International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8278-8285

Encryption Algorithm for defending PUE Attack in Cognitive Radios

T.Lakshmibai [1] and Dr. C. Parthasarathy [2]

[1]Research Scholar, Department of Electronics and Communication Engineering,
Sri Chandrasekharendra Saraswathi Viswa Maha Vidyalaya University,
Enathur, Kanchipuram, Tamilnadu, India.

Orcid Id 0000-0002-5483-0603

[2]Assistant Professor, Department of Information Technology,
Sri Chandrasekharendra Saraswathi Viswa Maha Vidyalaya University
Enathur, Kanchipuram, Tamilnadu, India.

Abstract

The Security is major problem in the Cognitive Radio communication. Several algorithms are designed and implemented for increase in the security of the Cognitive radio. To increase the High Security to overcome the Primary User Emulation Attacks, we proposed the new algorithm called Self Adaptive QUAD Encryption has been proposed. The proposed algorithm has been analyzed and simulated using the test beds designed using ARM CPU and simulated with the MATLAB. The proposed Algorithm has the unique feature in which the key is being generated based on the four important parameters such as RSSI, Distance, Power and ID which are adaptive to the environments and mode of the communication. The four tier encryption algorithm which is generated has been compared with the existing algorithms with the illustration of 70% of reduction of the PUE (Primary User Emulation) Attacks. The proposed algorithm has been tested with the experimental setup which has been designed. Also the Dynamic and Adaptive Four Tier Encryption finds its suitability for the real time CR Hardware which are first of its kind. This Encryption key finds its applications in Health care, banking and even in Consumer Electronics where the authentications of the primary users are necessary.

Keywords: Cognitive Radio, Quad-type Encryption, Primary user (PU), Secondary user (SU), Channel (CH).

INTRODUCTION

Hence allows the confidential conversation to be carried out in a secured way. Although in the present technological era, endless solution are proposed towards the various security concerns that are the subjects of conversation in the middle of the entire technical organization, but very few of them have been realize practically. Once a user wants to join a CR network, it must start a trust negotiation with the CH at closer proximity. The user encrypts its ID whose decryption key is provided to the CH beforehand. Here the CH analyses the RSSI and energy to localise the user and to classify it as a PU or a SU. For more secured spectrum allocation, the key used for encryption of the ID varies dynamically in the PU. A quad type encryption key for data (QED) has been issued by four levels of encryption which makes it unfeasible for SUs or malicious SUs to duplicate the PUs characteristics. [6]

QUAD-TYPE ENCRYPTION OF DATA (QED)

It may provide a dynamically varying four tier encryption procedure to the primary user once a user needs to join a CR system, it must start a trust negotiation with the CH at closer proximity. The user encrypts its ID which is regenerated by the Cognitive Hardware. Here the CH analyses the RSSI and energy to localise the user and to classify it as a PU or a SU or an attacker in the Cognitive radio by cryptographic authentication of primary users. We integrate various parameters of the users for the Cognitive Hardware to classify the users and to recognize the malicious user.

The parameters include

- RSSI
- ENERGY/POWER
- USER'S ID

Also, an encryption technique to overcome the PUE attack by authorize the spectrum share by the Cognitive Hardware (CH) is based on the assessment of conventional frame from the users.

RELATED WORK

1. Z. Jin proposed: [1] in this research, present a lucid replica as well as a sensible machine to become aware of refutation of service (DoS) assault on minor users in lively range right of entry (DSA) system. In hard, we look at main user emulation attacks (PUEA) in cognitive radio system without using any site in order and so are able to do away with any devoted sensor system.

2. Sugata Sanyal proposed: [2] here hold up for a variety of multimedia request in wireless networks stress extra bandwidth in the radio incidence range. Efficient range organization algorithms are necessary to achieve huge success in wireless infrastructure. Cognitive radio seems to be a panacea for better than before use of approved spectrum. It is dividing as the new state of art method that opportunistically shares the licensed spectrum while imposing minimum meddling to the approved users.

3. T. Charles Clancy proposed: [3] this document describes a new group of students of assault exact to cognitive radio network. Wireless tactics that can *study* from their environs can also be *trained* things by horrible basics of their environs. By putting false skill in accuse of wireless scheme devices, we are allow surprising, developing behavior, fitting a perhaps indistinct or manipulate height of optimality. The state space for a cognitive radio is total up of a variety of learned beliefs and current sensor inputs. [3]

4. Yufang Cheng proposed: [4] Cognitive-radio (CR) skill is to make your mind up the spectrum shortage difficulty, make accessible extra range bands necessary for the data transmit in mobile ad hoc networks (MANET) and provide an suitable level of security for CR network conventional far less attention than other areas regarding to ordinary key organization schemes for MANET as well. Key association and verification are two important factors in MANET safety. The recent enlargement in Identity-based cryptography has made the technique to be a potential applicant for MANET.[5]

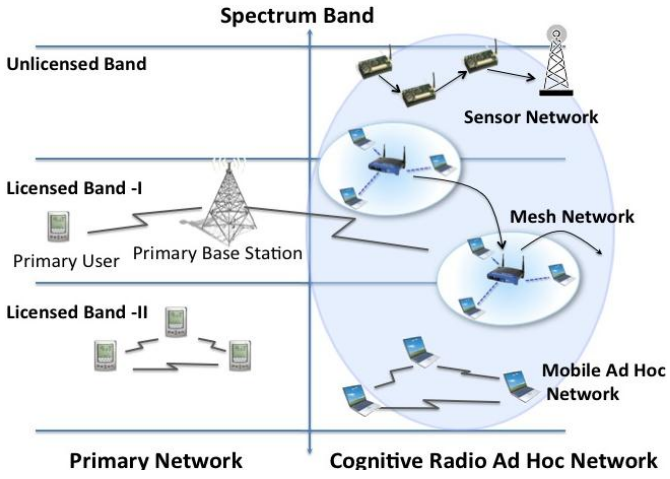


Figure 1: Spectrum Band in CR

PROBLEM IDENTIFICATION

In this highly spirited world, the risk of financial and supporting spying too has greater than before put a lot of management and being property at danger. A lot of method life form used for convey out communication are hesitant of you in the sense that their safety can be breach out and important chat can be listened to or record. Though they give good connectivity, but they are flat to a lot of safety intimidation as discuss proceeding. Still the usual mobile phone does not give end to end safety. Hence we can say that the secure message is necessary to attach and provide broadcast, processing, recording and monitor for various purpose such as: secure phone and network equipment and encryption management.

QUAD-TYPE ENCRYPTION OF DATA (QED)

A Cognitive Radio (CR) is capable of reconfiguring itself using its environmental interactions to accommodate the transmission parameters. It enables Dynamic spectrum allocation thereby provides efficient spectrum utilization. PUs are ensured better operation and SUs are allowed to effectively use the available spectrum. The dynamic spectrum sharing scheme that controls sharing between PUs, SUs and malicious users has serious security issues. [6]

Main consumer Emulation (PUE) assault is accepted out by a hateful minor user emulate a main user or secret as a chief user to get the capital of a agreed canal with not have to split them with other minor user. The assailant is able to get full band of a range in this attack. Hence an encryption technique has been proposed to overcome the PUE attack by authorizing the spectrum allocation by the Cognitive Hardware (CH) based on the evaluation of received frame from the users.[13]

Once a user wants to join a CR network, it must start a trust negotiation with the CH at closer proximity. The user encrypts its ID whose decryption key is provided to the CH beforehand. Here the CH analysis the RSSI and power to restrict the consumer and to categorize it as a PU or a SU. For more secured spectrum allocation, the key used for encryption of the ID varies dynamically in the PU. A Quad-type Encryption key for Data (QED) has been issued by four levels of encryption which makes it unfeasible for SUs or malicious SUs to duplicate the PUs characteristics. [8]

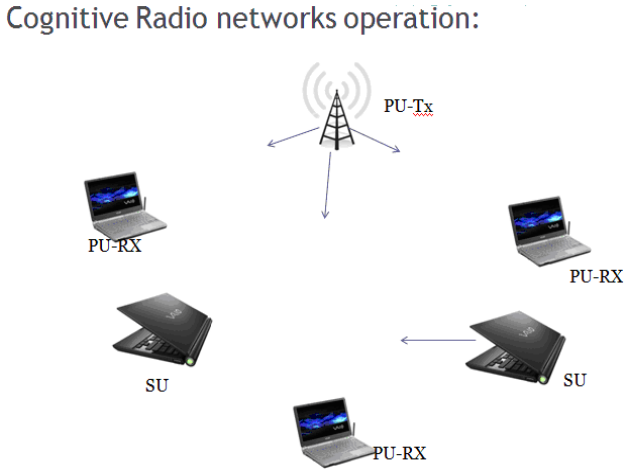


Figure 2: Proposed Quad-type Encryption of Data

The proposed Quad-type Encryption of Data (QED) provides an enthusiastically altering Four tier encryption procedure to the main user. Once a user needs to join a CR network, it must start trust arbitration with the CH at closer nearness. The user encrypts its ID which is regenerate by the Cognitive Hardware. Here the CH analyses the RSSI and energy to restrict the user and to categorize it as a PU or a SU or an assailant.[5] Also, an encryption technique to conquer the PUE attack by authorizes the spectrum share by the Cognitive Hardware (CH) based on the evaluation of received frame from the users. [3]

Frame Format 802.11 Encryption in CR

2Bytes	2	6	6	2	6	2	
Frame Control	Duration	Address 1(PU)	Address 2(SU)	Seq	Address 4(TX,RX)	Data	Check Sum

2Bits	2	2	1	1	1	1
Encyr Version	Type	SubType	To DS	From DS	RETRY	W	O

Adaptive QED over CH (Cognitive Hardware)

The objective is to generate a reliable Quad-type Encryption of Data (QED), to overcome the PUE attack by authorizing the spectrum allocation by the Cognitive Hardware (CH) based on the evaluation of received frame from the users. In the Cognitive radio by cryptographic authentication of primary users.[10]

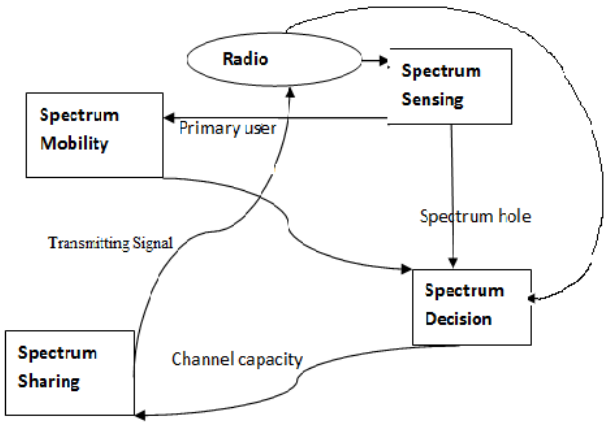


Figure 3

Primary user Emulation Attack:

The scheme is susceptible to spiteful attack that would disturb its process. One of the most common malicious attack is the primary user emulation attack (PUEA) in which an attacker occupies the idle frequency band(s) as the main user's sign so as to stop other less important users from accessing the matching white space(s). This leads to low range use and incompetent cognitive network process. In this attack, the attacker impersonates the primary user. The attacker tries to emulate the wireless signal characteristics of the primary user in his absence. The minor nodes require some way to differentiate the signal sent by the malicious PU emulator.

Proposed Algorithm Working Methodology

QED (Quad-type Encryption of Data) algorithm is improved version of DDOS (Distributed Denial of Services attacks). QED algorithms consider secure and energy implementation Three level hierarchy of QED:

Adaptive Distance Mechanism RSSI

Distributed Energy/Power

User's ID in Frame Format

The description level given below

Step 1: The data is encrypted using Distance as the key

Step 2: The result is encrypted using energy as its key

Step 3: Again the result is encrypted using user's ID as the key

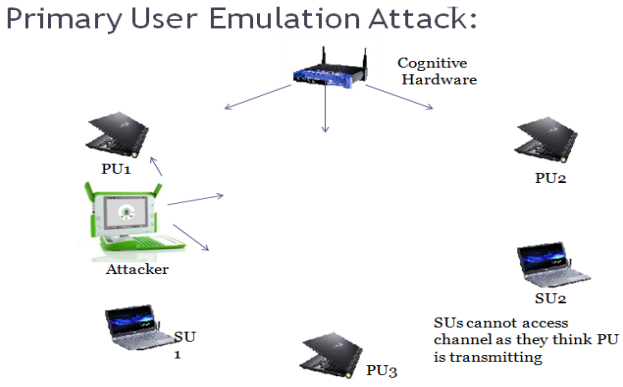


Figure 4

Flow execute of RSSI based PUE Attack

Step 1: RSSI based PU Localization

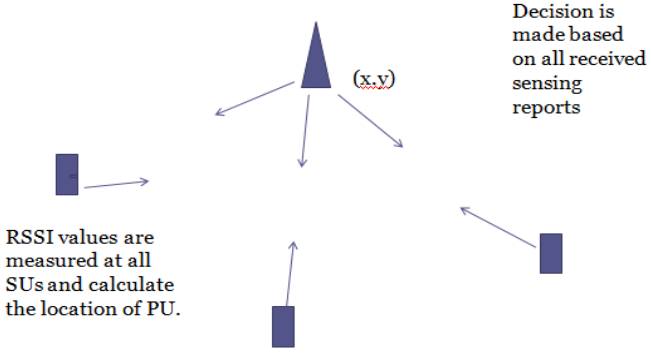


Figure 5

To determine the position of the transmitter, RSS values are needed. This PUEA create the call for safe exchange of information in order to avoid possible attacks, such as eavesdrop, insertion, alteration, or play repeat attack. Furthermore, it is also essential to keep the position of PUs secret as an assailant is conscious of it and could tactically select its broadcast place to outwit the confirmation scheme. [12]

RSSI Distance Formula

RSSI (dbm)=-[10×n×log(d)+A]

RSSI is the RSSI value received (dBm)

n is the path-loss exponent

d is the distance

A is the RSSI value at a reference distance (1m)

Distance = $10^{[(A+RSSI)/(10xn)])}$

Step 2: Energy Based PU Identification

To deal with PUEA, indication power level discovery is used in adding to localization of transmitters. This move toward is based on the next assumption: primary transmitters are users with a known site and show power. SUs are plans with limited broadcast power. As a result, energy level finding can positively be a robust measure to validate the genuineness of primary transmission. [12]

Step: 3 User ID Based Recognition

1. The CH consists a database of the users with their unique IDs, energy level and RSSI values
2. The users transmits their ID encrypted, which is recognised after decryption by the CH
3. Based on the ID, the CH classifies the PUs and SUs
4. In the future system, the main user generates a QED signal by performing encryption in 4 levels at the receipt end; the ID is regenerate for the discovery of the main user and hateful user.
5. Then, the energy and RSSI values are regenerated which are compared with the database to conclude the user as PU or SU.
6. Even if one of the parameters received doesn't match with the stored values, the user will not be allotted any bands

Dynamic Key

Active key are on one occasion symmetric cryptographic keys form a sequence of keys. The fourth level of encryption is performed by a randomly generated key. The dynamic key cryptography is one of the advanced techniques in cryptography where either a long message is divided into many parts or there are many message in both case each message is encrypted with the help of different parts of key i.e sub keys.[7]

STEPS FOR PROPOSED ALGORITHM

CR initialization step:

1: **for** each CR assign C_i **do**

2: /** PU initialize variable**/

3: PU ← CR_i; /**PU Primary Unit**/

4: SU←$CR_;$ /**SU Secondary Unit**/

5: H_o /**Multi Hop Sequences**/

Generation of Slot Position Vector v:

6: CRv ← ∂; /**Vector In CR**/

7: **if** receives a ACK message PU=< H_o,CR_i,H_o >

From node CR **then**

CRC Calculation

8: /**Hardware Initialization **/

9: **if** ENC y < CR and H_o>PU, SU **then**

10: /** where D is Distance, E (Energy) **/

11: CR_i←PU

12: CR_j ←SU

13: **Spectrum Allocation in Map Reduce**

14: construct a new ACK message 'CR' =< PU_i,SU_j,H_o >;

15: send 'Secure Data' to its neighbors;

16**: end if**

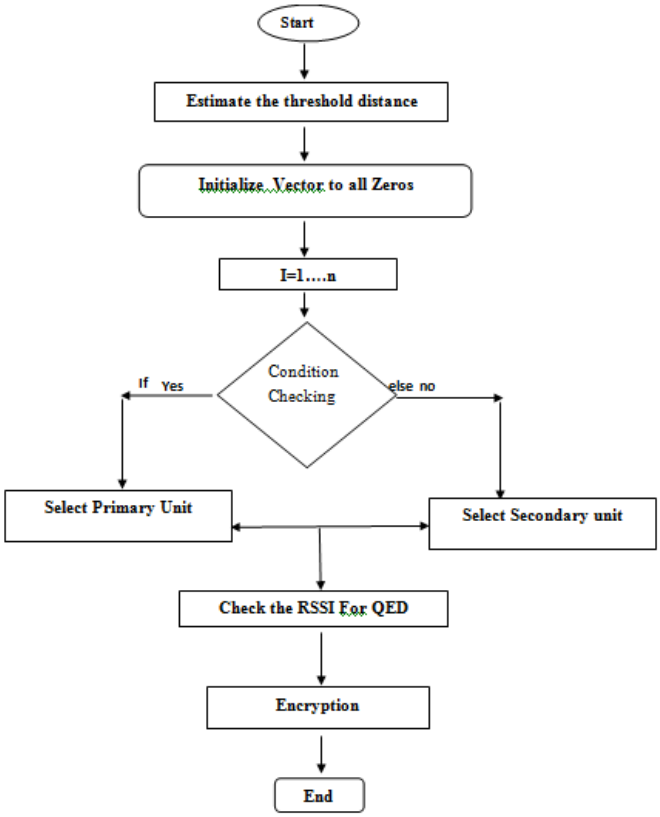
17**: end if**

Hardware Bench Setup Establishment

ARM7- LPC2148

Xbee RF module

FLOW CHART



ARM7- LPC2148

The LPC2148 microcontroller is base on a 32 bit ARM7TDMI-S CPU by means of concurrent emulation and entrenched draw hold up, that combine the microcontroller with entrenched far above the ground hurry flash reminiscence of 512KB. For dangerous system size application, the choice 16-bit Thumb form reduce code by additional than 30 % with negligible performance punishment. Due to their tiny size and low power use, LPC2148 are ideal for application where smallness is a key obligation, such as correct of admission manage and point-of-sale. A mix jointly of serial infrastructure border range from a USB 2.0 Full pace machine, multiple UARTS, SPI, SSP to I2Cs and on-chip SRAM of 8 KB up to 40 KB, create these tactics very well right for message gateways and procedure converters, soft modems, voice credit and low end imaging, as long as both large buffer size and high indulgence power.

ARM (Advanced Risk Machines) Features

1. Two 32-bit timers/external occasion counter (with four imprison and four evaluate channels each), PWM component (six outputs) and supervisory body.
2. Multiple serial interface counting two UARTs, two Fast I2C-bus (400 kbit/s), SPI and SSP with buffer and changeable data distance end to end capabilities.
3. Up to 45 of 5 V tolerant fast universal reasons I/O pins in a minute LQFP64 package.
4. On-chip included oscillator operates with an outside gemstone in range from 1 MHz to30 MHz and by means of an outside oscillator up to 50 MHz.
5. Power economy modes comprise idle and Power-down.
6. Solitary authority provide break off with Power-On rearrange (POR) and BOD circuits: CPU in force voltage variety.

Advanced Xbee Series Module

The Xbee RF unit were engineered to meet IEEE 802.15.4 Principles hold up the sole wants of low-cost, low-power wireless antenna network. The unit need insignificant power and provide consistent release of information flank by plans. The module purpose inside the ISM 2.4 GHz incidence band and are pin-for-pin well-matched with each other. The XBee radios can be used with the smallest number of quantity number of relations: power (3.3 V), ground, data in and data out through UART, and optional lines being Reset and Sleep.

SOFTWARE REQUIRED

- **Keil uvision and real view compiler**
- **X-CTU**

XCTU

I. After that age group pattern stage for XBEE/RF answer.

II. XCTU is a free, multi-platform request compatible with Windows, MacOS and Linux

III. Graphical system View for straightforward wireless system pattern and architecture

IV. API Frame Builder is an easy growth tool for rapidly structure XBee API frame.

V. XCTU include all of the gear a developer wants to rapidly get up and organization with XBee.

VI. Sole skin like graphical system view, which graphically represent the XBee system the length of with the sign power of each link, and the XBee API border designer, which instinctively help to construct and understand API frame for XBees life form used in API mode, unite to make growth on the XBee stage easier than ever.

FEATURE OF XCTU

- You can run and arrange manifold RF plans, still distantly (over-the-air) linked devices.

- The firmware informs procedure flawlessly restore your unit settings, mechanically treatment mode and baud speed changes.
- Two exact API and AT console, have been intended from scrape to converse with your means of communication plans.
- You can now save your cheer up session and weight them in a dissimilar PC organization XCTU.
- XCTU include a set of entrenched gear so as to can be execute with no have any RF unit linked:
    - Frames producer: Easily make any type of API border to save its value.
    - Frames predictor: Decode an API frame and see its exact border principles.
    - Recovery: get well radio module which have damaged firmware or are in indoctrination form.
    - Load cheer up sitting: Load a cheer up session saves in any PC organization XCTU.
    - Variety test: do a range test flanked by 2 radio modules of the same network.
    - Firmware traveler: find the way through XCTU's firmware records.
- An update procedure allows you to mechanically update the request itself and the radio firmware records without need to download any extra records.

SIMULATION RESULTS

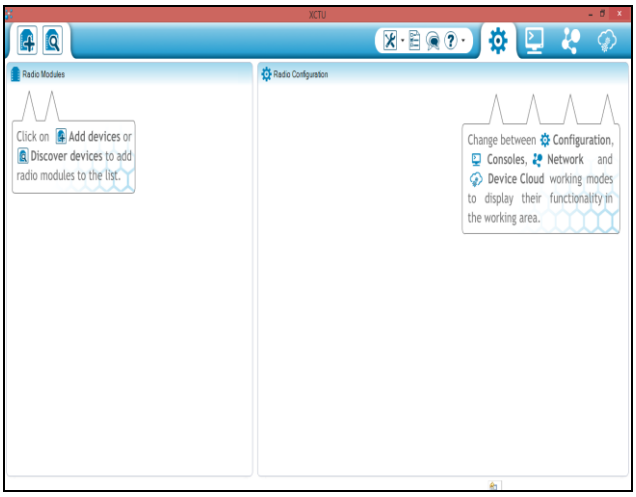


Figure 6: X-Ctu Software

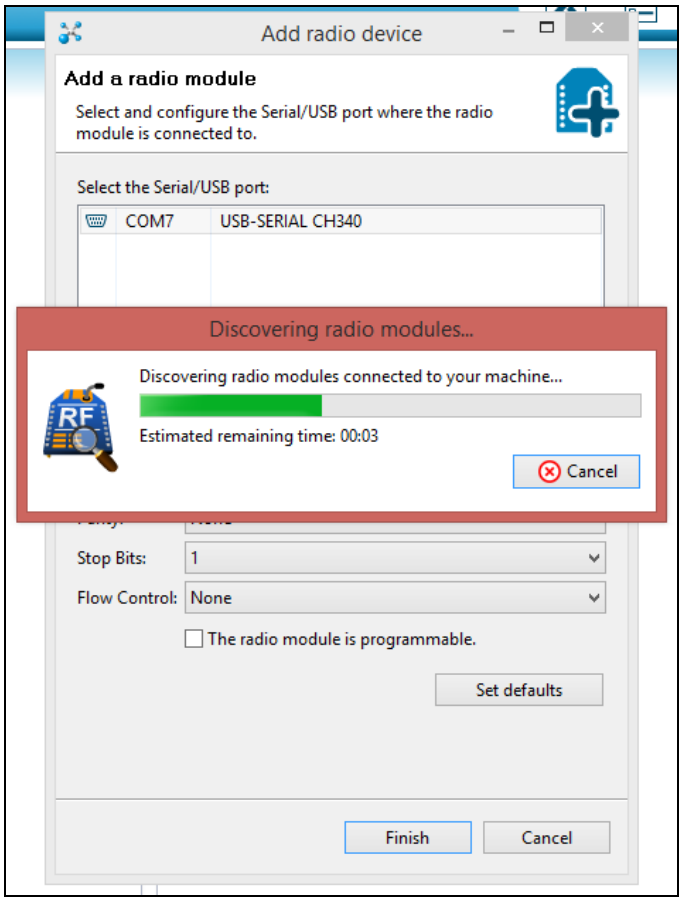


Figure 7: Discovering Radio Modules

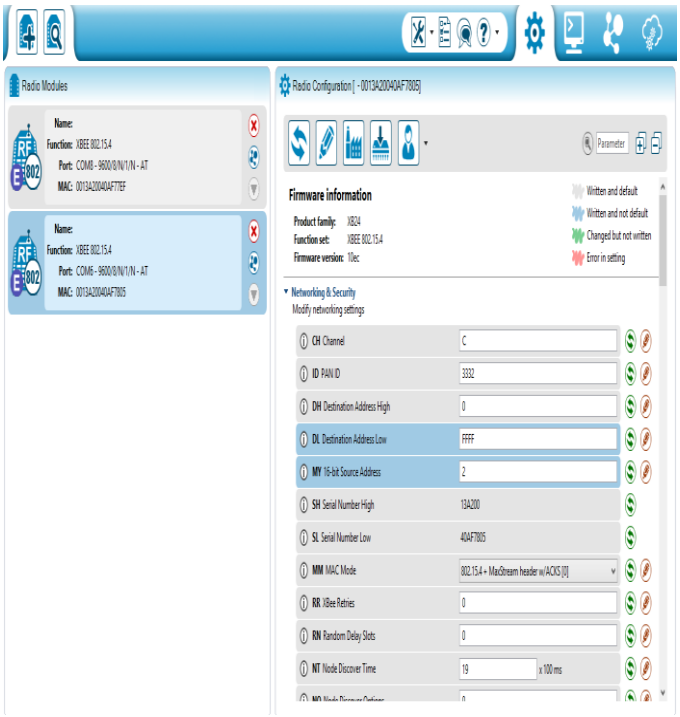


Figure 8: Modules of discovered modules in X-CTU

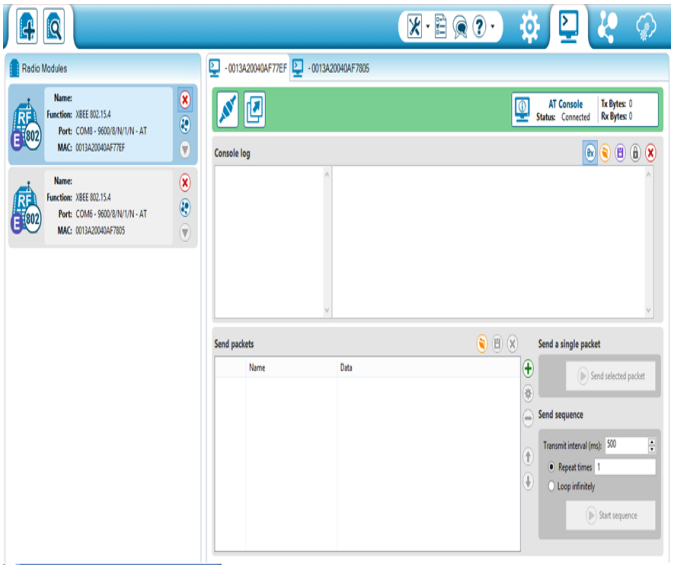


Figure 9: X-CTU for PUE

ATTENTION Commands for Xbee Configuration

1. X-CTU software is second-hand to border with and arrange Xbee Modules
2. Send a '+++' sequence to enable AT command mode.
3. The module should respond with 'OK'.
4. Then send a command 'ATDB'.
5. DB limit is used to read the inward signal power (in dBm) of the last RF packet received.

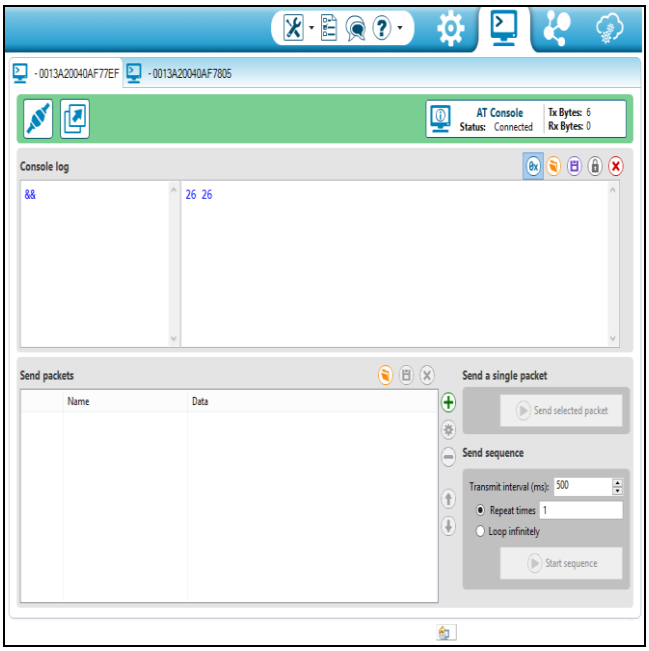


Figure 10: To Detect RSSI Mechanism

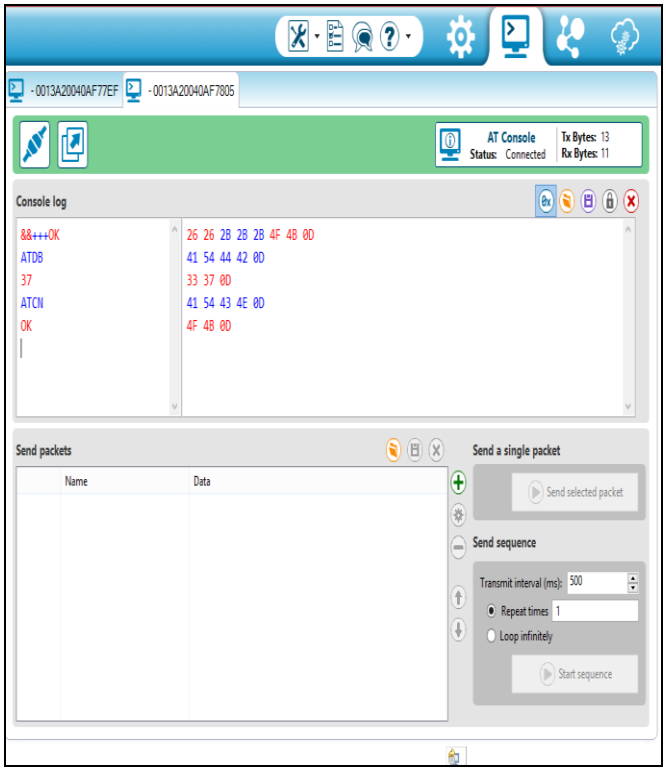


Figure 11: Final Result of Adaptable Encryption

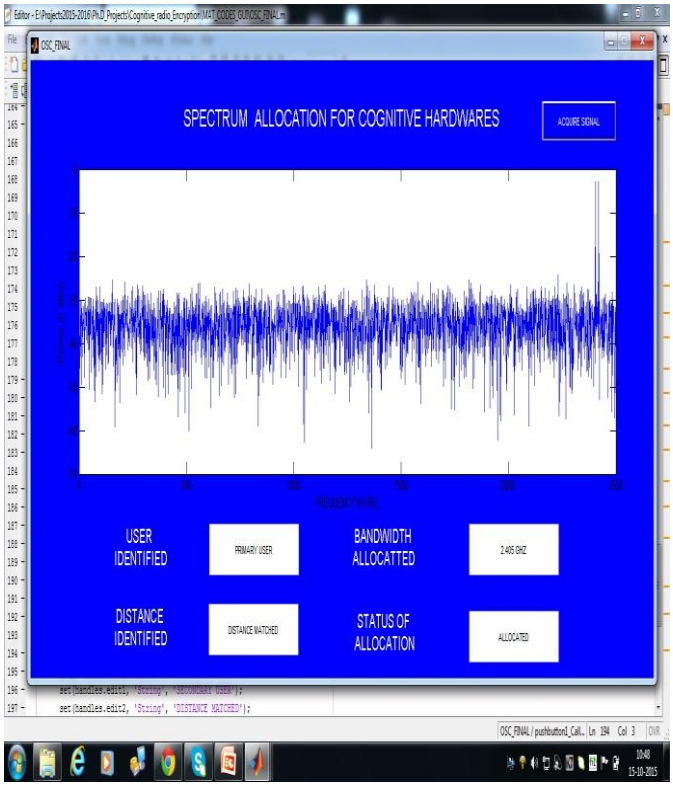


Figure 12: Final Encryption Result for Bandwidth allocation

CONCLUSION

We proposed an analytical and experimental model using QED and RSSI mechanism in cognitive radio networks. Thus the QED algorithm combats main user emulation attacks, and enables more robust scheme process and efficient spectrum contribution. An Attack Model against the approaches using RSSI and Energy is proposed and simulated A Novel approach to mitigate PUEA is proposed using QED.

REFERENCES

[1] Z. Jin, S. Anand, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks" Department of Electrical and Computer Engineering

[2] Sugata Sanyal "Safe message in Cognitive Radio network" 2009 International Conference on Computers and Devices for Communication

[3] T. Charles "Safety in Cognitive Radio Networks Threats and Mitigation", Electrical and Computer Engineering, University of Maryland, College Park.

[4] J. Mitola and G. Maguire, "Cognitive radio: Making software radios more personal," IEEE Personal Communications, vol. 6, Aug. 1999.

[5] S. Haykin, "Cognitive radio: Brain empowered wireless communications," IEEE Journa. on Selected Areas in Commn., vol. 23, no. 2, pp. 201–220,Feb. 2005

[6] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "Next generation/ dynamic spectrum access/cognitive radio: A survey," Elsevier Journal on Computer Networks, vol. 50, pp. 2127–2158, May 2006.

[7] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of TV transmission in support of dynamic spectrum sharing," Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2005, pp. 338–345, Nov. 2005.

[8] G. Jakimoski and K. P. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks," IEEE CogNets Workshop, IEEE International Conference on Communications 2008, May. 2008.

[9] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," Proc., IEEE Workshop on Networking Tech. for Software Defined Radio Networks (SDR) 2006, pp. 110– 119, Sep. 2006.

[10] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Jl. on Sel. Areas in Commn.: Spl. Issue on Cognitive Radio Theory and Applns, vol. 26, no. 1, pp. 25–37, Jan. 2008

[11] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," To appear in Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2008, Oct. 2008.

[12] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," Proc., IEEE Conference on Computer Communication (INFOCOM) 2008 mini-conference, Apr. 2008.

[13] T. S. Rappaport, "Wireless Communications: Principles and Practice", Prentice Hall Inc., New Jersey, 1996.