International Journal of Scientific Research & Engineering Trends
Volume 5, Issue5, Sept-Oct-2019, ISSN (Online): 2395-566X

A Secure Iot Communication against Reactive Jamming Attack in CRN Subtitle

Nitesh Yadav
Department of Electronic and Communication
Technocrats Institute of Technology
Bhopal, India

Dr. Abhishek Bhatt
Department of Electronic and Communication
Technocrats Institute of Technology
Bhopal, India

***Abstract* - The number of nodes or IoT devices is sense and control the communication. The primary users are more trustworthy than the secondary users, since these are authorized or licensed users. The purpose of CRN is to intellect the spectrum band and identify the free channels which will be used for un-authorized access user or attacker that flooded the unwanted packets to next node or destination node in network. CRN get better the efficiency of spectrum handling, but it also performance degrades due to new security threats with jamming attacks during the spectrum sensing process, which can corrupt the effectiveness of spectrum sensing. In this research we proposed security scheme against packet flooding Jamming attack. The performance is vitiated in high, medium and low jamming probability and applies the proposed scheme to reduces the flooding. The hop count value based on forward and reverse mechanism of detection and provides secure communication in IoT CRN . The reliability of link is equivalent from the forward and reverse path consistency i.e. more in proposed security scheme as compare to with Batch based SA-MAC scheme. The proper packet forwarding in particular link and the reverse and forward is counted properly but correctly, current node are in suspicious. The record value of hop count is based on the packets receiving but heavy flooding is also disturb it at starting connection establishment procedure.**

***Keywords*- IoTCRN, stations, Security, Routing, Jamming attack, hop count.**

I. INTRODUCTION

In the world of networking, spectrum is taken into account a decisive and important resource. Most of the spectrum required for wireless communication has been assigned. However, there's proof indicating that copious segments of the radio-frequency spectrum don't seem to be deployed for a considerable period of your time [1]. The interconnected “things” such as sensors or mobile devices, monitors collects all kinds of data about human social life.

These data can be further aggregated, fused processed, analyzed and mined in order to extract useful information to enable intelligent and ubiquitous services [2]. IoT is a rapidly emerging paradigm in which the essential concept is that a great variety of objects are instrumented in such a way that they can be queried and operated over the Internet either directly by the users or by programs that encapsulate their behavior and objectives [3].

Services of Internet of Things (IoT) have been emerging into markets in broad areas, e.g., surveillance, health care, security, transport, food safety, and distant object monitor and control This has piloted the innovation of psychological feature radio technology as an answer for the inconveniences created as results of this fastened spectrum allocation [4]. Security aspect in IoT includes the Internet security network that is used during the communication process. Plentiful alternative solutions can be used to secure the object or network in the IoT. For securing the network purpose, also use encryption mechanisms. Whereas to securing the object we can use hardware that have ability to resist the attacks instead of making some trustable objects. [5]. Jamming attack is a particular attack on a network or a computational resource, and the effect of attack may contribute to the reduction in network capacity.

It will enhance spectrum effectiveness through handling inefficient usage of authorized spectrum since radio instrumentation can determine the spectrum accessibility among their surroundings and invest the unused spectrum (spectrum holes) by authorized primary users Countermeasures are required to make sure secondary users of the spectrum and first users (incumbents) are totally protected. (PU) and allocate it to secondary users (SUs) [1,6].

Cognitive radio relies on the thought of permitting unlicensed users to use authorized bands whereas safeguarding the priority of primary authorized users. Cognitive Radio Networks (CRNs) are therefore composed of 2 styles of users, authorized 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

permitting them to find obtainable channels and change to them whenever they're not utilized by a primary user. Secondary users got to cater for the highest priority of PUs by detecting their presence and terminating their communications instantly to avoid any interference with PUs.

