Enhancing Secrecy Rate in Cognitive Radio Networks via Multi-level Stackelberg Game

***Abstract*—In this letter, physical layer (PHY) security is investigated for both primary and secondary transmissions of a cognitive radio network (CRN) that is in danger of malicious attempt by an eavesdropper (ED). In our proposed system, the secondary transmitter (ST) is acted as a trusted relay (TR) for primary transmission and the PHY security is facilitated by the cooperation between the primary transmitter (PT) and the ST using the multi-level Stackelberg game. In particular, we formulate and then solve the optimization problem of maximizing secrecy rates in different phases of primary and secondary transmissions. Finally, numerical examples are provided to demonstrate that the spectrum leasing based on trading secondary access for cooperation is a promising framework for enhancing secrecy rate in CRNs.**

I. Introduction

Cooperative jamming received significant attention over the past few years to increase physical layer (PHY) security. Cooperative jamming prescribes creating judicious interference by transmitting noise to impair the eavesdroppers' ability in decoding the confidential information [1]. The open nature of the wireless medium makes the transmission susceptible to malicious eavesdropping [2]. To cope with it, the authors in [3] proposed secondary cooperation to maximize the secrecy rate of the primary network while satisfying a required secondary rate of the secondary network. This is achieved by an optimal design of a beamformer at the multi-antenna secondary transmitter (ST) to generate interference to confuse eavesdroppers (EDs). The secrecy rate maximization problem is studied in [4] using game theory, where the jammer introduces charges for its jamming service based on the amount of interference caused to the EDs. This problem is formulated into a Stackelberg game, where the jammer and the transmitter play the roles of leader and follower of the game. In [5], the authors focused on maximizing secrecy rate and information rate of the cognitive radio networks (CRNs), where two secondary users acted as relay and jammer.

The aforementioned works focused on enhancing the secrecy rate for primary transmission and information rate for secondary transmission, with the assumption that the ED can intercept the primary transmission only. Inspired by the study in [6], we propose a new scenario where the primary transmitter (PT) allows the ST to access its spectrum for better secrecy performance. Here, we consider a more realistic case where the ED can intercept both the primary and secondary transmissions (i.e,, the worst case of security). In our approach, the ST is used as a trusted relay (TR) and a jammer for primary transmission. We also assume that PT and ST can allocate some of its transmission power to transmit the artificial noise to create interference at the ED. In a such network, a primary user may lease portions of a licensed spectrum to a secondary user in exchange for enhanced performance. This scenario avoids the regulatory issues that commonly hinder the implementation of the property-rights spectrum leasing concept. In our considered system, the primary users always have first priority and the secondary users are trying to maximize their benefits given the existence of primary users. This fits perfectly the model of leader and follower in the Stackelberg game. In addition, the ST also acts as a trusted relay to support and speed up the completion of the primary transmission. We therefore propose a novel multi-level game to reflect considered system model. The main contributions of this letter are detailed as follows:

- Using a Stackelberg game, we propose a resource allocation scheme (i.e. power and time resource) for spectrum leasing to maximize secrecy rates in different phases of primary and secondary transmissions (PSR), given the perfect knowledge of channel state information (CSI).
- We obtain the unique equilibrium value of the proposed Stackelberg game.
- We show that the secrecy rate of the proposed system using multi-level Stackelberg game is significantly higher than that using the single level Stackelberg game..
- Comparisons with previous works are provided to show the significant improvement of security in the proposed system.

II. System models

We consider a CRN where the primary transmission includes a pair of the PT and primary receiver (PR), and the secondary transmission includes a pair of the ST and secondary receiver (SR). All transmissions within the network is under threat from malicious attempt of an ED. Note that the ST will act as a TR in the second phase of primary transmission (so we interchange the names TR and ST depending the phase of transmission it is in). We assume the following: i) there is no direct transmission between the PT and the PR; ii) each node carries a single omnidirectional antenna; iii) the relaying strategy of decode-and-forward (DF) is considered; iv) global CSI is available by a standard channel estimator (CE) (e.g., [7]); and v) *a-priori* knowledge of jamming signals is available at legitimate receivers. Note that the last assumption can be achieved by the process of communicating the keys of artificial noise between the legal source and destination in two steps: The phase response of the channel is probed first, and then, the information bearing signal is modified to pre-compensate for the phase effects of the channel. Since the channels between the legal source and destination are completely different from the channels between the legal source and EDs, this process is secure [8], [9]. To enhance secrecy rates, we allow the

legitimate transmitters to use a portion of their power to transmit a jamming signal, in addition to transmitting their message signal.

In our system, we propose three phases of transmissions as follows: *i) Phase 1* - primary transmission of information from the PT to the TR (i.e, the ST); *ii) Phase 2* - relay transmission of primary information from the TR to the PR; and *iii) Phase 3* - secondary transmission of information from the ST to the SR. Because the ED can intercept any transmission during these three phases, our objective is to improve the secrecy rates of all transmission via transmitting appropriate jamming signals. For convenience, we define different secrecy rates according to each phase above as follows: primary secrecy rate (PSR) is used to refer to secrecy rate achieved in Phase 1 (primary transmission); relay secrecy rate (RSR) is used for secrecy rate achieved in Phase 2 (relay transmission); and finally, secondary secrecy rate (SSR) is used for secrecy rate achieved in Phase 3 (secondary transmission). In particular, the signals received in each phase are as follows:

Phase 1: Using a fraction of the considered time slot $(1-\alpha)$ where $0 < \alpha < 1$, PT sends its message signal and ST acts as the relay to receive as follows

$$x_{ST} = \sqrt{\epsilon_1 P_p} h_{ps} s_1 + \sqrt{(1-\epsilon_1)P_p} h_{ps} z_1 + n_{ST}, \quad (1)$$

where s_1 is the message signal, $z_1 \sim \mathcal{CN}(0,1)$ is the artificial noise, $n_{ST} \sim \mathcal{CN}(0,\sigma^2)$ is the noise at the ST, ϵ_1 is the PT's fraction of allocated power P_p for transmission of primary message $(0 < \epsilon_1 < 1)$ and $h_{ps} \sim \mathcal{CN}(0,\sigma_h^2)$ is the channel coefficient between the PT and ST. For notational convenience, let us define $\rho_{ps} = P_p |h_{ps}|^2 / \sigma^2$ and $\rho_{pe} = P_p |h_{pe}|^2 / \sigma^2$, where h_{pe} is the channel coefficient between the PT and ED. We assume that ST has a-priori knowledge of artificial noise. The achievable secrecy rate PSR at Phase 1, denoted by R_{PSR}, can be calculated as follows

$$R_{PSR} = (1-\alpha)\left[\log_2(1+\epsilon_1\rho_{ps}) - \log_2\left(\frac{(1+\rho_{pe})}{1+(1-\epsilon_1)\rho_{pe}}\right)\right]$$

Phase 2: The ST acts as a trusted relay to forward secure primary message to the PR in the fraction $\alpha\beta$ of the considered timeslot $(0 < \alpha, \beta < 1)$. The received signal at PR is

$$x_{PR} = \sqrt{\epsilon_2 P_s} h_{sp} \hat{s}_1 + \sqrt{(1-\epsilon_2)P_s} h_{sp} z_2 + n_{PR}, \quad (2)$$

where $\hat{s}_1$ is the re-encoded message signal of s_1, $z_2 \sim \mathcal{CN}(0,1)$ is the artificial noise, ϵ_2 is the ST's fraction of allocated power P_s for relaying of primary message $(0 < \epsilon_2 < 1)$ and $h_{sp} \sim \mathcal{CN}(0,\sigma_h^2)$ is the channel coefficient between the ST and the PR. After removing the artificial noise at the PR, the achievable secrecy rate RSR at Phase 2, denoted by R_{RSR}, can be calculated as follows:

$$\begin{aligned} R_{RSR} &= (\alpha\beta)\left[\log_2(1+\epsilon_2\rho_{sp})\right. \\ &\quad \left. - \log_2\left(\frac{1+\rho_{se}+(1-\epsilon_1)\rho_{pe}}{1+(1-\epsilon_2)\rho_{se}+(1-\epsilon_1)\rho_{pe}}\right)\right] \quad (3) \end{aligned}$$

where $\rho_{sp} = P_s |h_{sp}|^2 / \sigma^2$, $\rho_{se} = P_s |h_{se}|^2 / \sigma^2$, and h_{se} is the channel coefficient between the ST and ED.

Phase 3: The ST sends its own secure secondary message to the SR in the remaining timeslot fraction $\alpha(1-\beta)$. The received signal at SR can be written as follows:

$$x_{SR} = \sqrt{\epsilon_2 P_s} h_{ss} s_2 + \sqrt{(1-\epsilon_2)P_s} h_{ss} z_2 + n_{SR}, \quad (4)$$

where s_2 is the secondary message signal and $h_{ss} \sim \mathcal{CN}(0,\sigma_h^2)$ is the channel coefficients between the ST and SR. We assume that same codewords of artificial noise are used in both of primary and secondary transmission (i.e., the same z_2). After removing the artificial noise at the SR, we can obtain the secrecy rate at Phase 3, denoted by R_{SSR}, as follows:

$$\begin{aligned} R_{SSR} &= \alpha(1-\beta)\left[\log_2(1+\epsilon_2\rho_{ss})\right. \\ &\quad \left. - \log_2\left(\frac{1+\rho_{se}+(1-\epsilon_1)\rho_{pe}}{1+(1-\epsilon_2)\rho_{se}+(1-\epsilon_1)\rho_{pe}}\right)\right] \quad (5) \end{aligned}$$

where $\rho_{ss} = P_s |h_{ss}|^2 / \sigma^2$.

III. Secrecy Rates as a Game Theoretic Model

Throughout this work, the nodes are defined as selfish and rational to mimic a non-altruistic behavior. An appropriate framework for analyzing the interaction between such nodes is muti-level Stackelberg game. If this game includes M players with N levels, then the lth player is the follower of the $(l-1)$th player at the ith level and is a leader of the $(l+1)$th player at the $(i+1)$th level, where $1 < i < N$ and $1 < l < M$. Furthermore, the first player is the leader at the first level and the Mth player is the follower at the Nth level. In general, the number of levels is equal to the number of players minus one (i.e., $N = M-1$). For demonstration, in this section, we apply two levels only of the Stackelberg game, as shown in Fig.1, to maximize the secrecy rate in each phase of transmission.

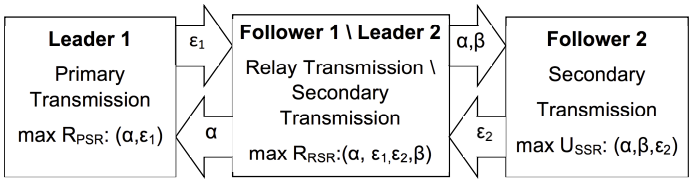

Fig. 1: Two-level Stackelberg game of proposed system

A. Level 1

The leader and follower are the PT (Phase 1) and the TR (i.e., the ST in Phase 2), respectively. We can find the optimal value ϵ_1^* to maximize the secrecy rate of the leader as follows

$$\epsilon_1^* = \arg\max_{\epsilon_1} R_{PSR}. \quad (6)$$

Lemma 1. *The secrecy rate at Phase 1 in* (2) *is concave in terms of* ϵ_1.

Proof: In order to prove the concavity of the primary transmission's utility, we derive the second derivative of (2) with respect to ϵ_1 as follows:

$$\frac{\partial^2 R_{PSR}}{\partial^2 \epsilon_1} = q_1\left[\left(-\frac{\rho_{ps}^2}{(1+\epsilon_1\rho_{ps})^2} - \frac{\rho_{pe}^2}{(1+(1-\epsilon_1)\rho_{pe})^2}\right)\right] \quad (7)$$

where $q_1 = (1-\alpha)/\ln 2$. Obviously, this second derivative in (7) is negative and R_{PSR} is concave in terms of ϵ_1. ■

According to Lemma 1, we can find ϵ_1^* from solving the following equation:

$$\frac{\partial R_{PSR}}{\partial \epsilon_1} = q_1 \left[\frac{\rho_{ps}}{(1+\epsilon_1\rho_{ps})} - \frac{\rho_{pe}}{(1+(1-\epsilon_1)\rho_{pe})} \right] = 0, \quad (8)$$

leading to

$$\epsilon_1^* = \frac{\rho_{ps} - \rho_{pe} + \rho_{ps}\rho_{pe}}{2\rho_{ps}\rho_{pe}}. \quad (9)$$

The follower then tries to maximize its secrecy rate R_{RSR} too. But because the follower of Level 1 also plays the role of the leader of Level 2, we will describe the maximization process of R_{RSR} in the next subsection.

