Countermeasure Against Physical Layer Attack in Cognitive Radio Networks

K. Anbukkarasi, Assistant professor, Electronics and Communication Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi, India, logicanbu@gmail.com

M. Sowmiya, Final year student, Electronics and Communication Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi, India, sowmiyamaheswaran@gmail.com

C. Nishanth, Final year student, Electronics and Communication Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi, India, nishanth2995@gmail.com

VS. Selva Kiruba, Final year student, Electronics and Communication Engineering, Dr. Mahalingam College of Engineering and Technology, Pollachi, India, selvakirubavs@gmail.com

Abstract—A “Cognitive radio” is a latest technology aiming to solve the spectrum scarcity problem by allocating the spectrum to secondary users. It aims to improve the utilization of the radio spectrum by reducing the spectrum holes. The existing systems that have been proposed so far provided the solution for some attacks in the Physical layer of Cognitive radio with a limited number of nodes, evaluated with the parameters like end to end delay, packet delivery with least security. Also the methods have not provided the accurate solution for specific application. Our project aims at providing solution for the physical layer attack with enhanced security considering large number of nodes and thus reduces the interference among primary and secondary users.

I. INTRODUCTION

Wireless technology shows a drastic enhancement in its technological and its application features. These primary and secondary users greatly trust on the available radio spectrum, which leads to a scarcity in the available spectrum. Certain portions of the spectrum are made available for public use, which is vacant claimed by The Federal Communications Commission (FCC). Cognitive radio (CR) is defined as software defined radio in wireless communication that sense the environment and detect the free space among the crowded channel, and utilize the vacant space efficiently.

This paper emphases on the analysis of security issues in various perspectives on the cognitive radio networks. On each layer of spectrum there exists attacks launched by attackers, but most commonly they target on the lower level layer i.e. physical layer [2]. The existing systems have considered only a few nodes with least security for the attacks, which will not be applicable for all the generic scenarios.

This paper aims at providing solution with increased number of nodes for a particular application and can also be applied for different scenarios. We use cryptography technique which relay on certificate concept like giving specific ID to users. Users ID is given for a precise period and then it can be changed after the period. Using energy consumption ratio and packet delivery ratio, the attack can be perceived and rejected at the entrance in spectrum.

II. COGNITIVE RADIO NETWORKS

Mitola introduced software defined radio in 1991 and cognitive radio in 1998. Software Defined Radio (SDR) is a multiband radio that supports reconfigurable through software which runs on Digital Signal Processor (DSP). A latest communication technology named “Cognitive Radio Network” is a network in which an unlicensed user can use a free channel in a spectrum band of licensed user without interference. Cognitive Radio (CR) is
an adaptive, intelligent radio and network technology that can automatically detect available channels in a wireless spectrum and change transmission parameters enabling more communications to run concurrently and improve radio operating behaviour.

Fig 1: CRN Architecture

The primary network is also called licensed user network or incumbent users network, which is an existing network, where primary users work in licensed spectrum bands.

A. Functions of CRN

Spectrum sensing, spectrum management, spectrum mobility and spectrum sharing are the functions of cognitive radio networks. Spectrum sensing is defined as sensing spectrum holes and allocation of the spectrum without interfering with further users. In DSA, the licensed users have the certificate to use the certain frequency band and when they are not in use, it is left idle. Thus, their available spectrum could be used by the secondary users. Such secondary user require sensing algorithm to detect the spectrum holes for communication.

Spectrum Management is the process of selecting the best available channel. It is accomplished of selecting the most appropriate bands from the available bands according to the QoS requirements of the application. Spectrum sharing avoids multiple users colliding the overlapping portion of the spectrum. Spectrum mobility refers to the maintenance of seamless communication during the transition to better spectrum. The implementation of these functionalities exposes severe security threats.

