Indian Journal of Science and Technology, *Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102134, October 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Optimal Tradeoff between Security and Reliability in systems of Cognitive Radio

K. S. Preetha* and S. Kalaivani

School of Electronics Engineering, VIT University, Vellore - 632014, Tamil Nadu, India;
kspreetha@vit.ac.in

Abstract

Objectives: To propose relay selection plans for a CR network. A network of Cognitive Radio (CR) is considered. It comprises of one Secondary Transmitter (ST), a set of multiple Secondary Relays (SRs) and one Secondary Destination (SD) and an eavesdropper is also present. Here the ST is transmitting to SD assisted by SRs, while eavesdropper attempts interception of secondary transmission. **Methods:** Care is exercised in selecting relay to protect ST-SD transmission. Protection is against eavesdropper both single-relay as well as multi-relay aid that. In particular, possibly best SR gets chosen in a single-relay type selection to assist transmission of secondary type. Multi-relay selections invoke multiple SRs for simultaneous forwarding of transmission of ST to SD. **Findings:** Both probabilities of intercept as well as outage are analyzed for the put forth single-relay as well as relay of multi type selecting methods meant for transmission of secondary type. This relies upon the realistic kind of sensing of spectrum. Evaluation of performance is done on the classic type transmission of direct kind and also the approaches of artificial noise based for comparing them with proposed schemes of relay selection. **Improvements/Applications:** It shows that relaxing intercept probability requirement improves performance of outage related to transmission of direct type, schemes for selection of relay and also-based on noise of artificial type-scheme and vice versa. This leads to the implication that a trade-off is done between reliability and security of secondary transmission when eavesdropping attacks are present. This implication is popularly coined as security to reliability - a trade-off (SRT). Also it is demonstrated that SRTs schemes of single-relay as well as multi-relay selection are normally better compared to classic direct transmission. It explicitly demonstrates the salient features of selection of relay scheme in question. This is related to offering protection to transmissions of secondary type from attacks of eavesdropping. Apart from this there is an increase in SRs' count, obviously SRTs about relay of single type in question now as well as relay of multi type selection method improve substantially.

Keywords: Attack Due to Eavesdropping, From Security to Reliability - A Trade-Off, Outage Probability, Probability due to Intercepting, Radio of Cognitive Type, Selection of Relay

1. Introduction

Aspects related to security of the Radio Of Cognitive type (CR) schemes are inviting due increase in attention from the community ventured into research[1]. This is an obvious fact that CR network architecture is highly dynamic in nature. Devices meant for CR are becoming visible in limelight to attackers in the internal and also the external domain. Obviously the extreme vulnerability to the malicious behaviour exists. So, CR clients fail to do accurate characterizing of their ambient radio situation. It amounts to getting carried away or even getting half way through and it ends up in a faulty functioning or even a total glitch. Consider the other possibility, a client who has no legitimacy will try tapping of eligible CR clients' communications through eavesdrop attempt and access information of confidential nature. Definitely, the networks meant for CR are facing a plethora of threats related to security. They are taking place at times of the sensing of spectrum, spectrum mobility, spectrum sharing and spectrum management[2].

**Author for correspondence*

By tradition, cryptographic techniques are being employed to guarantee transmitting confidential information protecting that from attack due to the act of eavesdrop[3]. It is introducing significant computational overhead and imposes more complexity being added to system also, by way of management of key of secret kind. Other than that, existing cryptographic approach is not so secure enough and so decryption by an eavesdropper (E) is still possible. Physical-layer security emerges as one of the efficient approach to do defending of authorized clients against that of attacks by way of eavesdrop which exploits characteristics of physical type belonging to the channels of wireless type[4]. It is possible to achieve perfectly secure as well as reliable transmission. In addition, maximum possible rate of secrecy is being realised at destination that is legitimate, termed as capacity of secrecy. That is nothing but variation between capacities of the main and the channel of wiretap kind.

For combating effects due to the fading, both the input of multiple type and output of multiple kind (MIMO) methods, the relaying of cooperative type as well as beam forming techniques are investigated for enhancing wireless secrecy capacity that is practically achievable[5]. Rate of secrecy that is achievable for the transmission of secondary type's investigation conducted the QoS constraint which is specific and that is being carried out on transmission of primary type. Unlike conventional non-cognitive networks of wireless type, security related to layer of physical type belonging to the networks of CR need considering the challenges exist in addition which are varied. It includes protecting primary client's requirements like QoS including the fact of getting relieved from interference of mutual type among primary and transmissions of secondary type. The consideration, enthuses one in exploring of security related to layer of physical type belonging to the networks of CR which includes Secondary Transmitter type (ST) that communicates to one destination of secondary kind (SD). The relays are of multiple kinds which are secondary in nature (SR) while an attacker of unauthorized type is present - such a situation is undertaken here.

SRT is of primary concern to do investigation. This finding is related to transmission which relays and this is of cognitive type while the sensing of spectrum of realistic type is present[6]. The very principle about SRT considering in the context of security of layer of physical type in wireless domain is being brought in and it is being under scrutiny. Here security as well as reliability is being characterized with respect to probability of intercept as well as probability due to outage. The paper's primary findings are given:

- Schemes related to selection of relay in two different ways, that is about both - selecting relay of single type as well as its counterpart namely relay of multiple type, for the protection meant for transmissions of secondary type; this is against the attacks by way of eavesdrop. Considering the scheme of selection of relay of single type (SRS) one and only a relay that is single, being taken by way of selecting. This is done among a group containing SRs in multiple existence. It is done to carry out forward transmissions of secondary type from a ST towards a SD. Considering on the contrary the method of selecting relay of multi type (MRS) is making use of SRs belonging to multiple group type for doing simultaneous assistance of ST-SD transmissions.
- Proposed schemes of SRS as well as MRS' analysis of SRT being done mathematically. This is done when sensing of spectrum in realistic manner is present. Results of SRT expressed numerically demonstrates SRS being put forth as well as methods of MRS in general excel the traditional transmission that is of direct type as well as the one based on noise that is artificial in the overall approach in terms of respective SRTs. These are being given for comparing purpose.
- Now presented matter is about the fact that when reliability of sensing related to spectrum is on the increase, while probability alarm of false kind being on reduction or the the latter alone occurs, there is an appreciable improvement in the methods of SRS as well as MRS' SRTs. Results expressed numerically demonstrates clearly the methods of SRS as well as MRS in general excel the traditional transmission of direct type as well as approach based on noise of artificial type in terms of respective SRTs.

2. System Model

Physical-layer security's general framework model in the CR systems is first presented. Next is sign model of ordinary direct transmission method. This will serve as the seat marker and of SRS as well as MRS plans to enhance security of CR framework against spying assaults.

Primary network that coexists along with secondary network is being considered as shown in Figure 1 (this is in addition to being mentioned as network of CR). Network of Primary type is including station of base type that is primary (PBS) as well as users who is primary (PUs) who are multiple in number, that communicates to PBS through spectrum that is licensed. In a contrasting way, network of secondary type consisting one otherwise even many of the STs as well as the SDs do exploitation to spectrum that is licensed in a manner that sounds very much like if there is a chance avail that. In particular, a specific type ST initially shall do detection employing the support of with aid of the sensing of spectrum such that PBS' occupancy is there in the spectrum that is licensed or not. In case that is there, ST has no freedom to do transmission so as to do avoiding interference with the PUs. If in case it is otherwise, spectrum that is licensed is being considered as there is a unoccupancy (for example one hole of spectrum being noticed), ST might afterwards do transmission towards SD over the noticed hole of spectrum. E in the mean time is trying to do interception of transmission of secondary type towards SD from that of ST. To suit to express in notation, considerH_0 as well as H_1 shall stand for an event when there is unoccupancy in spectrum that is licensed while the other has occupancy by that of PBS atone slot in time that is specific. One can assume$\widehat{H}$ stand for condition rather status about spectrum that is licensed being detected through the sensing of spectrum. To be specific $\widehat{H} = H_0$ represent the situation when spectrum that is licensed being considered when there is a unoccupancy and let$\widehat{H} = H_1$ indicate that spectrum that is licensed being supposed to have occupancy.

P_d stands for the probability representing the correctly detected PBS' presence as well as probability of alarm of false type that is associated, it is being represented as P_f is being given a definition by$P_d = P_r\left(\widehat{H} = {H_1}/{H_1}\right)$ and also $P_f = P_r\left(\widehat{H} = {H_1}/{H_0}\right)$, respectively[7]. Owing to noise of background as well as the fading effect, possibility to end up with an ideal kind of reliable type of the sensing of spectrum with non skipping of the act of detecting a type of PU being active while there is no alarm of false type, suggesting the fact a band of spectral kind is being with an occupancy by one PU; in actual case it is unoccupied. Besides that, PBS' presence that is missed without being detected is going to cause interfering event among the PU as well as the SU. For ensuring interference imposed on the PUs that it remains now at particular level that can be tolerated, it is required that detecting successfully, whose probability (SDP) is denoted by P_d as well as the probability of alarm that is false (FAP) denoted by P_f shall get confined inside a particular reasonable range of target.

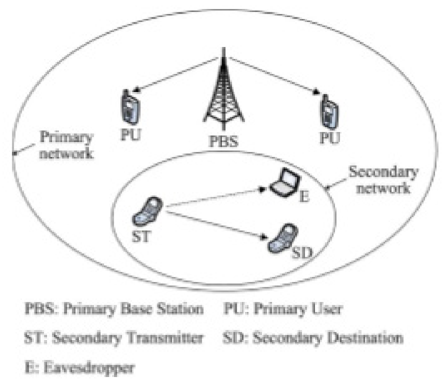

Figure 1. A primary wireless network in coexistence with a secondary CR network.

3. Proposed Relay Selection Scheme

3.1 Transmission of Direct type

To begin with, consider the traditional transmission of direct type being a measuring yardstick for this method. x_p and x_s stand for symbols that are random being on transmit through PBS as well as ST in an instant. In a situation when no generality kind of loss exist, let one take it for granted $E[|x_p|2] = E[|x_s|2] = 1$. Here $E(\cdot)$ represent that operator for value expected. Powers during Transmit by PBS as well as the ST is being P_p as well as P_s. When the fact is that spectrum which is licensed is being taken for granted that it is without occupancy of PBS (for example$\widehat{H} = H_0$), the ST is transmitting its signal x_s at a particular power P_s., received signal at a SD is expressed as follows:

$$y_d = \boldsymbol{h}_{sd}\sqrt{P_{sx_s}} + \boldsymbol{h}_{pd}\alpha P_{px_p} + n_d \tag{1}$$

Here $\boldsymbol{h}_{sd}$ and $\boldsymbol{h}_{pd}$ stand for channel's coefficients due to fading which spans up to SD from that of ST and then that up to SD from that of PBS. Combining the formula for capacity proposed by Shannon, ST-SD channel's capacity is realised as given:

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

Here $\gamma_s = P_s / N_0$ and $\gamma_p = P_p / N_0$. In the same way, the ST-E channel's capacity is

$$C_{se} = log_2(1 + |h_{se}| \, 2\gamma_s \alpha |h_{pe}| 2\gamma_p + 1) \quad (3)$$

3.2 Single-Relay Selection

This subsection considers cognitive relay network where both the SD and E are being taken for granted to exist beyond ST's area of coverage and the N relays of secondary type (SRs) are being employed to assist transmission of ST-SD that is cognitive. One can assume a channel with a control that is common (CCC) is being available to coordinate different network nodes' action and Decode-and-Forward (DF) relaying making use of a couple of two slots of time that are adjacent. To be specific, once the spectrum that is licensed is being considered to have unoccupancy; initially ST does broadcasting of its signal x_s to N SRs that attempt to do decoding of x_s from their respective signals received. Hence, received signal at one specific SRi is represented by:

$$y_i = h_{si}\sqrt{P_{sx_s}} + h_{pi}\alpha P_{px_p} + n_i \quad (4)$$

Here h_{si} and h_{pi} represent coefficients due to fading of ST-SRi channel as well as PBS-SRi channel. Received signal at a place SD is:

$$y_d = h_{id}\sqrt{P_{sx_s}} + h_{pd}\alpha P_{px_p} + n_d \quad (5)$$

Here h_{id} represents fading coefficient of SRi–SD channel.

3.3 Multi-Relay Selection

One MRS scheme is presented now. The subsection presents. Here SRs which are multiple are being employed for forwarding source signal simultaneously x_s to the SD. To be very specific, the ST first transmits x_s to N SRs over one detected hole in spectrum. Received signal at a SD is:

$$y_{multi\ d} = \sqrt{P_{sw}} T H d_{x_s} + \alpha P_{ph_p} d_{x_p} + n_d \quad (6)$$

MRS and SRS methods achieve almost same performance considering in terms of wiretap channel's capacity as given in Table 1. Once given a requirement of outage that is fixed, MRS scheme achieves an improved performance of intercept than method of SRS. This is because of the fact according to SRT, a reduction in outage is achieved by capacity enhancement of legitimate transmission based on MRS will be converted into an improvement in intercept.

Table 1. IP and OP values for SRS and MRS for N = 2, 4, 8

No. of channels	Relay	IP	OP
N = 2	SRS	0.3	0.3
	MRS	0.2	0.3
N = 4	SRS	0.01	0.1
	MRS	0.007	0.1
N = 8	SRS	0.009	0.01
	MRS	0.004	0.01

4. Results and Discussion

In this segment, we introduce our execution examinations among the immediate transmission, the SRS and MRS plans regarding their SRT. The IP of the immediate transmission, the artificial noise based and in addition of the proposed SRS and MRS conspires all enhance enduring a higher OP, suggesting that an exchange off exists between the IP (security) and the OP (dependability) of CR transmissions. Both the proposed SRS and MRS plans beat the immediate transmission and the artificial commotion based methodologies as far as their SRT. Additionally, the SRT execution of the MRS is superior to that of the SRS as appeared in Figure 2.

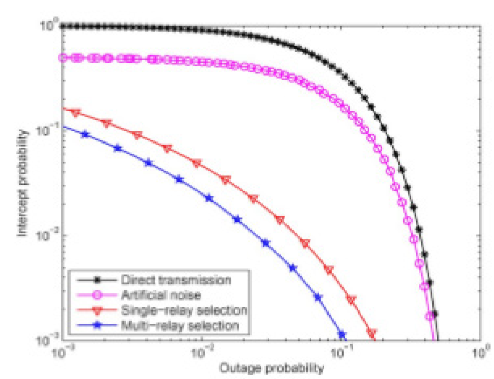

Figure 2. IP versus OP of the direct transmission, the SRS and the MRS schemes for different P_0 with $P_0 = 0.8$, $\gamma_s \in [0, 35\ dB]$, N = 6.

In Figure 2, we portrayed our numerical SRT examination between the SRS and MRS plans for $P_0 = 0.2$ and $P_0 = 0.8$. The MRS plan performs superior to the SRS as far as its SRT execution for both $P_0 = 0.2$ and $P_0 = 0.8$. As P_0 increments from 0.2 to 0.8, the SRT of both the SRS and MRS plans moves forward. This is on account of after expanding P_0 , the authorized band gets to be empty by the PUs with a higher likelihood and henceforth the auxiliary clients (SUs) have more open doors for getting to the authorized band for their information transmissions, which prompts a diminishment of the OP for CR transmissions. In the mean time, expanding P_0 may all the while result in an expansion of the IP, since the meddler additionally has more open doors for tapping the subjective transmissions.

The IP versus OP of the ordinary direct transmission and in addition of the proposed SRS and MRS plans for N = 2, N = 4 and N = 8 is appeared in Figure 3. It is watched that the SRTs of the proposed SRS and MRS plans are for the most part superior to that of the routine direct transmission for N = 2, N = 4 and N = 8. Besides, as the quantity of SRs increments from N = 2 to 8, the SRT of the SRS and MRS plots significantly progresses. As it were, the security and reliability of the auxiliary transmissions can be simultaneously enhanced by expanding the quantity of SRs. Furthermore, after expanding the quantity of SRs from N = 2 to 8, the SRT change of MRS over SRS increments.

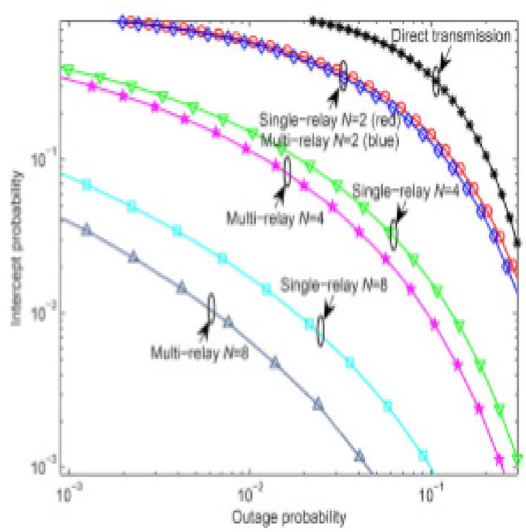

Figure 3. IP versus OP of the direct transmission, the SRS and the MRS schemes for different N with $P_0 = 0.8$, $\gamma_S \in [0, 30\ dB]$, N = 6.

