ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Analysis of Attacks in Cognitive Radio Networks

M.Padmadas[1], Dr.N.Krishnan[2], V.Nellai Nayaki[3]

Sub Divisional Engineer BSNL, Research Scholar, Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India[1]

Professor, Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India[2]

PG Scholar, Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India[3]

Abstract: As the wireless communication greatly depends on spectrum utilization, the increase in demand for new wireless services and their application leads to the spectrum scarcity. To efficiently access the unavailable spectrum cognitive radio is used. The demanding technology is introduced new spectrum allocation policies, which will allow unlicensed users (i.e., secondary users) to access the radio spectrum when it is not occupied by licensed users (i.e., primary users) will be exploited by the cognitive radio (CR) technology. Security is one of the critical attributes of any communication network. There are various papers covering the security issues over the threats in cognitive radio, but this paper provides an analysis of attacks and common threats and the possibility of securing the available spectrum from the attackers.

Keywords: Cognitive Radio, Primary User, Secondary user.

I. INTRODUCTION

The rapid growth in access of dynamic spectrum causes spectrum scarcity[1] [2], [3]. In order to avoid spectrum scarcity a new networks called CRNs is designed. It has the capacity to sense the spectrum as well as determine the unused bands [4], [5]. It has an opportunity to make use these vacant spectrum bands by changing its parameters dynamically. In which the primary users have the priority to access the channel any time because they are the users with a specific license to communicate over the allocated licensed band.

The secondary users can access the channel as long as they do not cause interference to the primary users [7], [10]. The unused spectrum is represented as white spaces. These are also called as spectrum holes. The spectrum holes are detected by cognitive radio for secondary users. Various security threats are involved in this spectrum sharing policy in CRNs.

II.COGNITIVE RADIO

Wireless communication in which the transmission or reception parameters are changed to communicate efficiently without interfering with licensed users. Parameter changes are based on the active monitoring off several factors in the radio environment (e.g.radio frequency spectrum). This approach is enabled by software-defined radio frequency spectrum.

CRN Functions:

- **Spectrum sensing:**
  Detecting the unused Spectrum and sharing the spectrum without harmful interference with other users.
- **Spectrum Management**:
  Capturing the best available spectrum to meet user communication requirement.
- **Spectrum Mobility:**
  Maintaining seamless communication on requirements during the transition to better spectrum.
- **Spectrum Sharing:**
  Providing the fair spectrum scheduling method among coexisting CR users.

III.ATTACKS IN COGNITIVE RADIO NETWORK

There are many attacks in cognitive radio networks, only few attacks we categorized through Three major layers: physical layer, link layer (also known as MAC layer), network layer .

A. Physical Layer:

The physical layer is the lowest layer of the protocol .It provides interface to the transmission medium. It consists of anything that is used to make two network devices communicate, such as the network cards, fiber, or, as in the cognitive radio network framework, the atmosphere[6]. The operation of the cognitive radio network is more complicated than other wireless communication networks because the cognitive radio uses the frequency spectrum dynamically.

i)Primary User Emulation Attack(PUE):

The cognitive radio network requires ability to distinguish between the primary and secondary user signals. In the primary emulation attack, an attacker may modify their air interface such that it emulates the primary user's signal characteristics causing other secondary users to falsely determine that the frequency is in use by the primary user, and so vacate the frequency[8]. The imposter may perpetrate the attack selfishly, so he can use the spectrum, or maliciously, so the other legitimate users will have their communication disrupted, resulting in a denial of service

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

attack[8]. Therefore, the primary user attack (PUE) can lead to an objective function attack.

ii)Objective function attack:

Cognitive radios are adaptive to the environment. Many radio parameters are available for manipulation in the effort to adapt the radio to the environment by maximizing objective functions, and therefore the radio's ability to communicate over the medium. Objective function attacks apply to an attack on any learning algorithms that utilize objective functions. Another name for objective function attacks is belief manipulation attacks [9]. Parameters manipulated include, but are not limited to, bandwidth, power, modulation, coding rate, frequency, frame size, encryption type, and channel access protocol.

iii)Overlapping secondary user:

Such a situation places dynamic spectrum access sharing at risk through both objective function and primary user vulnerabilities by one malicious node. A malicious user in one network may transmit signals that cause harm to the primary and secondary users of both networks. Signals transmitted maliciously may provide false sensing information, thereby negatively affecting the objective function in one or both networks[11][15]. The malicious user may intermittently falsely emulate the primary users of each network causing each network to vacate the channel.

iv)Jamming:

Jamming, one of the most basic types of attacks in the cognitive radio network, attempts to adversely affect the signal to noise ratio. In this attack, the malicious user intentionally and continuously transmits on a licensed band, making it unusable by the primary or other secondary users. The attack is amplified by transmitting with high power in several spectral bands. Jamming can be detected with triangulation and energy based techniques[12][14]. However, the time lost with these techniques allows the attacker to severely impact the network. A mobile attacker can be even more difficult to locate.

B.Link Layer Attacks:

i)Spectrum Sensing Data Falsification (Byzantine attack):

In the Byzantine attack, also known as spectrum sensing data falsification, the attacker injecting the false sensing information into the decision stream is a legitimate member of the network and is referred to as the Byzantine[13]. Byzantines may perpetrate the attack to selfishly acquire increased spectrum availability for themselves, or the attackers may have a goal of disrupting the throughput of the network for other nefarious reasons.

ii) Control channel saturation:

The control channel saturation attack is based on the fact that if a cognitive radio is unable to complete negotiations during the limited time of the control phase, the radio defers from transmission during the next data phase[15]. This situation may naturally occur when the channel is saturated by a large number of contending cognitive radios. An attacker can broadcast a large number of packets with the intent to saturate the control channel. By sending different types of packets, a malicious node reduces the risk of detection. Combining the control channel saturation attack with the small window backoff attack the attacker may be able to ensure the malicious node captures the control channel before other users.

iii)Control channel jamming:

Control channels facilitate the cooperation among cognitive radio users. As a single point of failure, common control channel jamming (CCC) is the most effective and energy efficient way for an attacker to destroy the entire network system[17]. With common control channel jamming, receivers are prevented from receiving valid control messages when a strong signal is injected into the control channel. This results in denial of service for users of the network.

C.Network layer Attacks:

The network layer provides the ability to route data packets from a source node on one network to a destination node on another network, while maintaining quality of service. It also performs fragmentation and reassembly of packets, if required. The cognitive radio network shares security issues with the classic wireless communication networks due to the three shared architectures of mesh, ad hoc, and infrastructure[16]. Cognitive radio networks also share similarities with wireless sensor networks. These include multi-hop routing protocols and power constraints. In addition, there are special challenges faced by cognitive radio networks due to the required transparency of the network activities to the primary user. Routing in the cognitive radio network is further complicated by the requirement of the radio to vacate the frequency when the primary user is sensed as present. Cognitive radio security vulnerabilities are therefore also inherited from these architectural requirements.

i)Sinkhole :

Cognitive radio networks often use multi-hop routing. A sinkhole attacker takes advantage of multi-hop routing by advertising itself as the best route to a specific destination. This activity spurs neighboring nodes to use it for packet forwarding [18]. In addition, the neighbors of the attacker will advertise the offender as the best route, creating a ''sphere of influence'' for the attacker. The attacker can begin the attack by building a trust base. The attacker can use a higher level of power so it can send any received packets directly to the base station. It can advertise that it is one hop from the base station, and forward all received packets appropriately for a time. After trust has been established, and advertising of the node as the best route has been propagated through the local area, the perpetrator can begin other types of attacks, such as eavesdropping.

ii)Wormhole:

The wormhole attack is closely related to the sinkhole attack. Basically, an attacker tunnels messages received in one part of the network over a low latency link. The messages are replayed in another part of the network. In the simplest example, a node situated between two other nodes forwards messages between the two of them. Wormhole attacks are usually administered by two

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

malicious nodes that understate the distance between them by relaying packets along an out-of-bound channel that is unavailable to the other nodes[16].

iii)HELLO attack

The attacker broadcasts a message to all nodes in a network. The packet may be advertising a high quality link to a specific destination. Enough power is used to convince each node that the attacking node is their neighbor. The nodes receiving the packets assume the attacker is very close due to the strength of the received signal, when in fact the attacker is a great distance away. Packets sent from the network nodes at the regular signal strength would be lost. In addition, network nodes may find themselves with no neighbors available to forward packets to a particular destination, since all nodes are forwarding packets towards the attacker. Protocols that depend upon localized information exchange between neighbors for topology maintenance are also subject to the attack. Note that an adversary need not to be able to read or construct legitimate traffic; the attacker needs only to capture and rebroadcast overheard packets with enough power to reach every node in the network [16].

IV.PREVENTION AGAINST ATTACKS OF COGNITIVE RADIO NETWORK

a) Physical layer*:*

i)Primary User Attack :

It provides a received signal strength indicator (RSSI)[19] based transmitter localization technique that can be used . Triangulation with a correction technique considering multipath signals and refraction provides an improved localization method. In a cooperative cognitive radio network each secondary user senses the spectrum periodically and reports the measurement results to the fusion center. The fusion center combines the data and makes a determination as to whether the primary user is present or not. If an attacker injects false positive offset data, the fusion center may determine the primary user is transmitting, when actually it is not.

ii)Objective function Attack:

In naively defining thresholds for each of the adjustable parameters. Communication would be prevented when one or more of the parameters did not fulfill its predefined threshold. The method presented by [20] uses a localized detection threshold at each node, and adapts the threshold with the diminishing behavior of state differences, exploiting the state convergence property. With this scheme, it is more difficult for an attacker to guess all of the thresholds of the neighbors at any instance. This attack can be especially hard to prevent since the malicious node may not be under the direct control of the secondary station or users of the victim network.

iii)Overlapping secondary user Attack:

- **Modifying the modulation scheme**: The use of frequency hopping and direct sequence spread spectrum techniques can make it more difficult to launch effective denial of service attacks. The attacks may still degrade service quality.
- **Detection and prevention of attacks**: Observing the primary user's location and signal characteristics, can help the network identify if a node is performing maliciously.
- **Using authentication and trust models**: In the paper [21] a system is designed to determine a suspicion level, trust value, and consistency value to identify and exclude a malicious user. Nodes become suspicious when the reported channel state is not in agreement with the channel state reported by others.A trust value for each node is calculated over time, and a consistency value reflects the consistent trust value over time. A node with a consistently low trust value will eventually be identified as a possible malicious user and dropped from the network.

iv)Jamming Attack:

In [12], the statistical analysis is a three step cross-layer process. First, statistical analysis is performed on the information gathered from multiple layers. Next, a multiple layer discrepancy search is conducted on the data collected by comparing the data from several layers. In the third step, simple statistical measures are used to determine if there are discrepancies among the data from the network and physical layers using only snapshot data. For instance, the physical layer may report numerous available channels in the area, but few nodes appear in the resultant paths. This may indicate jamming is occurring. Due to the possibility that there can be other reasons the nodes do not appear, there could be a high false alarm rate if a comparison to historic data is not conducted.

b) Media access control layer:

i)Byzantine attack:

A method of detection of Byzantines called Pinokio. Pinokio uses a Misbehavior Detection System (MDS) that maintains a profile of the network's normal behavior based on training data. The MDS detects misbehavior by monitoring the bit rate behavior. By protocol, the bit rate should change periodically and be adjusted by a node contiguously, the bit rates between two nodes should show some reciprocity, and the usage of a low bit rate should occur over a narrow channel. Nodes not exhibiting these characteristics are not acting in a manner conducive to spectrum efficiency, and so are suspect.

ii)Control channel saturation:

The paper [22] presents a method to react to control channel saturation with an alternative decision making strategy based on rendezvous negotiation to ensure user's communication coordination. In essence, the paper presents a mathematical analysis of the resources required for channel negotiation for the network based upon the number of secondary users present and the current channel throughput. When the common control channel usage approaches the point at which the additional allotment of resources to rendezvous channel negotiation will create a saturation condition, the network moves to the phase of rendezvous channel negotiation. This method avoids the situation in which common channel saturation is reached, and there are no resources available for additional channel rendezvous negotiation. Therefore, the early channel analysis and start of negotiation prevents the waste of data

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

transmission resources while the common control channel is saturated.

iii)Control channel jamming:

In the papers [23] the authors present methods to mitigate common control channel jamming for cluster based ad hoc networks using hopping sequences. In this case, the cluster head determines the hopping sequences and identifies the operating control channels for the cluster. Due to the nature of the clustering of the network, the network is partitioned into smaller groups. Therefore, when a jamming attack targets a cluster, the affected network area is reduced.

c)Network layer:

i)Sink Hole:

In Sink Hole attack Countermeasures for the sinkhole attack from outside the network are based upon link layer authentication and encryption. Using authentication, an outside attacker will be unable to join the network. Since the cognitive radio network will only use members for routing, the attacker will be unable to advertise as the best route [24].Countermeasures for the insider attack could be based upon a continually updated trust determination. The cognitive radio network would need a system to monitor dropped or changed packets, and report issues to the fusion center. After analyzing the received data, the base station would flood the network notifying its members of the communication issues recently experienced. It would then drop the attacker as a member of the community.

ii)Worm hole:

One prevention method for the wormhole attack was suggested by [24]. suggest using geographic routing protocols to forward packets in the network. Such protocols construct a topology based on routing traffic physically towards the base station. Using this routing method, it is difficult to attract traffic towards a sinkhole or wormhole. Local nodes would detect an artificial link because they would notice the distance between themselves and the attacker, or between the attackers, is beyond normal radio range.

iii)HELLO attack:

The HELLO attack can be defended against by verifying the bi-directionality of links before using the link established by a message received over the same link. Using a base station as a trusted third party to facilitate the establishment of session keys between parties in the network can provide verification of bi-directionality. The session key allows the communicating nodes to verify each other's identity, as well as provides an encrypted link between them. It should be noted the number of shared keys needs to be limited to prevent the attacker from establishing a link between every node. An alarm should be raised about the detection of an attacker if one node claims to be a neighbor to an inordinate number of nodes [12].

V.CONCLUSION

The cognitive radio network with software defined capabilities will open to users more spectrum frequencies, and hence, enhanced communication opportunities. However, the new technology also provides avenues for new attacks perpetrated by malicious or selfish users with the desire to inhibit communication, capture or change the message, or use the spectrum exclusively. As the cognitive radio network concept matures and comes to fruition, the network security sword play of thrust and parry will continue. The true challenge of the security warrior is prior preparation for the battle.

REFERENCES

[1] Sanjeev Khanna, Santosh S. Venkatesh, Member, IEEE, Omid Fatemieh, Fariba Khan, and CarlA.Gunter, Senior Member, IEEE, Member, ACM- ―Adaptive Selective Verification:An Efficient Adaptive Countermeasure to Thwart DoS Attacks‖ ,IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 3, JUNE 2012 .

[2] ZHANG FU- ―Multifaceted Defence Against Distributed Denial of Service Attacks: Prevention Detection‖ , Mitigation, Division of Networks and Systems Department of Computer Science and Engineering CHALMERS UNIVERSITY OF TECHNOLOGY Gothenburg, Sweden 2012

[3] M. Abadi, M. Burrows, M. Manasse, and T.Wobber, ―Moderately hard,memory-b functions,‖ Trans. Internet Technol., vol. 5, no. 2, pp. 299–327, 2005.

[4] C. A. Gunter, S. Khanna, K. Tan, and S. S. Venkatesh, ―DoS protection for reliably authenticated broadcast,‖ presented at the NDSS, 2004

[5] M. Arshey, C.Balakrishnan, ―Adaptive defense strategy: immunizing shared channel network from dos attacks‖ .International Journal of Emerging Technology and Advanced Engineering , vol. 3, no. 1, pp. 209,2013.

[6] SonicWALL, Inc.1160 Bordeaux Drive Sunnyvale, CA 94089-12091-888-557-6642 http://www.sonicwall.com

[7] Yongle Wu, Beibei Wang, KJRay Liu, TCharles Clancy, Anti-jamming games in multichannel cognitive radio networks, Selected Areas Commun. IEEE J.(1) (2012) 4–15.

[8] Rajni Dubey, Sanjeev Sharma, Lokesh Chouhan, Secure and trusted algorithm for cognitive radio network, in: 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), 2012, pp. 1–7 (IEEE).

[9] Olga. Leon, Juan. Hernandez-Serrano, Miguel. Soriano, Securing cognitive radio networks, Int. J. Commun Syst 23 (5) (2010) 633–652.

[10] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," J. Internet Technology (JIT), vol. 12, no. 2, Mar. 2011, pp. 181–98.

[11] Saman T. Zargar, Martin B.H, Weiss, Carlos E. Caicedo, James B.D. Joshi, Security in Dynamic Spectrum Access Systems: A Survey, University of Pittsburgh, 2011, <http://d-scholarship.pitt.edu/2823/>.

[12] Lijun Qian, Xiangfang Li, Shuangqing Wei, Cross-layer detection of stealthy jammers in multi-hop cognitive radio networks, in: 2013 International Conference, Computing, Networking and Communications (ICNC), 2013, pp. 1026–1030.

[13] Kefeng Tan, Shraboni Jana, Parth H. Pathak, Prasant Mohapatra, On insider misbehavior detection in cognitive radio networks, IEEE Netw. (2013) 5.

[14] Anubhuti Khare, Manish Saxena, Roshan Singh Thakur, KhyatiChourasia, Attacks & preventions of cognitive radio networks survey, Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) 2 (3)(2013) 1002.

[15] Liangping Ma, ChienChung Shen, Bo Ryu, Single radio adaptive channel algorithm for spectrum agile wireless ad hoc networks, in: 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007, 2007, pp. 547–558 (IEEE).

[16] Chris Karlof, David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Netw. 1 (2) (2003) 293–315

[17] A. Popescu, Cognitive radio networks, Communications (COMM), 2012 9th International Conference, 2012, pp. 11–15.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

[18] Alireza Attar, Helen Tang, Athanasios V. Vasilakos, F. Richard Yu, Victor C.M. Leung, A survey of security challenges in cognitive radio networks: solutions and future research directions, Proc. IEEE 100 (12) (2012) 3172–3186.
[19] KaiWang Lu, HaiZhou Ke, Jie Yang, LiangJun Zhang, Research of PUE attack based on location, in: 2012 IEEE 11th International Conference on Signal Processing (ICSP), vol. 2, 2012, pp. 1345–1348 (IEEE).
[20] Qiben Yan, Ming Li, Tingting Jiang,Wenjing Lou, Y. Thomas Hou, Vulnerability and protection for distributed consensus based spectrum sensing in cognitive radio networks, in: 2012 Proceedings IEEE INFOCOM, 2012, pp. 900–908 (IEEE).
[21] Wenkai Wang, Husheng Li, Yan Sun, Zhu Han, Attack proof collaborative spectrum sensing in cognitive radio networks, in: 43rd Annual Conference on Information Sciences and Systems,CISS 2009, 2009, pp. 130–134 (IEEE).
[22] Seyed Morteza Mirhoseni Nezhadal, Reza Berangi, Mahmood Fathy, Common control channel saturation detection and enhancement in cognitive radio networks, Int. J. 3 (2012).
[23] Loukas Lazos, Sisi Liu, Marwan Krunz, Mitigating control channel jamming attacks in multichannel ad hoc networks, in: Proceedings of the Second ACM Conference on Wireless Network Security, 2009, pp. 169–180 (ACM).
[24] Chris Karlof, David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Netw. 1 (2) (2003) 293–315.

BIOGRAPHIES

Padmadas.M is working as a Telecommunication Engineer in a public sector unit under Government of India in Trivandrum, Kerala. He has been managing the design and development of many software projects for more than ten years. He did his Engineering Masters in Computer and Information Technology with specialization in Digital Image Processing and also acquired Masters in Management. He acquired in-depth knowledge and hands-on experience in Telecommunication Switching, Transmission and Radio Systems, Data Communication, GSM, CDMA, Computer Networks, MPLS, Broadband Technologies, Software Project Management, Database Management, Digital Image Processing and Expert Systems using CLIPS. He presented his paper on "A Deployable Architecture of Intelligent Transportation Systems - A Developing Country Perspective" in the IEEE international conference-ICCIC-Coimbatore and made a live demonstration of the project implementation in the ITS conference Pune which is organized by CDAC along with Department of IT, Government of India in coordination with IIT Bombay, IIT Madras and IIM Calcutta .He is the National Level Topper of the Technical Competitive Examination conducted by BSNL in which he selected Data Communication as a special subject. He was awarded for the outstanding performance in BSNL during the year 2006. Now he is undergoing research in Network Security in which he is concentrating on the area of attacks on Network Nodes.

Dr.Krishnan Nallaperumal is a Passionate Researcher, Academic leader and Research Manager with substantial organizational experience. He completed his Doctorate in Computer Science and Engineering-Image Processing and did his masters in Computer and Information Sciences. He is a Senior Member of IEEE. In the initial stage of his career, he served in Indian Space Research Organization and IIT,Kharagpur. Currently he is in the chair of IEEE SIPCICOM: IEEE Signal Processing, Computational Intelligence and Computer Joint Societies Chapter of IEEE Madras Section. He is also in the Chair of – IEEE PODHIGAI Subsection of IEEE Madras Section. He has got extensive experience in handling a wide range of research projects involving Image Processing, image analysis and data mining. He got adequate experience in developing novel algorithms for applications in computer vision and medical imaging. He is an author of about 60 publications,3 books and supervised many research works. He has been leading an Image Processing and Computer Vision laboratory. His area of interests include Image Processing, Computer Vision, Machine Learning, Nonlinear filters for signal and image processing, Wide Dynamic range Imaging, ALPR techniques, Biomedical image analysis, Image Data Mining and Biometric Security.

NellaiNayaki.V, PG Scholar, Center for information Technology and Engineering ,Manonmaniam Sundarnar University, Tirunelveli, India is pursuing her Master Of Philosophy. Her area of interest include Network Security in Computer Networks and Mobile Networks.