OPTIMIZATION OF SECURITY RELIABLITY TRADE OFF IN COGNITIVE RADIOS USING RELAY SELECTION

[1]Manimegalai Munisamy, [2]Janani Munisamy

[1]Assistant Professor, [2]Assistant Professor
Department of ECE,
TPGIT, Vellore, India

***Abstract*: We consider a cognitive radio network (CR) consisting of a secondary transmitter (ST), a secondary destination (SD), and multiple secondary relays (SRs) in the presence of an interceptor, where the ST transmits to the SD using the SRs while the interceptor attempts to intercept the secondary transmission. We rely on careful relay selection to protect the ST-SD transmission from the interceptor, using both single and multiple relay selection. To be precise, single-relay selection selects only the "best" SR to support the secondary transmission, while multiple SRs are used in multi-relay selection to simultaneously relay the transmission from ST to SD. The proposed single and multi relay selection schemes are analyzed using intercept and outage probability for the secondary user transmission based on the realistic spectrum detection. We also evaluate the performance of classical direct transmission method to compare with the proposed relay selection methods. It is shown that the outage performance of the direct transmissionmethod and relay selection methods improves when the outage probability requirement is relaxed, and vice versa. Moreover, we show that the SRT (Security Reliability Trade off) of the single-relay and multi-relay selection schemes are generally better than that of the classical direct transmission, which explicitly demonstrates the advantage of the proposed relay selection in protecting the secondary transmissions from eavesdropping attacks.**

***Keywords*: Spectrum Sensing, Relay selection, Security Reliability Trade off ,Cognitive radios.**

I. INTRODUCTION

The research community is paying more and more attention to the security aspects of cognitive radio (CR) systems [1]– [3]. Legitimate CR devices are in fact exposed to internal as well as external attackers due to the very dynamic nature of the CR network architecture, making them incredibly susceptible to malicious activity. As an illustration, an unauthorised user might jam signals on purpose in order to artificially contaminate the CR environment [4]. As a result, the CR users may be mislead or compromised and fail to adequately characterise the radio environment around them, which causes a malfunction. Alternately, an unauthorised user might try to listen in on authorised CR users' conversations in order to intercept sensitive data.

It is evident that CR networks are exposed to a variety of security risks during spectrum sensing [5, 6], spectrum sharing [7], spectrum mobility [8], and spectrum management [9]. Numerous studies have been done to safeguard CR networks from denial-of-service (DoS) attacks as well as primary user emulation (PUE) attacks [10, 11]. Although it has received less attention in the literature on CR network security, eavesdropping is another major concern in preserving the confidentiality of the data, in addition to PUE and DoS attacks [12]. In the past, cryptographic methods have been used to protect transmission confidentiality from eavesdropping attempts. However, this adds a significant computational overhead [13] and increases system complexity [14] in terms of managing the secret key.Additionally, the current cryptographic techniques are not completely secure and can still be broken by an eavesdropper (E), provided that it is able to conduct a thorough key search using a brute-force attack [15].

We investigate the physical-layer security of a CR network made up of a secondary transmitter (ST) and a secondary destination (SD) in the presence of an unauthorised attacker. This network uses several secondary relays (SRs) to communicate with each other. The security-reliability trade-off (SRT) of the cognitive relay transmission in

the presence of actual spectrum sensing is the major topic of our investigation. In [16], the idea of the SRT in wireless physicallayer security was presented and discussed. Security and dependability were described in terms of the intercept probability and outage probability, respectively.

The main contributions of this work can be summarized as follows.

We propose two relay selection schemes, namely single-relay and multi-relay selection, to protect secondary transmissions from eavesdropping. More specifically, in the single relay selection (SRS) scheme where a single relay is chosen from the set of multiple SRs to forward the data from ST to SD. In contrast, the multi-relay selection (MRS) uses multiple SRs to simultaneously support the transmissions from ST-SD.

Closed-form expressions for the intercept probability (IP) and outage probability (OP) of both schemes for transmission over Rayleigh fading channels are derived.

Numerical results show that the proposed SRS and MRS methods generally outperform the conventional direct transmission approaches in terms of their SRTs.

