International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Types of Attacks and Security Scheme in CRN: A Survey

Manorama Mishra[1], Swatantra Tiwari[2]
[1]M. Tech. Scholar in Dept. of Electronics and Communication, Rewa Institute of Technology Rewa
[2]Asst. Prof. in Dept. of electronics and communication, Rewa Institute of Technology Rewa
Email address: {[1]manoramamishra542, [2]swatantratiwari84} @gmail.com

Abstract*—In The cognitive radio networks includes the primary user (PU) system with authorized spectrum and the secondly user (SU) system without authorized spectrum. When the SUs want to use the spectrum, they have to find the idle channels that are not occupied by the PUs. The devices are consider in this research are stationary and delivering information in between sender to receiver. In this paper we discuss the various security techniques like IDS (Intrusion Detection System), cryptography and other scheme against different attacks in multihop CRN network. The devices are nodes and these nodes are connected with each other through wireless link and exchange data packets and control information. The packet dropping attack is very harmful and also drops the whole data packets in network. The nodes are not known about the attacker because attacker is forward the fake reply of route in between sender to destination. The attacker is detected through not forwarded the data packets to next node or destination node in network. The proposed security scheme is based the calculate hop count and also maintain the record of hop count till the destination is not found. In this paper we highlight the different routing techniques, attacks effect and security proposed by different authors in field of CRN. The whole focus of this paper is on only security and major on packet dropping attack.*

***Keywords*—** *CRN, Attack, Security, Routing, PU, SU.*

I. INTRODUCTION

Cognitive radio networks (CRN) are an emerging multi-hop wireless networking technology where nodes are able to change their transmission or reception parameters based on interaction with the environment in which they operate. The Radio spectrum, which is needed for wireless communication systems, is a naturally limited resource. Recent studies by the spectrum regulatory authorities (e.g. the Federal Communications Commission (FCC)) highlight that many spectrum bands allocated through static assignment policies are used only in bounded geographical areas or over limited periods of time, and that the average utilization of such bands varies between 15-85% [1]. Operating in unlicensed bands, especially in the ISM band, has been prolific with a wide range of applications developed in different fields (e.g. WLANs, mesh networks, personal area networks, body area networks, sensor networks, etc.), which caused overcrowding in this band. This highlights two main problems with wireless networks:-

- Exhaustion of the scarce wireless spectrum
- Underutilization of the licensed spectrum in some areas.

Cognitive Radio Networks (CRN) emerged as a paradigm to address these problems. In CRN, wireless nodes change their parameters to communicate efficiently, avoiding interference with licensed (primary users (PUs)) or unlicensed users (secondary users (SUs)). This alteration of parameters is based on monitoring the radio environment, such as the radio frequency spectrum, user behaviour, and network state. CRN are composed of cognitive, spectrum-agile devices capable of changing their configurations on the fly based on the spectral environment. This capability opens up the possibility of designing flexible and dynamic spectrum access strategies with the purpose of opportunistically reusing portions of the spectrum temporarily vacated by licensed PUs. On the other hand, the flexibility in the spectrum access phase comes with an increased complexity in the design of communication protocols at different layers [3]. Most of the work in CRN has focused on the lower layers of the protocol stack, mainly at the physical and MAC layers [2] with single-hop forwarding. Their goal is to address the channel scarcity problem and achieve efficient wireless communication. It allows CRN to discover spectrum holes, and utilize them, which decreases contention on channels, minimizes interference between communicating nodes and improves the average channel efficiency. To support various wireless applications and services in a non-interfering basis, the fixed spectrum access (FSA) policy has traditionally been adopted by spectrum regulators, which 1assign each piece of spectrum with certain bandwidth to one or more dedicated users [4]. By doing so, only the assigned (licensed) users have the right to exploit the allocated spectrum, and other users are not allowed to use it, regardless of whether the licensed users are using it. With the proliferation of wireless services in the last couple of decades, in several countries, most of the available spectrum has fully been allocated, which results in the spectrum scarcity problem. On the other hand, recent studies on the actual spectrum utilization measurements have revealed that a large portion of the licensed spectrum experiences low utilization [5]. These studies also indicate that it is the inefficient and inflexible spectrum allocation policy that strongly contributes to spectrum scarcity and, perhaps, even more than the physical shortage of the spectrum. To maintain sustainable development of the wireless communication industry, novel solutions should be developed to enhance the utilization efficiency of the radio spectrum. Dynamic spectrum access (DSA) has been proposed as an alternative policy to allow the radio spectrum to more efficiently be used [6]. In DSA, a piece of spectrum can be allocated to one or more users, which are called primary users (PUs); however, the use of that

