MITIGATION OF PUE ATTACK USING PSO IN WIRELESS COGNITIVE RADIO NETWORKS

A.DHIVYA LAKSHMI (Student) dhivyabella@gmail.com, Department of IT, National Engineering College, Kovilpatti.
D.DIANA (Student) diantwila@gmail.com, Department of IT, National Engineering College, Kovilpatti.
Mr.S.VIMAL (Assistant Professor) vimal28.05.1984@gmail.com, Department of IT, National Engineering College, Kovilpatti.
Dr.L.KALAIVANI (Professor) anuprakad@gmail.com, Department of EEE, National Engineering College, kovilpatti.
Dr.M.KALIAPPAN (Associate.Professor) kalsrajan@yahoo.co.in, Department of IT, National Engineering College, Kovilpatti.

ABSTRACT

A cognitive radio wireless network plays a vital role for opportunistic spectrum access. It helps us to efficiently handle the spectrum resources. Here the wireless operations and services are the most important functions in the cognitive networks. Security is a very important problem in CR networks. The security issue happens due to primary user emulation (PUE) attackers in CR networks. The attackers are detected by using Diffie-Helman key exchange cryptographic algorithm and to provide security particle swarm optimization machine learning algorithm is used.

Keywords: Cognitive Radio Networks, Primary User Emulation Attack, Scheduling.

INTRODUCTION:

The concept of cognitive radio network (CRN) was introduced to increase the frequency spectrum utilization in wireless networks. A CRN comprises of two types of users in wireless networks: the Licensed or Primary users (PU) and the Unlicensed or Secondary users (SU). Security problems faced by a CRN are unique as compared to the ones in traditional Wireless Networks. The security attacks such as the Denial of Service attack at physical layer are capable of damaging the whole network. These attacks are to be prevented immediately. By using Elliptic curve cryptography based Diffie-Helman key exchange algorithm, PUE attack has been detected and by using Particle Swarm Optimization algorithm the PUE attacks are prevented. Diffie-Hellman key exchange algorithm provides security by exchanging two cryptographic asymmetric keys. Here the sender and the recipient have no knowledge of each other. They share a secret key over an insecure channel. In PSO algorithm by using node characteristics such as position, velocity, speed and energy are calculated. If there is a change in these node characteristics the attacker is detected and prevented immediately.

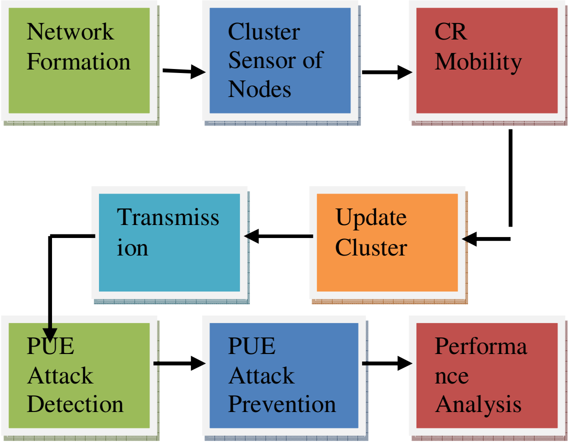
EXISTING SYSTEM:

A concept used in the existing system is Sensor Network which encourages the Cognitive network. The wireless sensor networks support the cognitive network. The Primary User activity and their information are usually detected by an associate sensor network and the information is send. Here information on PU activity detected by a separate sensor network is transmitted by means of multiple hops in Cognitive Radio Network in a single sink. Here the main goal is, without affecting or interfere the licensed network the capacity of the unlicensed network usage should be maximized. Also if the licensed and unlicensed users are presented in the same area the coexistence between them must be maintain. Normally the usage of the spectrum is examined by the wireless sensor network and the awareness of the currently available network will be notified and used efficiently by the secondary network. Once the information is got by the secondary user it will be very helpful for the secondary user to communicate and data transfer without affecting the licensed user called Primary Network. But here the major drawback is high energy consumption. Due to multi-hop transmissions to Cognitive Network the end-to-end delay will be more. CR user's cooperation is less since the mobile CRs are placed in the network.