The rest of this paper is organized as follows.

In Section II, we present the system model for the cognitive radio network in the context of direct transmission and SRS and MRS methods. In Section III, we analyze the SRTs of these methods in the presence of realistic spectrum sensing over Rayleigh fading channels. Subsequently, numerical SRT results of the direct transmission, SRS, and MRS methods are given in Section IV. Finally, Section V provides conclusion and future scope.

The system paradigm for Cognitive radio networks is presented first. Then, in order to increase the security of the CR system against eavesdropping attempts, we give the signal models of the SRS and MRS schemes as well as the standard direct transmission technique.

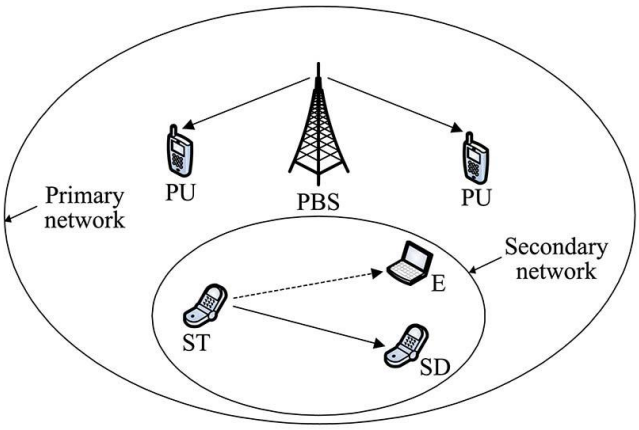

Figure 1.A primary wireless network in coexistence with a secondary CR network.

II. PROTECTION FROM EAVESDROPPING USING RELAY SELECTION IN CR NETWORKS

A. System Model

We take into account a primary network coexisting with a secondary network (also known as a CR network), as shown in Fig. 1. A primary base station (PBS) and numerous primary users (PUs), who connect with the PBS across licensed spectrum, make up the primary network. In contrast, the secondary network, which consists of one or more STs and SDs, makes opportunistic use of the licensed spectrum. To be more precise, a specific ST should first determine using spectrum sensing whether or not the PBS is using the licensed spectrum. If the primary user is transmitting using the licensed spectrum the ST is not free to transmit in order to prevent interfering with the PUs.The ST may transmits to the SD over the identified spectrum hole ifit is determined that the licenced spectrum is unoccupied (i.e., a spectrum hole is detected). Eavesdropper (E) tries to snare the secondary transmission going from the ST to the SD in the meantime. For ease of notation, let H_0 and H_1 stand in for the licenced spectrum being either empty or being used by the PBS during a specific time period. Let H further represent the status of the observed licensed spectrum using spectrum sensing.In particular, the cases when the licenced spectrum is judged to be unoccupied and occupied are represented by $H = H_0$ and $H = H_1$, respectively.

The probability P_d of correctly detecting the presence of PBS and the false alarm probability P_f are given by $P_d = Pr(H = H_1|H_1)$ and $Pf = Pr(H = H_1|H_0)$.Due to the background noise and fading effects, it is impossible to achieve perfectly reliable spectrum detection without missing the detection of an active PU and without false alarm, which suggests that a spectral band is occupied by a PU, when it is actually unoccupied. Moreover, the missed detection of the presence of PBS will result in interference between the PU and SU. To guarantee that the interference imposed on the PUs is below a tolerable level, both the successful detection probability $P_d$and false alarm probability $P_f$should be within a meaningful target range.Finally, all the received signals are assumed to be affected by additive white Gaussian noise (AWGN) having a zero mean and a variance of N_0.