In Figure 4, we delineate the IP versus OP of the SRS and MRS plans for various range detecting reliabilities, where $(P_d, P_f) = (0.9, 0.1)$ and $(P_d, P_f) = (0.99, 0.01)$ are considered. It is watched that as the range detecting reliability is enhanced from $(P_d, P_f) = (0.9, 0.1)$ to $(P_d, P_f) = (0.99, 0.01)$, the SRTs of the SRS and MRS plans enhance as needs be. This is on the grounds that for an enhanced detecting reliability, an abandoned authorized band would be identified all the more precisely and consequently less common obstruction happens between the PUs and SUs, which results in a superior SRT for the optional transmissions. Figure 3 likewise demonstrates that for $(P_d, P_f) = (0.9, 0.1)$ and $(P_d, P_f) = (0.99, 0.01)$, the MRS approach beats the SRS plan regarding the SRT, which further confirms the upside of the MRS for ensuring the optional transmissions against listening in assaults.

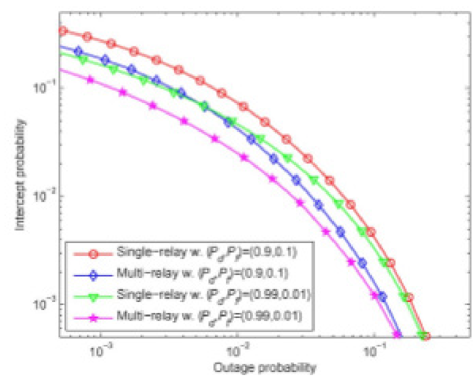

Figure 4. IP versus OP of the SRS and the MRS schemes for different (P_d, P_f) with $P_0 = 0.8$, $\gamma_S \in [0, 30\ dB]$, N = 6.

5. Conclusion

In the paper, relay selection plans for a CR network are proposed. The SRT execution is analyzed in the light of the SRS and additionally MRS helped optional sort transmissions in nearness of the practical sort range detecting. Here both security and unwavering quality of the auxiliary transmissions are being described regarding the individual IP and the OP separately. The SRT of traditional direct transmission as benchmark is additionally broke down. As reliability of spectrum sensing is increased, SRTs of both SRS and the MRS strategies get progressed. It is additionally demonstrated that proposed SRS and the MRS methods in general exceeds the conventional direct type transmission and also artificial noise based approach as far as the particular SRT. Moreover, SRT execution of the MRS is much better than SRS. In addition, as there is an increase in the number of SRs, SRTs of both SRS and of MRS strategies get enhanced significantly, exhibiting the respective advantages as far as both certainity and the reliability of the auxiliary transmissions getting upgraded.

6. References

1. Baldini G, Sturman T, Biswas AR, Leschhorn R, Godor G, Street M. Security aspects in software defined radio and Cognitive Radio networks: A survey and a way ahead. IEEE Communications Surveys and Tutorials. 2012 May; 14(2):355–79.
2. Cabric D, Mishra SM, Brodersen RW. Implementation issues in spectrum sensing for Cognitive Radios. Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers; 2004 Nov 1. p. 772–6.
3. Li H. Cooperative spectrum sensing via belief propagation in spectrum-heterogeneous Cognitive Radio systems. 2010 IEEE Wireless Communication and Networking Conference; 2010 Apr. p. 1–6.
4. Ma J, Zhao G, Li Y. Soft combination and detection for cooperative spectrum sensing in Cognitive Radio networks. IEEE Transactions on Wireless Communications. 2008 Nov; 7(11):4502–7.
5. Ghasemi A, Sousa ES. Fundamental limits of spectrum-sharing in fading environments. IEEE Transactions on Wireless Communications. 2007 Feb; 6(2):649–58.
6. Southwell R, Huang J, Liu X. Spectrum mobility games. 2012 IEEE Proceedings on INFOCOM; 2012 Mar. p. 37–45.
7. Akyildiz IF, Lee WY, Vuran MC, Mohanty S. A survey on spectrum management in Cognitive Radio networks. IEEE Communications Magazine. 2008 Apr; 46(4):40–8.