference can thus be eliminated by invoking the techniques of self-interference cancelation proposed in [12]. Thereby, each receiver will not be interfered by the artificial noise generated by itself.

II.2 Eavesdropper Network

There are n^{ν} eavesdroppers located in the same network area. Denote ε as the set of all the eavesdroppers and Z_e the position of eavesdropper $e \in \varepsilon$. We assume that the number of eavesdroppers is much larger than that of legitimate nodes, i.e.,$\nu > 1$. Therefor, the density of the eavesdroppers $\psi_e = n^{\nu-1}$ is much larger than 1, i.e., $\psi_e = \omega(1)$. Different from legitimate nodes, the eavesdroppers are assumed to be static, i.e., the position of each eavesdropper does not change with time. This is reasonable since the eavesdroppers may be detected easily if they move drastically. More precisely, each eavesdropper independently and uniformly select a point in the network area as its fixed position. The eavesdroppers always keep silent since they may be detected otherwise. Hence, instead of jamming the signal, the eavesdroppers can only overhear messages in our setup. The eavesdroppers have infinite computational capability and thus information-theoretic security is needed. We also assume that both CSI and location information of eavesdroppers are unknown to the legitimate nodes.

II.3 Secure Physical Model

The secure physical model is widely accepted in the literature and we describe it in the following. Denote $P^p_{t,i}(P^s_{t,i})$ the transmission power of node i if $i \in \mathcal{T}^p(\mathcal{T}^s)$. Similarly, denote $P^p_{r,j}(P^s_{r,j})$ the noise generation power of node j if $j \in \mathcal{R}$. The path loss between node i and node j is denoted by $l(X_i, X_j)$ with $l(X_i, X_j) = l(|X_i - X_j|) = min1, |X_i - X_j|^{-\alpha}$. Here, X_i is the position of node i and α is the path loss exponent. We assume that $2 < \alpha < 4$, which is a typical value range for outdoor path loss exponent. When node i is transmitting messages to node j, the signal to interference and noise ratio (SINR) at the receiver node j is given by(both the primary network situation and secondary network situation are listed below):

$$SINR^p_{ij} = \frac{P^p_{t,i} l(X_i, X_j)}{N_0 + I_p + I_s} \tag{1}$$

where

$$I_p = \sum_{k \in \mathcal{T}^p \backslash \{i\}} P^p_{t.k} l(X_k, X_j) + \sum_{k \in \mathcal{R}^p \backslash \{j\}} P^p_{t.k} l(X_k, X_j)$$

$$I_s = \sum_{k \in \mathcal{T}^s} P^s_{t.k} l(Y_k, X_j) + \sum_{k \in \mathcal{R}^s} P^s_{t.k} l(Y_k, X_j)$$

$$SINR^s_{ij} = \frac{P^s_{t,i} l(Y_i, Y_j)}{N_0 + I_p + I_s} \tag{2}$$

where

$$I_s = \sum_{k \in \mathcal{T}^s \backslash \{i\}} P^s_{t.k} l(Y_k, Y_j) + \sum_{k \in \mathcal{R}^s \backslash \{j\}} P^p_{t.k} l(Y_k, Y_j)$$

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

and N_0 denotes the ambient noise power of the network environment. Note that $P^p_{r,j}(P^s_{r,j})$ is not an interference to the receiver, node j in primary(secondary) network, since we adopt self-interference cancelation techniques.

On the other hand, $P^p_{r,j}(P^s_{r,j})$ do interfere with the eavesdroppers and the SINR at the eavesdropper e can be represented by:

$$SINR^p_{ie} = \frac{P^p_{t,i} l(X_i, X_j)}{N_0 + I_p + I_s} \tag{3}$$

where

$$I_p = \sum_{k \in \mathcal{T}^p \backslash \{i\}} P^p_{t.k} l(X_k, X_j) + \sum_{k \in \mathcal{R}^p} P^p_{t.k} l(X_k, X_j)$$

$$I_s = \sum_{k \in \mathcal{T}^s} P^s_{t.k} l(Y_k, X_j) + \sum_{k \in \mathcal{R}^s} P^s_{t.k} l(Y_k, X_j)$$

As in [9, 11], we say a transmission is secret if none of each eavesdropper could decode the messages. Specifically, we define a transmission to be successful and secret if the following conditions hold.

- $SINR_{ij} \geq \gamma_p$(primary network)
- $SINR_{ij} \geq \gamma_s$(secondary network)
- For any eavesdropper $f \in \varepsilon$, $SINR_{ie} \leq \gamma_e$(both primary and secondary network)

Here $\gamma_p, \gamma_s, \gamma_e$ are all positive constants. The first two condition assures that the receiver, node j, can decode the message successfully while the the second condition guarantees that none of each eavesdropper could decode the message.

We assume that the data rate for successful secure transmission is W bit per time slot. We call a couple of nodes a link if they form a transmitter-receiver pair, e.g.,(X_i, X_j). Given a communication (interference) model, in general there is a number of subsets of links that can be active simultaneously. We call such subsets of links together with the corresponding power management and node positions feasible states, and define the set of all feasible states as feasible family [13]. We denote $\mathcal{PH}(\gamma_p, \gamma_e)$ the feasible family of the secure physical model in primary network.