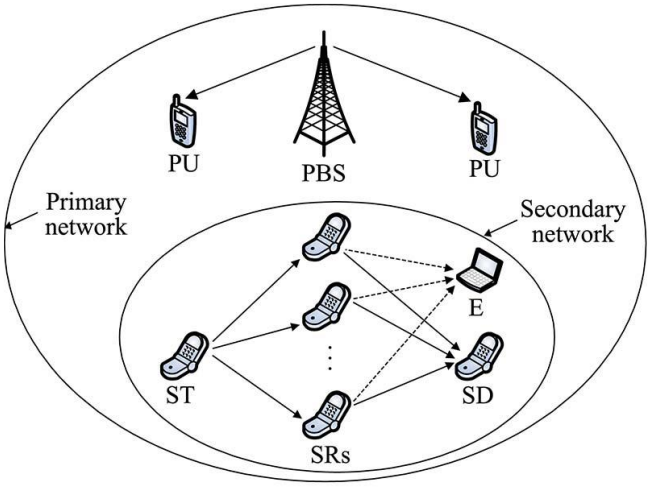

Figure 2. A cognitive relay network consists of one ST, one SD and *N* SRs in the presence of an E.

B. Single-Relay Selection

In this section let us consider a cognitive relay network shown in Figure 2, where SD and E are both considered to be beyond the ST's coverage area and N secondary relays (SRs) are used to aid cognitive ST-SD transmission. We assume that decode-and-forward (DF) relaying in which two adjacent time slots is used and a common control channel (CCC) is provided for coordinating the actions of the various secondary users. More specifically, after it is determined that the licenced spectrum is unoccupied, the ST broadcasts its signal x_s to the N SRs, who then try to decode x_s from the signals they receive. For the sake of notational simplicity, let D represent the collection of SRs that successfully decode x_s.

$$\Omega = \{\phi, D1, D2, \cdots, Dn, \cdots, D2^N - 1\}$$

whereD_n denotes the n^{th} non-empty subset of the N SRs and ϕ denotes the empty set. If the set D is empty, indicating that no SR successfully decodes x_s, then all the SRs remain silent, making it impossible for both SD and E to correctly decode x_s in this scenario. A specific SR is picked from the set D if it has non-empty elements in order to send

its decoded signal x_s to SD. Consequently, ST transmits its signal x_s to N SRs with a power of P_s and a rate of R assuming that H = H_0 (i.e., the licenced spectrum is declared empty). Thus, the signal received at a particular SR_i is represented by

$$s_i = h_{si}\sqrt{P_s}x_s + h_{pi}\sqrt{\alpha P_p}x_p + n_i (1)$$

where$h_{si}$and h_{pi}denote the fading coefficients of the ST-SR_ichannel and that of the PBS-SR$i$channel, respectively, with$n_i$representing the AWGN at SR_i. From (7), we obtain thecapacity of the ST-SR_ichannel as

$$C_{si} = \frac{1}{2} log_2 \left(1 + \frac{|h_{si}|^2 \gamma_s}{\alpha |h_{pi}|^2 \gamma_p + 1}\right) (2)$$

where the value 1/2 results from the necessity of two orthogonal time periods in order to transmit the message from ST to SD through SR_i.If we assume that SR_i is selected within D_n to transmit its decoded result x_s at a power of P_sThe signal received at SD can be written as

$$s_d = h_{id}\sqrt{P_s}x_s + h_{pd}\sqrt{\alpha P_p}x_p + n_d (3)$$

whereh_{id}symbolizes the fading coefficient of the SRi–SDchannel. From (11), the capacity of the SRi−SD channel is given by

$$C_{id} = \frac{1}{2} log_2 \left(1 + \frac{|h_{id}|^2 \gamma_s}{\alpha |h_{pd}|^2 \gamma_p + 1}\right) (4)$$

where$i \in D_n$. In general, the "best" SR for facilitating the ST's transmission is selected as the particular SR_i with the largest instantaneous capacity to SD. Consequently, the best relay selection criteria are written as

$$Best\ SR = \underset{i \in D_n}{arg\ max}\ C_{id} = \underset{i \in D_n}{arg\ max}\ |h_{id}|^2 (5)$$

which demonstrates that only the channel state information (CSI), and not the eavesdropper's CSI knowledge, is needed to perform the relay selection. Combining (4) and (5), we get the channel's capacity asthe “best” SR to SD as

$$C_{bd} = \frac{1}{2} log_2 \left(1 + \frac{\gamma_s}{\alpha |h_{pd}|^2 \gamma_p + 1} \underset{i \in D_n}{max} |h_{id}|^2\right) (6)$$

where the best SR is indicated by the subscript 'b' in C_{bd}. It can be seen from (6) that the maximum of independent random variables (RVs)$|h_{id}|^2$ for various SRs determines the SRS scheme's legal transmission capacity.

The signal received at E is also represented as, providing that the chosen SR broadcasts its decoded result xs at a power of Ps.

$$s_e = h_{be}\sqrt{P_s}x_s + h_{pe}\sqrt{\alpha P_p}x_p + n_e (7)$$

whereh_{be} and h_{pe} stand for the channel's "best" SR to E and PBS to E fading coefficients, respectively.The capacity of the channel extending from the "best" SR to E is given by in (8).

$$C_{be} = \frac{1}{2} log_2 \left(1 + \frac{|h_{be}|^2 \gamma_s}{\alpha |h_{pe}|^2 \gamma_p + 1}\right) (8)$$

where the relay selection criterion stated in (5), determines b ε D_n. As seen in (8), the channel state information (CSI) $|h_{be}|^2$ of the wiretap channel stretching from the "best" relay to the eavesdropper affects the eavesdropper's channel capacity. However, as can be seen from (5) the best relay is chosen from the decoding set $D_n$solely based on the CSI $|h_{id}|^2$ of the main channel, i.e. without taking into account the CSI knowledge of $|h_{ie}|^2$ of the eavesdropper. Since the main channel and the wiretap channel are independent of one another, choosing the best relay with the goal of maximising the legitimate transmission capacity of (6) would not have a materially positive or negative impact on the eavesdropper's channel capacity.

For instance, if the random variables (RVs) $|h_{ie}|^2$ associated with the various relays are i.i.d, we can easily conclude from the law of total probability that$|h_{be}|^2$ has the same probability density function (PDF) as $||h_{ie}|^2$, indicating that the best relay choice made by (5) has no impact on the eavesdropper's channel capacity. Therefore, in terms of reducing the capacity of the wiretap channel, the SRS scheme has no discernible advantage over the traditional direct transmission. To further explain, the SRT trade-off states that an improvement in the intercept probability (IP) would result from a reduction in the outage probability (OP) brought on by the capacity expansion of the main channel accomplished by employing the best relay.

C. Selection of a multiple relay

The MRS system described in this part uses several SRs to send the source signal x_s to SD concurrently. To be more precise, over an identified spectrum hole, ST broadcasts x_s to N SRs first. We designate by D the set of SRs that correctly decode x_s. Both SD and E are unable to decode x_s if D is empty because all SRs will fail to decode x_s and will

not forward the source signal if D is empty. All SRs in D_n are used for simultaneously transmitting x_s to SD if D is not empty (i.e., $D = D_n$). In contrast to the SRS system, which only selects one SR from D_n to convey x_s to SD, this is different.In order to use several SRs effectively, a weight vector with the notation $[w_1, w_2, ,w_{|Dn|}]$ should be used.T is used at the SRs to transmit x_s, where $|D_n|$ is the set D_n's cardinality. The total transmit power across all SRs inside D_n shall be limited to P_s for the purpose of a fair comparison with the SRS scheme in terms of power consumption, and as a result, the weight vector w should be normalised according to w = 1.

As a result, the signal received at SD is described as follows when $D = D_n$ and all SRs inside D_n are chosen to broadcast x_s with a weight vector w simultaneously.

$$s_d{}^{Multi} = \sqrt{P_s} W^T H_d x_s + \sqrt{\alpha P_p} h_{pd} x_p + n_d (9)$$

whereH_d= $[h_{1d}, h_{2d}, \cdots, h_{|Dn|d}]^T$.

Correspondingly the signal received at E can be expressed as

$$s_e{}^{Multi} = \sqrt{P_s} W^T H_e x_s + \sqrt{\alpha P_p} h_{pe} x_p + n_e (10)$$

whereH_e= $[h_{1e}, h_{2e}, \cdots, h_{|Dn|e}]^T$.

From (9) and (10), thesignal-to-interference-plus-noise ratios (SINRs) at SD and Eare, respectively, given by

$$SINR_d^{multi} = \frac{\gamma_s}{\alpha |h_{pd}|^2 \gamma_p + 1} |W^T H_d|^2 (11)$$

and

$$SINR_e^{multi} = \frac{\gamma_s}{\alpha |h_{pe}|^2 \gamma_p + 1} |W^T H_e|^2 (12)$$

In this work, the weight vector *w* is optimized by maximizingthe SINR at SD, yielding

$$\max_w SINR_d^{multi}, s.t \; ||w|| = 1 (13)$$

where the constraint is used for normalization purposes. Using the Cauchy-Schwarz inequality [17], we can readily obtain the optimal weight vector w_{opt} from (13) as

$$w_{opt} = \frac{H_d^*}{|H_d|} (14)$$

which indicates that the optimal vector design only requires the SR-SD CSI H_d, whilst dispensing with the eavesdropper's CSI H_e. Substituting the optimal vector $w_{opt}$from (14) into (11) and (12) and using Shannon's capacity formula, we can obtain the channel capacities achieved at both SD and E as

$$C_d^{multi} = \frac{1}{2} log_2 \left(1 + \frac{\gamma_s}{\alpha |h_{pd}|^2 \gamma_p + 1} \sum_{i \in D_n} |h_{id}|^2\right) (15)$$

and

$$C_e^{multi} = \frac{1}{2} log_2 \left(1 + \frac{\gamma_s}{\alpha |h_{pe}|^2 \gamma_p + 1} \frac{|H_d^H H_e|^2}{|H_d|^2}\right) (16)$$

where H stands for the Hermitian transposition and $D = D_n$. One can see from (6) and (15) that the capacity expressions C_{bd} and C_d^{multi} differ from one another. The sole difference between the SRS scheme and the MRS scheme is that the SRS scheme uses the maximum RVs $|h_{id}|^2$ for each SR (i.e., $\max_{i \in D_n} |h_{id}|^2$), whereas the MRS scheme uses the sum of RVs $|h_{id}|^2$ (i.e., $\sum_{i \in D_n} |h_{id}|^2$). It is obvious that $\sum_{i \in D_n} |h_{id}|^2 > \max_{i \in D_n} |h_{id}|^2$ leads to a performance advantage for MRS over SRS in terms of increasing the legal transmission capacity.The optimal weights set for the numerous relays based on H_d will also only marginally affect the eavesdropper's channel capacity because the main channel H_e and the wiretap channel H_e are independent of one another.

This indicates that in terms of the wiretap channel's capacity, the MRS and SRS systems function almost equally well. However, the MRS scheme can achieve a better intercept performance than the SRS scheme given a fixed outage requirement because, in accordance with the SRT, an outage reduction achieved by the capacity enhancement of the legal transmission relying on the MRS would be converted into an intercept improvement.To be more precise, in order to maintain a constant OP, we may increase the data rate R based on the OP definition of (17) which, in turn, results in a reduction of the IP because a higher data rate would produce a lower IP, in accordance with the IP definition of (18).

It should be noted that the MRS system requires a high-complexity symbol-level synchronisation for multiple distributed SRs when sending to SD at the same time, but the SRS does not require such a complex synchronisation mechanism.Therefore, MRS's performance advantage over SRS is gained at the expense of a more complex implementation. Additionally, the MRS scheme's synchronisation flaws will result in performance degradation, which might even cause the MRS scheme to perform worse than the SRS scheme.

The Rayleigh model is used to describe the fading amplitudes of wireless channels (such as $|h_{sd}|$, $|h_{si}|$, $|h_{id}|$, etc.), which implies that the fading square magnitudes $|h_{sd}|^2$, $|h_{si}|^2$, and $|h_{id}|^2$ are exponentially distributed random

variables (RVs). The presentation of the signal models for the direct transmission, SRS, and MRS techniques for CR networks applications in the presence of eavesdropping is currently complete.

