A Robust Collaborative Spectrum Sensing Decision against SSDF Attack in Cognitive Radio Network

Dharani D[1], Sharmila A[2]
PG Student[1], Assistant professor[2]
Dept. of ECE,CCET, Pondicherry University

Abstract-Cognitive radio is a promising technology to improve the utilization of wireless spectrum resources efficiently. A serious security threat to cognitive radio networks (CRN) which sense the spectrum in a cooperative manner is the spectrum sensing data falsification (SSDF) attack. The proposed scheme mitigates the effect of SSDF attacks and improves the robustness of cooperative spectrum sensing (CSS) based on the identity based AES cryptography. The SSDF attack is countered by two stages. In the first stage, the normal secondary users are identified using the AES encrypted ID. Following this is the second stage in which the majority voting rule is used to make correct spectrum sensing decision to all secondary users. The experimental results show the comparison of the proposed scheme with adaptive reputation based clustering algorithm. The effectiveness of proposed scheme provides efficient spectrum sharing of unused licensed spectrum to the cognitive radios and enable robust system operation.

Keywords-Cognitive radio, secure collaborative spectrum sensing, AES, Data link layer authentication, SSDF attack.

I. INTRODUCTION

In high speed wireless communications, spectrum scarcity has become a challenging issue to the emerging wireless technologies. Hence, spectrum sharing has become an important aspect in wireless communication networks due to spectrum shortage. The cognitive radio network (CRN) provides a promising solution to alleviate the spectrum shortage problem [6].CRN enables the usage of unused spectrum of licensed users (primary users) to the unlicensed users (secondary users) and provides highly reliable communication. Other adaptivity and efficiency are the key enabling functionality of CRN that has enabled extensive research in this area.

The Federal Communications Commission (FCC) mandates that the secondary users must evacuate the spectral bands when the primary transmission is detected. In CR networks, unused frequency bands (white spaces or spectrum holes) of primary user are identified through spectrum sensing, and these spectrum bands are utilized by the secondary users (also known as the cognitive radios) for data transmission. If a primary transmission signal is detected in the band that a CR operates in, then the CR must leave that band and operate in another band. The fig 1.1 shows the fallow licensed spectrum band otherwise known as spectrum holes.

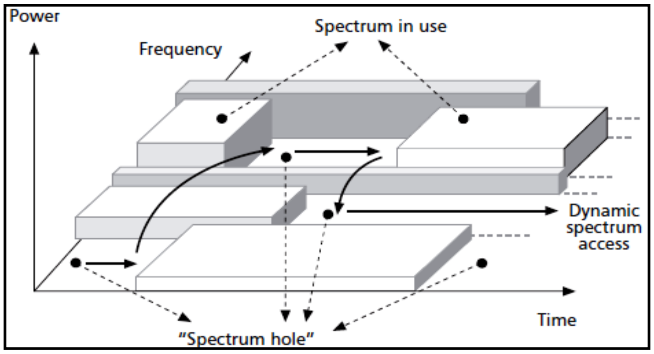

Fig 1.1 Illustration of spectrum holes

Unused spectrum band of the licensed frequency is being utilized by using IEEE 802.22 standard which is also known as Wireless Regional Area Network (WRAN) and it is the IEEE standard for cognitive radio networks. Specially, the main functions of CR technology including the spectrum sensing, spectrum management, spectrum sharing and spectrum mobility [14]. The spectrum sensing is to determine the available spectrum for secondary users (SUs) and detect the presence of primary users (PUs). The spectrum management is to select the best available channel spectrum sensing to meet users communication requirements. Spectrum sharing is to coordinate access to the channel with other users and spectrum mobility is to vacate the channel when a primary user is detected.

Security requirements play an increasingly important role in any type of networks. For CRNs, some security requirements are to be considered in general wireless networks due to SUs access the spectrum belonging to PUs in an opportunistic manner. Such security goals of confidentially, integrity and availability must be to ensure the reliable storing, transmitting and processing of information [18]. Confidentiality assures that the data is transformed unintelligible to an unauthorized entity, or otherwise ensures privacy of authorized users. Integrity is an assurance that the data received is exactly as sent by an authorized entity. Availability refers to the ability of PUs and SUs to access the spectrum.

