American Journal of Engineering Research (AJER) 2016
American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-2, pp-241-247
www.ajer.org
Research Paper Open Access

Analysis of Attacks in Cognitive Radio Networks

Manjurul H. Khan[1], P.C. Barman[2]
[1] *ICT Department-System, Janata Bank Limited, Head Office, Dhaka, Bangladesh.*
[2] *Department of Information & Communication Engineering, Islamic University, Kushtia, Bangladesh.*

***ABSTRACT*:** *Cognitive Radio (CR) is a promising technology for next-generation wireless networks in order to efficiently utilize the limited spectrum resources and satisfy the rapidly increasing demand for wireless applications and services. It solves the spectrum scarcity problem by allocating the spectrum dynamically to unlicensed users. It uses the free spectrum bands which are not being used by the licensed users without causing interference to the incumbent transmission. So, spectrum sensing is the essential mechanism on which the entire communication depends. Cognitive radio networks introduce new classes of security threats and challenges, such as licensed user emulation attacks in spectrum sensing and misbehaviours in the common control channel transactions, which degrade the overall network operation and performance. So that it causes the crucial threat in the cognitive radio network. In this paper, our objectives are to give the various security issues in cognitive radio networks and advantage and disadvantage of security mechanisms with the existing techniques to mitigate it.*

Keywords- *Cognitive Radio, Spectrum Sensing, Primary User, Secondary User, Malicious User.*

I. INTRODUCTION

Cognitive Radio (CR) is an enabling technology to effectively address the spectrum scarcity and it will significantly enhance the spectrum utilization of future wireless communications systems. In a CR network, the Secondary (or unlicensed) User (SU) is allowed to opportunistically access the spectrum "holes" that are not occupied by the Primary (or licensed) User (PU). Generally, the SUs constantly observe the spectrum bands by performing spectrum sensing. Once a spectrum "hole" is discovered, an SU could temporarily transmit on this part of the spectrum. Upon the presence of a PU in this part of the spectrum, however, the SU has to switch to another available spectrum band by performing spectrum handoff, avoiding interference with the PU transmission. The development of CR technology leads to the new communications paradigm called Dynamic Spectrum Access (DSA), which relaxes the traditional fixed spectrum assignment policy and allows a CR networks to temporally "borrow" a part of the spectrum from the primary network. As a consequence, the scarce spectrum resources are shared, in a highly efficient and resilient fashion, between the primary network and the CR network.

Organization of this paper is as follows: section II gives a brief overview of Cognitive radio core functions. Details of threats and attack categories are given in section III. In section IV and V, we give a defence mechanism and detection mechanism respectively in CRNs as well as advantage and disadvantage of mechanism. Finally, section VI concludes the paper with our future work.

II. COGNITIVE RADIO CORE FUNCTIONS

There are four fundamental functions which the CRN device must perform, as shown in Figure 1 and as stated below [1,2]

1) Spectrum sensing identifies the parts of the accessible spectrum and senses the presence of the PU operating in the licensed band.
2) Spectrum management determines the best channel to establish communication.
3) Spectrum sharing sets up a coordination access among users on the selected channel.
4) Spectrum mobility vacates the channel in case the PU is detected.

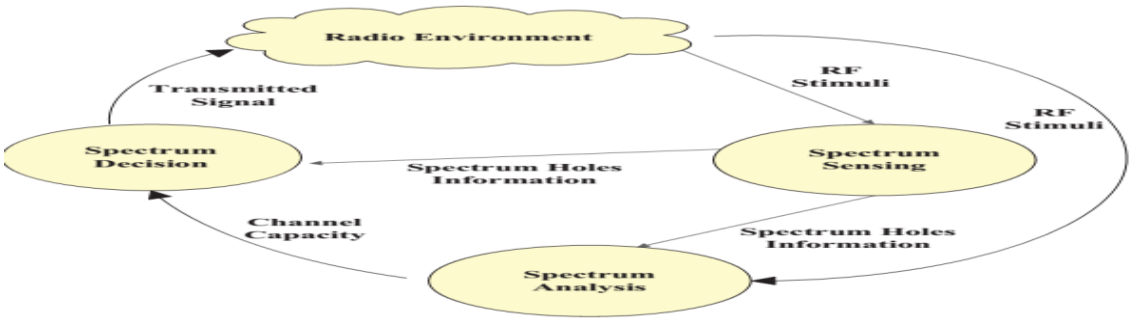

Figure 1. Cognitive Cycle [3].