PROPOSED SYSTEM:

The system proposes a CR network with disarticulate subset. It is one of the best methods for sensing. It can be obtained by high energy efficient resources. The cognitive network is composed of ad hoc CRs, assigning mobility to cognitive network to be more familiar. Here an ad hoc CR is considered as a cluster prime. It is surrounded by a cluster of sensor nodes within one-hop communication range and each cluster is further divided into subsets. To achieve energy efficiency, proper scheduling is used. It is based on the systematic behaviour of the primary users. The proposed system uses an energy-efficient cluster restoring and subgroup formation (CUSF) process. The cognitive radio network randomly move in time and the subgroup of the clusters in the sensor network are restored accordingly in which only one subgroup in a cluster is active at a time while others switch to sleep mode. This can be switched to sleep mode for a certain number of time slots by the proposed scheduling algorithm, based on the primary user activity. Due to free and frequent moves of the sensor nodes and the subsequent CUSF process for each move, energy consumption for every node is also considered. Here the energy for each sensing is considerably less when compared to the communication energy. Thus, reducing the sensing energy helps in lengthening the lifetime of the sensor nodes in the network. In physical layer, PUE attacker's behaviour are detected and reported to above layers. The cognitive radio network will not interact with a primary user network, and hence the secondary users usually lack information about the spectrum usage in the given network. The major four functionalities of CR networks are spectrum sensing, spectrum mobility, spectrum sharing, and spectrum management. These attacks cause risk to the information confidentiality and availability of a CR network. The attackers are detected by using Diffie-Helman key exchange algorithm and to provide security particle swarm optimization machine learning algorithm is used.

METHODOLOGY:



In the network formation, the primary user and secondary user nodes are created dynamically. Then the data packets are communicated among the primary users. TCP is used for establishing the connection between the source and destination. File transfer protocol (FTP) randomly choose different source-destination connections. Then cluster sensing takes place. Here we search for the neighbouring nodes. To discover the neighbour node, we send a request message and calculate node position. The node position, speed and velocity are updated for every millisecond. Then the PUE attacker is detected and prevented successfully.

IMPLEMENTATION:

In our project first we have created four static nodes called service provider for providing spectrum range and under this range of spectrum there will be a certain number of primary and secondary users are present. The primary user and secondary user are created dynamically. Every primary users and secondary users have their own energy, velocity, position and speed. Data transmission usually occurs between the primary users. The spectrum provider will provide spectrum to the users based on the needs of primary users. Sometimes the spectrum providers move to the location where there is a need for spectrum allocation. From there, the node which has highest energy will be selected as a base station for data transmission between the primary users under the particular spectrum range. During data transmission from one node to another there might be an attacker or hacker who affect the data transmission and also to spoil the whole network. In order to find the attacker Diffie-helman algorithm has been used. In this algorithm, key verification is done using openssl gendh command. The Diffie-helman parameters are generated and key verifications are done. If there is a mismatch in these key then the node will consider as an attacker. The attacker is prevented by using particle swarm optimization algorithm. In this algorithm the attacker is prevented based on the characteristics of the nodes.

PSO Algorithm:

In this algorithm, the primary emulation attacker is prevented by calculating the node characteristics. The node characteristics include node position, speed, velocity and energy. Since the sensor nodes move from one place to another these characteristics changes for every millisecond. So the node characteristics are calculated for each and every millisecond. These values are stored internally and it can be used as a reference for checking the node characteristics.

Step 1: Generate a cluster of nodes.

Step 2: Initialize each nodes with random position, velocity, speed and energy.

a. **Position** or location of the sensor node, X=(x, y)

b. **Velocity** of the node V=(v1, v2), where v1 is the average velocity of the sensor node and v2 is the current velocity

c. **Energy** of the sensor node, E

Step 3: Update the position and velocity of each and every nodes at base station.

Step 4: Then the Base Station makes the sensor nodes to perform clustering.

Step 5: Check the inequality constraints.

Step 6: If attacker is detected it is identified and prevented.

