International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 03 (May - June, 2018)

Reliable Security Scheme against Packet Dropping Attack for Cognitive Radio Network

Manorama Mishra
M. Tech. Scholar in Dept.of Electronics and Communication
Rewa Institute of Technology Rewa
manoramamishra542@gmail.com

Swatantra Tiwari
Asst.Prof. in Dept. of electronics and communication
Rewa Institute of Technology Rewa
swatantratiwari84@gmail.com

Abstract— *In CR adhoc networks there is no central controlling unit, while all the users are independent to join and leave the network at any time. The stations are mobile and also affected from attacker easily. The CRN are consisting of primary users (PUs) and Secondary Users (SUs) that are used the spectrum. The primary users are more reliable than the secondary users because these are licensed users. The objective of cognitive radio network is to sense the spectrum band and identify the free channels which will be used for opportunistic transmission attacker is detected through not forwarded the data packets to next node or destination node in network. CRN can improve the efficiency of spectrum usage, but it also introduces new security threats including internal attacks during the spectrum sensing process, which can degrade the effectiveness of spectrum sensing. In this paper we proposed security scheme against packet dropping Black hole attack. This scheme is based the reverse and forward path i.e. to proper hop count till data not reach to destination. The hop count value based on pow (Variable) function. The reliability of link is match from the forward and reverse path reliability. The variable is only check the proper packet forwarding in particular link and the reverse and forward is not identified correctly, current node are in suspicious. The record value of hop count is based on the power of variable assign at starting connection establishment procedure. The proposed IDS procedure is validating the attacker presence and also disables the attacker presence in network. The network performance provides better results in existence of security scheme and also totally renders inoperative presence of packet dropping attacker in network. The performance of proposed security scheme is compare with existing trust based scheme routing security scheme. The performance metrics are showing the better results in presence of proposed scheme and improves the network reliability.*

Keywords: - CRN, stations, Packet dropping attack, Security, Routing.

1. INTRODUCTION

Cognitive Radio Networks (CRNs) are promising wireless communications systems that can resolve the spectrum scarcity problem arising from the escalating demand of wireless radio frequency and spectrum under utilization by license holders [1]. The spectrum of particular companies has different bands for communication. In 1998, at a seminar in "Royal Institute of Technology, Stockholm", Joseph Mitola was very first researcher who used the term of CR Cognitive Radio (CR) [2]. After that, this phenomenal work published in IEEE and the author demonstrated that, CR is a particular addition to software radios and quite extra flexible than already used methods for software radios. The ultimate target of this methodology was to provide an intelligent and convenient assistance to the devices during communication. Cognitive radio networks are envisioned to alleviate the shortage of spectrum by defining more smart and flexible wireless networks that can dynamically optimize spectrum usage. The utilization of such networks is still a challenging problem that raises several open research paradigms. Securing communications in CRN is one among these open challenges. The open and dynamic feature of cognitive radio network causes cognitive radio systems to be vulnerable to various malicious attacks. In other words, the cognitive radio paradigm introduces entirely new classes of security threats and challenges. Securing wireless networks has never been an easy task. However, securing cognitive radio networks is even more complicated and challenging. This is because network security professionals have to deal with both the traditional wireless security threats and the newly added threats specific to CRNs. In addition to the traditional threats, such as packet dropping attack, eavesdropping, spoofing, and tampering, new threats include jamming, primary user emulation (PUE), and spectrum mangers attacks [3,4]. These can lead to the complete disruption of CRN. Therefore, strong security is essential to make cognitive radio a viable and reliable concept. In this paper proposed the reliable security scheme based on the forward and reverse path based mechanism in to identify the malicious packet dropping SUs in network. The proposed approach is not only detected but also provides the prevention from malicious users.

