Secure Communication in Relay Selection based on Cognitive Radio Systems

S. Nagarajan*, A. Nithya**, M. Nivetha***, P. Pooja Lakshmi**** & K. Priya Dharshini*****

*Assistant Professor, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
**UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
***UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
****UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
*****UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.

***Abstract*—**We consider a Cognitive Radio (CR) network consisting of a Secondary Transmitter (ST), a Secondary Destination (SD) and multiple Secondary Relays (SRs) in the presence of an eavesdropper, where the ST transmits to the SD with the assistance of SRs, while the eavesdropper attempts to intercept the secondary transmission. We rely on careful relay selection for protecting the ST-SD transmission against the eavesdropper with the aid of both single-relay and multi-relay selection. To be specific, only the "best" SR is chosen in the single-relay selection for assisting the secondary transmission, whereas the multi-relay selection invokes multiple SRs for simultaneously forwarding the ST's transmission to the SD. We analyze both the intercept probability and outage probability of the proposed single-relay and multi-relay selection schemes for the secondary transmission relying on realistic spectrum sensing. We also evaluate the performance of classic direct transmission and artificial noise based methods for the purpose of comparison with the proposed relay selection schemes. It is shown that as the intercept probability requirement is relaxed, the outage performance of the direct transmission, the artificial noise based and the relay selection schemes improves, and vice versa. This implies a trade-off between the security and reliability of the secondary transmission in the presence of eavesdropping attacks, which is referred to as the Security Reliability Trade-off (SRT). Furthermore, we demonstrate that the SRTs of the single-relay and multi-relay selection schemes are generally better than that of classic direct transmission, explicitly demonstrating the advantage of the proposed relay selection in terms of protecting the secondary transmissions against eavesdropping attacks. Moreover, as the number of SRs increases, the SRTs of the proposed single-relay and multi-relay selection approaches significantly improve. Finally, our numerical results show that as expected, the multi-relay selection scheme achieves a better SRT performance than the single-relay selection.

***Keywords*—**Cognitive Radio; Eavesdropping Attack; Intercept Probability; Relay Selection; Security-Reliability Trade-Off; Outage Probability.

***Abbreviations*—**Cognitive Radio (CR); Denial-of- Service (DoS); Secondary Destination (SD); Primary User Emulation (PUE); Secondary Relays (SRs); Security Reliability Trade-off (SRT); Secondary Transmitter (ST).

I. INTRODUCTION

THE security aspects of Cognitive Radio (CR) systems have attracted increasing attention from the research community. Indeed, due to the highly dynamic nature of the CR network architecture, legitimate CR devices become exposed to both internal as well as to external attackers and hence they are extremely vulnerable to malicious Behaviour. For example, an illegitimate user may intentionally impose interference (i.e. jamming) for the sake of artificially contaminating the CR environment. Hence, the CR users fail to accurately characterize their surrounding radio environment and may become misled or compromised, which leads to a malfunction. Alternatively, an illegitimate user may attempt to tap the communications of authorized CR users by eavesdropping, to intercept confidential information. Clearly, CR networks face diverse security threats during both spectrum sensing as well as spectrum sharing, spectrum mobility and spectrum management. Extensive studies have been carried out for protecting CR networks both against Primary User Emulation (PUE) and against Denial-of- Service (DoS) attacks. In addition to PUE

