ISSN (Print) : 0974-6846
**Indian Journal of Science and Technology,** *Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/105072, November 2016* ISSN (Online) : 0974-5645

# Reputation based Proposed Scheme to Ensure Reliable Decision by Fusion Centre

**Rohini Lohia and Isha Batra**

Department of Computer Science and Engineering, Lovely Professional University Jalandhar, Punjab, India; rohinilohia@yahoo.in, isha.17451@lpu.co.in

## Abstract

**Objectives:** Dynamic spectrum access is the promising feature of Cognitive Radio (CR). When Spectrum sensing is executed in a cooperative manner, shadowing and fading get reduced. Therefore, it gives an invitation to security threats. **Methods/Statistical Analysis:** This paper elaborates various security hazards in cognitive radio networks (CRN) along with their countermeasures. The paper elucidates the complication of Spectrum Sensing Data Falsification (SSDF) attack. The Primary objective of SSDF attack is to devastate the judgement of Fusion Centre (FC). With the aim to mitigate the influence of adversaries on the judgement given by FC, this paper proposes a scheme based on reputation and trust of cognitive users. **Findings:** Proposed scheme works on a well-defined strategy that will annihilate the impact of malicious users. In this FC doesn't possess any knowledge about the number of adversaries and strategy of attack. In order to minimize the influence of adversary, implementation of clusters is considered to be a good idea. Cluster formation takes place according to specified criteria. Encryption on the sensing reports of valid clusters is exercised, with the aim to prevent from attacks such as eavesdropping etc. Parameters such as false positive rate and true detection rate can use to judge the performance of the proposed scheme. **Applications/Improvements:** SSDF attack is the most dangerous attack and proposed scheme not only mitigates the effect of SSDF attack but also stands strong against other dangerous attacks such as eavesdropping attack.

**Keywords:** Cognitive Radio (CR), Cooperative Spectrum Sensing, Reputation, Sensing Data Falsification (SSDF), Spectrum

## 1. Introduction

WSN is the most pre-eminent field of networks. Technology of wireless communication is developing expeditiously. This emerging trend has lead to the improvement and development of the particular technology. The major problem faced during the development and improvement of this concept is the restriction of scanty spectrum resources. According to reports demonstrated by the FCC (Federal Communication Commission) meagreness of the spectrum is basically due to inefficacious use of spectrum resources[1].To solve this problem of spectrum scarcity a new concept came into limelight, which is popularly known as CR. Concept of CR is proposed to resolve the hurdle of deficiency of unlicensed bands( 5GHz and 2.5 GHz )[2]. There are two types of spectrum bands: licensed bands and unlicensed bands, so according to the reports of FCC, these unlicensed bands are overpopulated and cram-full and these licensed bands are not properly utilized. A survey conducted by FCC concludes that designated spectrum is not utilized smoothly by the licensed users and thus it has permitted unlicensed users or cognitive users to fill in the gaps[3].

CR is one of the most germane concepts of WSN. It provides a very trustworthy and dedicated communication and also enhances the efficiency of the spectrum resources. As we know that there are two types of users, licensed(primary ) users who are having the license to communicate in a predefined range of spectrum, on the other hand unlicensed (cognitive)users, "substitute the slots" by exploiting unexploited(unused) spectrum bands. In CRN, the spectrum is approached by

* *Author for correspondence*

cognitive users through overlay; opportunistic way and underlay with the aim to curtail the interference to the licensed users[4]. These two categories of users augment each other with an aim to issue paramount exploitation of spectrum. The authoritative difference between WSN and CRN is that the nodes present in CRN switches their reception and transmission parameters with respect to the radio environment.

