EXCELLENT PUBLISHERS

*International Journal of Current Research and Academic Review*

**ISSN: 2347-3215 Volume 3 Number 5 (May-2015) pp. 319-329**

www.ijcrar.com


# Root Based Packet Filtering Techniques to Protect Attacking In Spectrum Trading

**S. Suguna[1] and S. AnthoniRaj[2*]**

[1]Department of Computer Science and Engineering, Paavai College of Engineering, Namakkal [Dt], Tamilnadu, India

[2]Department of Information Technology, Paavai College of Engineering, Namakkal [Dt], Tamilnadu, India

***Corresponding author***

**KEYWORDS**

Cognitive radio network,
Spectrum sensing data falsification attack,
Dynamic spectrum access,
802.22,
Packet
filtering techniques,
Spectrum trading

**A B S T R A C T**

Cognitive radio is a revolutionary technology for efficient utilization of radio spectrum. It recommends collaborative spectrum sensing to avoid unreliability of spectrum sensing to detecting primary user signals .It's an opportunity for attackers to exploit the decision making process by sending false reports in spectrum trading. . In this paper, we investigate how attackers can modify or manipulate their sensing result independently or collaboratively. This problem is commonly known as spectrum sensing data falsification (SSDF) attack or Byzantine attack. To counter the different attacking strategies, we propose a reputation based clustering algorithm along with root base based packet filtering technique that can easily identify the location of the user since it provide the location information to the server, it also gets the link IP and connection IP of the user who is trying to get the information. We 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.

## Introduction

Current wireless devices are dominating as methods of communication, the necessary resources to support these conveniences are becoming ever harder to obtain. The radio frequency is a limited natural resource and getting enabled day by day due to growing demand of the wireless communication applications. To operate on a specific frequency band license are needed. The use of radio spectrum in each country is governed by the corresponding government agencies. In conventional technique each user is assigned a license to operate in a certain frequency band. Most of the time

spectrum remains unused and it is also difficult to find it. The allocated spectrum has been not utilized properly; it varies with time, frequency and geographical locations. Thus to overcome the spectrum scarcity and unutilized frequency band, a new communication techniques cognitive radio (CR) and dynamic spectrum access (DSA) is introduced. In order to maximize spectrum utilization, CRNs exploit an opportunistic approach to allocate frequencies. Under the scheme, two types of users exist: primary users (PU), and secondary users (SU). Individuals who have obtained a license to broadcast in a fixed spectrum range are classified as primary users. On the other hand, secondary users attempt to "fill in the gaps" by utilizing unused spectrums. The two types of users complement each other allowing maximum utilization of a specified spectrum. CR network provides efficient utilization of the radio spectrum and highly reliable communication to users whenever and wherever needed. DSA technology allows unlicensed secondary system to share the spectrum with licensed primary system [1]-[2]. The key enabling technology of dynamic spectrum access techniques is cognitive radio (CR) technology, which provides the capability to share the wireless channel with licensed users in an opportunistic manner.CR networks impose unique challenges due to the high fluctuation in the available spectrum, as well as the diverse quality of service (QoS) requirements of various applications. In order to address these challenges, each CR user in the CR network must determine which portions of the spectrum are available and select the best available channel to coordinate access to this channel with other users and vacate the channel when a licensed user is detected [2].Naturally, 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, define a centralized, for wireless regional area network (WRAN). This standard defines the implementation of opportunistic spectrum sharing (OSS) by outlining how/when wireless devices are able to utilize temporarily idle bands in licensed radio spectrums. The proposal also defines the cellular like communication interface between a base station (BS), and secondary users called Consumer Premise Equipments (CPE). The BS is responsible for controlling the spectrum usage and channel assignment to CPEs. All CPEs in a cell must periodically monitor primary user signals and the BS leverages the distributed sensing power of CPEs through continual spectrum reports obtained from them. To coordinate the process, a centralized BS collects sensing information from the secondary users attached to the cell. Each user submits a hypothesis regarding whether or not they suspect the primary user is transmitting. As radio waves are affected by physical barriers or environmental conditions, the detection accuracy of any node within sensing range of the PU's signal varies from time to time. Malfunctions associated with the sensing equipment may also influence the node's observed measurements. From the hypotheses supplied by the secondary users, the BS must decide on the actual state of the associated spectrum. Once a decision is made, the base station informs SUs and revokes permission of the users currently transmitting on that spectrum. Due to its unique characteristics, CRNs face new security threats in addition to the common existing security challenges in wireless networks. One typical type of attack is the Spectrum Sensing Data Falsification (SSDF) attack or Byzantine attack. 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. Constructing a decision-making strategy that mitigates the impact of both types of attackers will prove invaluable as the reach of CRNs expands. By strengthening the base station with route based filtering helps against malicious or malfunctioning users, the interference produced from CRNs will be minimized, potentially expediting the implementation of such network alternatives. To the best of our knowledge, only two paper [2][4] handles both independent and collaborative attacks using a reputation based method and limits the error rate in deciding channel status and identifying attackers. Although this approach's identification rate of attackers is high, it also misdirects a large number of honest users as attackers. Additionally, this approach fails to defend against collaborative attacks, and the error rate (i.e. number of incorrect decisions) increases almost linearly with the number of attackers. On the contrary, we proposed route based packet filtering along with adaptive reputation based clustering algorithm that does not require prior knowledge of attacker distribution or complete identification of malicious users. The whole process goes through a sequence of phases in each time step. First, 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. Route based packet filtering technique can easily identify the location of the user in decision phase and find number of times malicious user exists. We can find the occurrence of malicious users based on sensing history provide the location information to the server, it also gets the link ip and connection ip of the user who is trying to get the information .The final result is then used to adjust the number of clusters and to update the reputation of all nodes. Compare the performance of our algorithm with that of the algorithm proposed in [2] under different attacking scenarios. Our algorithm handles filtering techniques in decision making to counter attackers and minimizes the error in deciding channel status. This algorithm identifies a large portion of the attacking nodes and greatly minimizes the false detection rate of honest nodes.