and DoS attacks, eavesdropping is another main concern in protecting the data confidentiality, although it has received less attention in the literature on CR network security. Traditionally, cryptographic techniques are employed for guaranteeing transmission confidentiality against an eavesdropping attack. However, this introduces a significant computational overhead as well as imposing additional system complexity in terms of the secret key management. Furthermore, the existing cryptographic approaches are not perfectly secure and can still be decrypted by an eavesdropper (E), provided that it has the capacity to carry out exhaustive key search with the aid of brute-force attack. Physical-layer security is emerging as an efficient approach for defending authorized users against eavesdropping attacks by exploiting the physical characteristics of wireless channels. In Leung-Yan-Cheong and Hellman demonstrated that perfectly secure and reliable transmission can be achieved, when the wiretap channel spanning from the source to the eavesdropper is a further degraded version of the main channel between the source and destination. They also showed that the maximal secrecy rate achieved at the legitimate destination, which is termed the secrecy capacity, is the difference between the capacity of the main channel and that of the wiretap channel. In the secrecy capacity limits of wireless fading channels were further developed and characterized from an information-theoretic perspective, demonstrating the detrimental impact of wireless fading on the physical layer security. To combat the fading effects, Multiple-Input Multiple-Output (MIMO) schemes as well as cooperative relaying and beam forming techniques were investigated for the sake of enhancing the achievable wireless secrecy capacity. Although extensive research efforts were devoted to improving the security of traditional wireless networks, less attention has been dedicated to CR networks. In the achievable secrecy rate of the secondary transmission was investigated under a specific Quality-of-Service (QoS) constraint imposed on the primary transmission. Additionally, an overview of the physical-layer security aspects of CR networks was provided in, where several security attacks as well as the related countermeasures are discussed. In contrast to conventional non-cognitive wireless networks, the physical-layer security of CR networks has to consider diverse additional challenges, including the protection of the primary user's QoS and the mitigation of the mutual interference between the primary and secondary transmissions. Motivated by the above considerations, we explore the physical-layer security of a CR network comprised of a Secondary Transmitter (ST) communicating with a Secondary Destination (SD) with the aid of multiple secondary relays (SRs) in the presence of an unauthorized attacker. Our main focus is on investigating the Security-Reliability Trade-off (SRT) of the cognitive relay transmission in the presence of realistic spectrum sensing. The notion of the SRT in wireless physical layer security was introduced and examined in, where the security and reliability was characterized in terms of the intercept probability and outage probability, respectively. In contrast to the conventional non-cognitive wireless networks studied in the SRT analysis of CR networks presented in this work additionally takes into account the mutual interference between the Primary User (PU) and Secondary User (SU). The main contributions of this paper are summarized as follows [Zou et al., 1; 2].

II. RELATED WORK

2.1. Principles of Physical Layer Security in Multiuser Wireless Networks

This paper provides a comprehensive review of the domain of physical layer security in multiuser wireless networks. The essential premise of physical layer security is to enable the exchange of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers, without relying on higher-layer encryption. This can be achieved primarily in two ways: without the need for a secret key by intelligently designing transmit coding strategies, or by exploiting the wireless communication medium to develop secret keys over public channels. The survey begins with an overview of the foundations dating back to the pioneering work of Shannon and Wyner on information-theoretic security. We then describe the evolution of secure transmission strategies from point-to-point channels to multiple-antenna systems, followed by generalizations to multiuser broadcast, multiple-access, interference, and relay networks. Secret-key generation and establishment protocols based on physical layer mechanisms are subsequently covered. Approaches for secrecy based on channel coding design are then examined, along with a description of inter-disciplinary approaches based on game theory and stochastic geometry. The associated problem of physical layer message authentication is also briefly introduced. The survey concludes with observations on potential research directions in this area [Jeong et al., 3].

2.2. A Survey on Spectrum Management in Cognitive Radio Networks

Cognitive radio networks will provide high bandwidth to mobile users via heterogeneous wireless architectures and dynamic spectrum access techniques. However, CR networks impose challenges due to the fluctuating nature of the available spectrum, as well as the diverse QoS requirements of various applications. Spectrum management functions can address these challenges for the realization of this new network paradigm. To provide a better understanding of CR networks, this article presents recent developments and open research issues in spectrum management in CR networks. More specifically, the discussion is focused on the development of CR networks that require no modification of existing networks. First, a brief overview of cognitive radio and the CR network architecture is provided. Then four main challenges of spectrum management are discussed: spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility [Baldini et al., 4].

2.3. Existing Work

We consider a Cognitive Radio (CR) network consisting of a Secondary Transmitter (ST), a Secondary Destination (SD) and multiple Secondary Relays (SRs) in the presence of an eavesdropper, where the ST transmits to the SD with the assistance of SRs, while the eavesdropper attempts to intercept the secondary transmission. We rely on careful relay selection for protecting the ST-SD transmission against the eavesdropper with the aid of both single-relay and multi-relay selection. To be specific, only the "best" SR is chosen in the single-relay selection for assisting the secondary transmission, whereas the multi-relay selection invokes multiple SRs for simultaneously forwarding the ST's transmission to the SD.

III. PROPOSED WORK

In this proposed system, we analyze both the intercept probability and outage probability of the proposed single-relay and multi-relay selection schemes for the secondary transmission relying on realistic spectrum sensing. We also evaluate the performance of classic direct transmission and artificial noise based methods for the purpose of comparison with the proposed relay selection schemes. It is shown that as the intercept probability requirement is relaxed, the outage performance of the direct transmission, the artificial noise based and the relay selection schemes improves, and vice versa. This implies a trade-off between the security and reliability of the secondary transmission in the presence of eavesdropping attacks, which is referred to as the Security-Reliability Trade-off (SRT). Furthermore, we demonstrate that the SRTs of the single-relay and multi-relay selection schemes are generally better than that of classic direct transmission, explicitly demonstrating the advantage of the proposed relay selection in terms of protecting the secondary transmissions against eavesdropping attacks. Moreover, as the number of SRs increases, the SRTs of the proposed single-relay and multi-relay selection approaches significantly improve. Finally, our numerical results show that as expected, the multi-relay selection scheme achieves a better SRT performance than the single-relay selection. Relays that receive and retransmit the signals between base stations and mobiles can be used to increase throughput extend coverage of cellular networks. Infrastructure relays do not need wired connection to network thereby offering savings in operators' backhaul costs. Mobile relays can be used to build local area networks between mobile users under the umbrella of the wide area cellular networks. We analyze both the intercept probability and outage probability of the proposed single-relay and multi-relay selection schemes for the secondary transmission relying on realistic spectrum sensing. We also evaluate the performance of classic direct transmission and artificial noise based methods for the purpose of comparison with the proposed relay selection schemes. It is shown that as the intercept probability requirement is relaxed, the outage performance of the direct transmission, the artificial noise based and the relay selection schemes improves, and vice versa. This implies a trade-off between the security and reliability of the secondary transmission in the presence of eavesdropping attacks, which is referred to as the Security-Reliability Trade-off (SRT) [Mukherjee & Swindlehurst, 5].

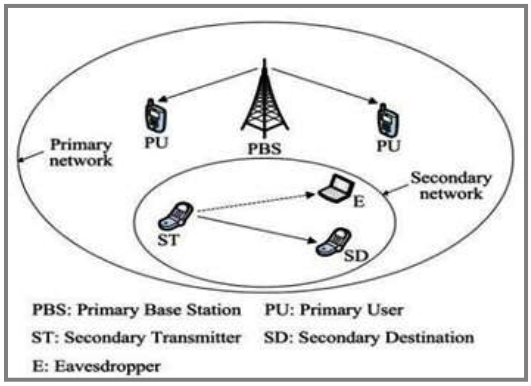

Figure 1: A Primary Wireless Network in Coexistence with a Secondary CR Network

Furthermore, we demonstrate that the SRTs of the single-relay and multi-relay selection schemes are generally better than that of classic direct transmission, explicitly demonstrating the advantage of the proposed relay selection in terms of protecting the secondary transmissions against eavesdropping attacks. Moreover, as the number of SRs increases, the SRTs of the proposed single-relay and multi-relay selection approaches significantly improve. Finally, our numerical results show that as expected, the multi-relay selection scheme achieves a better SRT performance than the single-relay selection**.** Physical-layer security is emerging as an efficient approach for defending authorized users against eavesdropping attacks by exploiting the physical characteristics of wireless channels. In Leung-Yan-Cheong and Hellman demonstrated that perfectly secure and reliable transmission can be achieved, when the wiretap channel spanning from the source to the eavesdropper is a further degraded version of the main channel between the source and destination. They also showed that the maximal secrecy rate achieved at the legitimate destination, which is termed the secrecy capacity, is the difference between the capacity of the main channel and that of the wiretap channel. In the secrecy capacity limits of wireless fading channels were further developed and characterized from an information-theoretic perspective, demonstrating the detrimental impact of wireless fading on the physical layer security. To combat the fading effects, multiple-input multiple-output (MIMO) schemes as well as cooperative relaying and beamforming techniques were investigated for the sake of enhancing the achievable wireless secrecy capacity. Although extensive research efforts were devoted to improving the security of traditional wireless networks less attention has been dedicated to CR networks. In the achievable secrecy rate of the secondary transmission was investigated under a specific quality-of-service (Qos) constraint imposed on the primary transmission. Additionally, an overview of the physical-layer

security aspects of CR networks was provided in where several security attacks as well as the related countermeasures are discussed. In contrast to conventional non-cognitive wireless networks, the physical-layer security of CR networks has to consider diverse additional challenges, including the protection of the primary user's Qos and the mitigation of the mutual interference between the primary and secondary transmissions. Motivated by the above considerations, we explore the physical-layer security of a CR network comprised of a secondary transmitter (ST) communicating with a secondary destination (SD) with the aid of multiple secondary relays (SRs) in the presence of an unauthorized attacker.

