Distributed Matching Algorithms: Maximizing Secrecy in the Presence of Untrusted Relay

Bakhtiar ALI[1], *Nida ZAMIR*[1], *Soon Xin NG*[2], *Muhammad Fasih Uddin BUTT*[1]

[1]Department of Electrical Engineering, COMSATS Institute of Information Technology Islamabad, Pakistan
[2]Department of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, United Kingdom

bakhtiar_ali@comsats.edu.pk, nida.zamir@comsats.edu.pk, sxn@ecs.soton.ac.uk, fasih@comsats.edu.pk

Submitted September 16, 2016 / Accepted December 14, 2016

Abstract. *In this paper, we propose a secrecy sum-rate maximization based matching algorithm between primary transmitters and secondary cooperative jammers in the presence of an eavesdropper. More explicitly, we consider an untrusted relay scenario, where the relay is a potential eavesdropper. We first show the achievable secrecy regions employing a friendly jammer in a cooperative scenario with employing an untrusted relay. Then, we provide results for the secrecy regions for two cases, one where we consider that there is no direct link between the source and the destination, for the second case we consider that in addition to the relay link we also have a direct link between the source and destination. Furthermore, a friendly jammer helps to send a noise signal during the first phase of the cooperative transmission, for securing the information transmitted from the source. In our matching algorithm, the selected cooperative jammer or the secondary user, is rewarded with the spectrum allocation for a fraction of time slot from the source which is the primary user. The Conventional Distributed Algorithm (CDA) and the Pragmatic Distributed Algorithm (PDA), which were originally designed for maximising the user's sum rate, are modified and adapted for maximizing the secrecy sum-rate for the primary user. Instead of assuming perfect modulation and/or perfect channel coding, we have also investigated our proposed schemes when practical channel coding and modulation schemes are invoked.*

Keywords

Physical layer security, spectrum matching, game theory, spectrum sharing, cognitive radio networks

1. Introduction

The boom in communication technology has brought about revolutionary changes in our lives. This growth along with its benefits has some demerits or challenges since we will be dealing with a huge amount of data coming through billions of connected devices. Current mobile systems would not be able to keep up sufficient provision of providing privacy and security due to the ever-growing number of customers. Enabling technologies like 5G are required for supporting future wireless systems having a large number of devices communicating at ultra high data rates with extreme low latency. 5G technologies such as heterogeneous networks, where lots of devices with different operating systems and protocols will be collaborating or cooperating, will make the problem of privacy and security even more challenging [1–4]. Similarly, Internet of Things (IoT) will be dealing with devices with limited hardware, low complexity and strict energy constraints which presents unique security challenges [5]. In these wireless environments, devices have limited capabilities and are not controlled by a central control station. Hence, the implementation of computationally intensive cryptographic techniques may be challenging. Motivated by these deliberations, substantial research work have been investigating the use of physical layer as a means to develop low-complexity and effective wireless security mechanisms. Such techniques are grouped under the umbrella of Physical Layer Security (PLS) [6]. More explicitly, friendly jamming is a promising PLS technique, which employs cooperating nodes to transmit artificial noise [7–10].

Most of the work in security considers eavesdropper as an outside entity, while authors in [11] presented the motivation for using an untrusted relay for the transmission of information from the source to the destination. They demonstrated that if an untrusted relay is asked to relay information towards the destination, the secrecy rates achieved are higher as compared to the case when the relay is only considered as an eavesdropper. In [12] a link adaptation with untrusted relay assignment framework for cooperative communications is proposed by utilizing arbitrary number of relays for reliable information transfer while ensuring secrecy at the relays. The authors in [13] consider a two-user interference relay channel with the aim to secure the messages from either destinations, as well as the untrusted relay, without the presence of direct link between either of the users. In [14] the authors present the secrecy rates for a dual-hop amplify and forward (AF) multiple-input multiple-output (MIMO) relay network. More specifically, a joint destination based cooperative jamming and joint source, relay and destination precoding based secrecy rate maximization problem is formulated in [14], where simple closed form expressions for asymptotic

DOI: 10.13164/re.2017.0601

secrecy rate in high signal to noise ratio (SNR) regime is also presented. In [15] a destination-assisted jamming for secure communication between a source and a destination via a wireless energy harvesting untrusted relay node is proposed. In [16] the authors defined an achievable secrecy rate region, using random binning at the sources and utilizing the compress and forward relaying strategy with the help of cooperative jamming from both destinations. They also derived a genie-aided outer bound on the secrecy rate region. The drawback of friendly jamming is that there have to be dedicated jamming nodes which are willing to share their resources with the nodes that are not related to the jammer except for the case where the jammer is the destination. In contrast, a two way resource sharing would be more practical where the jammer will assist in jamming the source signal from the eavesdropper and in return will gain access to the channel for transmission of its own information.

A game theoretic based friendly jamming mechanism is proposed in [17], where source-destination communication is secured by a Cooperative Jammer (CJ), which is then compensated by the source's spectrum hence enabling the jammer to transmit its own information towards its destination. In [18] a Stackelberg game for maximizing the source and jammer's utility subject to maximum jamming power at the jammer is presented. They provided a uniform pricing algorithm for maximizing the secrecy rate of the system. In [19] the authors proposed a model where each user can act as a data source as well as a friendly jammer. They formalized a coalition game based cooperation for their proposed model. Furthermore, a "merge and split rules", based distributed algorithm was proposed, where the dual-identity nodes can mutually affect and cooperate into disjoint independent coalitions for maximizing the total secrecy capacity participating users. The authors in [20] proposed a cooperative framework to enhance security in a multiple eavesdropper scenario. A game theoretic incentive mechanism was proposed to stimulate the partners to participate into cooperation.

Most of the work in game theoretic based jamming also considers the eavesdropper as an outside entity [17–20]. Here, we present user cooperation based PLS by employing a CJ to provide security by transmitting an artificial noise towards an untrusted relay. Firstly we provide the achievable secrecy regions for such a scenario for two different cases i.e. with and without the Source (S) - Destination (D) link. Then a user cooperation based game theoretic matching algorithm is presented based on the Conventional Distributed Algorithm (CDA) of [21] for maximizing the secrecy provided by the CJ. The CJ is then compensated for its service by the provision of the source's spectrum for a limited amount of time. The downside of the CDA was that the Primary Users (PU) which in this case are S compete among themselves for matching with the best possible Secondary User (SU) which is the CJ. Another matching algorithm called Pragmatic Distributed Algorithm (PDA) was presented in [22] where this competition was eliminated by introducing another game where the PUs participate in a round robin rotation manner for acquiring the best possible SU/CJ. In that way each of the PUs will gain access to its best possible SU for at least one round. Liang et. al. in [22] also provide results for Adaptive Turbo Trellis Coded Modulation (ATTCM) for her algorithm showing the practicality of the algorithm. For our system we also use PDA based cooperative jamming and compare it with CDA based cooperative jamming using idealistic situation where the system can operate at the capacity of the Continuous-Input Continuous-Output Memoryless Channel (CCMC) and that of the Discrete-Input Continuous-Output Memoryless Channel (DCMC) [23]. However these assume perfect modulation and/or perfect coding. For a more realistic scenario, we involve a realistic Self Concatenated Convolutional Coding (SECCC) [24] based scheme. More explicitly, SECCC is a low complexity, flexible and bandwidth-efficient coding scheme which involves only a single encoder and a single decoder. For higher code rates, puncturing can be used but it has a comparable performance to the Turbo Codes.