CR network is vulnerable to malicious attacks and selfish attacks that could disrupt its operation. The two well known security threats in CR networks are incumbent emulation (IE) or primary user emulation (PUE) attack and spectrum sensing data falsification attack.

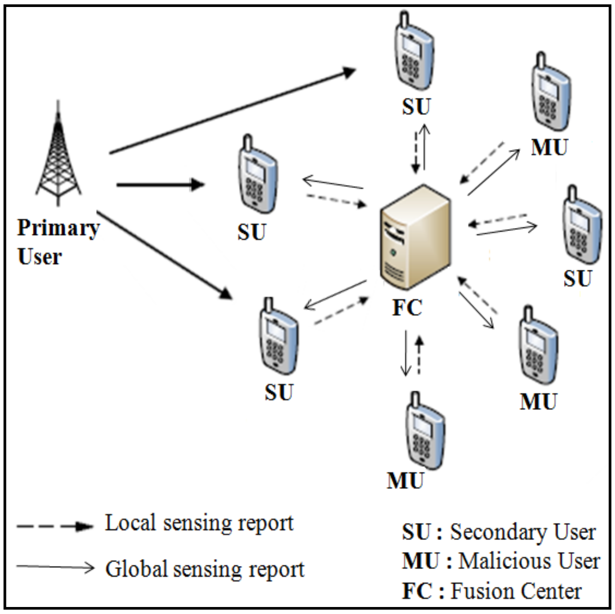

Fig 1.2 SSDF attack model in collaborative spectrum sensing

Spectrum sensing data falsification attack, also known as the Byzantine attack, takes place when an attacker sends a false local spectrum sensing result to the fusion center, thereby making a wrong spectrum-sensing decision. It causes inefficient spectrum sharing of the CRNs. Fig 1.2 shows the transmission flow of SSDF attack in collaborative spectrum sensing (CSS).This attack targets centralized as well as distributed CRNs.

In this paper, we initiate a reliable collaborative spectrum sensing decision against the spectrum sensing data falsification attack. This proposed scheme enables more robust system operation and provides efficient spectrum utilization of unused licensed spectrum band to the cognitive radios.

The rest of this paper is organized as follows. In section II, a brief review of traditional detection schemes to combat against the SSDF attack is presented. In section III, the proposed system model for SSDF attack detection based on identity based AES cryptography and secure collaborative spectrum sensing decision technique is to be discussed in detail. The simulation results and discussions of the proposed system compared with the adaptive reputation based clustering method are provided in section IV. Finally, the paper is concluded in the section V.

II. TRADITIONAL DETECTION SYSTEMS OF SSDF ATTACK

In [1] and [3], an adaptive reputation based clustering algorithm to defend against collaborative SSDF attack is detailed by a sequence of phases. Initially, the nodes in CRN are clustered based on the sensing information and initial reputation of the nodes. The final decision is decided through intra-cluster and inter-cluster voting. The results of final decision is propagated back to the clusters and then to the individual nodes for adjusting the reputation of the nodes.

In paper [2], a trusted collaborative spectrum sensing technique based on Location Reliability and Malicious Intention (LRMI) was proposed to detect the malicious user in mobile CRNs. In [4], the authors proposed the Enhanced Weighted Sequential Probability Ratio Test (EWSPRT) and Enhanced Weighted Sequential Zero/One Test (EWSZOT) techniques to defend against SSDF attack. To counter SSDF attacks in CR-MANETs (Cognitive Radio Mobile Ad-hoc Networks), a consensus-based cooperative spectrum sensing scheme was modeled in paper [5].

