International Journal of Security and Its Applications
Vol. 12, No. 5 (2018), pp.37-48
http://dx.doi.org/10.14257/ijsia.2018.12.5.04

Secure Prioritized Inter Cluster Channel Selection for Tracking User Attack in Cognitive Radio Networks

Chandra Sekhar Musinana[1,*], Kalyana Chakravarthy Chilukuri[1] and Prasad Reddy PVGD [2]

[1]*Department of Computer Science and Engineering, M.V.G.R College of Engineering (A), Affiliated to JNT University, Kakinada, India*
[2]*Department of Computer Science & Systems Engineering, College of Engineering, Andhra University, Visakhapatnam, India*
chandrasekhar.m@mvgrce.edu.in

Abstract

Dynamic spectrum allocation evolved in order to allow the spectrum holes to be occupied by secondary users (SUs), but they have to handoff when primary users (PUs) come back, which brings new security problems like Tracking User Attack (TUA) into consideration. TUA might block the control information shared by a Cognitive Radio Network (CRN), if the attacker predicts the control channel frequency based on traffic analysis. This is a typical Denial of Service (DOS) attack preventing users from handoff to available channels. In cluster based channel selection, cluster heads will receive the channel information, about two users at a time and transmit the common preferred channel that was allocated to the base station. The base station selects a channel and returns it to the cluster head which returns them to the requesting CR users. For secure channel selection, the information could be encrypted by the base station and decrypted at the cluster heads to prevent DOS attacks.

In this work, we propose selection of available channels based on the priority of the cluster which we term Prioritized Inter Cluster Channel Selection (PICCS). The priority is essentially the history based reputation of the cluster calculated from the attackers in the cluster. Thus, instead of a random choice of a cluster for the available channel, during inter-cluster channel selection, we select a channel from the best available cluster. We observe the effect of such selection on both the delay and the handoffs in the presence of attackers and compare it with the channel selection scheme based on the nearest available cluster.

Keywords *Cognitive Radio Network; Dynamic spectrum allocation; handoff; tracking user attack; Channel selection*

1. Introduction

Spectrum sensing refers to the identification of spectrum holes with the help of some techniques such as energy detection, interference based detection and matched filters. Accuracy and time are the important factors for sensing. Spectrum sensing bandwidth is an important attribute that must be incorporated into any cognitive radio spectrum sensing scheme. The number of channels on which the system will sense, whether they are occupied or not is to be primarily determined. By sensing channels apart from the one currently in use, the system will be able to build up a picture of alternative channels that can be used when the current one becomes occupied. Thus, channel selection along with spectrum

Received (April 15, 2018), Review Result (July 13, 2018), Accepted (July 23, 2018)

ISSN: 1738-9976 IJSIA

sensing provides an accurate estimation of spectrum availability. This further helps in learning when to sense which frequency channel [1].

Channel selection continues to be very prominent, owing to the dynamic nature of CRNs. In a cognitive radio, a secondary user is assigned a set of channels. These channels are the unused licensed channels which are allocated to PUs that can be accessed by SUs opportunistically in the absence of the PUs. Channel selection strategies have different aims such as maximizing throughput, reducing delay, channel switching, etc. Channel selection is also an integral part of routing in CRNs where channels with high bandwidth and connectivity, low primary user activity and low interference are chosen for routing.

Channel selection strategies in CRNs can be categorized into three types. They are:

1. Proactive
2. Reactive
3. Threshold based

Proactive channel selection involves in predicting the primary user activities and allocating the channel to the secondary user. Reactive channel selection strategy allows the secondary users to make use of the channel when vacated by the primary user by continuously monitoring the primary user's activity. Threshold channel selection strategy facilitates the secondary users to make use of the channel until the level of threshold defined for the interference has not yet crossed.

Handoff occurs whenever a channel has to be handed over by a cognitive user to the primary user. Handoffs are of two types. They are:

a. essential handoff which takes place when primary user comes back or if the allotted channel does not satisfy user requirements

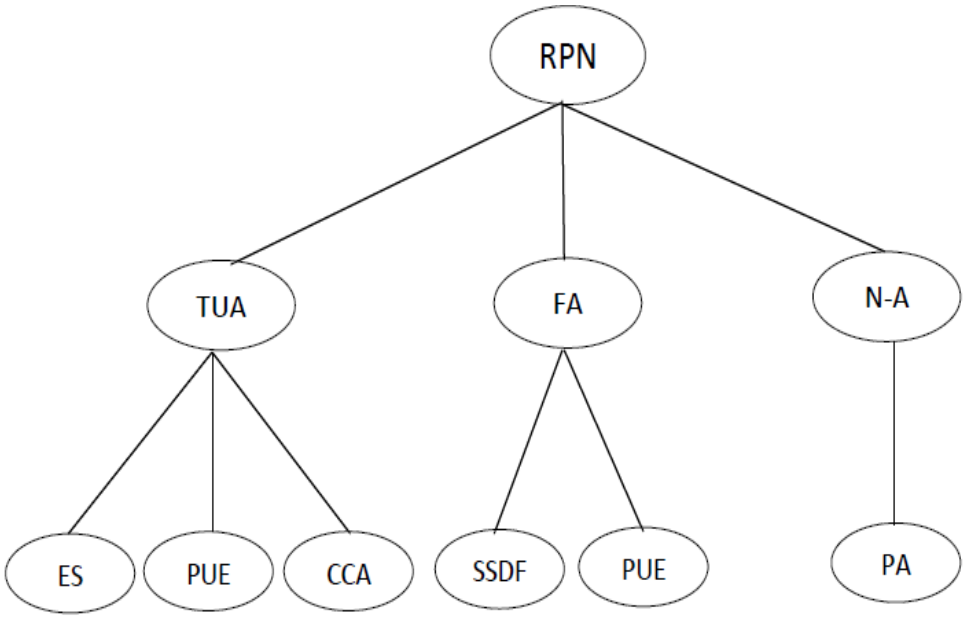
b. Non-essential handoff which takes place when primary user attacks (PUA) takes place.

Effective sensing and channel selection are the challenges of handoffs [2]. Channel selection strategies aim at selecting channels with low primary user activity, high availability and high connectivity to neighbors for routing that lasted for a long time. The main aim of intruders is to prevent channels from being allocated to the secondary users even if they are vacant. Some of the threats in cognitive radio networks are Denial of Service (DOS) attack, accessing private data of cognitive users by intruders, modification of data by intruders to their own advantage, injection of false data, *etc.* [3].

During allocation, some attacks may reduce the throughput of TCP by making the secondary user to handoff. In other class of attacks, attackers monitor the control channels, estimate the available data channels and finally launch Primary User Emulation (PUE) attacks on the available channels, preventing cognitive users from handoff. By finding the optimal channel to which handoff would be next made, it is possible for all users to sense the channels.

By performing PUE attacks, attackers will occupy the channels which the interrupted users are going to occupy [3]. This deprives the cognitive users from handoff to available channels and is one form of Denial of Service (DoS) attacks. This forms the basis for the tracking user attack.

Classification of various attacks, their causes and the effect of reduced performance of network is given and depicted in Figure 1.



Where RPN=Reduced performance of network,
ES= Estimation,
PUE= Primary user emulation attack,
CCA= Control channel attack,
FD= False decision,
SSDF=Spectrum sensing data falsification attack,
N-A= Non-adaptability,
PA= Parameter attack

Figure 1. Threats in Cognitive Radio Networks

Where estimation is used to defend against TUA because it hides the information which is selected by the cluster head. Even if secondary users' handoff to the next optimal channel, there will be no tracking user attack.

In the TUA,

1. Intruder intercepts the sensing result in common control channel.
2. Intruder performs primary user emulation in which the intruder acts like a primary user on the channel that will be used by a targeted secondary user, so that the secondary user has to vacate.
3. Intruder estimates the next channel of secondary user and performs primary user emulation attack, so that target user never gets chance to occupy the channel.

A generalized anti-attack model for TUA based on clustering should satisfy the following assumptions, when an attacker competes for the next optimal channel.

1. Primary users have more access to spectrum holes than secondary users.
2. Self co-existence between the clusters.
3. Cognitive users should not interfere with primary user's communication.
4. Cognitive users should take appropriate changes when environment changes.

2. Channel Selection Information Hiding (CSIH) scheme

Channel Selection Information Hiding scheme (CSIH) which makes use of cryptographic techniques that is used to defend tracking user attack. Two scenarios of Channel Selection Information Hiding scheme are intra-clustering and inter- clustering.

2.1. The Intra-Clustering Scenario

In the intra-clustering approach, as seen in Figure 2,

1. Both the users belong to same clusters sends request to cluster heads.
2. Let M and N are cognitive users.
3. CH1=CH2 and cluster heads calculate ST where

   ST=SM ∩ SN ∩ SCH.

   Where SM=performance set of cognitive user M.

   SN= performance set of cognitive user N.

   SCH= performance set of cluster.
4. If ST is not empty; cluster head sends ST to base station.

   The central base station selects the ST, enquires the corresponding sequence number, encrypts it and sends to cluster head. Then cluster head decrypts and again sends the encrypted data to users.
5. If ST is empty, base station itself allocates channels.

   The central base station selects a channel, enquires the corresponding sequence number of that channel, encrypts and sends to cluster head. Then cluster head checks which user have that selection number, encrypts and sends the encrypted data to users.
6. Cognitive user's handoff after receiving channel which is the selection information from cluster head.

If handoff is successful, cognitive users sends the channel selection information to central base station. If handoff is not successful, again the process repeats [4]. The central base station updates its channel list.

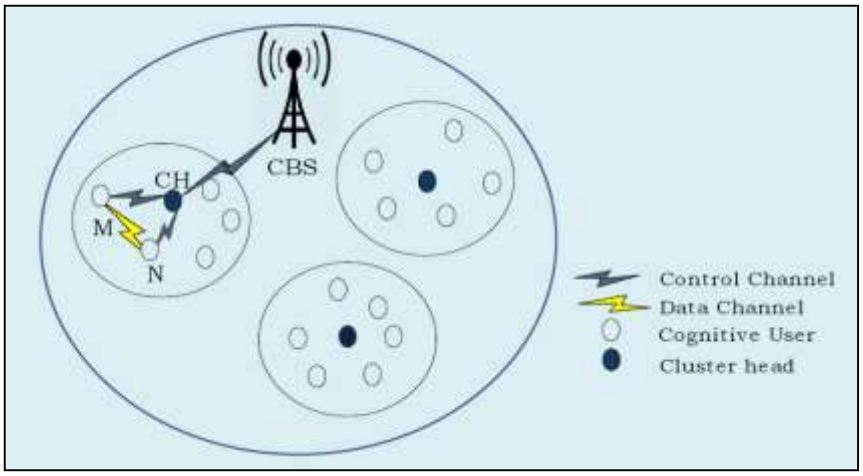


Figure 2. Channel Selection for Intra-clustering

2.2. The inter-clustering Scenario

In the inter-clustering approach,

1. Both the users belonging to different clusters request for channel to different cluster heads.
2. Let M and N are cognitive users.
3. As CH1≠CH2 then clusters head calculates ST where

   ST = SCH1∩ SCH2.

   where SCH1 = preference set of cluster head1.

   SCH2 = preference set of cluster head2.

4. If ST is not empty, the cluster head sends ST to base station.

   The central base station selects the channel ST, enquires the corresponding sequence number in both the cluster heads, encrypts the sequence number and sends to both the cluster heads. Then both the cluster heads decrypt and enquire the requested user to verify whether that channel is in its preference sets, and then encrypt and send the encrypted data to users.

5. If ST is empty, again user requests for new channel. Users have to start the process from the beginning.
6. After receiving the channel selection information from the cluster head, cognitive user's handoff. If the handoff is successful, cognitive users sends the channel selection information to central base station.

If handoff is not successful, again the process repeats. The central base station updates its channel list.

2.3. Synchronization Mechanism

Cognitive users use ordered sets to store the sensing result. Each element in ordered set has corresponding sequence numbers. Initialization is done by making elements in the preference sets as Φ. Updating is done when a channel has to be added. Addition is done by sending encrypted (e,1) to cluster head, where e = channel and 1 = sequence number. Cluster heads decrypt (e,1), enquire 1st position, send updates to user and user will update in the similar way. Deletion is done by sending the encrypted (e, 1) to cluster head. Cluster head decrypts (e, 1), enquires 1st position, and deletes the element beyond l to shift one position forward. Cluster head sends update to user and the user will update in the similar way.

3. Prioritized Inter Clustering Channel Selection scheme (PICCS)

3.1. Clustering and Spectrum Sensing

Clusters are formed based on the factors like location correlation coefficients of the unlicensed users *i.e.*, secondary users and previous history of attackers in the clusters. The cluster formation is done before unused spectrum is sensed by the secondary users. Problems like shadowing and multipath fading, which might cause communication overhead among secondary users, are resolved by taking spatial diversity as a factor among secondary users. In [5], a multitaper method for spectrum sensing is presented, that was observed to outperform other methods such as the periodogram and hamming-tapered methods. In [6], the advantages of co-operative sensing in cognitive radios are highlighted, that chiefly include mitigating the effects of fading and malicious users. A weighted

function that optimizes the number of secondary users, such as signal to noise ratio (SNR) is maximized for cooperative spectrum sensing is proposed in [7].

In [8], a collaborative approach for spectrum sensing has been found to be superior to direct spectrum sensing in terms of probabilities of detection and false alarms in the presence of log-normal shadowing. In [9], it is proven that dynamic channel selection improves the throughput by 40% compared to the static approach. This happens when the sensing makes an optimal trade-off between reducing the delay in occupying channels and waiting for the state information required to occupy channel with improved throughput in the future. The effects of hidden terminal problems and how they could be avoided using cooperative spectrum sensing were also presented. In [10], a novel approach is proposed to avoid the malicious cognitive radio user attack. It was observed that the effects of malicious CR users on the global spectrum decisions at the fusion centre reduce the benefits of cooperative spectrum sensing. On the other hand, the proposed fault-tolerant sensing based on the reputation degree of a CR was observed to be better than earlier cooperative schemes such as the Equal Gain Combination EGC.

There are many secondary user selection algorithms derived to resolve the communication overhead problem according to the sensing capacity and delay in reporting the data. In [11], a common control channel based CR user selection policy is proposed, which suggests that better results in terms of detection probability are obtained when users are correlated either CR mobility or due to variations in channel conditions. Reliable CR selection based on the instantaneous Channel Side Information (CSI), in a cooperative spectrum sensing scenario to improve detection probability is proposed in [12].

In [13], Binary Particle Swarm Optimization (BPSO) is used to optimize the performance based on characteristics of every individual cooperating node. Sensing capability, reporting delay are the characteristics considered in obtaining the minimum detection risk. It essentially studies the effect of reporting delay on the average Bayesian risk with increasing number of cooperative nodes. The proposed method was observed to reduce the Bayesian risk significantly on isolating some nodes based on the above factors.

The proposed model, PICCS is based on Reputation based hierarchical cooperative spectrum sensing scheme, in which spectrum sensing is both priority based and reputation based. There are two levels of cooperation. As in [14], clustering is performed such that there are atleast two idle channels available for use as control channels, to prevent migration even in case Primary Radio (PR) takes over one of the channels. The channel selection policy is the same as the one described in Section 2.2.

The first level of cooperation takes place within a cluster, and in each and every cluster, there are many secondary users depending on their location correlation coefficient factor. There is also a cluster head among them, where each secondary user senses the available and required spectrum, sends it to the cluster head. The cluster head collects all the sensing data and it also combines the sensing data with the Equal Gain Combination (EGC) rule to make a cluster level decision about the primary user status.

The second level of cooperation takes place at a higher level which consists of cluster head and fusion centre. Reputation mechanism integrates with the majority rule at the fusion centre, in order to improve the qualities like robustness [15]. The PICCS model, as seen in Figure 3[16] reduces the system overhead in terms of bandwidth consumption and delay in time [16]. This also helps in relieving from shadowing and elimination of Primary User Emulation Attack (PUEA) [17].

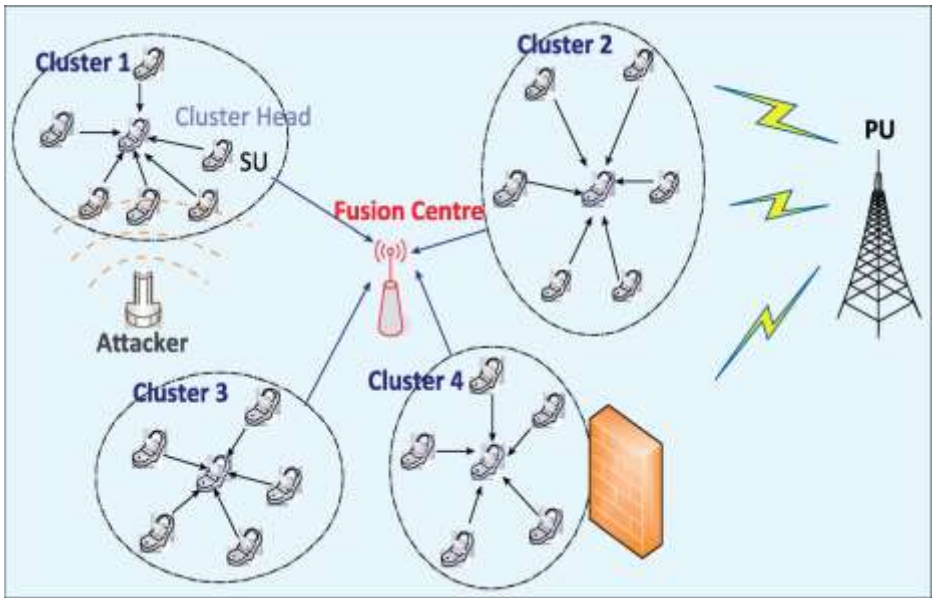


Figure 3. CRN Model for Hierarchical Cooperative Spectrum Sensing

The cooperative spectrum sensing scheme, with clustering has a two-bit combination [18]. The first bit is the cluster level decision given by the cluster head, which is taken by the sensed data sent by the secondary users via a control channel to the cluster head. The second bit is the final level decision given by the fusion centre, which is taken by the data sent by all cluster heads [19]. Cluster based sensing scheme was proposed to reduce the time for reporting the decision and also bandwidth availability during spectrum sensing [20].

3.2. Assumptions

Reputation-based hierarchically cooperative spectrum sensing scheme is proposed to improve the robustness of the cognitive radio system because of the assumption that multiple secondary users within a cluster may become abnormal due to shadowing, multipath fading or primary user emulation attack [17].

When there are many secondary users located far away from the primary user and fusion center in the CRN, then it is assumed that the signal received by the primary user is corrupted by the Additive White Gaussian Noise (AWGN).

4. Results

To make the CSIH scheme more secure, each cluster is assigned with a priority on the basis of the presence of attackers. The user from the high priority cluster shall occupy the channel earlier than the other cluster users.

As normally there may be many users who forward the request for the channel to the base station, base station can make use of this scheme to decide which user request has to be served first on the basis of cluster priority.

Graphs in Figure 4 shows that as the number of attackers increases, the handoffs decrease in the CSIH scheme with intra clustering. With this CSIH scheme, it is difficult for the attackers to know about the channel requested by the specific user to perform tracking user attack.

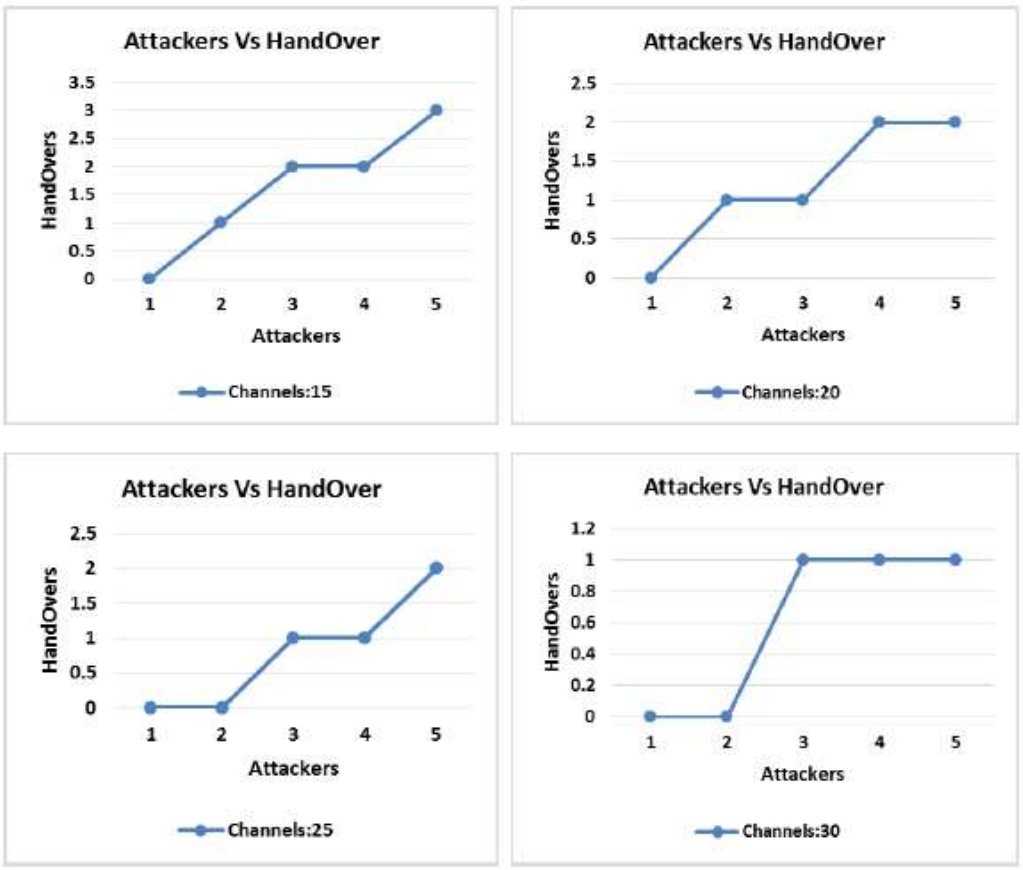


Figure 4. Attackers Graphs for Handoff in CSIH Scheme with intra-clustering

Graphs in Figure 5 shows that as the number of channels increase, the delay to occupy a channel reduces. When the number of channels is less and users are more, then the delay will be high.

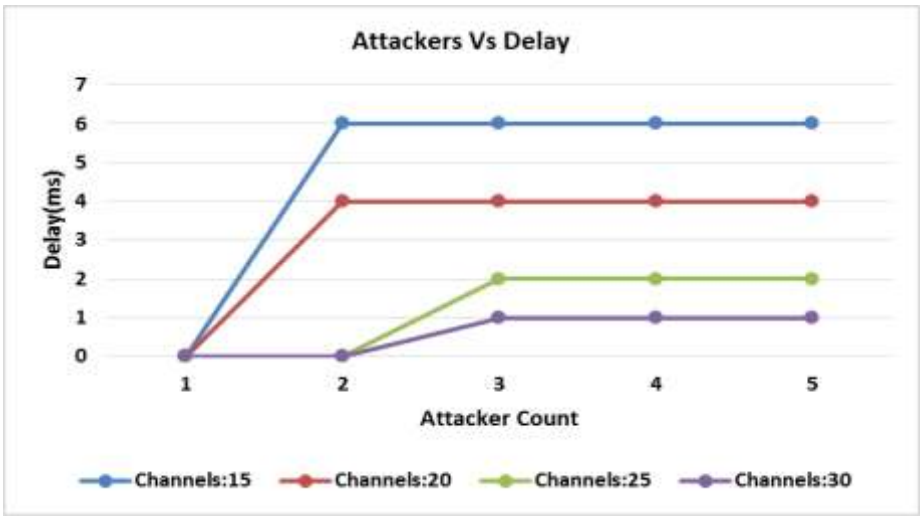


Figure 5. Attackers Graph for Delay in CSIH Scheme with intra-clustering

Graphs in Figure 6 shows that as the number of attackers increases, the handoffs decrease in CSIH scheme with inter clustering. With this CISH scheme, it is difficult for the attackers to know about the channel requested by the specific user to perform tracking user attack.

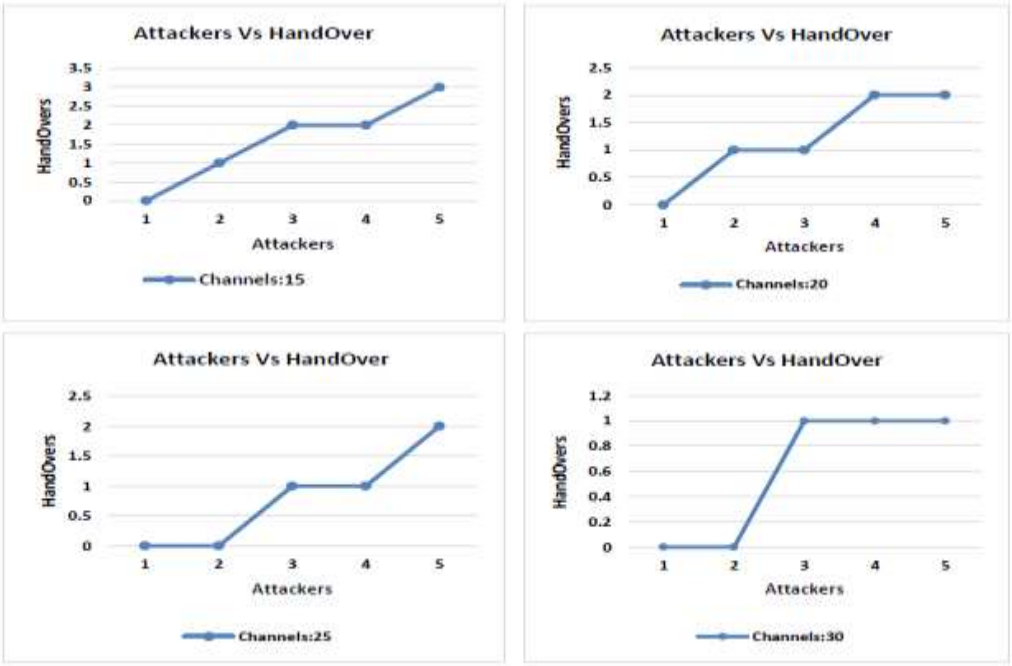


Figure 6. Attackers Graphs for Handoff in CSIH Scheme with inter-clustering

Figure 7 shows that when the number of channels are increasing then the delay to occupy a channel reduces. When the number of channels are less and users are more then, the delay will be high. As the users will have information about the channels, the users will take some time to vacate the channel if another user requests for that channel.

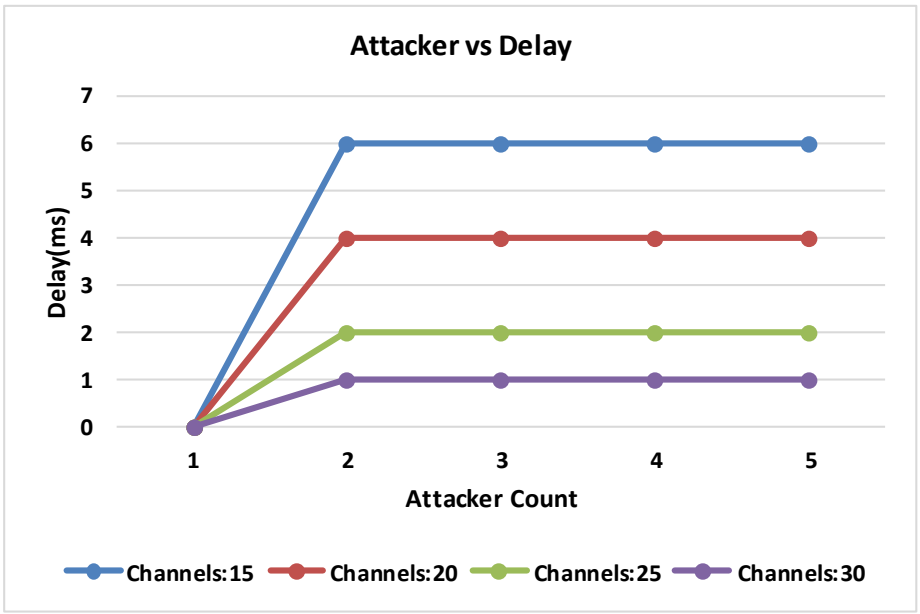


Figure 7. Attackers Graph for Delay in CSIH Scheme with inter-clustering

The results from PICCS in Figure 8 shows that with the proposed scheme, for the increasing number of attackers, the number of hand-offs reduce compared to the inter-channel selection (CSIH) scheme. However, the difference is more significant for lesser number of channels, considering the overhead of prioritization. Also a slight reduction in handoff delay was observed in Figure 9. The results are tabulated in Table.

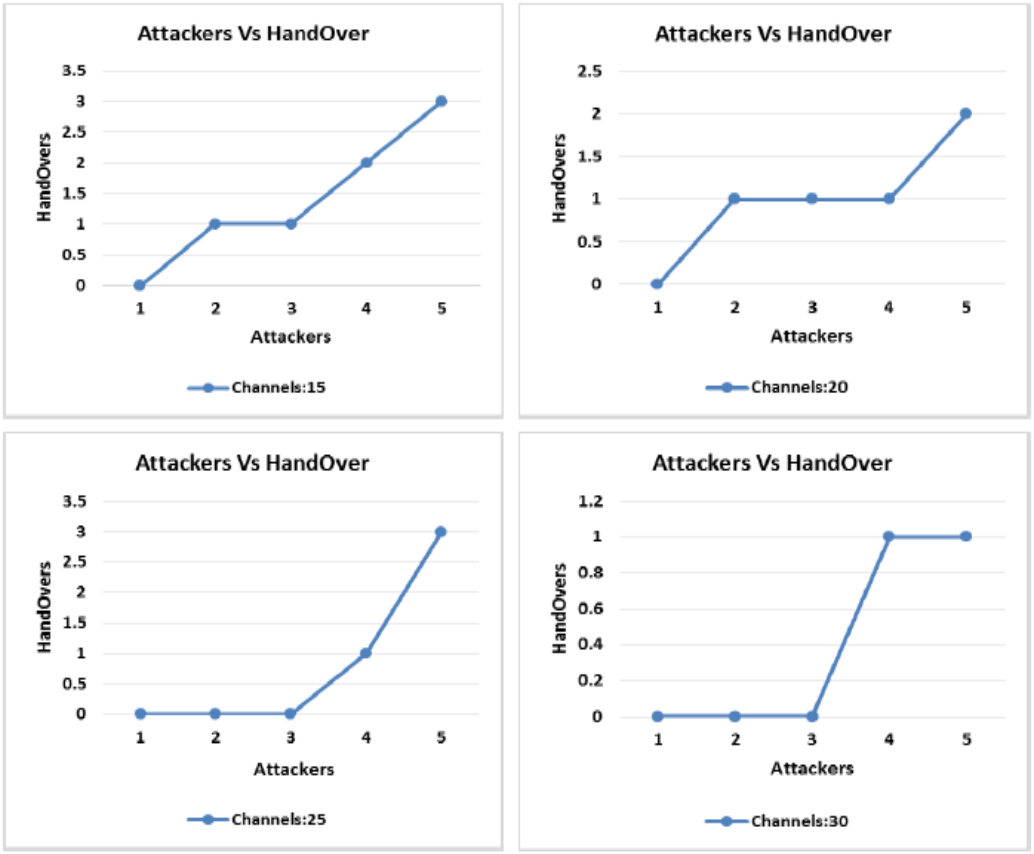


Figure 8. Attackers Graphs for Handoff in PICCS Scheme with inter-clustering

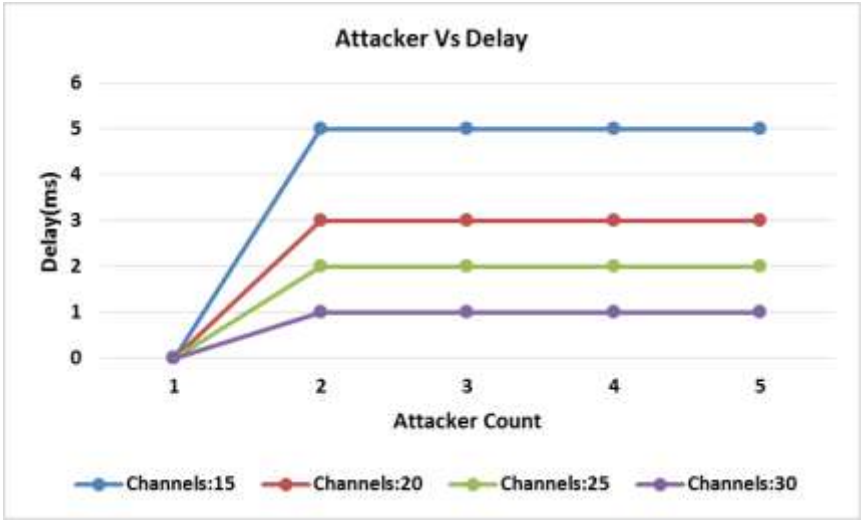


Figure 9. Attackers Graph for Delay in PICCS Scheme with inter-clustering

Table 1. Handoff and Delay Graph Comparison of CSIH Scheme and PICCS Scheme

Number of channels	Average handoff of channels			Average delay of channels		
	CSIH Scheme		PICCS scheme	CSIH scheme		PICCS scheme
	Inter - Clustering	Intra-Clustering	Inter-Clustering	Inter - Clustering	Intra - Clustering	Inter - Clustering
15	1.6	1.6	1.4	4.8	4.8	4
20	1.2	1.2	1	3.2	3.2	2.4
25	0.8	0.8	0.8	1.6	1.2	1.6
30	0.6	0.6	0.4	0.8	0.6	0.8
Average	**1.05**	**1.05**	**0.9**	**2.6**	**2.45**	**2.2**

5. Conclusion

Channel Selection Information Hiding Scheme is used to defend against tracking user attack, where intruders act as primary users and prevent the secondary users from occupying vacant channels. It also enables security to the secondary users while they handoff when primary users occupy the channel. The proposed Prioritized Channel Selection scheme (PICCS), applies reputation based cluster selection with the information hiding scheme and measures the effect on handoffs and delay. While offering the benefits of CSIH scheme, PICCS performs better on both the average handoffs and delay for increasing number of attackers, measured over varying channels. The idea of Priority Based Cluster Selection could possibly be extended to routing with secure channel selection and to secure energy efficient routing in cognitive radio networks.

References

[1] N. Rastegardoost and B. Jabbari, "On channel selection schemes for spectrum sensing in cognitive radio networks", Proceedings of the Wireless Communications and Networking Conference, pp. 955-959.
[2] Z. Jin, S. Anand and K. P. Subbalakshmi, "Performance analysis of dynamic spectrum access networks under primary user emulation attacks", Proceedings of the Global Telecommunications Conference, **(2010)**, pp. 1-5.
[3] R. Chen, J. M. Park and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks", IEEE J Sel Area Comm., vol. 26, no. 1, **(2008)**, pp. 25-37.
[4] A. A. El-Sherif and K. R. Liu, "Joint design of spectrum sensing and channel access in cognitive radio networks", IEEE T Wirel Commun., vol. 10, no. 6, **(2011)**, pp. 1743-1753.
[5] S. Haykin, D. J. Thomson and J. H. Reed, "Spectrum sensing for cognitive radio", P IEEE, vol. 97, no. 5, **(2009)**, pp. 849-877.
[6] S. M. Mishra, A. Sahai and R. W. Brodersen, "Cooperative sensing among cognitive radios", In: Proceedings of the Communications, IEEE International conference, **(2006)**, pp. 1658-1663.
[7] J. Yang and X. Shao, "Optimal number of secondary users in weighted cooperative spectrum sensing", Proceedings of the Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, pp 902-905.
[8] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments", Proceedings of the New Frontiers in Dynamic Spectrum Access Networks (DySPAN), First IEEE International Symposium, **(2005)**, pp. 131-136.
[9] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access", IEEE Signal Proc Mag., vol. 24, no. 3, **(2007)**, pp. 79-89.
[10] H. Chen, M. Zhou, L. Xie and X. Jin, "Fault-tolerant cooperative spectrum sensing scheme for cognitive radio networks", Wireless Pers Commun., vol. 71, no. 4, **(2013)**, pp. 2379-2397.

[11] A. S. Cacciapuoti, I. F. Akyildiz and L. Paura, "Correlation-aware user selection for cooperative spectrum sensing in cognitive radio ad hoc networks", IEEE J Sel Area Comm., vol. 30, no. 2, **(2012)**, pp. 297-306.
[12] W. Yue, B. Zheng, Q. Meng, J. Cui and P. Xie, "Robust cooperative spectrum sensing schemes for fading channels in cognitive radio networks", Sci China Ser F., vol. 54, no. 2, **(2011)**, pp. 348-59.
[13] W. Xia, W. Yuan, W. Cheng, W. Liu, S. Wang and J. Xu, "Optimization of cooperative spectrum sensing in ad-hoc cognitive radio networks", Proceedings of the Global Telecommunications Conference, **(2010)**, pp. 1-5.
[14] L. Lazos, S. Liu and M. Krunz, "Spectrum opportunity-based control channel assignment in cognitive radio networks", Proceedings of the Sensor, Mesh and Ad Hoc Communications and Networks, 6th Annual IEEE Communications Society Conference, **(2009)**, pp. 1-9.
[15] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications", IEEE communications surveys & tutorials, vol. 11, no. 1, **(2009)**, pp. 116-130.
[16] X. Ni, H. Chen, L. Xie and K. Wang, "Reputation-based hierarchically cooperative spectrum sensing scheme in cognitive radio networks", Proceedings of the Communications in China, IEEE/CIC International Conference, **(2013)**, pp 397-402.
[17] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks", In: Proceedings of the Networking Technologies for Software Defined Radio Networks, 1st IEEE Workshop, **(2006)**, pp. 110-119.
[18] J. Ma, G. Zhao and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks", IEEE T Wirel Commun., vol. 7, no. 11, **(2008)**, pp. 4502-4507.
[19] J. Duan and Y. Li, "A novel cooperative spectrum sensing scheme based on clustering and softened hard combination", Proceedings of the Wireless Communications, Networking and Information Security, IEEE International Conference, **(2010)**, pp. 183-187.
[20] N. Reisi, M. Ahmadian, V. Jamali and S. Salari, "Cluster-based cooperative spectrum sensing over correlated log-normal channels with noise uncertainty in cognitive radio networks", IET Commun., vol. 6, no. 16, **(2012)**, pp. 2725-2733.