In this contribution, we present achievable secrecy regions for the scenario where there is a weak link between the source and the destination, with the aid of an untrusted relay. We show results for the two cases i.e., with and without the direct link between the source and destination[1]. Secondly we provide a secrecy maximization framework where we considered the following cooperative distributed matching algorithms which are based on the adaptation of the PDA and CDA of [22]:

1. Secure Pragmatic Distributed Algorithm (S-PDA) which maximizes the secrecy sum-rate for the participating primary nodes.

2. Secure Conventional Distributed Algorithms (S-CDA) for secrecy maximization for the participating primary nodes.

The centralized matching algorithm is also investigated as a comparison to our proposed schemes.

The organization of the paper is as follows. In Sec. 2, we present the friendly jamming based PLS and provide results for the achievable secrecy regions. Based on the results from Sec. 2, we introduce game theoretic secrecy maximization mechanism to further enhance secrecy of the participating nodes in Sec. 3. Finally, we present the conclusion for our findings in Sec. 4.

2. Friendly Jamming Based PLS

Our network includes a source (S) and destination (D) pair, with an untrusted relay (R) and a friendly cooperative jammer (CJ). We consider an AF based network where the relay amplifies and forwards the composite signal resulting from the mixture of S signal mixed with the noise signal

[1] Part of this work was presented at the 24th European Signal Processing Conference (EUSIPCO 2016), Budapest, Hungary, 29th Aug- 2nd Sept 2016.

from the CJ. The noise signal being transmitted from the CJ is assumed to be known at the destination. We assume that there is a weak direct link between the S and D therefore the transmission by S is assisted by an untrusted relay. We consider two scenarios which are further elaborated below.

2.1 Cooperative Jamming Without S-D Direct Link

For our first scenario we consider that the only link available is the link with the untrusted relay and no S to D direct link is included for communication, as shown in Fig. 1. We consider a single antenna system with half duplex operation. The channel between terminal i and terminal j is considered to be a Rayleigh fading channel denoted by h_{ij} and w represents the additive white Gaussian noise (AWGN) at each receiver input with zero mean and variance of σ_w^2 and unilateral power spectral density $N_0 = 2\sigma_w^2$ watts per hertz. The total transmit power is limited by P.

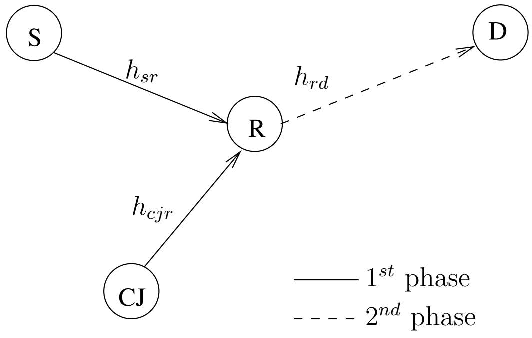


Fig. 1. Cooperative jamming system model (first scenario).

As seen in Fig. 1, S transmits the source signal x_s with power αP and a single selected CJ sends artificial noise η_CJ, with power $(1-\alpha)P$ which is known to D, where $\{0 \le \alpha \le 1\}$ is power distribution variant. Therefore we can write the signal received at R as:

$$y_\text{r} = h_\text{sr}\sqrt{\alpha P}x_\text{s} + h_\text{CJr}\sqrt{(1-\alpha)P}\eta_\text{CJ} + w_\text{r} \tag{1}$$

where w_r is the additive noise with unilateral power spectral density $N_0 = 2\sigma_w^2$ watts per hertz at R. After this, R amplifies and forwards the received signal y_r towards D, therefore the signal received at D is given as

$$y_\text{d} = h_\text{rd}\eta_\text{r} y_\text{r} + w_\text{d} \tag{2}$$

where w_d is the Additive White Gaussian Noise (AWGN) at D and the amplification factor is given by

$$\eta_\text{r} = \sqrt{\frac{P}{\alpha P|h_\text{sr}|^2 + (1-\alpha)P|h_\text{CJr}|^2 + N_0}}. \tag{3}$$

We can calculate the SNR γ_D at D as follows:

$$\gamma_\text{D} = \frac{\alpha\gamma_\text{rd}\gamma_\text{sr}}{\gamma_\text{rd} + \alpha\gamma_\text{rd} + (1-\alpha)\gamma_\text{CJr} + 1} \tag{4}$$

where γ_sr is the SNR for the S to R link, γ_rd is the SNR for the R to D link and γ_CJr is the SNR for the CJ to R links. Similarly, from (1) we can derive the SNR γ_r at R as follows:

$$\gamma_\text{r} = \frac{\alpha\gamma_\text{sr}}{(1-\alpha)\gamma_\text{CJr} + 1}. \tag{5}$$

Consequently, the achievable rates $\bar{R}_\text{D}$ at D and $\bar{R}_\text{r}$ at R will be calculated as

$$\begin{aligned}\bar{R}_\text{D} &= \frac{1}{2}\log(1+\gamma_\text{D}) \\ &= \frac{1}{2}\log\left(1 + \frac{\alpha\gamma_\text{rd}\gamma_\text{sr}}{\gamma_\text{rd} + \alpha\gamma_\text{rd} + (1-\alpha)\gamma_\text{CJr} + 1}\right),\end{aligned} \tag{6}$$

$$\bar{R}_\text{r} = \frac{1}{2}\log(1+\gamma_\text{r}) = \frac{1}{2}\log\left(1 + \frac{\alpha\gamma_\text{sr}}{(1-\alpha)\gamma_\text{CJr} + 1}\right). \tag{7}$$

Finally, the secrecy rate $\bar{R}_\text{s}$ of the system is given by

$$\bar{R}_\text{s} = \bar{R}_\text{D} - \bar{R}_\text{r}. \tag{8}$$

2.2 Cooperative Jamming with S-D Direct Link

For our second scenario we include the S to D direct link for our communication. Again the assumption is that the S to D direct link is weak and no communication is possible through this link without the help from the relay. The message signal is transmitted in two phases, where in the first phase a message is broadcasted by the S in parallel to the noise signal being broadcasted by the CJ and in the second phase which is the relaying phase, the relay amplifies the signal it received during the first phase and forwards it to the D, Fig. 2 shows the system model for our second scenario.

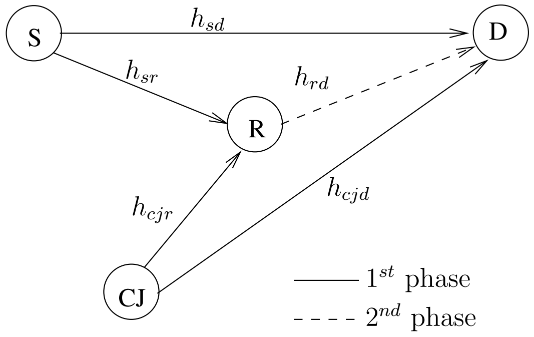


Fig. 2. Cooperative jamming system model (second scenario).

During the 1st phase, S transmits the source signal x_s with power αP and a single selected jammer CJ sends artificial noise η_CJ, with power $(1-\alpha)P$ which is known to the D, where $\{0 \le \alpha \le 1\}$ is the power distribution factor. Therefore the signals received at R and D are, given by

$$y_\text{r} = h_\text{sr}\sqrt{\alpha P}x_\text{s} + h_\text{CJr}\sqrt{(1-\alpha)P}\eta_\text{CJ} + w_\text{r} \tag{9}$$

and

$$y_\text{d}^{(1)} = h_\text{sd}\sqrt{\alpha P}x_\text{s} + h_\text{CJd}\sqrt{(1-\alpha)P}\eta_\text{CJ} + w_\text{d}^{(1)} \tag{10}$$

where w_r and $w_\text{d}^{(1)}$ represent the AWGN at R and D during the 1st phase, respectively. Then, R amplifies and forwards the received signal y_r during the 2nd phase, where the received signal at D can be expressed as

$$y_{\mathrm{d}}^{(2)} = h_{\mathrm{rd}}\eta_{\mathrm{r}}y_{\mathrm{r}} + w_{\mathrm{d}}^{(2)} \tag{11}$$

where $w_{\mathrm{d}}^{(2)}$ represents the AWGN at D during this phase and the amplification factor may be written as

$$\eta_{\mathrm{r}} = \sqrt{\frac{P}{\alpha P|h_{\mathrm{sr}}|^2 + (1-\alpha)P|h_{\mathrm{CJr}}|^2 + N_0}}. \tag{12}$$

By substituting equations (9) and (12) into (11), we get

$$\begin{aligned} y_{\mathrm{d}}^{(2)} &= h_{\mathrm{rd}}\eta_{\mathrm{r}}(h_{\mathrm{sr}}\sqrt{\alpha P}x_{\mathrm{s}} + h_{\mathrm{CJr}}\sqrt{(1-\alpha)P}\eta_{\mathrm{CJ}} + w_{\mathrm{r}}) + w_{\mathrm{d}}^{(2)} \\ &= \eta_{\mathrm{r}}h_{\mathrm{rd}}h_{\mathrm{sr}}\sqrt{\alpha P}x_{\mathrm{s}} + \eta_{\mathrm{r}}h_{\mathrm{rd}}h_{\mathrm{CJr}}\sqrt{(1-\alpha)P}\eta_{\mathrm{CJ}} \\ &+ \eta_{\mathrm{r}}h_{\mathrm{rd}}w_{\mathrm{r}} + w_{\mathrm{d}}^{(2)}. \end{aligned} \tag{13}$$

The composite signal at the destination after removing the known signals can be written as:

$$\begin{aligned} y_{\mathrm{d}} &= h_{\mathrm{sd}}\sqrt{\alpha P}x_{\mathrm{s}} \\ &+ \sqrt{\frac{\alpha}{\alpha P|h_{\mathrm{sr}}|^2 + (1-\alpha)P|h_{\mathrm{CJr}}|^2 + N_0}}Ph_{\mathrm{rd}}h_{\mathrm{sr}}x_{\mathrm{s}} \\ &+ \sqrt{\frac{P}{\alpha P|h_{\mathrm{sr}}|^2 + (1-\alpha)P|h_{\mathrm{CJr}}|^2 + N_0}}h_{\mathrm{rd}}w_{\mathrm{r}} + w_{\mathrm{d}} \end{aligned} \tag{14}$$

where $w_{\mathrm{d}} = w_{\mathrm{d}}^{(1)} + w_{\mathrm{d}}^{(2)}$, we can calculate the SNR at D as:

$$\gamma_{\mathrm{D}} = \frac{\alpha^2\gamma_{\mathrm{sd}}\gamma_{\mathrm{sr}} + \alpha(1-\alpha)\gamma_{\mathrm{CJr}}\gamma_{\mathrm{sd}} + \alpha\gamma_{\mathrm{sd}} + \alpha\gamma_{\mathrm{rd}}\gamma_{\mathrm{sr}}}{\gamma_{\mathrm{rd}} + \alpha\gamma_{\mathrm{rd}} + (1-\alpha)\gamma_{\mathrm{CJr}} + 1} \tag{15}$$

where γ_{sd} is the SNR for the S to D link, γ_{sr} is the SNR for the S to R link, γ_{rd} is the SNR for the R to D link and γ_{CJr} is the SNR for the CJ to R links. Similarly, from (9) we can derive the SNR at R as:

$$\begin{aligned} \gamma_{\mathrm{r}} &= \frac{|\sqrt{\alpha P}h_{\mathrm{sr}}|^2}{|\sqrt{(1-\alpha P)}h_{\mathrm{CJr}}|^2 + 1} \\ &= \frac{\alpha\gamma_{\mathrm{sr}}}{(1-\alpha)\gamma_{\mathrm{CJr}} + 1}. \end{aligned} \tag{16}$$

Consequently, the achievable rates at D and R are given as:

$$\bar{R}_{\mathrm{D}} = \frac{1}{2}\log(1+\gamma_{\mathrm{D}}) \tag{17}$$

and

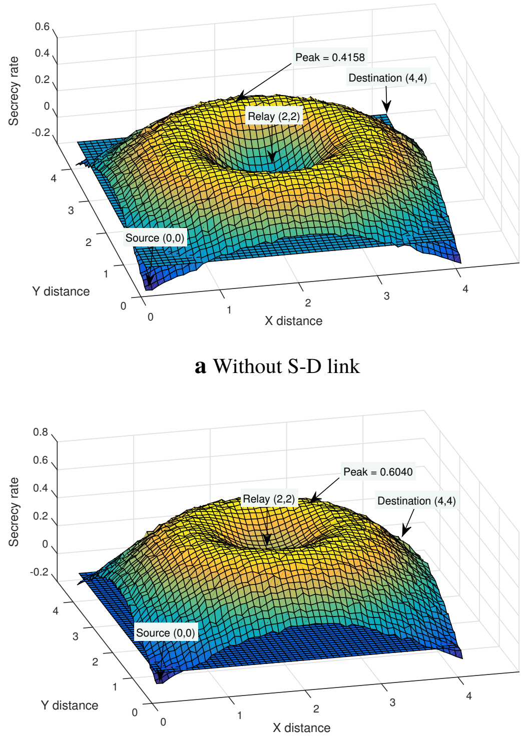
$$\bar{R}_{\mathrm{r}} = \frac{1}{2}\log(1+\gamma_{\mathrm{r}}) = \frac{1}{2}\log\left(1 + \frac{\alpha\gamma_{\mathrm{sr}}}{(1-\alpha)\gamma_{\mathrm{CJr}} + 1}\right). \tag{18}$$

The secrecy rate $\bar{R}_{\mathrm{s}}$ of the system can be calculated as

$$\bar{R}_{\mathrm{s}} = \bar{R}_{\mathrm{D}} - \bar{R}_{\mathrm{r}}. \tag{19}$$

2.3 Secrecy Regions

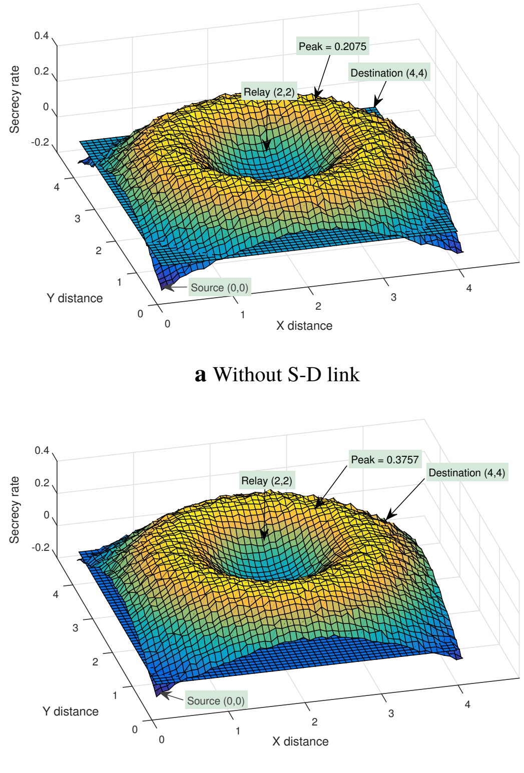
Figures 3, 4 and 5 presents the secrecy rates for both the cases when operating at the CCMC capacity and DCMC capacity as well as when practical adaptive SECCC is employed, respectively. The overall code rate of the SECCC encoder can be calculated as $R_{\mathrm{eq}} = \frac{R_1}{2\times R_2}$. Table 1 shows the different code rates used with their corresponding throughput as well as the mode switching thresholds of SECCC and DCMC.



a Without S-D link

b With S-D link

Fig. 3. Secrecy regions based on the CCMC capacity.