In the world of networking, spectrum is considered a decisive and critical resource. Most of the spectrum needed for wireless communication has been assigned. However, there is evidence indicating that abundant segments of the radio spectrum are not deployed for a substantial duration of time. This has piloted the innovation of cognitive radio technology as a solution for the inconveniences created as a result of this fixed spectrum allocation. This will enhance spectrum effectiveness through handling inefficient usage of licensed spectrum since radio equipment can identify the spectrum availability within their environment and invest the unused spectrum (spectrum holes) by licensed primary users

Countermeasures are needed to ensure secondary users of the spectrum and primary users (incumbents) are fully protected. (PUs) and reallocate it to secondary users (SUs) [5, 6] Cognitive radio is based on the idea of allowing unlicensed users to use licensed bands while safeguarding the priority of primary licensed users. Cognitive radio networks (CRNs) are hence composed of two types of users, licensed users or primary users (PUs) and unlicensed users (secondary users) (SUs). Primary users have access priority to the spectrum. Secondary users have cognitive radio capabilities allowing them to detect available channels and switching to them whenever they are not used by a primary user. Secondary users have to cater for the highest priority of PUs by detecting their presence and terminating their communications immediately to avoid any interference with PUs. CR is an outstanding concept to utilize spectrum efficiently and it is comprised of four basic operations [7]. This concept works in a cyclic transformation with the following four steps in the same order.

A. Sensing the Spectrum:

First of all, different methods and techniques are applied to sense which spectrum band is not in use by PUs.

B. Managing the Spectrum:

This step decides which channel could be the most useful and suitable among the list of available channels.

C. Sharing the Spectrum:

At this step, access is granted to the SUs to use the spectrum until unless it is free.

D. Mobility the Spectrum:

Here When a PU came back to utilize spectrum then this step is responsible to make it vacant for the PU and to avail some other empty by applying Step-A [8].

II. Security Issue in CRN

Cognitive Radio is a broader term with many prospective senses. The security requirements may be different with application environment; usually there are some common requirements providing basic safety controls like cognitive radio networks. With the nature of operating on wireless media the security requirements are the same as in a general wireless networks. These security requirements are [9, 10]

A. Access Control

The information transmission from an object to a subject is called access. Access Control to a resource is one of the major objectives of security. Access control addresses more than just controlling which users can access which files or services. The subjects and objects relationships are generally covered under the term of access Control.

B. Confidentiality

The International Organization of Standardization (OSI) is defined Confidentiality. Confidentiality involves by make it sure that each part of a system is appropriately secured and Accessible only by subjects who need it.

C. Authentication

Authentication is a process of verifying/testing that the demanded character is valid. Authentication requires that the subject provide additional information, which must exactly correspond to the identity mentioned. Password is the most common form of authentication.

D. Integrity

Integrity it offers a high level of assurance, that the data, objects, and resources are unchanged from their original protected state. This includes alterations occurring while the object is in transit, in storage and in process.

III. Routing protocols in CRN

There are many routing protocols applicable for wireless networks, but it is not feasible to apply these routing protocols for CRNs, due to their poor performance in dynamic spectrum environment. Routing protocols for CRN are classified according to their operation are in [11, 12].

A. Delay Based Routing

Delay based approach that combines many delay metrics (switching delay, backoff delay and queuing delay) to efficiently select minimum end-to-end delay route, the switching and backoff delay along the path or at the intersecting nodes are represented as PATH-delay (DP) and NODE-delay (DN) respectively, they are used to evaluate the cumulative delay of the path.

B. Link Stability based Routing

In traditional wireless Ad Hoc networks nodes communicate on the same channel and frequency. Hence, the distance among nodes and the adopted transmission power are the only parameters affecting the network connectivity. But in (Cognitive Radio Ad Hoc Network) CRAHN the concept of connectivity is changed because SUs experience spectrum heterogeneity. In CRAHNs two nodes can connect if they are in radio visibility and have at least one available channel, as a consequence, not only the nodes position and transmission power but also their communication Changing Spectrum Opportunities (SOP) affect network connectivity.

C. Throughput based Routing

Throughput can be defined as the average rate of successful packet delivery per second. Spectrum Aware Mesh Routing (SAMER) is a routing solution for CORNETs that considers both long term and short term spectral availability. It balances between long-term optimality (in terms of hop count) and shortest opportunistic gain (in terms of higher spectrum availability). Its main goal is to opportunistically utilize the spectrum in the network, by routing traffic across paths with higher spectrum availability while at the same time it achieves long-term stability by not deviating from the shortest hop-count path.

D. Location based Routing

Although location based routing has already been investigated generally for ad hoc networks, using it in CRNs will face many different and new challenges such as the dynamic changes in network connectivity due to the frequent changes in the spectrum opportunity of the CR nodes due to PU activity, another issue also is to make the routing protocol aware of this dynamic changes and to jointly select the route and the channel that will be used in the routing process.

