Pallavi Sharma, Manpreet kaur / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 3, May-Jun 2013, pp.1271-1275

Develop a scanning algorithm for the detection of selfish nodes in cognitive radio networks

Pallavi Sharma
Mtech student
Lovely professional university Phagwara

Manpreet kaur
Assistant Professor
Sukhchain Sahib College Phagwara

Abstract

Cognitive radio is a wireless based communication technology which has intelligence built into it. Secure communication is a key for any wireless network . Like all other networks, cognitive radios are susceptible to various kinds of attacks like DOS attack , PUE attack , tunnel attack and jamming attack . While performing these attacks nodes in the network becomes selfish and start maximizing their own spectrum usage and they prevent other users from communicating in the same network . In this paper an algorithm is generated which can detect selfish nodes in a network . This analysis will help to give better future products that could use the resources in a more efficient way .

Keywords : *Cognitive Radio , Selfish node , Spectrum band, Sweet spot .*

I. INTRODUCTION

Cognitive radio is a radio capable of being aware of its surroundings , learning and adaptively changing its operating parameters . It learns from its experiences to give reasoning and to decide which action to take in future so that it can meet the needs of users.A fundamental problem in facing future wireless systems is to find suitable carrier frequencies and bandwidths to meet the demands of users for future services .Radio frequency spectrum is considered to be a limited natural resource so its utilization is a very important factor for better future wireless products.Spectrum utilization is the most important aspect of the cognitive radio technology . Cognitive radios are fully programmable wireless devices that can sense their environment and dynamically adapt their transmission waveform, channel access method, spectrum use,and networking protocols as needed for good network and application performance.[5] Cognitive radios have the ability to implement protocols and spectrum policies in a way which differs from traditional communication systems .The primary objective of cognitive radio network is to provide reliable communication whenever and wherever needed . Cognitive radios are used to improve the efficiency of various resources in a wireless communication systems . Cognitive radios can either be deployed in licensed spectrum or unlicensed spectrum .The creation of new rules for spectrum sharing by using cognitive radio protocols will change the way spectrum will be used in the future . other aspect of cognitive radio network is that it offers a greater flexibility to the networks in a way that they can reorganize them according to the requirements and also repair them to provide more reliability.[6]

II. LITERATURE SURVEY

In year 2011, Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed discussed primary user emulation attack. In primary user emulation attack the attacker transmits the signal which shows same characteristics as of primary user. These attacks interfere with the spectrum sensing process and reduce the channel resources available to unlicensed users. To overcome this threat a technique transmitter verification scheme called LOCDEF which helps to distinguish between primary signals and signals transmitted by attacker by estimating its location and observing its signal characteristics. There is high probability of these attacks in the cognitive radio because of the fact that cognitive radios are highly reconfigurable because of the software based air interface. [1]

Trang V. Mai, Joseph A. Molnar and Dr. Kevin Rudd, "Security vulnerabilities in case of cognitive radio networks" discussed various attacks in Physical layer whether it is PUE, denial of service attack or jamming attack. Dynamic spectrum access in cognitive radio introduces many types of threats Data indicates that with a simple level of sophistication physical jamming could degrade the performance of DSA networks. These attacks could have a long term negative impact on the cognitive network because of its capability to learn from the environment to establish internal policy constraints.[2]Wang Weifang discussed the effect of Denial of Service (DoS) attacks in security of wireless network.Cognitive radio networks are vulnerable to DoS attack due to their own characteristics. This paper analyzed the architecture of cognitive radio networks and discussed the possible various DoS attacks in ad hoc cognitive radio networks in different protocol layers.[3]Husheng Li and Zhu Han discusses the approach of combating the primary user emulation attack .In cognitive radio systems, primary user emulation

(PUE) attack means that an attacker sends primary-user-like signals during the spectrum sensing period such that honest secondary users leave the corresponding channels, which causes a serious threat to cognitive radio systems. A passive anti-PUE approach, similar to the random frequency hopping in traditional anti-jamming schemes, is proposed and called dogfight in spectrum. In this scheme, the defenders randomly choose channels to sense and avoid the PUE attack. It is assumed that the channel statistics like availability probabilities are known. [4].

III ATTACKS IN COGNITIVE RADIO NETWORKS

Cognitive radio users are vulnerable to various kinds of attacks . One reason is that secondary users do not own spectrum usage and also cognitive radio support opportunistic spectrum sharing so attackers could take advantage of these flexibility features . As a result security considerations are very important for the successful deployment of cognitive radio networks [5]Before taking into consideration security countermeasures it is very important to understand different kinds of attacks . These kinds of attacks occur in PHY layer and they manipulate spectral environment of radios.

Denial of service attack **:** In case of denial of service attack the attacker does not allow authorized users to use network resources . the attacker basically flood the network with so many request objects which results in decrease of the network bandwidth and degradation of wireless network systems .[7]

PUE Attack **:** Primary users always have priority to access the spectrum because they are legitimitate users . In case primary user is detected , all other users immediately leave that band . but sometimes secondary users start behaving like primary users and imitate the characteristics of primary users to launch primary user emulation attack .[11]

Sybil Attack **:** In this attack single entity claims to be multiple identies at a same time resulting in ineffectiveness of many functions performed by sensor network like routing and resource allocation .This attack mostly occurs in peer to peer networks where it undermine the power and authority of established network . When any faulty node becomes part of such network it starts overhearing the communication and start controlling the network in its own way .Validation techniques can be used to prevent these attacks .[14]

Wormhole attack : In wormhole attack the attacker starts recording packets of data at any one location and then redistribute that data in whole network . it is difficult to prevent the network from wormhole attack even if the network communication system provides authenticity and confidentiality .[16]To establish a wormhole attack a direct link known as wormhole link is created between two dedicated nodes present in network . As soon as wormhole link becomes operational eavesdropping of messages start at origin point and those messages start replaying at destination point .During the route discovery the attackers makes the nodes believe that path through them is shortest.Under wormhole attack malicious nodes steal the identity of legitimitate nodes [17]. To detect such attack , the system requires special hardware and time based synchronization algorithm.

Node impersonation attack **:** In this attack an authorized entity called node is impersonated by breaking an procedural mechanism . The attacker assumes the identity of another node in the network, thus receiving messages are directed to the fake node. These attacks are also called spoofing attacks . this attack is considered to initialize the first step to enter in the network for carring out further attacks.[8] Depending on the access level of the impersonated node, the intruder may even be able to reconfigure the network so that other attackers can easily join or attacker could remove security measures to allow subsequent attempts of intrusion .these attcks can also inject false routing information in the network This kind of malicious behavior can be detected using the hash function and the signature that is associated with the incoming data packets .[18]

Timing attack **:** In case of timing attack attacker attempts to compromise the security and reliability of system by analyzing the time taken to execute the cryptographic nad network secutiy algorithms.Some information could be gathered by analyzing the time required to execute the queries which could differ depending on the required input.[12]These attacks are basically used to attack on weak computing device. Timing attacks enable an attacker to extract secrets maintained in a security system. The most widely accepted defense against timing attacks is to perform RSA blinding.This attack could be implemented without the knowledge of victim . the effectiveness of this attack depends upon various factors like cpu configuration , algorithms used and accuracy of timing measurements .

Illusion attack: In case of illusion attack the attacker creats fraud traffic safety message and the victim receive the message and believe it and changes its behavior according to the message parameters [9].

Sinkhole attack **:**Wireless networks are vulnerable to attack called sinkhole attack. This attack prevent the base station from obtaining complete and correct sensing data.Many current routing protocols in sensor networks are susceptible to the sinkhole attack. In a Sinkhole

attack , a compromised node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodeswith respect to the routing metric. As a result, the adversary node manages to attract all traffic that is destined to the base station.By taking part in the routing process, node can launch more severe attacks, like selective forwarding, modifying or even dropping the packets coming through.[10]
It locates a list of suspected nodes by checking data consistency, and then identifies the intruder in the list through analyzing the network flow information. Specific detection rules could be made that can make legitimate nodes become aware of the threat, whilethe attack is still taking place.[13]

IV PROPOSED APPROACH

After conducting a thorough survey we have arrived at this problem statement as follows :
It is to detect selfish nodes in a cognitive network and develop a scanning algorithm for its detection.
This research is based on the hypothesis that an efficient algorithm should be generated that could identify the nodes that are degrading the efficiency of network in which false positive rates are calculated in such a way that they help us to give less number of false rates .

The advantage of using this approach will be to develop a strategy to detect when the nodes turn selfish and how they are affecting overall routing of packets and packet delivery ratios. It will help us to simulate the spectrum characteristics for cognitive devices and to maintain an hierarchy /topology of primary users and secondary cognitive device users. It will generate an simulated environment for scanning and detecting selfish nodes.

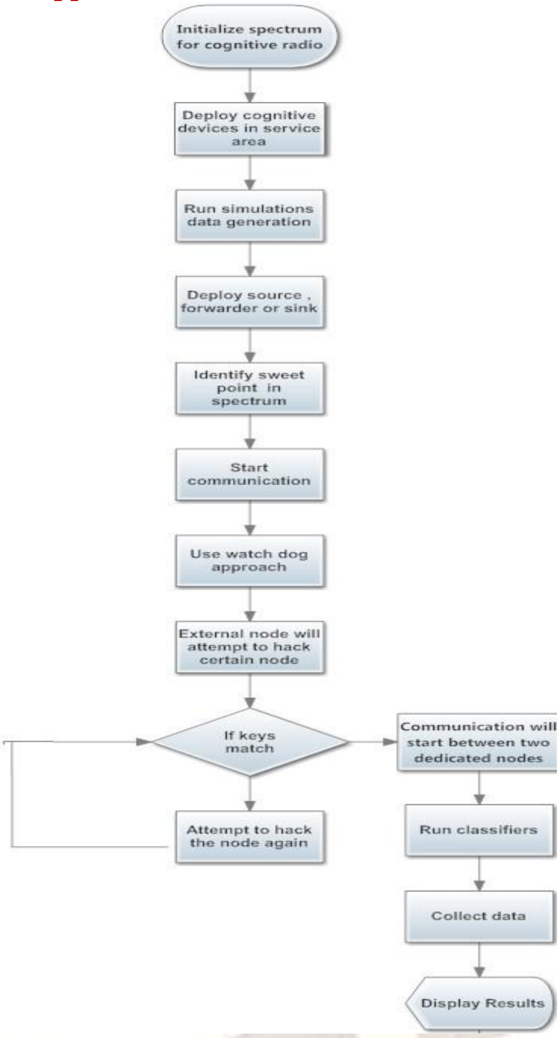

Figure1 : Research design

Under methodology we have described step by step procedure to detect selfish node in cognitive radio network.First we need to initialise a spectrum for cognitive radio networks. It is important to analyze the spectrum environment in which cognitive radio will operate. Second step is to deploy primary and secondary devices in a particularly defined area.After that deployment it is important to start communication between nodes. Deploy source , forwarder or sink. In an cognitive radio architecture one node will assume to be source , other node as sink and all other nodes are forwarding nodes. Identify sweet point in spectrum. Sweet spot is considered to be that point in spectrum where frequencies are low enough to provide good coverage with few amount of transmitters in that coverage area while accommodating large bandwidths. At the time all communication is happening between nodes in the background of scenario watch dog approach is used . In case of watch dog approach a buffer is maintained which contains all the packets that have been sent recently. It detects the selfish nodes in the network by overhearing the transmission in network . For the detection purpose , first it is really important to hack a certain nodes which simply means to make a node selfish . So an external node will attempt to hack a node in network by using keys. When the keys will match it will display a message hack attempt successful . In case keys does not match external node will try to hack the node again and will try an another attempt. In case hacker attempt is successful it will start communicating with that node with which it keys matches.so it means those nodes start behaving as selfish nodes .

For seeing the accuracy of algorithm classifiers are used. The results will come out in form of false positive and false negative rate which is defined in percentage.

V RESULTS AND CONCLUSION

Results :

True Positive (TP)	1548
True Negative (TN)	2143
False Negative (FN)	265
False Positive (FP)	645
Total Features	5
Positive Predicted Value (PPV)	0.71
Negative Predicted Value (NPV)	0.89
Specificity (SP)	0.77
Senstivity (SE)	0.85
Accuracy	80.22 %
Geometric Mean	1.27

Figure 2 – Results

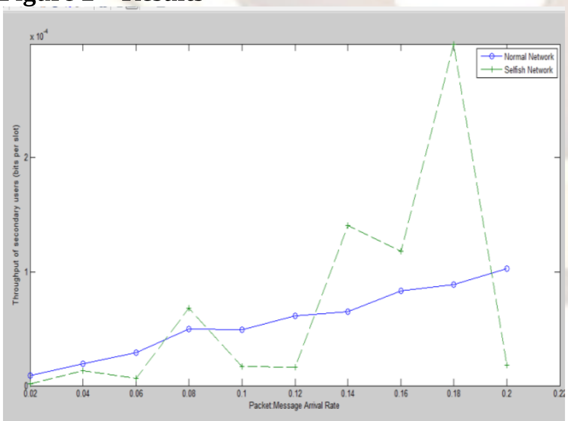

Figure 3 – Selfish Network Graph

This proposed methodology helps us to analyze the behaviour of cognitive network under various constraints of resources. By doing such analysis we can give better future products that will use the resources in a much more efficient way. It will help us to ensure and develop reliable cognitive networks since we will be delivering packet delivery ratio. It will help us to find out when does the nodes turn selfish and misbehave in the cognitive radio. This strategy ensures the system to detect such misbehaviours and to avoid loss of packets.

VII . CONCLUSIONS AND FUTURE SCOPE

So this results concludes that if any node attempts to behave selfish it could be identified by using our proposed algorithm. This algorithm provides an accuracy of 80.22% .

Our result graph shows that selfish node utilize all the resources of network and does not allow other users to use that spectrum which results in spectrum deficiency and underutilization of network resources .

This proposed algorithm works in certain scenario . But as the scenario will change and new methods would be developed to attack on a cognitive radio networks , it will require certain modifications in it .

REFERENCES :

[1] Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed ,"Defense against primary user emulation attacks in cognitive radio networks" , Virginia Polytechnic Institute and State University in 2008, Pages 25-37

[2] Trang V. Mai, Joseph A. Molnar and Dr. Kevin Rudd , "Security vulnerabilities in case of cognitive radio networks" Publication Year: 2011 , Page(s): 1 – 4 , IEEE 54th international Midwest symposium

[3] Husheng Li and Zhu Han ,"Combating Primary User Emulation Attacks in Cognitive Radio Systems" (IEEE transactions on wireless communications , Vol 9 , No.11, November 2010), Wireless Communications, IEEE Transactions on Volume: 9 , Issue: 11 , Publication Year: 2010 , Page(s): 3566 – 3577.

[4] Husheng Li and Zhu Han ,"Combating Primary User Emulation Attacks in Cognitive Radio Systems" (IEEE transactions on wireless communications , Vol 9 , No.11, November 2010), Wireless Communications, IEEE Transactions on Volume: 9 , Issue: 11 , Publication Year: 2010 , Page(s): 3566 – 3577.

[5] MacKenzie, A.B, Reed, J.H.,Athanas, P Bostian, C.W."Cognitive Radio and

Networking Research at Virginia Tech "Volume:97, Issue: 4,Publication Year: 2009,Page(s): 660 – 688.

[6] Fragkiadakis, A.; Tragos, E.; Askoxylakis,"A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks I."Volume:PP, Issue: 99,Publication Year: 2012 , Page(s): 1 – 18.

[7] Lau, F. Rubin, S.H. ; Smith, M.H. ; Trajkovic, L. "Distributed denial of service attacks" Publication year : 2000, Volume: 3, Page(s): 2275 – 2280

[8] Huaping Hu Comput. Sch., Nat. Univ. of Defense Technol., Changsha, China Jing Zhang ; Bo Liu ; Lin Chen ; Xin Chen "Simulation and analysis of distributed low-rate denial-of-service attacks" Publishing year : 2010,Page(s): 620 – 626.

[9] Siqin Zhao " Defend Against Denial of Service Attack" Publication year :2009 ,Page(s): 91 – 96.

[10] Xueping Chen "Distributed denial of service attack and defense "Publication year :2010Volume: 3, On Page(s): V3-318 - V3-320.

[11] Shaxun Chen ,Kai Zeng ; Mohapatra, P. "Hearing is believing: Detecting mobile primary user emulation attack in white space",Date of Conference: 10-15 April 2011,Page(s): 36 - 40.

[12] Zhou Yuan ,Niyato, D. ; Husheng Li ; Zhu Han "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks"Date of Conference: 28-31 March 2011,Page(s): 599 - 604.

[13] Husheng Li ,Zhu Han "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems"Publication year : November 2010Volume: 9, Issue: 11 ,Page(s): 3566 - 3577.

[14] Yi Tan ,Kai Hong ; Sengupta, S. ; Subbalakshmi, "Using Sybil Identities for Primary User Emulation and Byzantine Attacks in DSA ", Date of Conference: 5-9 Dec. 2011, Page(s):1-5.

[15] Xia Wang Iowa State Univ., AmesWong, J."An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks"Date of Conference: 24-27 July 2007,Page(s): 39 - 48.

[16] Yih-Chun Hu,Perrig, A. ; Johnson, D.B. "Wormhole attacks in wireless networks"Publication year: 2006,Volume: 24, Issue: 2 Page(s): 370 – 380

[17] Prasad, S. Dept. of Comput. Sci., North Carolina State Univ., Raleigh, NC, USA Thuente, D.J. Jamming attacks in 802.11g — A cognitive radio based approach,Date of Conference: 7-10 Nov. 2011,Page(s):1219-1224

[18] lancy, T.C. Electr. & Comput. Eng., Maryland Univ., College Park, MD Goergen, N.Security in Cognitive Radio Networks: Threats and Mitigation,Date of Conference: 15-17 May 2008,Page(s): 1 - 8