IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PERFORMANCE IMPROVEMENT IN COGNITIVE RADIO NETWORKS

S.Veeralakshmi2 , C.Vennila[1]

[#1] *Professor, Department of ECE,Saranathan College of Engineering,Trichy,India.*

[#2] *PG Student,Departmentof ECE, Saranathan College of Engineering, Trichy,India.*

Abstract: Secure wireless communications is very important to environmental and military concerns. This project investigates that the energy efficiency and secrecy performance of cognitive radio networks (CRNs), where primary and secondary users with different priorities of spectrum access can either interfere or cooperate with each other. Focusing on several key aspects that may have potential impacts on secure underlay CRNs, including the transmission power, the number of interfering users, and the designed interference resistance coefficient. Based on analytical results, propose a cooperative spectrum sharing paradigm to improve both the secrecy throughput and the energy efficiency of primary users. The main idea is that primary users allow secondary users to simultaneously access the licensed spectrum and in return, the secondary transmitter acts as both a relay for primary transmissions and a friendly jammer against eavesdropping, in case the primary transmission fails. fails. Both theoretical and numerical results reveal that: (i) When the interference from secondary transmitters is small, there is an optimal transmission power that maximizes the secrecy throughput for primary users compared to CRNs without the security issue; (ii) When the interference from secondary transmitters is large, the secrecy throughput increases with the transmission power for primary users ; (iii) The transmission power that maximizes the energy efficiency is smaller than that maximizes the secrecy throughput for primary users; (iv) The number of interfering users has a slight impact on the secrecy throughput and the energy efficiency of primary users due to the secondary power control; (v) The proposed cooperative paradigm is an efficient approach to boost both the secrecy throughput and the energy efficiency of primary users compared with the traditional non-cooperative spectrum sharing, and provides an alternative method to compensate for the interference caused by secondary users.

I. INTRODUCTION

Physical layer security has recently emerged as a key pillar to provide reliability and trustworthiness for wireless communications due to the broadcast characteristic of wireless channels. Cognitive radio technology has been identified as an extraordinary tool to improve the energy efficiency of wireless networks. Cognitive techniques mainly include spectrum sharing , spectrum sensing and dynamic spectrum access which are beneficial for the network performance of spectral efficiency, network security and energy efficiency. On the other hand cooperative techniques such as cooperative relaying , cooperative jamming and jointly cooperative relaying and jamming have been proven to achieve improvements in wireless network performance, especially in terms of the energy efficiency and the secrecy performance. Combining cognitive radio technology with cooperative techniques can further enhance the network performance with SUs acting as relays or friendly jammers for primary users (PUs). Costa and Ephremides improved the throughput and the energy efficiency of PUs by employing SUs to relay primary for PUs. Although some works have been done for CRNs with cooperative techniques, taking both secrecy and

energy performance into account, most of previous works concentrated on SUs with maximizing energy efficiency under the secrecy constraint and vice versa.

Harvesting energy from radio frequency (RF) signals, radiated by transmitters in the environment, is an effective technique to enhance the lifetime of energy limited wireless networks. On the other hand, RF signals have been widely used for wireless information transmission. Simultaneous wireless information and power transfer (SWIPT) combines both these functions by using the same emitted RF signal to transfer both energy that can be harvested at the receiver and information that can be decoded by the receiver, and thus, possibly increases operational efficiency. The idea of SWIPT was first studied the fundamental trade-off between the rates at which energy and reliable information can be transferred simultaneously over a noisy channel. However, they assumed that the operations of information decoding and power extraction can be performed at the receiver, without proposing a practical receiver for doing so. Thereafter, proposed a power splitting (PS) based receiver as a practical solution for implementing SWIPT.

In a CRN employing SWIPT for energy harvesting, the amount of energy harvested by a secondary receiver (SR) can be increased by increasing the transmission power by the secondary transmitter (ST). However, in such a CRN the presence of eavesdroppers will increase the information leakage, as transmitting with higher power makes the transmitted information more susceptible to eavesdropping. Moreover, the ability of the SR nodes to sense the surrounding RF environment makes it easier for any malicious SR node to launch attacks.

APPLICATIONS

- The application of CR networks to emergency and public safety communications by utilizing white space
- The potential of CR networks for executing dynamic spectrum access (DSA)
- Application of CR networks to military action such as chemical biological radiological and nuclear attack detection and investigation, command control, obtaining information of battle damage evaluations, battlefield surveillance, intelligence assistance, and targeting.

