International Journal of Advance Research and Innovation
Vol. 3(2), Apr-Jun 2015, pp. 40-43
Doi: 10.51976/ijari.321510

**Article Info**
Received: 04 Apr 2015 | Revised Submission: 30 Apr 2015 | Accepted: 20 May 2015 | Available Online: 15 Jun 2015

# Defense against Spectrum Sensing Data Falsification Attacks Based on Adaptive Reputation Based Clustering

*R. Amutha Priya* and S. Nandhakumar***

**ABSTRACT**

*The cognitive radio recommends collaborative spectrum sensing to avoid the unpredictability of personage spectrum sensing even as detecting primary user signals. A chance for attackers to take advantage of the decision making process by sending false reports. Security issues on the subject of dispersed node sensing in the 802.22 standard and talk about how attackers can modify or influence their sensing result independently or collaboratively. This problem is commonly recognized as spectrum sensing data falsification (SSDF) attack or Byzantine attack. To oppose the different attacking strategies, a reputation based clustering algorithm that does not necessitate preceding knowledge of attacker distribution or complete classification of malicious users. So provide an extensive probabilistic analysis of the performance of the algorithm. The performance of our algorithm in opposition to existing approaches across a wide range of attacking scenarios. Our planned algorithm displays a considerably reduced error rate in decision making in association to current methods. It also identifies a large portion of the attacking nodes and to the highest degree minimizes the false detection rate of truthful nodes.*

***Keywords:*** *Spectrum; Data Falsification Attack; Cognitive Radio Network; ARC; Byzantine Attack.*

## 1.0 Introduction

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as except that the first center is chosen uniformly random, each subsequent center is orderly chosen according to its squared distance from the closet center already chosen.

Energy memory, computational speed and communications bandwidth The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

A cognitive radio is an intelligent radio that can be programmed and configured dynamically. Its transceiver is designed to use the best wireless channels in its vicinity. Such a radio automatically detects available channels in wireless spectrum, then

**Corresponding Author: Department of Computer Science Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India (E-mail: amuthapiya11@gmail.com)*
***Department of Computer Science Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India*

accordingly changes its transmission or reception parameters to allow more concurrent wireless communications in a given spectrum band at one location. This process is a form of dynamic spectrum management.

The main functions of cognitive radios are Power Control and Spectrum Sensing. Power control is used for both opportunistic spectrum access and spectrum sharing CR systems for finding the cut-off level in SNR supporting the channel allocation and imposing interference power constraints for the primary user's protection respectively. Spectrum sensing is used to detecting unused spectrum and sharing it, without harmful interference to other users; an important requirement of the cognitive-radio network to sense empty spectrum. Detecting primary users is the most efficient way to detect empty spectrum. Spectrum-sensing techniques may be grouped into three categories. Those are transmitter detection, matched filter detection, energy detection.

Energy detection is a spectrum sensing method that detects the presence/absence of a signal just by measuring the received signal power. This signal detection approach is quite easy and convenient for practical implementation. To implement energy detector, however, perfect noise variance information is required. And surprisingly when there is noise uncertainty, there is an SNR wall below which the energy detector cannot reliably detect any transmitted signal. In, a new energy based spectrum sensing algorithm with noise variance uncertainty is proposed. This algorithm does not suffer from SNR wall and outperforms the existing signal detectors (see for example and its USRP implementation). And most importantly, the relationship between the energy detector of and that of is quantified analytically. Also when the noise variance is known perfectly these two energy detectors achieve the same probability of detection and false alarm rates.

Cyclostationary-feature detection is the type of spectrum sensing algorithms are motivated because most of manmade communication signals such as BPSK, QPSK, AM, OFDM exhibit cyclostationary behaviour. However, noise signals (typically white noise) do not experience this behaviour. These detectors are robust against noise variance uncertainty. The aim of such detectors is to exploit the cyclostationary nature of manmade communication signals buried in noise. Cyclostationary detectors can be either single cycle or multicyclecyclostatonary.

### 1.1 Attacks in the wireless sensor network

Wireless sensor networks are affected by the different attacks. Those are spectrum sensing data falsification (SSDF) attack, Independent attack, Collaborative attack. Spectrum sensing data falsification (SSDF) attackmeans that attackers devise their plan independently or collaboratively. Based on their attacking strategy, each attacker node may alter its sensing result from busy to idle and from idle to busy with different probability.

Assume that both of the probabilities are the same. Results can be easily extended for different probability. Accordingly, consider one independent and three collaborative attacking techniques. Selected the attacking techniques considering the ease of implementation, impact of the attack, frequency of attack and so on.

The first collaborative technique "L out of M" was already shown to be effective in. The second technique is considered here due to ease of implementation and it follows an intuitive attacking model. The third technique is considered to exploit the decision mechanism used in this project.

Independent Attack means each independent attacker changes its sensing result with probability Pmal. The detection probability of an individual attacker, Pmd while working independently. In collaborative Spectrum sensing data falsification (SSDF) attack, attackers exchange their sensing information and decide their response collaboratively. First, the collaboration strategy ‘L out of M’ attack. Only 35% of attackers using this approach can blind the decision mechanism of the BS.

Clustering techniques are often used in anomaly identification or outlier detection. Two of the prominent clustering techniques are K-means and K-medoid. K-means defines a cluster in terms of a centroid, which is usually the mean of the group of points. It clusters the objects in a way to minimize the sum of squared Euclidean distance.

On the other hand, K-medoid defines a cluster in terms of a medoid, which is the most representative object for a group of objects and can be applied to a wide range of data. The K-medoid algorithm requires only a proximity measure for a pair of objects and tries to minimize the total error.

We prefer K-medoidto K-means algorithm for clustering since the former is more robust to noise and outliers than the latter and minimizes a sum of pair wise dissimilarities instead of a sum of squared Euclidean distances. Several algorithms have been proposed to implement Kmedoid clustering. Partitioning Around Medoid (PAM) algorithm to cluster nodes based on their sensing reports. A medoid is the node of the cluster whose average dissimilarity to all other nodes in the same cluster is minimal. Given the number of clusters and sensing reports from all the nodes as input, PAM sequentially finds the same number of nodes as medoids around which all other nodes are clustered in a way so that the objective function is

minimized.PAM so that each cluster has an equal number of nodes. In existing system using K-neighborhood distance algorithm & Robust decision algorithm is detect independent malicious users. This approach does not need any prior knowledge of attacker distribution and exposes attackers across multiple sensing rounds. In the past Static spectrum allocation cannot efficiently support the demand of such pervasive wireless devices. Individuals who have obtained a license to broadcast in a fixed spectrum range are classified. Radio waves are affected by physical barriers or environmental conditions easily. Malfunctions associated with the sensing equipment may also influence the node's observed measurements. Existing system following techniques are having the drawbacks. Those are secondary users are attempt to "fill in the gaps" by utilizing unused spectrums, users and may begin sending modified sensing reports to the BS. The compromised nodes may work independently, or may collaborate to reduce spectrum utilization and degrade overall performance of the network and primary user positioning and path loss to the secondary user.

## 2.0 System Model

The existing solutions to combat against Spectrum sensing data falsification (SSDF) attack into three categories. Those are reputation-based, data mining based, and artificial intelligence approaches. Adaptive Reputation Based Clustering algorithm to protect against both independent and collaborative Spectrum sensing data falsification (SSDF) attacks that does not require prior information about the number of attackers or attacking strategies. To locate independent malicious attacks and collaborative attacks. Find number of attackers, attackers' distribution, attacking strategy our algorithm also identifies a significant number of attackers while keeping the misdetection rate to a minimum level. A trust based model and use a weighted sensing result aggregation scheme to remove malicious nodes from the decision making process and present a hybrid method called the weighted sequential probability ratio test (WSPRT) that combines a node's reputation and the use of a sequential probability ratio test to identify malicious or faulty units.

Our Proposed methods are having different advantages. Those are Base Station make the Decision differentiates between the honest users and the attackers. The nodes are clustered based on the sensing history and initial reputation of Nodes. The channel status is decided through intra-cluster and inter-cluster voting. Minimizes the error in deciding channel status and get the honest result in users.

### 2.1 Data collection phase

Data collection phase used to collect the sensing information from the User. Here users having two types. Those are Primary user and Secondary user. In this data collecting phase considering only the details given by the secondary users. From secondary users get the Information from the Cluster through query. Based on the request and response find who is the honest user and who is the false users. If user is honest send the original sensing result. If the user is false user modify the sensing result was send.

### 2.2 Data clustering phase

Second phase is data clustering phase, after finishing the data collection, it will be started. In this phase is using two types of clustering techniques to clustering the collection data from the secondary users. Those are PAM Algorithm Based Cluster Formation and Collect all users and Secondary Users Data.

### 2.3 Attacking phase

Independent attack, Collaborative Attack, Third party Attack disrupting the channel and send reply Channel busy. Malfunctions associated with the sensing equipment may also influence the node's observed measurements. Attackers devise their plan independently or collaboratively. Based on their attacking strategy, each attacker node may alter its sensing result from busy to idle and from idle to busy with different probability. ARC separates attackers from honest users based on sensing reports using an adaptive clustering technique. Attackers must make sure that their sensing reports are not too different from those of honest users to avoid being detected by ARC. Otherwise, attackers will be separated into the same cluster and thus, will be detected and eliminated.

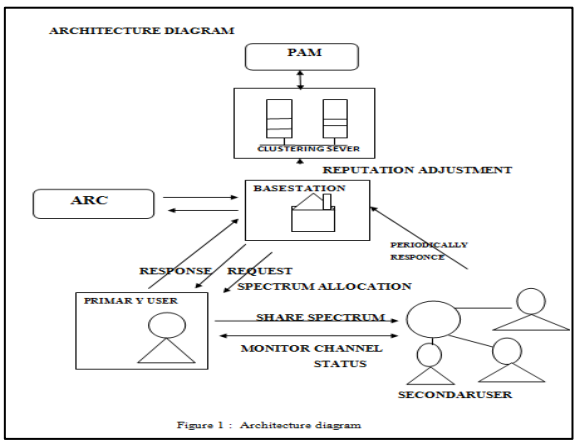

Figure 1 : Architecture diagram

**2.4 Match user decision phase**

After attacking phase we go into the match user decision phase. This decision phase used to Check Users Data's and based on the Clusters History match the correct users.

Here using the ARC Algorithm Implementation for making decision about how was match the user and finally calculate the Probability Result Matching with User Data.

**2.5 Reputation adjustment phase**

This is the final phase in our method. Reputation adjustment phase is used to verify the Algorithm Result Update again Cluster Area. That means used to ARC Algorithm finding the different from cluster history details. Finally convert Binary Result and Update Cluster Server.

**3.0 Conclusion**

This paper describes about the Cognitive Radio network. Here explained the major security problems afflicting cognitive radio networks and propose a reputation based clustering algorithm to defend against these attacks such as spectrum sensing data falsification (SSDF) attack, Independent attack, Collaborative attack.

Cognitive radio networks are sensing their history of the reputation of nodes to form clusters and then adjust their reputation based on the cluster output.

This recursive approach is tested in the presence of independent and collaborative spectrum sensing data falsification attacks. With respect to current approaches, our algorithm significantly reduces the error rate in the final decision making process, thus increasing spectrum utilization.

The false detection rate by our algorithm is almost negligible while true attacker detection rate performs reasonably well. On the other hand, the initial number of clusters plays an important role in overall performance of the algorithm.

Compare the performance of our algorithm against existing approaches across a wide range of attacking scenarios.

Our proposed algorithm displays a significantly reduced error rate in decision making in comparison to current methods. It also identifies a large portion of the attacking nodes and greatly minimizes the false detection rate of honest nodes in like 4G and Wi-Max and so on

**References**

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, S. Mohanty, A survey on spectrum management in cognitive radio networks, IEEE Commun. Mag., 46(4), 2008, 40–48

[2] K. Bian, J.-M. Park, Security vulnerabilities in IEEE 802.22, 4th Annu. Int. Conf. WICON, Brussels, Belgium, 2008, 9:1–9:9

[3] R. Chen, J.-M. Park, K. Bian, Robust distributed spectrumsensing in cognitive radio networks, 27th Conf. Computer Communications INFOCOM, Phoenix, AZ, USA, 2008, 1876–1884

[4] T. C. Clancy, N. Goergen, Security in cognitive radio networks: Threats and mitigation, Crown Com, Singapore, 2008, 1–8

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

[6] F. Farmani, M. A. Jannat-Abad, R. Berangi, Detection of SSDF attack using SVDD algorithm in cognitive radio networks, 3rd Int. Conf. CICSyN, Bali, Indonesia, 2011, 201–204

[7] L. Kaufman, P. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis. New York, NY, USA: Wiley, 1990

[8] T. Qin, H. Yu, C. Leung, Z. Shen, C. Miao, Towards a trust aware cognitive radio architecture, ACM SIGMOBILE MoblieComput. Commun. Rev., 13(2), 2009, 86–95

[9] S. Rawat, P. Anand, C. Hao, P. K. Varshney, Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks, IEEE Trans. Signal Process., 59(2), 2011, 774–786

[10] S. J. Shellhammer, Spectrum sensing in IEEE 802.22, in Proc. IAPR Workshop Cognitive Information, 2008