International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Malicious User Detection in Cognitive Radio Networks

Jithesh M[1], Harish Kumar C H[2]

[1]M. Tech Student, Department of ECE, MES College of Engineering, Kuttippuram, India

[2]Assistant Professor, Department of ECE MES College of Engineering, Kuttippuram, India

Abstract: ***The issue of spectrum underutilization in wire-less communication can be solved in a better way using Cognitive radio (CR) technology. Since cognitive radio networks (CRNs) are basically wireless networks, they inherit most of the well known security threats of wireless systems. Cooperative spectrum sensing is vulnerable to security attacks from malicious users. FastProbe algorithm efficiently detects the malicious users present in the system. If a malicious user exist in CR network, the entire operation of the network gets disturbed and to preclude such malicious behavior, some security solutions must be needed. In this paper, malicious users in CRNs are detected and then defends such behavior. Security solutions are presented which are used in furnishing a secure and reliable communication in cognitive radio networks. Elliptic Curve Cryptography (ECC) is used for the security in the CR network. ECC key sizes are shorter when comparable to RSA keys, the length of the public key and private key is much shorter in elliptic curve cryptosystems. This results into faster processing times, and lower demands on memory and bandwidth.***

Keywords: Cognitive radio networks (CRNs), Elliptic curve cryptography(ECC), Malicious users (MUs), Primary User Emulation (PUE), Secondary User (SU).

1. Introduction

The wide growth of wireless communications leads to the scarcity of frequency spectra and available radio spectrum is a limited natural resource, being congested day by day. Cognitive radio is a technique where secondary user looks for a free band to use when primary user is not in use of its licensed band. it is possible through spectrum sensing[1] and three types spectrum sensing are co-operative sensing, interference based sensing, and non cooperative sensing. The unoccupied frequency bands are called white space or spectrum holes. cognitive network is sensitive to security threats. The attackers may be external users or secondary users act as a malicious users. So, in order to overcome these issues, malicious user detection system is used. Cooperative sensing improves sensing accuracy but at the same time makes the system more susceptible to malicious users that may be present in the system. In cooperative spectrum sensing (CSS), multiple secondary users (SUs) cooperate to effectively detect a primary user (PU), However, the cooperation among SUs raises 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 influence the spectrum sensing decision taken by the fusion centre. The falsification of data may occur either by malfunctioning of SUs or by intentional manipulation of data by certain SUs, called malicious users (MUs). The data reported by malfunctioning SUs may differ from the actual data. In addition, MUs can attack by manipulating the reported data with selfish intention, i.e., to gain access to the channel, or to cause interference to PU. The security problems will occur in a cognitive radio environment are different ways. They are,

- False detection or sensing and misdetection of primary signal may happen due to denial of service or malicious user pretends as the primary signal.
- A malicious user could prevent the cognitive user from using available spectrum.
- A malicious user could access the data in a unauthorized way or modify/inject the false data.
- Environment could be controlled by a malicious user.

In cognitive radio network, packet sent from source node(S) to destination node(D),which maintains some security principles, ie Confidentiality(C), Integrity (I), Availability (Av), Authenticity (Au) and Non-Repudiation (NR).This kind of behavior is called normal behavior of node. When a node violate any of the security principles, Such types of nodes are usually called malicious nodes. They exhibit one or more of the following behaviour.

- Message Tampering- A malicious node can tamper the content of the packets.
- Link Break- This can result in restricting the two legitimate nodes from communicating if the malicious node is between them.
- Denying from Sending Message- Any malicious node may deny from sending messages to other legitimate nodes present in the cognitive radio system.
- Packet Drop- Simply consumes or drops the packet and does not forward it.
- Battery Drained- A malicious node can waste the battery by performing unnecessarily operations.
- Bandwidth Consumption- Whenever a malicious node consumes the bandwidth so that no other legitimate node can use it.
- Malicious Node Entering- A malicious node can enter in the network without authentication.
- Delay- Any malicious node can purposely delay the packet forward to it.