In terms of two new challenges arise. First, how to design a cooperative paradigm to achieve high energy efficiency and secrecy throughput of PUs whose performance should be preferentially guaranteed in CRNs allowing the interference among users with different priorities to access the spectrum. Second, what are the pivotal system parameters affecting the performance of Pus. To address these questions, first derive analytical expressions of the secrecy throughput and the energy efficiency for both primary and secondary users by capturing the relationship between the transmission power of PUs and that of SUs, as well as reveal the impacts of system parameters on the underlay network's performance. Second, based on the analytical results of the network characteristics, propose a novel cooperative spectrum sharing scheme to further improve both the secrecy throughput and the energy efficiency of PUs.

CONTRIBUTIONS

Compared with [11–14] that solely thought-about the relay choice for DF-relaying CCRNs and [15] that only thought-about the intercept chance for single AF-relaying CCRNs, we tend to investigate the physical layer security in terms of the chance of non-zero secrecy capability, the secrecy outage chance, the secrecy array gain, and also the secrecy diversity order for multiple AF-relaying CCRNs with cooperative distributed beamforming within the presence of single and multiple non-colluding eavesdroppers, severally, where distributed zero-forcing beamforming (D-ZFB) is employed at the relays while not busybodied with the primary users.

We derive the closed-form expressions of the likelihood of non-zero secrecy capability and therefore the secrecy outage likelihood moreover because the straight line expression at high SNR regimes. Our straight line results accurately predict the secrecy diversity order of M AF relay CCRNs with cooperative distributed beamforming, i.e., $M - 1$, that is totally different from the results obtained in [11] and [13]. this can be because of the fact that the planned cooperative distributed beamforming scheme is meant at relays to avoid the interference at PUs at the expense of 1 spacial degree. additionally, numerical and simulation results are provided to verify the correctness of the planned scheme.

II . LITERATURE SURVEY

H. Lei el. at [1], consider a single-input multiple output cognitive wiretap system over generalized-K channels, where the eavesdropper overhears the transmission from the secondary transmitter (ST) to the legitimate receiver. Both the primary user and the ST are equipped with a single antenna, whereas the legitimate and the eavesdropper receivers are equipped with multiple antennas. Simulations are presented to validate the accuracy of our proposed analytical results. The closed-form expression for the SOP of SIMO CRN systems over KG fading channels is derived and Monte Carlo simulation results are presented to verify the proposed analytical results.

R.xie.[3] ,investigates the game theory based cooperation method to optimize the PHY security in both primary and secondary transmissions of a cognitive radio network (CRN) that include a primary transmitter (PT), a primary receiver (PR), a secondary transmitter (ST), a secondary receiver (SR) and an eavesdropper (ED). In CRNs, the primary terminals may decide to lease its own given bandwidth for a fraction of time to the secondary nodes in exchange for appropriate remuneration. Consider ST as a trusted relay for primary transmission in the presence of the ED. The ST forwards the source message in a decode-and-forward (DF) fashion and, at the same time, allows part of its available power to be used to transmit an artificial noise (i.e., jamming signal) to enhance secrecy rates and avoid the employment of a separate jammer. In order to allocate power between message and jamming signals, formulate and solve optimization problem of maximizing the primary secrecy rate (PSR) and secondary secrecy rate (SSR).

Y. wu [4], study the problem of secrecy wireless information and power transfer in a cognitive relay network (CRN), where a secondary transmitter (ST) aids the signal transmission from a primary transmitter (PT) to a primary receiver (PR), while it also transmits its own signal to a second receiver (SR). Both PR and SR decode information and harvest energy from the received signals based on a power splitting strategy. Due to the open architecture of a CRN, the information for SR is prone to be eavesdropped by PR. This letter aims to minimize the transmit power at ST while guaranteeing minimum information rates and the amounts of harvested energy at PR and SR, and constraining the potential eavesdropping rate at PR. Also [5] B. Han, where involve multiple source-destination pairs and malicious eavesdroppers. By characterizing the security performance of the system by secrecy capacity, we study the secrecy capacity optimization problem in which security enhancement is achieved via cooperative relaying and cooperative jamming. Specifically, we propose a system model where a set of relay nodes can be exploited by multiple source-destination pairs to achieve physical layer security. We theoretically present a corresponding formulation for the relay assignment problem and develop an optimal algorithm to solve it in polynomial time.

In those Some works have been done to study the energy efficiency in Cognitive Radio Networks (CRNs). Specifically, Ghorbel et al. proposed a joint adaptive power allocation and dynamic spectrum access technique to account for cross-layer couplings and power consumption. In Haider et al. analyzed the required energy to achieve a specific spectral efficiency for secondary users (SUs) with the transmission power constraint. An energy-efficient traffic scheduling scheme for SUs was developed by adapting secondary transmissions to the change of primary traffic. Mili et al. jointly maximized the capacity and minimized the transmission power of SUs to bring the energy efficiency enhancement to SUs. Cooperative techniques such as cooperative relaying ,cooperative jamming, and jointly cooperative relaying and jamming have been proven to achieve improvement in wireless network performance ,in terms of energy efficiency and secrecy performance.

III. PROPOSED SYSTEM

The main idea is that one SU may transmit simultaneously with the PU at the cost of acting as both a relay for primary transmissions and a friendly jammer against the eavesdropper, in case the primary transmission fails. Intuitively, the secrecy throughput of PUs can be enhanced with the help of a friendly jammer; and the improvement in the energy efficiency of PUs can be achieved through exploiting the transmission power of the secondary transmitter to relay primary packets.

PROPOSED SYSTEM MODEL (Analytical Expressions of the Secrecy Throughput and the Energy Efficiency**)**

First elaborate on the network model, followed by the transmission model. Then we describe the secure encoding. Finally, we introduce two performance metrics.

NETWORK MODEL

We denote (S-D) as a source and destination pair. A multi-user CRN, as depicted in Fig. 1, consists of one primary source and destination pair (S1-D1), (N1) secondary source and destination pairs (Si-Di) with i = 2, · · · , N, and one passive eavesdropper E0. All users are equipped with a single antenna. Besides, we assume that all secondary pairs share one channel of bandwidth W that is licensed to the primary pair. Normally, the PU has a higher priority to access the spectrum, and SUs have opportunistic access to the spectrum without affecting primary transmissions. This project adopts the underlay spectrum sharing scheme, i.e., SUs can access the licensed spectrum of the PU as long as SUs control their transmission power within an acceptable level at the primary receiver side.

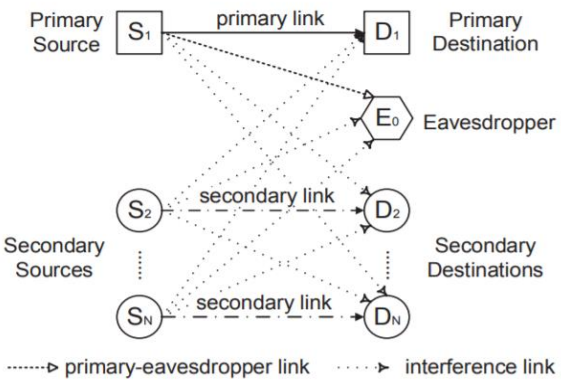


Fig. 1: Network model with underlay CRNs.

We assume that the receiver side has the global channel state information (CSI), legitimate transmitter side has the statistical CSI of the legitimate receiver, and only the statistical CSI of the eavesdropper is available at the legitimate transmitter, which is very generic and has been widely-adopted in the literature. In practice, this corresponds to, for example, the scenario where the eavesdropper was a legitimate user of the network previously but it becomes a passive eavesdropper at present. Besides, in the passive eavesdropper scenario, the eavesdropper aims at interpreting the transmitted information without trying to modify it or misleading legitimate users, and legitimate users do not receive or trust any feedback from the passive eavesdropper. Time is divided into slots of equal length, which is assumed to be 1, and only one packet is allowed to be transmitted by each user in a time slot. We assume there are sufficient packets for transmission. Hence, PU has random access to the spectrum, and the primary source S1 transmits a packet with probability $\tau 1$, $0 \leq \tau 1 \leq 1$, in each time slot. The i-th secondary source transmits a packet with probability τi (i = 2, · · · , N), $0 \leq \tau i \leq 1$, in each time slot. We assume $\tau i = \tau 2$ for i = 2, · · ·, N to simplify the calculation.

TRANSMISSION MODEL

The transmission power is P1 at the primary transmitter S1 and Pi at the secondary transmitter Si , where we assume Pi = P2 for i = 2, · · · , N. A unified channel model subjects to Rayleigh fading and standard path loss is adopted. Specifically, given the transmission power Pi at transmitter Si , the received power Pij at receiver Dj can be expressed as

$$P_{ij} = P_i h_{ij}^2 d_{ij}^{-\alpha}, \quad d_{ij} > 1,$$

where dij denotes the distance between Si and Dj , $\alpha > 2$ is the path loss exponent, and hij is the channel gain between Si and Dj , which follows a Rayleigh distribution with probability density function (pdf) given by

$$f_{h_{ij}}(x) = \frac{x}{\beta_{ij}} \exp\left\{ -\frac{x^2}{2\beta_{ij}} \right\}, \quad x \geq 0.$$

The successful transmission from source Si to destination Di embodies that both successful connection and secrecy of (Si-Di) are achieved:

Connection, where the received signal at Di can be decoded with an arbitrarily small error if Rt,i is less than the capacity of (Si-Di).

Secrecy, where the received signal at eavesdropper E0 provides no information about transmitted messages if the capacity of the eavesdropping link (SiE0) is less than Rt,i − Rs,i.