B. Level 2

At Level 2, the leader and follower are the TR (i.e, the ST in Phase 2) and the ST (in Phase 3), respectively. The optimal primary strategy ϵ_1^* , relay transmitter strategy (α^*, β^*) and the corresponding power choice of the secondary transmitter ${\epsilon_2}^*$ are jointly referred as the Stackelberg equilibrium. The ST is aware of parameters (α, β) and optimizes its power level towards the goal of maximizing its utility:

$$U_{SSR}(\alpha, \beta, \epsilon_1^*, \epsilon_2(\alpha, \beta)) = R_{SSR} - k\epsilon_2, \quad (10)$$

where k is pricing constant. According to Lemma 1, the utility of secondary transmission in (10) is also concave in terms of ϵ_2. The optimal solution of secondary transmission problem can be found as

$${\epsilon_2}^* = \arg\max U_{SSR}(\alpha, \beta, \epsilon_1^*, \epsilon_2(\alpha, \beta)), \quad (11)$$

subject to $0 < \alpha < 1$, $0 < \beta < 1$ and $0 < \epsilon_2 < 1$. To find optimum ${\epsilon_2}^*$, we can differentiate U_{ssec} with respect to ϵ_2 and equate it to zero. After simplification, we can obtain ϵ_2 by solving the equation $a{\epsilon_2}^2 + b\epsilon_2 + c = 0$, where $a = \rho_{ss}\rho_{se}$, $b = \rho_{se} - \rho_{ss} - \rho_{ss}\rho_{se} - \rho_{ss}\rho_{pe}(1 - {\epsilon_1}^*) - (2\rho_{ss}\rho_{se}q/k)$, $c = (q/k)(\rho_{ss} - \rho_{se} + \rho_{ss}\rho_{se} + \rho_{ss}\rho_{pe}(1 - {\epsilon_1}^*)) - \rho_{se} - 1 - \rho_{pe}(1 - {\epsilon_1}^*)$. Then, we can obtain the two roots of ϵ_2, denoted by $\epsilon_2^{*(1)}$ and $\epsilon_2^{*(2)}$.

Furthermore, the relay transmission determines the fraction α and ratio β towards the goal of maximizing its secrecy rate, knowing that its decision will affect the strategy selected by the ST in Phase 3, ad follows

$$\alpha^*, \beta^* = \arg \max_{0<\alpha,\beta,\epsilon_1,\epsilon_2<1} R_{RSR}(\alpha, \beta, {\epsilon_1}^*, {\epsilon_2}^*(\alpha, \beta)). \quad (12)$$

Theorem 1. *The allocated power levels $\epsilon_1^*, \epsilon_2^*$ and time slot fraction α^* are the Nash equilibrium of the proposed game.*

Proof: According to DF scheme, we assume that the transmission rate from the ST to the PR in Phase 2, denoted by R_{sp}, is not greater than the transmission rate from the the PT to the ST in Phase 1, denoted by, R_{ps}. We can consider the equality is the optimal case to find the relationship between α and β to facilitate the solution of the above optimization problem:

$$R_{sp} = R_{ps} \Rightarrow \beta = \frac{(1-\alpha)}{\alpha} \frac{\log_2(1+\rho_{ps})}{\log_2(1+\epsilon\rho_{sp})}. \quad (13)$$

According to Lemma 1, in Phases 1 and 3, R_{PSR} and U_{SSR} are strictly concave in terms of ϵ_1 and ϵ_2 for a given values of α and β. Furthermore, R_{RSR} is an increasing function of α then the relay transmission (leader) in Level 2 will select the best responses ϵ_1^* of leader in Level 1 and $\epsilon_2^*(\alpha)$ of the follower in Level 2 as follows:

$$\alpha^* = \arg\max R_{RSR}(\alpha, \epsilon_1^*, \epsilon_2^*(\alpha)). \quad (14)$$

Therefore, α^*, ϵ_1^* and $\epsilon_2^*(\alpha^*)$ form the Nash equilibrium of the proposed Stackelberg game. ■

Lemma 2. *The N-level Stackelberg game has higher secrecy rate than the (N-1)-level Stackelberg game.*

