International Journal of Engineering & Technology, 7 (4.6) (2018) 505-509

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Mitigating Multiple attacks in Cognitive Radio Networks

Sivasankari Jothiraj*, Sridevi Balu

*Faculty, Department of Electronics and Communication Engineering, *Ultra College of Engineering and Technology – Velammal Institute of Technology, Tamilnadu, India*
**Corresponding author E-mail: jsivash11@gmail.com*

Abstract

Database driven CRNs are taken into consideration because the promising technique to enhance the wireless spectrum usage, it faces serious safety demanding situations via location cheating attack. The number one challenges are location proof verification and region solitude verification. Malicious users create a faux region with the aid of self-seeking the all to be had spectrum bands. A region based totally service is used for imparting provider to the consumer. Wi-Fi authority verifies the place whether or not the proof is legitimate or no longer. If the person is valid, it passes the facts to the base station. This technique provides effective reduction of malicious user in the cognitive radio community.

Keywords: *Location falsification attack, location proof verification, certificate authority, database-driven CRNs*

1. Introduction

Wireless networks and services mostly rely on the spectrum resource. Rather the spectrum was not utilized and assigned efficiently by the authorized user. Hence it raises the issue of spectrum scarcity. By the prediction of International Telecommunications Union(ITU) report [1], around 2020 spectrum demand will be in the order of several thousands of MHz . However, the spectrum for the wireless gadgets evolving day by day is highly being a uncertainty in the IoT world. According to[2], a wide range of assigned spectrum is used periodically and varies with different geographical locations as shown in fig.1. Spectrum shortage is a number one problem occurs whilst looking to launch new wireless offerings. The outcomes of this scarcity is pretty considerable in the spectrum auctions wherein the users often need to make investments billions of dollars to comfortable get admission to exact bands inside the available spectrum. Even though this spectrum scarcity is being a prime trouble, latest spectrum utilization measurements have proven that the available spectrum possibilities are underutilized i.e. left unused.
The spectrum scarcity and underutilized spectrum leads to a new expertise evolved as neXt Generation Networks (XG Networks) and Cognitive Radio (CR) networks[3,4]. The ability of a cognitive radio was ensured to select the best accessible using Dynamic Spectrum Access technique, the immediate confront is to make the network protocols versatile to the available spectrum [2].

2. Cognitive Radio

Cognitive Radio was well defined by various authors mentioned in Table 1.With the help of the definition, CR can be characterized in two aspects,[3,5]

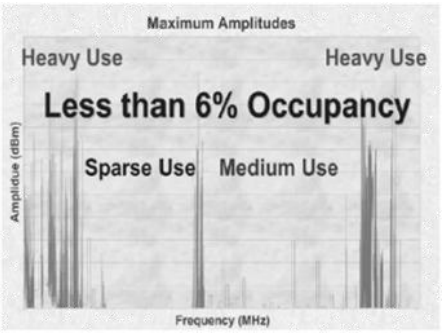


Fig. 1: Spectrum utilization[2,5]

Cognitive capability: It mainly focus on the process of sensing the information of free spectrum from its radio environment. With this characteristics cognitive radio can be used anywhere to find out the utilized/underutilized spectrum
Reconfigurability: The cognitive reconfigurability permits the radio to be animatedly programmed in sense of the environment. More particularly, CR is independent of the bandwidth utilized with respect to the transmission and its compatibility with any standard was high. [6].
CR act according to the cognition cycle as depicted in Fig.2.

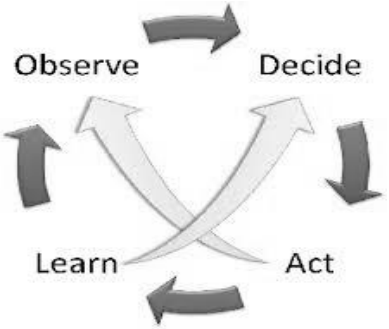


Fig.2: Cognition Cycle

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The underutilized spectrum named as spectrum hole /whitespace was identified using cognitive radio. If the identified hole was again used by the licensed user, cognitive radio user will move to the other hole of same frequency to continue its transmission by changing its modulation parameters, etc., as shown in Fig.3.
Main Functions of Cognitive Radio are

- ***Spectrum Sensing***: Identifying the ideal spectrum of a PU which operates in a particular band.
- ***Spectrum management***: Best vacant channel was decided
- ***Spectrum Sharing***: Free channel was shared to the demanded SU.
- S***pectrum Mobility***: Unauthorised user should move out when their analogous user return to its spectrum.

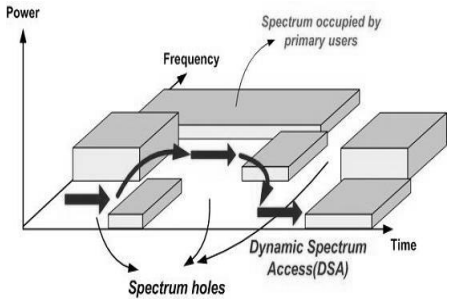


Fig.3: Spectrum Whole/White Space Concept

3. Spectrum Sensing Techniques

Spectrum sensing being one of the most important requirements as it finds the white space, as explained in Section II. Cognitive radio is intended to be conscious of and receptive to its environment [3]. Categorization of spectrum sensing techniques is shown in Fig.3. Among which matched filter and energy detection technique was widely employed and in our proposed technique cooperative spectrum sensing technique was used with the basic module of energy detector.

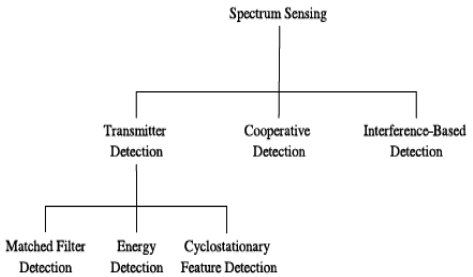


Fig.3: Spectrum Sensing Technique Classification [3]

3.1 Transmitter detection (non-cooperative detection)

The spectrum range of primary user has to be detected using cognitive capability. It can be done with the help of local anomalies of SU's. Detection process can be summarised as in algorithm 1.

Algorithm 1- *For Detection of Primary USER*
initialization
if necessary
end
while the algorithm is not stopped do
measure the current sample s[k]
decide between H0 and H1 //H0-Null Hypothesis
//H1-Presence of PU
if H1 decided then
store the sensing time n_s
estimate the detection time n_d
stop or reset the algorithm
end
end

3.2 Cooperative Spectrum Sensing(CSS)[13]

On discussing CSS, CR users are categorized as: centralized [14,15], distributed [16], and relay-assisted [17].A central identity called fusion center (FC)[14] controls the overall sequential flow in centralized CSS.

a. The FC decides best accessible channel and broadcast to all cooperating CR users.
b. FC merges the acknowledges the information of spectrum pool, and decides the occurrence of PU's, and sends the decision back to cooperating CR users.

The flow of process in cooperative spectrum sensing is represented in Fig.4

- Cooperation models regard as the representation of how CR users cooperate to carry out sensing. Co-operative sensing can be done either by parallel fusion method or game theoretical model

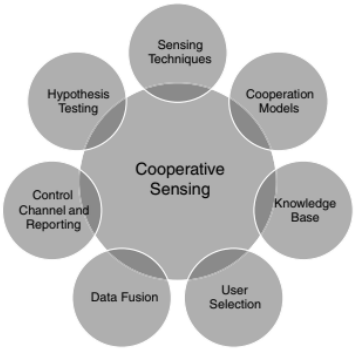


Fig.4: Essentials of Cooperative Spectrum Sensing

- ***Sensing techniques*** are utilized to sense the overall spectrum, defining the examination model, and utilizing basic signal processing methodology for detecting the presence of PU signal or the available spectrum.
- ***Hypothesis testing*** is a statistical analysis, decides between H_0(absence of PU) and H_1 (presence of PU), done by each user or the FC.
- ***Control channel and reporting*** used to accumulate the sensing result of $^{\text{Secondary}}$ users to the FC.
- ***Data fusion*** -merging sensing results to go with the cooperative decision. Some well known decision rules can be followed
- ***User selection*** goes with the selection of cooperating CR users and concludes with the proper path
- ***Knowledge base*** works as a database to improve the detection performance. The data base may be a priori knowledge or gathered through the experience.

3.3 Security Issues [15,18]

As in some other sort of remote systems, CRNs are defenceless against numerous security issues particularly amid the spectrum sensing stage. The radio innovation itself is helpless against security attacks. There is no influence over the conduct of these unlicensed clients, which debilitates the security of the authorized clients. The most critical practices of attacks can be arranged with respect to different types attacks encountered with CRN. A malicious user (MU) does not give genuine data about the system assets intentionally to build its nature of administration (QoS). A MU purposefully focuses on the system intentionally to debase alternate hubs QoS and the system effectiveness. On the off

chance that a hub carries on in one of the past classes, the hub will be an enemy hub and it may dispatch different assaults.

Table 1: Attacks and it's confront due to adversary nodes

Various Attacks	Adversary Nodes
PUEA	Misbehaving**, malicious**, and cheating
SSDF	Misbehaving, cheating, and selfish
DoS	Misbehaving, **malicious**, selfish, and cheating
Collusion	Misbehaving, selfish, **malicious**, and cheating

An attacker that carries on in one of these routes amid range detecting can copy PUs or send false detecting outcomes. The attacker means to keep different hubs from utilizing the range productively, keep organize assets for its very own advantages, lessen the nature of administration (QoS) of different hubs, and subsequently debase the system security and execution. In the existing system, a fake region is released by using the malicious users (MUs) based totally on reporting to the database with their personal wish.

3.4 Security related with CSS [16,17]:

The principle goal of MUs is to obtain the spectrum based on faux vicinity to the base stations. Right here a location Faker is used gadget tool in an android for wireless to conduct a fake location arbitrarily. SAI allows the SU's gadgets to ensure with their possible locations within its coverage range contemporary area and allowed to had channels inside that area. A novel privacy maintaining Framework is designed to save you area privations leaking and also improves the region privations of the secondary customers. The occurrence of a malicious consumer node seeks to take advantage of falsely the channel by way of reporting it to be as a number one person and results in interference.

In this example, a Fusion centre tries to console the vicinity privacy of a special user via using Geo-region procedure.

Drawbacks:

- In DLC attack, some of the places can only be inferred, and consequences most of the correlation to be now not actual.
- Those protocols could effectively do away with assaults by means of minimizing communication overheads a bit.

4. Proposed System

As mentioned earlier in the existing system, a fake location is launched by the malicious users (MUs) based on reporting to the database with their own wish. The main aim of MUs is to obtain the spectrum based on fake location to the base stations. Our proposed system focuses on reducing the malicious users information in the CRN based on Certificate Authority and Location Proof Server (LPS). To overcome the location spoofing attack, we introduce a secure authentication mechanism in the Cognitive Radio Network (CRN). Usually, a malicious user node sends information to the PU about the Spectral Availability Information (SAI) based on the Wi-Fi Access point (or) Cellular Base station. Here Fusion Center (FC) verifies the location coordinates of every SU in the network, since all user are enabled with GPS. If the ID of every user results as a legitimate user then the information was passed to the base station else the information is rejected. Then the base station verifies the location from the Location Proof Server (LPS) and Certificate Authority (CA).If the SU is a valid user then spectrum availability provider allocates spectrum to the corresponding user's location and store it in a database else the information is rejected.

4.1 Certificate Authority

It used for mapping between real identity and pseudonym. Location proof is encrypted by CA and secret key is send back to the location proof server. After getting the secret key from CA location proof server send the verified location to Spectrum database.

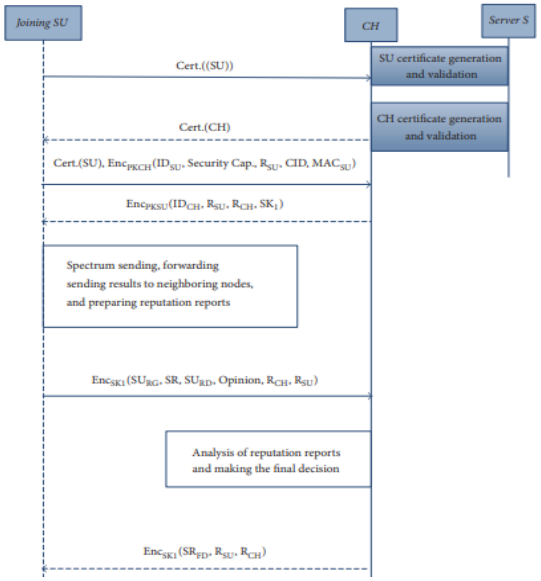


Fig.5: System Flow Diagram

Our proposed work has provided the specific identity for every user in the network and that are provided by the base station. Here there are some works allocated to fusion center are as follows: 1) It selects a channel for sensing and instructs all SU to perform local sensing individually, 2) All SU reports their sensing information to FC and 3) FC determines the presence of PU based on combining all results of SU and FC diffuses the decision back to all SU. If the ID is satisfied, then the value is passed to base station. Location based certificate authentication is specified for the secure authentication for every secondary user. This information is stored in a database of a base station. Certificate Authority (CA) is randomly generated pseudonym for protecting the privacy of user which contains a key pair (public key and private key).

The spectrum availability information is stored in the data base of a base station and it is more analogous to traditional one that are specified in existing stored database driven CRN systems. The Location Proof Server will verify location of the SU and compared with request sent and stored in Database.

Advantages:

- Location privacy is effectively secured from malicious user
- Effective detection of the malicious users.
- Enhanced service quality.

4.2 Proposed Architecture

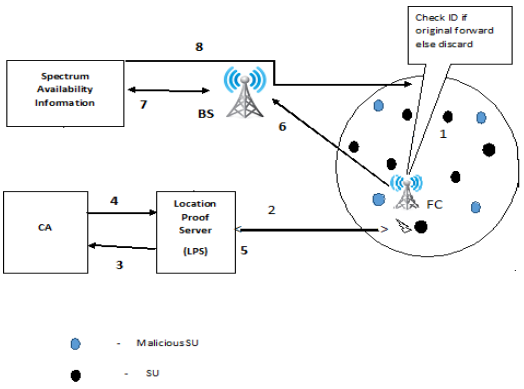


Fig 6: Proposed Architecture

Steps to be followed:

1. Secondary User sends request along with its location co-ordinates to the FC (Fusion Centre)
2. FC verifies the location of every user and sends to Location Proof Server (LPS)
3. LPS checks the location proof of every user and passes to Certificate Authority (CA)
4. CA verifies the original Id of every user and sends to LPS
5. Now the LPS pass the Id from CA to Fusion Centre (FC)
6. FC gives the Id to the base station
7. BS provides the necessary Spectrum Availability Information in a two way process.
8. BS allocates the SAI to every legitimate secondary user in a CRN

4.3 Component Description

a. Secondary Users

Unauthorized user enabled with cognitive radio agent search for the option of using the authorized spectrum. According to the specific rules, we specify the every secondary user is allowed to query a database for the SAI (Spectrum Availability Information). This is applicable when they are already originated in the cognitive radio network and they can obtain spectrums based on access point that helps to identify the specific location. These users are equipped with GPS, Wi-Fi and Cellular enabled devices that has the capacity to connect with internet facility

b. Fusion Centre

Our proposed work has provided the specific identity for every user in the network and that are provided by the base station. Here there are some works allocated to fusion Centre are as follows:

1) Decides the sensing of the available channels and insists SU to do the same separately,
2) Sensing information was accumulated at the FC and
3) On coalescing all the report of SU FC decides on the state of PU and relapse the decision to SU.

According to our proposed procedure, FC checks the identity of all users. If the ID is satisfied then the value is passed to base station.

c. Location Based Certified Authentication

Location based certificate authentication is specified for the secure authentication for every secondary user. This information is stored in a database of a base station. Certificate Authority is always available for every user for protecting user privacy. Certificate Authority (CA) is randomly generated pseudonym for protecting the privacy of user which contains a key pair (public key and private key).

d. Spectrum Availability

The spectrum availability information is stored in the data base of a base station that is more similar to traditional database that are specified in existing database driven CRN systems. After the verification of location proof, the Location Proof Server will submit the region in spectrum request to the SAI Provider Database.

4.4 System Sequence

The location proof request can be expressed as

$$Request = (Puser, k, d, t_r, Ruser, Clocuser) \quad (1)$$

Here, P_{user} -user's pen name; preamble's random number was denoted as k ; t_r denotes the request sending time. S_{user} is a group of cell *id*s whom the user reservation for.

$$Clocuser = (gr, ha+s) \quad (2)$$

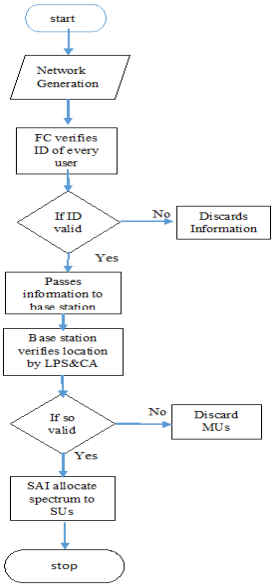
Grid cell id are generated with the help of *ha with respect the system level d.*

$$ClocAP = (u0,u1,u2) = (gw, hs\cdot(a2-a0)+w, hs\cdot(a2-a2)+w) \quad (3)$$

When the location proof request is received by user it checks whether it is currently being used, and an assumption is being considered that Wi-Fi AP accepts sequence number that is being broadcasted within lasted 100 milliseconds.

$$Response = sigGKpri(Puser; l; t; Ruser; ClocAP) \quad (4)$$

4.5 Flowchart of the proposed Work



5. Simulation Setup

The overall network setup was simulated in NS-3 environment and the corresponding result was obtained. In which Fig.7 describes the implementation setup of cognitive radio network with N and M number of primary users and secondary users, Fusion center, Base station and Location proof server. In the meanwhile, Fig 8 gives the detail regarding the validation process, by malicious user can be isolated as shown in fig.9. Location proof was verified with corresponding density ratio of Wi-fi access Point and it is compared with existing techniques and shown in Fig.10.

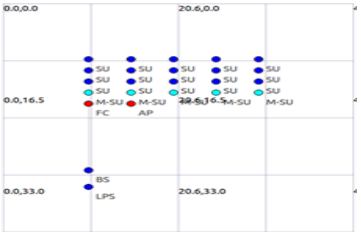


Fig.7: Initial Network Setup

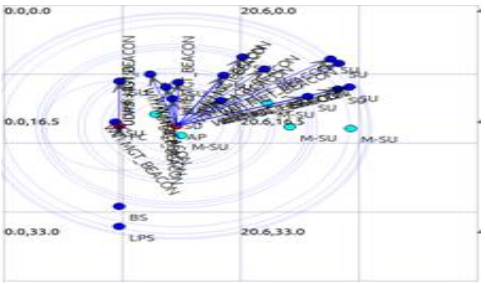


Fig.8: Validation process of every user

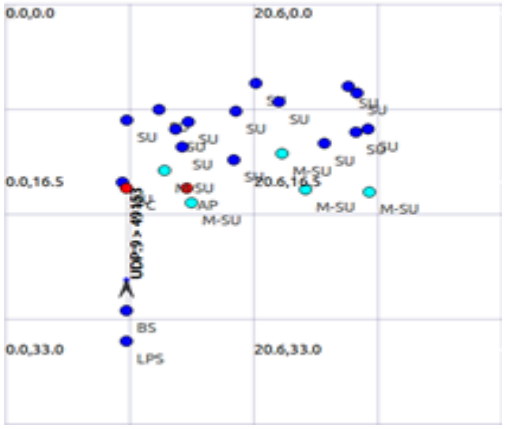


Fig.9: Process of isolating malicious users

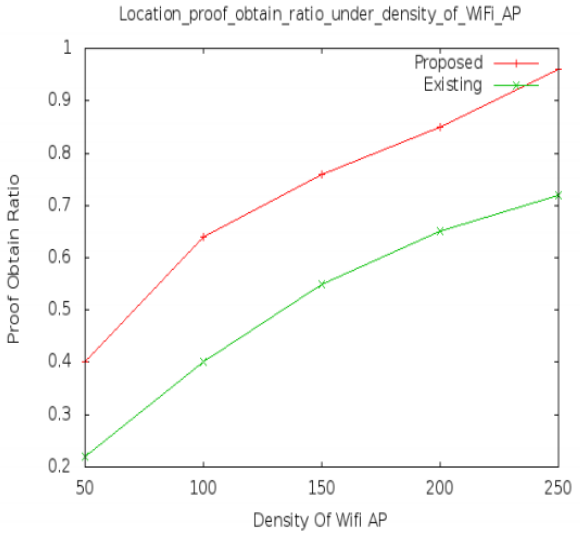


Fig.10: Location Proof obtain Ratio under density of Wi-Fi AP

6. Conclusion

Our proposed system focuses on reducing the malicious nodes in the network. Here every secondary user query the database about the spectrum availability. Hence the database driven location hoaxing attack was identified and the user was discarded to avoid interference caused to both PU and SU. We proposed a certificate authority based authentication for CRN. Initially FC checks identities of every user and base station checks certificate authority and SAI.

References

[1] International Telecommunications Union, "*Estimated spectrum bandwidth requirements for the future development of IMT-2000 and IMT-Advanced*," ITU-R Report M.2078, 2006.

[2] FCC, ET Docket No 03-222 Notice of proposed rule making and order, December 2003.

[3] F.Akyildiz(2006)," *NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey*,*Computer networks*, Volume 50 Issue 13, Pages 2127-2159

[4] DARPA XG WG, The XG Architectural Framework V1.0, 2003.

[5] L. Lu, X. Zhou, U. Onunkwo, and G. Li, "Ten years of research in spectrum sensing and sharing in cognitive radio," EURASIP J. Wirel. Commun. Netw., vol. 2012, no. 1, p. 28, 2012.

[6] S. Haykin(2005), "*Cognitive Radio: Brain-Empowered Wireless Communications," IEEE JSAC*, vol. 23, no. 2, pp. 201–20

[7] A. Ghasemi, E.S. Sousa, Collaborative spectrum sensing for opportunistic access in fading environment, in: Proc. IEEE DySPAN 2005, November 2005, pp. 131–136.

[8] R.W. Thomas, L.A. DaSilva, A.B. MacKenzie, *Cognitive networks*, in: Proc. IEEE DySPAN 2005, November 2005, pp. 352–360.

[9] F.K. Jondral, *Software-defined radio-basic and evolution to cognitive radio*, EURASIP Journal on Wireless Communication and Networking 2005

[10] Akyildiz, I. F., Lo, B. F., & Balakrishnan, R. (2011). *Cooperative spectrum sensing in cognitive radio networks: A survey*. Physical Communication, 4(1), 40–62

[11] J. Unnikrishnan, V.V. Veeravalli, Cooperative sensing for primary detection in cognitive radio, IEEE Journal of Selected Topics in Signal Processing 2 (1) (2008) 18–27.

[12] Z. Li, F. Yu, M. Huang, A cooperative spectrum sensing consensus scheme in cognitive radios, in: Proc. of IEEE Infocom 2009, 2009, pp. 2546–2550.

[13] B. Wild, K. Ramchandran, Detecting primary receivers for cognitive radio applications, in: Proceedings of the IEEE DySPAN 2005, November 2005, pp. 124–130.

[14] W. Zhang, K. Letaief, Cooperative spectrum sensing with transmit and relay diversity in cognitive radio networks— [transaction letters], IEEE Transactions on Wireless Communications 7 (12) (2008) 4761–4766.

[15] S. Alrabaee, M. Khasawneh, A. Agarwal, N. Goel, and M. Zaman, "Applications architectures and protocol design issues for cognitive radio networks: a survey," International Journal of Wireless and Mobile Computing, vol. 7, no. 5, pp. 415–427, 2014.

[16] Zeng, Kexiong, et al. "Location spoofing attack and its countermeasures in database-driven cognitive radio networks." Communications and Network Security (CNS), IEEE, 2014.

[17] Li, Muyuan, et al. "All your location is belong to us: Breaking mobile social networks for automated user location tracking." ACM Mobile Hoc. ACM, 2014.

[18] Jiajia Liu, Shangwei Zhang, Nei Kato, et al. "Device-to-device communications for enhancing quality of experience in software defined multitier LTE-A networks." IEEE Network, 2015, 29(4):46-52.