III. ATTACKS IN CRN

In the ISO/OSI model CRN attacks are involved in various layers. Attacks which are falling in physical layer is said to be a physical layer attack and attackers which rely on link layer is said to be MAC layer attacks, and over the network layer is said to be network layer attacks, and on transport layer is said to be transport layer attacks. Depending on the attacks, threats are perceived and the security measures are taken. In the Physical layer, Primary User Emulation attack and Jamming attack is discussed.

A. Jamming Attack

The jamming attack in the communication network is to deny service by eating up high part of bandwidth. In jamming attack, it maliciously send out packets continuously to obstruct the legitimate participants in a communication session from sending or receiving data; simultaneously it creates a denial of service situation.

Fig 2: Jamming Attack

The jammer can also interrupt communication by attacking a radio transmission resulting in the corruption of packets received by legitimate users. Thus, jamming is an attack that is known to both physical and MAC layers.

B. Primary User Emulation Attack

In CRN, primary users has the priority to access the channel. If a primary user begins to transmit through frequency band engaged by a unlicensed user, it is required to leave that particular specific spectrum band immediately. Conversely, when there is no primary user activity present within a frequency range, all the secondary users possess equal rights to the unoccupied frequency channel. When a secondary user is on, it is assumed that the
signal is that of a secondary user only; otherwise it concludes that the signal is of a primary user.

The existing detection approaches can be classified into Received Signal Strength (RSS) based detection, Feature detection, Location verification and Cooperative detection.

The approach then employs a cyclostationary calculation to represent the features of the user signals, which are then fed into an artificial neural network for classification. There are two location verification schemes called as Distance Ratio Test (DRT) and Distance Difference Test (DDT) respectively.

In both schemes, dedicated cognitive nodes (SUs or a cognitive BS) with enhanced functionality are involved for location verification. DRT uses a Received Signal Strength (RSS) based method, where two dedicated cognitive nodes measure the RSS of the signal source and calculate the ratio of these two RSS to check whether it coincides with their distances to the true PU (e.g., a TV broadcast tower). Using DDT, the arrival time of the transmitted signal from the source is measured by the two dedicated cognitive nodes.

V. PROPOSED METHOD

The Existing Systems have considered only a few nodes with least security for the attacks which will not be applicable for all the generic scenarios. The proposed method aims to provide solution for the physical layer attack with enhanced security considering large number of nodes. The betterment of the proposed system can be realised when comparing its performance with the existing system.

A. Introduction

The Proposed method provides solution for the Primary User Emulation attack. There are practical requirements for efficient PUE attack defense approaches. Our Proposed system fulfill the requirements with enhancement security. The proposed method analyzes the parameters like end to end delay, Packet delivery ratio with large number of nodes.

B. Block Diagram

The main purpose of the proposed system is giving enhanced security with better spectral efficiency among the users. The flowchart designates how the enhanced security system is implemented in the scenario where it sends the packets to the spectrum. There are two users i.e primary users and secondary users.
Both the users are given with certain keys. These keys are fed in the source at the initial stage.

![Block Diagram of Proposed System](image1)

**Fig 5: Block Diagram of Proposed System**

When the licensed user occupies the specific band and sends the signal it will be identified by the source with the key which was already provided. When it sends the signal it will check with the keys, if it is same it will allow otherwise it will revoke the node.

By the time an attacker comes and sends the signal like primary user the source will identify that it is an attacker by comparing with the key and that node is revoked by the source. If the source checks the user with the key that is already provided and found that it is not an attacker, it is allowed to deliver the packet. Thus an enhanced security is ensured among the users.

**C. Advantages**

1. Enhanced security among users.
2. Secure CRN from PUE attacks.
3. Spectrum hole will be reduced.
4. Reduces interference long users.

**VI. RESULTS AND ANALYSIS**

The Simulation output of CRN with PUE attack is shown in this chapter. The Existing system output is also given to compare with the Proposed system. Therefore Security concept is clearly analyzed in comparison with the existing system.