2. Related Work

Many centralized approaches have been proposed to detect malicious users and a hierarchical structure detection scheme was proposed in [2]. Secondary users are grouped into cells and multiple low level cells are grouped into a

high level cell. Each user computes an average value of its received reports. The average value is compared to a threshold, and then it is flagged as a low-outlier or high-outlier, to determine if the PU signal is active. P. Kaligineedi is proposed a scheme for secure cooperative spectrum sensing [3]. This scheme assumes a somehow simplified attack strategy, i.e., attackers launch only always yes or always no attacks. T. Zhao and Y. Zhao proposed a cooperative technique to detect PU under malicious users suppression [4]. Local decisions rather than detected energy are fused for global decision. Weighted combination is used in fusion center and weighted coefficients are updated recursively. The complexity of the scheme is low because the calculation of mean and standard deviation is avoided.A. Min, K. Shin, and X. Hu are used shadow-fading correlation-based filters to minimize the effect of abnormal sensing reports in detecting digital TV Pus[5]. P. Kaligineedi, M. Khabbazian, and V. Bhargava, proposed three schemes to detect malicious users based on outlier detection techniques. These schemes require some knowledge of the malicious user, e.g., the maximum number of malicious users[6]. This is one of the scheme to detect the malicious users present in the cognitive radio system. F. Liu, X. Cheng, and D. Chen are proposed a simple majority vote scheme to identify malicious sensors. The scheme uses 1/0 decision and if more than half of the votes consider that one sensor is malicious, then this sensor is deemed as an outlier. This scheme, does not work in some scenarios, especially when the number of participating sensors is small[7]. Q. Yan, M. Li, T. Jiang, W. Lou, and Y. Hou are proposed that each pair of SUs share a symmetric key. The sensing report includes time stamp, user ID, and the received signal strength. Before combining other sensing reports, SU does a validation to exclude the sensing reports that are sent from attackers. In this paper, the attackers are considered as outside attackers which are not authenticated by or associated with the network. Therefore, even traditional pre-shared key mechanisms can easily point out the outside attacker[8]. C. S. Hyder, B. Grebur, and L. Xiao are proposed a centralized adaptive reputation based clustering algorithm to defend against both independent and collaborative SSDF attack. However, the authors did not specify how the cluster would be updated; after updating the cluster, how to set the new reputation for each updated cluster; how to set the threshold for reputation, etc. Also, if a whole cluster is deemed as malicious, the false positive rate (some SUs treated as malicious ones) is expected to be quite high. DoS attack is one of the most serious threats in cognitive radio networks[9]. The jamming attack is one of DoS attacks that are simple to launch, and difficult to be counter measured.

3. Fastprobe: Malicious User Detection

FastProbe can be used to find the malicious user present in the cognitive radio networks. Cognitive radio conducts various sensing tests by using the sensing server and neighbor node is tested by transmitting primary user emulation (PUE) signals. On the basis of the received signal strength report obtained from the node being tested, it is possible to estimate whether this node is malicious or not. The tests can be actively delivered to nodes before the actual sensing needs to be done, allowing FastProbe [10] to proactively detect malicious users.

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

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

In this CR Networks, multiple secondary users are associated with secondary user base station (SBS) and this node is considered as master node in cognitive radio network. Control messages from SBS to secondary users and from secondary users to SBS are transmitted through the network. Assume that neighbouring cognitive radios have similar readings. If the reading is different for a Secondary User (SU), then it is called malicious user. Secondary user emulates primary user (PU) transmissions and malicious user cannot distinguish if a neighboring SU or a real primary user is transmitting. SBS also maintains reputation value for every secondary users present in the cognitive radio network. Intially,reputation value is equal to the expected probability of a node being malicious. Once the reputation value of a SU drops below a certain threshold (ω),then the node is considered as malicious node. After the execution of Fastprobe algorithm, obtained the updated reputation value for every secondary users. In this algorithm use a term which is indicated as noise floor level, ie when there is no transmitter on a particular channel, the received power level that a SU detects is called its noise floor level (denoted by φ) and this is known to SBS. Thus, on the basis of received signal strength reports from sensing tests, it is possible for the SBS to detect malicious SUs. However, there is a possibility that a malicious SU is selected for transmitting PUE signals and it does not transmit at the specified power level in order to get other SUs labeled as malicious. In order to detect such malicious SUs, FastProbe first verifies if the testing SU transmitted at the specified power level and test transmitter algorithm verifies these factors. SBS Compute minimum length testing schedule and it computes a set of SUs to be tested. Testing schedule S contains set of tuples(n_i,n_j ,T_j ,t_1), n_j tests n_i in slot t_1 by transmitting at a power level T_j and this compute schedule. must be error free. Testing all the node may require multiple time slot. When testing is ongoing the channel C_k, It contains no space for data transmission, So minimize the length of compute schedule S. In order to detect malicious SUs, the SBS needs to maintain path loss between all pairs of neighbors. Assume that the path loss between a pair of nodes varies approximately linearly with the log of frequency, therefore using the following equation, the expected path loss P_{ij}^{e} from n_i to n_j for any frequency f can be computed.

