



CRAODV-S: A Secure On-Demand Routing Protocol in Cognitive Radio Ad Hoc Network

Sangita Pal¹, Srinivas Sethi²

Department of CSE, Indira Gandhi Institute of Technology (IGIT),
Saranag, Orissa, INDIA.

Abstract: The Cognitive Radio Ad Hoc NETWORK (CRAHN) technology is a cutting-edge and novel technology in wireless communication era and it meets the requirements like self-configuring, self-healing, and strength with low organization cost. In this communication environment routing has vital role to form the path from source node to destination node and transmit the data between them. The efficient and secure route can be formed by selecting the trusted node and its channel for transmitting the data. In this paper, a novel scheme has been used to select efficient and trusted path by considering of multiple objectives. The scheme calculates trust values of node including secondary user/nodes in CRAHNs to distinguish between healthy and malicious nodes. It considers not only efficient and effective route but also the trusted level of neighbours or intermediate nodes from source to destination.

Keywords: CRAHN; Secure Routing; Trusted; On-Demand; malicious users;

I. Introduction

Dynamic spectrum access features and uses of distributed fashion in Cognitive Radio Networks (CRNs) it may introduce false information from malicious users. There may be chances of false information about spectrum occupancy by a malicious user. If the malicious user gives the information such that the primary user (PU) is unoccupied the spectrum and when the secondary user (SU) tries to occupy the spectrum, as a result interference takes place between PU and SU. Another case may happen if the malicious user gives the information such that the PU is occupied the spectrum so that the SU or PU are not utilized the spectrum even though the spectrum is free.

So, it is necessary to develop a trusted routing protocol. There are so many attacks to CRN like unacceptable interference to licensed PU causes unusable of PU's spectrum band. Missed opportunities for SU, which causes prevention of secondary user from using free available spectrum band[5]. Other attacks related to cryptographic aspects like access to private data causes unauthorized data access, modification of data causes loss of data integrity, injection of false data causes performance of cognitive radio network in an unpredictable way[1]. Game theory is a normal tool for designing the defense from attackers. Dynamic games like, stochastic games can be used to derive the optimized defense strategy that accommodates the environment dynamics as well as the adaptive attacking strategy [2]. In this paper, it has been introduced a trust-evaluation approach which computes trust values of nodes including secondary nodes in CRAHN to distinguish between healthy and malicious nodes successfully.

The rest of the paper is as follow. Security requirement discussed in the section II; followed by challenges in dynamic spectrum access environment in terms of security in section III. Selfish and malicious use action has been discussed in section IV. Section V discussed on Secure Routing Protocol in CRAHN. The proposed model has been described in section VI followed by result and discussion in section VII. Finally it has been concluded in section VIII.

II. Security Requirements

There are major security requirements which provide basic safety controls. They are discussed below as per figure 1 [3][21]:

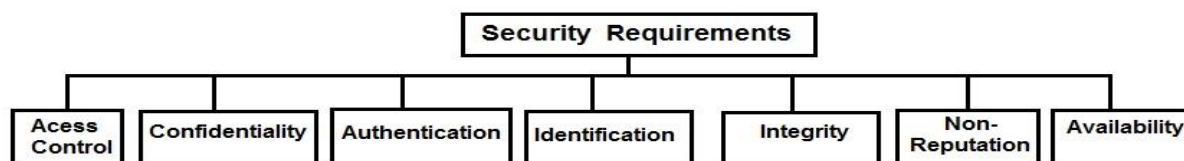


Fig.-1: Security requirements

- **Access control:** It is one of the major objectives of security and it is the physical layer security requirement. All users like SUs must be accessed and moved to the spectrum band by obeying certain policy like their sensing results. So the access control should coordinate the spectrum access to avoid collisions among different SUs.

- **Confidentiality:** It ensures the information should be secured and accessible only by authorized parties who need it. That is data should not be transferred to an unauthorized entity. In CRAHN, PUs and SUs are interested in keeping their communications confidential. The users want to make sure that, their communications are only disclosed to the authorized PUs and SUs. This is more important in CRAHN due to dynamicity of spectrum.
- **Authentication:** The main objective of an authentication approach is to ensure that CRAHN devices and components like PUs, SUs, and other devices, are communicating with a legal party. It is required to authenticate the users in the communication process. In CRNs, it is required to distinguish between PUs and SUs and authentication process in CRNs can be applied in the physical layer [4]. It has been proposed a approach which allows primary users to add a cryptographic link signature to its signal, so that the spectrum usage by primary users can be authenticated. Another authentication technique for CRNs based on third-party Certification Authority (CA) is proposed in [5]. But Providing CA for SUs is more challenging because SUs are spread over a large geographical area [6].
- **Identification:** It is a technique where a user's device is associated with its name or identity and one of the elementary security requirements for a communication system. For example, in cellular communication system, the mobile devices are identified by an international mobile equipment identifier (IMEI). Identification with tamper proof approach is built into the secondary user devices in CRNs. In [7], the authors mentioned a CR to know about the number of networks exist, numbers of users are connected with each network, and certain properties on the devices themselves which may be advantage for CR. To realize this level of information, it is necessary for a CR to collect correct information of the radio frequency environment. CRs detect different network services and device identification. The service detection and device identification provide the essential blocks for making efficient and reliable CRNs [7].
- **Integrity:** It ensures that, the resources, data and objects are not changed from their original secure state. Stored data, processed data and transit data in the network system needs to be protected from malicious activities. In wireless medium, data are easily accessible. So integrity is more important in wireless medium. It is required to maintain integrity to the messages sent by base station (BS), CRN, PU, or SU. The integrity of the network will be lost due to:
 - A malicious node, which can inject false data.
 - Unstable conditions due to wireless channel cause loss of data [8].

Cryptographic hash functions and MACS require ensuring message integrity. The security protocol used in wireless LANs at data link layer is named the counter mode encryption with CBC-MAC authentication protocol (CCMP)[9].The CCMP protocol uses Advanced Encryption Standard(AES), which is a private key data encryption algorithm [10] in cipher block chaining mode[11] to produce a message integrity check. To maintain data integrity higher cryptographic techniques can be applied in CRAHNs.
- **Non-repudiation:** This technique prevents from the sender or receiver denying a transmitted message. In a CRAHN, if malicious secondary users violating the protocol are recognized, the non-repudiation approach can be used to verify them and disassociates/ bans the malicious users from the secondary network [12][21].
- **Availability:** It denotes to the capability of PUs and SUs to access the spectrum in CRAHNs. In case of PUs the availability denotes to being able to communicate in the licensed band without harmful interference from SUs. As per FCC in dynamic spectrum access (DSA) policies, spectrum availability for PUs is definite. In case of SUs, the availability denotes to the presence of chunks of spectrum, where the SUs can communicate without affecting harmful the interference to PU. In CRAHNs, one of the important purposes of this service is to prevent energy starvation and denial of service attacks (DoS), and misbehavior, such as selfishness [12][21].

III. Challenges in Dynamic Spectrum Access Environment in terms of Security

CRs facilitate the SUs to use licensed spectrum band which are allocated to PUs without interfering to PUs. Therefore, correct spectrum occupancy information needs to be kept by a SU which minimizes the interference between users in CRAHN. A malicious user can try to falsify the spectrum use information in the network, which may cause interference between users. In dynamic spectrum access environment, the security threats are outlined below [18]:

a. Dynamic spectrum access attack:

This type of attack is called Primary User Emulation (PUE) attack, and can be active in dynamic spectrum access surroundings [16][17]. In this attack, a malicious user acts as a PUs and transmits signals which are very similar to the PUs. The SU consider that, the spectrum is occupied by the PU. In another case, the malicious user represents as a PU and informs the SU that the spectrum is in use. Thus, a malicious user can illegally access to the spectrum. In this circumstance the malicious users becomes as a "selfish" user.

b. Malicious behavior attack:

A selfish or misbehaving user masquerades to be a PU and broadcasts jamming waveform signals that is very difficult, to be detected by the SU, such that the cognitive radio mistakenly learns that, it can use the available spectrum when PU is transmitting. In another circumstance, the misbehaving user fakes as a PU and notifies the SU that, the spectrum is actually available, when it is still in use by the PU. Thus, it causes interference to PU. These types of misbehaving user becomes as a “malicious” user. In this, CR doesn’t follow any common rule for sensing and dealing with range of the spectrum.

c. Denial of Service (DoS) attack:

DoS attack is formed by the unintended failure of nodes or malicious action. The DoS is meant for the adversary’s try to destabilize, interrupt, or abolish a network. It also meant for every event that reduces a network’s ability to deliver a service. The key objectives of DoS attack are to set the problem on the resources and to break the utilization of the resources for the nodes in the network [13] [14]. There are three types of DoS attacks [15]. The first one being a low intensity attack which is on a single node that makes it work inefficiently and thus making it inaccessible by the neighboring nodes in the same network. The second one being the high intensity attack which attacks is for a group of nodes in an enclosed area, thus making it malfunction and deny services for the other areas in the same network and the last one being of the highest intensity distributed denial of service attack which is for the entire network and makes the network inaccessible due to unlimited traffic being pumped from many malicious users, resulting in the network outage. Grayhole attack is one of the DoS attack performed by malicious nodes. The node forwards the message packets at initial time in the network and ignores to do so after some time by the constructed route. This can be treated as routing misbehavior in the network.

d. Blackhole Attack:

Malicious nodes never send true information to the neighbor nodes in the network. This type of attack is treated as blackhole attack [35] by malicious users in the network. The malicious user sends a route reply message with high sequence number after receiving the route request message from requesting users to settle in the routing table of the victim node, before other nodes send a true one. So, requesting users consider that route discovery process is over and drop the other route reply message packets. Then the communication process starts with malicious users. In this way, malicious user attacks all route reply messages packets and all the packets are dropped without forwarding to any nodes. Generally, blackhole attack affects the entire network easily if it is in central place of the network.

IV. Actions of Selfish and Malicious Users

The selfish user uses more resources by misleading other unlicensed users to create the situation about a licensed user. It uses the spectrum with higher priority. As a result the selfish user occupies the spectrum resource as and when it wants. The selfish user increases its effectiveness and efficiency by Intentional Jamming Attack (IJA), since the misleading behavior does not obey the spectrum sharing approach [19]. In this, the malicious SU or selfish user jams the primary and other secondary users by purposely in the network and nonstop communicating in a licensed band [12]. The selfish or malicious SUs raise their accessing probability by altering the communication parameters to improve their own utilities by degrading the performance of other users. Whereas, a malicious user is a specialist in spoofing, this prevents other unlicensed users from using the spectrum and causes a DoS. So Malicious users decline the available bandwidth and break down the traffic. The Quality of Service (QoS) of the spectrum is infected and causing the network to be instable. Hence, the CRNs performance is degraded.

V. Secure Routing Protocol in CRAHN

Ad hoc wireless networks have no infrastructure and no central control unit for routing packets from source to destination. In this network any one can bring its own mobile units. So securing routing becomes a great challenge in ad hoc network. Hence there must be security challenges in Spectrum sensing, Spectrum management, spectrum sharing, and spectrum mobility in CRAHN.

The Routing protocols like Ad hoc On-demand Distance Vector routing protocol (AODV) and the Dynamic Source Routing protocol (DSR) are efficient routing protocols but they were not secure from DoS attack that means, the attacker can broadcast the false information in the network to redirect transmission. In [23], the authors proposed a protocol called Authenticated Routing for Ad hoc Networks (ARAN) which detects and protects the network from attacker against malicious actions. This protocol has been accomplished the requirements like authentication, message integrity, and non-repudiation to an ad hoc environment.

In [3], the authors precise that in IEEE 802.22 networks there are two special attacks that are primary user emulation attack (PUEA) and spectrum sensing data falsification attack (SSDF). PUEA means that a malicious SU identify itself as a PU and tries to gain priority over other SUs. Hence it utilizes a certain frequency band by itself. So that all the secondary users got false data about the network. In [17, 24, 25, 26], the authors proposed a methods to defense against PUEA. PUEA can be detected by analyzing the received signal strength and find the source of signal [17]. On the other hand, if the variation of transmitting power between PU and SU is insignificant, or the entities in CRNs are movable, this system is invalid. As per [24] and [25], PUEA can be

detected by cooperation and overcome by Neyman-Pearson composite hypothesis test. In [26], the authors detected the PUEA by extracting the variation of shadow fading as a channel parameter to detect the source of signal. In [27], the authors specified that there are two cooperative attackers. In PUEA attack, the two cooperative users adjust their transmit power respectively to duplicate the channel parameter to puzzle other SUs. Then this attack can be conquered by the joint decision of multiple SUs.

In [28], the authors detect the PUEA using belief propagation approach. In this strategy each SU calculates the local functions based on location information, broadcast the information with the neighboring nodes, and calculates the beliefs until convergence. Then, the PUEA will be sensed as per the mean of the final beliefs based on a threshold of belief. Subsequently all the SUs in the CRAHN will be broadcast the message on the characteristics of the attacker's signal, and avoid the attacker's signal in the future.

In [29], the authors proposed a new network layer attack called routing-toward-primary-user (RPU) attack in CRN. In this types of attack, the attacker nodes intentionally transmit a large amount of packets to PUs, which to cause interference to the PUs. This may increase time delay in the data transmission among the SUs. In this attack, the attacker claims the nodes to make problems in the data transmission, to which they forward the packets. It has been developed a strategy to defend in contradiction of RPU using belief propagation. In this approach each node in the route from source to destination is maintained a table which stores the feedbacks from the other nodes on the route and then broadcast feedback information and calculate beliefs. Finally, the source node can be detected the malicious nodes based on the final belief values. Hence this approach is reduced the data transmission delay and interference to PUs.

In [30], the authors proposed a protocol which provides privacy and confidentiality. The network entities authenticate each other using location information in CRNs. In [31], the authors are detected both malicious user and primary user in CRN using two parameters that are location reliability and malicious intention (LRMI). Location reliability is used to detect PU which reflect path-loss characteristics of the wireless channel. Malicious intention is used to detect the intention of SUs. In [32], the authors are proposed a new security approach for CR-MANET called as SCRAHN which elimination of SSDF attack in CRAHNs. It can be found the intruder nodes out of some neighbor node from the network. The authors in [33] has considered a parallel fusion network in which the nodes send their information to an access point which makes the final decision regarding presence or absence of the PU signal. They investigate the schemes to recognize the malicious users based on outlier detection techniques for a cooperative sensing system using energy detection at the sensors.

VI. Proposed Protocol

In this section, it has been discussed the adaptation of the trusted secondary node or user for in CRAHN to avoid different attacks of malicious node/ users and selfish nodes/ users.

In this segment, the proposed routing protocol CRAODV-S deliver the description of the routing protocol, by describing the route discovery and route maintenance process with secure channel in terms of trust value. The proposed secure protocol Cognitive Radio Ad hoc On-demand Distance Vector using Secure channel (CRAODV-S) is designed for efficient route discovery process using sets of trusted channel and compared with conventional CRAODV[38][39]. It has been deployed the essential functionality of control packets like RREQ, RREP, SU_RREQ, SU_RREP and HELLO, RERR similar to CRAODV. The PU-RERR and proper utilization of the spectrum by protocol have been also implemented.

The RREQ is announced by flooding and transmitted from nodes to other nodes in the network to find the route information during the route discovery. The originating node spreads a RREQ message to its neighbouring nodes, which communicates the message to their neighbour nodes and this process continues till it reaches to destination node in the CRAHN. A RREQ message is originated with defined time to live (TTL) and a specified hop distance by the originating node. If none of intermediate nodes has the route information of sink node, they retransmit the RREQ with a next hop number. This method continues till it reaches to the sink node. Then after it sends a RREP message to the originated node with the complete stored path information in it, which establishes the path from source to sink node and communicates the data through the established path. Nodes along with the path can be updated their routing table entries.

Now it has been discussed the route request by secondary users (SU_RREQ), which is important for CRAHN. It will verify whether a licensed channel is free from PU activities or not. After receiving a SU_RREQ message through the predefined channel it drop the RREQ packet if the licensed channel is not free from PU activity. Otherwise, it creates a reverse route through same channel. A node can keep numerous routes in CRAODV-S. The SU verifies the presence of a PU activity before transfer a packet using a channel. It sends a secondary user route reply (SU_RREP) to the source node using the same channel. Otherwise, it broadcasts a copy of the SU_RREQ message packet through the channel and it provides to check the duplicate SU_RREQ packet and discard it if found. Similarly, secondary user route reply (SU_RREP) is another control packet used in the CRAHN to reply the destination information regarding PU activity on a channel. The node updates the opposite path and sends SU_RREP through intermediate nodes in the CRAHN.

If any malicious node is available in the CRAHN, the route discovery process may be deviated by black hole attack or grayhole attack or selfish attack. To avoid this problem, it has been proposed to check the trust value of secondary user in the network. When intermediate nodes receive the SU_RREP through a free channel of any secondary users, it analyse the trust value of the secondary user using threshold values of lower limit time of route

reply message packet. The value of route reply time is less than the lower limit threshold value then the node is treated as malicious secondary node. This attack made by malicious node or user in terms of blackhole attack.

In blackhole attack, malicious users never send true messages. When the malicious user receives a secondary user route request (SU_RREQ) message, it sends immediately a false SU_RREP regarding PU activity on a channel assigning a high sequence number to settle in the routing table of the victim node, before other nodes send true ones. So, requesting secondary users assume that route discovery process is completed and ignore other SU_RREP messages and begin to send packets through the malicious secondary users. In this manner malicious node attacks all SU_RREQ message packets and packets are dropped without forwarding anywhere in CRAHN. This type of malicious users act as selfish nodes and their objectives are to make the jamming in the CRAHN and try to keep the PU's channel free from access by other SU. The said free channel of PU for can be accessed and used, when it requires. Similarly, it will check the grayhole attack of malicious secondary user/ node. The node initially forwards the packets and fails to do so afterwards. Initially the node replays true SU_RREP messages to nodes that initiate SU_RREQ message and it takes over the sending packets. After that, the node simply drops the received packets at its end to launch a denial of service (DoS). This is performed as routing misbehaviour in the CRAHN by malicious node or user.

It built up a path through the same free and secure channel of nodes to the source node as per the trusted value. Then it forwards the SU_RREP message along the opposite path using specified channel. The SU will update the onward path only if the new SU_RREP message is better and secure forward route received using the same channel.

Similar to route discovery process in the CRAHN the route maintenance process can be performed, as it is a vital role in routing protocol. There are two classes of route error (RERR) message in CRAODV-S. RERRs is one of them for topology alterations in such dynamic network as it is ad hoc in nature and other one is primary user (PU-RERRs) for handling activity of the PU. The node in the network cancels all the route records using an accessed channel and it notices the neighbour SUs that used licensed channel is inaccessible with a PU-RERR message when a PU activity is identified through a node in a same channel. The SUs get a packet nullify the used channel route entries whose succeeding hop is the PU-RERR sender. In this way, the SU nodes in the network affected by the PU activity must withdraw from the eventful channel. The PU-RERR packets are locally advertised and they will not allow to new route requests. When a node in the network detects a previously engaged channel becomes free, it re-evaluates the routing entries using the channel, so that received data may be forwarded along with such channel.

In this way the route discovery and maintenance can be performed using channel which make it more efficient and effective. The simulations have been carried out by using simulations through NS-2 [44], based on the CRCN integrated simulator [45] and evaluate the performance of protocol through throughput, end-to-end delay, packet delivery ratio and normalized routing load as per the following table.

TABLE-1: Simulation Parameters for CRAODV-S and CRAODV

S.No	Parameters	Values
1	Area size	500m x500 m.
2	PU Transmission range	250 m.
3	Simulation time	500 s.
4	Nodes speed	5 m/s
5	Pause times	5 s.
6	Data rate	5 Kbps
7	Mobility model	Random any point.
8	Interface	1
9	No. of channel	5
10	Numbers of SU Node	10,20,30,40,50,60,70,80,90,100
11	Numbers of PU Node	10
12	No. of Simulation	5

The parameters which are used to evaluate the performance of routing protocol can be obtained through the Trace Analyzer in NS2 are as follows:

The Normalized Routing Load (NRL) is used to calculate the total amount of routing overhead packets per total delivery packets in the network. The End-to-End delay shortly states as delay and refers as the average time taken to receive the data at destination node from source node in the network. The Packet deliver ratio (PDR) is used to calculate the average percentage of the ratio between the number of successfully received packets at destination nodes and the number of all packets sent by sources nodes. Generally, PDR is used to calculate the reliability and effectiveness of a routing protocol. The throughput is also taken to consideration the efficient of routing protocol and it is to calculate the rate at which a network receives data packets at receiver end.

VII. Result and Discussion

In this paper, trusted based secure node in the CRAHN has been calculated and makes the routing protocol more effective and efficient. It has been also tried to improve the packet delivery ratio and throughput, which denotes the efficiency and reliability of routing protocol and good channel efficiency.

As per fig.-2, the proposed routing protocol (CRAODV-S) has less routing load as compared to CRAODV. This indicates overhead is less as compared to base label cognitive radio routing protocol CRAODV. This indicates the packet collision is less in our proposed routing model in CRAHN environment. This is significantly better indication of proposed protocol for communication between the nodes via intermediate nodes including SUs in CRAHN.

As per fig.-3, the proposed routing protocol consumes less transmission time to transmit the data through intermediate nodes in the network as compared to conventional routing protocol CRAODV, from sender to receiver. This may cause of formation the better route using better channel selection process in a secure manner. The proposed secure routing model CRAODV-S in CRAHN shows better results in term of PDR as compared to conventional one (i.e., CRAODV) which is shown in fig.-4. Since end-to-end delay minimize with less overhead the efficiency and reliability of the proposed routing model is significantly better as compare to CRAODV. The system throughput has been also considered for better channel utilization for evaluation of routing protocols. It has been analyzed through the fig.-5 and found the performance in terms of system throughput of CRAODV-S is better as compared to CRAODV.

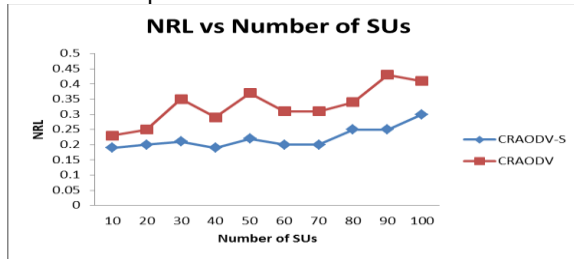


Fig.-2: NRL vs Number of SUs

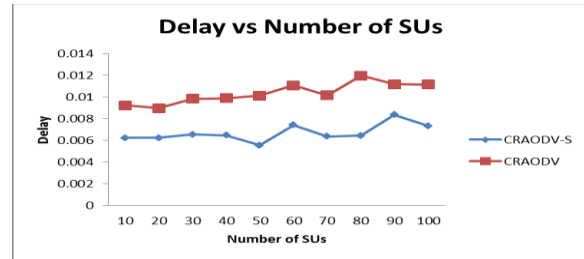


Fig.-3: Delay vs Number of SUs

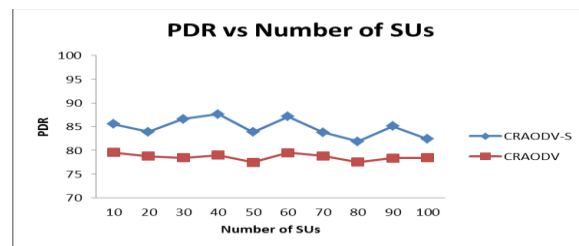


Fig.-4: PDR vs Number of SUs

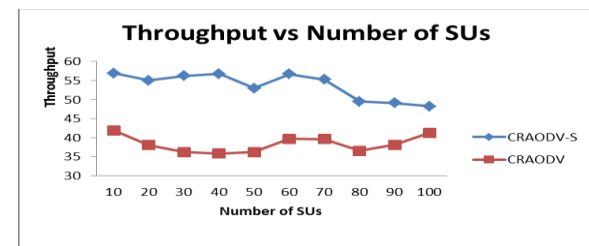


Fig.-5: Throughput vs Number of SUs

So it has been observed via different figures from 2 to 5 that, the proposed routing protocol CRAODV-S is better than conventional routing protocol i.e., CRAODV.

VIII. Conclusion

In this paper a proposed efficient and trusted based secure routing protocol CRAODV-S has been developed in the CRAHN. The proposed CRAODV-S in the CRAHN selects the trusted based reliable channel selection by using the malicious node detection process for better and secure route construction. Due to this efficient and secure channel through malicious node selection process, the route formation in proposed model CRAODV-S is better. It avoids jamming in the network system with more numbers of packet are transmitted as compared to conventional one. It improves the packet delivery ratio and throughput with minimum end-to-end delay and routing load as compared to an conventional routing protocol.

VI. References

- [1] O. Leon, J. Hernandez Serrano, and M. Soriano, "Securing Cognitive Radio Networks", International Journal of Communication Systems, 23:633-652, February 2010.
- [2] Beibei Wang, Yongle Wu, K.J. Ray Liu, "Game theory for cognitive radio networks: An overview", Elsevier Computer Networks, pp-2537-2561, April 2010.
- [3] Chen R, Park J-M, Hou YT, Reed JH., "Toward secure distributed spectrum sensing in cognitive radio networks", IEEE Communications Magazine, Special Issue on Cognitive Radio Communications 2008, b:50-5.
- [4] Tan X, Borle K, Du W, Chen B., "Cryptographic link signatures for spectrum usage authentication in cognitive radio", fourth ACM conference on wireless network security Hamburg, Germany; 2011. pp. 79-90.
- [5] Zhu L, Mao H., "An efficient authentication mechanism for cognitive radio networks", in pceedings of power and energy engineering conference (APPEEC) Wuhan, 2011, pp. 1-5.
- [6] Zhou D., "Security issues in Ad Hoc networks. Boca Raton", FL, USA: CRC Press, Inc.; 2003
- [7] Miller R, Wenyuan X, Kamat P, Trappe W., "Service discovery and device identification in cognitive radio networks", 4th annual conference on sensor mesh and Ad Hoc communications and networks- 2007, (SECON-07), San Diego, CA; 2007. pp. 670-7.
- [8] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002.
- [9] Winget NC, Housley R, Wagner D, Walker J., "Security flaws in 802.11 data link protocols", ACM Communications Magazine (Wireless networking security) 2003:35-9.
- [10] FIPS, Specification of the advanced encryption standard (AES). Federal Information Processing Standards Publication; 1987.
- [11] Schneier B., "Applied cryptography: protocols, algorithm, and secure code in C", New York, USA: JohnWileyandSons, Inc.; 1996.

- [12] Mathur CN, Subbalakshmi KP., "Security issues in cognitive radio networks", Cognitive networks: towards self-aware networks, John Wiley and Sons, Ltd; 2007 [chapter 11].
- [13] Shaukat, R. Khan, S.A. Ahmed, A., "Augmented Security in IEEE 802.22 MAC layer Protocol", 4th IEEE International Conference on Wireless Communications Networking and Mobile Computing, 2008. WiCOM 08..
- [14] KaiguiBian and Jung-Min, "Security Vulnerabilities In IEEE 802.22", ACM 4th Annual International Conference on Wireless Internet.
- [15] Khan, S., Loo, K., Naem, T., & Khan, M.A. Denial of service attacks and Challenges in broadband wireless networks. IJCSNS International Journal of Computer Science and Network,(2008).
- [16] R. Chen and J. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," IEEE Workshop on Networking Technologies for SDR 2006.
- [17] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Journal on Selected Areas in Communications, 2007.
- [18] Clancy, T.C., & Goergen, N., "Security in Cognitive Radio Networks: Threats and Mitigation. Laboratory for Telecommunications Sciences", US Department of Defense, Retrieved from <https://www.cs.umd.edu/~clancy/docs/cr-crowncom08.pdf>. (2008).
- [19] Akyildiz IF, Lee WY, Vuran MC, Mohanty S., "A survey on spectrum management in cognitive radio networks", IEEE Communications Magazine 2008, pp. 40-8.
- [20] Naveed A, Kanhere SS., "Security vulnerabilities in channel assignment of multiradio-multi-channel wireless mesh networks", In: Proceedings of IEEE conference in global telecommunications, GLOBECOM; 2006a. pp. 1-5.
- [21] Sazia Parvin a, FarookhKhadeerHussain b,n, OmarKhadeerHussain a, SongHan a, BimingTian a, Elizabeth Chang "Cognitive radio network security: A survey", Journal of Network and Computer Applications, Elsevier,2012.
- [22] Hanen Idoudi, Kevin Daimi, and Mustafa Saed, "Security Challenges in Cognitive Radio Networks" Proceedings of the World Congress on Engineering 2014 Vol I, WCE 2014, July 2 - 4, 2014, London, U.K.
- [23] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding- Royer, "A Secure Routing Protocol for Ad Hoc Networks", Supported in part by National Science Foundation awards ANI-522564 and EIA-0080199, and in part by U.S. Department of Justice.
- [24] Z. Jin, S. Anand, K.P. Subbaiahshmi, "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks", Proc. of New Frontiers in Dynamic Spectrum Access Networks, pp. 14-17, Oct. 2008.
- [25] Z. Jin, S. Anand, K.P. Subbaiahshmi, "Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks Using Hypothesis Testing," ACM SIGMOBILE Mobile Computer and Communications Review 1, vol. 13, no. 2, pp. 74-85, Apr. 2009.
- [26] Z. Chen, C. Todor, C. Chen, P.R. Carlos, "Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks," Proc. Of IPCCC'2009, pp. 208-215, Dec. 2009.
- [27] Tianhong Yang, Huifang Chen, Lei Xie "Cooperative Primary User Emulation Attack and Defense in Cognitive Radio Networks" IEEE 2011.
- [28] Zhou Yuan, Dusit Niyato, Husheng Li, Ju Bin Song, and Zhu Han "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 30, NO. 10, pp 1850-1860, NOVEMBER 2012.
- [29] Zhou Yuan, Zhu Han, Yan Lindsay Sun, Husheng Li, and Ju Bin Song "Routing-Toward-Primary-User Attack and Belief Propagation-Based Defense in Cognitive Radio Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 9, pp 1750-1760, SEPTEMBER 2013.
- [30] Kim HS. "Location-based authentication protocol for first cognitive radio networking standard. Journal of Network and Computer Applications", 2011;34(4): 1160-7.
- [31] Shraboni Jana, Kai Zeng, Wei Cheng, and Prasant Mohapatra, "Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 9, SEPTEMBER 2013.
- [32] Yufang Cheng, Jian Zhou, "S-CRAHN: A Secure Cognitive-Radio Ad-Hoc Network" HCTL Open Science and Technology Letters, Volume 6, August 2014.
- [33] Praveen Kaligineedi, Majid Khabbazi, Vijay K. Bhargava, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 8, AUGUST 2010.
- [34] Sanket S. Kalamkar and Adrish Banerjee, Ananya Roychowdhury, "S. Kalamkar, A. Banerjee, and A. Roychowdhury, "Malicious user suppression for cooperative spectrum sensing in cognitive radio networks using Dixon's outlier detection method," in Proc. National Conf. Commun., (IIT Kharagpur, India), pp. 1-5, Feb. 2012.
- [35] Deng, H., Li, W., Agrawal, D. "Routing Security in Wireless Ad Hoc Networks", IEEE Communication Magazine, pp. 70-75, 2002.
- [36] Marti, S., Giulì, T.J., Lai, K. and M. Baker., "Mitigating routing misbehavior in mobile ad hoc networks", Mobile Computing and Networking, MobiCom-2000, pp.255-265, 2000.
- [37] G. Vigna, S. Gwalani and K. Srinivasan, "An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks", Proc. of the 20th Annual Computer Security Applications Conference (ACSAC'04).
- [38] Sangita Pal, Srinivas sethi, "Selection of Reliable Channel by CRAODV-RC Routing Protocol in Cognitive Radio Ad Hoc Network", Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2, Volume 338 of the series Advances in Intelligent Systems and Computing pp 251-259.
- [39] Sangita Pal, Srinivas sethi, "Effective Routing Protocol in Cognitive Radio Ad Hoc Network using Fuzzy-based Reliable Communication Neighbor Node Selection", Springer FICTA-2013, India
- [40] C.E. Perkins, E.M., Belding-Royer, and S.R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing, Internet Draft, draft-ietf-manet-aodv-13.txt, Feb. (2003).
- [41] Angela Sara Cacciapuoti, Cosimo Calcagno, Marcello Caleffi, Luigi Paura :CAODV: Routing in Mobile Ad-hoc Cognitive Radio Networks, Wireless Days,pp:1-5, (2010).
- [42] Angela Sara Cacciapuotia, Marcello Caleffia, Luigi Paura,: Reactive routing for mobile cognitive radio ad hoc networks, Ad Hoc Networks, Volume 10, Issue 5, pp: 803-815, (2012).
- [43] Shelly Salim and Sangman Moh, : On-demand routing protocols for cognitive radio ad hoc networks, EURASIP Journal on Wireless Communications and Networking Regular submissions, pp: 1499-2013, (2013)
- [44] NS-2 Manual, (2009)
(<http://www.isi.edu/nsnam/ns/nsdocumentation.htm>)
- [45] CRCN integrated simulator.