Comprehensive Analysis of Secure Communication for Untrusted MISO Cognitive Radio Networks

Nikhil Ranjan
Ph.D. Scholar
SRK University, Bhopal

Dr. Bharti Chourasia
Associate Professor
SRK University, Bhopal

Abstract

The utilization of spectrum and secured communication in Cognitive radio network is big issue. The cognitive radio network used unlicensed spectrum for the process of communication. The mode of communication proceeds in three ways such as underlayer, overlay and joint form of underlayer and overlayer. The transmitter and receiver in these layers are combination of multiple input and single output. The process of security deals with physical layer of network. Beamforming is important methods of cognitive radio network design for the maximize the profit of secondary users. It also maintains the quality of service of primary users. In this paper study and analysis of secure communication and beamforming for cognitive radio networks (CRNs). Also, analysis of different models of CRNS and algorithms in terms of power utilization and spectrum allocation for secondary users to primary users. In the process of review finds some beamforming algorithms and finds some objective and direction in the area of cognitive radio networks

Keywords: CRNs, OFDM, MISO, Untrusted Channel Cooperative Communication, wireless, SDN

I. INTRODUCTION

Enhancement of spectrum efficiency in wireless communication used the process of cognitive radio networks. The cognitive radio network provides the facility of sharing of network to primary user to secondary users. In general, there are three models of cognitive radio networks (CRNs): interweave, underlay, and overlay. In the interweave model, the SUs first sense the spectrum holes and then transmit over the bands where the PUs is absent. In the underlay model, the SUs simultaneously transmits with the PUs over the same spectrum, while maintaining the performance of primary transmission under an acceptable threshold. In the overlay model, the SUs aids the PUs transmission by cooperative relay communication in return for their own transmission [1, 2]. Note that the three models have their own advantages and disadvantages, and are applicable for different applications and services. The overlay model recently has become a hot topic since cooperative communication not only enhances the spatial reusability but also enlarges the coverage range. Moreover, user cooperation in CRNs can also help to provide more SU's access opportunities. Therefore, cooperative CRN has been a new paradigm to improve the spectral efficiency where PUs and SUs seek opportunities to cooperate with each other[8]. Specifically, SUs can help to relay the information from the primary transmitters to primary receivers, and in return have the opportunity to transmit their own information. The authors considered a CRN where an SU acts as a two-way relay to help two PUs to exchange information and super imposes its own messages along with the primary transmission. The discussed cooperative spectrum sharing in CRNs, where the SU is equipped with multiple antennas and the zero-forcing beamforming is used to prevent primary and secondary systems from interfering with each other[10].

Secure communication in CRNs has also been demand of device to device communication. In [12], the authors studied the secure communication between an SU pair in the presence of eavesdroppers under an interference constraint of a PU. Moreover, physical-layer security has been also considered as a method to seek cooperation between PUs and SUs to avoid information leakage to a third-party eavesdropper. Cooperation strategies imposed at SUs were proposed in [13,16], where the SUs are allowed to concurrently transmit with Pus by acting as friendly jammers to providing the secrecy. The authors of [17] studied the beamforming design when Sus attempt to transmit secure messages in the presence of a third-party eavesdropper without interfering with a PU. Another important security issue arises when SUs tries to eavesdrop PU's message without permission, since SUs may easily know PUs' transmission spectrum by spectrum sensing. The rest of paper organized as in section II discuss related work. In section III discuss the models of CRNs. In section IV discuss the experimental analysis and finally conclusion & future work in section V.

II. RELATED WORK

In this section discuss the related work in the area of secured communication in cognitive radio network. For the process of secured communication used various security algorithms in physical layers of cognitive radio networks. Some work describes along with their authors.

Zhang, Meng, and Yuan Liu Et al. [1] author study the secure beamforming design for a cognitive radio network (CRN), where a primary transmitter-receiver pair coexists with an untrusted secondary transmitter-receiver pair. Each pair is a multiple-input single-output (MISO) link. Author consider two transmission schemes, namely underlay scheme and cooperative scheme. For the underlay scheme, the secondary user (SU) is allowed to transmit simultaneously in the presence of the primary transmission. For the cooperative scheme, the secondary transmitter acts as a relay to forward the secrecy information of the primary transmission in exchange for its own transmission. For both schemes, the SU is untrusted and considered as a potential eavesdropper.

Jiang, Li Et al. [2] author focus on secure information transmission for the primary system when the secondary users (SUs) are the potential eavesdroppers. Author aim to jointly design power splitting and secure beamforming to maximize the secondary system data rate subject to the secrecy QoS requirement of the primary system and the secondary transmitter (ST) power constraint. To solve this non-convex problem, author discussed a two-stage optimization approach. Simulation results demonstrate that our discussed scheme achieves a significant transmission rate of the secondary system while provides a high secrecy rate for the primary system compared to the scheme without energy harvesting.

Yuan, Can Et al. [3] This work presents a joint beamforming scheme for secure communication in cognitive hybrid satellite-terrestrial network (HSTN). In this network, a multibeam satellite communication network termed as the primary network under the intercept of an eavesdropper shares spectrum with a terrestrial network termed as the secondary network. Specifically, by considering that the powers of both the primary and secondary transmitters are limited to the certain values, author aim to maximize the secrecy rate for the primary user (PU), while the quality-of-service (QoS) of the secondary user (SU) is satisfied, and set up a constrained optimization problem. Since the optimization problem is nonconvex and its solution is very difficult to be obtained, author discussed a reformulation technique to convert the objective function into a second order cone constraint.

Feng, Youhong Et al. [4] author investigate cooperative secure beamforming for simultaneous wireless information and power transfer (SWIPT) in amplify-and-forward (AF) relay networks. Author discussed a joint cooperative beamforming and energy signal (CB-ES) scheme for providing both secure communication and efficient wireless energy transfer. By considering colluding eavesdroppers with imperfect channel state information, author formulate an optimization problem for maximizing the secrecy rate between the source and the legitimate information receiver (IR) under both the power constraints at the relays and the wire-less power transfer constraint at the energy-harvesting receiver (ER). Since such a problem is nonconvex and hard to tackle, author discussed a two-level optimization approach that involves a one-dimensional search and the semi-definite relaxation (SDR) technique to solve this problem. The discussed robust scheme is compared to some other non-robust schemes, a cooperative beamforming and artificial noise (CB-AN) scheme and a perfect scheme.

Mekkawy, Tamer Et al. [5] joint beamforming alignment and suboptimal power allocation (Sub-OPA) for a two-way untrusted relay network is presented. Considering the link between users is established via only an untrusted relay because of either the shadowing fading or long distance between users, author utilize a destination-assisted-jamming (DAJ) technique to improve the security performance. In each time slot, a user transmits confidential signals and the other emits jamming signals simultaneously to prevent the untrusted relay from intercepting the confidential signals. Author design a novel beamforming to align the confidential signal to the subspace corresponding to the confidential transmission channel and direct the cooperative jamming signal towards untrusted relay.

Wang, Xiaoyan Et al. [6] This work investigates the secure communication issue for cognitive radio networks with non-altruistic users. The design objective is to improve the secrecy rate of the primary user, and meanwhile, create the transmission opportunities for the secondary users to satisfy their diversified Quality of Service (QoS) demands. To achieve this goal, author discussed a novel non-monetary trading model, where the users are incentivized to participate in the market by a barter-like resource-to-resource exchange. Specifically, the primary user leverages the assist of the secondary user in the form of cooperative forwarding or friendly jamming, and yields part of the spectrum accessing time to the aided secondary user. The discussed spectrum auction framework jointly formulates the optimal co-operator selection and the corresponding resource allocation problems, by taking into consideration the QoS demands of individual users.

Wang, Wei, Kah Chan Teh, and Kwok Hung Li Et al. [7] In this work, the security aspect of an amplify-and-forward (AF) relaying network with untrusted relay nodes is considered. The untrusted nodes can help to forward the received signal and they may also try to decode such information, which can be regarded as potential eavesdroppers (Eves). To deal with such a challenging issue, a successive relaying scheme is adopted, where the multi-antenna source transmits to two selected nodes alternately, and the conventional detrimental inter-relay interference is used to jam the untrusted nodes without external helpers. Considering different complexity requirements, several relay selection schemes are proposed, and the closed-form expressions of the lower bound of secrecy outage probability are derived accordingly.

Alsaba, Yamen, Sharul Kamal Abdul Rahim, and Chee Yen Leow Et al. [8] The objective of this work, is to point out the state-of-the-art research activity on beamforming implementation in EH wireless networks. Author first review the basic concepts and architecture of energy harvesting wireless networks. In addition, author also discuss the effects of beamforming transmission scheme on system performance in EH wireless communication. Furthermore, author present a comprehensive survey of multi-antenna EH

communications. Author cover the supporting network architectures like broadcasting, relay and cognitive radio networks with the various beamforming deployment within the network architecture.

Xiang, Zhongwu Et al. [9] This work investigates physical layer security (PLS) in cognitive radio inspired non-orthogonal multiple access (CR-NOMA) networks with multiple primary and secondary users. To manage the interferences among the users and guarantee the quality of services (QoS) of primary users, a new secure NOMA transmission strategy is designed, where the primary and secondary users are paired according to their channel gains, respectively, and power-domain NOMA is employed to transmit the signal.

Mekkawy, Tamer Et al. [10] the relay selection of two-way untrusted relays network is presented, and a directed beamforming is aligned to zero-force the transmission at all other non-selected relays. Particularly, author discussed a selection scheme based on max-min criterion, which require an exhaustive search. Then, the Lower Bound (LB) of the secrecy rate is introduced to minimize the complexity of the selection criterion. The closed forms of the Secure Outage Probability (SOP) for the max-min LB scheme is formulated and compared with other schemes. The simulations results validate the discussed analytical forms, and the performance of max-min LB scheme appears to be quite close to that of max-min scheme with limited complexity.

Wang, Xiaoyan Et al. [11] This work investigates the secure information transfer issue for cognitive radio networks that have multiple non-altruistic primary users, secondary users and eavesdroppers. The design objective is to improve the secrecy rates of the primary users, and create the transmission opportunities for the secondary users. To achieve this goal, author discussed to incentivize the non-altruistic users to cooperate by a barter-like exchange. Specifically, the primary users leverage the assist of the secondary users in the form of cooperative transmitting or friendly jamming, and in return, yield certain licensed spectrum accessing time to the aided secondary users. Author discussed a truthful Double Auction mechanism for Secure Information transfer in cognitive radio networks, namely DASI, to jointly formulate the co-operator/jammer assignment and the corresponding resource allocation problems. Author prove that DASI preserves nice economic properties that are critical for the auction design, including truthfulness, individual rationality and budget balance.

Qiao, Jingping Et al. [12] This work focuses on the secure transmission of wireless-powered full-duplex (FD) relay systems, where a multi-antenna source communicates with a single-antenna destination with the help of a FD relay in the presence of a single-antenna eavesdropper. It is assumed that the FD relay is wireless energy harvesting-enabled, adopting both transmit and receive antennas to harvest energy in a time switching (TS) mode. As the objective of this work is to maximize the system secrecy rate through jointly designing the energy beamforming vector, the information beam-forming vector and the TS coefficient, an optimization problem is formulated.

Wang, Dawei Et al. [13] Author study the cooperative secure transmissions in (multiple input signal output) MISO vehicular relay networks where the infrastructure node with multiple antennas sends two confidential messages to two legitimate vehicles with only one antenna, respectively. By exploiting the signal superposition and cooperative jamming techniques, the legitimate vehicle near the infrastructure node directly decodes its own messages and is also responsible for relaying messages for the other legitimate vehicle who is distant from the infrastructure node. To combat eavesdropping threat from a malicious node for these two legitimate vehicles, author first provide comprehensive analysis of the secrecy performances and then design optimal secure transmission schemes for both vehicles.