Spectrum sensing is one of the dominant functions performed by cognitive users. During spectrum sensing, each cognitive user senses a particular licensed band with an aim to encounter the existence of licensed user. Once it has detected the existence of licensed user it will immediately evacuate the band to circumvent interference with authorized users. There are multifarious techniques of spectrum sensing such as Non-Cooperative Spectrum Sensing, Co-operative Spectrum Sensing, Interference based Spectrum Sensing and MIMO based Spectrum Sensing. But out of all these four techniques, Co-operative spectrum Sensing is considered to be robust. When spectrum sensing is performed by individual entity it usually suffers from shadowing and multipath fading effects. In order to mitigate these effects, co-operative spectrum sensing is considered to be prominent option[3]. In case of cooperative spectrum sensing, FC or base station is the judge. FC is the one that will perform integration of all sensing reports and deliver the final judgement regarding the occupancy or vacation of licensed users. As we know that a coin has two sides head and tail, similarly Cooperative spectrum sensing has both advantages and disadvantages. Where on side it provides a reliable judgement on the other side it invites time delay, auxiliary energy consumption and most important security threats[5].

The most vigorous and open facet of CRN is that CRs are pregnable to multifarious malevolent attacks. Securing CRN is considered to be most commanding and onerous task. The reason behind this is that while dealing with these types of attacks, attacks of traditional WSN are also taken into consideration[2]. Conventional attacks include spoofing, denial of service, eavesdropping etc. Whereas threats specific to CRN incorporates SSDF attack, Primary User Emulation (PUE) attack, hardware attacks, CR software attack, Spectrum Sensing Data attacks, Cryptographic based attacks, Sybil attack, Newbie attack etc. Next section deals with the study of various attacks that are specific to CRN.

## 2. Security Attacks and Counter Measures

CRN hold some exclusive features, as a result it is pregnable to multifarious security threats in addition to conventional attacks of the WSN. This particular section deals with study of various security threats in CRN and countermeasures. First part elaborates security threats in CRN and second part elaborates the countermeasures. There are many types of security threats particular to cognitive network environment. Figure 1 shows the classification of attacks in CRN.

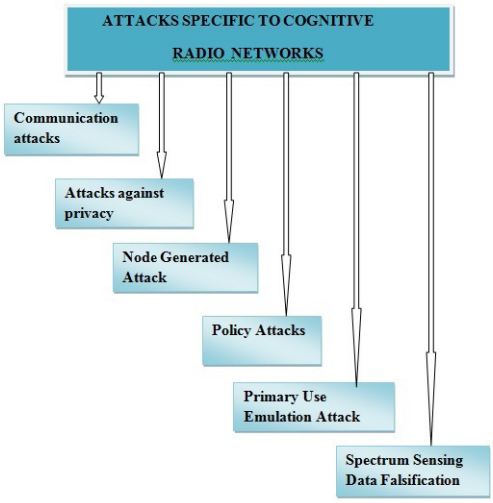


**Figure 1.** Classification of Attacks in CRN.

### 2.1 Security Threats in CRN

#### *2.1.1 Communication Attacks*

In this particular attack, primary aim of the adversary is to devastate communication between two or more parties .Attacks that come under this type of attacks are, Denial of Service (DoS) attack, Replay attack and Sybil attack[6]. Denial of service (DoS) is defined as the attack, where resources are not available to the desired users. Replay attack is defined as an attack in which communication between two parties is replayed or delayed by malevolent user. Here message is being forwarded to the node other than the desired recipient. Then comes the last and most important, Sybil attack, in which multiple identities are adopted by malevolent user. Basically this particular type of attack is efficacious against reputation systems, voting, routing algorithms etc.

### *2.1.2 Attacks against privacy*

In CRN resources are being shared to initiate the communication between two parties and to be well informed about the environment[7]. Malevolent users would utilize this access to shared resources with an aim to steal nodes information. Basically two types of attacks come under this category, eavesdropping attack and impersonating attacks. Eavesdropping attack is the one in which malevolent user peacefully hearken the communication between two parties with the aim to steal some meaningful information and launching a particular attack. Whereas talking about impersonating attack, malevolent user tries to mimic admissible cognitive user, with an aim to initiate communication with other admissible nodes.