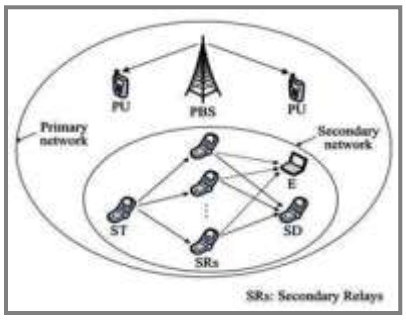

Figure 2: A Cognitive Relay Network consists of One ST, One SD and N SRs in the presence of an E

Our main focus is on investigating the security-reliability trade-off (SRT) of the cognitive relay transmission in the presence of realistic spectrum sensing. The notion of the SRT in wireless physical layer security was introduced and examined in where the security and reliability was characterized in terms of the intercept probability and outage probability, respectively. In contrast to the conventional non-cognitive wireless networks studied in the SRT analysis of CR networks presented in this work additionally takes into account the mutual interference between the primary user (PU) and secondary user (SU). Number of SRs increases, the SRTs of the proposed single-relay and multi-relay selection approaches significantly improve Protecting the secondary transmissions against eavesdropping attacks. In this paper, we proposed relay selection schemes for a CR network consisting of a ST, a SD and multiple SRs communicating in the presence of an eavesdropper. We examined the SRT performance of the SRS and MRS assisted secondary transmissions in the presence of realistic spectrum sensing, where both the security and reliability of secondary transmission are characterized in terms of their IP and OP, respectively. We also analyzed the SRT of the conventional direct transmission as a benchmark. It was illustrated that as the spectrum sensing reliability increases, the SRTs of both the SRS and MRS schemes improve. We also showed that the proposed SRS and MRS schemes generally outperform the conventional direct transmission and artificial noise based approaches in terms of their SRT. Moreover, the SRT performance of MRS is better than that of SRS. Additionally, as the number of SRs increases, the SRTs of both the SRS and of the MRS schemes improve significantly, demonstrating their benefits in terms of enhancing both the security and reliability of secondary transmissions.4G technology is also called as LTE Advanced systems, the use of MIMO is likely to involve further and more advanced techniques with additional antennas in the matrix to enable additional paths to be sued, although as the number of antennas increases, the overhead increases and the return per additional path is less. In additional to the numbers of antennas increasing, it is likely that techniques such as beam forming may be used to enable the antenna coverage to be focused where it is needed. There are a number of key technologies that will enable LTE Advanced to achieve the high data throughput rates that are required. MIMO and OFDM are two of the base technologies that will be enablers. Along with these there is a number of other techniques and technologies that will be employed [Olteanu & Xiao, 6].

IV. EXPERIMENT RESULT

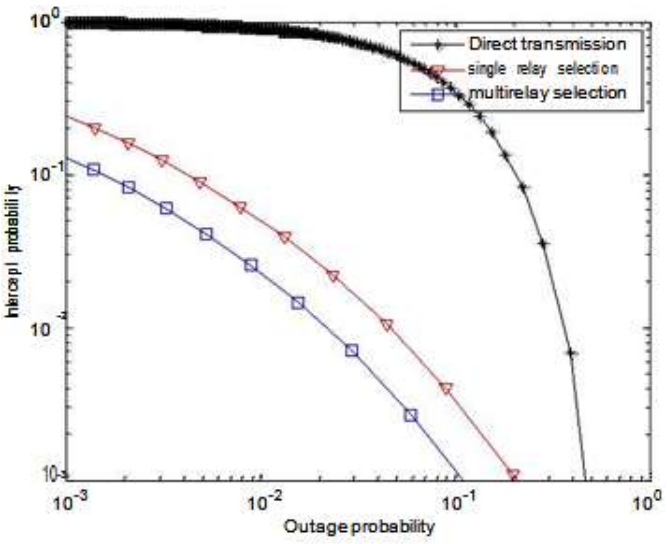

Figure 3: IP versus OP of the Direct Transmission, SRS and MRS for P_o=0.8

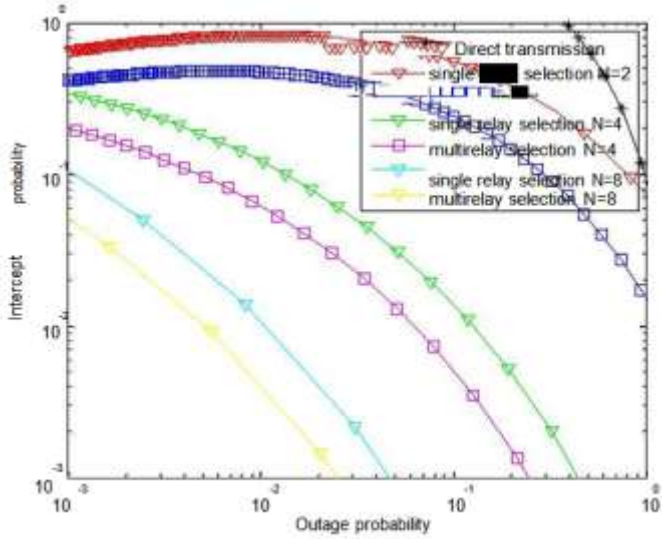

Figure 4: IP versus OP of the SRS and MRS Schemes for Different N= 2, 4, 8

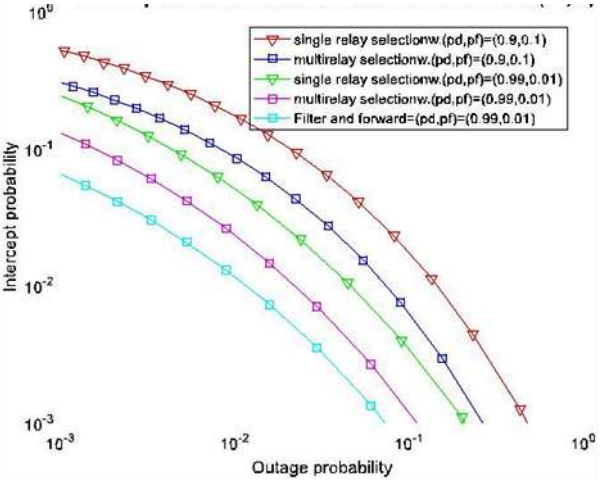

Figure 5: IP versus OP of the SRS and the MRS Schemes for Different (Pd, Pf)

V. CONCLUSION

In our project, we proposed relay selection schemes for a CR network consisting of a ST, a SD and multiple SR communicating in the presence of an eavesdropper. We examined the SRT performance of the SRS and MRS assisted secondary transmissions in the presence of realistic spectrum sensing, where both the security and reliability of secondary transmissions are characterized in terms of their IP and OP, respectively. We also analyzed the SRT of the conventional direct transmission as a benchmark. It was illustrated that as the spectrum sensing reliability increases, the SRTs of both the SRS and MRS schemes improve. We also showed that the proposed SRS and MRS schemes generally outperform the conventional direct transmission and artificial noise based approaches in terms of their SRT. Moreover, the SRT performance of MRS is better than that of SRS. Additionally, as the number of SRs increases, the SRTs of both the SRS and of the MRS schemes improve significantly, demonstrating their benefits in terms of enhancing both the security and reliability of secondary transmissions.

REFERENCES

[1] Y. Zou, X. Wang, W. Shen & L. Hanzo (2014), "Security versus Reliability Analysis of Opportunistic Relaying", *IEEE Transactions on Vehicular Technology*, Vol. 63, No. 6, Pp. 2653–2661.

[2] Y. Zou, X. Wang & W. Shen (2013), "Physical-layer Security with Multiuser Scheduling in Cognitive Radio Networks", *IEEE Transactions on Communications*, Vol. 61, No. 12, Pp. 5103–5113.

[3] C. Jeong, I. Kim & K. Dong (2012), "Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System", *IEEE Transactions on Signal Processing*, Vol. 60, No. 1, Pp. 310–325.

[4] G. Baldini, T. Sturman, A.R. Biswas & R. Leschhorn (2012), "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and a way ahead", *IEEE Communication Surveys Tutorials*, Vol. 14, No. 2, Pp. 355–379.

[5] A. Mukherjee & A. Swindlehurst (2011), "Robust Beamforming for Security in MIMO Wiretap Channels with Imperfect CSI", *IEEE Transactions on Signal Processing*, Vol. 59, No. 1, Pp. 351–361.

[6] A. Olteanu & Y. Xiao (2010), "Security Overhead and Performance for Aggregation with Fragment Retransmission (AFR) in Very High-Speed Wireless 802.11 LANs", *IEEE Transactions on Wireless Communications*, Vol. 9, No. 1, Pp. 218–226.