IV. Literature Survey

The band allocation in spectrum is provides by the particular company of telecommunication after the approval of government. There are many more different efficient techniques, which are proposed by various researchers in security from SUs in CRN. The some of the latest work are discuss in this section.

In this paper [13] considers routing disruption attacks, which are network layer attacks in CRN. In routing disruption attacks, the malicious nodes attempt to cause packets to be dropped or extra network resources to be consumed. If an attacker is on a certain route, it may drop all of (Primary Users) PUs packets or selectively forward some of PUs packets. In the primary network, PUs hold licenses for specific spectrum bands, and can only occupy their assigned portion of the spectrum. SUs do not have any licensed spectrum and opportunistically send their data by utilizing idle portions of the primary spectrum. In routing attacks, the malicious SUs may claim that they have optimum route to destination. In this way, the honest SUs will forward data packets to the malicious SUs and all traffic will be routed through it.

In this paper [14] Credit Risk Value based algorithm is proposed here for finding out the selfish nodes in the network. This technique is easy to compute. The CRV technique will sense the attacks of selfish SUs in the network by computing the credit risk value. This technology is being carried out in the fore coming steps. First computes the CRV value before transmitting any packet and route the packet. Again recalculate the CRV value after routing. The CRV value is a constant, which implies the energy consumed for the transmission of packets. In Spectrum Analysis, the spectrum channel network parameters are being analyzed for all the spectrum holes. Then, it will be used for the Spectrum Decision process. In Spectrum Decision, the most accurate spectrum hole will be selected by the Cognitive users.

In this paper [15], this has not been discussed in CSS with malicious users for all the extended method in the state of art. Meanwhile, to avoid a large interference at the licensed users, a constraint is put on the resulting missed detection probability so that the interference is kept within the acceptable range. Based on

the above mechanisms and motivated by the main existing problems, i.e., the power consumption and poor judgement between honest and malicious users, we propose a trust-based CSS scheme to defence the SSDF attack in CRN. Firstly, implement a pre-filter among all SUs to select *k* cooperative sensing users based on their SNR. It can save energy and guarantee the valid transmission of data. Because it is not necessary, that the nodes who are under the poor sensing circumstance to stop their communication to perform weak sensing. Secondly, it is possible that there are some selfish nodes among the selected candidates for sensing.

In this paper [16], they propose a distributed trust management solution that does not require fusion center and we show the effectiveness of mitigating belief manipulation attacks. This paper considers belief manipulation attacks and follows a distributed trust management approach to detect and mitigate such attacks. Most of the existing methods to enhance security use authentication and cryptography, aiming at providing data confidentiality, data integrity, and node authentication. However, mitigating against the aforementioned attacks cannot be solely done via cryptography and authentication. Trust management, as a complimentary strategy, has the potential to further increase the security of CRN because it does not assume the statistics are always correct, expire learned beliefs, consider risk of making decisions, and perform inconsistency checks on parameters and statistics.

In this paper [17], propose a trust based channel centric approach towards evading selfish collaborative Secondary Spectrum Data Falsification (SSDF) attacks. They also discuss two variants of selfish collaboration: static and dynamic. In the static case, the set of channels that is attacked does not change over time, while in the dynamic case, it does. First, present a three step monitoring technique that gathers channel centric evidence by capturing the anomalies in the advertised occupancy of a channel. In first estimate the lower and upper bounds on the received power level from a neighbour. The bonds are then compared with some predefined threshold that results in a predicted ternary decision: occupied, not occupied, or cannot be decided. This predicted decision is compared with what a neighbouring node actually advertised.

In this paper [18], they propose a reliable AES-assisted DTV scheme, where an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve accurate identification of authorized primary users. Moreover, when combined with the analysis on the auto-correlation of the received signal, the presence of the malicious user can be detected accurately no matter the primary user is present or not. The proposed scheme combats primary user emulation attacks, and enables more robust system operation and efficient spectrum sharing. It is shown that with the AES-assisted DTV scheme, the primary user, as well as malicious user, can be detected with high accuracy and low false alarm rate under primary user emulation attacks.

V. Proposed Security Algorithm to Prevent from Attack

The proposed security scheme i.e. Intrusion Detection System (IDS) is based on the routing history of packets forwarding in network. In presence of attack in CRN is not able to recognize the attacker presence because it is busy to control the different sensor nodes communication. The spectrum sensing allocation and use is the main purpose of CRN. The attacker identification is based on power function and this function is applied on ean intermediate node because data is almost sending to intermediate node. The trust of nodes is calculated from proposed IDS scheme for CRN. The value of the x is based in the number of hops are existing in between sender and receiver in network.