III. SRT ANALYSIS OVER RAYLEIGH FADING CHANNELS

The SRT analysis of Direct transmission, SRS and MRS schemes over channels that are fading due to Rayleigh is presented in this section. The security and dependability are quantified in terms of the IP and OP that are experiencedby the destination and eavesdropper. It is noted that in CR networks, ST only begins to send its signal when a recognised spectrum hole is available. The OP and IP are thereafter calculated on the presumption that the licenced spectrum is found to be vacant by the PBS. The definitions of OP and IP are provided in the following.

Definition 1: Assume that C_d and C_e stand for the corresponding channel capacity at the destination and eavesdropper. The definitions of the OP and IP are, respectively,

$$P_{out} = \Pr(C_d<R| \hat{H} = H_0) \quad (17)$$

and

$$P_{int} = \Pr(C_e> R| \hat{H} = H_0) \quad (18)$$

where R is the data rate.

The OP of the cognitive transmission dependent on SRS is provided by when $H = H_0$.

$$P_{out}^{single} = \Pr(C_{bd} < R, D = \emptyset \,|\, \hat{H} = H_0) + \sum_{n=1}^{2^N-1} \Pr(C_{bd} < R, D = D_n | \hat{H} = H_0) \quad (19)$$

whereC_{bd}represents the capacity of the channel from the "best" SR to SD.Additionally, the IP of the SRS scheme can be expressed as

$$P_{int}^{single} = \Pr(C_{be} > R, D = \emptyset \,|\, \hat{H} = H_0) + \sum_{n=1}^{2^N-1} \Pr(C_{be} > R, D = D_n | \hat{H} = H_0) \quad (20)$$

whereC_{be}represents the capacity of the channel spanning from the "best" SR to E.

The OP of the cognitive transmission dependent on MRS is provided by when $H = H_0$.

$$P_{out}^{multi} = \Pr(D = \emptyset \,|\, \hat{H} = H_0) + \sum_{n=1}^{2^N-1} \Pr\left(C_d{}^{multi} < R, D = D_n \middle| \hat{H} = H_0\right) \quad (21)$$

where$C_d{}^{multi}$ denotes the channel capacity achieved at the SD. Additionally, the IP of the SRS scheme can be expressed as

$$P_{int}^{multi} = \Pr\left(C_e{}^{multi} > R, D = \emptyset \,\middle|\, \hat{H} = H_0\right) + \sum_{n=1}^{2^N-1} \Pr\left(C_e{}^{multi} > R, D = D_n \middle| \hat{H} = H_0\right) \quad (22)$$

where$C_e{}^{multi}$ denotes the channel capacity achieved at E.

IV. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we compare the direct transmission, SRS, and MRS systems in terms of their SRT performance The SDP $P_d$and FAP P_f are set to $P_d = 0.99$ and $P_f = 0.01$, respectively. Our numerical analyses make use of the primary signal-to-noise ratio (SNR) of $\gamma_p = 10$ dB and the data rate of R = 1 bit/s/Hz.

The IP vs OP of the direct transmission is shown in Fig. 3, along with the SRS and MRS methods for P_0= Pr(H_0) = 0.8. A trade-off between the IP (security) and the OP (reliability) of CR transmissions is implied by the observation in Fig. 3 that the IP of the direct transmission, as well as of the proposed SRS and MRS methods, all improve upon tolerating a higher OP. Additionally, Fig. 3 demonstrates that the proposed SRS and MRS schemes outperform direct transmission approach in terms of their SRT, highlighting the benefit of utilising relay selection as a defence against eavesdropping.Additionally, the MRS performs SRT operations better than the SRS. Although the MRS outperforms its SRS-aided counterpart in terms of SRT performance, this advantage comes at the expense of a more complex implementation because multiple SRs need elaborate symbol-level synchronisation in order to transmit data to the SD simultaneously, whereas the SRS does not.