ElHalawany, Basem M., and Kaishun Wu Et al. [14] In this work, author study the outage probability and the secrecy outage probability in a two-users NOMA system at which the BS is pairing a legitimate/trusted user with another untrusted user due to the non-uniform distribution of trusted and untrusted users in the cell. Through the NOMA concept, author investigate the NOMA pair outage behaviour under secrecy outage probability constraint on the trusted user.

Yan, Peishun, YulongZou, and Jia Zhu Et al. [15] author consider an energy-harvesting underlay cognitive radio (CR) system, which is comprised of multiple cognitive users (CUs), a common cognitive base station (CBS) and multiple passive eavesdroppers (Es). When CUs transmit to CBS, Es may overhear the confidential transmissions from CUs. In the aforementioned system, all CUs are considered to be equipped with energy harvesters to collect energy from their surrounding environments. Meanwhile, the transmit power of CUs shall be limited by a tolerable interference temperature to guarantee the quality-of-service (QoS) of a primary user (PU).

Zeng, Weiliang, Yahong Rosa Zheng, and Chengshan Xiao Et al. [16] This work considers the precoder design for multi-antenna secure cognitive radio networks. Author use finite-alphabet inputs as the signalling and exploit statistical channel state information (CSI) at the transmitter. Author maximize the secrecy rate of the secondary user and control the transmit power and the power leakage to the primary receivers that share the same frequency spectrum. The secrecy rate maximization is important for practical systems, but challenging to solve, mainly due to two reasons: First, the secrecy rate with statistical CSI is computationally prohibitive to evaluate. Second, the optimization over the precoder is a non-deterministic polynomial-time hard (NP-hard) problem. Author utilize an accurate approximation of the secrecy rate to reduce the computational effort and then discussed a global optimization approach based on branch-and-bound method.

Zhang, Tao Et al. [17] author consider both half-duplex (HD) and full-duplex (FD) operations. For the HD, maximal-ratio combining (MRC) is adopted at Bob, while for the FD, author discussed two jamming schemes to deteriorate the quality of the eavesdropper's channel, i.e., selection combining/selection jammer (SC/SJ) and SC/zero forcing beamforming (SC/ZFB). Assuming Rayleigh fading, exact closed-form expressions for the secrecy outage probability of the cognitive wiretap network are derived.

Zhang, Meng, and Yuan Liu Et al. [18] author consider a cognitive radio network (CRN) consisting of a primary transmitter-receiver pair and an untrusted secondary transmitter-receiver pair, and each pair is a multiple-input single-output (MISO) link. Author consider

two transmission schemes, namely underlay scheme and cooperative scheme. For the underlay scheme, the secondary user (SU) is allowed to transmit simultaneously in the presence of primary transmission. For the cooperative scheme, the secondary transmitter acts as a relay node to increase the secrecy rate of primary transmission in exchange for its own transmission. For both schemes, the SU is untrusted and considered as a potential eavesdropper.

Qin, Mian Et al. [19] This work investigates the effect of multiuser gain provided by the secondary user selection on the secrecy performance of the primary users. author first discussed a simple scheme where the user with the minimal interference channel is selected, and derive a closed-form lower bound of the achievable ergodic secrecy rate (ESR) of the primary users. In the high signal-to-noise ratio (SNR) regime, asymptotic result shows that the multiuser gain scales logarithmically with the number of the secondary users for a fixed interference temperature. Inspired by non-orthogonal multiple access strategy, author then discussed a maximal jamming rate-based scheme, where the secondary with maximal interference channel is selected and it will transmit with an elaborately designed rate so that the primary receiver can cancel out the interference completely with successive interference cancellation. A closed-form expression of achievable ESR is also presented. Theoretical and simulation results show that the both discussed schemes can achieve multiuser gain and improve the security of the primary users significantly.