According to the Shannon formula, the connection probability of (Si-Di), denoted by piic, is expressed as

$$p_{iic} = \mathbb{P}\left(\log_2(1+\gamma_{ii}) > R_{t,i} \right) = \mathbb{P}(\gamma_{ii} > \varphi_i),$$

Where, $\phi i = 2R_{t,i} - 1$. The secrecy probability of (Si-Di) denoted by piis, is expressed as

$$p_{iis} = \mathbb{P}\left(\log_2(1+\gamma_{i0}) < R_{t,i} - R_{s,i} \right) = \mathbb{P}(\gamma_{i0} < \varphi_{i0})$$

where $\phi i0 = 2Rt,i-Rs,i - 1$. The connection probability gives a measure of the reliability level, while the secrecy probability provides a measure of the security level. Therefore, the definition of successful transmission can be determined by the received SINRs at destination Di and eavesdropper E0.

Successful Transmission

A transmission from source Si to destination Di is said to be successful if $\gamma ii > \phi i$ and $\gamma i0 < \phi i0$ ($\phi i0 < \phi i$), where γii and $\gamma i0$ denote the received SINRs at the primary/secondary receiver and the eavesdropper respectively ϕi and $\phi i0$ denote the corresponding threshold SINR values.

Accordingly, successful transmission probability characterizes the joint security and reliability performance. When the transmission power is not a random variable, the connection dx independent. Then we have the following definition. Successful transmission probability characterizes the probability that the confidential messages are reliably and securely transmitted from Si to the intended Di , which is given by

$$p_{ii} = \mathbb{P}\{\gamma_{ii} > \varphi_i, \gamma_{i0} < \varphi_{i0}\} = p_{iic} \cdot p_{iis}.$$

PERFORMANCE METRICS

ICS

In the performance metrics defines as the secrecy throughput and the energy efficiency. The secrecy throughput is defined as the number of message bits transmitted per second by the source. The energy efficiency is defined as the number of message bits transmitted per Joule by each pair of (S-D).

Secrecy Throughput

For a pair of (Si-Di) (i = 1, · · · , N), given the confidential message rate Rs,i of Si , the transmission probability τi of Si and the successful transmission probability pii, the secrecy throughput Ci .

Energy Efficiency

For a pair of (Si-Di) (i = 1, · · · , N), if Si transmits packets with power Pij within a fraction of time ij (P j ij = 1, j = 1, 2, 3 · · ·), the energy efficiency ηi is defined as

$$\eta_i = \frac{C_i}{\sum_j \epsilon_{ij} P_{ij}} \quad \text{(bits per Joule (bpJ))}$$

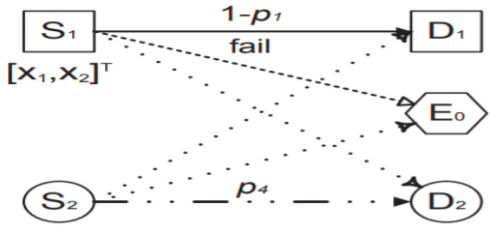
IV . PERFORMANCE ANALYSIS OF COOPERATIVE SPECTRUM SHARING SCHEME:

On the analysis of the secrecy throughput and the energy efficiency by employing a cooperative spectrum sharing scheme. Different from the traditional underlay spectrum sharing scheme that SUs can access the licensed spectrum as long as the secondary power is below a prescribed threshold, the cooperative spectrum sharing refers to that the PU allows one SU to simultaneously access the licensed spectrum, and as compensation for their interference, the SU cooperates with PUs to improve the performance of PUs. Here, the primary pair allows the secondary source to transmit packets simultaneously in each time slot, and the secondary source works as both a relay for primary transmissions and a friendly jammer against the eavesdropper, in case the primary transmission fails. In this work, we restrict our analysis to a simple cooperative mechanism, without the strategy of selecting the cooperative secondary pair.

First of all, we introduce the cooperative spectrum sharing scheme, followed by the performance analysis of both primary and secondary users. Finally, we provide the performance comparison between cooperative and non-cooperative schemes.

Cooperative Spectrum Sharing Scheme:

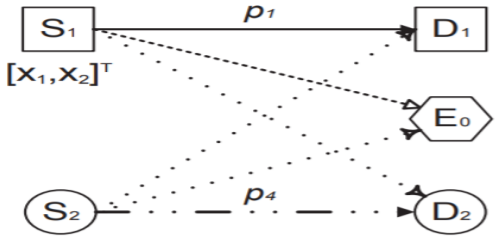
The primary transmission is described as follows. In each time slot, the primary pair and secondary pair transmit simultaneously, and the secondary source relays and protects the primary packet as a repayment for its caused interference. Error-free acknowledgment messages are assumed to be available to users through a control channel of negligible bandwidth. If primary destination D1 fails to receive the primary packet, the frame of the cooperative spectrum sharing scheme is triggered. (Corresponding to Fig. 2 (a)).



