IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 70-72

An Overview of Security Attack in Cognitive Radio Ad Hoc Network (CRAHN)

J.Ramkumar[1], Dr. R.Vadivel[2]
[1]*Asst Prof, Department of Computer Science, VLB Janakiammal College of Arts and Science, Coimbatore.*
[2]*Asst Prof, Department of Information Technology, School of Computer Science and Engineering, Bharathiar University, Coimbatore*

Abstract: - *Cognitive radio technology is engaging the development of Dynamic Spectrum Access (DSA) model which is envisioned to deal with the present spectrum shortage issue by empowering the contraption of new remote organizations. Cognitive gadgets have the comparable capability of CR and the network that they frame powerfully is called Cognitive Radio Ad Hoc Networks (CRAHNs). Because of predefined characteristics of wireless channels, security became a benchmark issues in CRAHN. The intention of attacks in CRAHN is not only to threaten the data, but also to reduce the network performance. The main objective of this paper is to discuss about various recent proposals and new types of attacks in CRAHN.*
Keywords: - *ad hoc network, attack, cognitive radio networks, routing, security*

I. INTRODUCTION

Cognitive Radio (CR) is a radio based technology which can change its transmitter parameters in pacific community with surroundings, wherein it firmly perform. In controlling an CR in a straightforward way, it will indisputably be software narrated radio nor being substance programmable are essentials of a CR. CR is an embodiment design of remote networking that senses its surroundings, trace the updating and commonly barter message with their networks. Adding this feature of understanding the network of ad hoc by a glance to the geo-location based network is known as cognitive radio ad hoc network (CRAHNs). CRAHN aims to improve the way the radio spectrum is utilized. The four basic functions [1] of CR networks are: (a) Spectrum Sensing (detects all the available spectrum holes in order to avoid interference); (b) Spectrum Sharing (shares the spectrum related information between neighbor nodes); (c) Spectrum Mobility (provides seamless connectivity between nodes); (d) Spectrum Decision (captures the best available vacant spectrum holes from detecting spectrum holes).

Routing is the procedure of choosing the best path in a network. CRAHN faces numerous security vulnerabilities because of its natural characteristics such as reliability, mobility and scarce resources. The major problems in the design of protocol for CRAHN are security, less delay tolerance, reduced throughput which results in poor packet delivery ratio. The above mentioned setbacks are due to the ineffective detection of spectrum nodes that are unlicensed devices (secondary users) have to quit the spectrum band once the licensed device (primary user) is detected. Protocols designed for CRAHNs are entirely different from those for traditional networks.

Objectives of this paper are: - (i) to survey the recent proposals made on security issues in CRAHN, and (ii) to discuss the security attacks that intents only on CRAHN.

The paper is organized as follows. This section introduces CRAHN, problem statement and objectives of this research paper. Section 2 provides the summary of the related works as review of literature. Section 3 discusses on security attacks intent only on CRAHN. Section 4 concludes the paper with future dimension.

II. LITERATURE REVIEW

A directional antenna concept [2] for smart environments was proposed to exchange cognitive control information whereas directional opportunistic PU free channel is used for application data transmission. Key managing concept namely composite trust-based public key management [3] with the goal of maximizing performance while mitigating security vulnerability, where each node employs a trust threshold to determine whether or not to trust another node. A classification was made on the attacks [4] that target the network layer functionalities of cognitive radio networks, also existing detection techniques, countermeasures and highlight the main security challenges were discussed. The importance of multi-objective optimization in cognitive radio networks were discussed in [5], where fundamental differences between single objective and multi objective optimization were also discussed. A differentiation was given between the possible relations such as, conflicting, supporting and design dependent, among these objectives. An adaptive strategy for robust dynamic

spectrum access [6] was proposed for the event of induced attacks. It was assumed that a rational player consider the notion of channel utility and the optimal strategy.