Zhang, Tao Et al. [20] In this work, author analyse the secrecy performance of multi-antenna cognitive wiretap network, where the secondary transmitter (Alice) communicates with the secondary receiver (Bob) in the presence of an eavesdropper (Eve). Specifically, author investigate the cases of maximal-ratio combining (MRC) with half-duplex (HD) and selection combining/Zero forcing beamforming (SC/ZFB) scheme with full-duplex (FD) operation, respectively. Assuming the Rayleigh fading, closed-form expressions for the secrecy outage probability of cognitive wiretap channels with MRC and SC/ZFB are derived.

III. SYSTEM MODEL

In the CR system based on OFDM, the frequencies that SU can access to may overlay some licensed frequencies allocation algorithm takes not only the transmitter power constraint into consideration, but also the interference constraint. We consider the resource allocation of a CR system with one PU and M $(m = 1,2, \ldots . M)$ SUs, but the proposed algorithm can be extended to situations with several Pus. Because we choose underlay as the spectrum access techniques, PU and SUs can access the same frequency at the same time [1,2,3]. As depicted in the figure, the available bandwidth is W Hz and is divided into $K(k = 1,2, \ldots . K)$ subcarriers each of which occupies $\Delta f = W_s Hz$. The PU occupies $W_P\ Hz$ among the total bandwidth. Since PU may not employ OFDM, the mutual interference (MI) between PU and SUs is necessary to be considered. The PU receiver locates randomly in a circle of protective field and within the area the interference cannot exceed the threshold l_{th}.

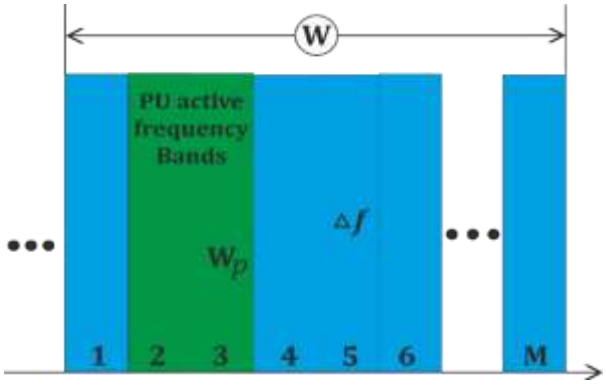


Figure 1: Primary User active frequency band diagram.

The power spectral density (PSD) of the kth subcarrier is modeled as

$$\Phi_k(f) = T_s\left(\frac{Sin\ (\pi f T_s)}{\pi f T_s}\right)^2 \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

The T_s is the symbol duration. The interference to the PU introduced by the k th subcarrier of m^{th} SU is

$$I_{m,k}(d_k, P_{m,k}) = P_{m,k} \int_{\frac{d_k - W_p}{2}}^{\frac{d_k + W_p}{2}} |g_{m,k}|^2 \Phi_k(f) df \ \ldots\ldots\ldots\ldots (2)$$

Where d_k, is the spectral distance between the k^{th} CR subcarrier and the PU band, $P_{m,k}$ is the transmit power of the k^{th} CR subcarrier occupied by m th SU and $g_{m,k}$ denotes the channel fading gain in the k^{th} subcarrier between the m^{th} SU transmit and the PU receiver. As to the interference caused by a PU to SUs, we regard it as white gauss noise in the signal processing.

We assume that the subcarriers change slowly with time and SU transmits have perfect channel state information (CSI). Then the maximum number of bits during an OFDM symbol transmitted on k^{th} subcarrier of the m^{th} SU is

$$b_{m,k} = \left\lfloor log_2 \left(1 + \frac{|h_{m,k}|^2 P_{m,k}}{\Gamma N_0 W_s}\right) \right\rfloor \dots\dots\dots\dots\dots\dots\dots\dots (3)$$

Where the symbol $\lfloor \blacksquare \rfloor$ denotes the flooring operation, $h_{m,k}$ is k^{th} channel gain of m^{th} SU, N_0 denotes the noise PSD and Γ is the single noise ratio (SNR) gap which present the SNR difference in Shannon capacity.