Proof: For convenience, we consider $N = 2$ for the proof. The general case can be similarly achieved. In the single-level game, we assume the PT is out of range of the ED to remove the impact of the PT (leader in Level 1) which is represented by ϵ_1. In this case, we need the single-level Stackelberg game between relay transmission (leader) and secondary transmission (follower). According to the same procedure of Phases 2 and 3 in aforementioned study of the multi-level Stackelbrg game, we can find the following single-level primary secrecy rate, which is actually relay secrecy rate and denoted by ${R_{RSR}}^{(1)}$, as follows

$${R_{RSR}}^{(1)} = \alpha\beta \left[\log_2(1+\epsilon_2\rho_{sp}) - \log_2(\frac{(1+\rho_{se})}{(1+(1-\epsilon_2)\rho_{se})}) \right].$$

To highlight the enhancement of primary secrecy rate by 2-level Stackelberg game, we need to prove that $R_{RSR} - {R_{RSR}}^{(1)} > 0$. This is obvious because $R_{sp} = \log_2(1+\epsilon_2\rho_{sp})$ is the same in both single- and two-level games while in the second term of (3), we have $\rho_{pe}(1-\epsilon_1) > 0$. ■

IV. Numerical Results

In this section, we present the numerical results and some related discussions. We consider two optimization problems from the previous section according to the Stackelberg game. Our simulation consists of two steps as follows: Firstly, we consider the following parameters to provide same setting as

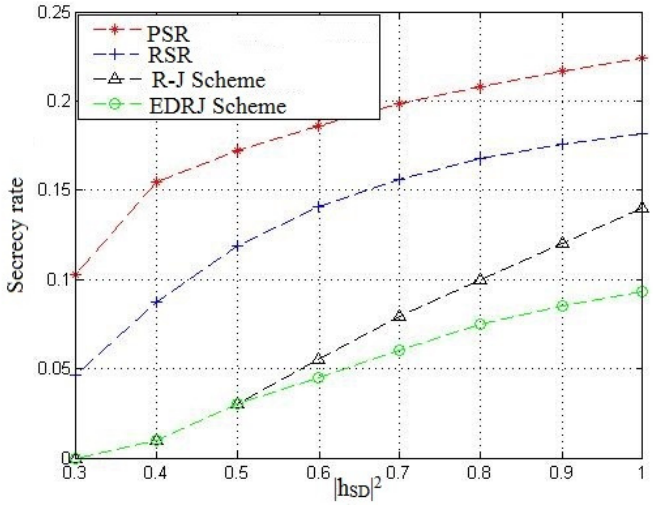

Fig. 2: Comparison for primary secrecy rate

previous study in [5] : $P_s = 2$mW, noise variance $\sigma^2 = 1$mW, pricing factor $c_1 = 0.25$, $|H_{ps}|^2 = 0.6$, $|H_{se}|^2 = 0.3$ and $|H_{ss}|^2 = 0.8$. Fig.2 evaluates our proposed scenario by comparing it with previous study, which used two secondary users: one for relay and another one for non-friendly jammer. In [6], the authors proposed relay and jammer (R-J) and equal-duration relay jammer (EDRJ) schemes to enhance secrecy rate in CR. Fig.2 plot the secrecy rate versus the channel gain between legitimate source and destination (h_{SD}). The main difference between EDRJ and R-J schemes is that the time durations for the first two phases in EDRJ are equal and the secrecy rate is maximized without considering time allocation. It is shown that our proposed system outperforms the R-J and EDRJ schemes significantly due to no interference at legal receiver by being able to remove the artificial noise at the receiver, and the increased interference at eavesdropper due to the interaction between two levels of Stackelberg game. Secondly, to find the effect of signal to noise ratio (SNR)

