International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 7; Issue 3(C); March 2018; Page No. 10648-10652
DOI: http://dx.doi.org/10.24327/ijcar.2018.10652.1814

Research Article

A SURVEY ON AUTHENTICATION MECHANISMS IN COGNITIVE RADIO NETWORKS

Himakeerthana C and Ganesh D

Department of Computer Science and Engineering, Sree Vidyanikethan Engineering College,
Tirupati, Andhra Pradesh, India

ARTICLE INFO

Article History:

Received 7th December, 2017
Received in revised form 21st January, 2018 Accepted 05th February, 2018
Published online 28th March, 2018

Key words:

Authentication, Cognitive radio, Primary User, Secondary User, Security.

ABSTRACT

Cognitive Radio Networks has proved as the Next generation wireless technology. Cognitive Radio Network provides solutions for spectrum scarcity and spectrum underutilization problems. This CRN technology has intelligent devices which are capable of detecting vacant channels. In CRN's unofficial users referred as Secondary Users(SU) are capable to access this vacant frequency channels whenever Primary Users (PU) are not utilizing these channels. Several issues and security concerns are occurred while deploying the cognitive radio technology. In these networks the cognitive nodes can also enter and vacate the spectrum dynamically. So there is a chance for malicious node to enter into the network. This will creates problem for making secure communication. For this reason, every node has to be validated before entering into the network. Authentication is used to validate the identity of the user and it is the primary security property. In this paper, we review about various authentication mechanisms applied to cognitive radio networks.

INTRODUCTION

In the past decade, utilization of the wireless devices are rapidly increased which creates problems for allocation of spectrum due to insufficient availability of spectrum. According to Federal Communication Commission(FCC), almost 70% of assigned spectrum is remained unused [3]. For this reason, allocated spectrum must be utilized effectively so that it would meet the spectrum requirements. In conventional spectrum management policies, spectrum bands are accessed only by licensed users. But according to Static Spectrum Allocation policies, a particular spectrum band is allocated to users permanently. These users are known as licensed users or Primary users. This spectrum bands are not used by licensed users most of the time. At that time utilization of spectrum is reduced because spectrum remains ide. For this reason FCC introduces a new policy which improves spectrum utilization. In this policy licensed bands can be utilized by unlicensed users without causing interference to the licensed users. This process is called Dynamic Spectrum Allocation (DSA).

The concept of DSA is implemented by the cognitive radio technology. Cognitive Radio is equipped with Software Defined Radio (SDR). In SDR parameters are replaced by the software and SDR supports the air interface. The Cognitive Radio Technology is capable enough to identify empty spectral bands and parameters are reconfigured according to it.

All Cognitive Radio enabled nodes combined together to form the Cognitive Radio Network. In this network, each node performs the spectrum sensing operation continuously and this information is shared within the network so that vacant bands can be selected. The licensed spectrum bands are accessed by the unlicensed users in the absence of primary users and unlicensed users has to vacate the bands whenever licensed users want it. Like this cognitive radio nodes utilizes available spectrum bands. Cognitive Radio network technology possesses various characteristics such as learning, co-operative spectrum sensing and spectrum handoff which causes security problems. Cognitive radio changes its parameters dynamically as it learns from past experiences and present environment and then adapt to that environment. During spectrum sensing process the malicious node sends the false sensing information in order to create the disturbances in the communication.

In CRN's security is one of the crucial areas. As CRN's are kind of wireless networks therefore they are sensitive to traditional attacks. Moreover, CRN's are sensitive to specific threats because of their functionalities. Security creates challenges in cognitive radio network implementation.

The rest of the paper is organized into four more sections. In Section II, security threats in cognitive radio networks are discussed. In Section III, different security requirements are discussed. In Section IV, different types of authentication mechanisms are reviewed briefly. In Section V, finally we discuss about various areas in cognitive radio network were focus should be kept.

*Corresponding author: **Himakeerthana C**
Department of Computer Science and Engineering, Sree Vidyanikethan Engineering College,
Tirupati, Andhra Pradesh, India

Security Threats in Cognitive Radio Networks

Cognitive radio networks have two special characteristics [1] a) Artificial Intelligence (AI) b) Dynamic Spectrum Access (DSA). Security threats can be divided into two types based on these characteristics.

A) Security Threats in Artificial Intelligence Characteristics

Because cognitive radio possesses artificial intelligence characteristics, they have ability to learn from their surroundings and are capable to adapt according to that. The characteristics of AI includes: Learning and Reasoning. Cognitive Radio's learning engine is used to predict the optimal spectrum based on the present and past situations. A Reasoning engine generally defined as set of logical interference rules [2] and it is capable to provide conditions under which actions has to be performed. Some reasoning policies are needed for cognitive radio's to deal in different environments.

With these characteristics cognitive radio networks are provided with flexible functionalities. These functionalities introduce a new security threats which offers a way for attackers.

i) Policy Threats

Normally reasoning engine has ability to deal with different environments but it requires some reasoning policies. In the knowledge base, unaffected code policies are present which are used to deal with all possible situations. The failure of policies occurs because of policies in knowledge base cannot handle according to current situation or knowledge base doesn't contain sufficient policies. This failure of policies causes policy threats. In policy threat, the attacker can get the access to knowledge base and has ability to modify or delete the existing policies and fault policies are placed in knowledge base.

ii) Learning Threats

Learning is the ability which is used to enable cognitive radio to learn from the experiences in the past and in the present situation. This information can be used to predict about availability of spectrum. Learning radios are easily affected by false or modified sensory information. Whenever knowledge base is maliciously updated then there is a chance that wrong decisions about spectrum can be made by learning engine. Learning radios falsely senses idle channel as busy and busy channel as idle because of this malicious updated policies in knowledge base. Due to this kind of threats knowledge base can become useless.

B) Security threats in Dynamic Spectrum Access

By using Dynamic Spectrum Access method, cognitive radio can be able to sense the spectrum which is vacant and make use of it. Spectrum handoff is one of the important techniques which are used by CR enabled devices to make the spectrum available for primary users when they want it. In cognitive radio network, we use a method called Co-operative spectrum sensing in which spectrum is sensed by all nodes individually and this information is shared with other nodes. This spectrum sensing information is used to select the best spectrum from available spectrum. During spectrum sensing there is a chance for cognitive radio to falsely sense the spectrum due to presence of some malicious users.

In cognitive radio devices threats also comes from spectrum sensors. These sensors code is replaced by the selfish node so that it can behave maliciously. By using these faulty sensors, primary users can be interference because they are not having ability to detect the spectrum holes and also detect spectrum which is busy as idle ones. Another important threat in DSA is to prevent cognitive radio node from receiving faulty information. Jamming attack can be performed by attacker in order to jam control channel. If the radio statistics are continuously analyzed and monitored by attacker then these radio statics are also modified by them so that attackers can provide false sensory information.

In cooperative spectrum sensing, the sensed information is shared by all nodes by using this information they can make decisions about the spectrum. The malicious nodes provide the false sensing information and they are cooperating with other nodes majority of threats comes from this technique.

Security Requirements

Among many wireless networks, cognitive radio network faces more security attacks. As cognitive radio networks contains radio technology which is vulnerable to attacks. Normally, CRN's differs from other wireless networks because cognitive radio networks have unique reliability issues such as high sensitivity to weak primary signals, unknown primary receiver location, tight synchronization and lack of common control channel [6].

In CRN's, security is one of the major issue and threats are more complex and requires more attention. In cognitive radio networks attack possibility is high when compared to other networks. For this reason security policies are to be developed to reduce probability of malicious node attack. The major concepts to be applied to satisfy secure communication are: confidentiality, integrity, availability, non-repudiation, identification, authorization and authentication.

1) Confidentiality

Confidentiality is used to protect data from unauthorized access or unauthorized exposure of data to the system or individuals. It is one of the important requirements which is used to maintain owner's data privacy in which data contains details about bank storing credits and balance information of the customer[4]. As Radio is used as the communication medium in cognitive radio networks, for every connection in wireless networks confidentiality should be guaranteed because it is more vulnerable to attacks.

2) Integrity

Integrity is another important property which is used to protect data or information from being modified. This modification may be accidental or maliciously altered or damaged. This means integrity provides the data to be transmitted between source and destination without modification. The sender is only person who has authority to modify the data in message. Integrity is the property which is used to provide protection against unauthorized creation, alteration or destruction of data. If someone accepts the modified message then it will cause infringement of integrity property[5].

3) Availability

In Availability users of the network makes use of network for their own purpose and maintains the details of the traffic in network. In cognitive radio networks, the secondary users (SU) use the channel when Primary users(PU) are idle. Whenever the secondary user's senses that primary user wants back the channel then secondary users have to vacate the spectrum and make available for them.

4) Identification

Identification is one of the basic security requirements for any communication device. It is a method to associate a user/device with their name or identity. A tamper-proof identification mechanism should be built into the secondary user devices in cognitive networks.

5) Authorization

In the context of cognitive networks, we have a unique authorization requirement which we call conditional authorization. It is conditional because the secondary users are authorized to transmit in licensed bands only as long as they do not interfere with primary users' communications in that band. As it is difficult to pinpoint exactly which of the secondary users is responsible for harmful interference to the primaries' transmission, this type of authorization is hard to enforce and even more so in a distributed setting. Hence conditional authorization poses a unique challenge in dynamic spectrum access.

6) Non-repudiation

Non repudiation technique prevents either the sender or receiver from denying a transmitted message. Therefore, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can in fact prove that the data received was by the alleged receiver. In cognitive radio network setting, if malicious secondary users violating the protocol are identified, non-repudiation techniques can be used to prove the misbehavior and disassociate/ban the malicious users from the secondary network.

7) Authentication

Authentication is an assurance that the communicating entity is the one that it claims to be. The primary objective of an authentication scheme is to prevent unauthorized users from gaining access to protected systems. It is a necessary procedure for verifying both an entity's identity and authority.

In cognitive radio networks, there is an inherent requirement to distinguish between primary and secondary users. Therefore, authentication can be considered as one of the basic requirements for cognitive networks. In centralized cognitive networks, where the primary and secondary base stations are connected to a wired backbone network, it may be easier to have the CA connected to the wired backbone. However, in distributed cognitive networks with a number of secondary users dispersed over a large geographical area, providing the functionalities of a CA can be quite a challenge.

Security has two major issues to be considered in the primary users signal detection. They are misdetection and false detection. In false detection, secondary user detects the signals falsely, which are exhibited by the malicious nodes as primary user's signals and vacate the spectrum. The misdetection method is opposite to false detection.
In CRN's as the network nodes are intelligent as designed, threats are complex and attack occurrence is more when compared to other networks

Authentication Mechanisms

In cognitive radio networks, the cognitive nodes can enter and vacate the spectrum dynamically. So there is a chance for malicious node to enter into the network. This will creates problem for making secure communication. For this reason, every node has to be validated before entering into the network. Authentication is used to validate the identity of the user and it is the primary security property.

Two level authentication mechanism

In two level authentication mechanism [11], the cognitive node and its user are validated. This authentication mechanism can be applied to different layers which provide more security and makes available resources accessible only for authenticated users.

In this authentication scheme [11], all the secondary users in the network is divided into different clusters based on their locations. Each cluster may have unique identifier which is called as Cluster ID within the network. A fusion center is used to control the traffic in network. This fusion center will chose a node in each cluster as the cluster head. Each and every node which wants to join the network has to be authenticated. The authentication is performed at fusion center level and cluster head level. The node can be joined into the network only after it is passed successfully through the authentication.

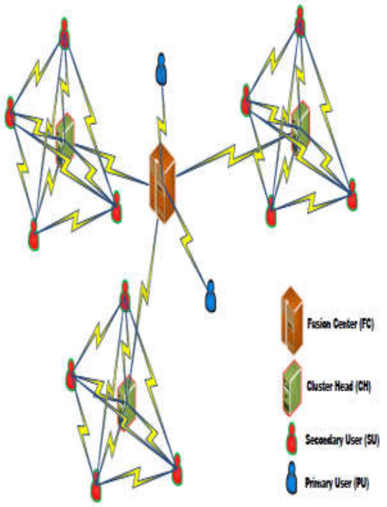

Fig System model of two level authentication mechanism

The server will grant the certificate for every node once it is manufactured. This certificate will comprise of logical identifier, mac address and a pair of public and private keys. Whenever node wants to validate the certificate of other node it will be sent to server because certificate of node is signed by server itself. During the validation process, server will provide all the information required by the node except the private key. Because private keys cannot beshared with anyone. Once certificate validation is completed then attacker cannot listens to the messages exchanged between joining node and authenticating parties. If the attacker tries to send the message then authenticating parties easily identify the attacker by using their certificates. By performing spectrum sensing, each secondary user tries to find out the available white spaces. If they found white spaces in any cluster then they contact the cluster head for their logical id's.

During authentication process, the joining node has to answer the three different questions which are asked by authenticating parties. If the joining node correctly answers to these questions then it leads to successful authentication. If the joining node is new node then fusion center asks, "what is the cluster id that joining node wants to join". But it is a returning node to the same cluster then in addition to before question it should answer "what is the joining code of the cluster that it want to join". During the second level of authentication which is done between the cluster head and joining node, joining node should answer to another question "what is the belief level of joining node" in addition to the above questions.

Digital signature based authentication mechanism

In digital signature based authentication scheme[12], public key cryptography with digital signature is used. This authentication scheme is used to identifying the efficient primary users in the network for making secure communications.

In this authentication mechanism, the architecture consists of both primary users and secondary users which are placed within the same geographical area. Here primary users are connected to their base stations which are called as primary user base station (PUBS) and secondary users are also connected to their base stations which are called as secondary user base stations (SUBS). These base stations of primary user and secondary user are connected to certificate authority (CA). This certificate authority is used to maintain secure authentication as both primary and secondary users are connected to CA via primary user base station(PUBS) and secondary user base station(SUBS)[12].

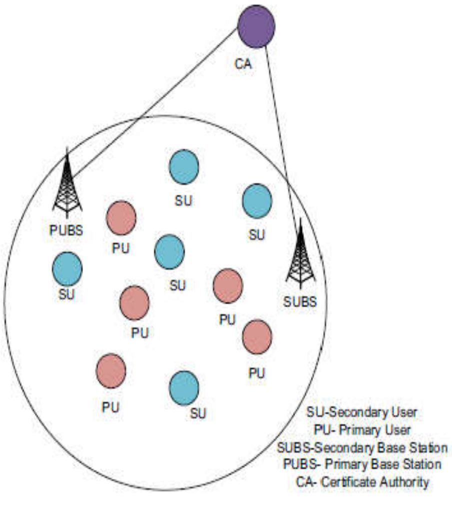
CA
SU
SU
PUBS
PU
SU
SU
SUBS
SU
PU
PU
PU
PU
SU
SU-Secondary User
PU- Primary User
SUBS-Secondary Base Station
PUBS- Primary Base Station
CA- Certificate Authority

Fig System model for Digital Signature based authentication

In digital signature based authentication scheme, certificate authority is one entity which is used to establish a connection with base stations of both primary and secondary users through a wire. The primary users generate a pair of public and private keys by using key generation algorithm. Once keys are generated they are sent to certificate authority through primary user base station. Then certificate authority is used to store all the keys generated by primary users. If these public and private keys are changed by primary users then certificate authority has to inform about it. Then certificate authority will make the updates to the key list.

The primary user encrypts its identity and time stamp in order to generate a digital signature. Then primary user signs the message using this digital signature and message will be transmitted. By using a sensing algorithm, secondary user senses the primary user transmission. Once the transmission is detected then secondary user decodes the primary users signed message and signature is detached and it is transmitted to secondary user base station. The secondary user base station obtains the list of primary user identities from certificate authority. Once message is received then it is decrypted by secondary user base station and checks whether or not decrypted id matches with anyone in the list and checks its time stamp. If id is present in the list then it is the licensed and efficient one. If the id doesn't match with anyone in the list then it is not licensed one.

Trust based authentication mechanism

In cognitive radio networks trust and security are linked with each other. In this method, the primary users will check the identity of the secondary user whenever secondary user wants to access the spectrum based on trust value.

In this trust based system architecture [10], both primary users and secondary users are placed within the same geographical area. Here primary users are connected to their base stations which are called as primary user base station (PUBS) and secondary users are also connected to their base stations which are called as secondary user base stations(SUBS). These base stations of primary user and secondary user are connected to certificate authority (CA). This certificate authority is used to maintain secure authentication as both primary and secondary users are connected to CA via primary user base station(PUBS) and secondary user base station(SUBS).

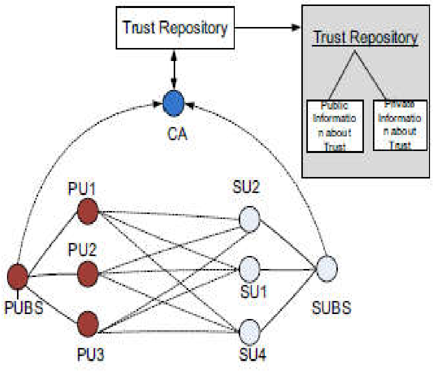
Trust Repository
Trust Repository
Public Informatio n about Trust
Private Informatio n about Trust
CA
PU1
SU2
PU2
SU1
PUBS
SUBS
PU3
SU4

Fig System model of trust based authentication

In trust based authentication mechanism, primary user has to check the trust value of secondary user before allowing the secondary user to access the spectrum in the absence of primary user. The CA has a repository which is used to store the trust value of each and every cognitive radio node. This trust repository contains two values for each node. Among these two values one value is known as public value and another one is known as private value. Public value means this value is visible to all nodes and can be easily accessible in the network. Private value means this value is only visible to Certificate Authority (CA) [9] and this is stored for secure communication. If any attacker modifies the trust value of the node then CA will identify this unauthorized modification by verifying its private value and acquires information about attacked node. In order to revoke the attacked node CA will broadcast a message.

The secondary user tries to access the spectrum whenever primary user is not using it. Then secondary user trust value is verified by primary user base station (PUBS). The primary user base station verifies secondary user trust from trust repository in CA. If trust value is greater than threshold secondary user is allowed to access it. If secondary user already holding a connection then primary user base station calculates the average reference value and verify trust value. If it is not greater than threshold then secondary user is not allowed to access the spectrum. If any new node wants to access the free primary user spectrum, then it should meet agreement with the base station. Then trust value for the new node will be assigned by the base stations by reviewing its past reports.

Future Work

In cognitive radio networks, security issues are still not getting attention. So, here are some research directions where more focus should be kept.

The cognitive radio networks can utilize the security protocols available in different networks. As cellular networks use a unique identity for each user which is used as international mobile user identity where a secret key which is shared between new nodes and base station to apply authentication similarly this type of authentication mechanisms can also be used.

The envious node behaves as primary user and make secondary user to believe so that it can start behaving wrongly. For this reason there should be clear differentiation between the legitimate primary user and attacker node. This can be done by verifying the identity of the node. Hence there is a need to develop more cryptographic algorithms.

If the secondary users are not correctly sensed then available bands cannot be properly used. For utilizing the unused licensed bands efficiently they should correctly sensed by the secondary users. So there is a need for proposing efficient spectrum sensing techniques.

References

1. Yuan Zhang, GaochaoXu, XiaozhongGeng, "Security Threats in Cognitive Radio Networks", proceeding of 10th IEEE International Conference on High Performance Computing and Communications, Changchun, China, 25-27 Sept. 2008, pp: 1036-1041.
2. T. Charles Clancy, Nathan Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation", proceeding of 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Singapore, May, 2008, pp:1-8.
3. Federal Communications Commission, Cognitive Radio Technologies proceeding.
4. W. El-Hajj, H. Safa, M. Guizani, "Survey of Security Issues in Cognitive Radio Network", *Journal of Internet Technology* Volume 12, No.2, 2011.
5. J. Zhao and G. Cao, "Robust topology control in multi-hop cognitive radio networks", In INFOCOM, 2012 Proceedings IEEE, pages 2032- 2040. IEEE, 2012.
6. D. Vir, Dr. S.K Agarwal, Dr. S.A Imam, "Power Analysis and Comparison of Reactive Routing Protocols for Cognitive Radio Ad Hoc Networks", IJAREEIE, July 2013.
7. Mahmoud Khasawneh, Anjali Agarwal," A survey on security in Cognitive Radio networks", proceedings on 4th international conference on CSIT.
8. Kamal Kumar Chauhan, Amit Kumar Singh Sanger,"Survey of Security threats and attacks in cognitive radio networks" proceedings on 2014 International Conference on ICECS.
9. C. Ben-Jye et al., "Markov Chain-Based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad Hoc Networks", Asia-Pacific Services Computing Conference 2008. APSCC '08. IEEE, 2008.
10. SaziaParvin, Song Han, BimingTian, FarookhKadeerHussain ,"Trust-Based Authentication for Secure Communication in Cognitive Radio Networks" proceedings on IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.
11. Mahmoud Khasawneh, Anjali Agarwal "A Secure and Efficient Authentication Mechanism Applied to Cognitive Radio Networks", published in IEEE Access ,vol. 5 2017.
12. Parvin.S, Khadeer F.H, & Khadeer O.H "Digital signature-based authentication framework in cognitive radio networks", 10th International Conference on Advances in Mobile Computing & Multimedia.

How to cite this article:

Himakeerthana C and Ganesh D (2018) 'A Survey on Authentication Mechanisms in Cognitive Radio Networks', *International Journal of Current Advanced Research,* 07(3), pp. 10648-10652.
DOI: http://dx.doi.org/10.24327/ijcar.2018.10652.1814

****