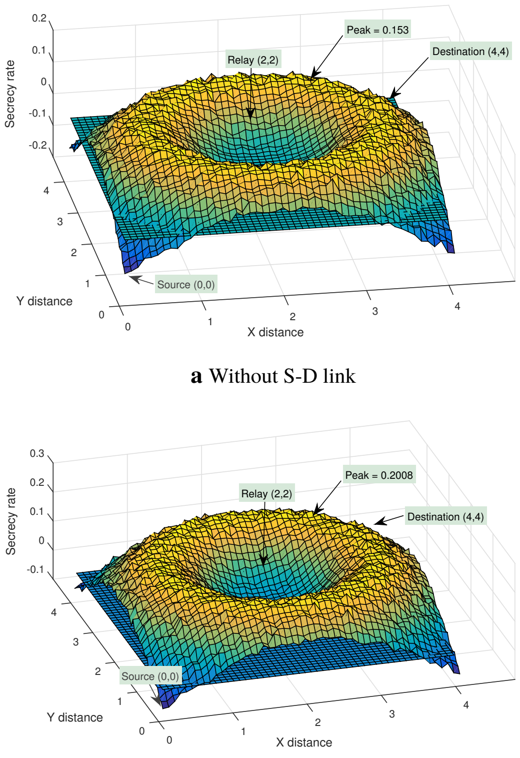
a Without S-D link

b With S-D link

Fig. 4. Secrecy regions based on the DCMC capacity as detailed in Tab. 1.

Mode	R_1	R_2	R_{eq}	Throughput	DCMC SNR	SECCC SNR @ BER = 10^{-5}
4QAM	1/2	1/2	1/2	1	2	5
8QAM	1/2	1/2	1/2	1.5	5	8
16QAM	1/2	1/2	1/2	2	8	11
32QAM	1/2	5/12	3/5	3	12.5	17
64QAM	1/2	3/8	4/6	4	16	21
256QAM	1/2	8/20	5/8	5	20	24

Tab. 1. Adaptive SECCC mode table.



a Without S-D link

b With S-D link

Fig. 5. Secrecy regions based on the adaptive SECCC scheme, as detailed in Tab. 1.

Here we present the secrecy sum-rate in a 3D space where the $\{X, Y\}$ axis represents the coordinates of the jammer, while the secrecy sum-rate is given on the Z axis for a specific jammer on that specific location of the jammer. The X and Y axis range from $\{X, Y\} = \{0, 0\}$ $\{X, Y\} = \{4, 4\}$ where the distance is represented in km in distance. In our simulations we placed S at $\{X, Y\} = \{0, 0\}$, R at $\{X, Y\} = \{2, 2\}$ and D at $\{X, Y\} = \{4, 4\}$. The path gain [25] is given by: $G_{ij} = \left(\frac{d_{\text{sd}}}{d_{ij}}\right)^n$, where d_{ij} is the distance between terminal i and terminal j. Furthermore we have $\bar{h}_{ij} = \sqrt{G_{ij}}h_{ij}$, where h_{ij} is the Rayleigh fading channel coefficients between terminal i and terminal j.

In our simulations we have used $\alpha = 0.9$, while the pathloss exponent is set to $n = 4$. We see an improved secrecy sum-rate when a direct link is considered between source and destination. Secrecy rate improves as the CJ is placed closer to the relay. We can observe a ring shaped region in Fig. 3a around the relay where the secrecy is maximum. If the CJ is placed closer than that ring then we see a degraded performance due to the amplification factor at the relay due to higher jamming interference. The secrecy sum rate is higher if we include the S-D direct link as compared to the case where the S-D link is not considered which can be observed from figures 3, 4 and 5. Figure 3 shows the peak secrecy rates are 0.4158 and 0.6040 for the CJ without S-D and the CJ with S-D scenario when operating at the CCMC capacity which assumes a perfect modulation and a perfect channel code were used. In Fig. 4 the peak secrecy rates are 0.2075 and 0.3757 for the CJ without S-D and the CJ with S-D scenario when operating at the DCMC capacity which assumes a perfect channel code was used. Finally, in Fig. 5 the peak secrecy rates are 0.153 and 0.2008 for the CJ without S-D and the CJ with S-D scenario when a perfect adaptive SECCC scheme is employed.

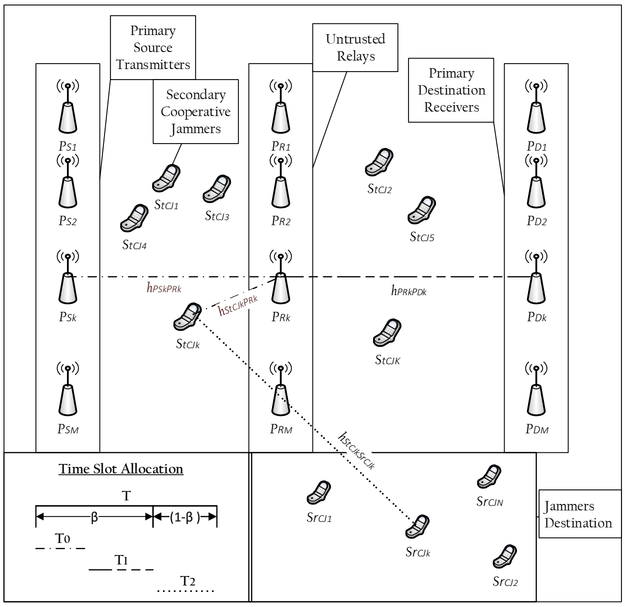


Fig. 6. Cooperative jamming system model.

3. Game Theoretic Secrecy Maximization

We consider an Amplify-and-Forward (AF) based network similar to the model presented in the previous section, but we now consider our network to consist of M pairs of Primary Source transmitters (P_S), Untrusted relays (P_R) and Primary Destination receivers (P_D) ($\{P_{\mathrm{S}_m}, P_{\mathrm{R}_m}, P_{\mathrm{D}_m}\}_{m=1}^{M}$) with the m^th pair having a secrecy rate requirement of greater than zero and K pairs of SU Cooperative Jammer transmitters (St_CJ) and SU Cooperative Jammer receivers (Sr_CJ) ($\{St_{\mathrm{CJ}_k}, Sr_{\mathrm{CJ}_k}\}$, k=1,...,K) with k^th pair having a sum rate requirement of $\bar{R}_{\mathrm{CJ}_{k,\mathrm{req}}}$ in an overlay cognitive radio network environment. Without loss of generality we assume that each $\{P_{\mathrm{S}_m}, P_{\mathrm{D}_m}\}$ pair has its unique untrusted relay P_{R_m} which is placed at the center of the $\{P_{\mathrm{S}_m}, P_{\mathrm{D}_m}\}$ pair. We assume that the S-D link is included for our communication as presented in Sec. 2.2. Each P_S offers a limited duration spectral access as a reward, which is mutually agreed upon, to the St_CJ in exchange for its service to securing its unique $\{P_{\mathrm{S}_m}, P_{\mathrm{D}_m}\}$ pair by transmitting an artificial noise towards its specific P_{R_m}. Our system model can be viewed in Fig. 6 with specific time allocation factors T_0, T_1 and T_2. Furthermore $\beta_{m,k}$ is the time allocation fraction which will be mutually agreed upon by the primary and secondary users based upon the spectrum matching algorithms, discussed in later sections, where $0 < \beta_{m,k} < 1$. During the time interval $T_0 = \beta_{m,k}/2$, P_{S_m} will be broadcasting its signal for P_{R_m} and P_{D_m}, while during the same interval St_{CJ_k} will be sending a noise/jamming signal to block the information leakage at the relay P_{R_m}. The time interval $T_1 = \beta_{m,k}/2$ is only dedicated to P_{R_m} which sends the mixed signal that it has received from S and CJ during interval T_0 to its destination P_{D_m}. Finally during time slot $T_2 = (1 - \beta_{m,k})$, St_{CJ_k} will send its own information towards its destination Sr_{CJ_k}.