A weighted decision fusion algorithm based on Least Mean Square (LMS) algorithm was proposed to reduce the effect of SSDF attack in [7]. In [8], the authors proposed a scheme to counter SSDF attacks based on hard decision regardless of independent attacks or cooperative attacks and to improve the robustness of CSS. In paper [9], a secure communication by spread spectrum modulation and encryption algorithm with CR technology was presented.

In [10], density based SSDF detection (DBSD) scheme was presented to countermeasure the SSDF attack in cooperative spectrum sensing CRNs. In the paper [11], a novel trust scheme called sensing guard was proposed to counter collusive SSDF attack based on the trustworthiness of each SU in CSS environment. To mitigate the intermittent SSDF attack based on Beta Sequential Probability Ratio Test (BSPRT) in [12].

A secure cooperative spectrum sensing scheme based on identity-based and threshold cryptography in [13] was designed especially for MANET security and to recognize the occurrence of SSDF attack. The analysis of AES cryptographic techniques are to be presented in [15]-[16].

III. SSDF ATTACK DETECTION BASED ON IDENTITY BASED AES CRYPTOGRAPHY AND SECURE CSS DECISION TECHNIQUE

The SSDF attack causes the data collector to make a wrong spectrum-sensing decision and the spectrum utilization to the malicious user. It also degrades the entire performance of the fusion center decision results to cognitive radios.

In the proposed method, the defense against SSDF attack is done by two phases. Figure 2.1 shows the representation of proposed system model.

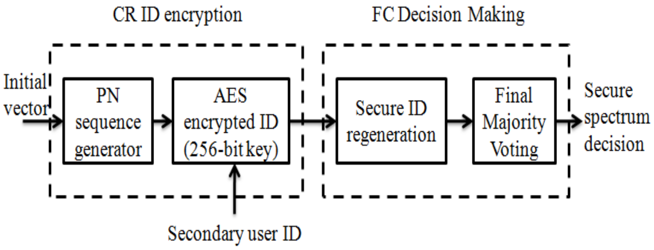

Fig 2.1 Proposed system model representation

The ID of secondary nodes is encrypted by AES algorithm along with the different sensing results of sensed spectrum in the initial phase. Then, the correct spectrum sensing decision is made based on the majority rule by the co-operation of all secondary users sensing results to the fusion center.

The secret key used for encryption is generated and distributed from a trusted third party, and it serves as an authentication center to carry out the key distribution to both CR user and fusion center. The key should be time varying, so the malicious user cannot be able to decrypt the authorized secondary user ID. Hence the fusion center can be able to easily identify the cognitive radio users and malicious users with high accuracy.

A. SUs ID encryption

In order to prevent the impersonation attack; each secondary user's ID sequence needs to be kept secret from the attackers and key should be time varying. The ID sequence is generated by using two steps: first a pseudo-random (PN) sequence is generated by using Linear Feedback Shift Register (LFSR) with a initial vector of unused primary spectrum sensing information. Then, the PN sequence is encrypted with the AES algorithm. Which uses a 256-bit secret key is used for the AES encryption. Hence it achieves maximum possible security against the malicious attackers and identifying authorized secondary users accurately.

The secure ID information is generated through a cryptographic algorithm using the shared secret key between the cognitive radios and fusion center. An AES 256-bit key is used to encrypt the ID information of each cognitive radio (secondary users) along with the identified spectrum holes by the primary users. This process is providing a more secure transmission of the spectrum hole information to the fusion center.

B. AES algorithm implementation

The Advanced Encryption Standard (AES) is a symmetric key block cipher algorithm and it is otherwise known as secret key cryptographic algorithm. It has a variable length of 128,192,256 bits and supports the block size of 128 bits in 10, 12, 14 rounds depending upon the key size.

In this paper, AES 256 bit key is used to encrypt the data blocks of 128 bits in 14 rounds. The fig 2.2 shows the general representation of AES algorithm implementation. It consists of four stages that have number of repetitions depending upon the key length of the AES encryption. The four stages are:

(1) Add Round Key

In this stage, each byte in the 4 × 4 array is to be added to the round key array using bit-wise XOR operation.