Proposed Algorithm

Algorithm: Secure Cognitive Radio Network against Routing Disruption Attack

Input:

M: mobile nodes
S: source node
R: receiver node
I: intermediate nodes
Channel Assign Policy: CRNs
P_u: Primary User
S_u: Secondary User
r_p: AODV
P_i: Preventer nodes
n: forward path length {1 to n}
m: reverse path length
x: No. of nodes in shortest path
Ψ: range 550 M

Output: Delay, Throughput, Trust analysis

Algorithm:

S initiate route to search R through broadcast to M
Generate route packet (S, R, r_p)
If I in Ψ & I! = R **than**
I← forward packet to next hop
n← n + 1 // n predecessor path length
initial 1
Else if I in Ψ & I == R **than**
R receives route packet
n ← n
Reverse path generate
send ACK to S node
m ← n
Call data (S, R, I)
Else
Route not found
End If
Data (S, R, I)
S_u want to send data to R node
S_u generate data
Execute CRN method to find un-assign channel
If channel == free & Route == available **than**
S_u send data to x node
While x != R **do**
Compare (m, n)
If m != n & x forward data to next hop **than**
Receiver R not found
x ← x + 1
Else if m != n & x not forward data **than**
x set as suspicious node
P_i execute the prevention method
Else
x ← x + 1
End If
End While
If m == n & x == R **than**
True receiver found
Receives data from x node
End if
Prevention module

While P_i detect x receive data & m != n **do**
Set as suspicious node
Check x profile by P_i
If x_id != r_id **than**
P_i set x as route modification
x detected as attacker
x block by P_i node
Broadcast blocking message to all M
Call local route repair
Research route without participation of x node
End if
End While

The current instance of packet dropping is happening because of no observation in network is present by that congestion condition and nodes limited energy resource is consume unnecessary. But the continuous malicious activities is performed by packet dropping attacker is the sign of abnormal routing procedure. It is also notable secure network from attacker. The attacker detection not very easy process for security system (IDS) but the contiguously watching procedure is identified the attacker and also improves the routing performance by blocking the attacker.

VI. Result Description

The simulation result is evaluated on the basis of performance parameters mentioned in table 1. In NS-2 simulator version NS-2.31[19] is used to simulate all the modules.

Table 1 Simulation Parameters

Simulator Used	NS-2.31
Number of nodes	100
Simulation time	200 seconds
Attacker	Blackhole
Security System	IDS
Dimension of simulated area	1000m×1000m
Routing Protocol	AODV
Antenna	Omni-directional
Transport Layer Protocol	TCP, UDP
Traffic type	FTP, CBR
Packet size	512 bytes
Number of traffic connections	6
Node movement at maximum Speed	random & 30 m/s
Transmission range	250m

The performance is evaluated in presence of attack, existing trusts based scheme and proposed trust based scheme are evaluated on the basis of different performance metrics. The performance of proposed scheme is provides the better results and also secure network from attacker.

A. End to End Delay Analysis

The communication between in sender and receiver is properly shows the better receiving of data in network. The Secondary User (SU) or attacker aim in network is only to drop the large amount of data or whole data packets are transfer in between sender PU and receiver PU. The performance of network is measure in different trust value also in different modules like without trust means performance in presence of attack. The delay due to packets drooping in network is more in without trust module but the performance of proposed scheme is reducing the delay in network because of that the spectrum utilization is enhance and frequency of band are reach to receiver properly in CRN.