The secrecy sum rate for the primary $\{P_{\mathrm{S}_m}, P_{\mathrm{R}_m}, P_{\mathrm{D}_m}\}_{m=1}^{M}$ pair using secondary St_{CJ_k} can be calculated from (17) and (18) as:

$$\bar{R}_{\mathrm{s}_{m,k}} = \bar{R}_{\mathrm{D}_{m,k}} - \bar{R}_{\mathrm{r}_{m,k}}. \tag{20}$$

The achievable rate at m^th D using k^th CJ is given by:

$$\bar{R}_{\mathrm{D}_{m,k}} = \frac{\beta_{m,k}}{2} \log(1 + \gamma_{\mathrm{D}_{m,k}}) \tag{21}$$

where $\gamma_{\mathrm{D}_{m,k}}$ is given as

$$\frac{\alpha^2 \gamma_{\mathrm{sd}_m} \gamma_{\mathrm{sr}_m} + \alpha(1-\alpha)\gamma_{\mathrm{CJr}_{m,k}} \gamma_{\mathrm{sd}_m} + \alpha\gamma_{\mathrm{sd}_m} + \alpha\gamma_{\mathrm{rd}_m}\gamma_{\mathrm{sr}_m}}{\gamma_{\mathrm{rd}_m} + \alpha\gamma_{\mathrm{sr}_m} + (1-\alpha)\gamma_{\mathrm{CJr}_{m,k}} + 1}$$

where $\gamma_{\mathrm{sd}_m} = \gamma_\mathrm{PU}|h_{\mathrm{sd}_m}|^2 d_{\mathrm{sd}_m}^{-n}$, $\gamma_{\mathrm{sr}_m} = \gamma_\mathrm{PU}|h_{\mathrm{sr}_m}|^2 d_{\mathrm{sr}_m}^{-n}$ and $\gamma_{\mathrm{rd}_m} = \gamma_\mathrm{PU}|h_{\mathrm{rd}_m}|^2 d_{\mathrm{rd}_m}^{-n}$ are the SNRs, h_{sd_m}, h_{sr_m} and h_{rd_m} are the Rayleigh fading channel coefficients while d_{sd_m}, d_{sr_m} and d_{rd_m} are the distances between the m^th S-D, S-R and R-D links, respectively. $\gamma_{\mathrm{CJr}_{m,k}} = \gamma_\mathrm{SU}|h_{\mathrm{CJr}_{m,k}}|^2 d_{\mathrm{CJr}_{m,k}}^{-n}$ is the SNR with $h_{\mathrm{CJr}_{m,k}}$ being the Rayleigh fading channel coefficients while $d_{\mathrm{CJr}_{m,k}}$ is the distance between the k^th CJ and m^th R. The achievable rate at m^th R using k^th CJ is given as:

$$\bar{R}_{\mathrm{r}_{m,k}} = \frac{\beta_{m,k}}{2} \log\left(1 + \frac{\alpha\gamma_{\mathrm{sr}_m}}{(1-\alpha)\gamma_{\mathrm{CJr}_{m,k}} + 1}\right). \tag{22}$$

The achievable sum-rate for the secondary $\{St_{\mathrm{CJ}_k}, Sr_{\mathrm{CJ}_k}\}$ pair can be computed as

$$\bar{R}_{\mathrm{CJ}_{m,k}} = (1 - \beta_{m,k}) \log(1 + \gamma_{\mathrm{CJ}_k}) \tag{23}$$

where γ_{CJ_k} is the SNR for $\{St_{\mathrm{CJ}_k}, Sr_{\mathrm{CJ}_k}\}$ pair. Each P_{S_m} has a list of all the St_{CK_k} which can provide a secrecy sum-rate of greater than zero in a descending order, denoted as $PULIST_m$. Similarly each St_{CJ_k} has a list of all the P_{S_m} that can provide a sum-rate greater than or equal to its minimum rate requirement in a descending order, denoted as $SULIST_k$. Based on this system model we present two secrecy maximization algorithms i.e, the Secure CDA and the Secure PDA which will be elaborated further.

3.1 Secure CDA

CDA was proposed in [21] for maximizing the sum-rate for PU. In our case we modified the algorithm to maximize the secrecy sum-rate while SU benefit in terms of limited duration spectrum access. The algorithm as seen in Algorithm 1 starts by the construction of the $PULIST_m$ by each of the PU, which is the set of all the SUs that provide secrecy of greater than the minimum required by the PU. The list is made in the descending order so that the first entry in the list is an SU which provides the highest secrecy as obtained in Sec. 2.2 of all and so on. Similarly each SU will also create its own $SULIST_k$ which is the set of all the PUs that provide a sum-rate of greater or equal to the minimum required in descending order. In the Secure-CDA each PU offers a limited time allocation factor $\beta_{m,k}$ to the first SU in its $PULIST_m$ in exchange for its service to provide secrecy to the PU. Matching will be made if the offerer PU is present in the $SULIST_k$ of the k^th SU. If that PU is not present in the $SULIST_k$, match will not be made and the PU will enhance its time allocation factor for that specific SU by decreasing the time allocation factor by ϵ and the PULIST will be updated accordingly. In this fashion each PU will be making an offer to its desired SU and will try to match with its desired SU. Matching will be broken if any SU which is already matched receives a better offer in terms of its sum-rate from another PU. In that case previous match will be broken and the SU will be matched to the new PU. In this way the algorithm will continue until all the PUs are matched to their desired SUs or until no further matchings are possible.

3.2 Secure PDA

PDA was proposed in [22] also for maximizing the sum-rate for the PU. PDA was better than CDA in terms of the PU sum-rate as it catered for the losses endured by the CDA due to competing primary nodes for acquiring the best SU in terms of secrecy maximization obtained in Sec. 2.2. In Secure-CDA the PUs compete with each other for the acquisition of their desired SU by trying to out-bid their rivals. Due to this competition among the PUs, they end up compromising their secrecy rate. The SUs upon receiving a better