(2) Sub Bytes

In this stage, each byte in the 4 × 4 array is simply mapped to another byte based on a lookup table called S-box (Substitution or transposition box).

(3) Shift Rows

Here except the first row of an array matrix, each byte from the second row of a 4 × 4 array is shifted to left by a number of bytes.

(4) Mix Column

Each byte in a column is replaced by a combination of 4 bytes within the same column and this operation provides diffusion property.

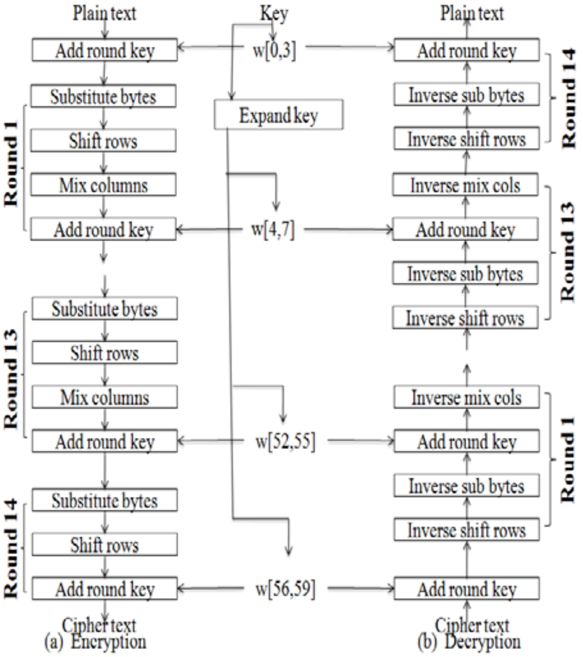

Fig 2.2 AES 256-bit key implementation process

The key should be extended based on variable length of the AES cryptography and assigned to each round of the AES 256-bit key implementation process. The AES 256-bit key encryption process has been proved to be secure under all well-known attacks and malicious users are computationally infeasible to break the 256-bit key in real time. Significantly, this approach provides accurate identification of authorized secondary users and malicious users.

C. FC Decision Making

The fusion center (FC) identifies the trusted secondary users from the attackers by recovering the ID of each secondary node with a shared 256 bit secret key. After the global decision is taken depends upon majority voting rule of local spectrum sensing results of all secondary users. According to the spectrum detection technique, the binary hypothesis test for spectrum sensing can be written as follows.

H_0: the primary user is absent (Channel is free)

H_1: the primary user is present (Channel is busy)

The authorized secondary user under SSDF attack is to be identified by the shared AES 256 bit key and the process is defined as follows.

$$I_F = \begin{cases} 1, if\ I_S = I_R \\ 0, if I_S \neq I_R \end{cases} \qquad (1)$$

HereI_F denotes the identification of trusted secondary user at the fusion center; I_S indicates the ID of individual secondary user and I_R denotes the regenerated ID of secondary user at the fusion center.From equation (1), the fusion center easily identifies the authorized secondary users and the malicious users.

The majority rule as a special case of voting rule is to be considered as a fusion decision rule can be defined as follows:

$$D = \begin{cases} H_1 = 1, if \sum_{i=1}^{N} D_i \geq \frac{N}{2} \\ H_0 = 0, if \sum_{i=1}^{N} D_i < \frac{N}{2} \end{cases} \qquad (2)$$

Here N denotes the total number of secondary users, D indicates the finalspectrum sensing decision of fusion center or global sensing result, H_0 andH_1 indicates the two binary hypotheses, and$D_i \in \{0,1\}$ represents the individual SU sensing decision result.

The special case of N/2 is referred to as a majority voting rule. When, the sum of individual SU decision more than N/2, indicates the correct spectrum sensing result of the fusion center about the presence of primary user signal to the normal secondary users (D = 1). When, the sum of individual SU decision becomes less than N/2, indicating the fusion center takes correct spectrum sensing result about the absence of primary user signal to the normal secondary users (D = 0).