**A. Existing System Output**

The figure shows the communication between the nodes in Cognitive radio. In the spectrum, specific bandwidth are assigned to the users from the router.

![Scenario of Nodes from Source to Destination in the Existing System](image2)

**Fig 6: Scenario of Nodes from Source to Destination in the Existing System**

The figure depicts the existing system in the cognitive radio network where primary user and secondary users are assigned to specific bandwidth.

![Scenario of CRN Simulation](image3)

**Fig 7: Scenario of CRN Simulation**

The below figure shows the Cognitive radio sensing in the spectrum. Among the four functions of CRN, the most important sensing is simulated among the users in the spectrum. The sensing services to identify whether the spectrum is free or not to the users. When the spectrum is free the secondary user will utilize the band, if the primary user enters the spectrum the secondary user must leave the spectrum as the primary user has the higher priority to use the spectrum.

![Scenario of Attacks in CRN](image4)

**Fig 8: Scenario of Attacks in CRN**

In PUE attack, the attacker sends the signal same as that of a Primary user and thus the secondary user gets cheated which results in spectrum hole.
B. Proposed System Output

The Proposed system reduces the attack and thus an efficient use of spectrum is achieved by the cognitive radio.

![Image of Scenario of CRN with Increased Number of Nodes in the Proposed System.](image1)

In this method, key authentication is implemented which is used for transferring encrypted message among the users.

![Image of Scenario of Proposed Concept With PUE Attack](image2)

This scenario represents a large number of nodes which is not present in the existing method. This scenario is helpful for considering the performances of the users. The below figure shows the CRN with individual key provision for the users.

![Image of CRN with Security Provision](image3)

This ensures security among the users which is not available with the existing system. Initially, the keys are assigned for every node in the CRN. This key is the identity for the node while sending packets. The Keys are fed in the Source at the initial stage. When the Primary user occupies the specific band and sends the signal it will be identified by the Source as it is already provided enough information about the key. When the users send the signal it will check with the Keys, if it is same, the communication will be permitted among the users otherwise it will revoke the node. When an attacker comes and sends the signal like Primary user the source will identify that it is an attacker by comparing with the key and that node is revoked by the Source.

VII. SIMULATION RESULT

A. Throughput

Throughput is the rate of successful message delivery over a communication channel. In this regard the output shows that, in existing method the throughput is less which is indicated in third curve (Blue).

![Image of Throughput](image4)

Throughput is better in the proposed system by using security key provision with a common source for many users which is indicated in second curve (Green). Throughput is much better by using security key provision with a unique source for separate set of users is indicated in first curve (Red).

B. Delay

Packet delay is the difference in end to end one way delay between selected packets in a flow with any lost packets being ignored. In this regard the output shows that, in existing method the delay is high since there is no security between the users, this is indicated in first curve (Red).
Fig 13: Delay
Delay is better by using security key provision for many users which is indicated in second curve (Green). Delay is much better by using security key provision with a unique source for separate set of users is indicated in third curve (Blue).

C. Energy
Energy is an important parameter in data transmission. In this regard the output shows that, in existing method the energy is low between which is indicated in third curve (Blue).

Fig 14: Energy
Energy is better by using security key provision with a common source for many users which is indicated in second curve (Green). Energy is much better by using security key provision with a unique source for separate set of users is indicated in first curve (Red).

VIII. CONCLUSION
We report successful simulation of Primary User Emulation attack on physical layer in cognitive radio network with implementing high security among the users. The lack of available spectrum and increase in the applications on wireless systems made the CR an adaptable method in the demanding wireless technology. This method diminishes the attack and thus an efficient use of spectrum is achieved by the cognitive radio networks. This method also reduces the interference among licensed and unlicensed users and also reduces the spectrum holes. In our project, a background on CRNs security and common threats/attacks on physical layer are analyzed and addressed with their countermeasures.

IX. REFERENCES