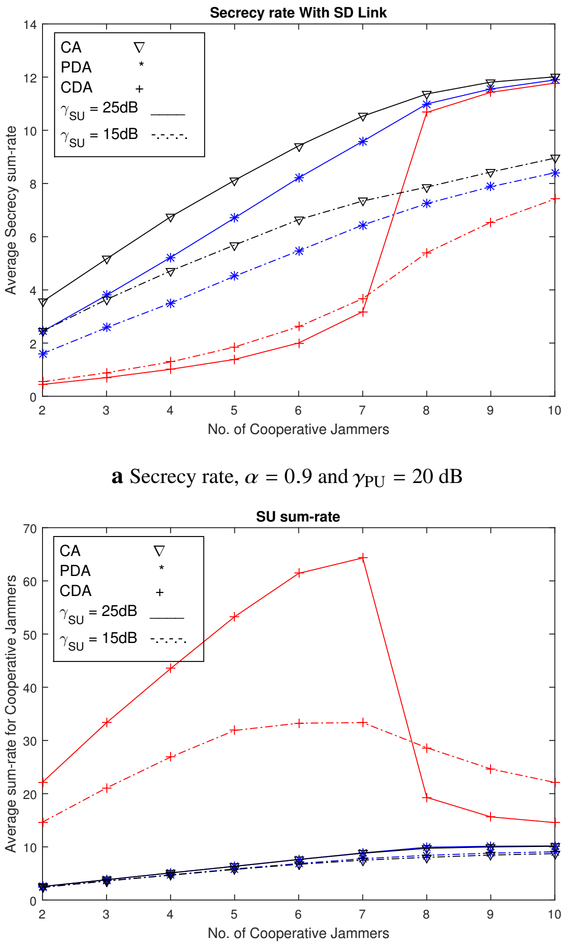
Algorithm 1 Secure CDA

```
Require: $\bar{R}_{\mathrm{CJ}_{m,k}} \geq 1 \wedge 0 < \beta_{m,k} < 1$
Ensure: $\bar{R}_{\mathrm{s}_{m,k}} > 0$
 1: Initialization
     2: Set matchlist for the set of $P_{\mathrm{S}_m}$ to be matched (i.e. ){1, ..., M}.
     3: Set the initial TS allocation to $\beta_{init} = 0.99$, and set the step size of TS increment to $\tau = 0.05$.
     4: Construct $PULIST_m = \{St_{\mathrm{CK}_k} | \bar{R}_{\mathrm{s}_{m,k}} > 0\}$ and $SULIST_k = \{P_{\mathrm{S}_m} | \bar{R}_{\mathrm{CJ}_{m,k}} \geq 1\}$ in descending order, where $m = \{1, \dots, M\}$ and $k = \{1, \dots, K\}$.
     5: Set $j = 1$ for the first transmission.
 6: Do the matching for the $j$th transmission.
     7: $P_{\mathrm{S}_m}$ offers $\beta_{m,k}$ to the first SU in its preference list $St_{\mathrm{CJ}_k}$.
         8: If $P_{\mathrm{S}_m}$ is not in the preference list of $St_{\mathrm{CJ}_k}$ then decrease the TS allocation to $\beta_{m,k} = \beta_{m,k} - \tau$ and update both $PULIST_m$ and $SULIST_k$.
         9: If $P_{\mathrm{S}_m}$ is in the preference list of $St_{\mathrm{CJ}_k}$, then $St_{\mathrm{CJ}_k}$ and $P_{\mathrm{S}_m}$ are matched.
        10: If $St_{\mathrm{CJ}_k}$ is already matched to $P_{S_{curr}}$
        11: If the $P_{\mathrm{S}_m}$ is higher up in the $SULIST_m$ than $P_{S_{curr}}$, then rematch $St_{\mathrm{CJ}_k}$ to $P_{\mathrm{S}_m}$.
        12: Else decrease the TS allocation to $\beta_{m,k} = \beta_{m,k} - \tau$ and update $PULIST_m$ and $SULIST_k$.
        13: If no more matchings are possible then goto step 6.
14: If $j = k$, then the algorithm ends
```

offer from another PU, breaks the previous match and creates a new match until it receives another better offer. Secure-PDA on the other hand discourages competition among the PUs in their matching, which results in better performance for the PUs in terms of their sececy. It does so by introducing a game where all the PUs prioritize their acquisition of SU in a round robin rotation basis. In Secure-PDA the PUs in addition to their $PULIST_m$, prepare a priority list known as the $ALIST_1 = \{P_{S_1}, P_{S_2}, \dots, P_{S_M}\}$ which is the PUs priority list for acquiring the best SU. After the first round the $ALIST_i$ is updated in a round robin rotation manner and the new list will be $ALIST_2 = \{P_{S_M}, P_{S_1}, P_{S_2}, \dots, P_{S_{(M-1)}}\}$ and so on. Therefore, there will be m rounds of our game where each PU will be able to match with its best SU for atleast 1 round. During each round the PU which is at the top of the $ALIST_i$ will have the priority to chose from the available SUs. The PU will make an offer of a limited time allocation factor $\beta_{m,k}$ to the first SU in its $PULIST_m$. If that PU is also present in the $SULIST_k$ of the SU, the match is made. Otherwise the PU will decreasing the time allocation factor by ϵ and update the $PULIST_m$ and make another offer to the first SU in its updated $PULIST_m$. After the first PU is matched, second PU from the $ALIST_i$ will try to make a match with the best SU from the remaining unmatched SUs. In this way the algorithm will continue until all the PUs are matched or until no further matches are possible. During the next round the $ALIST_{i+1}$ will be updated as listed in $ALIST_2$ stated above and new matchings will be made. In this way matchings will be made which will last for at-least m rounds. The detailed PDA algorithm is presented in Algorithm 2.

3.3 Results

We investigated the secrecy sum rate and SU sum rate for our system model for Amplify and Forward (AF) based



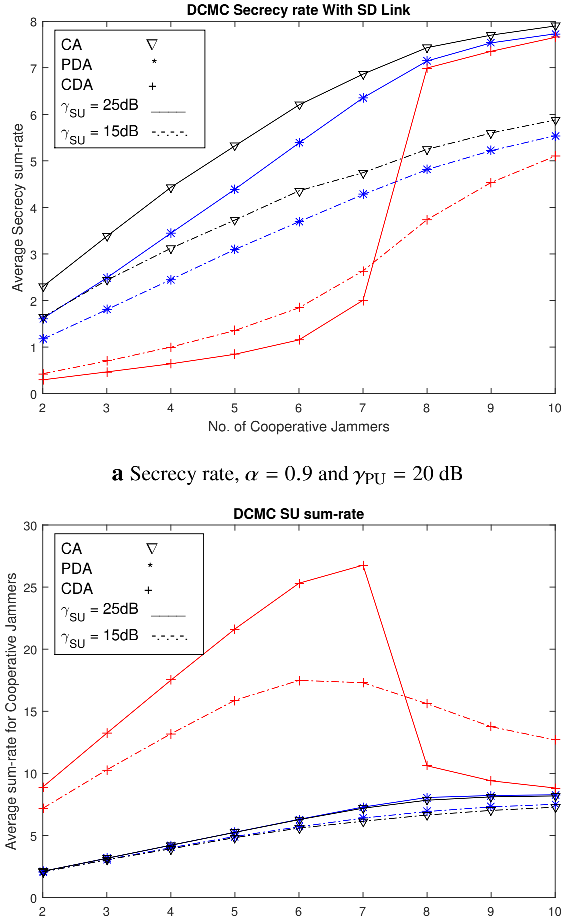
a Secrecy rate, $\alpha = 0.9$ and $\gamma_{\mathrm{PU}} = 20$ dB

b SU rate, $\alpha = 0.9$ and $\gamma_{\mathrm{PU}} = 20$ dB

Fig. 7. AF based relaying when operating at the CCMC capacity, the number of primary transmitter, relay and receiver pairs is 8.

Algorithm 2 Secure PDA

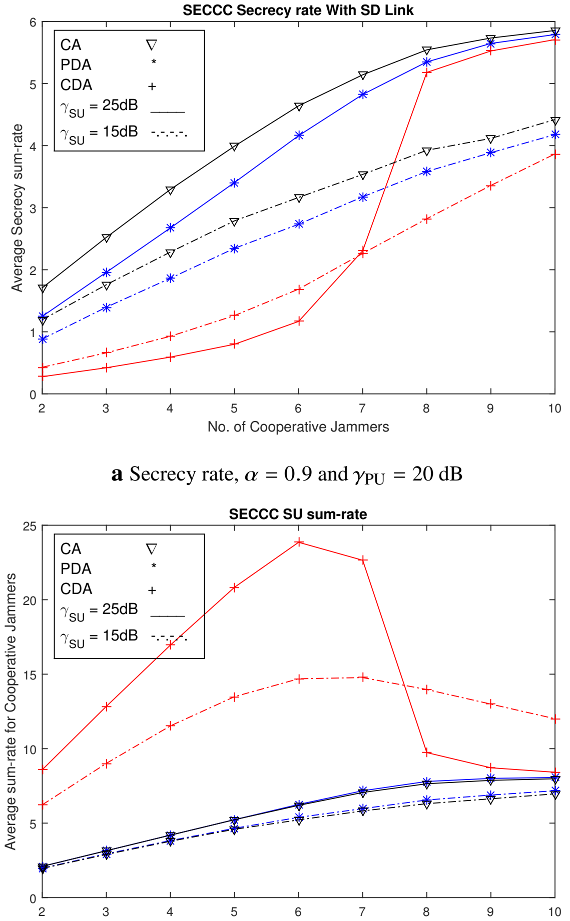
```
Require: $\bar{R}_{\mathrm{CJ}_{m,k}} \geq 1 \wedge 0 < \beta_{m,k} < 1$
Ensure: $\bar{R}_{\mathrm{s}_{m,k}} > 0$
 1: Initialization
      2: Set up the first priority list $ALIST_1 = \{P_{S_1}, P_{S_2}, \dots, P_{S_M}\}$.
      3: Set $i = 1$ for the first round.
 4: Matching for the $i$th round
      5: Set the initial TS allocation to $\beta_{init} = 0.99$, and set the step size of TS increment to $\tau = 0.05$.
      6: Construct $PULIST_m = \{St_{\mathrm{CK}_k} | \bar{R}_{\mathrm{s}_{m,k}} > 0\}$ and $SULIST_k = \{P_{\mathrm{S}_m} | \bar{R}_{\mathrm{CJ}_{m,k}} \geq 1\}$ in descending order, where $m = \{1, \dots, M\}$ and $k = \{1, \dots, K\}$.
      7: Set $j = 1$ for the first transmission.
      8: Do the matching for $j$th transmission.
           9: Find the corresponding $P_{\mathrm{S}_m}$ for transmission, based on the $ALIST_i$ (i.e) $j$th element of $ALIST_i$
          10: $P_{\mathrm{S}_m}$ selects the best available $St_{\mathrm{CJ}_k}$ from its $PULIST$ and offer a time slot $\beta_{m,k}$
          11: If $P_{\mathrm{S}_m}$ is in the preference list of $St_{\mathrm{CJ}_k}$ then $St_{\mathrm{CJ}_k}$ and $P_{\mathrm{S}_m}$ are matched.
          12: If $P_{\mathrm{S}_m}$ is not in the preference list of $St_{\mathrm{CJ}_k}$ then decrease the TS allocation to $\beta_{m,k} = \beta_{m,k} - \tau$ and update both $PULIST_m$ and $SULIST_k$.
          13: If $PULIST_m$ is empty then $P_{\mathrm{S}_m}$ is left unmatched.
          14: Set $j = j + 1$ and goto step 8 until $j = K$.
15: Set $i = i + 1$ and goto step 4 for the next round, until $i = K$
```



a Secrecy rate, $\alpha = 0.9$ and $\gamma_{\mathrm{PU}} = 20$ dB

b SU rate, $\alpha = 0.9$ and $\gamma_{\mathrm{PU}} = 20$ dB

Fig. 8. AF based relaying when operating at the DCMC capacity, the number of primary transmitter, relay and receiver pairs is 8.



a Secrecy rate, $\alpha = 0.9$ and $\gamma_{\mathrm{PU}} = 20$ dB

b SU rate, $\alpha = 0.9$ and $\gamma_{\mathrm{PU}} = 20$ dB

Fig. 9. AF based relaying when a practical adaptive SECCC scheme is employed, the number of primary transmitter, relay and receiver pairs is 8.

relaying, when operating at the CCMC capacity, DCMC capacity and when practical adaptive SECCC scheme is used. The performance of the DCMC and SECCC based scheme relies on the SNR thresholds and throughputs in Tab. 1. The results for the Secure Conventional Distributed Algorithm (S-CDA) and Secure Pragmatic Distributed Algorithm (S-PDA) for our system model are shown in Fig. 7 in comparison to the Centralized Algorithm (CA) for secrecy maximization. We consider $M = 8$ with $\gamma_{\text{PU}} = 20$ dB and $K = \{2, 3, \ldots, 10\}$ with $\gamma_{\text{SU}} = \{15, 25\}$ dB. The power distribution factor α is kept at 0.9 while the pathloss exponent n is kept at 4. All the results indicate a superior secrecy sum rate for the S-PDA system which is comparable to that of the CA scheme, while for $K \geq 7$ we see that the S-CDA and S-PDA almost perform similar for the case where the γ_{SU} is kept at 25 dB. The SU sum rate is better for the S-CDA system because of the competition amongst the PUs for acquiring the best SU. As the number of SUs/CJs increases we see a rise in the secrecy sum rate and a decrease in the SU sum rate which again is due to high competition when the number of SUs/CJs is less as compared to the case when the number of SUs/CJs is higher and a decrease in competition is witnessed. Similarly we see an opposite trend in the secrecy sum-rate for the S-CDA where the secrecy sum-rate is lower when we have less number of CJs as all the PUs compete with each other for matching with the CJ, while the secrecy sum-rate increases close to the S-PDA when the number of CJs is equal or greater than the number of PUs due to lesser competition among the PUs for matching with CJs. S-PDA system on the other hand does not have competition amongst the PUs by including them in a round robin rotation based game which encourages the PUs not to acquire the SU which have been assigned to another PU, hence we see a stable increase in the secrecy sum rate as more SU CJs are available, while the SU sum rate will always be closer to their minimum rate requirements.

4. Conclusion

In this paper, we first investigated the secrecy rate regions for friendly jamming in a cooperative network where communication was assisted by an untrusted relay. A friendly jammer was used for providing secrecy by transmitting a noise signal in parallel to the source signal. We investigated the secrecy rate when assuming idealistic performance operating at the CCMC and DCMC capacities, as well as when a practical adaptive SECCC coding scheme was invoked. It was observed that the secrecy rate can be maximized if the jammer is at a certain distance from the relay. We then further proposed the novel S-PDA and S-CDA schemes for maximizing the secrecy based on the cognitive radio approach. More explicitly, selected jammers were rewarded with a limited access to the spectrum for their service in providing the secrecy. The proposed S-PDA and S-CDA schemes were further compared with the CA and it was shown that the S-PDA provides maximum secrecy when the number of jammers is less than the number of primary sources. By contrast, the S-CDA provides a better sum-rate for the jammers and a reduced secrecy for the sources as compared to those of the S-PDA.

References

[1] YANG, N., WANG, L., GERACI, G., et al. Safeguarding 5g wireless communication networks using physical layer security. *IEEE Communications Magazine*, 2015, vol. 53, no. 4, p. 20–27. DOI: 10.1109/MCOM.2015.7081071

[2] ZHONG, Z., PENG, J., LUO, W., et al. A tractable approach to analyzing the physical-layer security in k-tier heterogeneous cellular networks. *China Communications*, 2015, vol. 12, p. 166–173. DOI: 10.1109/CC.2015.7386165

[3] LI, S., XU, L. D., ZHAO, S. The internet of things: A survey. *Information Systems Frontiers*, 2015, vol. 17, no. 2, p. 243–259. DOI: 10.1007/s10796-014-9492-7

[4] WANG, H. M., ZHENG, T. X., YUAN, J., et al. Physical layer security in heterogeneous cellular networks. *IEEE Transactions on Communications*, 2016, vol. 64, no. 3, p. 1204–1219. DOI: 10.1109/TCOMM.2016.2519402

[5] MUKHERJEE, A. Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, 2015, vol. 103, no. 10, p. 1747–1761. DOI: 10.1109/JPROC.2015.2466548