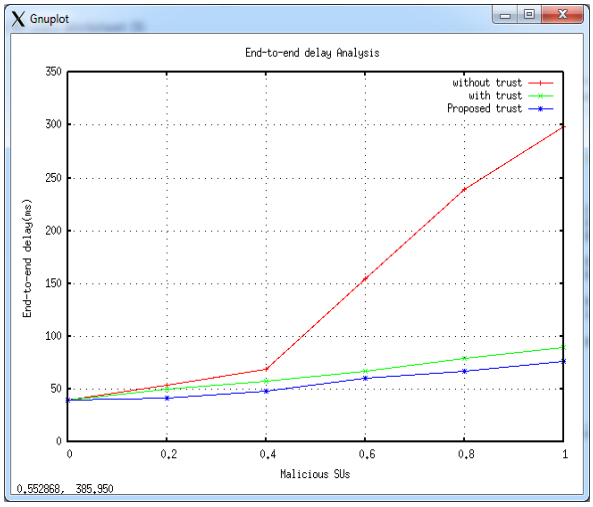

Fig. 1. Delay Analysis

B. Trust Performance Analysis

The trust based communication is counted in network on the basis of certain threshold value. The secondary user is also some time attacker these users are un-licensed users and if the spectrum having free range of frequencies is allocating by spectrum holes to SUs. The primary users are not creating the problem but due to SUs. The PUs is not facing the problem in sending data to receiver through licensed. In this graph the performance of all three modules are measure and the performance of trust value is degrades. The performance of proposed trust based communication in CRN is more. The trust value in proposed trust is highest about reaches to higher probability. The performance of proposed scheme

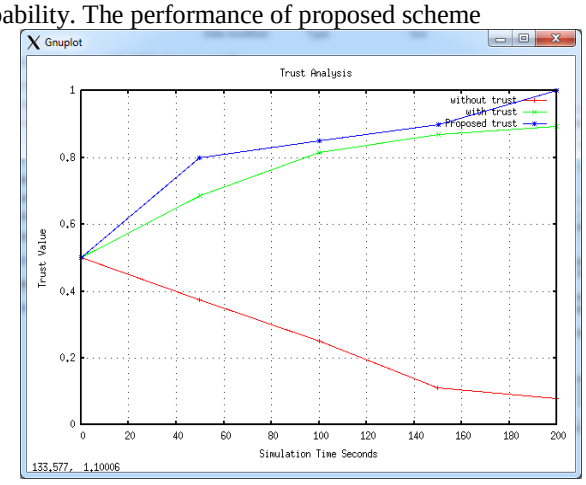

Fig. 2. Trust Analysis

C. End to End Throughput Analysis

The performance of data packets is evaluated through also throughput Performance Analysis. The SUs are communicated to receiver. The primary user's performance is also well collected by you to secure communication between PUs and SUs. The performance of proposed trust based scheme is reduces the throughput as compare to previous trust scheme in CRN. The performance of proposed trust is provides the 98% throughput performance. As compare to previous scheme the proposed trust performance is about provides 15% more better performance and this is only possible by working of frequency bands of spectrum. The low or high rates of frequency are reaches to destination properly in CRN.

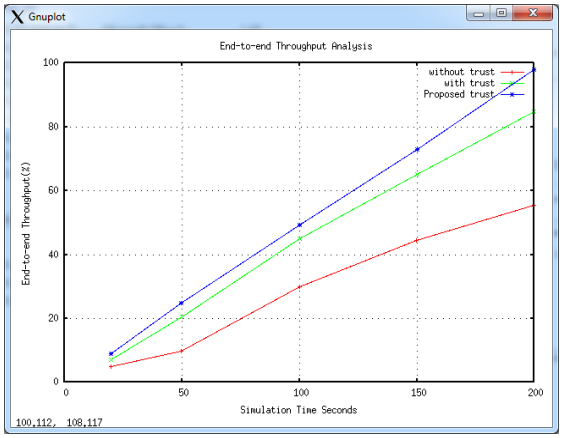

Fig. 3. Throughput End to End Analysis

VII. Conclusion and Future Work

In CRN the communication and controlling of available spectrum in different nodes and other devices are possible. For communication between the devices the proper spectrum availability is necessary and this spectrum availability. Security is the major concern in any network and this factor is also very necessary for secure communication. The number of unlicensed used are use the spectrum due to that CRN security is affected and also the attacker is used the information of licensed users. The numbers of sensor nodes are also sending and receiving data in network. In this research work we use the AODV (Ad hoc on demand Routing Protocol) protocol is exploiting for routing with in stationary network. The improving in trust value as compare to previous scheme is better that shows the better ad hoc network performance. The packet dropping Blackhole attacker is very active and really harmful for network data. The proposed reliable security scheme is proving the secure routing in between sender to destination. The proposed approach is check the reliability of data receiving in each hop count and according to rule if data receiving is affected and hop count value is not increment according to function then the nodes is expected as the attacker. The proposed scheme is check the reliability by detected the attacker with amount of packet loss in CRN. The performance of existing trust based scheme is also providing the security and proposed performance is may be better than the existing scheme. The proposed reduces is reduces the packet loss and also reduces routing overhead. The better packet receiving is improves the throughput, delay and improving the trust factor in CRN.

