A Review on Security Improvements by Relay Selection in Cognitive Radio Networks

Hima Anna thomas[1], Sajan Xavier[2]
1 P.G Student, Dept. of Electronics and Communication, NCERC Thiruvilwamala,himaanna20@gmail.com
2 Asst. professor, Dept. of Electronics and Communication, NCERC Thiruvilwamala,sajanxavier100@gmail.com

ABSTRACT

In this paper, various methods for security improvement in cognitive radio networks are discussed and relay selection methods have found more effective. Relay selection is utilizing the cooperative communication technique and along with decode and forward configuration various relay selection methods are found implemented successfully. According to relay selection the number of relays participating in secondary transmission is also act a vital role. The multi-relay relay selections methods can be treated as the most appropriate method that provides maximum security and reliability in CR networks.

Key Words: Cognitive radio, relay selection, secondary transmission, security.

1. INTRODUCTION

Recently, Cognitive Radio Networks (CRNs) are being considered as a new incarnation in wireless networks that can improve the utilization of the electromagnetic spectrum. The dynamic spectrum access (DSA) enabling technique of CRNs allows unlicensed users (known as secondary users) to communicate with each other over the unused licensed bands (called spectrum holes) detected through spectrum sensing. Thus the chances of effective utilization of licensed bands by secondary users occur without affecting the quality of primary user communication. The dynamic spectrum access in CR networks includes spectrum management, spectrum sharing, spectrum migration and spectrum sensing. These techniques are vulnerable to various wireless network attacks. Relay selection techniques can be considered as an answer for the emerging security challenges and quality compromises in cognitive radio networks

.

2. SECURITY ISSUES AND COUNTER MEASURES IN CR NETWORKS

Several security issues in CRN occur due to various aspects of dynamic spectrum access technology. The different security attacks in physical layer are like below.

The attackers may mimic the primary users by generating signals resembling them. These signals will result in wrong perception of the secondary users about the channel state. This is called as primary user emulation attacks (PUE) and it can be of selfish type or malicious type depends on the purpose and usage of the attacker. Another one type of attack which greatly affects the goodwill of CR network is primary user interference. When secondary users are occupying in the grey space of frequency band along with the primary users the consequences of this attack is getting increased. The tampering of the control information reaching at the fusion centre will affect the entire network. This type of attack is known as data tamper attack of spectrum sensing.

The manipulation of different parameters used in cognitive networks by the attacker may also cause decreasing the security level. Different parameters like center frequency, bandwidth etc is taken as inputs for calculating the required goals of the cognitive radio users. The major goals of radios are low power, high rate and high security. According to the usage of the channel (whether for audio, video or voice transmission) the channel requirement of the radio users varies. When a radio starts to calculate the objective function with the available parameters, the attacker may result into an objective function that will reduce the level of security. That will ease the intrusion of the adversary into the licensed frequency bands.

The secondary users may turn into jammers due to the effects of attacker. Secondary users are using some spectrum sensing algorithms to know the channel vacancy. The attackers may work on the parameters used for calculating this objective functions. Thus the secondary users will lead to end up in the decision such that to occupy in the frequency bands when it is occupied by primary users. This will reduce the throughput and increase the interference to the primary users and secondary users become malicious unknowingly.

When an attacker send manipulated local spectrum sensing results to its neighbours or to the fusion centre, causing the receiver to make a wrong spectrum-sensing decision. This is known as spectrum sensing data falsification (SSDF)[5]. This effect is mainly in distributed CRNs. When many CR users want to communicate at the same time the communication control channel becomes insufficient. An attacker can utilize this feature and generate forged MAC control frames for the purpose of saturating the control channel and thus decreasing the network performance due to Link layer collisions [6]. In a multi-hop CRN, a CR host can refuse to forward any data for other hosts [5][6]. This will allow it to conserve its energy and increase its own throughput which resulted from selfish channel concealment [6]. This type of attack is called selfish channel negotiation. Several network and transport layers will also cause degradation of the cognitive radio reputation.

The physical layer attacks can be avoided by means of tests that calculate signal strength and phase difference etc to find out malicious nodes. Jamming techniques are also used. Implementing certain decision thresholds will reduce the link layer security issues. Some trust based architectures can be used for identifying the malicious CR hosts. Usage of trusted third parties and encryption methods to encrypt, decrypt and authentication of CR users are widely used as the solution to the network and transport layer security attacks

3. RELAY SELECTION METHODS USED IN CR NETWORKS

Cooperative communication is implemented in CR networks because of the inadequacy of a single wireless device in various network services. Channel parameters like frequency, time etc varies randomly so the usage of single network device will lead to insufficient battery power consumption and reduced battery life. In cooperative communication the node concept is changed to three nodes where a supporting node called relay node is added within the network including sender and receiver. The relay node is also a CR user, who acts as an intermediate node to help forwarding of signal to the destination. Thus the secondary users who were previously had considered as interference to the primary users turned into supporting agents. The following figure 1 shows a cooperative communication model [7].

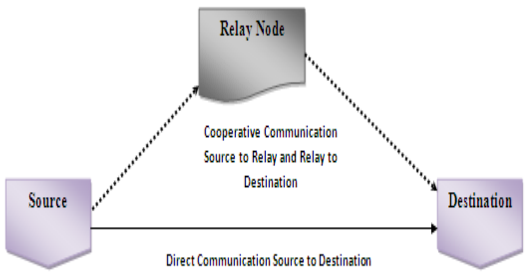

Figure 1: Basic modeling of cooperative communication

The important task in cooperative communication is the selection of a relay node or a set of relay nodes. Due to abundance of secondary users and the presence of hostile nodes this task becomes crucial.

Nature of relay selection techniques are based on the time of selection and the level of interaction. Opportunistic relay selection schemes include measurement based, performance based, threshold based, contention based, table based, adaptive relay selection and multi-hop relay selection. In measurement based relay selection method the channel state information obtained from local measurements is utilized for relay selection. But this measurement based methods suffers from the disadvantage of computational complexity. Performances based relay selection method is the optimization of the measurement based method. In this method the suitable relays are selected depending on the performance factors like delay, energy efficiency etc. If the performance conditions are not met for any relay nodes then transmission will be continues in the direct link. In threshold based method some threshold values are set (like SNR, BER) to evaluate the quality of the competing relay nodes. Those nodes satisfying the threshold condition will only get the approval for forwarding the signal to the destination. The challenge in this method is the update of the threshold value according to the varying channel conditions. Table based relay selection approach is similar to a look-up table mechanism. The source will keep a CSI record of all potential relay nodes and potential channels. The relay node path will be selected by the source only if the total time for transmission is less than that of the direct transmission. Contention based relay selection methods are mainly aiming good resource allocation. This cooperative approach uses the contention window as the standard for selecting the best relay.

Adaptive relay selection scheme restricts the usage of helper nodes to the situations where the direct transmission is not at all possible. Sometimes, varying channel conditions may eliminate the need of a relay path where it had been used. Adaptive methods will decide the relay nodes adaptive to the channel variations.

In multi-hop relay selection the single relay or set of relays are selected based upon some predefined conditions but, when applied to multi-hop networks, this method requires the repetition of the relay selection procedure for each hop from sender to destination. But this method affects the capacity of channel. In multi-hop relay selection, the destination node may receive more than two independent signals of the same packet; this extra spatial diversity increases the performance and robustness.

4. SIGNIFICANCE OF RELAY SELECTION IN COGNITIVE RADIO NETWORKS

The main characteristics of good communication network are improved data rate, good signal strength, and broader coverage area. The application of relay selection have significant place in cognitive radio networks since all these basic characteristics are offered by it. When distance between the sender and receiver increases the relay nodes act as intermediate connecting nodes ensuring the good signal quality. The deployment of multi-hop relay nodes will reduce the need of additional base stations by extending the coverage area. Thus reducing the base station implantation cost. Slow and low data rate communications are always dejecting the broadband users, while relay selection offers a solution for this by providing nearby RF access points. Sometimes, relay nodes can act as hotspots to increase the capacity of the overall system. Since capacity increase and interference reduction are the gifts of relaying the overall transmission power is also reduced.

The secrecy of the signals transmitted is protected along with the reliability improvement in relay assisted cognitive radio networks. Several researches are now going on in application of relay selection methods in CR networks to improve security. Relay-jammer pair selection was utilized for increased security. Where one node will act as the relay node which transmits the signal to the source and the other node will act as a jammer to the eavesdropper. Different combinations of best relay, best jammer, random relay and random jammer can be used effectively for improving the secrecy rate [1]. The relay nodes are also selected based on the value of SNR too. In this scheme the relay node having the highest SNR is selected to forward the packet to the destination but the one with low SNR is chosen for source-relay and relay-eavesdropper transmissions [2]. These relay selection techniques are implemented in Decode and Forward (DF) cognitive radio networks using different coding schemes. The different coding schemes are turbo coding, Reed-Solomon coding and convolution coding [2]. Countless researches and implementation of relay selection methods are done to improve the security of cognitive radio networks.

4.1. Single and multi-relay selection methods for security enhancement

Consider the scenario of a secondary source and secondary destination transmit signal in the presence of an eavesdropper. The direct transmission between source and destination will not use any relay elements. The system model has two channels; one channel span the source to destination and other one span the source to eavesdropper. In direct transmission, the capacity of the channel between source and eavesdropper is as good as source to destination channel due to the absence of any factor which diminishes capacity of source to eavesdropper channel.

In relay selection methods the network is considered as the eavesdropper is beyond the coverage area of the secondary transmitter and N secondary relays are employed for secondary transmitter to secondary destination transmission. Also assuming a common control channel is employed for coordinating different nodes and decode -and-forward relaying [3]. More correctly, when there is a spectrum vacancy is found

ISSN 2229-5518

secondary transmitter will send their signal to N secondary relays and these relays attempts to decode the signal and transmits to the destination. For convenience we can represent these set of relay elements that succeed in decoding the signal as a set D which consist of 2^N subsets. The sample space of this set can be written like Eq.1 [3].

$$\Omega = \{\emptyset, D_1, D_2, ... D_{2^{N-1}}\} \quad (1)$$

Where Ø represents the empty set and Dn represents the n th non-empty subset of the N SRs (Secondary relays). If the set D is empty, implying that no SR decodes the secondary source transmitted signal successfully, then all the SRs remains silent and thus both SD (Secondary destination) and E (Eavesdropper) are unable to decode signal in this case. If the set D is non-empty, a specific SR is chosen from D to forward its decoded signal to SD.

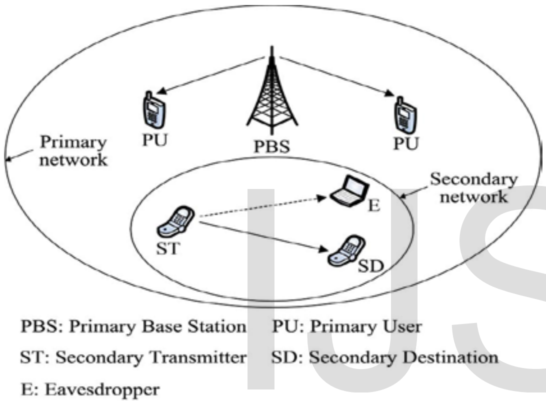

Figure 2: Graphical representation of single relay selection method

In single relay selection method as shown in figure 2 [3], only one relay element from the set D is used for forwarding the signal to the receiver. According to Shannon's coding theorem for successful transmission the capacity of the channel should be greater than that of channel data rate. When compared to direct transmission the channel capacity will be reduced to a factor of ½ since two orthogonal channels are utilized for the transmission from ST to SD via a single secondary relay (i^{th} secondary relay, SRi). The selection of the secondary relay is related to the ST-SR_i channel capacity CS_i and the data rate R. Thus event of selecting none of the relay ($D = \emptyset$) can be represented like Eq.2 as in [3].

$$CS_i < R, \ I \in \{1,2,.....,N\} \quad (2)$$

The event of $D=D_n$ can be represented using Eq.3 and Eq.4 as in [3]

$$CS_i < R, \ i \in D_n \quad (3)$$

$$CS_j < R, \ j \in D^-_n \quad (4)$$

Where D^-_n represent the complementary set D_n

The prime objective of relay selection is improving the ST-SD transmission, so the exact relay selection is based on the capacity of the channel from SR_i- SD denoted as C_{id} . So the 'best relay' selection can be written like Eq. 5 as in[3],

$$\text{Best SR} = \max C_{id(i \in Dn)} \quad (5)$$

C_{id} is independent of eavesdroppers channel state information (CSI). So we can select the best relay without the need of channel CSI. In multi-relay selection method multiple relay nodes are used for simultaneously forwarding the signal to the secondary destination. When the set D_n is not a null set we can understand that some relay nodes are successful in forwarding the signal to the destination. The use of multiple relay elements can made more effective by employing a weight factor [3].

$$w = [\, w_1, w_2, ... w_{|Dn|} \,]^T \quad (6)$$

Where $|D_n|$ is the cardinality of set D_n.