Hence, this collaborative spectrum sensing decisionby fusion center makes secure spectrum sensing results to the cognitive radios. And, it is more robust under SSDF attack and provides efficient spectrum sharing to the cognitive radios.

IV. SIMULATION RESULTS AND ANALYSIS

In section V, demonstrates the performance of identity based AES cryptography detection scheme against SSDF attack in CR networks. The security in cognitive radio networks are implemented by using network simulator is mainly used to implement the protocols in the networking research.

The analyses of parametric performancesare to be designed based on the simulated environment. The detailed simulated parameters of designed simulated environment are presented in the Table 1.

TABLE 1. SIMULATED ENVIRONMENT

PARAMETERS	SETTINGS
Access Node	IEEE 802.22
Antenna type	Omni Antenna
No. of Nodes	40
Propagation model	Two ray Ground
Routing Protocol	AODV
Protocol Layer	MAC
Common Control Channel	1
Data channel	8
Network size	1000m×1000m

The performance evaluation of proposed method is compared with the conventional method by the performance metrics are detection rate, false alarm rate and throughput.

The above figure represents the detection of honest secondary user under SSDF attack in the simulation environment of cognitive radio network. It consists of 40 nodes and each cognitve radio users coverage area is 540m.

The accuracy in the detection of honest secondary users is measured by the detection rate. And set the number of malicious users as 20 in the simulation environment.

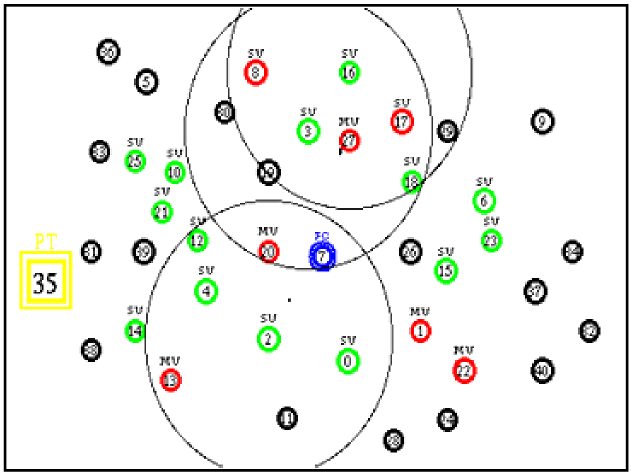

Fig 4.1: Honest SU & MU detection model

$$\text{Detection rate} = \frac{\text{Number of detected attackers}}{\text{Number of actual attackers}}$$

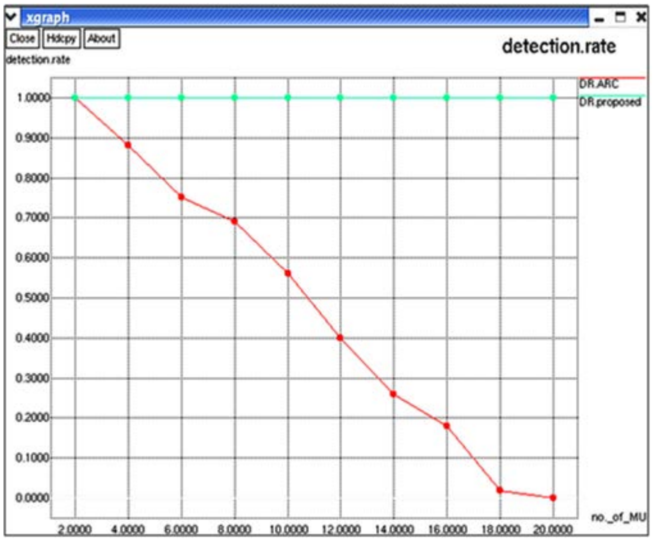

Fig 4.2 Detection rate of honest SUwith varying number of attackers

The detection accuracy of trusted SU comparison between ARC model and proposed model are illustrated in Fig 4.2. Here the proposed model achieves high detection accuracy and provides significant identification of trusted SU accurately with varying number of malicious users.

In fig 4.2, shows the comparative analysis of false alarm rate of both the proposed and existing ARC (Adaptive reputation based clustering) model.

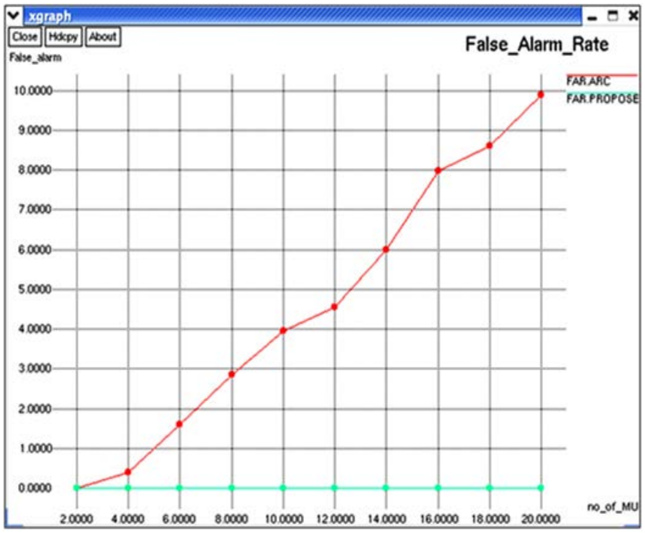

Fig 4.3 Comparison of False Alarm Rate

The evaluation of false alarm are to be measured for the purpose of measuring how many nodes are misidentified as an attacker. False alarm is to be described as the fusion center, are mistakenly identifingthe malicious users as a honest secondary user.

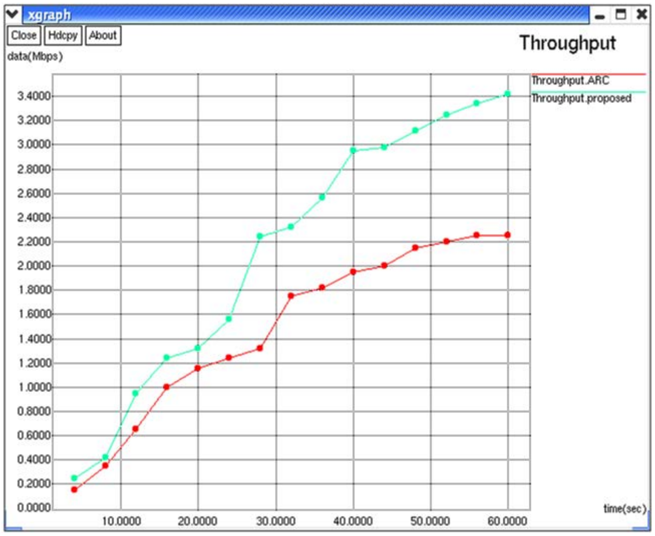

Fig 4.4 Comparison of Throughput

When compared with the existing model,the proposed model achieves zero false alarm rate under varyingnumber of malicious users. The false alarm rate (FAR)is given by,

$$\mathrm{FAR} = \frac{\text{Number of honest SU misidentified}}{\text{Number of actually identified attackers}}$$

The throughput comparison of both existing ARC and proposed scheme are evaluated in fig 4.3. Compared with ARC method, the throughput for proposed model is to be increased gradually according to corresponding time in seconds.

$$\text{Throughput} = \frac{\text{Received data}}{\text{Transmission time}}$$

From the above discussions, the proposed model achieves high detection rate accuracy than the ARC method. And produce zero false alarm rate under varyingnumber of malicious users. Therefore, the proposed method should effectively combat against SSDF attack in CRN.

V. CONCLUSION

In this paper, an identity based AES cryptography detection technique to effectively combat the SSDF attack in cognitive radio network is illustrated. The comparative analyses of proposed scheme with the existing adaptive reputation based clustering method are analyzed in the simulation results. The honest secondary users in large scale cognitive radio networks are effectively identified under number of malicious nodes. The proposed approach provides more security, very less false alarm rate and produce high detection accuracy. The effectiveness of proposed scheme enables efficient spectrum sharing of unlicensed spectrum to the secondary users and provides robust system performance to the cognitive radios.

REFERENCES

[1] Chowdhury S. Hyder, Brendan Grebur, Li Xiao and Max Ellison, “Adaptive Reputation based Clustering against Spectrum Sensing Data Falsification Attacks”, *IEEE Transactions on Mobile Computing*, Vol. 13, no. 8, pp. 1707-1719, Aug. 2014.

[2] Shraboni Jana, Kai Zeng, Wei Cheng, and PrasantMohapatra, “Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks”,*IEEE Transactions on Information Forensics and Security*, Vol. 8, no. 9, pp. 1497-1507, Sep. 2013.

[3] Li Li, Fangwei Li, Jiang Zhu ,“A Method to Defense against Cooperative SSDF Attacks in Cognitive Radio Networks”, in proc. *IEEE Symp.Commun.*,2013.

[4] Feng Zhu and Seung Woo Seo, “Enhanced Robust Cooperative Spectrum Sensing in Cognitive Radio”, Journal of Communications and Networks, vol. 11, no. 2, pp. 122-133, April 2009.

[5] F. Richard Yu, Helen Tang, Minyi Huang, Zhiqiang Li and Peter C. Mason,“Defense against Spectrum Sensing Data Falsification Attacks in Mobile Ad Hoc Networks with Cognitive Radios”, in proc *IEEE Int.Conf.Commun.*,2009.

[6] S. Haykin, “Cognitive radio: Brain-empowered wireless communications”,*IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[7] ShaahinTabatabaeeand VahidTabatabaVakili, “A New Method for Sensing Cognitive Radio Network under Malicious Attacker”, *Int. J. Communications, Network and System Sciences*, no. 6, pp. 60-65, 2013.

[8] Jianqi Lu, Ping Wei and Zhe Chen, “A Scheme to Counter SSDF Attacks based on Hard Decision in Cognitive Radio Networks”, *WSEAS Transactions on Communications*, Volume 13, pp. 242-248, 2014.

[9] SugataSanyal, RohitBhadauria,ChittabrataGhosh , "Secure Communication in Cognitive Radio Networks", *Int. Conf. on Computers and Devices for Comm.*, 2009.

[10] Changlong Chen, Min Song, ChunShengXin, "A Density Based Scheme to Countermeasure Spectrum Sensing Data Falsification Attacks in Cognitive Radio Networks", *IEEE Symp. Globecom Communication and Information System Security*, pp. 623-628, 2013.

[11] JingyuFeng, Yuqing Zhang, Guangyue Lu and Liang Zhang, "Defend against Collusive SSDF Attack using Trust in Cooperative Spectrum Sensing Environment", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1656-1661, 2013.

[12] JingyuFeng, Yuqing Zhang,Guangyue Lu, "A Soft Decision Scheme against Intermittent SSDF Attack in Cooperative Spectrum Sensing", *IEEE International Conference on Computer and Information Technology*, pp. 293-298, 2014.

[13] RashinSaboor, Ali Payandeh, and HojatolahRohi, "A Secure Cognitive Radio Ad-Hoc Network with the Capability of SSDF Attack Detection", *International Journal of Future Computer and Communication,* vol. 2, no. 6, pp. 648-653, Dec. 2013.

[14] A. Fragkiadakis, E. Tragos, I. Askoxylakis, "A survey on security threats and detectiontechniques in cognitive radio networks",*IEEE Commun.Surv.Tuts.*, vol. 15, no. 1, pp. 428–445, Mar. 2013.

[15] N. Singhal and J. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," *Int. J. Comput. Trends Technol.*, pp. 177–181, Aug. 2011.

[16] C. Sanchez-Avila and R. Sanchez-Reillo, "The Rijndael block cipher (AES proposal): A comparison with DES," in *Proc. IEEE 35th Int. Carnahan Conf. Security Technol.*, Oct. 2001, pp. 229–234.