Cognitive Radio Networks (CRN) emerged as a paradigm to handle these issues. In CRN, wireless nodes modification their parameters to speak with efficiency, avoiding interference with authorized (primary users (PUs)) or unlicensed users (secondary users (SUs)). This alteration of parameters relies on watching the radio surroundings, like the frequency spectrum, user behavior, and network state. CRN are composed of cognitive, spectrum responsive IoT devices capable of fixing their configurations on the fly supported the spectral surroundings. This capability disclose the chance of designing versatile and dynamic spectrum access ways with the aim of opportunistically reusing parts of the spectrum quickly vacated by authorized PUs [7]. On the opposite hand, the pliability within the spectrum access part comes with an multiplied quality within the style of communication protocols at completely different layers..

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. The recent advance and future direction with respect to applications [8] of CRN are mentioned below:-

- 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.
- 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.

III. LITERATURE SURVEY

There are many more different efficient techniques, which are proposed by various researchers in security from attacks of IoT devices in CRN. The some of the latest work are discuss in this chapter.

In this paper [9], they focus on how to enable CRIoT networks to function under channel unavailability security threats. This work presents a solution to compute the most secured channel assignment while maximizing the number of served devices with minimum packet-invalidity probabilities with four design constraints like spectrum occupancy, hardware, interference, and invalidity probability. The proposed solution addresses the jamming issue at the level of the CR MAC-layer level and relieves CRIoT network from implementing additional capabilities whether at the level of the IoT devices or controllers. new communication protocols and mechanisms are needed to inherently mitigate jamming attacks in IoT architectures with minimal additional resources and overhead.

In this paper [10], they present the DIO suppression attack, which can severely degrade the routing service in RPL. The DIO suppression attack induces victim nodes to suppress the transmission of DIO messages, which are the RPL messages necessary to build the routing topology. This causes a general degradation of the routes' quality that can lead, eventually, to network partitions. Unlike other RPL attacks in the literature, the DIO suppression attack does not require the adversary to forge bogus RPL messages. It is sufficient that she periodically replays previously heard messages. The attack can thus be mounted without stealing cryptographic keys from legitimate nodes. The DIO suppression attack uses the replay technique, which is a classic attack technique, for a radically different purpose. Indeed, the replay technique is usually used to make a victim accept old information as new. On the other hand, in the DIO suppression attack it is used to make a victim believe that the routing information it is about to send is already being transmitted many times by other nodes.

In this paper [11], proposed approach concentrates on attacks that actively try to omit crucial communication between nodes. First , trust is implemented in a centralized manner then second distributed approach to collect and evaluate the trust values from the network and third is reduces the surveillance of nodes. For reduce the computing efforts for the small devices, we use a trust management technique. That enables IoT devices to build up a measurement about the trustworthiness of adjacent nodes in a resource-friendly way. For that, the neighbors

are monitored and depending on positive and negative experiences, trust values are built. In addition, one can use special trust management policies which, for example, exclude certain nodes when their trust values display malicious behavior.

In this paper [12], they propose a novel lightweight authentication scheme for heterogeneous WSNs in the context of IoT. The scheme authenticates each object and establishes a secure channel between the sensor node and the remote user. It provides authentication with less energy consumption, protects the sensor node identity from disclosure, and terminates with a session key agreement between a sensor node and a remote user. The scheme provides also mutual authentication and a high security level against several attacks. The proposed communication system enables collected data from a sensor node to be transmitted directly to the mobile remote user after a successful mutual authentication between a sensor node and the remote user.

In this paper[13], they investigate the secure transmission from a source (e.g., surveillance camera) to a destination (e.g., controller) in the IoT with non-colluding unknown eavesdroppers. We assume that the locations of eavesdroppers are randomly distributed according to homogenous PPP. Besides the source and the destination, a relay (e.g., sensor node) is employed to retransmit the secret message. They concentrate on the single antenna system where all the devices including eavesdroppers are equipped with the single antenna. With the assumption that the locations of eavesdroppers change independently from hop to hop, we derive an expression for the secrecy outage probability of the two-hop transmission, which is shown to be the upper bound of the outage probability when the locations of eavesdroppers remain unchanged. Following this expression, we formulate a secrecy rate maximization problem with the secrecy outage probability constraint. The optimal rate design for codebooks and power allocation between the source and relay are derived