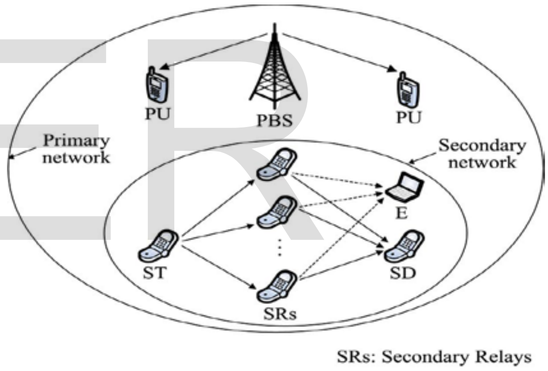

Figure 3: Graphical representation of multi-relay selection method

Figure 3 shows the multi-relay selection scheme representation [3]. The relay selection criteria in this case is depending upon the quantity called signal –to –interference –plus –noise ratio (SINR). SINR is a quantity used to give theoretical upper bounds on channel capacity (or the rate of information transfer) in wireless communication systems such as networks. Analogous to the SNR used often in wired communications systems, the SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise. The weight factor used for selection of the relays is optimised by maximising SINR at the SD yielding [3],

$$\max_{w} SINR_d^{mylti}, \ \text{s.t.} \ ||w||=1 \quad (7)$$

Using the Cauchy-Schwarz inequality , we can readily obtain the optimal weight vector w_{opt} from above equation as [3],

$$w_{opt} = H_d^* / |H_d| \quad (8)$$

which indicates that the optimal vector design only requires the SR-SD CSI *Hd*, whilst dispensing with the eavesdropper's CSI *He*[3]. H_d represents the set of all fading coefficients of the channels from relay elements to SD. H_e represents the set of fading coefficients of channels spanning from relay elements to eavesdropper. The difference between single and multi-relay schemes lies in the fact that the best relay selection is depends on the maximum value of the random variable h_{id} in single relay whereas sum of maximum value of h_{id} in multi relay selection. Based on this fact, we can say that multi relay selection have performance gain over single relay selection scheme.

4.2. Advantages of multi-relay selection scheme

As per the above relay selection methods MRS (multi-relay selection) is always outperforming the SRS (single relay selection scheme). The reason is that in SRS the relay which having the maximum h_{id} is selected but in MRS scheme the set of relay combinations that provide maximum value for the sum of h_{id} is utilized for transmission. Thus the channel capacity towards the SD is increased in MRS compared to SRS. MRS and SRS will not provide any considerable increase or decrease in the performance of the wiretap channel (channel towards eavesdropper). 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. As the number of relay elements increases the performance of the multi-relay selection method is also improving. Since multiple number of relays are simultaneously transmitting to the destination the synchronization problem can consider as complexity of MRS. But the increased ST-SD channel capacity can consider as inevitable and this feature makes MRS usage is widespread in cognitive radio communication networks.

5. CONCLUSION

Analyzing various methods for security and quality improvement in cognitive radio networks, relay selection methods have found more effective. Among relay selection the number relays participating in secondary transmission is also act a vital role. The multi-relay relay selection methods can be treated as the appropriate method that provides maximum security and reliability in CR networks. Moreover different methods for selecting multiple relay elements include trust based methods provide improved performance and further studies on transmission to multiple destinations are under progress which may increase security level much better.

REFERENCES

[1] "Relay selection for security enhancement in cognitive relay networks" Yuanwei Liu, Lifeng Wang, Tran Trung Duy, Maged Elkashlan, and Trung Q. Duong, IEEE wireless communications letters, Vol. 4, no. 1, Feb 2015

[2] "Secrecy rate maximization under improved relay selection with different coding schemes for cooperative wireless network" Akanksha Rai1, Mrs. Rupali Phatak IJARC C E, Vol. 4, Issue 7, July 2015.

[3] "Relay-selection improves the security-reliability trade-off in cognitive radio systems", Yulong Zou, Benoit Champagne, Wei-Ping Zhu, and Lajos Hanzo, IEEE transactions on communications, Vol. 63, No. 1, January 2015.

[4] ,"Relay selection approaches for wireless cooperative networks" Tauseef Jamal, Paulo Mendes

[5] "Attacks & Preventions of Cognitive Radio Network-A Survey", Dr. Anubhuti Khare, Manish Saxena , Roshan Singh Thakur , Khyati Chourasia IJARCET, Vol 2, Issue 3, March 2013

[6] "Survey of security issues in cognitive radio networks", Wassim El-Hajj, Haidar Safa, Mohsen Guizani, J IT Vol. 12, No.2,2011

[7] "Cooperative Beam forming Using Multiple Relay path based Multiple Destination Analysis on Cognitive Radio Networks" Nagabelly Aranya Tejan, S.Srinivas Rao IRJET, Vol 02, Issue:07, Oct-2015