Manorama Mishra and Swatantra Tiwari, "Types of attacks and security scheme in CRN: A survey," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 3, pp. 178-183, 2018.

spectrum is not exclusively granted to these users, although they have higher priority in using it. Other users, which are referred to as secondary users (SUs), can also access the allocated spectrum as long as the PUs are not temporally using it or can share the spectrum with the PUs as long as the PUs' can properly be protected. By doing so, the radio spectrum can be reused in an opportunistic manner or shared all the time; thus, the spectrum utilization efficiency can significantly be improved. To support DSA, SUs are required to capture or sense the radio environment, and a SU with such a capability is also called a cognitive radio (CR) [6] or a CR user. There are different types of cognitive capabilities with which a CR may be equipped. For example, a CR may sense the ON/OFF status of the PUs [6] or can predict the interference power level that is received at the primary receiver (Rx**) [**7]. In an extreme case, if a CR is a genie user, it may also acquire the messages that are transmitted by the primary Tx [8].

II. Applications of CRN

The demand of spectrum increased incredible due to the recent Improvements in wireless communication. This dramatic requirement of spectrum has challenged to the current spectrum licensing system and inspired authority to legalize opportunity for spectrum access. Recently, many researchers, hardware manufacturers, and many authorities are working to solve this virtual Shortage issue. Cognitive radio networks (CRN) are suitable in this mitigation, by utilizing licensed spectrum are opportunistically. (CRN) is rapidly Growth into many wireless communication fields. Spectrum sensing, spread spectrum, coexistence, spectrum sharing, and MIMO techniques have become areas of Interest over the past decade. Recently many researchers are working in various application areas of cognitive radio wireless sensor networks (CR-WSNs) and cognitive radio networks (CRNs). These issues are mainly focused on recent advance [1, 2, 5, 6] and future direction with respect to applications of Cognitive radio networks (CRN):

- Focuses on the application of CR concepts to vehicular network environments. It provides taxonomy of the existing literature in the area, highlighting the key research problems and identifying how spectrum management functions can take into account the characteristics of the vehicular environment.
- The area of CR networks applied to emergency networks and public safety communications. tochastic- geometric model to capture the reduction of effective service area when adjacent networks share the TV white space spectrum and defines the fractional service area as a metric to evaluate the capability of providing services in different scenarios
- Covers another relatively unexplored application of CR technologies to enable underwater acoustic communications. In particular, dynamic spectrum sharing mechanisms are applied, which take into account the characteristics of the underwater channel.
- The application of CR technologies and DSA to deploy small independent service providers networks that form coalitions with each other to offer coverage in larger areas. The article proposes the use of cyclo-stationary signatures both to identify coalitions and to enable the hand- over process between providers.
- Potential Application Areas of CR-WSNs may have a wide range of applicat ion domains. Indeed, CR-WSN can be deployed anywhere in place of WSNs. Some examples of prospective areas where CR-WSNs can be deployed are as follows: facility management, machine surveillance and preventive maintenance, precision agriculture, medicine and health, logistics, object tracking, telemetries, intelligent roadside, security, actuation and maintenance of complex systems, monitoring of indoor and outdoor environments.

III. Challenges in CRN

There are still challenges and open problems for realizing effective and efficient spectrum sharing for CR communications [4] as follows.

- *Common Control Channel*

There is a pertinent question on whether we need a common control channel for CR operations. A common control channel will pave the path to an easier way of enabling information exchange during spectrum sensing and access in CR networks. However, unlike conventional networks, a common control channel may not be available in the initial phase when spectrum holes are not sufficiently identified. Furthermore, an identified channel may be re-occupied by the PUs at any time, which may interrupt the coordinating messages if it is used as a common control channel. How we can set up and maintain the common control channel is particularly crucial for proper operations in CRN.

- *Joint Spectrum Sensing and Access*

Spectrum sensing and access are usually separately designed, because spectrum sensing achieves certain detection performance, whereas spectrum access mainly focuses on improving the system capacity based on the identified spectrum hole. However, the two aspects are inevitably coupled. For example, different transmission power levels of the CR users may require different decision thresholds in spectrum sensing, and vice versa. Furthermore, the joint design of multichannel sensing and distributed random access will be a challenging issue in CRN.

- *True Opportunities and Economy Models.*

We need to quantify the economic and engineering benefits of using CRN-based systems over the traditional wireless communications systems. In addition, the underlying network economy models need to be developed so that the commercial community can feel comfortable with CRN. More spectrum measurements are required to understand how many of the spectrum holes are commercially viable. The low utilization does not necessarily mean that the SUs can use the opportunity in any economically sensible way.

Manorama Mishra and Swatantra Tiwari, "Types of attacks and security scheme in CRN: A survey," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 3, pp. 178-183, 2018.

- *CRN and CR Implementation Architectures*

The actual implementation architecture for supporting fully functioning prototypes needs a cross-layer design concept, and it becomes challenging to build. In particular, handling the coordination and control of various levels of protocol stack and enforcing cooperation among the CRs still require considerable research and development work.

IV. Routing protocols in CRN

Routing in multi-hop CRN, however, is an important problem that affects the performance of the entire network [4]. Different from traditional routing protocols in ad hoc networks, routing in CRN has to deal with a number of challenges, including adapting to the dynamic changes of spectrum availability due to the stochastic behaviour of the primary and secondary users, the heterogeneity of resources such as the availability of different channels and radios on the same node, and synchronization between nodes on different channels. 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 [9, 10].

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.

V. Attacks in CRN

In wireless technology, the communications takes place ‘through the air’, thus the risk of security attack is greater than with the wired networks [11, 12. 13]. The various common traditional wireless security threats and challenges that is also applicable to CRN technology along with some proposed mitigation techniques have been studied below in the literature.

1) Jamming Attack

Jamming attack or Denial-of-Service (DoS) attack is a malicious attempt meant to prevent the legitimate users from accessing a system resource they expects or delays the system operations and functions. In the context of CRN, DoS attack can be accomplished by two ways. In the first type, it prevents the authorised user from accessing the available spectrum holes. Secondly, the attacker may try to mask the licensed user’s presence, which may cause interference and thus breaks the basic etiquette of CRN operation. Jamming attack is a particular class of DoS attack that can heavily affect both the legitimate PU and SU in a CRN. In jamming, the attackers jam or flood the medium by continuously transmitting on a licensed band and thus disturb the legitimate participants in a communication session.

2) Sinkhole Attack

In a sinkhole attack, an attacker advertises itself as the best route to a specific destination. The CR users consider that false route as the optimal one and use it to forward their traffic and can be easily tamper by the attacker. These attacks are typically more harmful in infrastructure-based and mesh architectures as the entire communication takes place through a common BS. The sinkhole attack enable an adversary to lunch other types of attack like eavesdropping, selective forwarding and black hole attack. In general by lunching Eavesdropping, the adversaries monitor the on line traffic transmission to collect some useful data that can later be analysed to extract some sensitive information.

3) Wormhole Attack

Wormhole attack basically requires two or more adversaries to lunch. In this attack, a malicious node tunnel packet received in one part of the network by depicting a low latency link. Then start replaying packets in another part of the network. For example, an attacker could convince the CR users that are usually far away from the BS that the distance reduces only to one or two hops via the wormhole. In this way, the attacker attracts nodes to adapt this route in to their

communication paths by pretend it as a quality and shorter path to the BS. It is a serious attack in wireless network as it is independent of MAC layer protocols and also is immune to cryptographic system. Moreover; an attacker closely located to a BS can completely disrupt the routing process through a significantly placed wormhole. It is hard to identify a wormhole as they use an out-of-band private channel that is invisible to the underlying networks and also the information it insert to the network is real.

