Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

Overview of Challenges in Securing a Cognitive Radio Network

Simi Ranjith
Asst. Professor, Dept. of ECE
NHCE
Bengaluru, India

Dr. Sanjay Jain
HOD, Dept. of ECE
NHCE
Bengaluru, India

***Abstract*— Going forward, wireless communications will require more efficient use of licensed radio frequency spectrum. The cognitive radio (CR) technology provides a suitable framework for this purpose. Cognitive Radio Network (CRN) is a promising wireless network where smart devices are able to opportunistically exploit the spectrum holes and optimize the overall radio spectrum use. Secure communication is the key of success for any wireless network. As cognitive radio networks are wireless in nature, they face all classic threats present in the conventional wireless networks. Along with the realization of cognitive radios, new security threats have been raised. In this paper, we discuss various security threats which are unique to CRNs along with various DoS attacks in ad hoc cognitive radio networks spread across different protocol layers.**

Keywords*— Cognitive Radio; Cognitive Radio Network; CRNs security; DoS attack.

I. INTRODUCTION

In the digital era frequency spectrum is a vital natural resource and due to its importance, is also one of the heavily regulated resources. In the last decade almost all the spectrum suitable for wireless communication has been allocated. But the spectrum occupancy between various wireless applications is not uniformly distributed. This has led to an unbalanced spectrum usage. Some parts of the spectrum are overcrowded, while others are rarely used. As business try to satisfy ever growing need for speed and seem less data connectivity, more and more effective use of available radio spectrum is required.

A novel idea was proposed by Mitola [1], for the opportunistic use of the under-utilized portions of the spectrum, using novel devices called Cognitive Radios (CR). CR is an opportunistic communication technology designed to utilize the maximum available licensed bandwidth for unlicensed users. The main goal of cognitive radio is to optimize the radio spectrum by dynamically and efficiently exploiting the spectrum white spaces. When interconnected, CRs form Cognitive Radio Networks (CRNs).

II. CR NETWORK: AN OVERVIEW

CRNs have two types of users, namely primary and secondary. Primary users (PRI) are users who have purchased license for the spectrum and hence have rights to access it. However, secondary users (SEC) are unlicensed users (or CR terminals) having CR capabilities to opportunistically access the unused spectrum. A basic difference between CR network and traditional Wireless network is that in case of the CR network, there is no statically allocated fixed spectrum for use by the secondary user. Therefore, a secondary user in a CR network, using a particular channel to communicate with its neighbour, might have to give way to a primary user when it requires service on that channel. Due to this fundamental difference, data communication in CR networks is always a challenge.

III. SECURITY CHALLENGES IN CR NETWORK:

CRNs use wireless technology for transmission and reception and hence are prone to all common security threats found in the traditional wireless networks such as MAC spoofing, congestion attacks, jamming attacks, etc. In general, due to their open nature, wireless networks are susceptible to several attacks targeting the physical or medium access (MAC) layers. Attacks targeting the physical layer through RF jamming can severely disrupt network's operation. Above and beyond the traditional wireless network security challenges, CRNs face new security threats and challenges that have come up due to their unique cognitive characteristics.

A basic operation of the CRs is spectrum sensing. Whenever, a primary signal is detected, CRs have to vacate the specific spectrum band. Malicious users can mimic incumbent transmitters so as to enforce CRs vacate the specific band. This is called as primary user emulation attack (PUEA). Another attack exists that is related to collaborative spectrum sensing, a technique used to improve spectrum sensing in fading environments where multiple CRs collaborate. Here, a malicious CR can provide false observations on purpose. This is called as spectrum sensing data falsification (SSDF) attack. IEEE 802.22 [2] is the first standard for enabling the use of the fallow TV bands by infrastructure single-hop CRNs with the presence of one base station (BS) that performs spectrum management. This standard supports the provision of broadband fixed wireless data in sparsely populated rural areas and it has a security mechanism for authentication, data integrity, etc. However, several attacks can be feasible against this mechanism such as the beacon falsification attack (BF). As CRs adopt the layered architecture of the conventional networks, several cross-layers attacks are possible. These can include a combination of a SSDF attack with a small-back off window attack (SBW), and the so-called lion attack [3]. CRs are usually based on Software Defined Radios (SDRs), devices with radio functionalities implemented in software. SDRs are vulnerable to a number of software and hardware related threats.

In this paper we attempt to describe and classify security threats related to Cognitive Radios and Networks

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

IV. CR NETWORK SECURITY ATTACKS AN OVERVIEW

This section describes various attacks against cognitive radios and network.

A. Primary user emulation attacks(PUEA)

A fundamental characteristic of a CR is its ability for spectrum sensing, as it shall use the spectrum in an opportunistic manner. This means that the CR has to vacate a currently used spectrum band if an incumbent signal is detected. In this case, CRs perform spectrum hand-off seeking for different spectrum holes for transmissions. Performing spectrum hand-off very often results in degradation of the CR performance since more time for sensing of the spectrum is required, and this decreases the available time for accessing the spectrum. This inherent operation of CRs can be exploited by adversaries that mimic incumbent signals. Nodes launching PUEAs can be of two types:

• Greedy nodes that by transmitting fake incumbent signals force all other users to vacate a specific band (spectrum hole) in order to acquire its exclusive use.

• Malicious nodes that mimic incumbent signals in order to cause Denial of Service (DoS) attacks. Malicious nodes can co-operate and transmit fake incumbent signals in more than one band, thus causing extensive DoS attacks making a CRN hop from band to band, severely disrupting its operation. Furthermore, malicious nodes could also cause DoS attacks to PRI user networks by creating harmful interference.

Regardless of the type of misbehaving node (greedy or malicious), the consequences to a CRN are the same: operation disruption and unfairness among the nodes. Referring to the cognitive cycle, shown in Fig. 1, a PUEA can affect all of its parts. Initially, PUEAs affect the Radio Frequency (RF) environment by "spamming" it with fake incumbent signals. An immediate effect of RF spamming is a cascading phenomenon affecting spectrum sensing, analysis, and decision.

B. Spectrum sensing data falsification attacks (SSDF)

Several transmission features such as signal fading, multi-path, etc., can cause the received signal power to be lower of what path loss models have predicted [4]. This leads to undetected primary signals and harmful interference to PRI users. There are two types of fading: shadow fading that is frequency independent, and multi-path fading that is frequency dependent. Shadow fading can cause the "hidden node" problem where a SEC user, although located within the transmission range of a primary network, fails to detect primary transmissions. Fig. 2 shows a primary transmitter, a number of PRI users and several SEC users. SEC user1 fails to detect the transmission of incumbent signals because of shadow fading, so it accesses the incumbent frequency band causing harmful interference to PRI user1. A solution to this problem is the collaborative spectrum sensing technique [5], [6], where a number of users sense the environment and send their observations to a fusion center (FC). FC then fuses the provided information taking the final decision regarding the presence or absence of incumbent transmissions.