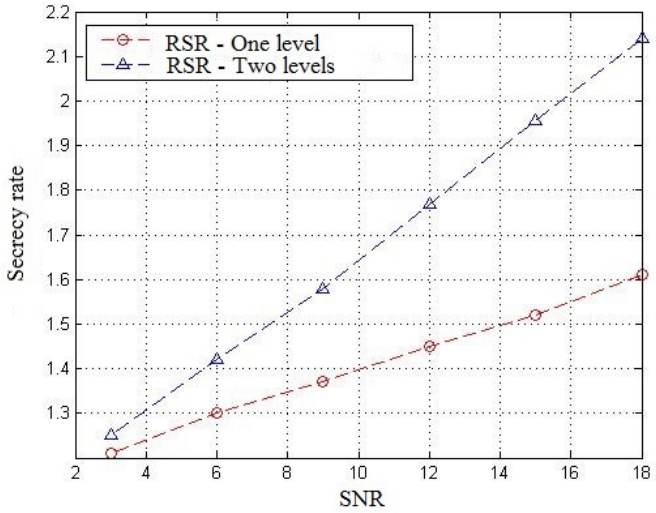

Fig. 3: Secrecy rate comparison versus SNR

on the secrecy rates in three phases. We fix the locations of the PT, PR, ST, ED and SR at the coordinates (0.2,0),(0.6, 0), (0, 0),(0,1) and (0, 0.4), respectively. We assume the path loss model $h_{ij} = d^{-\delta}$ with path loss exponent $\delta = 3.0$ and the pricing coefficient $k = 0.25$. Fig.3 shows the optimum primary secrecy rates of the single- and two-level games versus the SNR. It is noted that the PSR is improved by the multi-level Stackelberg game, which is consistent with our finding in Lemma 2. Furthermore, it is indicated that the PSR of the two-level Stackelberg game increases significantly than that of the single-level case due to the residual effect of ρ_{ps} on the secrecy of two-level case according to (3). Thirdly, we consider same locations of PT, ST, SR and ED as same as in Fig.2 except the different location of PR to find effect of the destination location on the allocation of primary and secondary power and time resources. Fig. 4 plots the optimum PSR, RSR and SSR versus SNR. It is noted that the optimum secrecy rates of three phases increase significantly with SNR due to the increased ρ_{ps}, ρ_{sp} and ρ_{ss}.

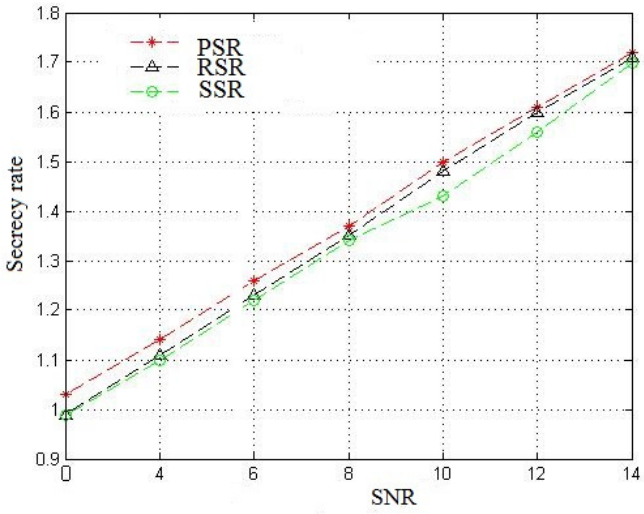

Fig. 4: Secrecy rate versus SNR

V. Conclusion

In this letter, we proposed a multi-level Stackelberg game based cooperation scheme to optimize the PHY layer security of both primary and secondary transmissions in CRNs. In particular, we formulated and solved an optimization problem aiming at maximizing the achievable secrecy rates on the primary, relay and secondary transmissions subject to power allocation and lease time slot constraints. Numerical results confirmed that our proposed cooperative scheme significantly improves the secrecy rates of CRNs.

References

[1] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153-3167, May 2011.

[2] E. Tekin and A. Yener, "The general Gaussian multiple access and two way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

[3] K. Lee, C. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, Nov. 2013.

[4] Z. Chu, K. Cumanan, Z. Ding, M. Johnston and S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative Jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, May 2015.

[5] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. (Sherman) Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, Mar. 2013.

[6] L. Dong, H. Yousefizadeh and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," *Proc. IEEE International Conf. Communications (ICC)*, 2011.

[7] Q. Ma and C. Tepedelenlioglu, "Antenna selection for space-time coded systems with imperfect channel estimation," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 710-719, Feb. 2007.

[8] H. Xing, L. Liu and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, no. 99, Jan. 2015.

[9] H. Koorapaty, A. A.Hassan and S. Chennakeshu, "Secure information transmission for mobile radio" *IEEE Commun. Lett.*, vol. 4, no. 2, Feb. 2000.