VOL. 11, NO. 17, SEPTEMBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A SURVEY OF SECURITY ISSUES IN COGNITIVE RADIO NETWORK

Elangovan K. and Subashini S.
School of Electronics Engineering, VIT University, Chennai, India
E-Mail: elangovan.k2013@vit.ac.in

ABSTRACT

In wireless communication systems it is important to identify the suitable frequency spectrum bands for future functionalities. The radio spectrum is allocated to various functions, services and applications but most part of the spectrum is not utilized efficiently. To solve this underutilization of frequency spectrum problem Cognitive Radio (CR) concept has been put forwarded. This survey paper brings the importance of cognitive radio in the dynamic spectrum access and the various CR attacks. The main objective of Cognitive Radio is to utilize the limited and under-utilized frequency spectrum effectively without disturbing the primary users. As the effect of it, Cognitive radio has to interact with the environment in which it is operating and to find the unused band of spectrum to transmit accordingly and subsequently adapts to the environment in which it is operating. This paper categories the various Cognitive Radio Network attacks and various issues related to it.

Keywords: cognitive radio, cognitive cycle, cognitive attacks, primary emulation attack.

1. INTRODUCTION

The demand for wireless radio spectrum is increasing rapidly. As the number of users and data rates is increasing day by day it is very difficult to accommodate them within the limited radio frequency spectrum. Federal communication commission (FCC) allocates spectrum to licensed users. Most of the spectrum is not efficiently used by them. Licensed users are called primary users and the unlicensed users are called secondary users. Cognitive radio technology is the intelligent network which makes use of unused spectrum of primary users. Spectrum scarcity problem is solved by cognitive radio network by allowing the unlicensed or secondary users to make use of primary user's unused spectrum without causing interference. The essential security mechanism is necessary for the successful implementation of cognitive radio network and the realization of benefits. The taxonomy of security threat is presented and the active threat related to cognitive radio is shown. Different types of active attacks related to spectrum sensing manipulation like primary emulation attacks, spectrum sensing data falsification are discussed. Network layer attacks such as the sinkhole attack, hello flood attack, and transport layer attack like lion attacks, sybil attacks are discussed here.

2. OVERVIEW OF COGNITIVE RADIO NETWORK

Cognitive radio is the possible approach of implementing dynamic spectrum access on software defined radio. It is an intelligent network that effectively changes environment to make use of the spectrum. Cognitive radio network consists of licensed users called primary users (PU) and unlicensed users called secondary users (SU) or cognitive radio users. Primary users can only use their licensed spectrum whereas Cognitive Radio users can utilize primary user's spectrum bands when it is free.

2.1. Cognitive cycle

The process of spectrum sensing and sharing can be explained by a cognitive cycle. A simpler model of cognitive cycle is shown above. The sensing information includes spectrum unused spaces, PU& SU locations. The learning process includes interference limits, channel capacity and network parameters. The adaptation takes place at any of single or cross layered layer approach.

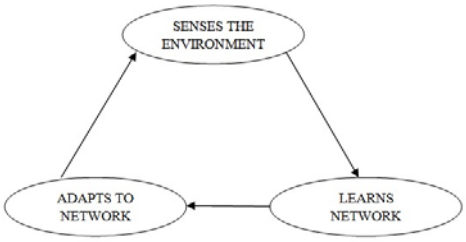

Figure-1. A Simple cognitive cycle model.

Cognitive radio network is equipped with cognitive radio base station (BS). The Spectrum brokers divide the spectrum to various cognitive radio networks for proper spectrum sharing of both licensed and unlicensed band. It makes use of Adhoc access to communicate with other CR users. It uses its own base station to utilize licensed and unlicensed band. The main focus of cognitive radio network is on the detection of primary users (licensed users).So effective methods of spectrum sharing are necessary for efficient utilization of spectral bands.

Cognitive radio performs three access types:

a) Cognitive radio network access: cognitive radio users can access their own cognitive base station on both licensed and unlicensed bands. Spectrum sharing is independent of primary network.

b) Primary network access: cognitive radio users can also access licensed bands through primary base station.

c) Cognitive radio ad-hoc access: cognitive radio users can communicate with other cognitive users through

ad-hoc network for both licensed and unlicensed bands.

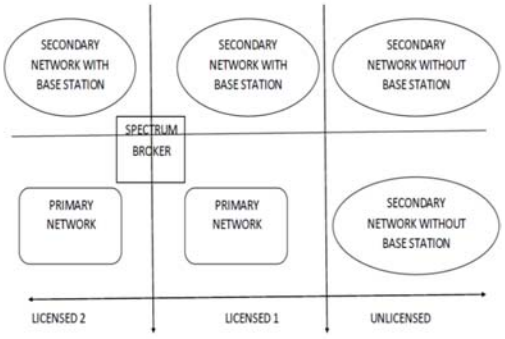

Figure-2. Architecture of Cognitive Radio Network.

For spectrum management in cognitive radio network spectrum sensing plays a vital role, spectrum decision, spectrum sharing, spectrum mobility keeps the network to carry out their functions properly.

2.2 Spectrum sensing

Spectrum sensing is the process of finding radio spectrum when it is not used by the licensed users. Efficient spectrum sensing makes the cognitive radio network more effective. Cognitive radio finds spectrum opportunity based on proactive or periodic and reactive or on demand. A simple approach of spectrum sensing is to detect the primary user's receiver in the operating range of spectrum. But, it is not possible in the entire situation so generally primary transmitter detection based sensing is used.

Spectrum sensing is classified into cooperative sensing and non cooperative sensing. Cooperative sensing involves centralized and decentralized schemes. Non-cooperative involves primary user transmitter detection.

2.2.1 Non-cooperative sensing

A secondary user uses non-cooperative spectrum sensing to detect the primary user transmitted signal by using local observations and local measurements.

The signal detection is analyzed by binary hypothesis model,

$$x(t) = \begin{cases} n(t), & 0 < t \leq T \quad H_0 \\ hs(t) + n(t), & 0 < t \leq T \quad H_1 \end{cases}$$

Where,
x (t) is CR received signal
n (t) is additive white Gaussian noise
s (t) is primary user transmitted signal
h is the channel gain
H_0 represents absence of primary signal
H_1 represents that the spectrum is occupied

The various methods of non-cooperative spectrum sensing are,

a) Energy detection method

Energy Detection is known as non-coherent detection in which the primary user's signal attributes are mostly unknown to the secondary users. The detection is based on comparing received signal strength of transmitter with the threshold level defined by the user.

b) Cyclostationary sensing

The primary user's signal attributes (data rates, carrier frequency and the modulation type) are often known to the secondary users in the operating frequency band. The periodicity of the received signal characteristics is used to detect the presence of legitimate users. Fast Fourier Transform (FFTs) is used for the easy implementation of this form of detection. In the presence of RF non-linearity, this method of detection degrades the overall system performance.

c) Matched filter

Matched filter is known as coherent detection method in which the prior knowledge of primary user signal information is required. This detection is based on comparing known signal with input signal. The optimal detector increases output SNR for the given input signal. The limitation of this detection is performance degradation in the presence of frequency and timing offsets.

The general challenges in non cooperative spectrum is restricted to sensing ability, High detection sensitivity requirements, vulnerability of primary receiver to secondary transmission, sensing in multiuser environment etc.,

2.2.2 Cooperative sensing

The major limitation in transmitter detection is the multipath fading and shadowing effects. In the spectrum environment few secondary users are in fading and shadowing region also, there may be other secondary users with strong signal strength. Whereas in the case of cooperative sensing, the secondary users in an area shares their channel occupation details and the different CR information get combined this results in reliable spectrum information.

Distributed sensing and centralized sensing are the popular cooperatives sensing approach. The sensing information is decided by sending the data through neighborhood CR users in distributed sensing. In centralized sensing the fusion centre decides the spectrum holes (unused areas) by collecting local sensing information from cooperative secondary users.

The prime challenge includes the sensing delay and synchronization issues in the cooperative sensing CRs.

3. COGNITIVE RADIO NETWORK ATTACKS

Cognitive radio Network (CRN) is vulnerable to various attacks. In CRN there is an agreement between primary users and Secondary users and malicious users can break this agreement. Another potential risk occurs when some users in the network are not trustworthy. For the successful deployment of cognitive radio Network the

security mechanism is necessary. The various Cognitive Radio Network attacks are discussed here.

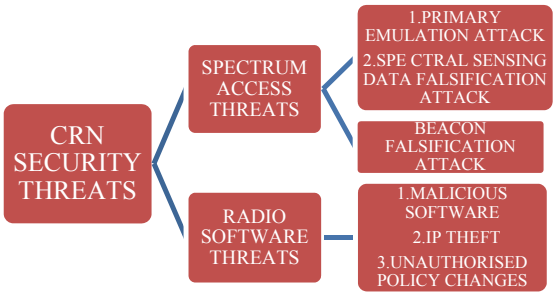

Figure-3. Overview of security threats.

3.1 Primary emulation attack

This attack is related to spectrum sensing manipulation. In primary user emulation attack, a malicious secondary user try to gain priority over original secondary users by transmitting signals that resemble the characteristics of primary signals. The attacker sends signals related to incumbent users during spectrum sensing and this result in false information to original secondary users if the primary users are not present. This primary users emulation attack causes serious degradation in the performance of cognitive radio systems.PUE attacks classified in to selfish PUE attack and malicious PUE attack.

a) SelfishPUEattacks

The main objectives of attacker are to maximize its own spectrum usage by preoccupying the spectrum holes. When the selfish PUE attackers detect a fallow spectrum band, they prevent other secondary users from competition so; it transmits signals that relate to the signal characteristics of incumbent users. This attack is usually carried out by two mutually agreed secondary users intended in preoccupying the temporally available spectrum.

b) MaliciousPUE attacks

The objective of this kind of attack is to block the legitimate secondary users from sensing the spectrum bands causing denial of service (DoS).The attacker obstructs the dynamic spectrum access in multiple bands. So, the malicious user prevents licensed users from accessing the unused part of a spectrum band.

3.1.1 Detection of primary emulation attack

Detection of primary user emulation attacks using wireless sensor networks (WSN)

The attack verification scheme in WSN uses localization based defense by creating received signal strength (RSS) map of the network with the help of large number of sensors distributed across the network. The peak RSS values are compared with known location of transmitters. The presence of larger peaks in the RSS shows the availability of licensed users in the spectrum band.

Detection of primary user emulation attack using cryptographic and wireless link signatures

The primary user signal is authenticated using cryptographic and wireless link signatures. The helper node is placed close to primary user. The helper node acts as relay to enable secondary users to verify cryptographic and wireless link signatures. The amplitude ratios are calculated using measurements on channel impulse response functions. The helper node along with cryptographic signature detects the primary users presence.

Detection based on signal activity pattern (SAP)

A signal activity pattern acquisition and reconstruction system (SPARS) is the novel detection system for detecting primary emulation attacks. The signal activity pattern (SAP) of a transmitter has ON and OFF periods. ON period is busy period of transmitter. OFF period refers to idle period of transmitter. SPARS get SAP of transmitter through spectrum sensing and compare SAP of primary users through SAP reconstruction model. If the observed SAP is not like the actual SAP of primary user (which is measured by the reconstruction error method), then the transmitter is an attacker.

Identifying primary user emulation attacks using non parametric Bayesian classification

A new method called Decloak is used to identify the primary user emulation attacks. It employs radio-metrics as finger prints. A radio metric is a component of radio signal like amplitude, frequency, and bandwidth. This radiometric cannot be altered and it is used to distinguish primary users and attackers. Decloak exploits non parametric Bayesian classification.

3.1.2 Defensive mechanism of primary emulation attack

Advanced Encryption Standard (AES)

If suppose primary emulation attack in cognitive radio network in white spaces of digital TV, Advanced Encrypted Standard is used here to counterpart the attack. AES encrypted reference signal is generated at TV transmitter and used as synchronous bits of DTV data frames. The reference signal is again generated at the receiver to accurately identify the original primary users. From analysis on the auto correlation of received signal, the malicious users can be detected.

Transmitter signal location verification

This type of detection involves the detection of legitimate primary users. Signal verification finds whether the primary user is legitimate or not. Local verifiers have

set of GPS enabled trusted network entities in the verification procedure. Distance Ratio Test (DRT) and Distance Difference Test (DDT) are the two types of tests that determine the reliability of primary signal. In DRT the ratio between the received signals strength at more location verifiers is calculated. The ratio between the two - location verifiers depends on ratio between distances of respective location verifiers. If both the ratio is close then the user is legitimate primary user. In DDT the relative phase difference of received signal at different location verifiers is measured. If the difference is close then the user is legitimate.

Examination of Pdf of received signal

By examining the Probability Density Function of received signal we can detect the occurrence of legitimate primary user. Neyman Pearson Composite Hypothesis test and Wald's sequential probability ratio test are the two techniques to find pdf of received signal.

3.2 Sinkhole attack

The need for transparency with existence of cognitive radio activities to primary users creates routing challenges. Cognitive radio nodes need to leave channel as soon as it detects primary users in that channel. This shifts complicates routing design.Cognitiveradio network have similarities with sensor network. Cognitive radio network has more relevant attack called sinkhole attack.

In sinkhole attack, the attacker claim itself as a good route with neighboring node to forward packets to specific destination. Attackers make use this way to discard or change packets from any destination in the network. This is called selective forwarding. Infrastructure and mesh architecture are the very suitable for this attack.

Defensive mechanism

Sinkhole attack is very difficult to detect. Geographic Routing Protocol (GRP) is resistant to sinkhole attack. Geographic protocols construct a topology on demand using only the localized interaction information and without initiation from the base station. Because the traffic is naturally routed towards the physical location of a base station, it is difficult to attract it elsewhere to create a sinkhole.

3.3 Hello flood attack

This attack also occurs while routing. When the attacker sends message to all nodes that it has enough power to act as their neighbor. It claim itself as a high quality link to forward packets as a good neighbor so the nodes believe them as a good neighbor. When they start forward packets it discovers that there is no neighbor as all the original neighboring nodes are busy forwarding other packets.

Defensive Mechanism

Symmetric key protocol is the defensive mechanism of hello flood attack. The easiest defense is to verify the directionality of a link. The identity verification protocol is sufficient to prevent HELLO flood attacks. Not only does it verify the directionality of the link between two nodes, but even if a well-funded adversary had a highly sensitive receiver or had worm- holes to a multiple locations in the network, a trusted base station that limits the number of verified neighbors for each node will still prevent HELLO flood attacks on large segments of the network when a small number of nodes have been compromised.

3.4 Sybil attack

Sybil attack is one of the security attacks. A single malicious node acts as a multiple identities and behaves as multiple nodes. As many small networks are operated it is difficult to maintain database to record identity thus causes Sybil attack in cognitive radio network. Single malicious attacker pretends as many secondary users competing for spectra causes other original secondary users ineffective to utilise the available spectrum. This attack is Sybil attack. This attack can be generated either by hardware or software.

3.5 Spectrum sensing data falsification attack

The attacker sends false sensing information to base station by compromising one or more secondary users called spectrum sensing data falsification attack. This is also said to be Byzantine attack. To counter this attack adaptive reputation based cluster algorithm is proposed. Here the nodes are clustered based on sensing report. A channel status is decided through intra and inters cluster voting. The final decision is propagated back to clusters and then to individual nodes for adjusting the reputation of nodes.

3.6 Jamming attack

Jamming attack is a major threat where several malicious attackers inject interference to interrupt communication of secondary users. Markov decision approach is one of the defensive mechanisms. Here the secondary user estimates the useful parameters based on past observations using the Maximum Likelihood Estimation (MLE).

3.7 Cross layer attack

The attacker launches several attacks in different layers coordinately called cross layer attack. Different defense techniques can be used at different layers to counter cross layer attack.

4. RESEARCH CHALLENGES

The performance of cognitive radio is linked with different research attributes such as,

4.1 Interference to primary user

The main objective of cognitive radio is to provide security to the primary user from the interference of various secondary users, as of now there are no methods for identifying the influence of cognitive radio in the licensed users.

4.2 Detection accuracy

The cognitive radio is to be implemented in the real time world, so it is necessary to formulate a robust scheme for spectrum sensing.

4.3 Detection in speeded spectrum

The licensed users utilizing the speeded spectrum are hard to find the spectrum holes, because the power of the licensed user is occupied through a wide range.

5. CONCLUSIONS

Cognitive radio technology research is increasing rapidly. An overview of CR network is discussed. As the demand for larger data rates, along with increase in more number of licensed and unlicensed users and the competition to utilize unused and underused spectrum tend to increase in rapid manner. This leads to different attack in cognitive radio network. Here we have presented various CR attacks, its detection and defensive mechanisms and different attack types in different layer is discussed. The research to deal with security threats are still in incipient stage. Many open challenges and its solution need to be addressed before the implementation secure Cognitive radio network.

REFERENCES

[1] R. Chen, J.M. Park, J.H. Reed. 2008.Defense against primary user emulation attacks, IEEE J. Sel. Areas Commun:Spl. Issue Cognit. Radio Theory Appl. 26(1): 25-37.

[2] T. Charles Clancy and Nathan Goergen. 2008. Security in Cognitive Radio Networks: Threats and Mitigation.International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCom), Singapore. pp.1-8.

[3] Xueying Zhang and Cheng Li. 2009. The Security in Cognitive Radio Networks: A Survey, Proceedings of the 2009 ACM International Conference on Wireless Communications and Mobile Computing:Connecting the World Wirelessly (IWCMC '09), New York.

[4] Kwang-Cheng Chen, Peng-Yu Chen, Neeli Prasad and Ying-Chang LiangnandSumei Sun. 2010.Trusted Cognitive Radio Networking, Wireless Communications and Mobile Computing. 10: 467-485.

[5] 2003. Secure Routing in wireless Networks: Attacks and Countermeasures, Adhoc Networks. 1: 293315.

[6] Yih-ChunHu,David B.Johnson and AdrainPerrig, Chetan Mathur and KoduvayurSubbalakshmi. 2007. Security Issues in Cognitive Radio Networks, Wiley. pp.284-293.

[7] S. Anand, K. Hong, S. Sengupta, R. Chandramouli. 2011. Is channel fragmentation bonding in IEEE 802.22 networks secure, in: Proc. of IEEE ICC. pp. 1-5.

[8] Q. Peng, P.C. Cosman, L.B.Milstein. 2009.Tradeoff between spoofing and jamming acognitive radio, in: Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers. pp. 25-29.

[9] T.W. Rondeau, C.J. Rieser, B. Le, C.W. Bostian. 2004. Cognitive radios with genetic algorithms: intelligent control of software defined radios, in: SDR Forum Technical Conference, Phoenix. pp. C-3-C-8.

[10] M. Stahlberg. 2000. Radio jamming attacks against two popular mobile networks, in Seminar on Network Security.

[11] C. Sun, W. Zhang, K.B. Letaief. 2007. Cooperative spectrum sensing for cognitive radios under bw constraints, Proc. IEEE WCNC. 200: 1-5.

[12] S. T. Zargar, M. B. H. Weiss, C. E. Caicedo and J. B. D. Joshi, 2009. Security in Dynamic Spectrum Access Systems: A Survey. in Proc. Telecommunications Policy Research Conference, Arlington VA.

[13] R.Umar, A.U.H Sheikh. 2012. A comparative study of spectrum awareness techniques for cognitive radio oriented wireless networks, Physical communication.