II.4 Operation Rule

The essential differences between cognitive networks and normal ad hoc networks are the operation rules. Though primary and secondary users overlap and share the channel,they are different essentially because of their behavior. In principle, primary nodes are spectrum license holders and have the priority to access the channel. It is followed by two important implications. First, primary nodes may operate at their own will without considering secondary nodes. They may be legacy devices running on legacy protocols, which are fixed and unmanageable. Therefore, the assumptions made about primary networks should be as few and general as possible. Moreover, the secondary network, which is opportunistic in nature, should control its interference to the primary network and prevent deteriorating the performance of primary users. The challenge is that the primary scheduler may not alter its protocol due to the existence of the secondary network, and its decision model could be different from the physical model (1), i.e., the interference term from the secondary network in the denominator is not available. However, in order to leave some margin for secondary nodes, it is necessary for the decision model to operate at an SINR larger than γ_p by an allowance ϵ.

Operation Rule1 :*Decision model for the primary network:* The primary scheduler consider the transmission from X_i to X_j to be feasible if

$$\frac{P^p_{t,i} l(X_i, X_j)}{N_0 + I_p} \geq \gamma_p + \epsilon \tag{4}$$

where

$$I_p = \sum_{k \in \mathcal{T}^p \setminus \{i\}} P^p_{t.k} l(X_k, X_j) + \sum_{k \in \mathcal{R}^p \setminus \{j\}} P^p_{t.k} l(X_k, X_j)$$

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

Then, as the operation rule, secondary nodes should guarantee that the feasible state under the decision model $\mathcal{D}$ above should be indeed feasible under the physical model.

Operation Rule2 :*Decision model for the secondary network:* Let $\mathcal{S}^p$ and $\mathcal{S}^s$ be the sets of active primary links and active secondary links. If $\mathcal{S}^p \in \mathcal{D}(\gamma_p + \epsilon)$, then $\mathcal{S}^p \cup \mathcal{S}^s \in \mathcal{SPH}(\gamma_p, \gamma_s)$, *w.h.p*

II.5 Definition of Performance Metrics

Definition 1 :*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 by operating the primary network in a multihop fashion and buffering at intermediate nodes when awaiting transmission opportunities, every primary source can send $g(n)$ b/s to its destination on average.

Definition 2 :*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

$$lim_{n\to\infty} Pr\{\lambda_p(n) = cg(n) \; is \; feasible\} = 1$$

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

Similarly, we can define the asymptotic per-node capacity for the secondary network.

III. Overview of Idea and Solution

The key issue that we aim to address in this paper is how the cognitive principles, i.e., Operation Rules 1 and 2, may impact network performance, on asymptotic network secrecy capacity and delay.

Clearly this is a nontrivial problem: Operation Rules 1 and 2 have introduced fundamental heterogeneities into the network in the sense that nodes now have different levels of priority. Such heterogeneities are exactly the most essential idea of how cognitive networks operate. However, though the two operation rules are ideal de?nitions for cognitive principles, they are not convenient from the perspective of analysis and practice because, despite their simple forms, they actually involve numerous underlying details such as the whole network topology, transmission power, and aggregate interference from both primary network and secondary network and both their transmitter and receiver. Therefore, we introduce the *hybrid secure protocol model*, which loosely speaking is a subset of Operation Rules 1 and 2 in the sense that it is a somewhat ąřstricterąś criterion. The hybrid secrecy protocol model is significantly simpler to analyze because it only relies on the geometry of node positions and conceals other details. To establish the correspondence between the operation rules and the hybrid protocol model is the main mission of Section IV, where we design the protocol parameters and the underlying power assignment schemes. Then, we may use the hybrid secrecy protocol model instead of the operation rules in later analysis of network performance, only at the cost of losing a marginal portion of secondary transmission opportunities due to the slight inequivalence between the two sets of criteria.

The throughput and delay in a network are dependent on the specific scheduling and routing schemes. In Section V, we consider whether there is a class of scheduling or routing schemes to which the cognitive behaviors are benign. In other words, this implies that under the hybrid protocol model, both the primary and secondary networks can achieve the same order of performance as if they are separate without mutual interference. This is especially important for the secondary users because it indicates that though they are inferior in priority, their performance is still guaranteed.

IV. The hybrid secure protocol model

Since we assume the primary network to be a general network that operates according to decision model $\mathcal{D}(\gamma_p + \epsilon)$, it is our starting point.$\mathcal{D}$ is of physical concern and cares about the aggregate interference and SINR, but the following lemma relates it to a simpler pairwise model. This alternative model is known as the *secure protocol model* in literature and often plays the role as interference model. However, here we use it as a tool to characterize the relative position of active primary nodes.

Definition 3 :Secure Protocol Model for primary network: A transmission from X_i to X_j is feasible if for any $k \in \mathcal{T}^p$

$$|X_k - X_i| \geq \Delta_p (1 + |X_i - X_j|)^2 \qquad (5)$$

where Δ_p defines the guard zone for the primary network. The corresponding feasible family is noted as $\mathcal{SPR}(\Delta_p)$. Likewise, we define secure protocol model $\mathcal{SPR}(\Delta_s)$ for the secondary network.

First we need to consider the relation ship between different feasible families.

Lemma1: Under four weak assumptions, $\mathcal{S}^p \in \mathcal{D}(\gamma_p + \epsilon)$ and $\mathcal{S}^p \in \mathcal{SPR}(\Delta_s)$ are equivalent.

Proof: The proof is too long. But the four assumptions are listed below.

(1)There are at least two simultaneously active transmitters. For any point P in the network area, there is at least one active transmitter within the disk $D(P, 2d^*)$, where $d^* = min_{i,j}\left\{|X_i - X_j| i, j \in \mathcal{T}, i \neq j\right\}$

(2)For any transmitter-receiver pair (X_i, X_j), we have $d^* \geq 8(|X_i - X_j| + 1)$.

(3)For the secure physical model, all the transmitters utilize the same transmission power,i.e., $P^p_{t,i} = P^p_t (P^s_{t,i} = P^s_t), \forall i \in \mathcal{T}^p(\mathcal{T}^s)$ and all the receiver utilize the same noise generation power, i.e., $P^p_{r,j} = P^p_r (P^s_{r,j} = P^s_r), \forall j \in \mathcal{R}^P(\mathcal{R}^s)$

(4)For the decision model, $\gamma_p + \epsilon > 2^{3\alpha+1}\gamma_s$

Definition 4 : The The Hybrid Secure Protocol Model with feasible family $\mathcal{H}(\Delta_p, \Delta_{ps}, \Delta sp, \Delta_s) : \forall \mathcal{S} \in \mathcal{H}$, let $S^p = \{(X_i, X_j) \in \mathcal{S}\}$ and $S^s = \{(Y_i, Y_j) \in \mathcal{S}\}$, then $S^p \in \mathcal{SPR}(\Delta_p), S^s \in \mathcal{SPR}(\Delta_s)$. Futhermore, $\forall (X_i, X_j) \in \mathcal{S}^p$

$$|Y_k - X_i| \geq \Delta_{sp}(1 + |X_i - X_j|)^2 \qquad (6)$$

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

$$|X_k - Y_i| \geq \Delta_{ps}(1 + |Y_i - Y_j|)^2 \qquad (7)$$

where Δ_{sp}, Δ_{ps} define internetwork guard zones.

The hybrid protocol model only depends on pairwise distance between transmitters and receivers. Such simplicity will facilitate our analysis in the next section. Moreover, it is compatible with the classic protocol interference model. Thus, rich communication schemes and results based on the protocol model can be easily extended to cognitive networks, as will be shown in Section V.

V. Main Results

Unfortunately, Iąŕm still working on this part. But I can give some intuitions.

V.1 Intuition

- By controlling the transmission power(in other words range) of the secondary nodes with a constructed hybrid protocol model, we can prove the secondary network can achieve the same throughput and delay scaling as a standalone network without harming the performance of the primary network. Since we assume the primary network operates in a generalized TDMA fashion which will give every secondary link at least a constant fraction of time to be active.
- And the capacity-delay tradeoff will not be much worse, if not better, than the result in [11] since the secondary user introduce extra artificial noise into the network and further check the SINR at the eavesdroppers.

References

[1] C. Shannon, "Communication theory of secrecy system," in J. Bell. Syst. Tech, vol. 28, pp. 656-715, 1948.

[2] . Wyner, "The wire-tap channel," in J. Bell. Syst. Tech, vol. 54, no. 8, pp. 1355-1367, Oct. 1975.

[3] . Csiszar and J. Korner, "Broadcast channels with con?dential messages," in IEEE Trans. Information Theory, vol. 24, no. 3, pp. 339-348, July 1978.

[4] . Goel and R. Negi, "Guaranteeing secrecy using arti?cal noise," in IEEE Trans. Wireless Communications, vol. 7, no. 6, pp. 2180-2189, 2008.

[5] . Perron, S. Diggavi, E. Telatar, "On cooperative wireless network secrecy," in Proc. IEEE INFOCOM, Rio de Janeiro, Brazil, Apr. 2009.

[6] . Liu and S. Shamai, "A note on the secrecy capacity of the multiple antenna wiretap channel," in IEEE Trans. Information Theory, vol. 55, no. 6, pp. 2547-2553, June 2009.

[7] . Khist and G.Wornell, "Secure transmission with multiple antennas- part II: the MIMOME wiretap channel," in IEEE Trans. Information Theory, vol. 56, no. 11, pp. 5515-5532, 2010.

[8] . Vasudevan, D. Goeckel, D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in Proc. ACM MobiHoc, Chicago, Illinois, USA, Sept. 2010.

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

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

[11] . Cao, X. Wang, "Optimal Secrecy Capacity-Delay Tradeoff in Large-Scale Mobile Ad Hoc Networks"

[12] . Huang and X. Wang, "Throughput and delay scaling of general cognitive networks," in Proc. IEEE INFOCOM, 2011, pp. 2210ÍC2218.