In this paper [14], proposed a consistent Advanced Encryption Standard (AES) assisted Digital TV or DTV scheme, where an AES encrypted reference signal is produced at the TV transmitter and used as the synchronous bits of the DTV data frames. By consent to a mutual secret between the transmitter and the receiver, the reference signal can be reinforce at the recipient end and used to accomplish precise identification of authoritative prime users. It is revealed that with the AES assisted DTV scheme, the prime user, as well as attacker or malicious user, can be perceive with high accuracy and low false alarm rate under primary user emulation attacks.

IV. MALICIOUS NODES PRESENCE ISSUE IN CRNIOT

A malicious user can try to falsify the spectrum occupancy information, which may cause interference. Besides, CRNs not only face all the security threats in traditional wireless networks, such as eavesdropping, tampering, imitation, forgery, and noncooperation etc., but also new security threats related to unique cognitive characteristics, such as primary user emulation attack, falsifying data, denial of service attack etc. Security vulnerability in cognitive radio technology becomes an unavoidable challenge which diverts the attention of present researchers towards it.

As CRN operates in wireless media, i.e., 'through the air' using radio frequency, it faces all the traditional wireless network security threats. In addition, CRN introduces significant new classes of security threats and vulnerabilities due to its unique characteristics and functioning techniques. The former have been broadly studied in the literature covering traditional wireless security [36] and therefore we have mainly focused on the latter. Thus, the proper detection and initiating countermeasure against those security threats is a major issue of CRN with keeping the basic security goals in mind, i.e., preserving confidentiality, ensuring integrity, and maintaining availability of the information (CIA).

V. PROPOSED SCHEME TO SECURE CRNIOT

The proposed security scheme i.e. proposed flooding based identification is based on the routing history of unwanted packets forwarding in network as well as check hop count value of . In presence of jamming attack in IoTCRN is not able to recognize the attacker presence because it is busy to control the different IoT nodes communication. The spectrum sensing allocation and use is the main purpose of CRN. The attacker identification is based on forwarding function and this function is applied on an intermediate node because data is almost sending to intermediate node. The trust of nodes is calculated from proposed security scheme for CRN. The value of the x is based in the number of hops are existing in between sender and receiver in network.

Algorithm: Secure Cognitive Radio Network against jamming Attack

Input:

M: IoT devices or Nodes
S: Sender node
D: Destinationr node
I: Intermediate nodes
Channel Assign Policy: CRNs
Pu: Primary User
Su: Secondary User

rp: AODV
Pi: Security Provider nodes
p: path length (forward) {1 to n}
q: path length (reverse)
x: Nodes in Shortest path
Rr: Radio range 550 Meters
Output: Throughput, Attacker flooding
While PVi detect x flooded unwanted data & q != m do
Set as suspicious node
Ensure x profile by PVi
If x_id != D_id than
PVi set x as Flooding unwanted data
Confirm detected x as attacker
Confirm x block by PVi node
message of attacker is broadcast to all M
Call local route repair
Research route again without contribution of x node
End if
End While

This data concerning wrongdoer is predicated on the output of used spectrum but because of alternative reason like common channel and joint spectrum sensing also attainable to not use full utilization of spectrum and spectrum hole utilization is additionally impossible. The packet flooding assaulter is that the attacker that forwards the wrong data of destination to sender by that sender is prepared to transmit information to receiver through region node. If the packet flooding attacker node is receives the information packets and flooded unwanted packets in network. However the most reason reliable ness of a packet flooding node is it forwards the request packets however not information packets.

VI. SIMULATION PARAMETERS

The simulation result is evaluated on the basis of performance parameters mentioned in Table 1. In NS-2 simulator version NS-2.31[15] is used to simulate all the modules. The following simulation parameters are used to make the scenario of routing protocols. The detailed simulation model is based on NS-2 is used in the evaluation.

