International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 6 –OCTOBER 2016 (SPECIAL ISSUE).

Selfish Attack Detection and Mitigation using Route Error Packet in Cognitive Ad-hoc Network

Deepa[1], Jayashree Agarkhed[2]

Professor, Dept of computer science and engineering, PDACEG, Kalaburgi, India
P.G Student, Dept of computer science and engineering, PDACEG, Kalaburgi, India

Abstract— **The most popular technology is wireless, it will be used in many users like laptop, mobiles these becoming overcrowded on wireless network. To solve this problem the Cognitive network is used, it allocates the dynamic spectrum to the users. It is also have some vulnerability i.e. selfish attack. The proposed work is detecting this attack using the seqno.**

Index Terms—Cognitive radio network. selfish attack;vulnerabilities

I. INTRODUCTION

The wireless mesh network is literally a cognitive radio network (CRN), to connect the underneath node to the internet, generally we connect to the internet through a gateway router. This gateway is just like a router, which gets connected to the internet. The other device like laptop and mobiles gets connected through the internet via modem. If we take the of 3G connection to the mobile, from mobile it gets connected through directly to the gateway over a 3G connection, this is how the basic traditional way of getting connected with the internet. The problem here is that the number of devices which is increased in last five years. The device likes mobile, laptop they require an internet connection, but every device doesn't have 3G connectivity, like a laptop, it is impossible to get connected to the internet, using modem we can get connected with the internet. These devices are called unlicensed users.

In a wireless network, a fixed spectrum is allocated to the licensed users (primary user), the primary user (PU) has purchased the spectrum from the government. The base station uses a frequency of 2.4GHz to 5GHz, which is used by unlicensed users (secondary users). Due to fixed spectrum, there is a lot of wastage of bandwidth & the unused users (secondary users) become overcrowded. To overcome this, the new architecture comes into existence that is Cognitive Radio Network (CR). In CR the Spectrum is always sensed the primary user is active or not, if the primary user is inactive then it is called a spectrum hole. In CR allows the unlicensed users to use the primary user's unused bandwidth to the secondary users (SU). If the primary user is active, then the secondary user should drop its service & give back the service to the primary user.

The other type of network is cognitive, ad-hoc network. The ad-hoc network is used in CRN to avoid the network setup problem. If we consider the airport wifi network it has huge area, single router cannot handle the all the devices. The wifi repeaters are used. Routers are used to handle the both PU and SU. CR network is opportunistic to the SU; it switches the spectrum to the PU to the SU, when PU is inactive. These devices are moving randomly, as they move the network topology and protocol is changed. To avoid this ad hoc network is used in CR network. Cognitive ad-hoc network is also having some threat and challenges that degrade the performance of network i.e. selfish attack.

The Proposed work is organized in 6 sections. Section 1 presents a general introduction of cognitive radio network and ad-hoc network. Section 2 presents the related work of the different types of attacks. Section 3 presents the design of the proposed system with block diagram are discussed. Section 4 presents Results and Discussion. Section 5 presents performance analysis Section 6 concludes the work with future enhancement.

II. RELATED WORK

The main objective of the authors [1] is to analyze the Software Defined Radio based Cognitive radio network, threats and issues of the main recent advancements and architectures of (SDR) and cognitive radio networks.

The authors [2] considered a problem, i.e. primary user emulation (PUE) attacks in cognitive radio networks; this type of attack is operating in the white spaces of the digital TV band. In this attack the SU emulate the primary user and he access the primary user signal. TO avoid this attack primary user generates a pseudo-random AES-encrypted reference signal that is used as the segment sync bits. The synch bit is used to detect malicious user.

The author [3] considered a problem, i.e. primary user emulation (PUE) attacks on CR network. They used different methods to avoid the PUE attack in CsR network. The method

is database assisted PUE detection approach. In this method they have taken two databases, one for local database is integrated in each SU, the second is global database is built up in the cognitive BS.

The authors [4], Consider the problem of localization of base station in wireless networks has been mainly studied in a non-adversarial setting. A number of solutions have been proposed to detect and prevent attacks on localized systems. They propose a new method to secure localization based on hidden and mobile base stations using the covert base station.

The authors [5], investigated how to improve the security of collaborative sensing. Particularly, they develop a malicious user detection algorithm that calculates the suspicious level of consistency of secondary users based on their past reports and they calculated that how much time the node behaves badly.

From the literature survey, we found the two problems which are bandwidth allocation and primary user emulation attacks are non deterministic so we proposed a selfish attack detection technique.

The proposed method is based on the route error (RERR) and nodes energy.

III. PROPOSED WORK

As shown in below fig1 a radio network with a base station, which is operating in licensed frequency.

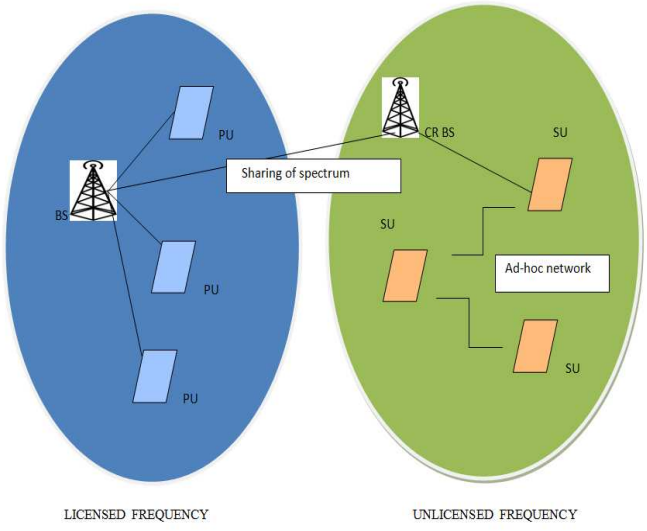


Fig 1.Cognitive radio architecture

Licensed frequency is acquired by the service provider for 3G services. Free-frequency is operating 2.4GHZ, which can be used by anybody whose range is very limited and which can be used by any number of devices, because many devices can use same band. The congestion and the collision of the packets will be too high in the free frequency band. Whoever licensed frequency band either it can be a CDMA technique or it can be a DMA technique are used. Basically, we have a communication area divided into cells, which each cell being allocated with a slice of the frequency. The frequency is divided into licensed and unlicensed. A spectrum is the range of the frequency in which a network can operate is called a spectrum.

In any network not all users communicate at the same instance of time. Now network can have other type of users like small laptop, mobile, small handled devices which wants to access the internet services. Generally they are operating in a free frequency range for example, our local network, is operating with 2.4GHZ wifi network, because the bandwidth is very expensive, we need to pay a lot of amount to reserve this spectrum from the government any free spectrum nothing but the looseness of money for the network.
There are many other devices like laptop, tablet these are also want to access internet, these devices has not purchased the internet. CR is a new architecture that allows the service provider to reallocate the part of the unused spectrum to the secondary user if they demand, suppose we have a secondary user who wants to access the internet and the spectrum is free, spectrum of 3 users is free 3 user spectrum it can reallocate to the free frequency of at least 3 devices. When another primary user wants to access this service, because the primary user pays more money and whenever it wants to access this service it take away the service from one of the users and it can give the link to the primary user. If the topmost primary user has finished its operation and don't use the network and that situation again if there are more number of secondary users they want to access the internet it can reallocate spectrum to the secondary user, this is the basic principle of CR network.

IV. ALGORITHM

Begin

Step1: BS==SU

Step 2: infoAlter (Packet* p);

Step 3: AODV::inforAltered (Packet*p)

{

p->data->bw= p->data->(bw-100);

}

Step 4: if(strncasecmp(argv[1], "selfish", 9) == 0)

{

malicious=1000;

}

Step 5: AODV::recvRequest(Packet *p)

Step 6: else if (malicious==1000)

{

seqno = max(seqno, rq->rq_dst_seqno)+1;

Step 7: RERR-> SU

Step 8: if (RERR (node) >MAX)

Step 9: node-> black list && mac_add(node)->block

Stop

The info alter function will be called by the attacking node, where simulate the alteration of the BW there is coming from the BS. In ad-hoc network, every node can communicate with each other and they share the information. The node actually gets the data from the BS it alters that data and transmits neighbouring SU nodes. The other SU nodes think that the less amount of spectrum is left, so that they hesitate to request the BW from the BS. They think BS doesn't have enough resources. The packet will have field called data, the data will have field called BW.

This info Altered() function is called an attacking node, the attacking node always change total BW information contain and it reduce the actual BW information. In ad-hoc one node send request to the other node to communicate with their data. Whenever the RREQ comes to selfish node it's increment the seqno count, that network is assigned the maximum available seq it increase that seq count. Whenever the nodes receive the RREP from selfish node, they find that this hop is invalid. In this case the entire RREQ packet coming from the neighbour nodes it doesn't receive that packet. The selfish node is not the part of the any path, in this way it save its BW. Such node is called selfish node. The current node which is received RREQ is the malicious or not, if the malicious it increase the seqno, the maximum allowed plus 1 seq+1. So that it doesn't forward any data. By increasing the BW of the transmission and changing information in the allocated packet and altering the seqno shows that the node is selfish. It can be detected by using packet energy and seq no of maximum node.

V. RESULT ANALYSIS

A simulation model based on NS2 is used, assumed that the dimension of the scenario as1000mx1000m in that 7 wireless node randomly deployed. Each wireless nodes initials energy is 3.4j, 10 Mbps bandwidth and each packet size 512 kbps. A two way propagation model is assumed by radio model. AODV protocol is used.

SIMULATION PARAMETERS

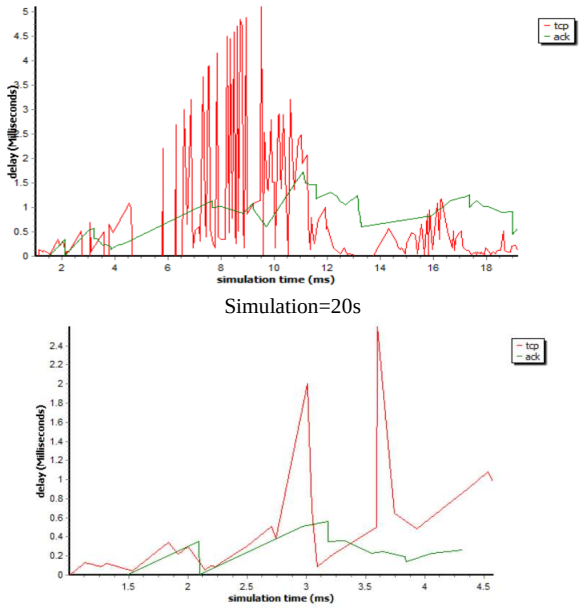
Table 1.simulation parameters

Parameter	Setup
set Val (Chan)	Channel/Wireless Channel
set Val(prop)	Propagation/Two Ray Ground
set Val(net if)	Wireless Physical
set Val(Mac)	Mac/802_11
set Val(if q)	Queue/Drop Tail/Pri Queue
set Val(LL)	LL
set Val(ant)	Antenna/Omni Antenna
set queue length	50
set Val(nun nodes)	7
set Val(routing protocol)	AODV
set Val(x)	1131
set Val(y)	909
set Val(stop)	20

.

VI. PERFORMANCE ANALYSIS

BASE STATION



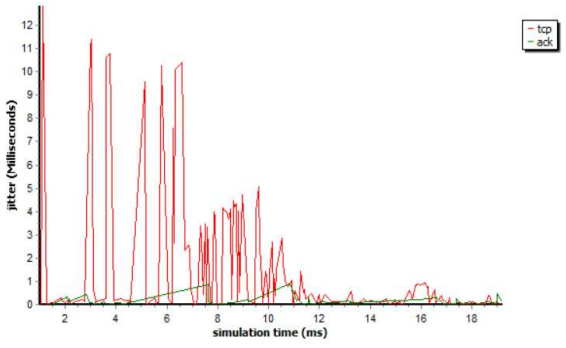
Simulation=20s

Simulation=5s

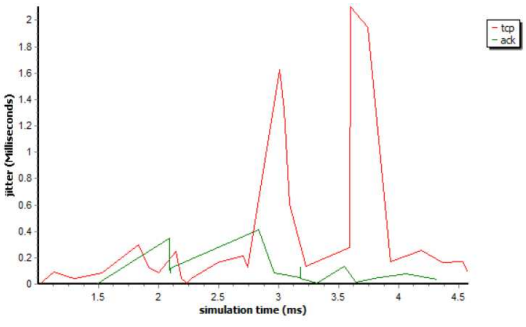
Fig 2. Delay versus simulation time

The fig 2 shows delay of the packet, how much the BS sends the Ack packet of the received packet from the SU, however the attacker is changing the spectrum of BS, the BS finds the slow delay while receiving the packet because SSU nodes trying to sends packet to the BS. The 10-12s when the attacker was attacking it showing that it increasing the packet of distance. Once the attacker was detected after 12s its showing the delay of the BS can get reduced. At less simulation times it shows that the delay of packet that is instance on which attacking node creates a misinformation in the spectrum, which makes PU and SU to keep their packet in queue such that the packets are transmitted afterwards, this helps to reducing the latency at the BS by mitigating the attack.

Jitter



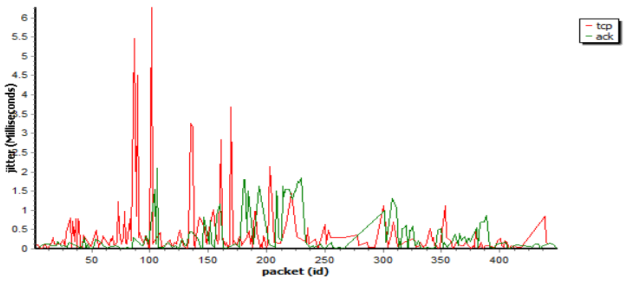
Simulation=20s



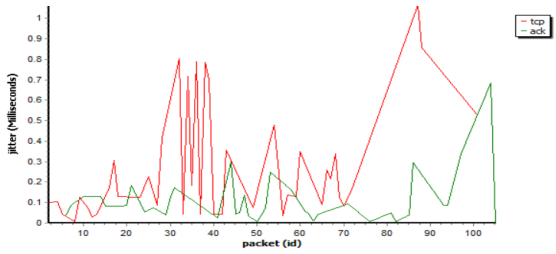
Simulation=5s

Fig 3. Jitter versus simulation time

The fig 3 shows jitter over a time the jitter is extremely high between 6-12s, where the attacker was attacked and that attack is selfish. Changing of BW information causes a significant amount of delay because re-routing and re-transmitting and waiting for the channel to become idle the delay is suffered by the BS is tremendous. The fig 12 shows the amount of TCP jitter is observed is much higher than that ACK value. Simulation is less the attack effect is less and the TCP packet and ACK packet is same.



Simulation=20s

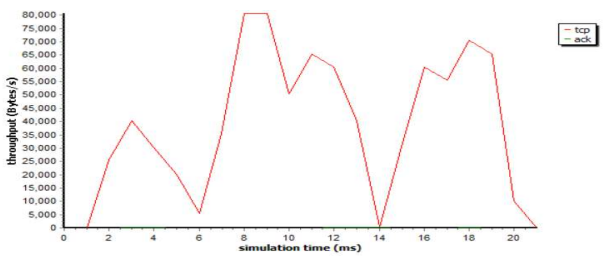


Simulation=5s

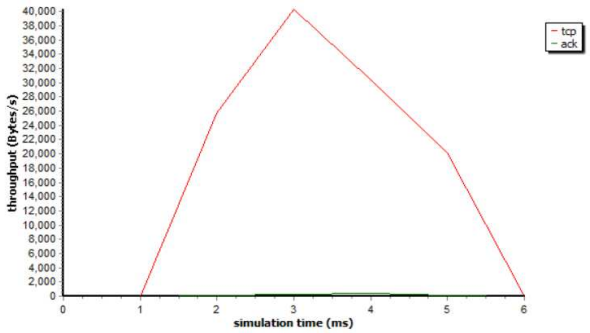
Fig 4. Jitter versus packet id

In fig 4 shows per packet jitter the two peaks which are the instance when the attacker is starting attack, therefore it can detect attacks and mitigating the attack. In less simulation of time it is quite high.

Throughput



Simulation=20s



Simulation=5s

Fig 5. Throughput

Fig 5 shows throughput, whenever there is been attack instance 6-40s the throughput is going to be down, once the attack was detected and mitigated again throughput starts increasing.

VII. CONCLUSION

In Cognitive radio network spectrum allocation is done dynamically to avoid wastage of spectrum, due to this many attacks will be done. In this selfish attack is considering and avoid using the method of counting seq no and RERR . The performance analysis is shows that the efficiency of the attack detection and mitigation.

VIII. PREFERENCES

1) Awanish kumar kaushik “A Comparative Study of Software Defined Radio and Cognitive Radio Network Technology Security”, International Journal of Advances in Engineering Science and Technology www.ijaestonline.com

2) 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,ISSUE NO. 5, MAY 2014.

3) Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed “Defense against Primary User Emulation Attacks in Cognitive Radio Networks”, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 26, ISSUE NO. 1, JAN 2008.

4) S. Capkun, M. Cagalj, and M. Srivastava, ―Secure localization with hidden and mobile base stations,‖ Proc. IEEE Infocom, April.2006. I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, ―NeXt

5) W. Wang, H. Li, Y. Sun, and Z. Han, ―Attack-proof Collaborative Spectrum Sensing in Cognitive Radio Systems,‖ in Proc. Conferenc on Information Sciences and Systems (CISS’09), March. 2009.

6) K. B. Letaief and W. Zhang, "Cooperative spectrum sensing", Cognitive Wireless Communication Networks, Springer, 2007.

7) C. H. Lee and W. Wolf, "Energy efficient techniques for cooperative spectrum sensing in cognitive radios", in Proceedings of IEEE Consumer Communications and Networking Conference, Jan. 2008.

8) Wassim El-Hajj; Haider Safa; Mohsen Guizani, “Survey of Security issues in Cognitive Radio Network,” journal of internet technology, vol 12 2011.

9) Mathur CN, Subbalakshmi KP. “Security issues in cognitive radio networks. In: Cognitive networks: towards self-aware networks.” John Wiley and Sons, Ltd; 2007.

10) Zhaoyu Gao; Haojin Zhu; Shuai Li; Suguo Du; Xu Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *Wireless* Communications, *IEEE* , volume.19, Issue no.6, pp.106,112, December 2012.

11) Romero, E.; Mouradian, A.; Blesa, J.; Moya, J.M.; Araujo, A., "Simulation framework for security threats in cognitive radio networks," Communications, IET , volume.6, no.8, pp.984,990, May 22 2012.

.