A SURVEY ON HOSTILE USER DETECTION IN COGNITIVE RADIO NETWORKS

Reshma Rajan, Syamesh K G, Jeethumol K Joy

Abstract— The most important threats in cognitive radio networks is detection of primary user signal. Cooperation among secondary users expands the performance of the system significantly. In cooperative sensing in hostile environments, intruder nodes send incorrect sensing results to the fusion center and make the fusion center erroneously decides about the presence of the primary user. Most of the detection methods have been proposed to nullify effects of malicious nodes. If a malicious user exist in CR network, the whole operation of the network gets disturbed and to preclude such malicious behavior, Cooperative sensing has been shown to enhance the performance of channel sensing. However, cooperative sensing is susceptible to hostile users that may not faithfully pursue sensing instructions to save energy and/or time, or to throw denial of service attacks against the network.

***Index Terms*— Cognitive radio, cooperative spectrum sensing, Hostile Users, Primary User Emulation (PUE),ADSP**

I. INTRODUCTION

The wide surge of wireless communications leads to the scarcity of frequency spectra and available radio spectrum is a limited natural resource, being massed day by day. Cognitive radio is a technique where secondary user looks for a free band to sense when primary user is not in use of its licensed band. it is possible through spectrum sensing[1] and three types of spectrum sensing are co-operative sensing, interference based sensing, and non cooperative sensing. The unused frequency bands are called white space or spectrum holes. Cognitive network is sensitive to security hazards. The attackers may be external users or secondary users deed as a malicious users. So, in order to overcome these issues, hostile user detection system is used.

Cooperative sensing improves sensing accuracy but at the same time makes the system more susceptible to hostile users that may be present in the system. In cooperative spectrum sensing (CSS), multiple secondary users (SUs) collaborate to effectively detect a primary user (PU), However, the cooperation among SUs increments concerns about reliability and security of cooperative spectrum sensing, as some of the SUs may report incorrect sensing data . The falsified reported data can easily effect the spectrum sensing decision taken by the fusion centre. The falsification of data may develop either by malfunctioning of SUs or by intentional manipulation of data by certain SUs, called hostile users . The data reported by malfunctioning SUs may differ from the actual data.

A malicious user may (i) have a hardware glitch due to which its readings are erratic; (ii) be hacked by the owner so that it reports erratic sensing results without performing any sensing to save time and/or energy; (iii) report the channel to be busy so as to either assent the channel free for its own personal usage [3] or to initiate a Denial-of-Service attack against the network [4]; (iv) miserly report the channel to be free so that it can operate on that channel; or, (v) skip in-band sensing ias save energy and/or throughput. The recent increase in attacks against TCP Protocol [5], mobile devices and other metalware devices [6] as well as the software based design of CRs suggests that in the future CRs will be very sensitive to similar kinds of attacks. Such attacks may affect the sensing capability of CRs and may result in nodes causing interference to Pus.

One of the most common techniques used for detecting hostile users is based on the supposal that neighboring CRs have identical readings. These algorithms uses a passive approach that detects hostile users at the same time while sensing the channel for the existence of PUs. The algorithms based on this technique converge readings from all CRs and then mark those nodes as hostile whose readings differ significantly from their neighbors

II COGNITVE RADIO NETWORKS

An infrastructured network of CRs (Fig 1)where multiple nodes (or Secondary Users, SUs) may be associated with a secondary Base Station (SBS) and the location of SUs is unknown. Although cognitive radio was initially thinking of as a software-defined radio , most research work targets on spectrum-sensing cognitive radio . The chief problem in spectrum-sensing cognitive radio is scheming high-quality spectrum-sensing devices and algorithms for rearranging spectrum-sensing data between nodes. It has been shown that a facile energy detector cannot guarantee the exact detection of signal presence,[9] calling for more refined spectrum sensing techniques and requiring data about spectrum sensing to be regularly exchanged between nodes. Incrementing the number of cooperating sensing nodes decays the probability of false detection.

Manuscript received DEC, 2015.

***Reshma Rajan**, Electronics And Communication, Cochin University Of Science And Technology, Kerala, India,*

***Syamesh K.G**, Electronics And Communication, Cochin University Of Science And Technology ,Kerala, India,*

***Jeethumol K Joy**, Electronics And Communication, Cochin University Of Science And Technology , Kerala, India,*

c

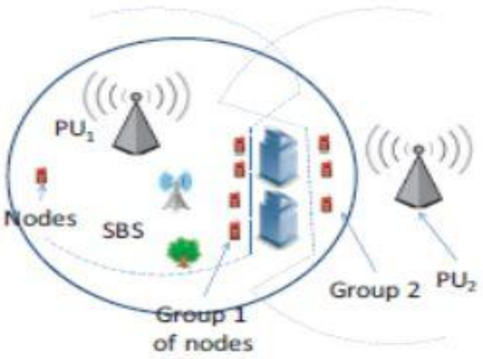

Fig 1:Cognitive Radio Network

CR can sense its environment and, without the interference of the user, can adapt to the user's communications needs while harmonious to FCC rules in the United States. In theory, the amount of spectrum is infinite; practically, for propagation and other reasons it is limited because of the desirability of certain spectrum portions. Assigned spectrum is far from being fully used, and efficient spectrum use is a growing concern; CR offers a solution to this problem. A CR can intelligently detect whether any part of the spectrum is in use, and can temporarily use it without interfering with the transmissions of other users.

Reliable detection of primary users (PUs) is an essential task for cognitive radio (CR) systems. Cooperation among a few spectrum sensors has been shown to offer symbolict gain in the performance of the CR spectrum-sensing system by responds the shadow-fading effects. We consider a parallel fusion network in which the sensors send their sensing information to an access point which makes the ultimate decision regarding presence or absence of the PU signal. It has been shown in the literature that the presence of hostile users sending false sensing data can severely degrade the performance of such a cooperative sensing system. We take into consideration denies imposed by the CR scenario such as the lack of information about the primary signal propagation status and the less amount of the sensing data samples. Considering partial information of the PU performance, we propose a novel method to identify the hostile users. We further propose malicious user detection schemes that take into delibration the structural information of the CR sensors.

III HOSTILE USER DETECTION IN CRNS

One of the most familiar techniques used for detecting malicious users is based on the assumption that neighboring CRs have similar readings. These algorithms uses a passive approach that detects malicious users at the same time while sensing the channel for the survival of PUs. The algorithms based on this technique collect readings from all CRs and then mark those nodes as hostile whose readings differ significantly from their neighbors.

An algorithm proposed by Min et al. [7] first guess the transmission level of the PU and the path-loss exponent on the basis of sensing readings of all CRs. But, their algorithm requires knowledge of the exact locations of CRs. Further, they assume that the path loss exponent is equal for all CRs which may not be true depending on exact location of obstacles [8], [9]. ADSP, proposed by Min et al. [10], [11] for secure sensing entirety by arranging CRs in clusters. It is assumed that nodes in the cluster have interaction among themselves, and here also, knowledge of distance between all pair of nodes is needed. Kaligineedi et al. [3] have uses outlier detection technique that finds hostile users by comparing the report of users with its neighbors. Most of the algorithms for the detection of hostile users in cognitive radio networks [3], [7], [10]–[12] are based on the hypothesis that neighboring nodes have equal readings.

.

A ATTACK-TOLERANT DISTRIBUTED SENSING PROTOCOL

Distributed sensing has been recognized as feasible means to enhance the incumbent signal detection by exploiting the diversity of sensors.But, it is challenging to make such distributed sensing secure due mainly to the unique features of DSA networks—acceptance of a low-layer protocol stack in SDR devices and non-existence of communications between primary and secondary devices.

Sensors are grouped into a cluster, and sensors in a cluster cooperatively safeguard distributed sensing. The heart of ADSP [7]is a innovative shadow fading correlation-based filter tailored to anomaly detection, by which the fusion center prefilters irregular sensor reports via cross-validation. By realizing this correlation filter, ADSP minimizes the impact of an attack on the completion of distributed sensing, while incurring minimal processing and communications overheads.

ADSP for DSA networks that filters out the abnormal sensor reports by exploiting shadow fading correlation in RSSs. ADSP that selectively filters out abnormal sensor reports, and thus maintains the accuracy of incumbent detection. The key idea behind this technique is that the measured primary signal strength at nearby sensors should be coordinate due to shadow fading, which had not been examined before. To realize this idea, we proposed a sensor clustering method and designed filters and data-fusion rules based on the correlation analysis of the sensor reports. ADSP(Fig 2) can be implemented in 802.22 WRANs, incurring very low processing and communication overheads

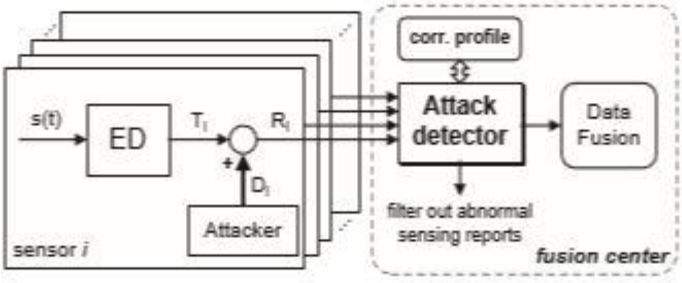

Fig 2. Fig 2 The ADSP framework

ADSP that has the following features: It 1) successfully tolerates attacks (or faults or effects) of malicious sensors, 2)deed physical-layer signal propagation characteristics with less processing overhead, 3) preserves compatibility with existing security and data fusion techniques, and 4) achieves high detection accuracy and efficiency.

B .OUTLIER DETECTION TECHNIQUE

Reliable disclosure of primary users (PUs) is an important effort for cognitive radio (CR) systems. Cooperation among a few spectrum sensors has been shown to offer momentous gain in the act of the CR spectrum-sensing system by countering the shadow-fading effects. We consider a duplicate fusion network in which the sensors send their sensing data to an access point which makes the ultimate decision regarding presence or absence of the PU signal. The presence of malicious users sending false sensing data can degrade the performance of such a cooperative sensing system. To identify the malicious users, outlier detection techniques for a cooperative sensing system exploit energy detection at the sensors. We take into consideration constricts imposed by the CR scenario such as the default information about the primary signal propagation environment and the lack of the sensing data samples. Considering imperfect information of the PU activity, we propose hostile user detection schemes that take into consideration the structural information of the CR sensors.

To identify the malicious users in the system ,[5]compare the magnitudes of the outlier factors, computed using bi-weight as the location evaluate and BWS as the scale estimate , with a threshold $\theta 1$ during each iteration. The users which have the magnitude above the threshold are considered hostile. If the number of such users is more than $Mmax$, then only the $Mmax$ users with the greater outlier factor magnitudes are considered hostile.

If the PU system is dynamic, with the PU signal appering and disappearing after every few sensing iterations, the hostile user detection schemes can be further improved. Significant increase in the energy values of the CR users from one sensing iteration to another would,almost, imply that the PU has started transmission during the distinct sensing iteration. In addition, when the energy values of sensors show significant decrease might indicate that PU has stopped transmission. The difference in the energy values of the CR users, the state of the PU changes over a period of time, can be used to detect those hostile users which do not exhibit similar behavior as rest of the users.

Identifying the malicious users which decrease the CR throughput by sending false high energy values when the PU is absent. Several important constraints imposed by the CR scenario have been taken into consideration. The proposed malicious user detection schemes do not require feedback from the PU network or knowledge of the additive noise variance and the location of the primary transmitter. Assuming partial knowledge of the PU activity, we proposed a novel method to improve the performance of the malicious user detection scheme. For the case of a CR cooperative sensing system spread over a wide area with significant difference in path loss components of the channels between the PU and various sensors.

Existing techniques for hostile users detection in CRNs have some limitations these are,

The actual state of the PU is unknown to the system, therefore, this makes it much harder for existing algorithms to detect hostile users. Thus, if multiple hostile CRs are present in the system, it is viable that before they are detected, they are able to assure the sensing server to make incorrect decisions about the occupancy of the channel. This lead to CRs causing interference to the PU transmissions ..

2) Due to the presence of obstacles and multipath [2], [8], the expectations that neighbors have equal readings or the readings follow a particular correlation model do not hold well [9] resulting in either huge false positives or huge false negatives even if precise location of CRs is known..

3) The existing algorithms do not allow detection of hostile users that do not perform in-band sensing

IV FASTPROBE:MALICIOUS USER DETECTION

FastProbe [12]can be used to find the hostile user present in the cognitive radio networks. Cognitive radio conducts various sensing tests by sensing server and neighbor node is tested by transmitting primary user emulation (PUE) signals. Based on the received signal strength report obtained from the node which is tested, it is possible to estimate whether this node is hostile or not. The tests can be strongly delivered to nodes before the actual sensing needs to be done, FastProbe [12] used proactive approach to detect hostile users.

The detection process is more accurate because of the following reasons:

- Secondary user base station(SBS) have entire knowledge about the ground truth (e.g. transmission power level and pathloss information) for the tests, thus it can more exactly conclude if the received power level reported by a receiver is correct or not.
- Information of received signal strength at a receiver for a given transmitter are compared with the earlier readings for the same transmitter receiver pair. This is very useful for detect the malicious users in the cognitive.

For finding the hostile users, first check the observed pathloss and expected pathloss. If the value of observed pathloss is change from expected pathloss, this means that noise associated with the transmission or nj is maliciously reporting incorrect reading. If the observed pathloss is similar to expected pathloss, then the node is not a malicious one.

After that process, check the expected and received power level reported by node nj and if the power level is less than or equal to noise floor level, then the node is not a hostile user and renew the reputation value of all secondary users. Otherwise it persuade node is malicious.

V Conclusion

Cognitive network is sensitive to security hazards. The attackers may be external users or secondary users acting as a malicious user. So, in order to overcome these issues malicious user detection system is used. Compared with existing algorithms which are reactively detect hostile SUs FastProbe , a novel active transmissions based algorithm for detecting such malicious SUs. FastProbe is the first algorithm that can proactively detect malicious SUs, thereby preventing Cognitive Radio Networks from making incorrect sensing decisions. This helps in reducing the interference to Primary Users as well as increases the accuracy of sensing. FastProbe [12]reduces the throughput loss due to sensing by as much as 65% while achieving higher accuracy compared to existing algorithms.

REFERENCES

[1] H. Kim and K. G. Shin, "In-band Spectrum Sensing in Cognitive Radio Networks: Energy Detection or Feature Detection?" in Proc. of ACM MobiCom, 2008.

[2] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative Sensing Among Cognitive Radios," in Proc. of IEEE ICC, 2006.

[3] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System," IEEE TWC, vol. 9, no. 8, pp. 2488–2497, 2010.

[4] O. Fatemieh, A. Farhadi, R. Chandra, and C. Gunter, "Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks," in Proc. of NDSS, 2011

. [5] A. W. Min, K.-H. Kim, and K. G. Shin, "Robust Cooperative Sensing via State Estimation in Cognitive Radio Networks," in Proc. of IEEE DySPAN, 2011.

[6] T. Bansal, B. Chen, and P. Sinha, "DISCERN: Cooperative Whitespace Scanning in Practical Environments," in Proc. of IEEE INFOCOM, 2013

[7] A. Min, K. Shin, and X. Hu, "Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks," in Proc. of IEEE ICNP, 2009

. [8] A. W. Min, K. G. Shin, and X. Hu, "Secure Cooperative Sensing in IEEE 802.22 WRANs Using Shadow Fading Correlation," IEEE Transactions on Mobile Computing, 2010.

[9] O. Fatemieh, R. Chandra, and C. Gunter, "Secure Collaborative Sensing for Crowd Sourcing Spectrum Data in White Space Networks," in Proc. of IEEE DySPAN, 2010.

[10] H. Li and Z. Han, "Catch Me If You Can: An Abnormality Detection Approach for Collaborative Spectrum Sensing in Cognitive Radio Networks," IEEE Transactions on Wireless Communications, vol. 9, no. 11, pp. 3554–3565, 2010.

[11] W. Wang, H. Li, Y. Sun, and Z. Han, "Securing Collaborative Spectrum Sensing Against Untrustworthy Secondary Users in Cognitive Radio Networks," EURASIP Journal on Advances in Signal Processing, 2010

[12] T. Bansal, B. Chen, and P. Sinha, "Malicious User Detection in Cognitive Radio Networks Through Active Transmissions," Tech. Rep., http://www.cse.ohio-state.edu/~bansal/FastProbeTechRep.pdf.

Reshma Rajan In 2012, she graduated with a Degree in Electronics and Communication Engineering from the Cochin University of Science and Technology, Kerala, India. She is doing M.Tech in Wireless Technology from the Cochin University of Science and Technology, Kerala, India. Her research interests include smart sensor and wireless sensor networks.

Syamesh K G, He is an Assistant Professor in Electronics And Communication Engineering Department at University of CUSAT he graduated with a Degree in electronics and communication engineering from the MG University, Kerala, India. and post graduated from CUSAT, Kerala, India. Her research interests include smart sensor and wireless sensor networks.

Jeethumol K Joy In 2014, she graduated with a Degree in Electronics and Instrumentation Engineering from the Cochin University of Science and Technology, Kerala, India. She is doing M.Tech in Wireless Technology from the Cochin University of Science and Technology, Kerala, India. Her research interests include smart sensor and wireless sensor networks.