Diffie-Helman Key Change Algorithm:

In this algorithm, Key verification is done by generating an asymmetric key. The two main components for generating key are the node id and the candidate key. The node id is a unique id which is used to uniquely identify each and every node. The certificate id is used for generating a public key. The openssl is a general purpose cryptographic library which is a toolkit for transport layer security. The openssl gendh is used for generating Diffie-helman parameters.

Step 1: Requires two large numbers, one prime (P), and (G), a primitive root of P.

Step 2: P and G are both publicly available numbers.

Step 2a: P is at least 512 bits.

Step 3: Users pick private values a and b.

Step 4: Compute public values.

Step 4a: x = ga mod p

Step 4b:y = gb mod p

Step 5: Public values x and y are exchanged.

Step 6: Compute shared, private key.

Step 6a: ka = ya mod p

Step 6b: kb = xb mod p

Step 6c: Algebraically it can be shown that ka = kb.

Step 7: Now we have a symmetric secret key to encrypt

Performance Measure:

The simulation has been done with parameters listed below[16]:

Metrics	**Ranges**
Geographic area	300 x 300
M	5 to 60
N	500
U (utility $SU_{1\ldots n}$)	2 x 10^5

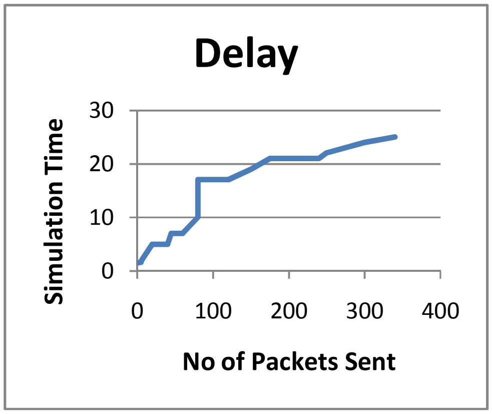


Fig 1. Delay Analysis

$$\text{Delay} = \frac{\text{No of packets sent}}{\text{Simulation Time}}$$

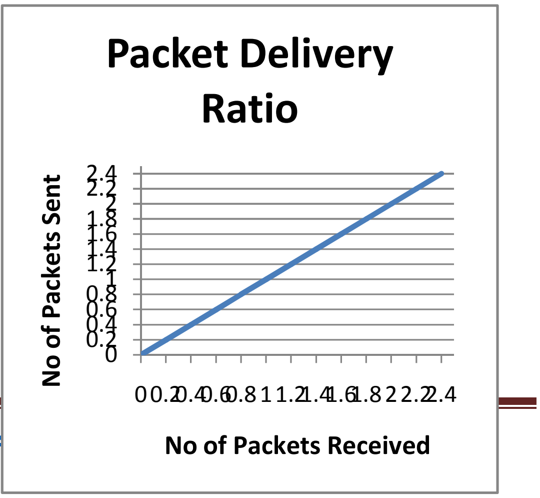


Fig 2. Packet Delivery Ratio Analysis

$$\text{PDR} = \frac{\text{No of packets received}}{\text{No of packets Sent}}$$

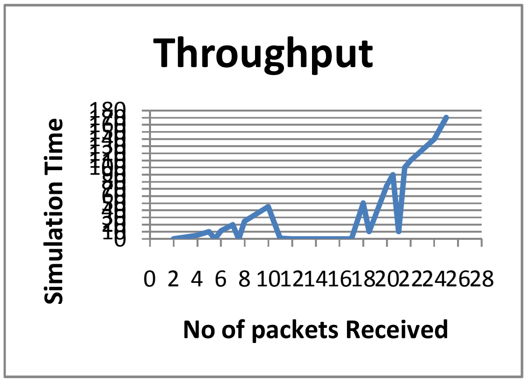


Fig 3. Throughput Analysis

$$\text{Throughput} = \frac{\text{No of packets received}}{\text{Simulation time}}$$

CONCLUSION:

This project mainly focuses on the security problem that arises due to PUE attack in CR networks. Here we have dynamically created primary user and secondary user nodes. Service providers are made static initially but based on the primary user requirements they move from their location to allocate spectrum for every cluster of nodes. By using Diffie – Helman based key exchange algorithm, the PUE attacker is detected. Then to prevent these kinds of attacks, Particle Swarm Optimization algorithm is used.