A review on classification [7] on hybrid routing mechanisms and categorize it into four mesh, tree, zone, and multipath structure with their relative performance, where it also compares routing mechanisms against routing efficiency, reliability, packet delay, packet delivery ratio, control overheads, and QoS (Quality of Service). Spectrum sensing data hijack [8] a proposal on discovery of novel attack was reported to disguise as routers to hijack and tamper with spectrum sensing data during the transmission. Hybrid control channel based cognitive AODV routing protocol [9] with directional antennas was proposed to discover the channel-route from the source to the destination that was connected within the Cognitive Radio Networks. An adaptive trust-Stackelberg game model [10] was designed to improve the energy efficiency and defend against insider attacks in CRNs, where a demonstration was made on the utility and comparison was done with other models using a numerical investigation. A trust-based multi-hop cooperative spectrum sensing method [11] was proposed to deal with falsifications attack.

III. ATTACKS FACED BY CRAHN:

More the security solutions provided by the researcher, attacks are being proposed by attacker to gain advantage. It's our duty to study about new and trending security attacks rather than the old traditional type of attacks and be safe from stacks. This section discusses about the different variety of trending attacks in CRAHN.

- ✓ Egotistical Attacks: An egotistical attack happens in a circumstance where the aggressor needs to utilize the spectrum with higher preference. This kind of attack meets its objective by deceiving other unlicensed clients to trust he is an authorized client. Therefore, the ill-disposed client can misuse the spectrum as long as he or she needs. Since this egotistical conduct does not comply with the spectrum sharing plan, it is considered as egotistical attack.
- ✓ Malicious attack: This attack implies that the foe keeps other unlicensed clients from utilizing the spectrum and causes a denial of service (DoS) attack. As a genuine outcome, malicious attack will definitely diminish the accessible bandwidth and separate the entire activity.
- ✓ Spectrum Manger Attacks: It isn't shrewd to utilize just a single spectrum administrator for relegating recurrence groups as it might be a solitary purpose of disappointment on the system. Spectrum manager is playing an important role between cognitive radio nodes, because without spectrum manager communication is not possible. Therefore, the spectrum accessibility ought to be circulated and repeated in CRNs.
- ✓ Purposeful Congesting Attack: This is a standout amongst the most fundamental sorts of attack that can be done by SUs in CRNs. The malignant SU congests essential and other optional clients by purposefully and persistently transmitting in an authorized band [12]. This attack can be more severe and unsafe in CRNs by a rare SU.
- ✓ Essential Beneficiary Congestion Attack: In CRAHNs, an absence of information about the area of essential recipients can be utilized by a pernicious element to purposefully make hurtful impedance a casualty essential collector. This attack happens at whatever point a malicious SU moves near to the casual beneficiary user and misusing the available spectrum.
- ✓ Spectrum Sensing Attack: Few PU recognition systems have higher sensitivity towards essential transmissions with a view to counteract impedance to the essential system. SUs are defenseless against this type of attack, where this attack prompts to visit false location and missed on chances.
- ✓ Overlapping Attack: In concentrated and circulated designs of CRAHNs, different networks may exist together over the same land area. Data transmissions from vindictive elements can hurt SU and PU in the network, as well as of different CRAHNs.
- ✓ One-sided Utility Attack: CRAHNs vulnerable to malicious SUs, who can deliberately change parameters of the utility capacity to build his/her bandwidth. In this attack, SU are tuned to not identify this malignant conduct, this may chunk the data transmission for different SUs.
- ✓ Asynchronous Sensing Attack: A malignant SU intends and transfer the data asynchronously as opposed to synchronizing the detecting action with different SUs in the system amid detecting tasks. It results to botched chances at whatever point the base station or different SUs in CRAHNs think about this occasion as a genuine transmission from a PU.
- ✓ False Opinion Attack: False input from one or a gathering of malevolent uses could make different SUs make wrong move and abuse the terms of the convention. There exists a lot of chance to get happen in centralized and decentralized structures in CRAHNs.
- ✓ Authorized Client Copying Attack: All CRAHNs are designed to utilize the authorized spectrum when it is available, otherwise it will utilize the unlicensed band. The attacker may create congestion towards the

authorized band and copy the PU, along these lines constraining the CRAHN to working in the unlicensed groups and restricting CRN limit.