$$P_{ij}^{e} = a_{ij} \log f + b_{ij} \quad (1)$$

The value of a_{ij} and b_{ij} is depending on the environment. In order to use the above equation, SBS computes an initial

value of a_{ij} and b_{ij}. Observe that if the receiver is malicious, it is possible that it may report incorrect signal strengths. Fastprobe have multiple time slots. Each SUs have a reputation value and this reputation value lies in a certain range. B_t indicates a set of testing nodes (n_i) and they transmit primary user emulation signals at the power level specified in compute schedule S. By using test transmitter algorithm, SBS compute probability Pi of each node based on the observed transmission power reported by node n_i. SBS computes this power by taking a weighted average of observed transmission power at secondary users. If the value of P_i is less than a threshold level, so transmission is said to be malicious. So SBS does not update the reputation value of SUs.

For finding the malicious users, first check the observed pathloss and expected pathloss. If the value of observed pathloss is different from expected pathloss, this means that noise associated with the transmission or n_j is maliciously reporting incorrect reading. If the observed pathloss is equal to expected pathloss, then the node is not a malicious one. After that process, check the expected and received power level reported by node n_j and if the power level is less than or equal to noise floor level, then the node is not a malicious user and update the reputation value of all secondary users. Otherwise it assure node is malicious.

4. Security Solution To Defend Malicious Behavior

Malicious behavior of a node is defined and to defend such behavior, security solutions are presented which are used in furnishing a secure and reliable communication in cognitive radio network. In order to defend the malicious behavior there are several security solutions which are used in the cognitive radio networks. Security can be provided through the methods of Cryptography, Protocols, Intrusion Detection System (IDS) and Trusted Third Party (TTP). In cognitive radio Network, the data is sent using cryptography [27] and the security can be provided through this method.