REFERENCES:

- [1] Rong Yu, Yan Zhang, Yi Lui, Stein Gjessing and Mohsen Guizani, “Securing Cognitive Radio Networks against Primary User Emulation Attacks”, in IEEE Journal , November/December 2016.
- [2] Angelo Furno, Diala Naboulsi, Razvan Stanica and Marco Fiore, “Mobile Demand Profiling for Cellular Cognitive Networking”, in IEEE journal, MARCH 2017.
- [3] Kamal Tourki and Mazen O.Hasna, “A Collaboration Incentive Exploiting the Primary-Secondary Systems’ Cross Interference for PHY Security Enhancement”, in IEEE journal, vol. 10, no. 8, DECEMBER 2016.
- [4] Mohamed Grissa, Attila A. Yavuz and Bechir Hamdaoui, “Location Privacy Preservation in Database-Driven Wireless Cognitive Networks through Encrypted Probabilistic Data Structures”, in IEEE journal, vol. 3, no. 2, JUNE 2017.
- [5] Anestis Tsakmalis, Symeon Chatzinotas and Bjorn Ottersten, “Interference Constraint Active Learning with Uncertain feedback for Cognitive Radio Networks”, in IEEE journal, vol. 16, no. 7, JULY 2017.
- [6] Yao Zheng, Wenjing Lou, Assad Moini, Thomas Hou and Yuichi Kawamoto, “Cognitive Security: Securing the Burgeoning Landscape of Mobile Networks”, in IEEE journal, July /August 2016.
- [7] Hong Xing, Xin Kang, Kai-Kit Wong and Arumugam Nallanathan, “Optimizing DF Cognitive Radio Networks with Full-Duplex-

Enabled Energy Access Points", in IEEE journal, vol. 16, no. 7, JULY 2017.

- [8] Huayan Guo,Wei Jiang and Wu Luo, "Linear Soft Combination for Cooperative Spectrum Sensing in Cognitive Radio Networks", in IEEE journal, 2017.
- [9] Idris Abubakar Umar,Zurina Mohd Hanapi,A.Sali and Zuriati A.Zulkarnain, "TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks", in IEEE Journal, vol. 14, no. 8, AUGUST 2015.
- [10] Doha Hamza and Jeff S.Shamma, "BLMA: A Blind Matching Algorithm with Application to Cognitive Radio Networks", in IEEE Journal, 2017.
- [11] Xingzheng Zhu, Bo Yang, Cailian Chen, Liang Xue, Xinping Guan and Fan Wu, "Cross-Layer Scheduling for OFDMA-Based Cognitive Radio Systems With Delay and Security Constraints", in IEEE Journal, vol. 64, no. 12, DECEMBER 2017.
- [12] Jei Hu, Lie-Liang Yang and Lajos Hanzo, "Energy-Efficient Cross-Layer Design of Wireless Mesh Networks for Content Sharing in Online Social Networks", in IEEE Journal, 2017.
- [13] Jacob Wurm, Yier Jin, Yang Liu, Shiyan Hu, Kenneth Heffner, Fahim Rahman and Mark Tehranipoor, "Introduction to Cyber-Physical System Security: A Cross Layer Perspective", in IEEE journal , 2016.
- [14] Hadi Saki and Mohammad Shikh-Bahaei, "Cross-Layer Resource Allocation for Video Streaming Over OFDMA Cognitive Radio Networks", in IEEE journal, vol. 17, no. 3, MARCH 2015.
- [15] Trong Nghia Le, Wen-Long Chin and Wei-Che Kao, "Cross-Layer Design for Primary User Emulation Attacks Detection in Mobile Cognitive Radio Networks", in IEEE Journal, vol. 19, no. 5 MAY 2015.
- [16] Vimal, S., Kalaivani, L. & Kaliappan, "Collaborative approach on mitigating spectrum sensing data hijack attack and dynamic spectrum allocation based on CASG modeling in wireless cognitive radio networks", M. Cluster Computing (2017).