- ✓ Channel Controlling Attack: For this situation, the attacker sends periodical data packets in the control channel spectrum. The congestion in one channel obstructs the communication between all nodes of different CRAHN.
- ✓ Spectrum Detecting Information Adulteration Attack: In this attack, an attacker may send false neighborhood spectrum detecting results to an information gatherer, making the information authority to take a wrong spectrum detecting choice.

IV. CONCLUSION

CR is an embodiment design of remote networking that senses its surroundings, trace the updating and commonly barter message with their networks. There exists no end for the security attacks in wireless network, where CRAHN is one among them. Even though multiple proposals are proposed towards the security attack in CRAHN, but still it is not said that there exist no security attacks. This paper discussed the recent proposals made towards avoiding the attacks in CRAHN with different kinds of recent attack and also with an introduction about CRAHN. Future dimension of this research work can be tending towards a solution of avoiding attacks in proactive manner rather than reactive manner.

REFERENCES

[1]. Jaime Lloret Mauri, Kayhan Zrar Ghafoor, Danda B. Rawat, and Javier Manuel Aguiar Perez, *Cognitive Networks: Applications and Deployments, CRC Press*, 2015, pp: 203-235.

[2]. Anil Carie, Mingchu Li, Satish Anamalamudi, Prakash Reddy, Bhaskar Marapelli, Hayat Dino, Wahab Khan, and Waseef Jamal, *An internet of software defined cognitive radio ad-hoc networks based on directional antenna for smart environments, Sustainable Cities and Society, Volume 39*, 2018, Pages 527-536.

[3]. Jin-Hee Cho, Ing-Ray Chen, Kevin S. Chan, *Trust threshold based public key management in mobile ad hoc networks, Ad Hoc Networks, Volume 44*, 2016, Pages 58-75.

[4]. Mounia Bouabdellah, Naima Kaabouch, Faissal El Bouanani, and Hussain BenAzza, *Network layer attacks and countermeasures in cognitive radio networks: A survey, Journal of Information Security and Applications, Volume 38*, 2018, Pages 40-49.

[5]. Muhammad Rashid Ramzan, Nadia Nawaz, Ashfaq Ahmed, Muhammad Naeem, Muhammad Iqbal, and Alagan Anpalagan, *Multi-objective optimization for spectrum sharing in cognitive radio networks: A review, Pervasive and Mobile Computing, Volume 41*, 2017, Pages 106-131.

[6]. Saad Mneimneh, Suman Bhunia, Felisa Vázquez-Abad, and Shamik Sengupta, *A game-theoretic and stochastic survivability mechanism against induced attacks in Cognitive Radio Networks, Pervasive and Mobile Computing, Volume 40, 2017*, Pages 577-592.

[7]. Gyanappa, A. Walikar, and Rajashekar C. Biradar, *A survey on hybrid routing mechanisms in mobile ad hoc networks, Journal of Network and Computer Applications, Volume 77*, 2017, Pages 48-63.

[8]. Jingyu Feng, Guangyue Lu, Honggang Wang, and Xuanhong Wang, *Supporting secure spectrum sensing data transmission against SSDH attack in cognitive radio ad hoc networks, Journal of Network and Computer Applications, Volume 72*, 2016, Pages 140-149.

[9]. Satish Anamalamudi, Abdur Rashid Sangi, Mohammed Alkatheiri, and Ahmedin Mohammed Ahmed, *AODV routing protocol for Cognitive radio access based Internet of Things (IoT), Future Generation Computer Systems, Volume 83*, 2018, Pages 228-238.

[10]. He Fang, Li Xu, Jie Li, Kim-Kwang Raymond Choo, *An adaptive trust-Stackelberg game model for security and energy efficiency in dynamic cognitive radio networks, Computer Communications, Volume 105*, 2017, Pages 124-132.

[11]. Adele Khalunezhad, Neda Moghim, and Behrouz Shahgholi Ghahfarokhi, *Trust-based multi-hop cooperative spectrum sensing in cognitive radio networks, Journal of Information Security and Applications, Volume 42*, 2018, Pages 29-35.

[12]. Mathur, and Subbalakshmi . (*Cognitive networks: towards self-aware networks*. John Wiley and Sons, Ltd; 2007).