### *2.1.3 Node Generated Attacks*

Node generated attacks are of utmost importance in CR environment because distribution of information is the dominant factor in the accurate working of CRN[8]. As the name indicates in this particular attack, nodes are targeted by the malevolent users. It happens that in this attack malevolent user crash the cognitive node. As a result not only node gets destroyed but the entire network is affected. Sometimes a node is abducted and reverse engineering approach is applied by the adversary and this may give invitation to various security threats. In simple words, this node will now act as device that will invite various security threats.

### *2.1.4 Policy Attack*

Each of the privacy and security policies are based on the principles of working, so policy attacks in CRN can be categorised as, excuse attack and newbie picking attack[5]. In case of excuse attack, according to the policy of network, if it will be magnanimous towards the recovery of the wrecked nodes, and also at the same time does not require them to prove that they are preserving their quota, then the malevolent user will exploit the particular attack by continually professing to be wrecked and vandalized. Next comes, Newbie picking attack in which if any of the newly created nodes is having the desire to share resources, then according to the policy it will have to pay the charges in terms of information for a particular time span. Then only that particular node will be criterion from newbie to another node and thus leeching the information by not granting any return of information.

### *2.1.5 PUE Attack*

Primary User Emulation Attack is most commonly known as PUE attack. Basically this attack is a kind of masquerading attack in which malevolent user tries to behave like a authenticated and legal entity by emanating a signal which is analogous to the signal emanated by licensed user[9].

### *2.1.6 SSDF Attack-*

Spectrum Sensing Data Falsification Attack is commonly known as SSDF attack or Byzantine Failure Attack. In this type of attack whole procedure is performed by fusion process and FC is the leading entity. The main objective of adversaries in this type of attack is to corrupt the judgement of FC. In simple words, malevolent users deliver false sensing reports at the FC with an aim to invalidate the decision delivered by the FC. Thus due to the introduction of false reports at the FC, false judgement is delivered by the FC about the existence or vacation of licensed user[7]. Particular attack is considered to be the most dangerous attack in CRN.

## 2.2 Counter measures

As we have seen from the previous section that there are multifarious security threats in CRN, in addition to the attacks from conventional WSN. So it is of utmost importance to find countermeasures to these attacks. Many countermeasures are introduced to mitigate the effect of these killer attacks. Countermeasures can be listed as: based on behaviour, data mining approaches, based on geolocation, based on trust and reputation of the node. In this particular section we will discuss in brief about countermeasures based on behaviour, geolocation and trust and reputation.

### *2.2.1 Based on Geolocation*

As we know that the primary function of CR is to operate radio spectrum in situations where base stations are not being utilized properly. Accordingly, first simulated and real scenarios were considered to be static in nature in which base stations are playing the role of licensed user devices of cognitive users[10]. In this case when malevolent user mimics the licensed user, geolocation is taken as appropriate method. This approach works under certain assumptions only. This approach is not well utilized in CRN. In case of WSN also, nodes and adversaries can

switch their position according to their wish. As a result adversaries are not able to be detected by this scheme. The major disadvantage of node mobility from the viewpoint of security is that if we want to locate the position of licensed user then we have to continuously perform spectrum sensing with the aim to trace new locations[5]. Further this continuous spectrum sensing will lead to very high battery consumption of the nodes. Also if licensed user is located in spatial location, its location is taken as irrelevant from security point of view.

### *2.2.2 Based on Behaviour*

As the name indicates "behaviour" this countermeasure is used analyse the behaviour of each individual node. Based on this analyses adversaries are distinguished from the normal or legitimate users[14]. Algorithms that are used to analyse the behaviour of each individual node are self organizing or genetic algorithms. The main objective of these algorithms is to analyse the patterns of their behaviour. The two main factors that should be taken into consideration while discussing about these algorithms are, battery of each individual node and computational cost. At last it can be concluded that this countermeasure is a good option to alleviate against the attack.

### *2.2.3 Reputation and Trust Based Approach*

Basically reputation is the characteristic of each and every node. The advantage of reputation is derived from the trait of WSN i.e., adaption and redundancy. Redundancy is that particular characteristic which is used to identify malevolent users. These reputations are basically used to indicate that whether licensed and cognitive users are behaving as expected. Versatility is considered to be the big advantage of this particular process[5]. This countermeasure is explained in detail in the next section.

## 3. Spectrum Sensing Data Falsification Attack

From the previous section, we have seen that there are many killer security threats that aim to destroy the functionality of CRN. In this particular section, we will discuss in detail about SSDF Attack or Byzantine attack and will discuss in detail about Reputation based approach.

Spectrum Sensing Data Falsification Attack is commonly known as SSDF attack or Byzantine Failure Attack. In this type of attack, whole procedure is performed by fusion process and FC is the leading entity. The main objective of adversaries in this type of attack is to corrupt the judgement of FC. In simple words, malevolent users deliver false sensing reports at the FC with an aim to invalidate the decision delivered by the FC. Thus due to the introduction of false reports at the FC, false judgement is delivered by the FC about the existence or vacation of licensed user[11]. The particular attack is considered to be the most dangerous attack in CRN. Here the adversary has the mindset that firstly, it should produce a very serious and dangerous attack and secondly, to protect itself from being detected.

Next, we will discuss modelling of SSDF attack. Basically, modelling of SSDF attack can be clustered in two categories, hard SSDF attack and soft SSDF attack[12]. In the case of hard SSDF attack, malevolent users vitiate their local binary decision whereas in case of soft SSDF attack malevolent users vitiate their received energy values. But soft SSDF attack is considered to be more dangerous and harmful as compare to hard SSDF attack. The reason behind this is that some adversaries prefer to falsify the energy values because of its value space instead of binary decisions.

- Always Yes SSDF attack-In case of Always Yes attack, the same result is always delivered by the adversary. Here local observations are increased by the adversary by introducing a positive offset in each sensing slot. In simple words, in this particular attack an adversary always predicts the existence of primary signal and status of channel is indicated as busy.
- Always No SSDF attack - In the case of Always No SSDF attack local observations are decreased by introducing a negative offset in each slot. In simple words, in this particular attack, an adversary always predicts that licensed user is absent or channel is free to use. As a result of this interference is caused by licensed and unlicensed user.
- Always Adverse attack-In the case of Always Adverse attack, binary hypothesis testing is performed by the adversary. H0 indicates non existence of licensed user and H1 indicates the existence of licensed user. After that observations are increased by malevolent users when hypothesis is H0 and are decreased when hypothesis is H1.

As SSDF attack is taken as the most dangerous attack in CRN, so it is very important to alleviate the influence of attack. Basically there are various approaches that are used to alleviate the influence of SSDF attack so that reliable decision is given by the FC. Reputation based Approach, Artificial intelligence approach and data mining approach are some of the approaches that are used to mitigate the effect of malevolent users in the fusion process[13]. In this paper, we will discuss only reputation and trust based approach.

## 3.1 Reputation and Trust Based Approach

Reputation and trust based approach is considered to be genuine and trustworthy approach against SSDF attack. Each user is assigned a particular reputation value on the grounds of which malevolent users are identified by the FC. FC maintains the reputation database of each and every node. Threshold factor is taken as comparison factor. Nodes which are having low reputation than a pre-initialized threshold, is tagged as malevolent user (adversary).

Basic architecture of reputation and trust based approach describes three cardinal steps which are executed sequentially in each sensing round at the fusion centre[14]. Figure 2 shows basic architecture of reputation and trust based approach.

### *3.1.1 Filtering*

In this particular step malevolent users are identified by comparing reputation with a pre-initialized threshold. Nodes which are having low reputations are filtered out from the decision process i.e., their reports will not be incorporated into the decision process and only the reports of legitimate users are incorporated into the decision process.

### *3.1.2* Data Fusion

In this particular step, fusion rules are executed on the sensing reports of legitimate users(selected from the previous step).Basically there are three types of fusion rules, AND rule, OR rule and MAJORITY rule. Out of them Majority rule is considered to be more robust and reliable. After the execution of these rules final judgement is delivered about the existence or vacation of licensed user.

### *3.1.3 Update*

As the name indicates in this particular phase reputation or trust value of each user is updated. Update phase is performed by comparing the final judgement with the individual decision. If that matches with the individual one node gets positive score otherwise it gets negative score.

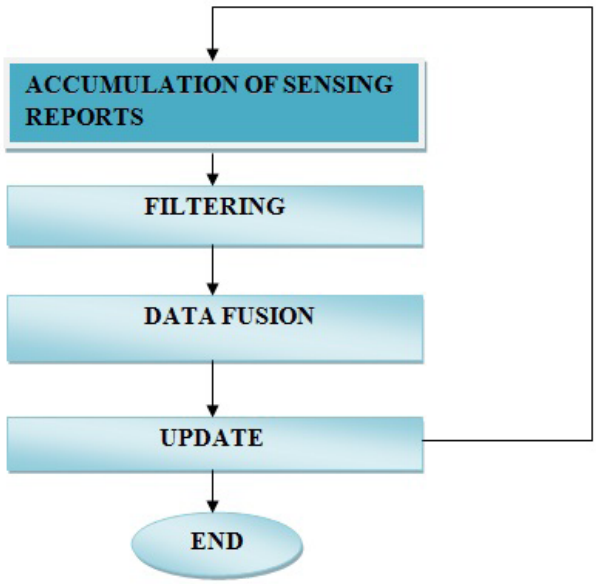


**Figure 2.** Basic Architecture of Reputation and Trust Based Approach.

# 4. Proposed Scheme

This section discusses about the scheme with primary objective to mitigate SSDF attack or byzantine attack. As we know that SSDF attack is the attack in which malevolent users manoeuvre the judgement of FC, hence giving a wrong impression about the status of primary user. Proposed scheme is based on decision based approach to mitigate the effect of adversaries on judgement delivered by FC. In this FC doesn't possess any knowledge about the number of adversaries and strategy of attack. In order to minimize the influence of adversary, implementation of clusters is considered to be good idea[1,13]. Cluster formation takes place according to specified criteria. The benefit of cluster formation is that nodes with certain similar attributes should be in one cluster. Each individual cluster will give single vote. And final judgement is given

by FC on the basis of majority voting. The intention behind cluster formation is that adversaries and normal users will be present in different clusters because of the variation in attributes of adversaries and normal users taken into consideration.

Here concept of reputation is used. Each node is having reputation value that is inversely related (proportional) to the distance between node and median of particular cluster. That is larger the distance lower is the reputation and vice versa. In the same way, voting weight of each node present in cluster is inversely related (proportional) to the distance between node and median.

The proposed scheme basically consists of six phases that are performed in each sensing round. First is the report collection phase, second is clustering phase, third is voting phase which further depends on intra cluster voting and inter-cluster voting, fourth is encryption phase, fifth is Decryption and Final judgement phase and sixth phase is Reputation refinement phase. Figure 3 shows the flowchart of proposed scheme. Details of these phases are given below:-

## 4.1 Report Collection Phase

This is the phase during which FC gathers sensing reports from all the CRU. This phase acts as a ground for the further phases, as all other phases would start only after the exit of this phase.

Clustering Phase-As the name indicates clustering, during this phase cluster formation takes place. Clustering is considered as a tremendous method used for the identification of adversaries. Two very popular techniques that are used for clustering are K-medoid and K-means[13]. In case of K-medoid cluster formation takes place using medoid. Medoid is highly representative node of the group. In simple words, medoid is that node in a cluster that possesses minimum dissimilarity with remaining nodes. In K-means cluster is introduced using centroid. In this particular approach nodes are clustered to reduce sum of squared Euclidean distance. Proposed scheme executes clustering using both K-means and K-medoid techniques. Attributes that will be considered for clustering are distance between the nodes and sensing history of nodes.

## 4.2 Voting phase

This particular phase further splits into intra cluster voting and inter cluster voting. In case of intra cluster voting each individual cluster will cast a vote and deliver its decision to the FC. Response of each node is weighted using influence factor. Basically influence factor depends upon two factors, first is distance between median and node, and second is energy of node. At last cluster decision is evaluated using influence factor and sensing report of all nodes that are present in the particular cluster. In case of intercluster voting, validity of clusters will be scrutinized. If magnitude of average of reputation of all CU in a cluster is less than the threshold, that cluster is considered as invalid cluster and is named as adversaries.

## 4.2 Encryption

After the selection of valid clusters, the next step is to perform encryption on the sensing reports of valid clusters, with the aim to prevent from attacks such as eavesdropping etc.

## 4.3 Decryption and Final Judgement

After receiving the encrypted reports FC will decrypt them and applies fusion rules on the received reports and at last delivers the final judgement regarding the absence or presence of primary user.

## 4.4 Reputation Refinement Phase

This phase is also known as update phase. In this phase reputation value of each individual node is refined. Based on these refined values, new cluster formation takes place in the next sensing round. After the declaration of final judgement, it is broadcasted to the entire CU. Then the final judgement is compared with the decision of cluster and individual node. This process of comparison is performed in two stages, firstly final judgement of FC is matched with cluster and if that matches, cluster will gain positive score and if not will score negative score. Secondly, cluster decision is matched with decision individual node and if it matches node will gain positive score otherwise negative.

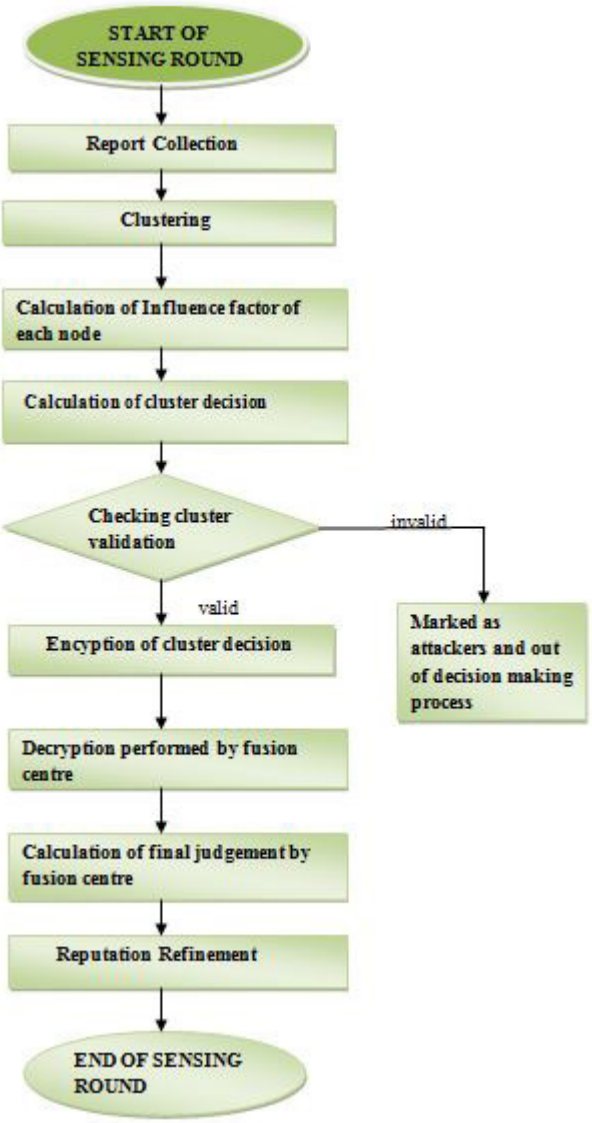


**Figure 3.** Flowchart of Proposed Scheme.

## 5. Conclusion

CR is one of the most germane concepts of WSN. It provides a very trustworthy and dedicated communication and also enhances the efficiency of spectrum resources. Spectrum sensing is one of the dominant functions performed by cognitive users. Co-operative spectrum Sensing is considered to be robust and trustworthy spectrum sensing technique. CRN hold some exclusive features, as a result, it is pregnable to multifarious security threats in addition to conventional attacks of the WSN. SSDF attack is considered to be a hazardous attack with foremost objective to manipulate the judgement of FC. Out of all the countermeasures, Reputation and trust based approach is believed to be robust in providing reliable judgement. Reputation value of individual nodes are updated which are further considered as a basis of cluster formation in next sensing round. The performance of proposed scheme can be analysed using a number of CU and magnitude of probability of false alarm and detection.

## 6. References


1. Li J, Feng Z, Wei Z, Feng Z, Zhang P. Security management based on trust determination in cognitive radio networks, EURASIP Journal on Advances in Processing,2014;(48),pp.1-16.
2. Idoudi H, Daimi K, Saed M. Security Challenges in Cognitive Radio Networks, Proceedings of the World Congress on Engineering ,2014;1,pp.1-7.
3. Xiao H, Yang K, Wang X, Shao H, Laboratories B, Hill M. A Robust MDP Approach to Secure Power Control in Cognitive Radio Networks, IEEE International Conference on Communication, China, 2012; pp.4642-47.
4. Althunibat S, Denise B J, Granelli F. A Punishment Policy for Spectrum Sensing Data Falsification Attackers in Cognitive Radio Networks, IEEE 80th Conference on vehicle Technology, Vancouver, Canada, 2014; pp.1-5
5. Araujo A, Blesa J, Romero E, Villanueva D. Security in cognitive wireless sensor networks , Challenges and open problems, EURASIP Journal on Wireless Communications and Networking,2012;(48), pp.1-8.
6. Chen C, Cheng H, Yao Y. Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack, IEEE Transactions on Wireless Communications, 2011;10(7),pp.2135-41.
7. Department of Electrical Engineering Indian Institute of Technology. https://www.ee.iitb.ac.in/web .Date Accessed: 2016.
8. Zhang L, Wu Q, Ding G, Feng S, Wang J. Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing, EURASIP Journal on Advances in Signal Processing ,2014;(81),pp.1–9.
9. Hyder C S, Grebur B, Xiao L, Member S, Ellison M. ARC : Adaptive Reputation based Clustering Against Spectrum Sensing Data Falsification Attacks, IEEE Transactions on Mobile Computing, 2014;13(8),pp.1707–19.
10. Pous H R, Blasco M J, Garrigues C. Review of Robust Cooperative Spectrum Sensing Techniques for Cognitive Radio Networks, Wireless Personal Communication , 2011;67(2),pp. 175–98.
11. Luhach A K, Luhach R. Research and Implementation of Security Framework for Small and Medium Sized E-Commerce Based on SOA, Journal of Theoretical and Applied Information Technology, 2015,82(3),pp.395-400.
12. Luhach A K, Dwivedi S ,Jha C K. Applying SOA to an

E-Commerce System and Designing a Logical Security Framework for Small and Medium Sized E-Commerce Based on SOA, In Computational Intelligence and Computing Research , IEEE International Conference on India, 2014; Dec, pp. 1-6.

13. Kumar A, Luhach A K, Pal D. Robust Digital Image Watermarking Technique using Image Normalization and Discrete Cosine Transformation, International Journal of Computer Applications, 2013;65(18),pp.5-13.
14. Malik A, Pandey B. Performance Analysis of Various Data Collection Schemes used in VANET, Indian Journal of Science and Technology, 2015;8(15),pp.1-8.