(a) Initial State

Fig. 2: Cooperative network model with underlay spectrum sharing scheme.

Specifically, in each frame of the cooperative scheme, S1 retransmits each packet until either D1 or the secondary relay S2 receives the primary packet successfully.



If D1 successfully receives the primary packet, the primary transmission ends. (Corresponding to Fig. 2 (b)).

If S2 receives the primary packet successfully before D1, S1 randomly rotates and changes the form of symbols in pre-crypto-coding matrix.

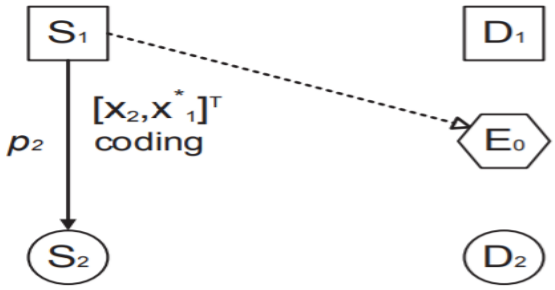


Fig. 2 (c1) p2 ≥ p1 phase2

Cooperative network model with underlay spectrum sharing scheme.

Then S2 encodes one pair symbols (two consecutive symbols) of the changed primary packet through a secure Alamouti Space-Time Block Coding (STBC). (Corresponding to Fig. 2 (c1)).

Then in the next time slot, S1 and S2 simultaneously transmit the changed and encoded primary packets to D1 until D1 successfully receives the packet, as shown in Fig. 2. Here perfect synchronization is assumed between S1 and S2. Although both S1 and S2 transmit simultaneously, they do not interfere with each other. The reason is that the Alamouti STBC constructs a packet that is orthogonal to the changed packet.

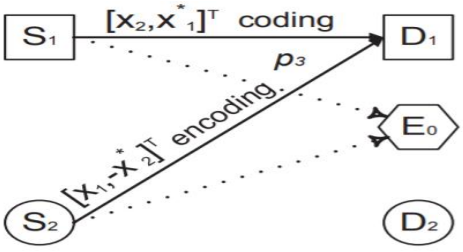


Fig. 2 (c2) p2 ≥ p1 phase2

Cooperative network model with underlay spectrum sharing scheme.

Besides, D1 is assumed to know the channel gains s11 and s21, and the rotation operation given by S1. (Corresponding to Fig. 2 (c2)).

If the original primary packet is [x1, x2] T and S2 receives the primary packet successfully before D1, the changed primary packet transmitted from S1 to S2/D1 is [x2, x∗1] T , and the encoded packet by the Alamouti STBC from S2 to D1 is [x1, x∗2] T , where · T and ·∗ denote transposition and conjugation, respectively. Since the changed primary packet [x2, x∗1] T from S1 to D1 and encoded primary packet [x1, x∗2] T from S2 to D1 are mutually orthogonal, simultaneous transmissions do not interfere with each other.

The rotated estimation of the original primary packet and the encoded estimated of the changed primary packet are regarded as noise at the eavesdropper E0, so the corresponding SINR at E0 is 0. However, D1 receives the primary packet by rotating channel matrix according to the pre-known rotation given by S1. Hence the SINR at D1 is

If the original primary packet is [x1, x2] T and S2 receives the primary packet successfully before D1, the changed primary packet transmitted from S1 to S2/D1 is [x2, x∗1] T , and the encoded packet by the Alamouti STBC from S2 to D1 is [x1, x∗2] T , where · T and ·∗ denote transposition and conjugation, respectively. Since the changed primary packet [x2, x∗1] T from S1 to D1 and encoded primary packet [x1, x∗2] T from S2 to D1 are mutually orthogonal, simultaneous transmissions do not interfere with each other.

$$\gamma_{11}^{c} = \frac{P_1 s_{11} + P_2 s_{21}}{\sigma^2}$$

V. SIMULATION RESULTS AND DISCUSSION

According to the Shannon formula, the connection probability detection the initialized signal shown below. Without loss of generality, we assume that $\phi 1 = \phi 2 = 0.4$, and $\phi 10 = \phi 20 = 0.1$. The confidential message rates of both primary and secondary sources are assumed to be same with 1, e.g., $Rs,1 = Rs,2 = 1$. Moreover, we assume all channel gain $\lambda ij = 1$ and $\sigma\ 2 = 1$. The interference resistance coefficient $\kappa = 0.8$ and $\tau 1 = \tau 2 = 0.5$. In addition, given the statistical CSI and the interference resistance coefficient κ, the transmission power P1 is determined by φ based on equation, and the maximum transmission power P max 2 is determined by P1 based on equation. Therefore, we change the transmission power for both PUs and SUs with φ in (0, 1).

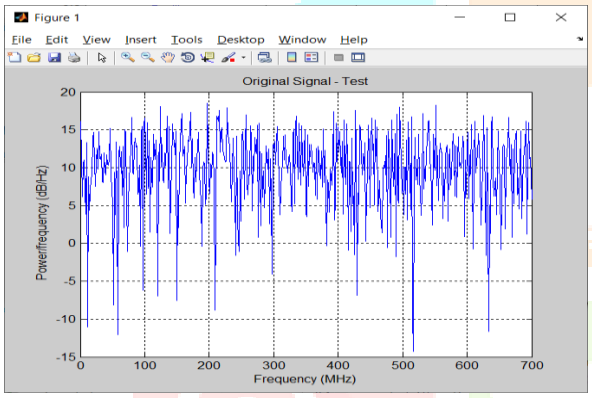


Fig.3. Input Signal

Let C(Rt,I, Rs,i) denote the set of all possible Wyner codes, where Rt,I is the rate of the transmitted codewords and Rs,I is the rate of the confidential messages with Rs,I< Rt,i. The rate difference Rt,I–Rs,I reflects the cost of securing the message against eavesdropping.

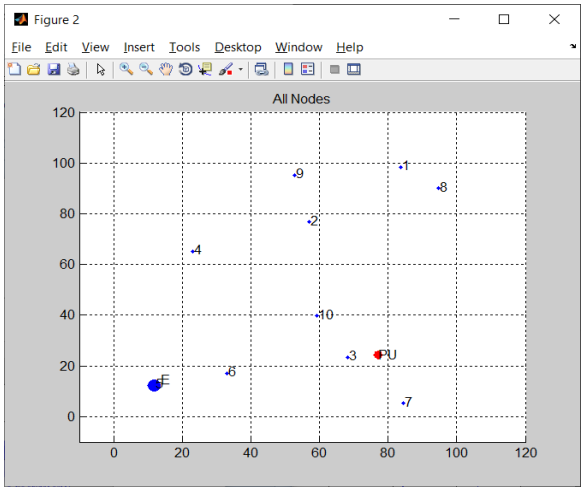


Fig.4. CRN Network Model

We denote (PU-(1-10)) as a source and destination pair. A multi-user CRN, as depicted in Fig., consists of one primary source and destination pair (S1-D1), (N1) secondary source and destination pairs (Si-Di) with i = 2, · · · , N, and one passive eavesdropper E0(E). All users are equipped with a single antenna. Besides, we assume that all secondary pairs share one channel of bandwidth W that is licensed to the primary pair. Normally, the PU has a higher priority to access the spectrum, and SUs have opportunistic access to the spectrum without affecting primary transmissions.

The successful transmission from source Si to destination Di embodies that both successful connection and secrecy of (Si-Di) are achieved

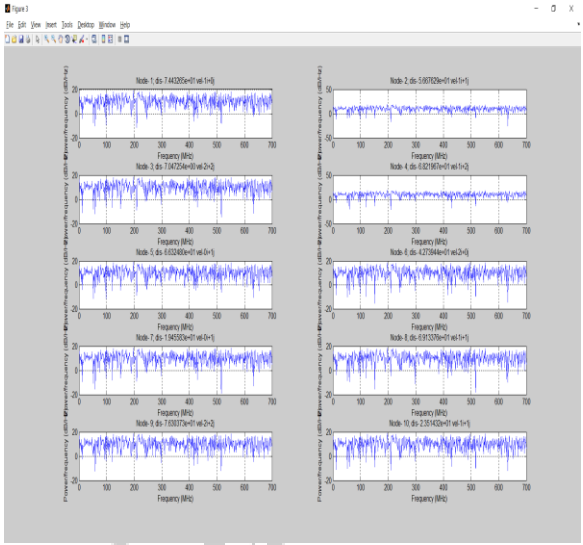


Fig.5. Successful Transmission

- **Connection**, where the received signal at Di can be decoded with an arbitrarily small error if Rt,i is less than the capacity of (Si-Di);
- **Secrecy**, where the received signal at eavesdropper E0 provides no information about transmitted messages if the capacity of the eavesdropping link (SiE0) is less than Rt,i − Rs,i.

A transmission from source Si to destination Di is said to be successful if γii>ϕi and γi0 < ϕi0 (ϕi0 <ϕi), where γii and γi0 denote the received SINRs at the primary/secondary receiver and the eavesdropper respectively; ϕi and ϕi0 denote the corresponding threshold SINR values.

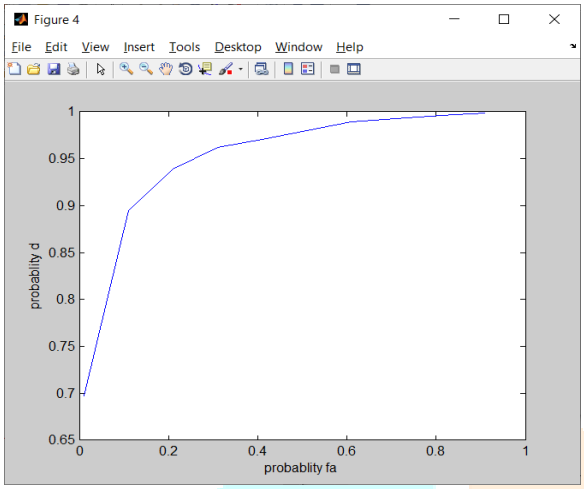


Fig.6. Probability Detection and False Alarm

A pair (S-D) is active if S transmits packets to D. When k secondary pairs are active in one time slot, we denote the connection probability, secrecy probability and successful transmission probability of the primary pair as p (k) 11c , p (k) 11s and p (k) 11 respectively.

Specifically, in each frame of the cooperative scheme, S1 retransmits each packet until either D1 or the secondary relay S2 receives the primary packet successfully.

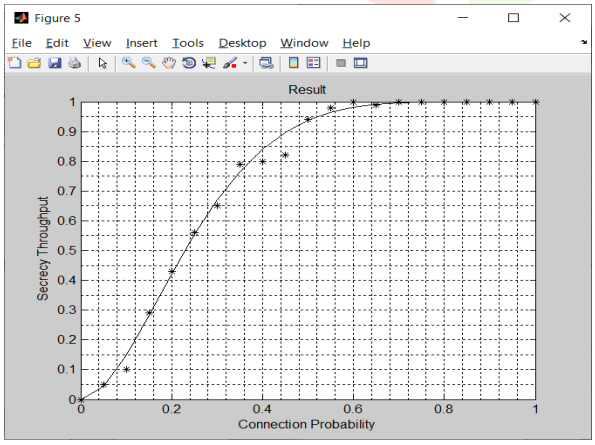


Fig.7. The secrecy throughput of the primary pair

The effect of primary transmission power on the secrecy throughput and the energy efficiency of the primary pair.

a) > (u/v) N−1 . Note that when wireless channels and the number of users are fixed, the relation between (1 + a) and (u/v) N−1 can be adjusted by P2 and τ2 etc.

Fig. plot the secrecy throughput of primary and secondary users, respectively, with $0 \le \tau1 < 1$ or $0 \le \tau2 < 1$, taking both non-cooperative and cooperative spectrum sharing scheme.

The secrecy throughput of PUs employing the cooperative scheme outperform those without cooperation when $0 \le \tau1 < 1$ or $0 \le \tau2 < 1$ (taking $\tau1 = \tau2 = 0.5$ for an example). As both C1 and η1 are increasing functions of τ1 and τ2, C1 and η1 in the case of $\tau1 = \tau2 = 1$ are larger.

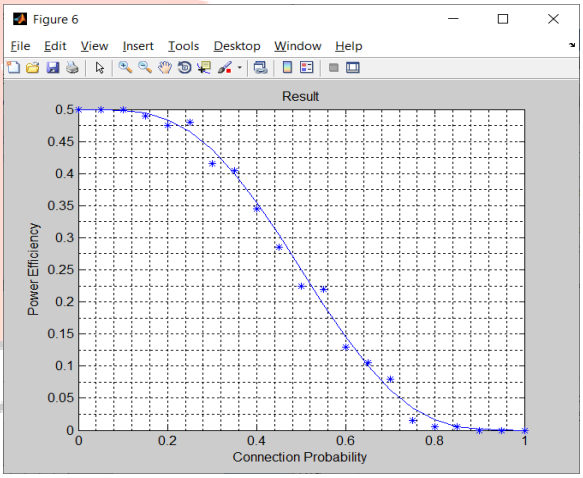


Fig.8. The energy efficiencyof the primary pair

Fig. plot the energy efficiencyof primary and secondary users, respectively, with $0 \le \tau1 < 1$ or $0 \le \tau2 < 1$, taking both non-cooperative and cooperative spectrum sharing scheme.

The energy efficiencyof PUs employing the cooperative scheme outperform those without cooperation when $0 \le \tau1 < 1$ or $0 \le \tau2 < 1$ (taking $\tau1 = \tau2 = 0.5$ for an example). As both C1 and η1 are increasing functions of τ1 and τ2, C1 and η1 in the case of $\tau1 = \tau2 = 1$ are larger.