The object is to maximize the overall bit rate allocated SUs under the power, interference and fairness constraints. The optimization problem can be formulated as

$$\max \sum_{m=1}^{M} \sum_{k=1}^{K} x_{m,k}\, b_{m,k} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (4)$$

$$\text{s.t.} \sum_{k=1}^{K} x_{m,k} p_{m,k} < P_m, \forall\, m \in \{1, 2, \dots\dots, M\} \dots\dots\dots\dots\dots (5)$$

$$\sum_{m=1}^{M} \sum_{k=1}^{K} x_{m,k} p_{m,k}\, I_{m,k} < I_{th} \dots\dots\dots\dots\dots\dots\dots\dots (6)$$

$$x_{m,k} \in \{0, 1\}, \sum_{m=1}^{M} \sum_{k=1}^{K} x_{m,k} \leq 1, \forall k, m \dots\dots\dots (7)$$

$$R_1 : R_2 : \dots\dots\dots : R_M \approx \lambda_1 : \lambda_2 : \dots\dots\dots\dots : \lambda_M \dots\dots\dots\dots (8)$$

Where $x_{m,k}$ is an allocation indicator which indicates whether subcarrier k is allocated to SU m or notand guarantees that one subcarrier that one subcarrier can only be allocated to at most one SU. P_m is the transmit power constraint of the m th SU while I_{th} the total interference constraint. $R_m = \sum_{k=1}^{K} b_{m,k}$ is the number of bits allocated to SU m. Consider different quality of services (QoS) of SUs, λ_m is defined as the bit weight factor (BWF). $\frac{\lambda_m}{\sum_{i=1}^{M} \lambda_i}$ indicates the percentage of the bits allocated to SU m in total loaded bits. So, the equation (8) satisfied all QoS of all SUs.

IV. EXPERIMENTAL ANALYSIS

In this section validated the performance of secured beamforming communication for cognitive radio network. The validation and analysis of algorithms in four condition such as underlayer, cooperative, overlayer and joint. The process of simulation carried in MATLAB software. The variance of each entry of the channel responses is given by $\alpha_{i,j} = c \cdot d_{i,j}^{-n/2}$, where $d_{i,j}$ denotes the distance between receiver i and transmitter j, c is the attenuation constant set to be 1, meaning the received power at reference point is normalized to be 1; and n is the path loss exponent set to be 3. The noise power $\sigma^2$is set to be 1.

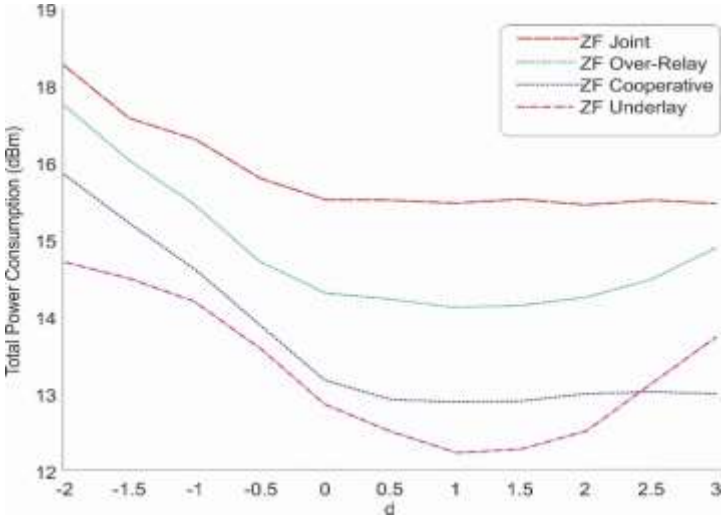


Figure 2: The total power consumption versus coordinate d of PU-Tx, where the PU-Tx, PU-Rx, SU-Tx and SU-Rx are placed at (d, 0), (1, 0), (0, 0) and (5, 0). In the above graph we can see the value of d is -2 to 3 on the x axis and total power consumption 12dBm to 19dBm with all schemes ZF-joint, ZF-Overlay, ZF-cooperative, ZF-underlay on the y-axis.

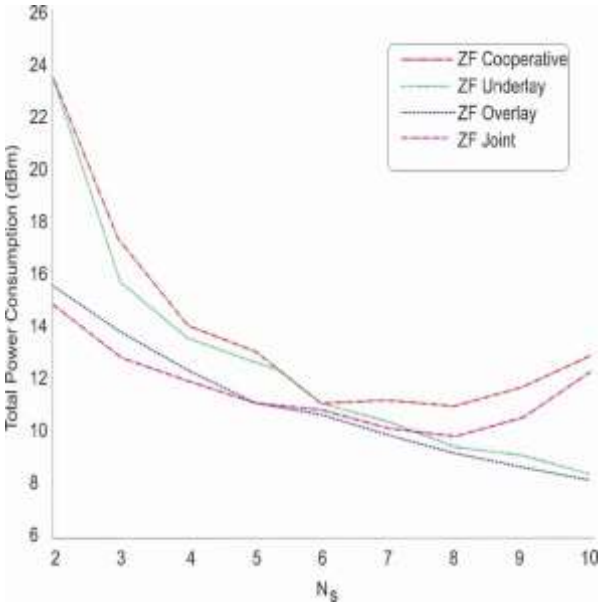
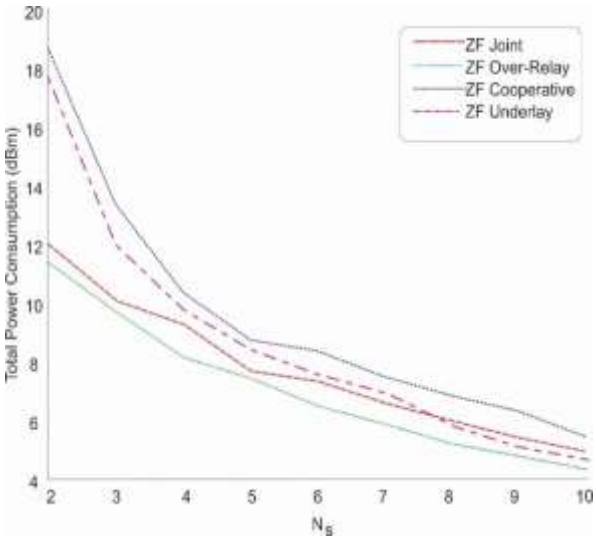


Figure 3: The total power consumption versus the number of antennas at SU-Tx Ns, where the PU-Tx, PU-Rx, SU-Tx and SU-Rx are placed at (âˆ’1, 0),(1, 0), (0, 0) and (5, 0). In the above graph we can see the value of N_S is 2 to 10 on the x axis and total power consumption 6dDm to 26dBm with all schemes ZF-joint, ZF-Overlay, ZF-cooperative, ZF-underlay on the y-axis.



The total power consumption versus the number of antennas at SU-Tx Ns, where the PU-Tx, PU-Rx, SU-Tx and SU-Rx are placed at (a1, 0),(1, 0), (0, 0) and (5, 0). In the above graph we can see the value of N_S is 2 to 10 on the x axis and total power consumption 4dDm to 20dBm with all schemes ZF-joint, ZF-Overlay, ZF-cooperative, ZF-underlay on the y-axis.

V. CONCLUSION & FUTURE SCOPE

In this paper, we have studied the secured communication for cognitive networks with multiple spectrum. in order to find out in which way we can enable an effective secured algorithm. Different power allocation algorithms were studied to discover which features are the most relevant to achieve a performance that higher efficiency.The cooperative communication is able to achieve NE distributing the power among the less interfered channels. Nevertheless, it needs a high computational effort in comparison to the other algorithms. In future used optimization technique for reduction of computational complexity. The optimization algorithms such as genetic algorithm, ant colony optimization and many more swarm-based algorithm.