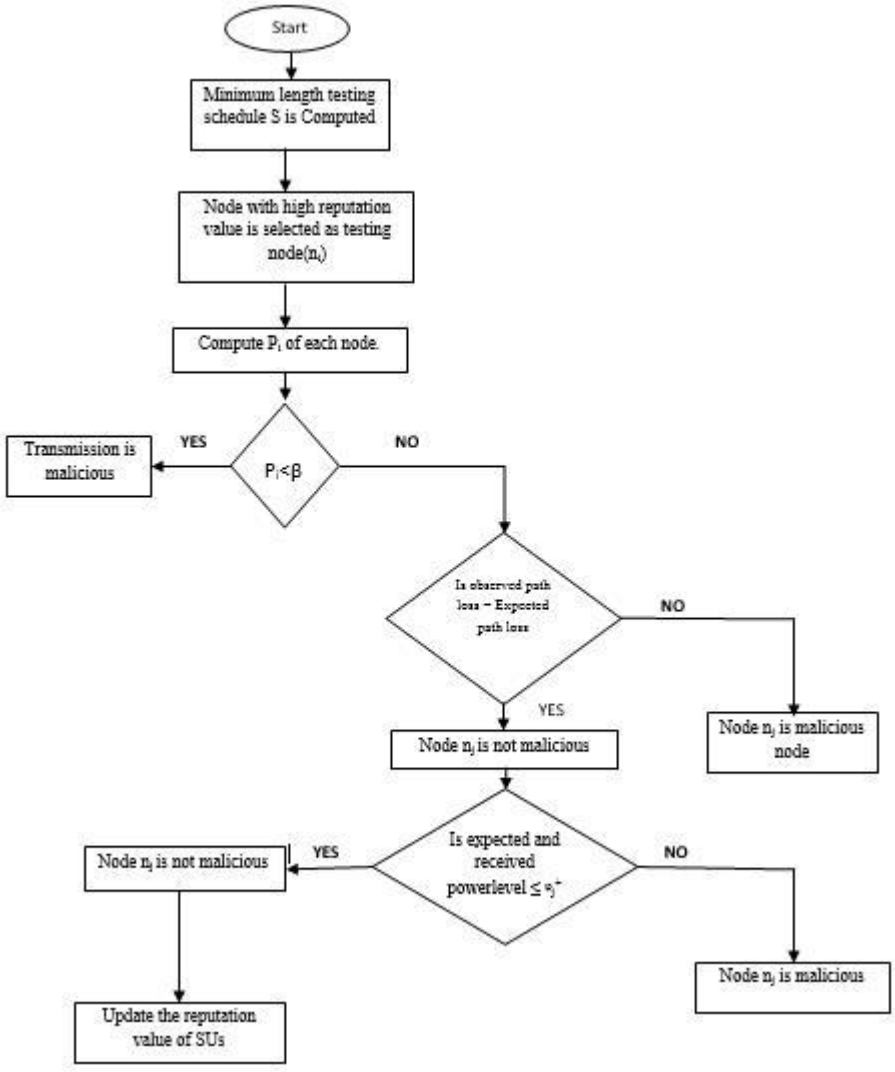

Figure 1: Flow Chart of FastProbe Algorithm.

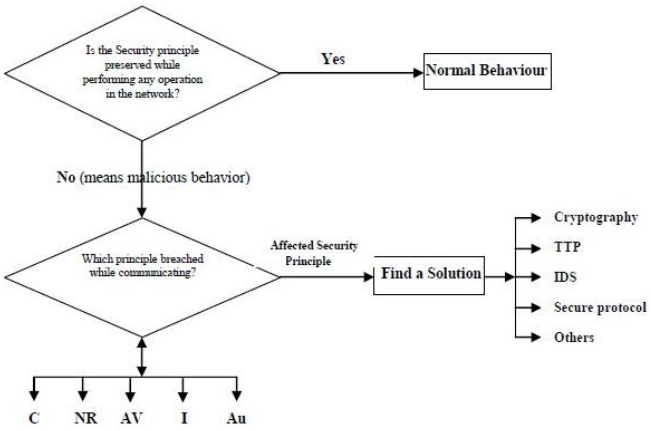

Figure 2: Various Security Solutions to defend Malicious Behavior

Cryptography means to convert (or encrypt) the original data (which is to be send) into the unreadable format. Even if the malicious user accesses the data, it should not be able to understand the content of it. Cryptography can be symmetric (which uses same key to encrypt and decrypt the data) and asymmetric (which uses one key to encrypt and other to decrypt the data). This security preserves the integrity and confidentiality of data. Techniques like Elliptic curve cryptography (ECC) and RSA are used to preserve the security principles.

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys.ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields[11]. One of the main benefits in comparison with non-ECC cryptography is that same level of security provided by keys of smaller size.

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b \qquad (2)$$

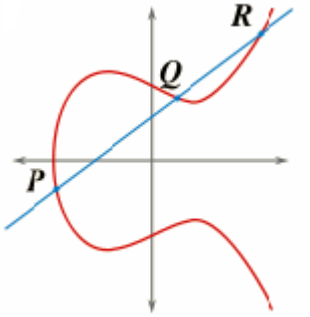

Figure 3: Simple elliptic curve

Key Generation: Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. select a number 'd' within the range of 'n'. Using the following equation we can generate the public key

$$Q = d * P \qquad (3)$$

Where d is the random number that we have selected within the range of (1 to n-1). P is the point on the curve.'Q' is the public key and 'd' is the private key.

Encryption: Let 'm' be the message that we are sending and represent this message on the curve. Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from 1 to n-1.Two cipher texts will be generated let it be C_1 and C_2.

$$C_1 = k * P \qquad (4)$$

$$C_2 = M + k * Q \qquad (5)$$

C_1 and C_2 will be send.

Decryption: Decryption is as follows, M is the original message that we have send.

$$M = C_2 – d * C_1 \qquad (6)$$

Reason for selecting ECC for providing security to the cognitive radio networks is that, the size of the key required for encryption is surely far less than other systems.A successful discovery of an attack on the cognitive radio system.

Table 1: ECC and RSA Key Comparison.(key size in bits)

ECC Key Size	RSA Key Size	Key-Size Ratio
163	1,024	1:6
256	3,072	1:12
384	7,680	1:20
512	15,360	1:30

Since the ECC key sizes are so much shorter than comparable RSA keys, the length of the public key and private key is much shorter in elliptic curve cryptosystems. This results into faster processing times, and lower demands on memory and bandwidth; some studies have found that ECC is faster than RSA for signing and decryption.ECC is particularly useful in applications where memory, bandwidth, and/or computational power is limited.

5. Simulation Results

The algorithms based on this technique collect readings from all CRs and then mark those nodes as malicious whose readings differ significantly from their neighbors. Elliptic curve cryptography (ECC) is used for the security in CR networks.

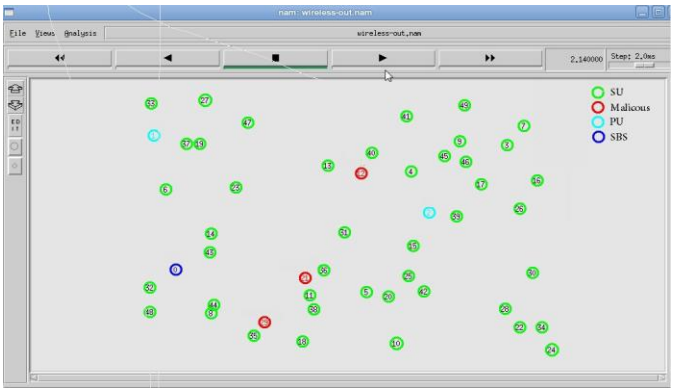

Figure 4: Detection of malicious users in cognitive radio networks

The Fig 4-7 shows the simulation results. The simulation results show the total no. of transmissions, throughput loss, and malicious user detection delay. Total transmissions deals with number of tests performed by Fastprobe over a certain period of time. Plot of total transmission contains two graph, first one indicates total transmission of Fastprobe algorithm and the second one is that adding elliptic curve cryptography to the CRNs.

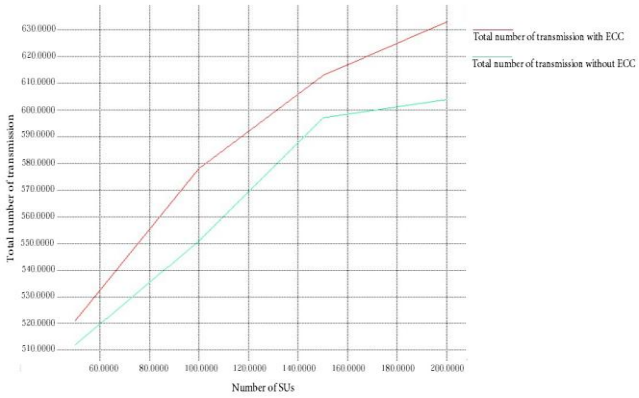

Figure 5: Total number of transmission with and without ECC

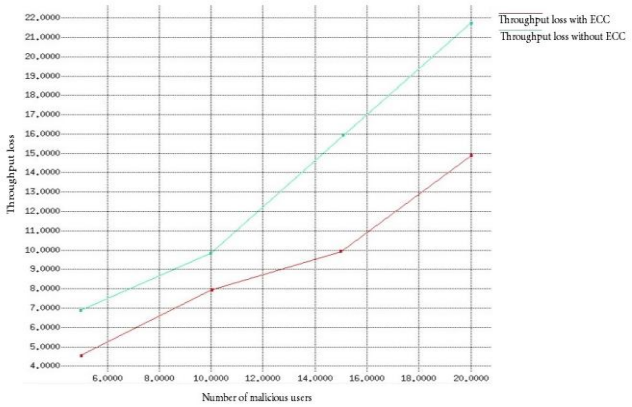

Figure 6: Throughput loss with and without ECC

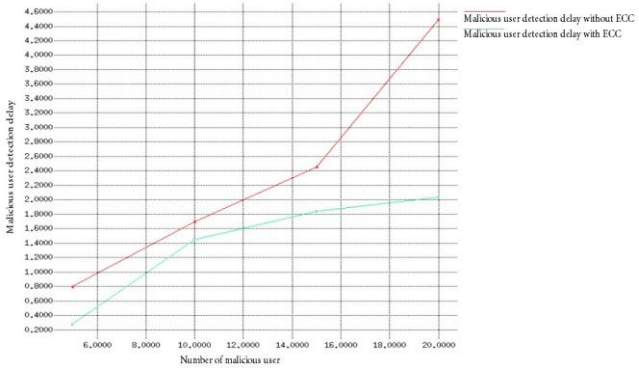

Figure 7: Malicious user detection delay with and without ECC

Throughput loss per user, which define as the average fraction of time spend by SUs as well as SBS in sensing, transmitting and receiving data related to sensing. The simulation shows that throughput loss is reduced when using the elliptic curve cryptography. In the case of malicious user detection delay, simulation result shows that detection delay is reduced when ECC is added to the CR network. Fig. 7 shows the plot of malicious user detection delay with or without ECC. Simulation is carried out in NS2.

6. Conclusion

Cognitive network is sensitive to security threats. 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. Cooperative sensing improves sensing accuracy but at the same time makes the system more susceptible to malicious users that may be present in the system. In cooperative spectrum sensing (CSS), cooperation among SUs raises concerns about reliability and security of cooperative spectrum sensing, as some of the SUs may report incorrect sensing data .All the control messages from SBS to SUs and from SUs to SBS are encrypted that can only be decrypted by the intended recipient. SBS gives a unique key to the other nodes participated in the CR network. The simulation results shows that Fastprobe with ECC reduces the throughput loss and malicious user detection delay.

References

[1] S. Mishra, A. Sahai, R. Brodersen, "Cooperative sensing among cognitive radios", in: Proc. of IEEE ICC 2006, vol. 4, 2006, pp. 1658-1663.
[2] O. Fatemieh, R. Chandra, and C. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," in Proc. 4th IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2010, pp.112.
[3] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in Proc. IEEE International Conference on Communications (ICC), 2008, pp. 3406-3410.
[4] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in Proc. IEEE International Conference on Communications (ICC), 2009, pp. 15.
[5] A. Min, K. Shin, and X. Hu, "Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation," IEEE Transactions on Mobile Computing, vol. 10, no. 10, pp. 1434-1447, 2011
[6] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," IEEE Transactions on Wireless Communications, vol. 9, no. 8, pp. 2488-2497, 2010.
[7] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in Proc. 26th IEEE International Conference on Computer Communications (INFOCOM), 2007, pp. 1937-1945.
[8] Q. Yan, M. Li, T. Jiang, W. Lou, and Y. Hou, "Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks," in Proc. 31st IEEE International Conference on Computer Communications (IN-FOCOM), 2012, pp. 900-908.
[9] C. S. Hyder, B. Grebur, and L. Xiao,"Defense against spectrum sensing data falsification attacks in cognitive radio networks," in Security and Privacy in Communication Networks. Springer, 2012, pp. 154-

171.
[10] T. Bansal, B. Chen, and P. Sinha, "Malicious User Detection in Cognitive Radio Networks Through Active Transmissions," Tech.
[11] Kiyomichi Araki, Takakazu Satoh and Shinji Miura. "Overview of Elliptic Curve Cryptography", Lecture Notes in Computer Science Vol.1431, 1998.