Table 1. Simulation Parameters

Parameters	Value
Network Type	CRCN-IoT
Nodes/Devices	100
Physical Medium	Wireless
Simulation Iteration	500
MAC Layer	SMAC, Macng
Routing Protocol	AODV
Traffic Type	CBR, FTP
Number of Connection	Random
Propagation radio model	Two ray ground
Rate	10 Packet/s

VII. RESULT DESCRIPTION

The simulation result in presence of jamming attack with existing scheme and proposed flooding based scheme are evaluated on the basis of performance metrics. The proposed scheme performance is secure the communication between IoT devices and provides secure communication in CRN.

1.Server Jamming Attack Analysis

The Secondary User (SU) or jamming attacker aim in network is only to flooding the large amount of data or drop whole data packets that are transfer in between sender and receiver. The throughput performance is measures at higher jamming rate in network. The communication between in sender and receiver is properly shows the better receiving of data in network. In previous scheme performance measurement is low as compare to proposed flooding identification based scheme. The delay is enhanced by unwanted packets flooding in IoTCRN is more because of that the spectrum utilization is enhance and signals jamming consumes fully frequency band.

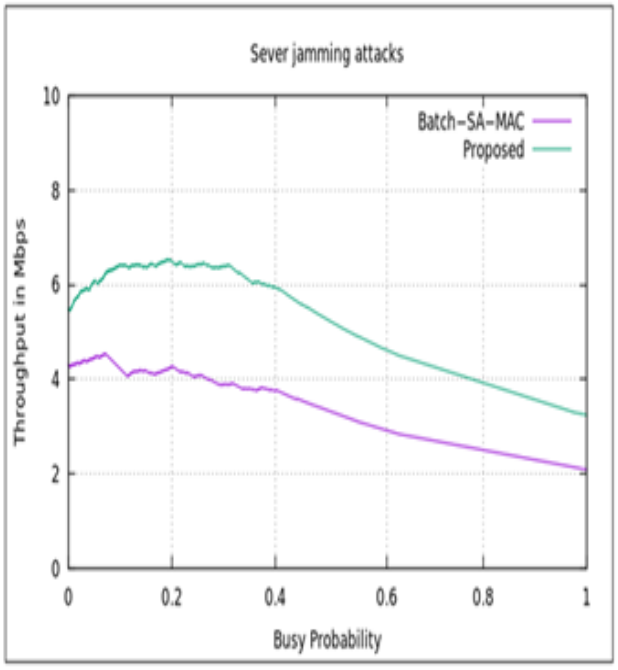

Fig.1. Server Jamming Attack Performance Analysis.

2. Moderate Jamming Attacks Analysis

The moderate jamming attacker means the flooding is reduced and its effect is shows in graph the throughput is also enhances. The secondary user is jamming attacker and these users are un-licensed users.

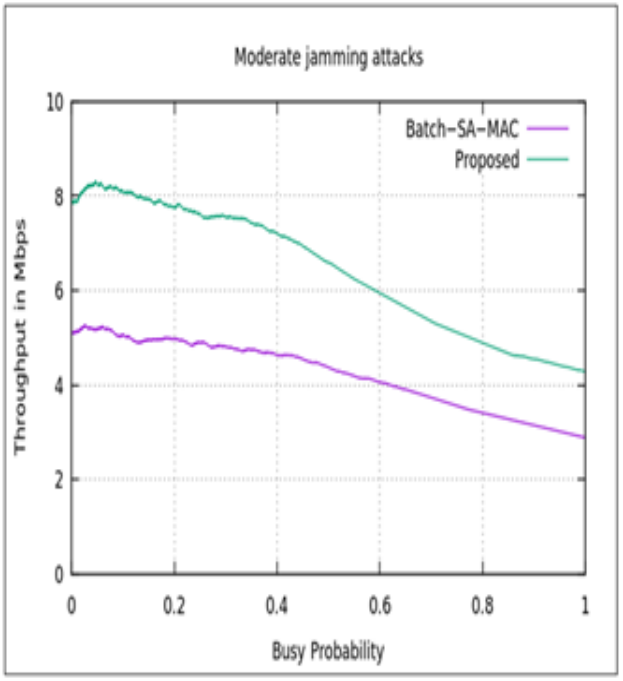

Fig.2 Moderate Jamming Attack Performance Analysis.

If the spectrum having free range of frequencies is assigning by spectrum holes to SUs. The PUs is not in front of the trouble in sending data to receiver through licensed. In this graph the performance of previous Batch-SA-MAC and proposed flooding based identification scheme is compare and the throughput of proposed scheme is more. The jamming of signals are also consumes the fixed bandwidth and due to unwanted flooding throughput is degrades.

3. Light Jamming Attack Analysis

The performance of proper data receiving is evaluated through throughput metrics. The Secondary Users are communicated to receiver in network. The Primary User's performance is also well collected to secure communication between PUs and SUs. The performance of proposed jamming identification based scheme is reduces the throughput as match up to Batch-SA-MAC scheme in IoTCRN. The performance of proposed scheme provides the 8.5 Mbps throughput performance. As compare to Batch-SA-MAC proposed performance busy probability is more than 0.3. The low or high rates of frequency are arrived at destination correctly in CRN.

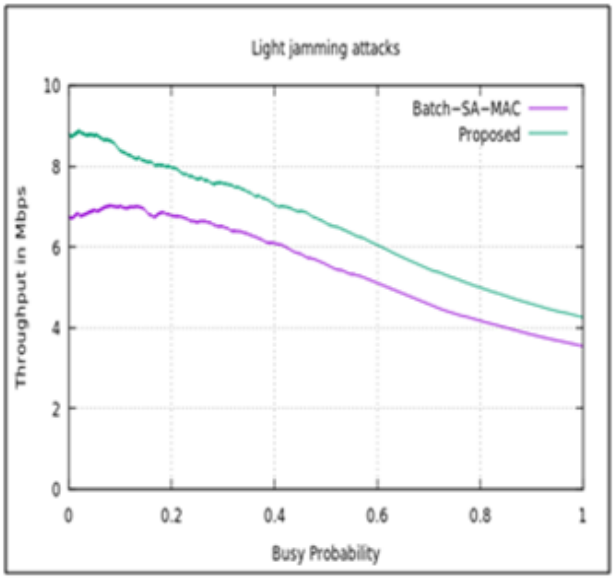

Fig.3. Light Jamming Attack Performance Analysis.

4. High PR Activity Analysis

The successful data receiving in any network is shows the possibility of better performance. In this graph the performance of packets receiving percentage is evaluated in case of packet flooding jamming attack or without trust, in presence of existing Trust based scheme and proposed security scheme. The performance of proposed security scheme is shows the better data receiving in network because of that packet receiving percentage is also high. The proposed security scheme is very reliable to check the data packets forwarding in each hop value and if the value of variable is not satisfied then the attacker existence is confirm in Cognitive Ad hoc network and the performance is degrades. After applying proposed scheme again performance is improves in network.

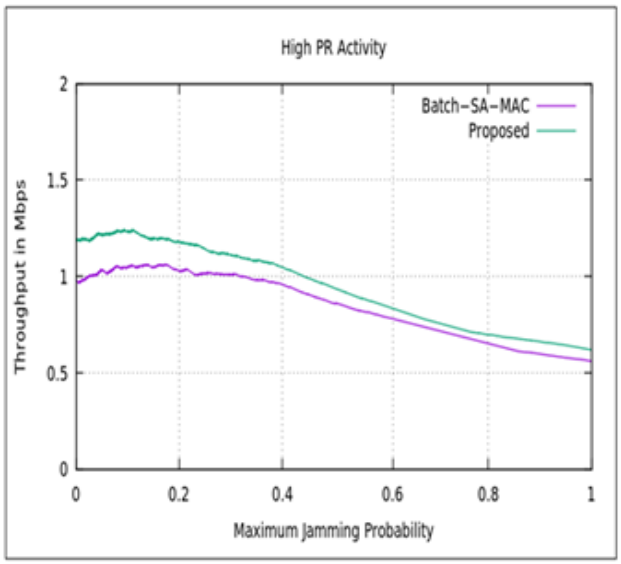

Fig.4 High PR Activity Performance Analysis.

5. Moderate PR Activity Analysis

The secondary users subsistence is important because they complete the communication if required and also space available after allocation of licensed spectrum. In this graph also the overhead quantity of packets in presence is more as compare to proposed security scheme. After applying proposed jamming detection scheme the concert is improves and the flooding of routing packets are minimized. The Moderate PR Activity performance of proposed security scheme is produces throughput more than 6 Mbps i.e. more than Batch -SA-MAC. It means packets receiving percentage is more and also successful receiving is higher in proposed approach.

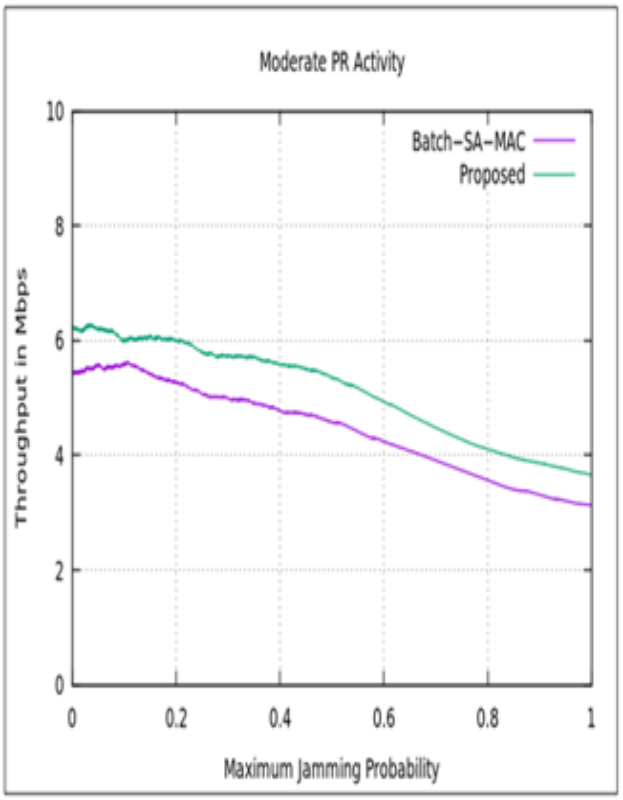

Fig.5. Medium PR Activity Performance Analysis.

6. Light PR Activity Analysis

The light jamming attacker is absolutely flooded the less number of packets among IoT nodes and these nodes processing speed is affected for forwarding and receiving signals in IoTCRN. The number of Secondary user is responsible of flooding and the previous Batch-SA-MAC scheme is provides the 4 Mbps throughput in 1.0 probability. The performance of proposed scheme is more and it provides the higher throughput performance about 6 Mbps at receiver end. The proposed flooding based identification scheme is more efficient then previous scheme in Light PR activity.

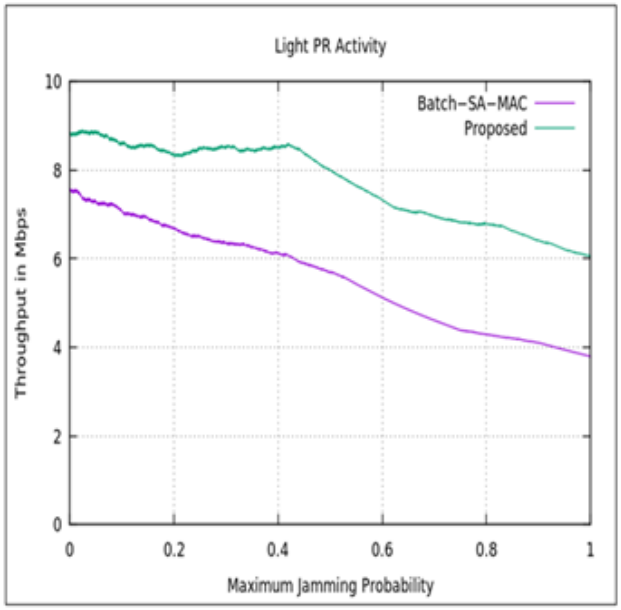

Fig.6 Light PR Activity Performance Analysis.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

Security is the major anxiety part in any network and this factor is also very essential for protected communication. The number of unlicensed used are use the band due to that CRN security is pretentious and also the jamming attacker is used the information of licensed users. The jamming attacker flooded the huge amount of data in network In this research we proposed security scheme against packet flooding Jamming attack. The performance is vitiated in high, medium and low jamming probability and apply the proposed scheme to reduces the flooding. The hop count value based on forward and reverse mechanism of detection and provides secure communication in IoTCRN.

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 increase according to condition to forward signals then the nodes is expected as the jamming attacker. The proposed scheme is check the consistency by detected the attacker with amount of packet loss in CRN. The performance of existing Batch-based SA-MAC is also providing the security and proposed performance is may be better than the existing scheme. The proposed is diminish the packet loss and also reduces routing overhead. The better packet receiving is improves the throughput performance in IoTCRN.

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 security approach in in DTN

(Delay Tolerant Network). The DTN is support the Bundle based multicast communication approach and applies the proposed security scheme to improve multicast routing performance.

REFERENCE

[1]. 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.
[2]. CL. Tan and N. Wang, ``Future Internet: The Internet of Things," in Proc. 3rd International Conference of Advanced Computation Theory Engineering (ICACTE), Vol. 5, pp. V5-376_V5-380, Aug. 2010.
[3]. L. Atzori, A. Iera, and G. Morabito, "The internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[4]. Mukrimah Nawir1, Amiza Amir, Naimah Yaakob, Ong Bi Lynn, "Internet of Things (IoT): Taxonomy of Security Attacks", 3rd International Conference on Electronic Design (ICED), 2016.
[5]. Vera Suryani, Selo , Widyawan, "A Survey on Trust in Internet of Things", 8th International Conference on Information Technology and Electrical Engineering (ICITEE), 2016.
[6]. 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.
[7]. 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.
[8]. 8 Jordi Perez-Romero, Linda Doyle, Mehmet Can Vuran, "Applications of Cognitive Radio Networks", IEEE vehicular technology magazine, pp. 22-23, June 2012.
[9]. Haythem Bany Salameh, Sufyan Almajali, Moussa Ayyash, and Hany Elgala, "Securing Delay-sensitive Cognitive Radio IoT Communications under Reactive Jamming Attacks: Spectrum Assignment Perspective", Fifth International Conference on Software Defined Systems (SDS), pp.20-24, 2018.
[10]. Pericle Perazzo, Carlo Vallati, Giuseppe Anastasi, and Gianluca Dini, "DIO Suppression Attack Against Routing in the Internet of Things", IEEE Communications Letters, pp. 2524 - 2527, 2017.
[11]. Zeeshan Ali Khan and Peter Herrmann, "A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things", EEE 31st International Conference on Advanced Information Networking and Applicationspp.1169-1176, 2017.
[12]. Hamza Khemiss, Djamel Tandjaoui "A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things", Wireless Telecommunications Symposium (WTS), 2016.
[13]. Qian Xu, Pinyi Ren, Houbing Song, Qinghe Du, "Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations", IEEE Access Special Section on Internet of Things (Iot) In 5g Wireless Communications, pp. 2840-2853, June 7, 2016.
[14]. 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.
[15]. K Fall and K. Varadhan, The NS Manual, Visit in Website inFebruary,2018,http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf.