Collisions for Secrecy in Cooperative Cognitive Radio Networks with Time-Varying Connectivity

Karim Khalil and Eylem Ekici
Department of Electrical and Computer Engineering
Ohio State University, Columbus, Ohio
Email: {khalilk, ekici}@ece.osu.edu

***Abstract*—We study user cooperation in a cognitive radio network with random connectivity and collision channels, where the primary user has secrecy constraints. We characterize secure stable throughput region for multiple packet-level cooperative transmission protocols that incorporate packet relaying and collision generation. Stable throughput region is derived for each protocol and then compared to other protocols, including non-cooperative protocol. We show that a collision generation protocol can always provide gains over the non-cooperative protocol while it is not the case for the relaying protocol. In addition, we show that collision generation protocol may achieve superior performance compared to a protocol that involves both cooperative relaying and collision generation, even if the performance of the latter protocol is superior to the non-cooperative protocol.**

I. Introduction

Networks with different classes of users have become more prominent recently. In particular, cognitive radio networks, in which primary users (PUs) have higher access priority than secondary users (SUs), are envisioned to alleviate the scarcity of the finite wireless spectrum with respect to the surging demand [1]. The main idea is to intelligently reuse the spectrum already allocated only for PUs, subject to constraints on the impact to PUs' performance.

Recently, user cooperation was shown to achieve significant performance gains by capitalizing on the spatial diversity of different users to combat channel impairments such as fading or shadowing [2]. Most of the studied cooperation models employ physical layer techniques such as decode-and-forward or amplify-and-forward [3] relaying, where information-theoretic metrics, such as capacity region and outage probability are considered. In addition, physical layer cooperation was also introduced to improve secrecy, i.e., increasing equivocation rate of the message at certain unintended receivers [4]. Through means of artificial noise generation, secrecy rates of legitimate transmitters can be improved [5], [6].

In more recent years, it was shown that packet (or network) level cooperation can achieve both throughput and delay gains for wireless networks [7]. Stable throughput region is characterized for different cooperative schemes at the network layer. For example, a cooperative scheme in a cognitive radio network based on overheard primary feedback was developed in [8]. In [9], stability region is characterized for a cooperative protocol in which SU relays primary traffic and randomly access the channel during PU's transmissions.

The problem of network control when users have secrecy constraints was recently studied in [10], where optimal cross-layer resource allocation schemes are derived. In this paper, and in contrast to the aforementioned literature, we study performance gains of user cooperation for users with bursty traffic sources and different access classes, where one class of users has access priority but also has secrecy constraints. We consider collision channels with time varying connectivity and focus on the case when users have full knowledge of the channel state information (CSI) at each time slot. In [11], stability region is derived for cognitive radio networks where SU employs a hybrid access protocol with both underlay and interweave modes for channels with time varying connectivity. Users employ CSI knowledge to transmit only at the instances when the channel is connected. In our work, users decide their transmission each time slot based on the states of both the channel to the destination and to the unintended receiver.

Our contributions can be summarized as follows. First, we introduce the secure stable throughput metric at the network level as a performance measure to complement secrecy notions both on the physical layer and at higher layers. Next, we propose three cooperation protocols that employ packet collision generation and relaying as means of secrecy throughput amplification. These protocols differ in the activity of SU during PU's transmission. Specifically, in the collision generation protocol (C), SU transmits dummy packets to cause packet collisions at the eavesdropper but not at the destination, thus improving the secure rate of PU. In the relay-only protocol (R), SU attempts to decode PU's packet to relay them in later time slots. In the third protocol, i.e., relaying and collision generation protocol (RC), SU can either decode PU packets or send dummy packets according to the channel conditions. We characterize the secure stable throughput region of the different suggested protocols and compare their performance to a baseline non-cooperative protocol.

II. System Model

A. Network Setup and Channel Model

In our network model, we consider two source nodes and two receiving nodes as shown in Figure 1. The source nodes are the primary user (PU) and the secondary user (SU), denoted as nodes 1 and 2, respectively. Both users are interested in communicating their messages to a common destination (D), denoted as node 3 (e.g., a base station with

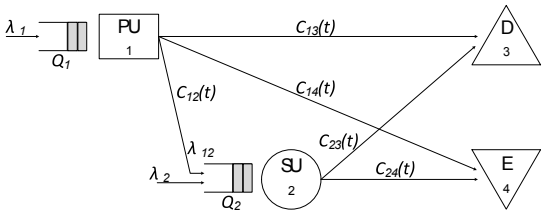

Fig. 1. System Model.

two classes of users in LTE networks). PU's transmission has higher priority than SU's transmission. The second receiver node, denoted as 4, overhears the transmissions intended to node 3. The messages of PU are private and are to be secured from eavesdropping at node 4.

We consider a time slotted system. Packets arrivals at sources are modeled as independent Bernoulli processes with mean λ_1 and λ_2 packets per time slot. We assume that the transmission of one packet occupies exactly one time slot. Each source is equipped with an infinite-sized buffer to store incoming packets. Primary and secondary queues evolves according to the following queue equation

$$Q_i(t+1) = [Q_i(t) - S_i(t)]^+ + A_i(t), i \in \{1, 2\}, \quad (1)$$

where $A_i(t)$ and $S_i(t)$ are the packet arrival and service, respectively, at time slot t. The service processes depend on both the transmission protocol adopted by each node as well as the underlying channel conditions.

In this paper, we consider channels with time-varying connectivity as in [11]. More concretely, in each time slot, each channel can be either connected or disconnected. The connectivity process is represented by a binary variable $C_{ij}(t)$ for the channel between nodes i and j at time slot t, such that $\text{Prob}[C_{ij}(t) = 1] = c_{ij}$. When a channel is connected, a transmitted packet from i to j is decoded with probability q_{ij}. We denote the probability of a successful packet transmission from i to j as $p_{ij} = c_{ij}q_{ij}$. This channel model abstracts the physical layer effects such as shadowing, fading and noise. In addition, we consider collision channels with erasures in which if both users transmit at the same time slot while corresponding channels are connected, packets collide at the receiver and are not decoded.

When there is no cooperation between transmitters, PU has channel access priority. That is, if both users have packets to transmit, PU will transmit while SU has to wait for PU to be idle. Here, to focus our study on channel effects and cooperation gains, we assume that SU can perfectly sense PU transmissions every time slot. When a packet (either primary or secondary) is correctly decoded by node 3, an acknowledgment message is transmitted and the packet is removed from the corresponding queue. Acknowledgments are assumed to be sent on a feedback error-free channel. If packet transmission was not successful, the packet is kept in the corresponding queue for retransmission in a subsequent time-slot. In our model, we assume that SU is a trusted node with respect to PU packets. In other words, we do not consider the confidentiality cost of SU relaying cooperation protocols.

B. Definitions

In our work, we employ the following definition for queue stability. A queue Q_i is said to be stable if there exists a proper limiting distribution for the random variable $Q_i(t)$ [12]. In other words, a queue is stable if the following condition is satisfied.

$$\lim_{t\to\infty} \text{Prob}[Q_i(t) < x] = F(x) \quad \text{and} \quad \lim_{x\to\infty} F(x) = 1. \quad (2)$$

Throughout the paper, we employ Loynes' Theorem [13] which states that if the arrival and service processes of a queue are jointly stationary and the average arrival rate is less than the average service rate, then the queue is stable. If the average arrival rate is larger than the average service rate, the queue is unstable. Note that in our model, the arrival processes are stationary. In addition, we employ stationary transmission protocols and thus service processes can be shown to be stationary as well.

The stable throughput region (or stability region) of the network, denoted as $\mathcal{R}$, is defined as the closure of the arrival rate pairs (λ_1, λ_2) for which all queues are stable. When queues are stable, the packet departure rate at each queue and from the network is equal to the arrival rate. However, for PU packets, a portion of the packets successfully decoded at node 3 may also be decoded by node 4 and thus are not secured. Consequently, we define the *secure throughput* of PU as the rate packets are decoded at 3 (and thus exiting the network) but not at 4, which is generally a function in the arrival rate, the channel conditions as well as the transmission protocol. The *secure stable throughput region* $\mathcal{R}^s$ is thus defined as the closure of the rate pairs $(\lambda_1^s(\lambda_1, \lambda_2), \lambda_2)$ such that $(\lambda_1, \lambda_2) \in \mathcal{R}$, where $\lambda_1^s(\lambda_1, \lambda_2)$ is the secure throughput corresponding to the stable throughput pair $(\lambda_1, \lambda_2) \in \mathcal{R}$. Thus $\mathcal{R}^s \subset \mathcal{R}$ by definition. In this paper, since we assume knowledge of CSI at each time slot, transmitter i will not send a secure packet whenever $C_{i4}(t) = 1$ in a time slot t. Thus, we have $\mathcal{R}^s = \mathcal{R}$ in this case.

III. Results and Stability Analysis

In this section, we characterize the secure stable throughput for the network for both non-cooperative and cooperative transmission protocols. The state of channels $C_{ij}(t)$ are known at transmitter i at every time slot t. In addition, we assume the existence of a 1-bit feedback channel between SU and PU to enable cooperation based on channel conditions. Practically, knowledge of the channel state is possible using pilot signals sent by the receivers each time slot. In particular, knowledge of $C_{14}(t), C_{24}(t)$ is possible if node 4 is actually the receiver node for another transmitters in the network, also sending pilot signals that PU and SU can overhear. In addition, by assuming the knowledge of the eavesdropper channels, the performance derived serves as an upper bound for the setting without this information at the transmitters. We study the scenario with only statistical knowledge of channel conditions in our future work.

Since transmitters have knowledge of CSI at each time slot, secure packets are withheld whenever it is possible for node 4 to decode the transmission in a given time slot. In addition, transmission is withheld if the channel to the destination is disconnected. In the following, we assume that $q_{14} = q_{24} = 1$, that is, we assume that node 4 can decode transmitted packets whenever its channel is connected.

A. Non-cooperative Protocol (NC)

Here, we characterize the secure throughput region when users do not cooperate. This serves as a baseline scenario for the evaluation of the cooperative protocols discussed in the next sections. In the non-cooperative transmission protocol (NC), PU transmits a packet whenever $C_{13}(t) = 1$ and $C_{14}(t) = 0$. SU senses the channel at the beginning of each time slot. When the channel is sensed idle, then it transmits a packet from its queue if $C_{23}(t) = 1$.

Following the independence of the channel processes, the average service rate for the primary queue is then given by

$$\mu_1^{nc} = \bar{c}_{14} p_{13}, \tag{3}$$

where we use the notation $\bar{c} = 1 - c$. For SU transmission, the channel is idle if PU is not transmitting, either because of unfavorable channel conditions, or because of an empty queue. Thus, the average service rate of SU is given by

$$\mu_2^{nc} = p_{23} \left(c_{14} + \bar{c}_{14}\bar{c}_{13} + \bar{c}_{14} c_{13} \text{Prob}[Q_1 = 0]\right) \tag{4}$$

$$= p_{23} \left(1 - \bar{c}_{14} c_{13} \frac{\lambda_1}{\mu_1^{nc}}\right), \tag{5}$$

where we have used $\text{Prob}[Q_1 = 0] = (1 - \frac{\lambda_1}{\mu_1})$ which is true when Q_1 is stable [14]. Thus, the secure stable throughput region $\mathcal{R}^{nc}$ is given by

$$\mathcal{R}^{nc} = \{(\lambda_1, \lambda_2) : \lambda_1 < \bar{c}_{14} p_{13}, \lambda_1 \frac{p_{23}}{q_{13}} + \lambda_2 < p_{23}\}. \tag{6}$$

The region $\mathcal{R}^{nc}$ is convex where the boundary is the intersection of two straight lines since TDMA is the sharing scheme. SU can achieve a strictly positive throughput (up to $p_{23}(1 - \bar{c}_{14} c_{13})$) at the maximum PU stable throughput since PU cannot transmitting in some time slots due to unfavorable channel conditions.

B. Collision Generation Protocol (C)

We introduce a cooperative collision generation (C) protocol, in which SU helps PU to transmit at time slots where transmission was otherwise not possible due to secrecy constraints. In particular, at a given time slot t in which $C_{14}(t) = 1, C_{23}(t) = 0$ and $C_{24}(t) = 1$, simultaneous transmission by both PU and SU causes collision at receiver 4, but not at receiver 3. Here, SU can utilize the 1-bit feedback channel at the beginning of the time slot to notify PU of its ability to jam the eavesdropper channel and provide security for PU transmission. Note that since $C_{23}(t) = 0$, SU cannot transmit its own packets to node 3 at time slot t, even if PU is not transmitting. Our model is different than related information theoretic cooperative jamming models in that we study bursty arrivals where queues can be empty with positive probability.

Under C protocol, the average service rate for PU is

$$\mu_1^c = (\bar{c}_{14} + c_{14}\bar{c}_{23}c_{24}) p_{13}. \tag{7}$$

Note that PU's service rate under this cooperative policy is strictly larger than the service rate in the non-cooperative baseline case.

Since SU can transmit only at the same channel conditions as in NC protocol, the average service rate for SU under C protocol is also given by (4). The only difference is in the term $\text{Prob}[Q_1 = 0]$ since the service rate of PU is different. Thus, we have

$$\mu_2^c = p_{23} \left(1 - \bar{c}_{14} c_{13} \frac{\lambda_1}{\mu_1^c}\right). \tag{8}$$

The secure stable region is then given by

$$\mathcal{R}^c = \{(\lambda_1, \lambda_2) : \lambda_1 < \mu_1^c, \lambda_2 < \mu_2^c(\lambda_1)\}. \tag{9}$$

Since $\mu_1^c > \mu_1^{nc}$, it can be seen that $\mathcal{R}^c$ strictly contains $\mathcal{R}^{nc}$. Thus, by creating collisions at certain time slots, SU allows PU to transmit its own packets more frequently, thus emptying Q_1 faster compared to non-cooperative scenario. This gives SU more idle time slots, hence more chances to transmit own packets.

C. Relaying Protocol (R)

Relaying policies for cooperative cognitive networks were previously proposed in [9], [15]. Here, we adapt the protocol in [9] for collision channels with time varying connectivity and secrecy constraints.

In this cooperative transmission protocol, PU transmits only when $C_{14}(t) = 0$ and either $C_{12}(t) = 1$ or $C_{13}(t) = 1$. When PU transmits, SU attempts to decode the packet transmitted. If the packet is decoded, SU buffers the packet in a new queue (Q_{12}). Then, if PU's packet is correctly decoded at node 3, both PU and SU removes that packet from Q_1 and Q_{12}, respectively, on receiving the ACK signal. If the packet is not decoded correctly at node 3 but correctly decoded at SU, then SU sends an ACK signal to PU and the packet is dropped from Q_1. In this case, PU's packet retransmission becomes the responsibility of SU in the subsequent time slots.

For the time slots in which PU is not transmitting, SU attempts to transmit packets in its queues giving priority to queue Q_{12} if transmission is secure, i.e., $C_{24}(t) = 0$. Otherwise, packets from Q_2 are directly transmitted. We now derive the secure stable throughput region. Let $p_1 = p_{13} + \bar{p}_{13} p_{12}$ and $c_1 = c_{13} + \bar{c}_{13} c_{12}$. The average Q_1 service rate is given by

$$\mu_1^r = \bar{c}_{14} p_1. \tag{10}$$

We now study the stability of queue Q_{12}. The input rate of Q_{12} is the portion of the packets that are dequeued from Q_1 but not correctly decoded at node 3. Given that Q_1 is stable, the departure rate of Q_1 is λ_1. Of the packets departing Q_1, some portion is directly decoded at node 3 and some packets are stored in Q_{12} for later retransmission. The arrival rate of

$$\mu_2^r = p_{23}\left[\bar{c}_{14}\bar{c}_{24}\left(1-\frac{\lambda_{12}}{\mu_{12}^r}\right)\left(\bar{c}_1+c_1\left(1-\frac{\lambda_1}{\mu_1^r}\right)\right)+\bar{c}_{14}c_{24}\left(\bar{c}_1+c_1\left(1-\frac{\lambda_1}{\mu_1^r}\right)\right)+c_{14}\bar{c}_{24}\left(1-\frac{\lambda_{12}}{\mu_{12}^r}\right)+c_{14}c_{24}\right] \quad (14)$$

PU packets into Q_{12} is given by $\lambda_{12}^r = \lambda_1 \frac{\bar{p}_{13}p_{12}}{p_1}$. The service rate of Q_{12} can be derived as follows.

$$\begin{aligned}\mu_{12}^r &= p_{23}\bar{c}_{24}\left(\bar{c}_{12}\bar{c}_{13}+c_1c_{14}+c_1\bar{c}_{14}\left(1-\frac{\lambda_1}{\mu_1^r}\right)\right)\\ &= p_{23}\bar{c}_{24}\left(1-\bar{c}_{14}c_1\frac{\lambda_1}{\mu_1^r}\right). \quad (11)\end{aligned}$$

For Q_{12} to be stable, we need $\lambda_{12} < \mu_{12}^r$. By rearranging terms of (11), we get the following condition

$$\lambda_1 < \tilde{\mu}_1^r = \frac{p_{23}\bar{c}_{24}p_1}{p_{23}\bar{c}_{24}c_1+\bar{p}_{13}p_{12}} = \Phi^r(p_{23}\bar{c}_{24}), \quad (12)$$

where $\Phi^r(x) = \frac{p_1 x}{\bar{p}_{13}p_{12}+c_1 x}$. Depending on the different channels parameters, $\tilde{\mu}_1^r$ can be either greater than or less than μ_1^r. Thus, for the network of queues to be stable, the condition $\lambda_1 < \min\{\mu_1^r, \tilde{\mu}_1^r\}$ must be satisfied.

We now derive the average service rate for Q_2. SU transmits its own packets in this case if PU is not transmitting and $C_{23}(t) = 1$. In addition, if $C_{24}(t) = 0$, then Q_{12} must be empty for SU to transmit packets from Q_2, since Q_{12} has higher transmission priority. Thus, μ_2^r is given by equation (14) at the top of the page, which, after a few algebraic operations, can be reduced to

$$\mu_2^r = p_{23}\left(1-\frac{\lambda_1}{\bar{\mu}_1^r}\right), \quad (14)$$

where $\bar{\mu}_1^r = \Phi^r(p_{23})$. The secure stable throughput region is then given by

$$\mathcal{R}^r = \{(\lambda_1,\lambda_2) : \lambda_1 < \min\{\mu_1^r, \tilde{\mu}_1^r\}, \lambda_2 < \mu_2^r(\lambda_1)\}. \quad (15)$$

We now compare the secure stable throughput region of the cooperative relaying protocol $\mathcal{R}^r$ to that of NC protocol $\mathcal{R}^{nc}$. First, since $\mu_1^r > \mu_1^{nc}$, it can be seen that R protocol improves the (maximum) secure stable throughput of PU over NC protocol if and only if

$$\tilde{\mu}_1^r > \mu_1^{nc}. \quad (16)$$

In addition, stable throughput of SU is improved if

$$\bar{\mu}_1^r > q_{13}. \quad (17)$$

Conditions (16) and (17) imply that, according to different channel parameters, the region $\mathcal{R}^r$ can be generally overlapping with or even a subset of $\mathcal{R}^{nc}$.

D. Relaying and Collision Generation Protocol (RC)

In this section, we introduce a cooperation protocol that incorporates both cooperative relaying and collision generation policies. Similar to R protocol, SU attempts to decode PU packets when PU is transmitting. In addition, SU helps PU secure its transmission when $C_{23}(t) = 0$ and $C_{24}(t) = 1$ by sending dummy packets that collides with PU packets at node 4. When PU is not transmitting, SU transmits packets from Q_{12} if secrecy is satisfied (if $C_{24(t)} = 0$). Otherwise, SU transmits its own packets from Q_2.

Given the description of the cooperative protocol, we derive the secure stable throughput region as follows. The average primary service rate is given by

$$\mu_1^{rc} = \bar{c}_{14}p_1 + c_{14}\bar{c}_{23}c_{24}p_{13}, \quad (18)$$

where the second term represents the probability that PU packets are decoded at node 3 while secured by collisions.

We now turn to study stability of queue Q_{12}. The input packet arrival rate of Q_{12} is the same as that in Section III-C. However, the service rate of Q_{12} is different and is derived as

$$\begin{aligned}\mu_{12}^{rc} &= p_{23}\left(c_{14}\bar{c}_{24}+\bar{c}_{14}\bar{c}_{24}\left(\bar{c}_{12}\bar{c}_{13}+c_1\left(1-\frac{\lambda_1}{\mu_{12}^{rc}}\right)\right)\right)\\ &= p_{23}\bar{c}_{24}\left(1-\bar{c}_{14}c_1\frac{\lambda_1}{\mu_1^{rc}}\right). \quad (19)\end{aligned}$$

For Q_{12} to be stable, we must have $\lambda_{12} < \mu_{12}^{rc}$. We define the following auxiliary function

$$\Phi^{rc}(x) = \frac{p_1 x}{\bar{p}_{13}p_{12}+\frac{p_1\bar{c}_{14}}{\mu_1^{rc}}c_1 x}. \quad (20)$$

By rearranging terms in the condition $\lambda_{12} < \mu_{12}^{rc}$, we get the equivalent condition $\lambda_1 < \tilde{\mu}_1^{rc} = \Phi^{rc}(p_{23}\bar{c}_{24})$. Thus, Q_{12} is stable if $\lambda_1 < \min\{\mu_1^{rc}, \tilde{\mu}_1^{rc}\}$.

For the average service rate of SU, and since collision generation does not change the transmission protocol of SU with respect to R protocol in Section III-C, μ_2^{rc} is given by (14), with μ_1^r replaced by μ_1^{rc}. Thus, we have

$$\mu_2^{rc} = p_{23}\left(1-\frac{\lambda_1}{\bar{\mu}_1^{rc}}\right), \quad (21)$$

where $\bar{\mu}_1^{rc} = \Phi^{rc}(p_{23})$. The stable region is given by

$$\mathcal{S}^{rc} = \{(\lambda_1,\lambda_2) : \lambda_1 < \min\{\mu_1^{rc}, \tilde{\mu}_1^{rc}\}, \lambda_2 < \mu_2^{rc}(\lambda_1)\}. \quad (22)$$

We now discuss the relations between the stable throughput regions achieved by protocols C, R, and RC . First, for the RC protocol, it can be seen that the (maximum) secure stable throughput of PU and stable throughput of SU are improved over NC protocol if and only if $\tilde{\mu}_1^{rc} > \mu_1^{nc}$ and $\bar{\mu}_1^{rc} > q_{13}$. Since $\Phi^{rc}(x) > \Phi^r(x)$ and $\mu_1^{rc} > \mu_1^r$, it follows that $\mathcal{R}^r \subset \mathcal{R}^{rc}$. This also implies that if $\mathcal{R}^{nc} \subset \mathcal{R}^r$, then we have $\mathcal{R}^{nc} \subset \mathcal{R}^{rc}$. More importantly, it can be shown that the stable throughput region of RC protocol is generally overlapping with that of C protocol, i.e., $\mathcal{R}^c \not\subset \mathcal{R}^{rc}$, even if $\mathcal{R}^{nc} \subset \mathcal{R}^{rc}$. We give an example of this case in Section IV.

Finally, we note that the proposed cooperation policies can be modified by letting PU transmit dummy packets when $C_{13}(t) = 0, C_{14}(t) = 1$. In this *primary assisted* cooperation, SU will have more chances to relay the secure PU packets and thus the stable throughput region can be enlarged.

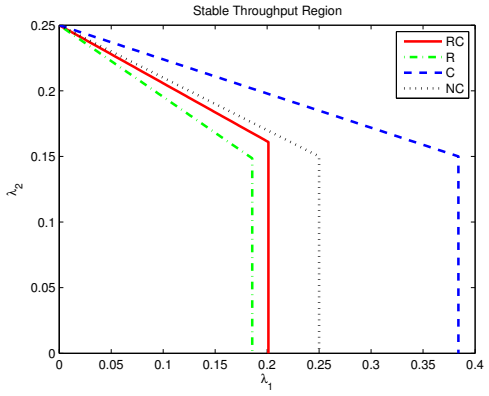

Fig. 2. Stable Throughput Region for case 1 where C protocol achieves superior performance compared to RC protocol.

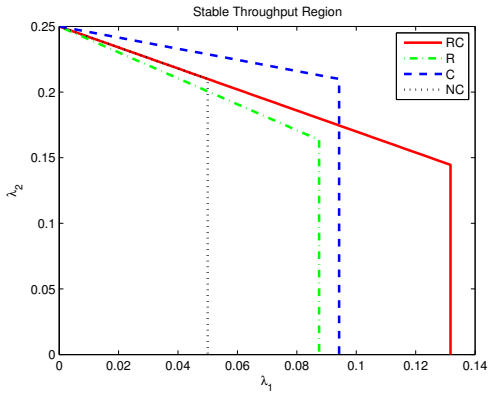

Fig. 3. Stable Throughput Region for case 2 where both protocol C and RC outperforms NC and overlap.

IV. Numerical Results

Here, we present illustrative numerical example to elaborate on the theoretical results derived in Section III. Specifically, to the see how different protocols compare in performance, we plot the stable throughput region for the different proposed protocols proposed at different channel conditions.

First, note that for any given channel statistics, we always have $\mathcal{R}^{nc} \subset \mathcal{R}^{c}$ and $\mathcal{R}^{r} \subset \mathcal{R}^{rc}$. In addition, as p_{12} becomes small, we have $\mathcal{R}^{r} \approx \mathcal{R}^{nc}$ and $\mathcal{R}^{rc} \approx \mathcal{R}^{c}$. Moreover, conditions (16) and (17) determine the overlap between $\mathcal{R}^{nc}$ and $\mathcal{R}^{r}$. If (16) is satisfied but (17) is not, then we have a larger maximum λ_1 for protocol R but less slope (and thus less λ_2 for a given λ_1), and vice versa.

In Figure 2, the stable throughput region is plotted for a case in which the C protocol achieves the largest region. In this example, PU channel parameters are $c_{13} = 0.8, p_{13} = 0.5, c_{14} = 0.5$, SU channel parameters are $c_{23} = 0.33, p_{23} = 0.25, c_{24} = 0.8$ and $p_{12} = 0.25$. Here, since SU channel statistics are worse that PU's, both conditions (16) and (17) are not satisfied.

Finally, Figure 3 shows the more interesting case in which protocol RC is outperforming the non-cooperative protocol, yet overlapping with protocol C. Here, we have $p_{13} = 0.25, c_{14} = 0.8, c_{24} = 0.33$ and rest of parameters are similar to the first case. Here, PU is having less fortunate channel statistics compared to the first case, thus both relaying protocols R and RC can provide large gains. In addition, since SU's channel to node 4 is now less frequently connected, relaying can provide larger gains than collision generation.

V. Conclusion

We studied a fundamental problem in which users with bursty packet arrivals and different access priority share the spectrum under secrecy constraints. Using cooperative protocols at the network level, we characterized the cooperation gain of several cooperation policies in terms of secure stable throughput region. We showed that a simple collision generation protocol may in general achieve a stable throughput region which is not a subset of that achieved by a hybrid relaying and collision generation protocol. In our future work, we will study cooperative protocols in scenarios with unknown instantaneous channel state information.

References

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[2] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *Communications Magazine, IEEE*, vol. 42, no. 10, pp. 74–80, 2004.

[3] J. N. Laneman, D. N. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *Information Theory, IEEE Transactions on*, vol. 50, no. 12, pp. 3062–3080, 2004.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[5] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *Information Theory, IEEE Transactions on*, vol. 54, no. 9, pp. 4005–4019, 2008.

[6] X. He and A. Yener, "Cooperative jamming: The tale of friendly interference for secrecy," in *Securing Wireless Communications at the Physical Layer*. Springer, 2010, pp. 65–88.

[7] B. Rong and A. Ephremides, "Protocol-level cooperation in wireless networks: stable throughput and delay analysis," in *7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009*, pp. 1–10.

[8] N. M. Helal, K. G. Seddik, A. El-Keyi, and T. El Batt, "A feedback-based access scheme for cognitive-relaying networks," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*. IEEE, 2012, pp. 1287–1292.

[9] S. Kompella, G. D. Nguyen, J. E. Wieselthier, and A. Ephremides, "Stable throughput tradeoffs in cognitive shared channels with cooperative relaying," in *Proceedings 2011 IEEE INFOCOM*, pp. 1961–1969.

[10] C. Koksal, O. Ercetin, and Y. Sarikaya, "Control of wireless networks with secrecy," *Networking, IEEE/ACM Transactions on*, vol. 21, no. 1, pp. 324–337, 2013.

[11] J. Jeon, A. Ephremides, M. Codreanu, and M. Latva-aho, "On hybrid access for cognitive radio systems with time-varying connectivity," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, 2013, pp. 819–823.

[12] W. Szpankowski, "Stability conditions for some distributed systems: Buffered random access systems," *Buffered Random Access Systems, Adv. Appl. Probab*, vol. 26, pp. 498–515, 1993.

[13] R. Loynes, "The stability of a queue with non-independent inter-arrival and service times," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 58, no. 03. Cambridge Univ Press, 1962, pp. 497–520.

[14] H. Takagi, *Queueing analysis*. North-Holland Amsterdam, 1991, vol. 1.

[15] O. Simeone, Y. Bar-Ness, and U. Spagnolini, "Stable throughput of cognitive radios with and without relaying capability," *IEEE Transactions on Communications*, vol. 55, no. 12, pp. 2351–2360, 2007.