Besides, smaller τ1 and τ2 lead to a smaller critical connection probability φ^{-}. If $\varphi > \varphi^{-}$, the energy efficiency

of SUs using the cooperative scheme outperforms that without cooperation, and vice versa.

The both output show the transmission power that maximizes the energy efficiency is smaller than that maximizes the secrecy throughput for primary users;The number of interfering users has a slight effect on the secrecy throughput and the energy efficiency of the primary pair due to the secondary power control; The proposed cooperative scheme is beneficial for the secrecy throughput and the energy efficiency of theprimary pair, and can be employed to compensate for the interference caused by secondary users.

VI.CONCLUSION

This project first studied the tradeoff between the secrecy throughput and the energy efficiency in CRNs, allowing the interference among users. Specifically, in CRNs without cooperation, we derived the secrecy throughput and the energy efficiency for both primary and secondary users, as well as explored the impacts of system parameters, such as the transmission power, the number of interfering users and the defined interference resistance coefficient on the network performance. Then based on the analytical results, we further proposed a cooperative spectrum sharing scheme to enhance both the secrecy throughput and the energy efficiency of the primary pair.

Our work provides a tractable analytic framework to explore the tradeoffs associated to the energy efficiency or the secrecy throughput in CRNs. Our results provide insights on how system parameters affect the network performance, and shed light on the design of energy-efficient secure primary networks. Future works include more practical network models, such as positive attacks, and more comprehensive cooperative schemes, such as an efficient strategy to select the secondary relay. We also think it is an interesting direction to study large-scale networks.

REFERENCES:

[1] H. Lei, H. Zhang, I. Ansari, G. Pan, and Qaraqe, “Secrecy outage analysis for simo underlay cognitive radio networks over generalized-fading channels,” IEEE Signal Process. Lett., vol. 23, no. 8, pp. 1106–1110, 2016.

[2] D. Wang, B. Bai, W. Chen, and Z. Han, “Achieving high energy efficiency and physical-layer security in af relaying,” IEEE Trans. Wireless Commun., vol. 15, no. 1, pp. 740–752, 2016.

[3] R. Xie, F. Yu, and H. Ji, “Energy-efficient spectrum sharing and power allocation in cognitive radio femtocell networks,” in IEEE INFOCOM, Orlando, Florido, USA, Mar. 2012.

[4] H. Yue, M. Pan, Y. Fang, and S. Glisic, “Spectrum and energy efficient relay station placement in cognitive radio networks,” IEEE J. Sel. Areas Commun., vol. 31, no. 5, pp. 883–893, 2013.

[5] W. Wang, L. Chen, K. G. Shin, and L. Duan,“Secure cooperative spectrum sensing and access against intelligent malicious behaviors,” in IEEE INFOCOM, Toronto, Canada, May 2014

[6] M. B. Ghorbel, B. Hamdaoui, R. Hamdi, M. Guizani, and M. NoroozOliaee, “Distributed dynamic spectrum access with adaptive power allocation: Energy efficiency and cross-layer awareness,” in IEEE INFOCOM WKSHPS, Toronto, Canada, May 2014.

[7] Haider, C. Wang, H. Haas, E. Hepsaydir, X. Ge, and D. Yuan, “Spectral and energy efficiency analysis for cognitive radio networks,” IEEE Trans. Wireless Communi., vol. 14, no. 6, pp. 2969–2980, 2015.

[8] Ding, H. Yue, J. Liu, P. Si, and Y. Fang, “Energy-efficient secondary traffic scheduling with mimo beamforming,” in IEEE Globecom, SanDiego, CA, USA, Dec. 2015.

[9] M. Mili, L. Musavian, K. Hamdi, and F. Marvasti, “How to increase energy efficiency in cognitive radio networks,” IEEE Trans. Commun., vol. 64, no. 5, pp. 1829–1843, 2016.

[10] Abuzainab and A. Ephremides, “Energy efficiency of cooperative relaying over a wireless link,” IEEE Trans. Wireless Commun., vol. 11, no. 6, pp. 2076–2083, 2012.

[11] 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, 2011.

[12] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, “Secrecy capacity optimization via cooperative relaying and jamming for wanets,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 4, pp. 1117–1128, 2015.

[13] M. Costa and A. Ephremides, “Energy efficiency versus performance in cognitive wireless networks,”

IEEE J. Sel. Areas Commun., vol. 34, no. 5, pp. 1336–1347, 2016.

[14] Lee, C. B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," IEEE Trans. Veh. Technol., vol. 62, no. 9, pp. 4672–4678, 2013.

[15] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," IEEE Trans. Wireless commun., vol. 13, no. 2, pp. 1058–1073, 2014.