4) HELLO Flood

In HELLO flood attack, an attacker broadcasts HELLO packets to all the CR users in the network with enough transmission power. Thus, the receiving node would believe that the sender is within the radio range. This would result even the far away nodes to start the communication with the attacker by assuming it as their neighbour. However, their packets routed through the attacker node may leads to simply lost or corrupted. The HELLO flood attack can be prevented by verifying the capacity of the link to communicate bi-directionally before utilising that link for any actual communication. In an effort to countermeasure the HELLO flood attacks, a symmetric key is shared between the nodes and the trusted BS proposed a non-cryptographic technique for HELLO flood attack detection in WSN, which calculates the received signal strength (RSS) and distance between nodes and cluster head to find the malicious node.

5) Sybil Attack

In this attack, a single CR node uses multiple fake identities to all other nodes that pretend to be present at different location of the network at the same time. This misleads other nodes to believe its each identity as a legitimate node and its further association with other types of attacks causes significant vulnerability to the CRN. To defend against Sybil attack, a unique shared symmetric key can be used for each CR user with the BS.

VI. CRN Security Constraint

The security constraints of CRN mentioned in [14] are as follows:-

- *Availability*

Within CRN, the Base stations (BSs) should ensure the availability of spectrum needed by PUs and SUs. BSs should be equipped with the needed security measures to detect DoS attacks including distributed DoS.

- *Authentication*

To ensure that CRN devices and components are communicating with a legal party, PUs, SUs, and other devices, authenticating them is essential. This applies to BS authenticating CRN and CRN authenticating each other. All components involved in the CRN must be able to identify other legitimate devices and systems. Various cryptographic techniques are used for this purpose. CRN should be capable of preventing or at least detecting various attacks on cryptographic protocols including man-in-the- middle attack.

- *Integrity*

It is demanding to ensure that the messages sent by BS, CRN, PU, or SU have not been modified when arriving at their destination. This assurance entitles that the messages received have not been through any modification, insertion, deletions, or replay on its way to its destination. Commands and signals issued by various constituents of the CRN are critical messages, and therefore, need to be clear of any modifications. Cryptographic hash functions and MACS need to be adopted to ensure message integrity.

- *Confidentiality/Privacy*

PUs and SUs are interested in keeping their communications confidential. They want to ensure that their messages are only disclosed to the authorized CRN, PUs, and SUs. In many applications, such as healthcare applications, privacy is essential. CRN should adopt cryptology to enforce privacy.

- *Nonrepudiation*

Communicating parties with the CRN infrastructure do not want the receiver to deny receiving a message (destination non repudiation), and the sender to deny sending a message (source destination). Cryptology can be deployed to ensure, for example, that a CRN cannot deny it has received a request for spectrum from PUs and SUs, and a CRN cannot deny a message received from a BS.

VII. Literature Survey

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 [15] 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 CRN routing context, we define the concept of trust as a representation of the degree that secondary users (SUs) honestly forward data packets to the next hop. In this paper, we will use the statistics of SU forwarding behaviors to construct the trust of neighboring SU *j* from SU *i* at time t, which is denoted by *T*ij(t). When the data packet of SU *i* needs to be sent to destination SU *j*, a route should be decided between the source and destination pair.

In this paper [16] 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

Manorama Mishra and Swatantra Tiwari, "Types of attacks and security scheme in CRN: A survey," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 3, pp. 178-183, 2018.

the credit risk value. This technology is being carried out in the fore coming steps. First it 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 [17], 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 defense the SSDF attack in CRN. Firstly, we 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. To address this problem and increase access opportunities, we propose a trust-based model to reflect the trustworthy degree of the local decision of each sensing node.

In this paper [18], 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 [19], we propose a trust based channel centric approach towards evading selfish collaborative Secondary Spectrum Data Falsification (SSDF) attacks. We 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, we present a three step monitoring technique that gathers channel centric evidence by capturing the anomalies in the advertised occupancy of a channel. First we estimate the lower and upper bounds on the received power level from a neighbor. 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 neighboring node actually advertised. The comparison yield has three possible outcomes like match, mismatch, or undecided. The observation data formed by the outcomes from all neighbors on a particular channel gives the frequency of occurrence of matches, mismatches, or undecided. More matches are indicative of agreement on channel occupancy while more mismatches means presence of misleading advertisements.