The CRN is the technique to provide the spectrum, sense the spectrum for ant wireless network. The wireless network has limited resources of communication. In future we proposed the routing improvement in DTN (Delay Tolerant Network). This network supports the multicast approach and applies the proposed security scheme to improve multicast routing performance.

References

[1] W.-Y. Lee and I. F. Akyildiz, “Spectrum-Aware Mobility Management in Cognitive Radio Cellular Networks,” IEEE Transaction Mobile Computation, Vol. 11, No. 4, pp. 529–542, 2012.

[2] A. Khare, M. Saxena, R. S. Thakur, and K. Chourasia, “Attacks & Preventions of Cognitive Radio Network-A Survey,” Vol. 2, No.3, pp. 1002–1006, 2013.

[3] G. A. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, “A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks,” IEEE Communications Surveys and Tutorials, Vol. 15, No. 1, 2013, pp. 428-445.

[4] J. L. Burbank, “Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security,” in Proceeding of 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), pp. 1-7, Singapore, 2008.

[5] R. Pal, D. Idris, K. Pasari, N. Prasad, “Characterizing Reliability in Cognitive Radio Networks,” in Proc. First International Symposium on Applied Sciences on Biomedical and Communication Technologies, (ISABEL '08), pp. 1-6, Aalborg, 2008.

[6] M. Youssef, M. Ibrahim, M. Abdelatif, L. Chen, and A. V. Vasilakos, “Routing Metrics of Cognitive Radio Networks: A Survey,” IEEE Communications Surveys and Tutorials, Vol. 16, No. 1, pp. 92-109, 2014.

[7] S. V Wankhede, M. N. Thakare, and R. Vaidya, “Design Approach for Cross Layer Attacks Defence in Cognitive Radio,” pp. 763–766, 2015.

[8] I. C. and J. L. I. Christian, S. Moh, “Spectrum Mobility in Cognitive Radio Networks,” IEEE Communication Magazine Vol.50, No.6, pp. 114–121, 2012.

[9] Xueying Zhang, Cheng Li “The Security in Cognitive Radio Networks: A Survey” ACM International Conference on Communications and Mobile Computing, 2009.

[10] Ying-Chang Liang, Kwang Cheng Chen, Geoffrey Ye Li, and Petri Mahanen, “Cognitive Radio Networking and Communications: An Overview”, IEEE Transactions on Vehicular Technology, Vol. 60, No. 7, pp. 3386-3407, September 2011.

[11] Samar Abdelaziza, Mustafa ElNainay, "Survey of Routing Protocols in Cognitive Radio Networks " Preprint submitted to Elsevier, pp1-20, October 1, 2012

[12] G. Baldini, T. Sturman, A.R. Biswas, "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead" IEEE Communication Survey Tutorial 14, 2012.

[13] Ling Hou, Angus K. Y. Wong, Alan K. H. Yeung, Steven S. O. Choy "Using Trust Management to Defend against Routing Disruption Attacks for Cognitive Radio Networks" IEEE International Conference on Consumer Electronics-China (ICCE-China), 2016.

[14] R. Ahila Priyadharshini, K. Uma Haimavathi, "Detection of Attacks and Countermeasures in Cognitive Radio Network", this full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET conference, 2016.

[15] Fanzi Zeng, Jie Li, Jisheng Xu, Jing Zhong, "A Trust-based Cooperative Spectrum Sensing Scheme Against SSDF Attack in CRNs" ,IEEE Trust Com. / Big Data SE/ISPA, 2016.

[16] Lei Ding, Onur Savas, Gahng-Seop Ahn, Hongmei Deng, “Securing Cognitive Radio Networks with Distributed Trust Management against Belief Manipulation Attacks", IEEE Globecom Workshops (GC Wkshps), 2015

[17] Shameek Bhattacharjee and Mainak Chatterjee, "Trust based channel preference in Cognitive Radio Networks under Collaborative Selfish Attacks", IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications, 2014.

[18] Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, and Tongtong Li, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard", IEEE Transactions on Information Forensics And Security, Vol. 9, No. 5, May 2014.

[19] K Fall and K. Varadhan, The NS Manual, http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf.