A Survey on Attacks in Cognitive Radio Networks

Neema Gonsalves[1]

[1] *PG Student, Dept. Of Information Science and Engineering, Acharya Institute of Technology, Karnataka, India*

***

Abstract - *Now a day, on the entire communication process completely depends on the wireless medium. The wireless technology significantly depends on the radio frequency spectrum, whereas the vacant spectrum is low when compared to their utilization. Thus the effective use of these spectra becomes a necessity and so the CR becomes the promising technology. Security, one of the major factor of any communication network. The challenge over the cognitive radio network is mainly due to transparency to primary users. This paper provides a complete survey on various attacks and security threats in CRNs.*

Key Words: *PUE attack, Spectrum sensing, Legitimate SU, Efficient Utilization of network.*

1. Introduction

Cognitive radio network is a favourable technology for next-generation wireless networks in order to resourcefully utilize the limited spectrum resources and fulfill the rapidly increasing demand for wireless applications and services. The cognitive radio is named as the software defined radio technology that provides license to the unlicensed users without any interpretation. The strategy of CRN architecture is toward the objective of improving utilization of the network completely, rather than just a link spectral.

2. Cognitive Radio Network

CRN, form of wireless communication in which a transceiver can logically detect which communication channels are in use and which are not, and immediately move into vacant channels while evading occupied ones. CRN will considerably enhance the spectrum utilization of impending wireless communication.

The Cognitive radio network devises two types of users: Primary Users and Secondary Users. The major users have the priority to access the channel any time because they are the users with an exact license to communicate over the allocated licensed band. The minor users can access the channel as long as they do not cause interventions to the major users.

Cognitive Radio Network Roles:

1. Spectrum sensing: Identifying the unused Gamut and sharing the gamut without damaging interference with other users.
2. Spectrum Management: Seizing the best available spectrum to encounter user communication requirement.
3. Spectrum Mobility: Preserving continuous communication on requirements throughout the transition to better spectrum.
4. Spectrum Sharing: Providing the fair spectrum scheduling technique among synchronized CR users.

3. Classification of Attackers

Since the refuge problem caused by PUE attacks was recognized, various types of PUE attacks have been studied. We now bring together different types of PUE attackers related with their classification criteria.

3.1 Selfish and Malicious Attackers:

A selfish attacker wishes to steal bandwidth from genuine SUs for its personal transmission. Invader observers the spectrum. Once an unused spectrum band is revealed, it contends with the legitimate SUs by imitating the primary signal. A selfish attacker is a sensible attacker in the sense that if it is noticed by the legitimate SUs and the SUs retrieve the spectrum opportunity by switching back to the band, it has to vacant the band. The purpose of a malicious attacker, however, is to interrupt the DSA of SUs but not to abuse the spectrum for its private transmission. Being different from a selfish attacker, the malicious attacker may imitate a primary signal in both a vacant spectrum band and a band presently used by legitimate SUs. When an attacker attacks a link being used by a legitimate SU, there is the opportunity that the SU fails to determine the signal, and hence, intrusion happens between the attacker and the legitimate SU.

3.2 Power-Fixed and Power-Adaptive Attackers:

The capability to emulate the power stages of a primary signal is essential for PUE attackers, because most SUs hire an energy detection technique in spectrum sensing. A power-fixed attacker practices a constant predefined power level irrespective of the authentic transmitting power of the PUs and the neighboring radio environment. Compared to the power-fixed attacker, the power-adaptive attacker is intense in the sense that it can adjust its transmitting power according to the expected transmitting power of the primary signal and the channel parameters. Specifically, the attacker employs an estimation technique and a erudition method against the detection by the legitimate SUs.

It is demonstrated that such an advanced attack can defeat a innocent defense approach that focuses only on the received signal power.

3.3 Static and Mobile Attackers:

The position of a signal source is also a key feature to validate the characteristics of an attacker. A static attacker has a fixed location that does not change in all sequences of attacks. By exhausting positioning techniques such as time of arrival or enthusiastic positioning sensors, the location of a static attacker could be revealed. A static attacker can effortlessly be acknowledged due to the difference between its location and that of the PUs. A mobile attacker will frequently change its location so that it is hard to trace and discover. A practical detection approach that adventures the correlations between RF signals and acoustic information is proposed in to validate the existence of a mobile PUE attacker.

4. Attacks in CRN

There are different attacks in CRNs, only few attacks we considered through three major layers: physical layer, MAC layer, network layer.

4.1 Physical Layer:

This layer is the lowest layer of the protocol. It provides boundary to the transmission medium. It comprises of anything that is used to sort two network devices communicate, such as the network cards, fiber or the atmosphere. The operation of the CRN is more complicated than other wireless communication networks because the cognitive radio uses the frequency spectrum vigorously.

1. **PUE Attack:** The cognitive radio network needs ability to differentiate between the major and minor user signals. In the primary emulation attack, an attacker may adapt their air boundary such that it imitates the primary user's signal features causing other secondary users to falsely determine that the frequency is in use by the major user, and so free the frequency. The fraud may perform the attack selfishly, so he can use the spectrum, or maliciously, so the other legitimate users will have their communication disturbed, resulting in a denial of service attack. Therefore, the primary user can lead to an unbiased function attack.

2. Objective function attack: Cognitive radios are adaptive to the situation. Many radio factors are available for manipulation in the effort to adjust the radio to the environment by make the most of objective functions, and therefore the radio's ability to transfer over the medium. Belief manipulation attacks apply to an attack on any learning algorithms that make use of objective functions. Parameters manipulated include bandwidth, power, modulation, coding rate, frequency, frame size, encryption type, and channel access protocol.

3. Overlapping secondary user: Such a condition places dynamic spectrum access sharing at danger through both objective function and primary user vulnerabilities by one malicious node. A mischievous user in one network may transmit signals that cause destruction to the primary and secondary users of both networks. Signals conducted maliciously may provide false sensing information, thereby adversely affecting the objective function in one or both networks. The mean user may intermittently falsely match the primary users of each network causing each network to vacate the channel.

4. **Jamming:** One of the most basic types of attacks in the CRN'S, efforts to adversely affect the signal to noise ratio. In this attack, the attacker intentionally and continuously transmits on a licensed band, making it unusable by the primary or other secondary users. The attack is intensified by transmitting with high power in several spectral bands. Jamming can be spotted with triangulation and energy based techniques. However, the time vanished with these techniques allows the attacker to rigorously impact the network. A mobile attacker can be even more tough to locate.

4.2 Link Layer Attacks:

1. Spectrum Sensing Data Falsification: In the Byzantine attack, the attacker shoot up the false sensing information into the decision stream is a legitimate member of the network and is referred to as the Byzantine. Byzantines may perform the attack to selfishly gain increased spectrum availability for themselves, or the attackers may have a goal of distracting the throughput of the network for other immoral reasons.

2. Control channel saturation: The control channel saturation attack is based on the circumstance that if a cognitive radio is not capable to complete negotiations during the restricted time of the control phase, the radio defers from transmission during the next data phase. This state may naturally occur when the channel is saturated by a large number of challenging cognitive radios. An attacker can broadcast a large number of packets with the determined to saturate the control channel. By sending different kinds of packets, a malicious node reduces the danger of detection. Combining the control channel saturation attack with the minor window back off attack the attacker may be able to guarantee the malicious node captures the control channel before other users.

3. **Control channel jamming**: Control channels enable the collaboration among cognitive radio users. As a single point of failure, CCJ is the most active and energy efficient

way for an attacker to destroy the complete network system. With common control channel jamming, receivers are not permitted to receive valid control messages when a strong signal is injected into the control channel. This results in denial of service for genuine users of the network.

4.3 Network layer Attacks:

The network layer delivers the capability to route data packets from a source node on one network to a destination node on another network, while retaining quality of service. It also performs fragmentation and reassembly of packets, if necessary. The CRN shares security disputes with communication networks due to the three shared architectures of mesh, ad hoc, and infrastructure. CNRs also share similarities with wireless sensor networks. These include multi-hop routing protocols and power constraints. There are special challenges faced by CNRs due to the required transparency of the network activities to the primary user. Routing in the CRN is further complicated by the requirement of the radio to vacate the frequency when the major user is sensed as present. Cognitive radio security vulnerabilities are therefore also genetic from these architectural requirements.

1. **Sinkhole:** CRNs often use multi-hop routing. A sinkhole attacker takes help of multi-hop routing by advertising itself as the best route to a specific destination. This bustle spurs neighboring nodes to use it for packet forwarding. In addition, the neighbors of the attacker will announce the offender as the best route, creating a 'sphere of influence' for the attacker. The attacker can initiate 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 properly for a time. After trust has been established and publicizing of the node as the best route has been propagated through the local area, the offender can begin other types of attacks, such as eavesdropping.

2. ***Wormhole:*** This attack is closely related to the sinkhole attack. Basically, an attacker channels 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 located between two other nodes forwards messages between the two of them. Wormhole attacks are usually managed by two malicious nodes that minimize the distance between them by relaying packets along an out-of-bound channel that is unavailable to the other nodes.

3. **HELLO Attack:** The attacker broadcasts a message to all nodes in a network. The packet may be advertising a great quality link to a specific destination. Enough power is used to prove each node that the attacking node is their neighbor. The nodes receiving the packets accept 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 link nodes at the regular signal strength would be lost. In addition, nodes may find themselves with no neighbors available to forward packets to a particular destination, since all nodes are forwards the packets in the direction of the attacker. Protocols that depend upon local information exchange between neighbors for network maintenance are also subject to the attack. Note that opponents need not to be able to read or create legitimate traffic; the attacker needs only to seizure and rebroadcast overhead packets with enough power to reach every node in the network.

5. Impact of Attacks in CR Networks

The existence of PUE attacks causes a number of difficulties for CR networks. The list of potential consequences of PUE attacks is below.

5.1 **Bandwidth waste:** The eventual objective of deploying CR networks is to address the spectrum underutilization that is caused by the existing fixed spectrum usage policy. By energetically accessing spectrum holes, SUs are able to recover these otherwise wasted spectrum resources. However, PUE attackers may steal the spectrum holes from the SUs, leading to spectrum bandwidth waste again.

5.2 **QoS degradation:** The arrival of a PUE attack may brutally degrade the quality of service of the CR network by destroying the stability of secondary services. For instance, a malicious attacker could distract the ongoing services and force the SUs to continuously change their operating spectrum bands. Numerous spectrum handoffs will bring unproductive delay and jitter for secondary services.

5.3 **Connection unreliability:** If a real-time secondary service is criticized by a PUE attacker and finds no available channel when carrying out spectrum handoff, the service has to be dropped. This real-time service is then concluded due to the PUE attack. In principle, the secondary services in CR networks intrinsically have no guarantee that they will have steady radio resource because of the nature of DSA. The existence of PUE attacks considerably increases the connection unreliability of CR networks.

5.4 **Denial of service**: Consider PUE attacks with great attacking frequency; then the attackers may conquer many of the spectrum opportunities. The SUs will have inadequate bandwidth for their transmissions, and hence, some of the SU services will be interrupted. In the worst case, the CR network may even find no frequencies to set up a common control channel for transporting the control messages. As a consequence, the CR network will be deferred and unable to serve any SU. This is called DoS in CR networks.

5.5 **Interference with the primary network:** Though a PUE attacker is interested to steal the bandwidth from the SUs, there is the chance that the invader generates added interference with the primary network. This occurs when the attacker fails to detect the happening of a PU. On the other hand, when the SUs are attacking a PUE attack, it is also possible to mistakenly identify the true PU as the attacker and restrict with the primary network. In any case, causing intervention with the primary network is strictly prohibited in CR networks.

6. CONCLUSIONS

This paper deals with the basics of cognitive radio networks. We can see the different types of users and their priority to access the channels. Security is a major factor for data transmission in any type of network. Then we concentrate on different types of attacks and its impact on the networks.

REFERENCES

[1] Attacks in Cognitive Radio Networks (CRN) - A Survey, S. Bhagavathy Nanthini , M. Hemalatha, D. Manivannan1 and L. Devasena, Vol 7(4), 530–536, April 2014.

[2] Securing Cognitive Radio Networks against Primary User Emulation Attacks, Rong Yu, Yan Zhang, Yi Liu, Stein Gjessing, and Mohsen Guizani, December 2016.

[3] Analysis of Attacks in Cognitive Radio Networks, M.Padmadas, Dr.N.Krishnan, V.Nellai Nayaki, Vol. 4, Issue 8, August 2015.

[4] Future Directions in Cognitive Radio Network Research, Peter Steenkiste, Douglas Sicker, Gary Minden, Dipankar Raychaudhuri, March 9-10, 2009.

[5] Cognitive Radio Network Architecture: Part I - General Structure, K. –C. Chen, Y. –J. Peng, N. Prasad, Y. –C. Liang, S. Sun.

[6] Defense against Primary User Emulation Attacks in Cognitive Radio Networks, Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed, January 2008.

[7] A. Popescu, Cognitive radio networks, Communications (COMM), 2012 9th International Conference, 2012.

[8] A survey of security challenges in cognitive radio networks: solutions and future research directions, Alireza Attar, Helen Tang, Athanasios V. Vasilakos, F. Richard Yu, Victor C.M. Leung , IEEE 2012.

[9] Research and analysis on cognitive radio network security. Computer Science & Communications, Tang L, Wu J., April, 2012.