References

[1]. Zhang, Meng, and Yuan Liu. "Secure beamforming for untrusted MISO cognitive radio networks." IEEE Transactions on Wireless Communications 17.7 (2018): 4861-4872.

[2]. Jiang, Li, et al. "Secure beamforming in wireless-powered cooperative cognitive radio networks." IEEE Communications Letters 20.3 (2016): 522-525.

[3]. Yuan, Can, et al. "Joint security beamforming in cognitive hybrid satellite-terrestrial networks." 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring). IEEE, 2016.

[4]. Feng, Youhong, et al. "Robust cooperative secure beamforming for simultaneous wireless information and power transfer in amplify-and-forward relay networks." IEEE Transactions on Vehicular Technology 66.3 (2016): 2354-2366.

[5]. Mekkawy, Tamer, et al. "Joint beamforming alignment with suboptimal power allocation for a two-way untrusted relay network." IEEE Transactions on Information Forensics and Security 13.10 (2018): 2464-2474.

[6]. Wang, Xiaoyan, et al. "A nonmonetary QoS-aware auction framework toward secure communications for cognitive radio networks." IEEE Transactions on Vehicular Technology 65.7 (2015): 5611-5623.

[7]. Wang, Wei, Kah Chan Teh, and Kwok Hung Li. "Relay selection for secure successive AF relaying networks with untrusted nodes." IEEE Transactions on Information Forensics and Security 11.11 (2016): 2466-2476.

[8]. Alsaba, Yamen, Sharul Kamal Abdul Rahim, and Chee Yen Leow. "Beamforming in wireless energy harvesting communications systems: A survey." IEEE Communications Surveys & Tutorials 20.2 (2018): 1329-1360.

[9]. Xiang, Zhongwu, et al. "Physical layer security in cognitive radio inspired NOMA network." IEEE Journal of Selected Topics in Signal Processing 13.3 (2019): 700-714.

[10]. Mekkawy, Tamer, et al. "Secure relay selection for two way amplify-and-forward untrusted relaying networks." IEEE Transactions on Vehicular Technology 67.12 (2018): 11979-11987.

[11]. Wang, Xiaoyan, et al. "DASI: A truthful double auction mechanism for secure information transfer in cognitive radio networks." 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 2015.

[12]. Qiao, Jingping, et al. "Joint beamforming and time switching design for secrecy rate maximization in wireless-powered FD relay systems." IEEE Transactions on Vehicular Technology 67.1 (2017): 567-579.

[13]. Wang, Dawei, et al. "Security provisioning for MISO vehicular relay networks via cooperative jamming and signal superposition." IEEE Transactions on Vehicular Technology 66.12 (2017): 10732-10747.

[14]. ElHalawany, Basem M., and Kaishun Wu. "Physical-layer security of noma systems under untrusted users." 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 2018.

[15]. Yan, Peishun, YulongZou, and Jia Zhu. "Energy-aware multiuser scheduling for physical-layer security in energy-harvesting underlay cognitive radio systems." IEEE Transactions on Vehicular Technology 67.3 (2017): 2084-2096.

[16]. Zeng, Weiliang, Yahong Rosa Zheng, and Chengshan Xiao. "Multiantenna secure cognitive radio networks with finite-alphabet inputs: A global optimization approach for precoder design." IEEE Transactions on Wireless Communications 15.4 (2016): 3044-3057.

[17]. Zhang, Tao, et al. "Secure multiantenna cognitive wiretap networks." IEEE Transactions on Vehicular Technology 66.5 (2016): 4059-4072.

[18]. Zhang, Meng, and Yuan Liu. "Joint secure beamforming for cognitive radio networks with untrusted secondary users." 2015 IEEE Global Communications Conference (GLOBECOM). IEEE, 2015.

[19]. Qin, Mian, et al. "Enhancing security of primary user in underlay cognitive radio networks with secondary user selection." IEEE Access 6 (2018): 32624-32636.

[20]. Zhang, Tao, et al. "Secure transmission in cognitive wiretap networks." 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring). IEEE, 2016.