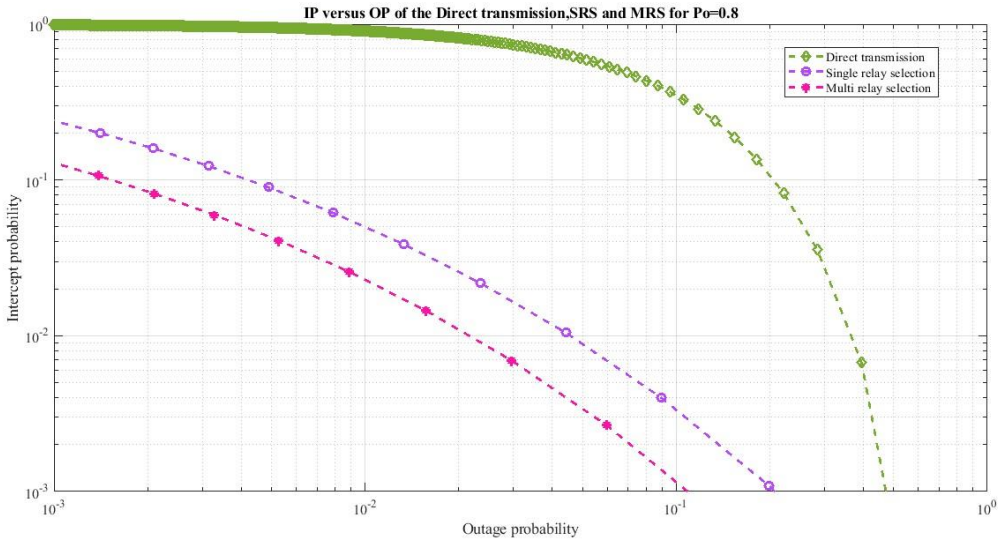

Figure 3.IP versus OP of the direct transmission, the SRS and the MRS schemes with P_0= 0.8

Our numerical SRT comparison of the SRS and MRS systems for P_0 = 0.2 and P_0 = 0.8 is shown in Fig. 4. The MRS scheme outperforms the SRS in terms of SRT performance for both P_0 = 0.2 and P_0 = 0.8, as can be seen in Fig. 4.The SRT of both the SRS and MRS schemes improves as P_0 rises from 0.2 to 0.8, as can also be shown in Fig. 4.This is due to the fact that as P_0 increases, the licenced band is less likely to be occupied by PUs. As a result, secondary users (SUs) have more opportunities to access the licenced band for their data transmissions, which lowers the OP for CR transmissions. As the eavesdropper has more opportunities to intercept the cognitive transmissions, increasing P_0 may also raise IP at the same time. The relay selection is carried out in the SRS and MRS systems, nevertheless, in order to maximise the lawful transmission capacity without reducing the eavesdropper's channel capacity.Thus, uponincreasing P_0 makes it more likely that the decrease in OP will be greater than the increase in IP, resulting in anSRS and MRS scheme SRT improvements overall.

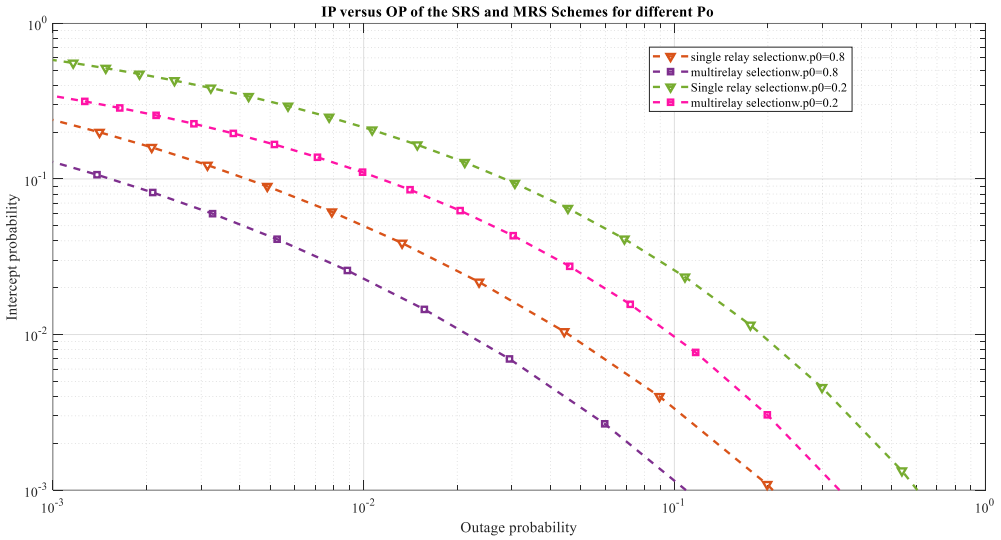

Figure 4. IP versus OP of the SRS and the MRS schemes for different P_0

V. CONCLUSION

For a CR network with a ST, SD, and numerous SRs interacting in the presence of an eavesdropper, we suggested relay selection strategies in this research. In the presence of realistic spectrum detection, we looked at the SRT performance of SRS and MRS supported secondary transmissions. The security and reliability of secondary transmissions are defined by their IP and OP, respectively. As a comparison, we also examined the SRT of the typical direct transmission. It was demonstrated that the SRTs of both the SRS and MRS methods improve as the spectrum sensing reliability rises. Additionally, we demonstrated that the proposed SRS and MRS schemes perform generally

better than the traditional direct transmission approach in terms of their SRT.Additionally, MRS performs better on SRT than SRS does.

REFERENCES

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.
[2] IEEE 802.22 Working Group, IEEE P802.22/D1.0 draft standard forwireless regional area networks part 22: Cognitive wireless RAN mediumaccess control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands, Apr. 2008.
[3] G. Baldini, T. Sturman, A. R. Biswas, and R. Leschhorn, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 355–379, May 2012.
[4] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proc. 38th Asil. Conf. Signal,Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2004, pp. 772–776.
[5] H. Li, "Cooperative spectrum sensing via belief propagation in spectrumheterogeneouscognitive radio systems," in *Proc. IEEE WCNC*, Sydney, N.S.W., Australia, Apr. 2010, pp. 1–6.
[6] J.Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Trans. WirelessCommun.*, vol. 7, no. 11, pp. 4502–4507, Nov. 2008.
[7] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.
[8] R. Southwell, J. Huang, and X. Liu, "Spectrum mobility games," in *Proc. 31st INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 37–45.
[9] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "A surveyon spectrum management in cognitive radio networks," *IEEE Commun.Mag.*, vol. 46, no. 4, pp. 40–48, Apr. 2008.
[10] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems part I: Known channel statistics,"*IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3566–3577 Nov. 2010.
[11] T. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," in *Proc. 2nd Int. Conf. CROWNCOM*, Orlando, FL, USA, Aug. 2007, pp. 456–464.
[12] S. Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *Proc. 28th ICDCS*, Beijing, China, Jun. 2008, pp. 19–27.
[13] A. Olteanu and Y. Xiao, "Security overhead and performance for aggregation with fragment retransmission (AFR) in very high-speed wireless 802.11 LANs," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 218–226, Jan. 2010.
[14] Y. Xiao, V. K. Rayi, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Comput.Commun.*,vol. 30, no. 11–12, pp. 2314–2341, Sep. 2007.
[15] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.
[16] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Tech.*, vol. 63, no. 6, pp. 2653–2661, Jun. 2014.
[17] L. Di Stefano and S. Mattoccia, "A sufficient condition based on the Cauchy-Schwarz inequality for efficient template matching," in *Proc. Int.Conf. Image Process.*, Catalonia, Spain, Sep. 2003, pp. 269–272.

Profile:

Manimegalai Munisamy. She received her B.E degree in Electronics and communication engineering from Thanthai Periyar Government Institute of technology, Vellore and M.E degree in Communication systems from College of Engineering, Guindy, India. She is currently working as Assistant Professor in Thanthai Periyar Government Institute of Technology, Vellore, India. Her field of interest includes Wireless communication and Wireless Sensor networks. She is currently pursuing her Ph.D in the field of Wireless communication.

Janani Munisamy. She received her B.E degree in Electronics and communication engineering from Thanthai Periyar Government Institute of technology, Vellore and M.E degree in Applied Electronics from College of Engineering, Guindy, India. She is currently working as Assistant Professor in Thanthai Periyar Government Institute of Technology, Vellore, India. Her field of interest includes VLSI, Wireless communication, Image Processing and Wireless Sensor networks. She is currently pursuing her Ph.D in the field of VLSI.