[6] SAAD, W., ZHOU, X., DEBBAH, M., et al. Wireless physical layer security. *IEEE Communications Magazine*, 2015, vol. 53, no. 12, p. 18. DOI: 10.1109/MCOM.2015.7355560

[7] ELETREBY, R., RAHBARI, H., KRUNZ, M. Supporting phy-layer security in multi-link wireless networks using friendly jamming. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*. 2015, p. 1–6. DOI: 10.1109/GLOCOM.2015.7417141

[8] BERGER, D. S., GRINGOLI, F., FACCHI, N., et al. Friendly jamming on access points: Analysis and real-world measurements. *IEEE Transactions on Wireless Communications*, 2016, vol. 15, no. 9, p. 6189-6202. DOI: 10.1109/TWC.2016.2581165

[9] SHEN, W., LIU, Y., HE, X., et al. No time to demodulate - fast physical layer verification of friendly jamming. In *Proceedings of the IEEE Military Communications Conference (MILCOM)*. 2015, p. 653–658. DOI: 10.1109/MILCOM.2015.7357518

[10] XING, H., WONG, K. K., CHU, Z., et al. To harvest and jam: A paradigm of self-sustaining friendly jammers for secure af relaying. *IEEE Transactions on Signal Processing*, 2015, vol. 63, no. 24, p. 6616–6631. DOI: 10.1109/TSP.2015.2477800

[11] HE, X., YENER, A. Cooperation with an untrusted relay: A secrecy perspective. *IEEE Transactions on Information Theory*, 2010, vol. 56, no. 8, p. 3807–3827. DOI: 10.1109/TIT.2010.2050958

[12] KHODAKARAMI, H., LAHOUTI, F. Link adaptation with untrusted relay assignment: Design and performance analysis. *IEEE Transactions on Communications*, 2013, vol. 61, no. 12, p. 4874–4883. DOI: 10.1109/TCOMM.2013.111513.120888

[13] ZEWAIL, A. A., YENER, A. The two-hop interference untrusted-relay channel with confidential messages. In *Proceedings of the IEEE Information Theory Workshop - Fall (ITW)*. 2015, p. 322–326. DOI: 10.1109/ITWF.2015.7360788

[14] XIONG, J., CHENG, L., MA, D., et al. Destination aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems. *IEEE Transactions on Vehicular Technology*, 2015, vol. 65, no. 9, p. 7274-7284. DOI: 10.1109/TVT.2015.2490099

[15] KALAMKAR, S. S., BANERJEE, A. Secure communication via a wireless energy harvesting untrusted relay. *IEEE Transactions on Vehicular Technology*, 2016, vol. 66, no. 3, p. 2199–2213. DOI: 10.1109/TVT.2016.2572960

[16] ZEWAIL, A. A., NAFEA, M., YENER, A. Multi-terminal networks with an untrusted relay. In *Proceedings of the 52nd Annual Conference on Communication, Control, and Computing (Allerton)*. 2014, p. 895–902. DOI: 10.1109/ALLERTON.2014.7028549

[17] STANOJEV, I., YENER, A. Improving secrecy rate via spectrum leasing for friendly jamming. *IEEE Transactions on Wireless Communications*, 2013, vol. 12, no. 1, p. 134–145. DOI: 10.1109/TWC.2012.120412.112001

[18] QU, J., CAI, Y., LU, J., et al. Power allocation based on stackelberg game in a jammer-assisted secure network. In *Proceedings of the International Conference on Cyberspace Technology (CCT 2013)*. 2013, p. 347–352. DOI: 10.1049/cp.2013.2150

[19] ZHILING, H., BAOYUN, W. Coalition formation game of dual-identity nodes for improving phy security of wireless networks. In *Proceedings of the 27th Chinese Control and Decision Conference (2015 CCDC)*. 2015, p. 3658–3662. DOI: 10.1109/CCDC.2015.7162560

[20] ZHANG, N., CHENG, N., LU, N., et al. Partner selection and incentive mechanism for physical layer security. *IEEE Transactions on Wireless Communications*, 2015, vol. 14, no. 8, p. 4265–4276. DOI: 10.1109/TWC.2015.2418316

[21] BAYAT, S., LOUIE, R. H. Y., VUCETIC, B., et al. Dynamic decentralised algorithms for cognitive radio relay networks with multiple primary and secondary users utilising matching theory. *Transactions on Emerging Telecommunications Technologies*, 2013, vol. 24, p. 486–502. DOI: 10.1002/ett.2663

[22] LIANG, W., NG, S. X., FENG, J., et al. Pragmatic distributed algorithm for spectral access in cooperative cognitive radio networks. *IEEE Transactions on Communications*, 2014, vol. 62, no. 4, p. 1188–1200. DOI: 10.1109/TCOMM.2014.030214.130326

[23] NG, S. X., HANZO, L. On the MIMO channel capacity of multidimensional signal sets. *IEEE Transactions on Vehicular Technology*, 2006, vol. 55, no. 2, p. 528–536. DOI: 10.1109/TVT.2005.863357

[24] BUTT, M. F. U., NG, S. X., HANZO, L. Self-concatenated code design and its application in power-efficient cooperative communications. *IEEE Communications Surveys Tutorials*, 2012, vol. 14, no. 3, p. 858–883. DOI: 10.1109/SURV.2011.081511.00104

[25] OCHIAI, H., MITRAN, P., TAROKH, V. Design and analysis of collaborative diversity protocols for wireless sensor networks. In *Proceedings of the 60th IEEE Vehicular Technology Conference (VTC2004-Fall)*. 2004, p. 4645–4649. DOI: 10.1109/VETECF.2004.1404971

About the Authors . . .

Bakhtiar ALI received his M.Sc. degree in Personal and Mobile Radio Communications from Lancaster University, UK in September 2008. He is currently pursuing a doctoral degree at COMSATS Institute of Information Technology, Islamabad, Pakistan. His current research interests include the radio resource management in cooperative cognitive radio networks, space time block coding, cooperative communications, physical layer security, game theory and the study of future radio communications systems, i.e., 5G.

Nida ZAMIR received her Bachelor's degree in Electrical Engineering with specialization in Telecommunications from COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan in 2014. She is currently pursuing her MS in Electrical Engineering from the same institution. Her current research interests include channel coding, physical layer security and game theory.

Soon Xin NG received the B.Eng. degree (First class) in electronics engineering and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a postdoctoral research fellow working on collaborative European research projects known as SCOUT, NEWCOM and PHOENIX. Since August 2006, he has been a member of academic staff in the School of Electronics and Computer Science, University of Southampton. He is involved in the OPTIMIX and CONCERTO European projects as well as the IUATC and UC4G projects. He is currently an Associate Professor of Telecommunications with the University of Southampton. He has authored over 200 papers and co-authored two John Wiley/IEEE Press books in his research field. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum error correction codes and joint wireless-and-optical-fiber communications. He is a Chartered Engineer and a Fellow of the Higher Education Academy in the UK.

Muhammad Fasih Uddin BUTT received his B.E. degree from National University of Sciences & Technology (NUST), Pakistan in 1999. He received his M.E. degree from Center for Advanced Studies in Engineering, UET Taxila, Pakistan with specialization in Digital Communication/Computer Networks in 2003 and his Ph.D. degree from Communications Research Group, School of Electronics and Computer Science, University of Southampton, U.K in June 2010. Currently he is working as Assistant Professor in the Department of Electrical Engineering, COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan where he has been serving as an academic since 2002. His research interests include channel coding, iterative detection, cooperative cognitive radio networks, mm Wave radio-over-fiber technologies, energy harvesting and physical layer security. He has published over 25 research papers in various reputed journals and conference proceedings.