## Related work

Until recently, security issues in CRN have not been addressed well in research works. However, in this section, we present existing solutions to combat against SSDF attack into three categories: reputation-based, neighborhood distance based, and artificial intelligence approaches.

## Reputation based approaches

Wang et al. [8] propose an onion peeling approach based on Bayesian statistics to assign suspicion levels for all nodes in the network. If the suspicion level of any node exceeds a certain threshold, it is marked as malicious and removed from decision making. They tested their heuristic based approach for false alarm attacks, miss detection attacks, and combinations thereof. However, they assume that base station has prior knowledge about the activities of attackers which is not very common. Without such information, the thresholds are approximated, resulting in significant false detections of attackers. Chen et al. [3] propose a hybrid method named weighted sequential probability ratio test (WSPRT) that combines reputation and a sequential probability ratio test to identify malicious or faulty units. However, WSPRT was only tested against attackers utilizing an always-false or always-free response. They

determined optimal attacking strategies for collaborating attackers where the fusion center cannot possibly discriminate between honest and attacking CRs.

## Data mining approaches

In [1], a new approach based on K-neighborhood distance algorithm is presented to detect independent malicious users. The approach does not need any prior knowledge of attacker distribution and exposes attackers across multiple sensing .Defense against SSDF Attacks in CRN 5 rounds. However, when attackers collaborate and have secondary user data, they can successfully evade detection. Further work has been done by [6] in establishing a more robust fusion center decision algorithm. Specially, particular pieces of sensing information are used to validate the primary user hypothesis presented by each secondary user. Information regarding PU positioning and path loss to the secondary user can corroborate the hypothesis. The proposed method dramatically increases misdetections when using incorrect static thresholds. Inaccurately identified secondary users could be excluded from the decision making process, resulting in a PU signal being ignored. Ultimately, the correct setting of the detection thresholds can only be achieved with prior knowledge of attacker distribution. Again, the information is unlikely to be available.