In this paper [20], 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. The effectiveness of the proposed approach is demonstrated through both theoretical analysis and simulation examples. 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.

VIII. Conclusion and Future Work

The numbers of sensor nodes are also sending and receiving data in network. The CRN is resolve the problem of spectrum allocation but having also the problem of attacks that affect the actual performance. In this paper the different security scheme proposed by different authors are proving the secure routing in between sender to destination. These techniques is check the reliability of data receiving according to rule if data receiving is affected then according to function the nodes is expected as the attacker. The schemes are check the reliability by detected the attacker with amount of packet loss or flooding and any other issue in CRN. The routing protocol is only used for routing and this protocol having different technique to route data in between source station to destination station. The different scheme is only used to handle the large network as well as small network scenario with new concept and also possible to work more efficiently. The better packet receiving is improves signal strength that reduces the loss of data. The wireless devices having limited bandwidth capacity and these devices are controlled by server, base station or also may be possible to interchange information independently in network. In future we proposed security scheme against packet dropping attack apply the proposed IDS.

References

[1] FCC Spectrum Policy Task Force, "Report of the spectrum efficiency working group," FCC, Tech. Rep., November 2002.

[2] I. Akyildiz, W.-Y. Lee, and K. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks (Elsevier)*, vol. 7, no. 5, pp. 810–836, 2009.

[3] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/ dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer. Network*, vol. 50, pp. 2127–2159, May 2006.
[4] 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.
[5] A. Chamam and S. Pierre, "Power-efficient clustering in wireless sensor networks under coverage constraint," in *Proceeding IEEE International Conference of Wireless Mobile Computer Network Communication (WIMOB)*, Avignon, France, 2008, pp. 460–465.
[6] G. Miao, N. Himayat, and G. Li, "Energy-efficient link adaptation in frequency-selective channels," *IEEE Transaction of Communication*, Vol. 58, No. 2, pp. 545–554, Feb. 2010.
[7] O. Akan, O. Karli, and O. Ergul, "Cognitive radio sensor networks," *IEEE Network, Magazine*, vol. 23, no. 4, pp. 34–40, 2009.
[8] G. Vijay, E. Ben Ali Bdira, and M. Ibnkahla, "Cognition in Wireless Sensor Networks: A Perspective," *IEEE Sensors* Journal, vol. 11, no. 3, pp. 582–592, March 2011.
[9] Samar Abdelaziza, Mustafa ElNainay, "Survey of routing protocols in cognitive radio networks," Preprint submitted to Elsevier, pp1-20, October 1, 2012.
[10] 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.
[11] Sumit Kar, Srinivas Sethi, Manmath Kumar Bhuyan, "Security challenges in cognitive radio network and defending against byzantine attack: A survey," *International Journal of Communication Networks and Distributed Systems*, vol. 17, no. 2, 2016.
[12] Ramesh babu B, Meenakshi Tripathi, Manoj Singh Gaur, Dinesh Gopalani, Dharm Singh Jat, "Cognitive radio ad-hoc networks: Attacks and its impact," *IEEE International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, pp. 125-130, 2015.
[13] Subbalakshmi, K.P. and Mathur, C.N., *Security Issues in Cognitive Radio Networks: Cognitive Networks: Towards Self-Aware Networks*, pp. 284–293, John Wiley and Sons, Ltd., New York.
[14] Hanen Idoudi, Kevin Daimi, and Mustafa Saed, "Security challenges in cognitive radio networks," *Proceedings of the World Congress on Engineering*, vol. 1, WCE 2014, July 2 - 4, 2014.
[15] 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.
[16] 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.
[17] Fanzi Zeng, Jie Li, Jisheng Xu, Jing Zhong, "A trust-based cooperative spectrum sensing scheme against SSDF attack in CRNs," *IEEE TrustCom/BigDataSE/ISPA*, 2016.
[18] 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
[19] 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.
[20] 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.