III. CATEGORIES OF THREATS AND ATTACKS

3.1 Analysis of Access Point

CR facilitates in secondary usage of licensed band by dynamically spectrum allocation manner. Therefore, secondary user (SU) must sense the spectrum accurately to avoid interference with the PU. With this, the CR management experiences different kinds of anomalous behaviour from the other Access points (Aps) [4].Which represent in table 1.

Table1. Analysis of access Point

Types of Access Point	Definition
Misbehaving Access Point	It does not obey any rules for sensing, recognizing and managing the spectrum.
Malicious Access Point	It aims to vandalize the networks by falsely reporting the spectrum sensing results to SUs in order to cause interference between PU and SUs.
Cheat Access Point	It aims to increase its utility function by decreasing profit of other SUs.
Selfish Access Point	It occupies the channel for longer time to make profit to itself only.

3.2 Overviews of the attacks occurring at different CR functions

Spectrum sensing, Spectrum management, Spectrum sharing and Spectrum mobility are performed in CR functions. Overviews of the attacks occurring at different CR functions are figure out in Table 2.

Table 2.Overview of the attacks occurring at different CR functions

Attack Name	CR function	Description
Forgery & Data tamper	Spectrum Sensing	Spectrum Management system makes wrong decision by receiving the attackers sensing information.
Overlapping		An attacker impacts other networks by transmission to a specific network.
Denial of Service		An adversary user decreases the availability of the spectrum bandwidth by blocking the communication, through creating noise spectrum signals which cause interference with PU.
Lion or Jamming message		An attacker transmits high signalling power to disturb the or the secondary user which results forcing the cognitive user to hop to different channel to utilise.
Spectrum Sensing Data Falsification(SSDF)		In collaborative spectrum sensing, a collaboration technique used among CR nodes to generate and utilise a common spectrum allocation for the exchange of information about available channels. However adversary node gives false observations information to other users.

Eaves dropping	Spectrum Sharing	Weaknesses within the layer due to the poor authentication and no existing encryption mechanisms.
Denial of Service & masquerade		Repetition of the frequent packets that result in Overcrowding the channel which is being busy to be utilised by legitimated users.
Selfish Behaviour or selfish masquerade attack		an attacker does not follow the normal communication process for maximising their throughput, saving energy or gaining unfair beneficial access of using spectrums through injecting frequent anomalous behaviour.
Key depletion		An attacker attempts to break the cipher by repetition of the session key.
Forgery Attack		Lack of authentication mechanism leads to the occurrence of modification and forgery on MAC CR Frames which result in the launch of DoS attacks.
Biased Utility	Spectrum Management	An attacker tries to reduce the bandwidth of other SUs in order to obtain more bandwidth by changing the spectrum parameters.
False feedback		An attacker secretes the incidence of the PU in order to disturb the information sensing of other SUs.
Routing information jamming	Spectrum Mobility	A malicious node causes a targeted node to initiate spectrum handoff before the routing information is exchanged.

3.3 Attack Scenario on Protocol Layer

We categorize the various attacks depending on their behaviour shown towards the five layers of the protocol stack [5] as shown in Table 3.

Table 3.Attack scenario on Protocol Layer

Types of attacks	Definition	Protocol Layer
PUEA	The physical layer attack is classified as a primary user emulation attack (PUEA), where the malicious user (MU) mimics the primary user's signal characteristics, thereby causing SUs to erroneously identify the attacker as the primary user.	Physical Layer
Jamming	Jamming is when the jammer sends a continuous packet of data into the channel, making the SU to never sense the channel as idle.	
Objective function attack(OFA)	The objective function attack (OFA) is when the MU may try to change the parameters of utility resource, so that the CR node fails to adapt correctly.	
Common control data attack(CCDA)	Common control data attack (CCDA) is a major risk which disrupts the transmission by preventing the elements of the channel from sharing information about the spectrum usage and also provides all the information to the attacker.	
spectrum sensing data falsification (SSDF)	Here the attacker falsifies the fusion centre decision by sending wrong spectrum sensing result.	Link Layer
Control channel saturation Denial-of-service (DoS)	When the attacker saturates the control channel by reserving it.	
Selfish channel negotiation(SCN)	Where the malicious node provides wrong channel information, so that other nodes change their route.	
Wormhole attack	An attacker builds bogus route information and tunnels the	Network

	packet to another location. This creates routing loops and wastes energy.	Layer
Sink hole attack	Here, the attacker advertises itself as the best route to a specific destination and lures the neighbour nodes to use this route and forward their packets so as to drop those packets.	
Hello flood attack	When the attacker sends a broadcast message to all the nodes in a network with enough power to convince them that, it is the closest neighbour of those nodes.	
Lion attack	The attacker launches PUEA and forces the CR nodes to perform frequency hopping among channels in order to disrupt TCP.	Transport Layer
Jellyfish attack	Jellyfish attack is performed on the network layer but it affects the performance of the transport layer, especially the TCP protocol.	
Cognitive radio virus attack	The cognitive radio network is vulnerable to viruses that can effect radio function and learning Policy of the radio is changed or not allowed to be updated, providing the attacker unfair spectrum access.	Applicati-on Layer
Logic Error Attack	Those attacks corresponding to all the layers may have an adverse effect on the application layer.	
Buffer Overflow attack		

IV. DEFENCE MECHANISM IN CRNs [6]

A number of researchers have made efforts to address the security requirements and provide secure communication among SUs by applying different security mechanisms, such as authentication and authorisation access by different techniques, within a CRN.

4.1 Digital Signature

In[7,8,9] proposed different protection systems based on applying a digital signatures for protecting the network from DoS attacks and providing secure communication. Their approaches involve the activities of a CA, PUs, and both PUs' and SUs' base stations. However, the main differences of these mechanisms are that the BSs are connected to the CA using wire links in[10], while in[11] the approach, an asymmetric key scheme instead of a CA is mainly used.

Advantage:

i.Low complexity and using the basic architectures of symmetric and asymmetric key infrastructures.

Disadvantage:

i.It has not been simulated and tested to proof the security. It also does not work in Ad-hoc environment due to being based on centralised entities.

4.2 Certificate Authority

Another effective traditional approach-based CA on the application layer for achieving the same purpose of authentication is presented in [12,13].The proposed method uses both EAP-TTLS(for establishing a secure connection) and EAP-SIM (for authenticating the user) algorithms.

Advantage:

i.Effective security mechanism due to identifying and verifying the user and the server respectively.

Disadvantage:

i.Requires a third-party to verify the user identity. Also the mechanism has not been simulated and tested to ensure security against malicious behaviours.

4.3 Trust Values

Trust values technique procedures are proposed in [14,15] to address and analysis the issues within CRNs. Based on this, the trust value will be calculated, which leads to the decision that will either allow the current user to utilise the available licensed channel or not.

Advantage:

i.It is an additional procedure that can be built on the top of other security techniques to increase the level of the protection and detection in term of secure communication.

Disadvantage:
i.Requires a third party procedure is to provide previous information of a node. Moreover, when a new node joins the network, the CA will not be able to provide reference for that particular user. Hence the mechanism does not operate in strong fixed level of the authentication for all cognitive users equally.

4.4 User Identification

User identification process generating by using specific port. Here, each user has a fixed port.

Advantage:
i. Low complexity by generating two virtual ports for secure transmission: the first is for control traffic information and another is for data transmission which is blocked by default unless the user has been authenticated.
Disadvantage:
i. It requires a third party to provide information like user preferences.

4.5 Deadlock

In [16] the author proposed a new method, called Deadlock, which utilizes device dependent radio metrics as a fingerprint. It uses non-parametric Bayesian classification to model the feature space of a single device as a multi variable Gaussian distribution with unknown parameters, and feature space of multiple devices as an infinite Gaussian mixture. Collapsed Gibb's sampling algorithm is applied to get samples from the posterior distribution, and active devices found out. Then the MAC addresses are collected.
Advantage:
i. One physical device sharing only one ID as a result it is free from any attack.
Disadvantage:
i.If more than one physical device is sharing the same ID, then PUE attack is identified.

4.6 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.
Advantage:
i. It is very effective scheme for overlapping secondary user attack.
Disadvantage:
i. It needs a third party to complete the task.

V. DETECTION MECHANISM IN CRNs

5.1 Puzzle Punishment & COOPON Activity

Selfish behaviour detection techniques for the CCC are proposed in [17,18] where a puzzle punishment model is applied for bad behaviour activities in a situation where a receiver is asked for a new hidden channel that has not been included previously. Thus, the sender would be a suspicious case. Therefore, the receiver applies the puzzle punishment to detect whether the sender is a selfish node or not. If the sender node solves the puzzle, they will be considered as a legitimate user and communication will be resumed normally; otherwise, the communication will be disconnected.
Cooperative neighbouring cognitive radio Nodes (COOPON) is applied among a group of neighbouring users to detect selfish nodes who broadcast fake channel lists. Consequently, neighbouring users can detect the selfish users by comparing the transmitted channel list of the target user with their lists.
Advantage:
i. Applied in both CCC and data channel which decreases the potential of misbehaviour in different stages of the network.
Disadvantage:
i. Focuses only on detecting selfish behaviour and does not provide the complete secure communication between sender and receiver.

5.2 Timing parameter

In timing parameter works proposed in [19] MAC Layer. When the negotiation phase is taking place, the node, which receives a request, sets up timing parameters for controlling the time interval. This forces the sender to transmit data without getting a higher rate. If the sender does not obey and sends packets more frequently, the receiver node takes action against the sender. Then the receiver node analyses the sender's misbehaviour and broadcasts the information over the current network.

Advantage:
i.Detecting misbehaving nodes during the negotiation phase. It helps to maintain the channel from getting saturated.
Disadvantage:
i.Theoretical and has not been simulated and tested to provide the detection scheme results.
ii.Weak against eavesdropping and forgery attacks especially once the FCL is not hidden which is exploited to launch Jamming attacks.

5.3 Anomalous Spectrum Usage Attacks

In [20] presented a cross-layer technique for CRNs for detecting ASUAs. Collecting the information on both the physical and network layers provides an awareness of the current spectrum. It operates against the PUE and jamming attacks to provide successful access to the spectrum.
Advantage:
i.Combining both physical and network layers for detecting malicious users give a better achievement instead of selecting only a layer.
Disadvantage:
i.Focuses only on the detection approach and does not consider a significant protection scheme against both jamming and PUE attacks mobility.

5.4 Pinokio

A method of detection of Byzantines called Pinokio. Pinokio uses a Misbehavior Detection System (MDS) that maintains a profile of the networks normal behavior based on training data. The MDS detects misbehavior by monitoring the bit rate behaviour. 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.[21]
Advantage:
i. It uses training data, which is very effective in MAC layer.
Disadvantage:
i. Sometimes bit rate behaviour is not fair.

VI. CONCLUSION

The awareness, reliability and adaptability nature of CR networks make it more precious to be deployed successfully in near future. Along with this realization, it has also opened the door for lots of threats, especially in security because of the presence of malicious nodes, who want to vandalize the entire communication networks. Cognitive radio is a promising concept which uses the available spectrum more efficiently through opportunistic spectrum deployment. As security has a significant priority in CR networks, the security threats that face CRN were discussed. We were also discussed protection mechanism and detection mechanism respectively in CRNs as well as advantage and disadvantage of mechanism. For future work, the physical layer will more efficient in terms of detection of this MU, because this is the primary layer whose information is to pass to the upper layers.

REFERENCES

[1] Baldini, G., Sturman, T., Biswas, A., Leschhorn, R., Godor, G., and Street, M., (2012)"Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead," Communications Surveys & Tutorials, IEEE, vol. 14, no, 2. pp. 355-379.
[2] Domenico, A., Strinati, E., Benedetto, M., (2012) "A Survey on MAC Strategies for Cognitive Radio Networks," Communications Surveys &Tutorials, IEEE, vol. 14, no. 1, pp. 21-44.
[3] S. Haykin, "Cognitive radio: brain empowered wireless communications," IEEE Journal on Selected Areas in Communications, pp. 201–220, February 2005.
[4] Arkoulis, S.; Kazatzopoulos, L.; Delakouridis, C.; Marias, G.F.,"Cognitive Spectrum and Its Security Issues," Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08.The Second International Conference on , vol., no., pp.565,570, 16-19 Sept. 2008.
[5] Wassim El-Hajj; HaiderSafa; MohsenGuizani, "Survey of Security issues in Cognitive Radio Network," journal of internet technology,volume 12, 2011.
[6] A.Wajdi,M.Ali&A. S. Ghazanfar "Spectrum Sharing Security and Attacks in CRNs: a Review"Luton, United Kingdom,(IJACSA)International Journal of Advanced Computer Science and Applications,Vol. 5, No. 1, 2014.
[7] Sanyal, S., Bhadauria, R. and Ghosh, C., (2009) "Secure communication in cognitive radio networks," in Computers and Devices for Communication. CODEC. 4th International Conference on, pp. 1-4.
[8] Parvin, S., and Hussain, F.. (2011), "Digital signature-based secure communication in cognitive radio networks," in Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on, pp. 230-235.

[9] Mathur, C., Subbalakshmi, K., (2007), “Digital signatures for centralised DSA networks”Consumer Communications & Networking Conference, CCNC. 4th IEEE.
[10] Parvin, S., andHussain, F.. (2011), "Digital signature-based secure communication in cognitive radio networks," in Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on, pp. 230-235.
[11] Mathur, C., Subbalakshmi, K., (2007), “Digital signatures for centralised DSA networks”Consumer Communications & Networking Conference, CCNC. 4th IEEE.
[12] Zhu, L., Mao, H., (2010) "Research on authentication mechanism of cognitive radio networks based on certification authority," in Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on, 2010, pp. 1-5., 101.
[13] Zhu, L., Mao, H., (2011), "An Efficient Authentication Mechanism for Cognitive Radio Networks," Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific, pp.1-5, 25-28 March 2011.
[14] Parvin, S., Han, S., Tian, B., Hussain, F., (2010), "Trust-based authentication for secure communication in cognitive radio networks,"in Embedded and Ubiquitous Computing (EUC), IEEE/IFIP 8th International Conference, pp. 589-596.
[15] Parvin, S., Hussain, F., (2012) "Trust-based Security for Community based Cognitive Radio Networks",. 26th IEEE International Conference on Advanced Information Networking and Applications, pp. 518-525.
[16] Nguyen, N.T.; RongZheng; Zhu Han, "On Identifying Primary User Emulation Attacks in Cognitive Radio Systems Using Nonparametric Bayesian Classification," Signal Processing, IEEE Transactions on , vol.60, no.3, pp.1432,1445, March 2012.
[17] Wu, H., and Bai, B., (2011) "An improved security mechanism in cognitive radio networks," in Internet Computing & Information Services (ICICIS), 2011 International Conference, pp. 353-356.
[18] Jo, M., Han, L., Kim, D., In, H.P., (2013) "Selfish attacks and detection in cognitive radio Ad-Hoc networks," Network, IEEE , vol.27, no.3, pp.46,50.
[19] Shaukat, R., Khan, S., Ahmed, A., (2008) "Augmented security in IEEE 802.22 MAC layerprotocol,"in Wireless Communications, Networking& Mobile Computing,. '08. 4th International Conference, pp 1-4.
[20] Sorrells, C; Potier, P; Qian, L; Li, X., (2011) "Anomalous spectrum usage attack detection in cognitive radio wireless networks," in Technologies for Homeland Security (HST), 2011 IEEE International Conference, 2011, pp. 384-389.
[21] M.Padmadas,Dr.N.Krishnan&V.NellaiNayaki, "Analysis of Attacks in Cognitive Radio Networks”,international Journal of Advanced Research in Computer and Communication Engineering ,Vol. 4, Issue 8, August 2015.