## Artificial intelligence approaches

Clancy et al. [4] take a practical look into devising security for the physical transport layer of CRNs, focusing on CRs with artificial intelligence. When implementing such schemes, the CRs are highly susceptible to short-term and long-term manipulations caused by corrupted sensory data, altered node statistics, and inaccurate beliefs regarding the current environment. The paper addresses a series of steps to combat these sensitive areas by assuming a noisy environment, implementing levels of common sense, and programmatically resetting learned values to avoid extended corruption from attackers. The proposals on how these CRs should operate in the field are presented without details for verification. They also did not address how to incorporate this new information into the current 802.22 system. The current state of research holds very few proposals that work on realistic knowledge of the operating environment. Furthermore, misidentification of attackers could also severely impact the effectiveness of strategies. Such considerations must be respected to develop a truly robust scheme. Ultimately, the approaches will need to face real attacks while producing acceptable error rates. Recently, few more research works have addressed the spectrum sensing data falsification attack by using suspicious level[19], ,weighted sequential approach[3],incumbent approach[7], incentive based approach[6].

## System model

Figure 1 shows the detailed classification of spectrum Sensing techniques. They are broadly classified into three main types, transmitter detection or non cooperative sensing, cooperative sensing and interference based sensing. Transmitter detection technique is further classified into energy detection, matched filter detection and Cyclostationary feature detection [7].

## Primary transmitter detection

## Energy detection

Due to its simplicity and no requirement on a priori knowledge of primary user signal,

energy detection (ED) is the most popular sensing technique in cooperative sensing .In this method, signal is passed through band pass filter of the bandwidth W and is integrated over time interval. The output from the integrator block is then compared to a predefined threshold. The ED is said to be the Blind signal detector because it ignores the structure of the signal. It estimates the presence of the signal by comparing the energy received with a known threshold derived from the statistics of the noise.

## Matched filter

A matched filter (MF) is a linear filter designed to maximize the output signal to noise ratio for a given input signal. When secondary user has a priori knowledge of primary user signal, matched filter detection is applied.

Matched filter operation is equivalent to correlation in which the unknown signal is convolved with the filter whose impulse response is the mirror and time shifted version of a reference signal. Matched filter detection needs less detection time because it requires only O(1/SNR) samples to meet a given probability of detection constraint. When the information of the primary user signal is known to the cognitive radio user, matched filter detection is optimal detection in stationary gaussian noise [9].

## Cyclostationary feature detection

It exploits the periodicity in the received primary signal to identify the presence of primary users (PU). The periodicity is commonly embedded in sinusoidal carriers, pulse trains, spreading code, hopping sequences or cyclic prefixes of the primary signals. Due to the periodicity, these Cyclostationary signals exhibit the features of periodic statistics and spectral correlation, which is not found in stationary noise and interference [9].

Thus, Cyclostationary feature detection is robust to noise uncertainties and performs better than energy detection in low SNR regions. Although it requires a priori knowledge of the signal characteristics, Cyclostationary feature detection is capable of distinguishing the CR transmissions from various types and their sensing accuracy shown in figure 2.

## Cooperative techniques

High sensitivity requirements on the cognitive user can be alleviated if multiple CR users cooperate in sensing the channel. Various topologies are currently used and are broadly classifiable into three regimes according to their level of cooperation

## Decentralized uncoordinated techniques

The cognitive users in the network don't have any kind of cooperation which means that each CR user will independently detect the channel, and if a CR user detects the primary user it would vacate the channel without informing the other users.

## Centralized coordinated techniques

In such networks, an infrastructure deployment is assumed for the CR users. One CR that detects the presence of a primary transmitter or receiver, informs a CR controller which can be a wired immobile device or another CR user.

The CR controller notifies all the CR users in its range by means of a broadcast control message. Centralized schemes can be further classified according to their level of cooperation as: Partially cooperative where network nodes cooperate only in sensing the channel.

### Decentralized coordinated techniques

This type of coordination implies building up a network of cognitive radios without having the need of a controller. Various algorithms have been proposed for the decentralized techniques among which are the gossiping algorithms or clustering schemes, where cognitive users gather to clusters, auto coordinating themselves [6].

### Benefits of cooperation

Cognitive users selflessly cooperating to sense the channel have lot of benefits among which the plummeting sensitivity requirements channel impairments like multipath fading, shadowing and building penetration losses, impose high sensitivity requirements inherently limited by cost and power requirements.

### Disadvantages of cooperation

The CR users need to perform sensing at periodic intervals s sensed information become obsolete fast due to factors like mobility, channel impairments etc. This considerably increases the data overhead; large sensory data: since the cognitive radio can potentially use any spectrum hole, it will have to scan a wide range of spectrum, resulting in large amounts of data, being inefficient in terms of data throughput, delay sensitivity requirements and energy consumption.

### Algorithm design - attackers Vs BS

In this section, we discuss the viewpoints of attackers and BS and explain the defense mechanism taken by BS to defend against different attacking strategies. As stated in Section 3, attackers' detection rate varies with their strategy and is different from that of honest users. So, if the attackers can successfully manipulate the decision making process, detection rate will be significantly how, error rate in decision making will be high and spectrum utilization will be degraded. From the attackers' point of view, the more error they make in decision making, the more successful they are. So, the most common attacking strategy is to falsify about channel status in every time step and send it to BS. In collaborative attack, since attackers share their information, they may have better idea about the actual channel status and devise their attacking plan in a more effective way. The collaboration makes it easier to manipulate the BS decision mechanism than independent attack and increases their success rate. However, if the malicious users try to strengthen their attacks and continuously send false channel status, the pattern of their sensing report will be almost the same. In this way, their sensing history will be significantly different from honest users and will be easily identifiable. So, the best attacking strategy is to attack occasionally or try to behave like an honest user otherwise. In summary, attackers' success depends on attacking frequency (i.e. when to attack) and how long they can attack without being identified. Together, all attackers can follow the same plan and can make the decision making process more complicated.

Now, from BS's point of view, its decision mechanism should be robust and capable of defending against any attacking strategy adopted by any number of malicious users. However, BS does not have any exact information about the attacking strategies or number of attackers. The only information available to BS is the sensing reports sent by users. So, the defense mechanism should be able to nullify (or at least reduce) the impact of collaboration of attackers, identify them and quarantine them from the decision

process. Accordingly, we design an adaptive reputation based clustering (ARC) algorithm with filtering techniques to sense the defend against both types of SSDF attack. The algorithm works against the intention and motivation of malicious users and tries to nullify their influence on the final decision. To reduce the impact of attackers, we create clusters .so that nodes with similar sensing history will be in the same cluster. Then, each cluster has only one vote to cast and channel status is decided based on majority voting of clusters. The idea hind this defense mechanism is that if the attackers attack frequently, attackers and honest nodes will be in separate clusters due to their different sensing reports. Also, collaboration of attackers will not help to increase the error rate since each cluster has only one vote. The key to attackers' success is to avoid being in the same cluster and take control of the majority of the clusters. To handle these issues, we introduce distance weighted voting in a cluster and a feedback impotent in each node's reputation. Voting power of each node in the cluster is inversely proportional to its distance from the median of that cluster. Root based filtering techniques is used for cluster formation and clustering location details are updated in server. Similarly, each node gets reputation inversely proportional to its distance from the median of that cluster. By distributing the reputation based on distance from the median, nodes are only impacted relative to their confidence of that group (see Figure 3).Furthermore, from the next round, nodes' modified reputation is also used to cluster nodes in addition to sensing history. In this way, even if an attacker and an honest user incorrectly fall in the same cluster, attackers cannot establish their decision. Furthermore, as time goes, the distance between an honest user and an attacker will be amplified due to the joint consideration of reputation and sensing history.

## Root based packet filtering techniques

The proposed Root based packet filtering techniques used in adaptive reputation based clustering (ARC) algorithm executes a sequence of phases to reach the final decision (Fig. 4). In the *collection* phase, the BS collects the sensing reports with ip address of users and update in server from all the nodes in its cell. In the *clustering* phase, the modified version of the partitioning around medoids (PAM) algorithm is applied to create *k* equal sized virtual clusters. In the *voting* phase, final decision is made based on intra-clustering and inter-clustering voting. This is followed by an *update* phase where the number of clusters is adjusted and the reputation of all nodes is reevaluated. Next, the major components of our algorithm are explained.

## Cluster formation (*Clustering Phase*)

Clustering techniques are often used in anomaly identification or outlier detection. Two of the prominent clustering techniques are K-means and K-medoid [12]. 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-medoid to K-means algorithm for clustering former is more robust to noise and outliers than the latter and minimize a sum of pair wise dissimilarities instead of a sum of squared Euclidean distances. Several algorithms have been proposed to implement Kmedoid clustering. We use the Partitioning Around

Medoid (PAM) algorithm [6] 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. We modify *PAM* so that each cluster has an equal number of nodes. The BS maintains a $d$+1 dimensional vector ($X1$ = [$r1$,1, $x1$,1, ... $xd$,1]) to store information for each node. The first dimension represents reputation and the remaining ones represent sensing report of last $d$ time steps. The most recent $d-1$ sensing reports of each node are directly considered in calculation while the prior history is also maintained in one dimension as weighted average of previous sensing reports. So, the effect of past sensing reports decrease with time. Sensing report details are maintained in server with their ip address and cluster formed by K-mediod and PAM algorithm .

## Decision making (*Voting Phase*)

One of the key features in our algorithm is how we reach the final decision and use that decision recursively to update the clustering. As stated earlier, the BS considers the most recent $d$ sensing report sof each node in addition to their reputation during cluster formation. The reputation score is always between 0 and 1. We assume that the BS is unaware of the location of nodes attached to it. All nodes are assigned 0.5 as the initial reputation score. The decision process goes through two sub steps: intra-cluster voting and inter-cluster voting. Decision making are done by comparing root path of the cluster formation details in server along with voting phase and both should have same threshold value.

## Intra-cluster voting

Each cluster finalizes its decision about channel status in a unique way. Only the last round sensing report of each node in the cluster is considered. However, each response is weighted with an impact factor that is inversely proportional to the distance between the node and the median of that cluster.

## Inter-cluster voting (Final decision)

After each cluster finalizes its decision, the BS checks the validity of each cluster and makes the final decision $V(t)$ on the basis of majority voting among the valid clusters. If the average reputation of all member nodes of a cluster is below a threshold, the cluster is invalid; then the members in that cluster cannot vote and are marked as attackers. The cluster validation process is performed periodically.

## Reputation adjustment (*Update Phase*)

At the end of every time step, the BS updates the reputation of all the nodes according to the algorithm and if needed, increases the number of clusters. The final result is propagated back to the clusters, and then to the individual nodes. If the final decision matches with a cluster decision, that cluster gets a positive feedback; otherwise, it gets negative feedback. Similarly, if a node's decision matches with its cluster decision, it gets positive feedback while it receives negative feedback for a mismatch. The final result is also used to adjust the number of clusters. Initially, we start with 5 clusters with 5 random medoids. After each validation period, if all clusters pass the validation (i.e. average reputation score exceeds threshold, we increment the number of clusters and continue the same process.

**Figure.1** Classification of spectrum sensing techniques

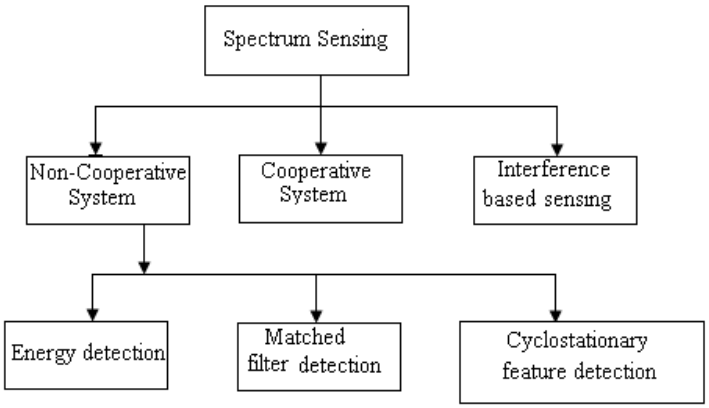



**Figure.2** Sensing accuracy and complexity of various sensing methods

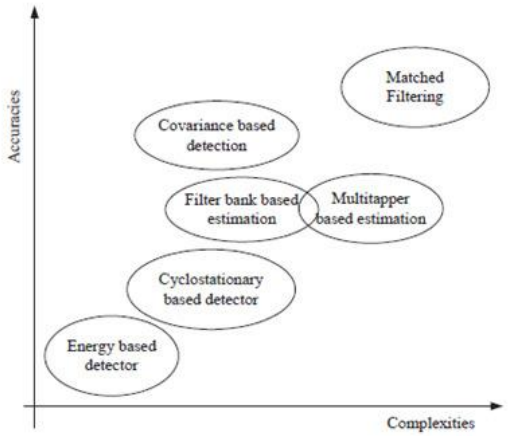



**Figure.3** Reputation distribution

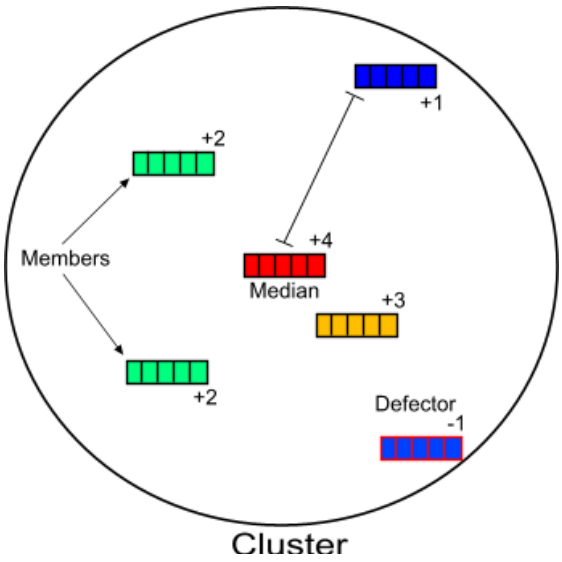
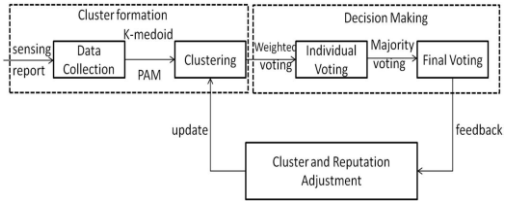


**Figure.4** Block diagram of different phases of the algorithm




Otherwise, we remove all the nodes in the cluster that fails the test. After few periods, we go back to initial state removing "attacker" tag and start the algorithm from the beginning.

## Conclusion

A root base based packet filtering technique used to solve major security problems afflicting CRNs and by using these techniques in reputation based clustering algorithm to defend against these attacks. We use the reputation of nodes in addition to their sensing history to form clusters and then adjust their reputation based on the cluster. This recursive approach is tested in the presence of independent and collaborative spectrum sensing data falsification attacks. Packet filtering in decision making is used to find the attacker in decision making and 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. However, the initial number of clusters plays an important role to give overall performance of the algorithm.

## References

1.H. Li and Z. Han, "Catching attackers for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in *Proc. DySPAN*, Singapore, 2010, pp. 1–12.

2. 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.

3.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.

4. T. C. Clancy and N. Goergen, "Security in cognitive radio networks:Threats and mitigation," in *Proc. CrownCom*, Singapore,2008, pp. 1–8.

5.K. Bian and J.-M. Park,"Security vulnerabilities in IEEE 802.22,"in *Proc. 4th Annu. Int. Conf. WICON*, Brussels, Belgium, 2008,pp. 9:1–9:9.

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

7.Weifang Wang (2009), "Spectrum Sensing for Cognitive Radio'', Third International Symposium on Intelligent Information Technology Application Workshops, pp: 410-412.

8.W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: Detect malicious nodes in collaborative spectrum sensing," in *Proc. GLOBECOM*,Piscataway, NJ, USA, 2009, pp. 1–6.

9.V. Stoianovici, V. Popescu, M. Murroni (2008), "A Survey on spectrum sensing techniques in cognitive radio" Bulletin of the Transilvania University of Brasov, Vol. 15 (50).

10.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.

11.T. Yucek and H. Arslan "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, Jan. 2009.

12. F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data Defense against spectrum sensing data radios," in *Proc. IEEE MILCOM*, Boston, MA, USA, Oct. 2009, pp. 1–7.

13.T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao,"Towards a trust aware cognitive radio architecture," *ACM SIGMOBILE Moblie Comput. Commun. Rev.*, vol. 13, no. 2, pp. 86–95, Sep. 2009.

14.S. Sodagari, A. Attar, V. C. M. Leung, and S. G. Bilén, "Denial of service attacks in cognitive radio networks

15.L. Duan, A. W. Min, J. Huang, and K. G. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks,"*IEEE J. Select. Areas Commun.*, vol. 30, no. 9, pp. 1658–1665,Oct. 2011.

16.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,Aug. 2010.

17. R.Chen, J.-M. Park Y. T. Hou, and J. H. Reed", Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008.

18.I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty,"A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 40–48, Apr. 2008.