International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 2 (March-April, 2016), PP. 221-226

SPECTRUM SENSING WITH OPTIMAL RELAY SELECTION FOR SECONDARY TRANSMISSION IN CRN

Mrs.N.Arunpriya[1], G.Sandhiya[2], D.Swathisri[3], V.Swetha[4]
[1]Senior Member IEEE
Department of ECE, Panimalar Engineering College, Chennai.
swathisri2595@gmail.com

Abstract— **In this paper we propose the secure transmission for secondary user in cognitive radio network(CRN). Here the relay selection is used to protect the secondary transmitter(ST) and secondary destination (SD)against eavesdropper with the aid of both single and multi relay selection. In multi relay selection of secondary transmission are chosen for simultaneous forwarding from ST–SD. In the presence of eavesdropping ,on relaxing the intercept probability it is observed that outage probability of direct transmission and relay selection improves. This phenomenon is called security reliability trade-off(SRT).From our deduction ,using filter and forward relay we conclude that SRT of single and multi relay schemes are better than that of direct transmission and as the number of secondary relay increases the SRT of single and multi relay selection scheme improves therefore we can conclude that when using filter and forward relay transmission scheme performance of multi relay selection is found to be comparatively better than single relay selection scheme.**

Index terms- **Cognitive radio network, eavesdropper, filter and forward relay, intercept probabaility, outage probability, multi relay selection, secondary relay, single relay selection, security reliability trade-off.**

I. INTRODUCTION

I n the last several years, the spectrum sharing (SS) systems have been widely studied due to their advantage in solving the spectrum demand. For instance, reference evaluated the channel capacity under a received power constraint and for different channel fading conditions. In addition, reference studied spectrum sharing systems with multiuser diversity in which the secondary user with the best channel condition is

selected first for signal transmission. In practice, the cooperation between the secondary and primary users is loose, which results in imperfect channel state information CSI) of the interference channel Therefore investigated the effect of imperfect CSI on the system capacity So far most of the research results for SS systems focused on the single antenna case. Recently, applying the multiple input multiple-output (MIMO) technology to cognitive radio networks has received growing interest. For instance employed multiple antennas at the secondary transmitter to manage the tradeoff between throughput and interference constraint More recently, considered the capacity limits of a multiuser multi-antenna CR network where only the base stations are equipped with multi-antennas. This paper extends the results of to a more general MIMO system

Where every node is equipped with multiple antennas We focus on orthogonal space-time block coding (OSTBC) and transmit antenna selection (TAS) CR systems with multi-user diversity and analyze the resulting average capacity and bit-error rate (BER) performance. It is known that TAS yields a better performance than OSTBC in a conventional down-link multiuser diversity MIMO system. Therefore, in this paper we want to check whether such a result is applicable to the cognitive radio environment. To investigate the diversity order of such kind of systems, the asymptotic BER expressions will be also derived.

The ideas put forth in this project are

- We consider single and multi relay selection schemes to improve the security of secondary user network. On analysis it is observed that when using single relay only the best secondary relay is chosen for secondary transmission from ST-SD.but if we use multi relay selection multiple secondary relay are chosen for forwarding secondary transmission to the destination.
- In the spectrum sensing of both relay selection schemes we derive intercept probability and outrage probability for transmission over Rayleigh fading channels.SRT mathematical analysis of the relay selection schemes is done and direct transmission is provided for comparsion.
- From above scenario,by using filter and forward relay transmission the spectrum sensing reliability is increased or false alarm probability is reduced .Hence the SRTs of both the relay selection schemes are improved .Analysing numerical

results we conclude that the proposed SRS and MRS schemes are better the direct transmission interms of SRTs.

- Hence Filter and forward relay selection scheme is proposed due to its low power consumption,less transreceiver complexity and reduction in noise level

II. ENHANCING THE SECURITY AGAINST EAVESDROPPING IN CR NETWORK

The physical-layer security in CR networks. We then present the signal model of the conventional direct transmission approach, which will serve as our bench marker, as well as of the SRS and MRS schemes for improving the CR system's security against eavesdropping attacks.

We consider a primary network in coexistence with a secondary network (also referred to as a CR network). The primary network includes a primary base station (PBS) and multiple primary users (PUs), which communicate with the PBS over the licensed spectrum. By contrast, the secondary network consisting of one or more STs and SDs exploits the licensed spectrum in an opportunistic way. To be specific, a particular ST should first detect with the aid of spectrum sensing whether or not the licensed spectrum is occupied by the PBS. If so, the ST is not at liberty to transmit to avoid interfering with the PUs. If alternatively, the licensed spectrum is deemed to be unoccupied (i.e. a spectrum hole is detected), then the ST may transmit to the SD over the detected spectrum hole. Meanwhile, E attempts to intercept the secondary transmission from the ST to the SD. For notational convenience, let H0 and H1 represent the event that the licensed spectrum is unoccupied and occupied by the PBS during a particular time slot, respectively. Moreover, let ˆH denote the status of the licensed spectrum detected by spectrum sensing Specifically, ˆH = H0 represents the case that the licensed spectrum is deemed to be unoccupied, while ˆH = H1 indicates that the licensed spectrum is deemed to be occupied. The probability Pd of correct detection of the presence of PBS and the associated false alarm probability Pf are defined as Pd = Pr(ˆH = H1|H1) and Pf = Pr(ˆH = H1|H0), respectively. Due to the background noise and fading effects, it is impossible to achieve perfectly reliable spectrum sensing 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.

$$y_e = h_{se}\sqrt{P_s}x_s + h_{pe}\sqrt{\alpha P_p}x_p + n_e,$$

where *hse* and *hpe* represent the fading coefficients of the channel spanning from ST to E and that from PBS to E, respectively, while *ne* represents the AWGN received at E. Upon combining Shannon's capacity formula

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

Single-Relay Selection:

Where both SD and E are assumed to be beyond the coverage area of the and *N* secondary relays (SRs) are employed for assisting the cognitive ST-SD transmission. We assume that a common control channel (CCC) is available for coordinating the actions of the different network nodes and the decode-and-forward (DF) relaying using two adjacent time slots is employed. More specifically, once the licensed spectrum is deemed to be unoccupied, the ST first broadcasts its signal *xs* to the *N* SRs, which attempt to decode *xs* from their received signals. For notational convenience, let *D* represent the set of SRs that succeed in decoding *xs*.

1.

$$y_i = h_{si}\sqrt{P_s}x_s + h_{pi}\sqrt{\alpha P_p}x_p + n_i,$$

$$\Pr\left(|h_{si}|^2 < \Lambda\right) = 1 - \exp\left(-\frac{\Lambda}{\sigma_{si}^2}\right),$$

for a given number of SRs. In this extreme case, the classic direct transmission may perform better than the SRS scheme

Pr(
$max[hid]^2 < \Delta[hpd]^2\gamma_p + \Delta) = 1 +$
$\sum_{m=1}^{2^{[Dn]}-1}(-1)[Dn(m)]\exp(-\sum_{i\in Dn(m)}\Delta/\sigma id^2)\times$
$(1+\sum_{i\in Dn(m)}\Delta\gamma_p\sigma^2$
pd/$\sigma\hat{}2_{id})\hat{} - 1$

It is worth mentioning that in practice, the average fading gain of the SR*i* −SD channel, |*hid* |2, should not be less than that of the ST-SD channel |*hsd* |2,

$$\Pr\left(|h_{si}|^2 < \Lambda|h_{pi}|^2\gamma_p + \Lambda\right) = 1 - \frac{\sigma_{si}^2}{\sigma_{pi}^2\gamma_p\Lambda + \sigma_{si}^2}\exp\left(-\frac{\Lambda}{\sigma_{si}^2}\right),$$

since SRs are typically placed in the middle between the ST and SD. Hence, a performance improvement for the SRS scheme over classic direct transmission would be achieved in practical wireless systems.

B .Multi-Relay Selection

This subsection presents a MRS scheme, where multiple SRs are employed for simultaneously forwarding the source signal *xs* to SD. To be specific, ST first transmits *xs* to *N* SRs over a detected spectrum hole all SRs fail to decode *xs* and will not forward the source signal, thus both SD and E are unable to

decode *xs*. If *D* is non-empty (i.e. *D* = *Dn*), all SRs within *Dn* are utilized for simultaneously transmitting *xs* to SD. This differs from the SRS scheme, where only a single SR is chosen from *Dn* for forwarding *xs* to SD

$$P_{\text{out}}^{\text{multi}} = \pi_0 \prod_{i=1}^{N} \Pr\left(|h_{si}|^2 < \Lambda\right) + \pi_1 \prod_{i=1}^{N} \Pr\left(|h_{si}|^2 < \Lambda |h_{pi}|^2 \gamma_p + \Lambda\right)$$
$$+ \pi_0 \sum_{n=1}^{2^N-1} \prod_{i\in\mathcal{D}_n} \Pr\left(|h_{si}|^2 > \Lambda\right) \prod_{j\in\bar{\mathcal{D}}_n} \Pr\left(|h_{sj}|^2 < \Lambda\right) \Pr\left(\sum_{i\in\mathcal{D}_n} |h_{id}|^2 < \Lambda\right)$$
$$+ \pi_1 \sum_{n=1}^{2^N-1} \prod_{i\in\mathcal{D}_n} \Pr\left(|h_{si}|^2 > \Lambda |h_{pi}|^2 \gamma_p + \Lambda\right) \prod_{j\in\bar{\mathcal{D}}_n} \Pr\left(|h_{sj}|^2 < \Lambda |h_{pj}|^2 \gamma_p + \Lambda\right)$$
$$\times \Pr\left(\sum_{i\in\mathcal{D}_n} |h_{id}|^2 < \gamma_p \Lambda |h_{pd}|^2 + \Lambda\right)$$

gain for MRS over SRS in terms of maximizing the legitimate transmission capacity. Moreover, since the main channel *Hd* and the wiretap channel *He* are independent of each other, the optimal weights assigned for the multiple relays based on *Hd* will only slightly affect the eavesdropper's channel capacity. This means that the MRS and SRS schemes achieve more or less the same performance in terms of the capacity of the wiretap channel. Nevertheless, given a fixed outage requirement, the MRS scheme can achieve a better intercept performance than the SRS scheme, because according to the SRT, an outage reduction achieved by the capacity enhancement of the legitimate transmission relying on the MRS would be converted into an intercept improvement.

$$P_{\text{int}}^{\text{multi}} = \pi_0 \sum_{n=1}^{2^N-1} \prod_{i\in\mathcal{D}_n} \Pr\left(|h_{si}|^2 > \Lambda\right) \prod_{j\in\bar{\mathcal{D}}_n} \Pr\left(|h_{sj}|^2 < \Lambda\right)$$
$$\times \Pr\left(\frac{|H_d^H H_e|^2}{|H_d|^2} > \Lambda\right)$$
$$+ \pi_1 \sum_{n=1}^{2^N-1} \prod_{i\in\mathcal{D}_n} \Pr\left(|h_{si}|^2 > \Lambda |h_{pi}|^2 \gamma_p + \Lambda\right)$$
$$\times \prod_{j\in\bar{\mathcal{D}}_n} \Pr\left(|h_{sj}|^2 < \Lambda |h_{pj}|^2 \gamma_p + \Lambda\right)$$
$$\times \Pr\left(\frac{|H_d^H H_e|^2}{|H_d|^2} > \gamma_p \Lambda |h_{pe}|^2 + \Lambda\right),$$

I. SRT ANALYSIS FOR DIFFERENT RELAY SELECTION METHODS

SRT analysis of the direct transmission, SRS and MRS schemes over Rayleigh fading channels. The security and reliability are quantified in terms of the IP and OP experienced by the eavesdropper and destination, respectively. It is pointed out that in CR networks, ST starts to transmit its signal only when an available spectrum hole is detected. Similarly to the OP and IP are thus calculated under the condition that the licensed spectrum is detected to be unoccupied by the PBS. The following gives the definition of OP and IP.

$$P_{out}^{direct} = \pi_0 \Pr(|hsd|^2 < \Delta) + s\pi_1 \Pr\left(|hsd|^2 - |hsd|^2 \gamma_p \Delta < \Delta\right)$$

When the capacity of the ST-E channel becomes higher than the data rate. Thus, given that a spectrum hole has been detected (i.e. ˆ*H* = *H*0), ST starts transmitting its signal to SD and E may overhear the ST-SD transmission.

That an intercept event occurs, when the capacity of the ST-E channel becomes higher than the data rate. Thus, given that a spectrum hole has been detected (i.e. ˆ*H* = *H*0), ST starts transmitting its signal to SD and E may overhear the ST-SD transmission. The corresponding IP is given by

$$P_{int}^{direct} =$$
$$pr(c_{se} > R | H = H_0, H_0) \Pr(H_0 | H = H_0) +$$
$$\Pr(c_{se} > R |$$
$$\text{H}=(H_0 | H = H_1) \Pr(H_1 | H = H_0) = \pi_0 \Pr(|hse|^2 > \Delta) +$$
$$\pi_1 \Pr\left(|hse|^2 - |hpe|^2 \gamma_p \Delta > \Delta\right),$$

III. RELATED WORKS

Amitav Mukherjee[1], 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.

Timothy X Brown [2], Cognitive radios sense spectrum activity and apply spectrum policies in order to make decisions on when and in whatbands they may communicate. These activities go beyond what isdone when traditional radios communicate. This paper examinesthe denial of service vulnerabilities that are opened by theseadditional activities and explores potential protection remediesthat can be applied. An analysis of how vulnerable are victimcognitive radios to potential denial of service attacks is presentedalong different axis, namely the network architecture employed,the spectrum access technique used and the spectrum awarenessmodel. The goal is to assist cognitive radio designers to incorporateeffective security measures now in the early stages of cognitiveradio development.

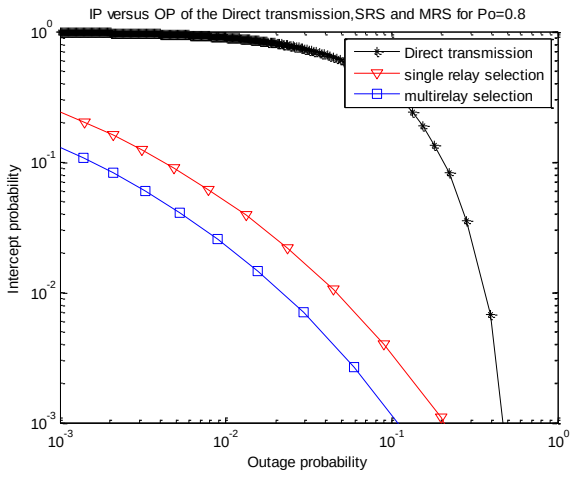
Sriram Lakshmanan[3], We describe the scope of the work namely the environment, metric and the assumptions about the eavesdropper. Then, we describe the need for and use of a"physical space security" approach. Subsequently, we describe how beamforming canbe applied as a baseline strategy for securing against eavesdropping. We highlight why such a technique is insufficient by itself and summarize the motivations for a better physical space security technique.

Ian F. Akyildiz[4], Cognitive radio networks will provide high bandwidth to mobile users via heterogeneous wireless architectures and dynamic spectrumaccess techniques.. 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.

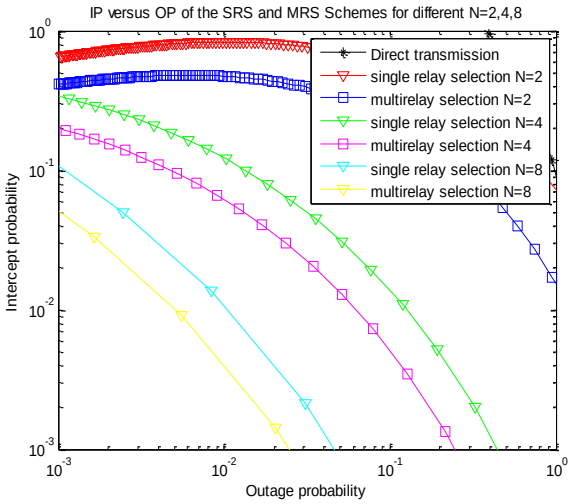
Yulong Zou[5],proposes the Extensive studies have been carried out for protecting CR networks both against primary user emulation (PUE) and against denialVof-service (DoS) attacks . In addition to PUE and DoS attacks,eavesdropping is another main concern in protecting the data confidentiality , although 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.

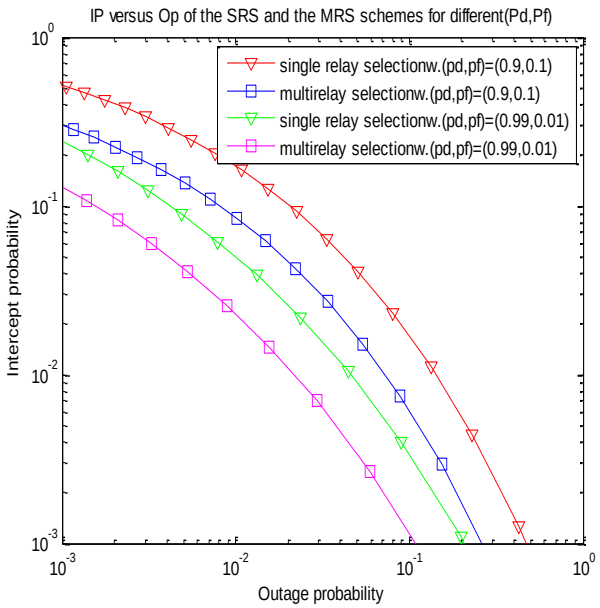
II. statistical analysis and results

We present our performance comparisons among the direct transmission, the SRS and MRS schemes in terms of their SRT. The simulated IP and OP results of the three schemes are also given to verify the correctness of the theoretical SRT analysis. In our computer simulations, the fading amplitudes (e.g., $|hsd|$, $|hsi|$, $|hid|$, etc.) are first generated based on the Rayleigh distribution having different variances for different channels. Then, the randomly generated fading amplitudes are substituted into the definition of an outage (orintercept) event, which would determine whether an outage (orintercept) event occurs or not. By repeatedly achieving this process, we can calculate the relative frequency of occurrence for an outage (intercept) event, which is the simulated OP (or IP). Additionally, the SDP Pd and FAP Pf are set to Pd = 0.99and Pf = 0.01, unless otherwise stated. The primary signalto-noise ratio (SNR) of γp = 10 dB and the data rate of$R$ = 1 bit/s/Hz are used in our numerical evaluations.

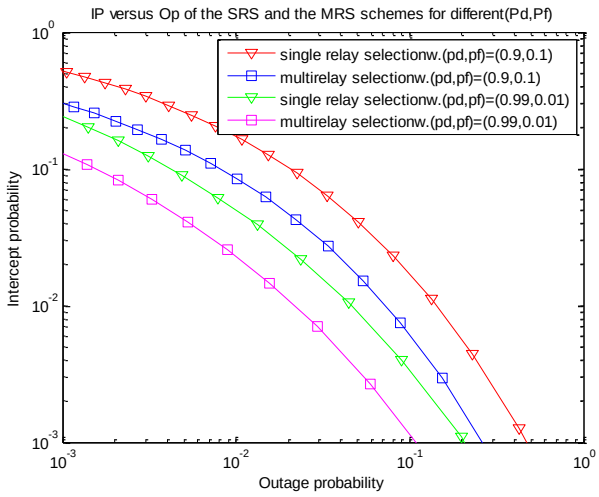


For a fair comparison,the total transmit power of the desired signal *xs* and the artificial noise are constrained to *Ps*. Moreover, the equal power allocation method is used in the numerical evaluation IP versus OP of the direct transmission,as well as the SRS and MRS schemes for $P0$ = 0.8, where the solid lines and discrete marker symbols represent the analytical simulated results, respectively. It can be seen from that the IP of the direct transmission, the artificial noise based as well as of the proposed SRS and MRS schemes all improve upon tolerating a higher OP, implying that a trade-off exists between the IP (security) and the OP (reliability) of CRtransmissions. Proposed SRS and MRS schemes outperform the direct transmission and the artificial noise based approaches in terms of their SRT, showing the advantage of exploiting relay selection against the eavesdropping attack. Moreover, the SRT performance of the MRS is better than that of the SRS





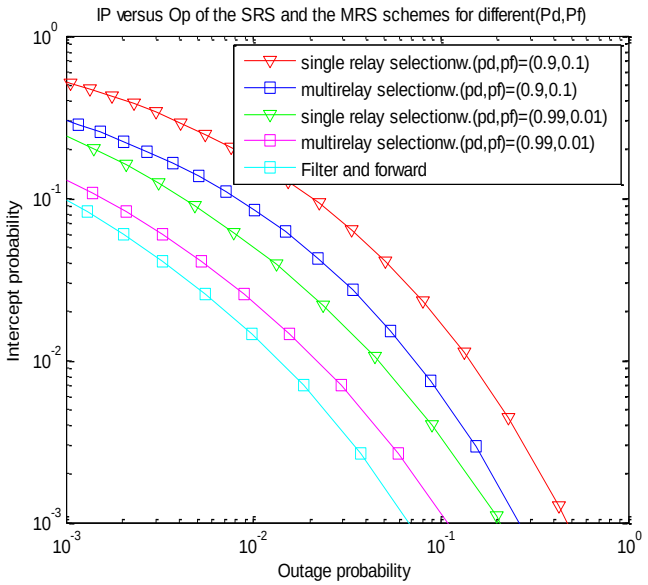
Although the MRS achieves a better SRT performance than its SRS-aided counterpart, this result is obtained at the cost of a higher implementation complexity,since multiple SRs require high-complexity symbol-level synchronization for simultaneously transmitting to the SD, whereasthe SRS does not require such elaborate synchronization our numerical SRT comparison between theSRS and MRS schemes for $P0 = 0.2$ and $P0 = 0.8$. Observe from that the MRS scheme performs better than the SRSin terms of its SRT performance for both $P0 = 0.2$ and $P0 = 0.8$.That as $P0$ increases from 0.2 to0.8, the SRT of both the SRS and MRS schemes improves.This is because upon increasing $P0$, the licensed band becomes unoccupied by the PUs with a higher probability and hence the secondary users (SUs) have more opportunities for accessingthe licensed band for their data transmissions, which leads to a reduction of the OP for CR transmissions. Mean whileincreasing $P0$ may simultaneously result in an increase of the IP,since the eavesdropper also has more opportunities for tapping the cognitive transmissions. However, in both the SRS and MRS schemes, the relay selection is performed for the sakeof maximizing the legitimate transmission capacity withoutaffecting the eavesdropper's channel capacity. Hence, uponincreasing $P0$, it becomes more likely that the reduction of OPis more significant than the increase of IP, hence leading to anoverall SRT improvement for the SRS and MRS schemeswe depict the IP versus OP of the SRS and MRSschemes for different spectrum sensing reliabilities, where$(Pd,Pf) = (0.9,0.1)$ and $(Pd,Pf) = (0.99,0.01)$ are considered.It is observed that as the spectrum sensing reliability is improvedfrom $(Pd,Pf) = (0.9,0.1)$ to $(Pd,Pf) = (0.99,0.01)$, theSRTs of the SRS and MRS schemes improve accordingly. Thisis due to the fact that for an improved sensing reliability, anunoccupied licensed band would be detected more accuratelyand hence less mutual interference occurs between the Pusand SUs, which results in a better SRT for the secondarytransmissions.That for $(Pd,Pf) = (0.9,0.1)$and $(Pd,Pf) = (0.99,0.01)$, the MRS approach outperforms theSRS scheme in terms of the SRT, which further confirms the advantageof the MRS for protecting the secondary transmissionsagainst eavesdropping attacks



The above figure the IP versus OP of the conventional direct transmission as well as of the proposed SRS and MRS schemes for $N = 2$, $N = 4$, and $N = 8$. that the SRTs of the proposed SRS and MRS schemes are generally better than that of the conventional direct transmission for $N = 2$,$N = 4$ and $N = 8$. Moreover, as the number of SRs increases from $N = 2$ to 8, the SRT of the SRS and MRS schemes significantly improves, explicitly demonstrating the security and reliability benefits of exploiting multiple SRs for assisting the secondary transmissions. In other words, the security and reliability of the secondary transmissions can be concurrently improved by increasing the number of SRs. Upon increasing the number of SRs from $N = 2$ to 8, the SRT improvement of MRS over SRS becomes more notable. Again, the SRT advantage of the MRS over the SRS comes at the expense of requiring elaborate symbol-level synchronization among the multiple SRs for simultaneously transmitting to the SD.

The network relays use the filter-and-forward (FF) strategy to compensate for the transmitter-to-relay and relay-to-destination channels using finite impulse response (FIR) filters. With the channel state information (CSI) being available at the receiver, the transmit relay power is minimized subject to the destination quality-of-service (QoS) constraint

TS



FILTER AND FORWARD

IV. CONCLUSION

1. In this paper, we improve the security of transmission in a secondary network in the presence of an eavesdropper. Wee examined the SRT performance of the SRS and MRS assistedd secondary transmissions in the presence of realistic spectrumm sensing, where both the security and reliability of secondaryy transmissions are characterized in terms of their IP and OPP respectively. We also showed that the proposed SRS and MRSS schemes generally

outperform the conventional directt transmission 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[5].

The usage of filter and forward relay selection improves co-operative and non co-operative spectrum sensing. Further it helps to reduce the power consumption and to simplify the transmitter receiver network. This relay helps to boost the signal and so increases reliability of the system. As a result the probability of loss in the channel is decreased

REFERENCES

[1]G. Baldini, T. Sturman, A. R. Biswas, and R. Leschhorn, "Security aspectsin software defined radio and cognitive radio networks: A survey and away ahead," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 355–379,May 2012.

[2] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues inspectrum sensing for cognitive radios," in Proc. 38th Asil. Conf. Signal,Syst. Comput., Pacific Grove, CA, USA, Nov. 2004, pp. 772–776.

[3] H. Li, "Cooperative spectrum sensing via belief propagation in spectrumheterogeneous

cognitive radio systems," in Proc. IEEE WCNC, Sydney,N.S.W., Australia, Apr. 2010, pp. 1–6.

[4] J.Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperativespectrum sensing in cognitive radio networks," IEEE Trans. WirelessCommun., vol. 7, no. 11, pp. 4502–4507, Nov. 2008.

[5] yulong zou,champagneand wei-ping zhu,"relay selection improves the security –reliability trade-off in cognitive radio systems"IEEE

[6] R. Southwell, J. Huang, and X. Liu, "Spectrum mobility games," in Proc.31st INFOCOM, Orlando, FL, USA, election Mar. 2012, pp. 37–45.

[7] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty,"A surveyonspectrum management in cognitive radio networks," IEEE Commun.Mag., vol. 46, no. 4, pp. 40–48, Apr. 2008.

[8] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulationattacks in cognitive radio systems part I: Known channel statistics,"IEEE Trans. Wireless Commun., vol. 9, no. 11, pp. 3566–3577,Nov. 2010.