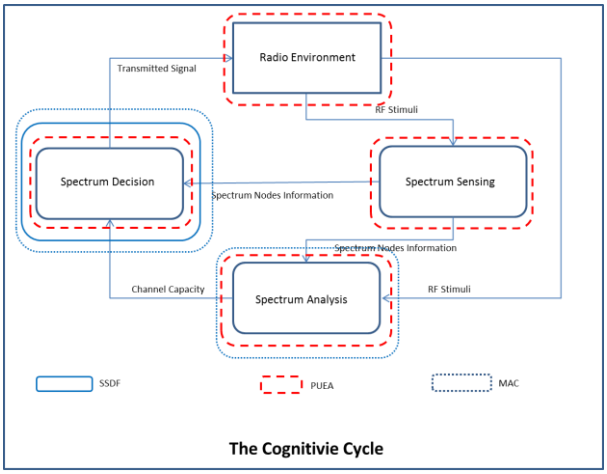

Fig 1: The Cognitive Cycle

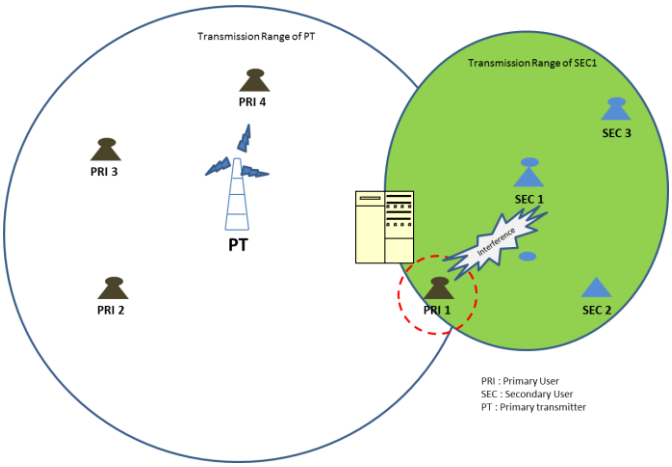

Fig 2: Hidden Node Problem

Another type of sensing is the collaborative distributed sensing where no FC is used. In this case, each SEC user makes its decision based not only on its observations but also on observations shared by other SEC users. For both types of collaboration, distributed or centralized, SEC users have to share their observations or transmit them to a FC. There is always the possibility that one or more SEC users send false observations, intentionally or unintentionally. Similarly to PUEAs, nodes sending false observations can be categorized as follows:

Malicious users that send false observations in order to confuse other nodes or the FC. They aim to lead FC or the rest of the nodes to falsely conclude that there is an on-going incumbent transmission where there isn't, or make them believe that there are no incumbent transmissions when there are. In the first case, the legitimate SEC users will evacuate the specific band, while in the second case they will cause harmful interference to the PRI users.

Greedy users continuously report that a specific spectrum hole is occupied by incumbent signals. The goal of these users is to monopolize the specific band by forcing all other nodes to evacuate it.

Unintentionally misbehaving users that report faulty observations for spectrum availability, not because they are malicious or greedy, but because parts of their software or hardware are malfunctioning. Regardless of the type of the

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

misbehaving users, the reliability of collaborative spectrum sensing can be severely degraded by faulty provided observations. This is called as *Spectrum Sensing Data Falsification* (SSDF) attack. Fig. 3 depicts an example of this type of attack. FC receives observations from SEC users and then it decides about the presence or absence of primary transmissions. This type of cooperation can be exploited by malicious users that send malicious reports to the FC on purpose.

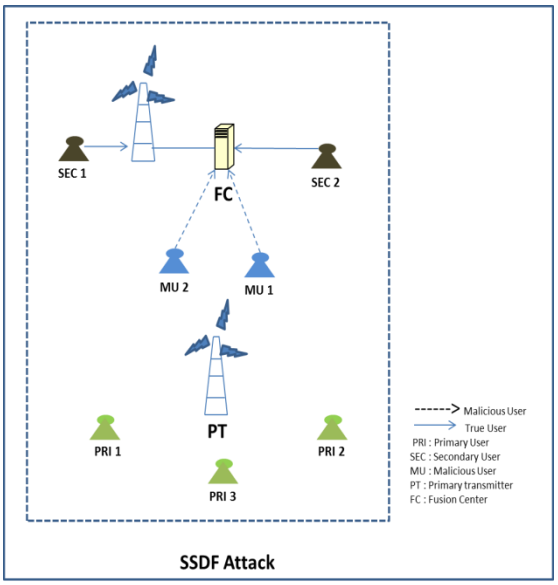

Fig 3: SSDF Attack

Even a single malicious user can substantially degrade the performance of collaborative sensing [7]. Referring to Fig. 1, SSDF attacks affect the spectrum decision part of the cognitive cycle as faulty observations can lead to faulty decisions

C. Common control channel(CCC) threats and vulnerabilities

CCC plays an important role in enabling CRs to exchange control information. It is an out-of-band channel, which means that the control information and messages are being transmitted using a pre-defined frequency channel, which is different than the one(s) used for exchanging the actual data (that are known as in-band channels). CCC is used for the exchange of several control information regarding for example collaborative sensing, channel negotiation, spectrum hand-off, etc. Protecting the CCC is very important, as this could be the first mechanism that a sophisticated adversary will try to compromise. If he succeeds, network performance will be severely affected since CCC is the main mechanism for controlling the network operations.

The threats that a CCC faces can be categorized as follows:

MAC spoofing, where attackers send spurious messages aiming to disrupt the operation of CRN (e.g. channel negotiation). Multi-hop CRNs are more vulnerable to this type of attack as there is no central entity to control the authentication between the nodes and protect data integrity.

Congestion attacks, where attackers flood CCC in order to cause an extended DoS attack.

Jamming attacks, where attackers cause DoS attacks at the physical layer by creating interference.

Cognitive radio networks can have three types of network structures according to the topology of the secondary users: ad hoc cognitive radio networks,

Infrastructure based cognitive radio networks and mixed cognitive radio networks. Ad hoc cognitive radio networks also called multi-hop cognitive radio networks where cognitive radios can communicate with each other through ad hoc connection. In infrastructure based cognitive radio networks, cognitive radio users communicate by base station of cognitive radio networks. In mixed cognitive radio networks, cognitive radio users communicate with others either by base station or by ad hoc connection.

V. DoS ATTACKS IN COGNITIVE RADIO NETWORKS

A denial of service is characterized by an explicit attempt by an attacker to prevent legitimate users from gaining access to the desired network resources. An attacker may attempt to: “flood” a network and thus reduce a legitimate user’s bandwidth, prevent access to a service, or disrupt service to a specific system or a user. Denial of service attacks often attempt to monopolize network resources. DoS attacks have the ability to destruct an entire wireless networks. Therefore DoS is treated as the highest security risk for any wireless network.

Cognitive radio networks as special wireless communication networks are vulnerable to denial of service attacks [8].

This section surveyed the possible denial of service attacks in ad hoc cognitive radio networks in different layers such as in physical layer, link layer and network layer.

A. DoS Attacks in Physical Layer

In cognitive radio networks, not only conventional jamming attacks can launch DoS attacks but also other attacks produced by characteristic of cognitive radio. In cognitive radio networks, spectrum sensing technology is adopted to detect the presence of primary users and quit the frequency band as quickly as possible if the corresponding primary user emerges in order to avoid interference to primary users. We can say that spectrum sensing is the most important difference of the physical layer between cognitive radio networks and conventional networks.

Due to the introduction of the spectrum sensing, two kinds of new denial of service attacks in physical layer may be launched. First, selfish secondary user or malicious secondary user launches Primary User Emulation (PUEA) attack to prevent other legal secondary users from using the idle spectrum band. Second, attackers may launch the mask primary user attack [8] to avoid the primary users to use the licensed spectrum band.

1) Conventional jamming attack: The simplest jamming attack launched from a secondary user to another legal secondary user is to continuously transmit high-power signals on the available channel, preventing being attacked from using the idle spectrum. However, this type of jamming is expensive in terms of energy cost, and can be easily detected. An alternative means is that an attacker transmits jamming packets at constant intervals.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

2) Primary User Emulation Attack (PUEA): In cognitive radio network, when a primary user is detected in a given frequency band, all secondary users should avoid accessing the band, however, when a secondary user is detected, other secondary may choose to share that same band. So attackers may emulate the characteristic of the primary user to launch Primary User Emulation attack (PUEA). There are two kinds of PUEAs: selfish PUEA and malicious PUEA. In selfish PUEA, an attacker aim to maximize its own interests of using spectrum. When a selfish PUE attacker detects an idle frequency band, they prevent other secondary users from competing for the band by transmitting signals that emulate the signal characteristics of the primary user signals. In malicious PUEA, the objective of this attack is to prevent legitimate secondary users from detecting and using fallow licensed spectrum bands. A malicious attacker does not necessarily use idle spectrum bands for its own communication purposes. Both attacks could have destructive effects on cognitive radio networks.

3) Mask primary user attack: In order to avoid interfering with primary users, secondary users should vacate the spectrum band as soon as they detect the presence of the primary users. The attacker may try to mask primary users so that the secondary users will mistakenly communicate and make interference to primary users. The kind of attack is called mask primary user attack or interference to primary users' attack [8]. In this attack, attackers achieve the goal to interference the primary users by making secondary users not receive the message of the presence of the primary user. A non-cooperating cognitive radio user is more susceptible to this attack.

B. DOS Attacks in Link Layer

Link layer frames the data and regulate the access to physical resources. There are multiple differences of link layer between the conventional wireless network and cognitive radio network. First, the characteristic of communication channels are different. In conventional networks, the users have fixed channels to use according to their protocols. However, in cognitive radio networks the channels are not fixed and may exist anywhere in the whole spectrum due to accessing spectrum dynamically. Another difference is that cognitive radio users always utilize multiple channels to transmit data simultaneously in order to increase the throughput. DoS attacks at the link layer are a significant threat to the availability of network services. An attacker's objective in launching a DoS attack is to prevent or hamper non-malicious nodes from accessing the channel.

1) Vulnerabilities in ad hoc CR MAC Protocols

a) Lack of MAC layer authentication: There is security sub layer that provides confidentiality and authentication of MAC frames in wireless regional area network. The security sub layer defeat MAC-layer DoS attacks by preventing the modification or forgery of MAC frames. But in an ad hoc CR network there is no trusted entity to act as a server to control distribution of keying material. Without an authentication mechanism, adversaries can forge MAC control frames to launch DoS attacks.

b) Control channel saturation problem: The common control channel is used for supporting the transmissions coordination and spectrum related information exchange between cognitive radio users. The control channel can become a bottleneck for network performance in the MAC layer of CR network. So reliable and dynamic changing control channel must be devised.

c) Predictable control channel hopping sequence

If control frames are exchanged in unencrypted form, the candidate channel list can be readily acquired by any secondary user, including an adversary. With the candidate channel list, an attacker can easily predict the next control channel in the hopping sequence. This capability enables the attacker to continually saturate the control channel, even if the control channel continuously hops among different bands due to the presence of incumbent signals.

2) DoS attacks in link layer

a) Common control channel attack: From the perspective of security, common control channel plays a key role in network availability. If attackers can successfully saturate the control channel, they can severely obstruct the channel negotiation and allocation process, thus causing denial of service. In a multi-hop CR MAC protocol, an adversary can readily forge channel negotiation frames to launch a DoS attack. Such spurious MAC frames can saturate the control channel so that legitimate users cannot use their share of the control channel to negotiate and assign data channels. Attacker can simply transmit periodical pulses which have the same spectrum as common control channel of cognitive radio network but with higher power than primary users.

b) False feedback attack:

A malicious secondary user prevents legal secondary users using idle spectrum band by false information feedback of spectrum sensing.

C. DOS Attacks in Network Layer

The Network Layer is responsible for end-to-end packet delivery including routing through intermediate hosts while maintaining the quality of service and error control functions [9].Cognitive radio network makes the routing scheme more complicated because of using of the dynamic spectrum band relative to conventional networks where the paths are designed directly by the router. However, it is different in cognitive radio networks. Since the spectrum can be accessed openly, reconfiguration information greatly influences the routing scheme. Network layer security provides end-to-end security across a routed network and can provide authentication, data integrity, and encryption services. These services are only provided for specific network and transport layer services. Once the network endpoints are authenticated, IP traffic flowing between those endpoints is protected. However, all other non-IP traffic is not secured and is unprotected [10].

The following ways are adopted to launch DoS attacks in network layer [11]:

1) Black hole attacks: force all packets to go through an adversary node to launch DoS attacks.

2) Gray hole: drop some packets to launch DoS attack.

3) Wormhole: use a tunnel between two attacking nodes to launch DoS attack.

4) Rushing attack: drop subsequent legitimate RREQ to launch DoS attack.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 01, January-2016

5) Blackmailing: ruining the routing reputation of a Network layer security provides end-to-end security across a routed network and can provide authentication, data integrity, and encryption services. These services are only provided for specific network and transport layer services. Once the network endpoints are authenticated, IP traffic flowing between those endpoints is protected. However, all other non-IP traffic is not secured and is unprotected [10].

The following ways are adopted to launch DoS attacks in network layer [11]:

1) Black hole attacks: force all packets to go through an adversary node to launch DoS attacks.

2) Gray hole: drop some packets to launch DoS attack.

3) Wormhole: use a tunnel between two attacking nodes to launch DoS attack.

4) Rushing attack: drop subsequent legitimate RREQ to launch DoS attack.

5) Blackmailing: ruining the routing reputation of a node to launch DoS attack.

6) Inject extra traffic: consume energy and bandwidth to launch DoS attack.

7) Detours: force sub-optimal paths to launch DoS attack.

8) Rooting loop: force packets to loop and consume bandwidth and energy to launch DoS attack

VI. CONCLUSION

In this paper, we discussed various security issues and classification of attacks in CRNs .We also surveyed Denial of Service (DoS) attacks in different protocol layers in ad hoc CRNs. With increased adoption of CR, threats specific to CRN are growing fast. Hence an efficient cross-layer design is required to be designed for CRNs to provide protection against DoS attacks.

REFERENCES

[1] J. Mitola, “Cognitive radio for flexible mobile multimedia communications,” in Proc. IEEE International Workshop on Mobile Multimedia Communications (MoMuC), 1999, pp. 3–10.

[2] C. Stevenson, G. Chouinard, W. Hu, S. Shellhammer, and W. Caldwell, “IEEE 802.22: The first cognitive radio wireless regional area network standard,” IEEE Commun. Mag., vol. 47, pp. 130–138, 2009.

[3] J. Hern´andez-Serrano, O. Le´on, and M. Soriano, “Modeling the lion attack in cognitive radio networks,” EURASIP Journal on Wireless Communications and Networking, vol. 2011, p. 10 pages, 2011.

[4] R. Chen, J. Park, T. Hou, and J. Reed, “Toward secure distributed spectrum sensing in cognitive radio networks,” IEEE Commun. Mag., vol. 46, pp. 50–55, 2008.

[5] T. Aysal, S. Kandeepan, and R. Piesewicz, “Cooperative Spectrum Sensing with Noisy Hard Decision Transmissions,” in Proc. ICC, 2009, pp. 1–5.

[6] Y. Chen, “Collaborative spectrum sensing in the presence of secondary user interferences for lognormal shadowing,” Wireless Communications and Mobile Computing, 2010.

[7] W. Wang, H. Li, Y. Sun, and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks,” in Proc. CISS, 2009, pp. 130–134.

[8] Sethi A,Brown T X, “Potential cognitive radio denial-of-service vulnerabilities and countermeasures,”International Symposium on Advanced Radio Technologies,February 2007.

[9] http://en.wikipedia.org/wiki/Network_Layer

[10] http://www.lucidlink.com/.../Link_and_Network_Layer_White paper.pdf

[11] http://www.ccs.neu.edu/home/ahchan/wsl/symposium/noubir. ppt.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)