BYZANTINE ATTACK DETECTION USING CLUSTERING ALGORITHM IN COGNITIVE RADIO NETWORKS

C.Gowthami[1], S.Priyanga[1], G.Nithya[1],T.Aruna[2]

[1]UG Student, Department of ECE, Thiagarajar College of Engineering, Madurai

[2]Assistant Professor, Department of ECE, Thiagarajar College of Engineering, Madurai

ABSTRACT

Cognitive radio networks are intelligent networks that are being widely used in wireless communication technologies for effective utilisation of the bandwidth and efficient allocation of spectrum to the users. The major security issue faced in the cognitive radio networks is misdetection of users and spectrum wastage because of misperception and faulty allocation of channels. This issue is caused by a set of attackers called Byzantine attackers or Spectrum sensing data falsification attackers. With the help of error rates of independent attackers and collaborative attackers along with the detection strategies of these attackers bymeans of k medoid clustering algorithm and PAM algorithm these issues can be resolved. The existing technology of cognitive radio networks is extended to support large number of users with the help of CLARA clustering algorithm- clustering for large applications. The results are simulated using MATLAB.

Keywords - Cognitive radio network, Spectrum Sensing, Byzantine attack, k medoid clustering, clara.

I. INTRODUCTION

An interconnected set of cognitive radio devices that share information is defined as a Cognitive Radio Network (CRN). The cognitive radio is able to provide a wide variety of intelligent behaviors. It can monitor the spectrum and choose frequencies that minimize interference to existing communication activity. Cognitive radio network is considered as the promising technology to improve spectrum utilization.CRNs solve the spectrum shortage problem by allowing unlicensed users to use spectrum band of licensed user without interference. Generally licensed users are known as primary users and un-licensed users are secondary users. When information is send through a licensed spectrum band is a primary user, only some channel of band is used, others are empty. These empty channels are used by un-licensed user called secondary user. Secondary users always watch the activities of primary user, and detect the empty channel and occupy the channel without disturbing the primary user. When the primary users are active, the secondary user should either avoid using the channel. An Empty channel also known as spectrum holes. The complications arise as secondary users must release a spectrum when the primary user for that channel starts to transmit. Several research groups are working to develop standards to meet these requirements. 802.22, the first CR based network standard defines a centralized, single hop, point to multi-point communication standard for wireless regional area network.

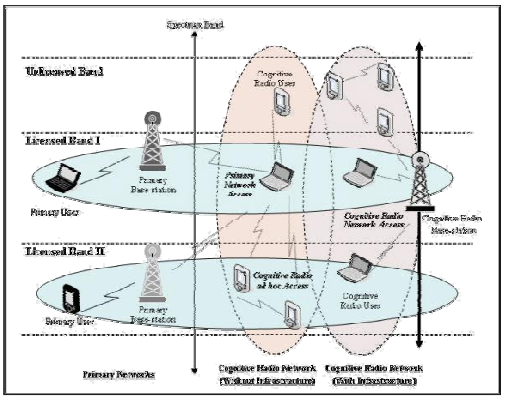

Figure 1 Architecture of cognitive radio network.

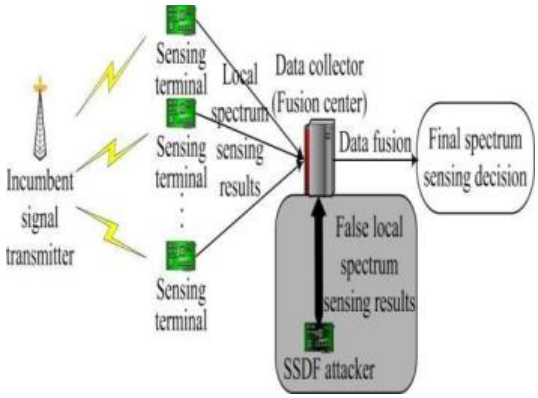

Figure 2 Spectrum Sensing data falsification attack

II. SECURITY THREATS IN COGNITIVE RADIO NETWORKS

There are many attackers in cognitive radio networks which can be categorized with respect to four layers. The attackers in physical layers are Primary User Emulation (PUE), Objective function attack and jamming. The PUE attackers are actually secondary users, who act as primary or licensed users to obtain full band of spectrum. In data link layer, we focus on Spectrum sensing data falsification (SSDF) or byzantine attack, Control Channel Saturation dos Attack (CCSD), and Selfish Channel Negotiation (SCN). In Network Layer, the routing attacks, HELLO Flood attack and Sinkhole attack. In transport Layer, we focused the Lion Attack. It may be possible that jamming attack can be done on physical layer or MAC layer.

A. BYZANTINE ATTACK:

Spectrum Sensing Data Falsification, also known as the Byzantine Attack, takes place when an attacker sends false local spectrum sensing results to its neighbors or to the fusion center, causing the receiver to make a wrong spectrum-sensing decision. This attack mainly targeted to centralized as well as distributed CRNs. SSDF attack is more harmful in a distributed Cognitive Radio Network. During such an assault, the malicious user compromises one or more of the secondary users and may begin sending modified sensing reports to the BS. In this way, an attacker tries to influence the BS into producing a wrong decision about the channel status. Compromised nodes may work independently, or may collaborate to reduce spectrum utilization and degrade overall performance of the network.

III. DESIGN OF CLARA CLUSTERING

In the existing k medoid algorithm, only limited number of nodes or users can be efficiently detected. For example, say upto 100 nodes can be detected with minimum error rate when k medoid techniques are used. The evolving technology of cognitive radio networks can be made more effective such that it supports large number of users in a network. The smartness of the cognitive radio technology in auto detection and smart allocation of channels to the authorized users and switching over control between authorized users and the non authorized users can be extended to support large networks with the use of clustering techniques for large applications CLARA.CLARA techniques use the existing k medoid algorithms in a modified format along with PAM algorithms.

A. WORKING METHODOLOGY

All the nodes in the network are subjected to k medoid clustering algorithm initially to form multiple clusters. From each cluster, a random sample is chosen such that the chosen sample should be a representation of the attributes of all other nodes in the cluster. In general a node which has the median characteristics of all other nodes in the cluster is chosen as the sample node. The deviation in attributes of this sample node when compared with the other nodes in that particular cluster is set to be minimal. After electing the sample, PARTITIONING AROUND MEDOID (PAM) algorithm is applied to each and every sample. The purpose of this algorithm is that when the sample nodes are subjected to PAM algorithm, it returns the best possible cluster.

The selection of the best cluster by the PAM algorithm is based on the attributes of the sample data presented by each cluster. The PAM algorithm will check for the minimum deviation levels of the samples with respect to the nodes and also the extent

to which the sample data is capable of representing the whole dataset of clusters. Based on these the best cluster id being selected . The entire process is carried out in multiple iterations . So the complexity of each iteration is given by

$$O(ks^2 + k(n-k))$$

where

k represents the clusters

s represents the size of the cluster

n represents the number of clusters

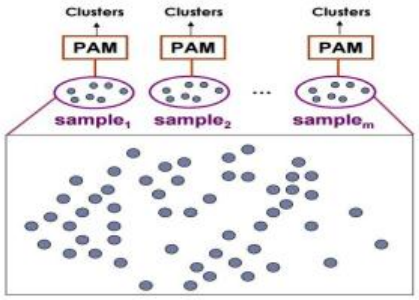

Figure 3 Formation of clusters- Clara clustering algorithm

From the figure, the formation of clusters by applying the k-medoid clustering techniques is shown.

The expression to calculate the deviation of the sample set from the rest of the nodes in a particular cluster is given by

$$COST(M,D)=\Sigma_{i=1}^{n} dissimilarity(O_j , rep(M , O_i))/n$$

From the above equation we have,

D : Data matrix (rows = observations, columns = variables).

k-clusters : The number of desired clusters.

n=Number of samples to be drawn from the dataset. O=nodes in the cluster.

M=Set of selected Medoids.

Initially the clusters are formed with the help of k medoid algorithm. Christo Ananth et al. [2] discussed about a Secure system to Anonymous Blacklisting. The secure system adds a layer of accountability to any publicly known anonymizing network is proposed. Servers can blacklist misbehaving users while maintaining their privacy and this system shows that how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services. This work will increase the mainstream acceptance of anonymizing networks such as Tor, which has, thus far, been completely blocked by several services because of users who abuse their anonymity. In future the Nymble system can be extended to support Subnet-based blocking. If a user can obtain multiple addresses, then nymble-based and regular IP-address blocking not supported. In such a situation subnet-based blocking is used. Other resources include email addresses, client puzzles and e-cash, can be used, which could provide more privacy. The system can also enhanced by supporting for varying time periods. This process is continued for all the other clusters in the dataset. Because of the increased number of iterations that ensures the deviation level or dissimilarity of the attributes that a node in a cluster possesses this algorithm will give more preciseness in results .

IV. RESULTS AND DISCUSSIONS

In this project the main objective is to detect and nullify the spectrum sensing data falsification attackers using clustering algorithm, thereby reducing the error rate of the system.

A. SYSTEM DETECTION ACCURACY:

Before analyzing the presence of attackers, the system analysis is made. The system is designed in such a way that the accuracy is maintained for the number of users. The system provides good accuracy for certain users and the accuracy decreases with increase in number of users. The System gives good output for the independent attackers whereas in collaborative attackers the accuracy of the system decreases.

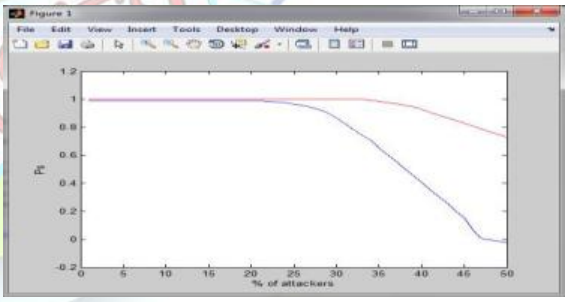

Figure 4.1 System detection accuracy with varying attackers.

The idle rate of the channel P_I =0.9.

The busy rate of the channel P_B=0.1.

The false alarm probability P_{fa}=0.2.

The misdetection probability P_{md}=0.2.

The detection probability of the system is calculated by using the above given probabilities.

B. PERFORMANCE METRICS

To evaluate the performance of this algorithm, there are three performance metrics. The error rate is calculated and it is denoted as Q_E. The error rate denotes how many times the base station makes the incorrect decision. The algorithm is good

if the error rate is less. The second metric is called true detection rate or recall and is denoted as Q_D. It is widely used in data mining applications to evaluate the successful detection of members of a class that are considered more significant than the detection of members of other classes. Algorithms with higher value of recall are desirable. In our work, identifying attackers is more significant than identifying honest users. The third metric is false positive rate and is denoted as Q_F. This metric represents how many nodes are misidentified as attackers. In this case, the lower the false positive rate, the better the algorithm is. The true detection rate with the sum of false positive rate gives the error rate.

C. ERROR RATE DETECTION:

The error rate is compared with the rawat's algorithm with the above proposed algorithm. The error rate of the algorithm using adaptive reputation clustering is less when compared to that of rawat's algorithm. The true detection rate in rawats algorithm is calculated using the detection probability of honest and byzantine attackers and the number of honest and byzantine attackers. The positive false alarm in rawat's algorithm is calculated using the false alarm rate of honest and malicious users in cognitive radio networks.

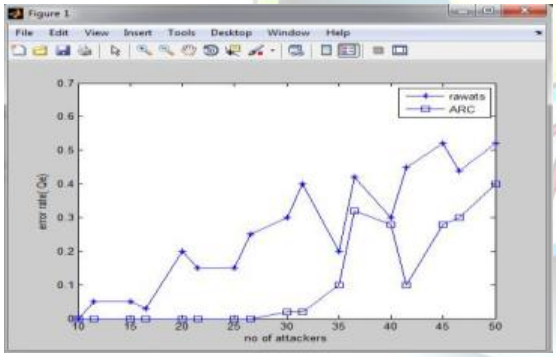

Figure 4.2 The error rate comparison

From the simulation results, it is inferred that the error rate of finding the byzantine attackers by using k-medoid clustering technique is minimized compared to all the previous algorithms in cognitive radio network. The error rate Q_E is determined for varying attackers.

D. INDEPENDENT VS COLLABORATIVE ATTACKERS:

There are two different types of attackers attack commonly in all networks. They are collaborative and independent attackers. The independent attackers are similar to honest users and the minimum detection probability of independent attackers is 0.5 while the minimum detection probability of collaborative attackers is 0.35. This implies that 35% of attackers is enough in collaborative for blinding the base station and 50% of independent attackers are required to blind the base station.

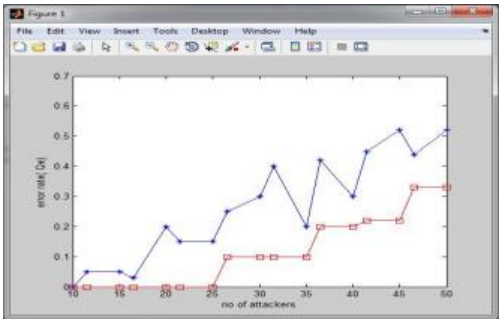

Figure 4.3 comparison of Independent and Collaborative attackers.

From the simulation, the probability of error rate in independent attackers is less when compared to probability of error rate in collaborative attackers. As the number of attackers increases the probability of error rate also increases. It is inferred that upto limited users the independent attacker's acts as honest users. After reaching certain threshold, the probability of the error rate the spectrum sensing data falsification attacker's increases. But in case of collaborative attackers, the error rate increases little steadily from minimum number of users.

E. RESULTS FOR CLARA CLUSTERING

Figure 4.4 Minimum number of clusters required to perform Clustering operation

Figure 4.5 When the nodes in the same cluster takes dissimilar decisions

Fig 4.6 When the nodes in the same cluster takes similar decisions

Fig 4.4 represents the minimum number of clusters required to perform CLARA Clustering operation. In case of inter-clustering operations, It is observed that atleast a minimum of three clusters are required by the fusion centre to take a final decision.

Fig4.5 depicts the result when the nodes in the same cluster takes dissimilar decisions. Based on the deviation level or dissimilarity of the object node from the selected medoid in the cluster, the results are displayed. If the dissimilarity value is more the result is shown as in fig 7.5.Else if the dissimilarity level is less, then they are supposed to be similar clusters with attributes that match each other. And so the shows that the nodes in the same cluster takes similar decisions.

V. CONCLUSION AND FUTURE WORK

This study explains the use of cognitive radio networks and to protect the network against the attackers.The results are simulated for error detection of byzantine attackers using partially around medoid clustering and compared with the previous algorithm. The clustering algorithm depicts the minimum error rate comparatively. The error rate is calculated for independent byzantine attackers and collaborative byzantine attackers and compared and simulated which depicts that the independent attackers provides less error rate than collaborative attackers. The comparison is done using k-medoid clustering algorithm.

To decrease the error rate in detecting the SSDF attackers in the base station the partially around medoid clustering is replaced by clustering in large applications. As the number of users increases, the detection rate decreases.But if CLARA clustering is used, it minimizes the error rate of the system. The decision of each cluster is taken into consideration and compared with the other cluster and the final decision is made with the voting machine with majority number of votes of cluster.

In future work, the error rate for CLARA clustering is determined. It is then compared with the partially around medoid clustering.The output determines error rate for many number of users with greater accuracy than the previous determined cluster.

REFERENCES

[1] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in Proc. 27th Conf. Computer Communications INFOCOM, Phoenix, AZ, USA, 2008, pp. 1876–1884.

[2] Christo Ananth, A.Regina Mary, V.Poornima, M.Mariammal, N.Persis Saro Bell, "Secure system to Anonymous Blacklisting", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015,pp:6-9

[3] Chowdhury S. Hyder, Brendan Grebur, Li Xiao, Senior Member, IEEE, and Max Ellison, "ARC: Adaptive Reputation based Clustering Against Spectrum Sensing Data Falsification Attacks", IEEE transactions on mobile computing, vol. 13, no. 8, August 2014.

[4] A. S. Rawat, P. Anand, C. Hao, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," IEEE Trans. Signal Process., vol. 59, no. 2, pp. 774–786, Feb. 2011.

[5]P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE* Trans. Wireless Commun., vol. 9, no. 8, pp. 2488–2497, August. 2010.

[6] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in Proc. 43rd Annu. Conf. Information Sciences and Systems, Baltimore, MD, USA, Mar. 2009.

[7] W. Zhang, R. Malik, and K. B. Letaief, "Cooperative spectrum sensing optimization in cognitive radio networks," in Proc. IEEE Int. Conf. Commun. (ICC'08), May 2008, pp. 3411–3415.