International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 2, March - April 2017 **ISSN 2278-6856**

Primary User Emulation Attack (PUEA) Analysis in Cognitive Radio Network

P.S Dinesh1, S. Dinesh 2, S. Tephillah 3 , A.M. Balamurugan4

[1] UG scholar, St.Joseph's College of Engineering, Electronic and communication, OMR, Chennai-119, India

[2] UG scholar, St.Joseph's College of Engineering, Electronics and communication, OMR, Chennai-119, India

[3] Associate professor, St.Joseph's Institute of Technology, Department of ECE, OMR, Chennai-119, India

[4] Associate professor, St.Joseph's College of Engineering, Department of ECE, OMR, Chennai-119, India

Abstract

With the progression in wireless networking, there is an escalating problem of spectrum scarcity. To resolve this issue, a technology called Cognitive Radio (CR) was introduced, in which the secondary users can sense the spectrum and use the licensed bands when the spectrum is not being used by the primary user. So, spectrum sensing is the essential mechanism on which the entire communication depends. If the spectrum sensing result is disrupted, the entire networks activities will be breached. Because of its wireless nature, there are various security threats specific to CR, which these networks are susceptible to. One of the most overriding threats among these is the Primary User Emulation Attack (PUEA).It is an acute threat in physical layer of CR network in which a malicious secondary user exploits the spectrum access etiquette by mimicking the spectral characteristics of a primary user. In this paper, we propose different frameworks to secure CR networks against PUEA to capitulate better results than existing techniques.

1. Introduction

Since spectrum scarcity has become a major concern, with the help of rapid proliferation of new technologies and services in the wireless domain cognitive radio networks have became a solution to it. Cognitive radios have enabled the opportunity to transmit in several licensed bands without causing harmful interference to licensed users. Due to these unique characteristics of CR and unreliable nature of wireless communication channel, cognitive radio networks (CRNs) acquire many research confronts, especially in aspects of security.

"A radio network that can change its transmitter parameters based on transmitted signal interaction with the environment it operates is called a cognitive radio network" [1]. The target of a CR is to seek for transmission opportunities in the white spaces RF stimuli and choose the optimal one, in terms of maximizing several spectrum decision, spectrum sensing ,efficacy functions such as users' throughput, fairness, etc., while instigating no or minutest interference to primary users.

In general, users are divided into two categories: (i) **Primary** or incumbent users that hold a license for a specific portion that use parts of the spectrum in an opportunistic

2. SECURITY ATTACKS AND VULNERABILITIES

Security threats are mainly related to two vital characteristics of cognitive radios: cognitive competence and reconfigurability. Threats related to the cognitive competence include attacks launched by adversaries that mimic primary transmitters, and transmission of deceptive observations related to spectrum sensing. Reconfiguration can be exploited by attackers through the use of malicious code installed in cognitive radios. Because of the wireless nature of cognitive radio, they face all classic threats present in the traditional wireless networks.

The dynamic spectrum allocation aids the secondary usage of licensed band. The licensed band must be carefully utilized by the Secondary User (SU) in order to avoid interference with the Primary User (PU)[2]. Based on the behavior of the protocol stack various attacks are categorized as follows.

The primary user emulation attack (PUEA)[3] is occurs in the physical layer, in which the PU signal characteristics are mimicked by the malicious user (MU) therefore the SUs may think the MU as the PU. The CR cannot adapt to the changing environment when the utility resource parameters are modified, thus causes the objective function attack (OFA). These attacks maybe malicious or obstructive attack and selfish or greedy attack. In the case of malicious attack ,the attacker only launches PUEA on the spectrum band whereas in greedy attack, the attacker reserves the bands for its own profit and prevents other SUs from using the idle spectrum band by launching PUEA.

In the link layer data transfer takes place from one node to another which results in three types of attacks such as spectrum sensing data falsification (SSDF) or the byzantine attack in which because of the wrong spectrum

sensing results the fusion centers decision is falsified. The malicious user can change the route information of the node by providing wrong information about the node called the selfish channel negotiation (SCN). The control channel is reserved by the attackers and is saturated such attack is called the Control channel saturation Denial-of-service (DoS)

The network layer attacks are sink hole and hello flood. In sink hole attack the attacker mocks itself as the best route and pulls the neighbours to use this route to forward the packets and to discards those packets. In the hello flood attack the attackers uses enough power and sends broadcasting signals to all the nodes in the network to convince them that it is the closest neighbour.

The most significant attack in transport layer is the LION attack. In LION attack, it uses the PUEA to interrupt transmission control protocol (TCP) connection. It is said to be a transport layer pointed cross layer attack where emulating a licensed transmission will force a CRN to achieve a frequency handoffs and thus degrading TCP performance.

Since all the layers are unified the attacks occurring in other layers may cause adverse effect on the application layer.

3. SECURITY SOLUTIONS

The essential security features used to resolve the various threats available in the different layers of the cognitive radio network are confidentiality, authentication and integrity.

Confidentiality is the major attribute of cryptography, it is attained by encrypting and decrypting the data thus providing more security, this technology is termed as Ciphering. Classical cryptography and Modern cryptography are the two kinds of cryptography. In classical cryptography the codes and cipher are used for encipherment and decipherment. Historically, cryptography was split into a dichotomy of codes and ciphers. However, by using codes there is variety of drawbacks, including susceptibility to cryptanalysis and there is difficulty of managing a cumbersome codebook. So, the usage of codes has fallen into disuse in modern cryptography, and ciphers are the dominant technique. Whereas in Modern cryptography, by the type of the key and by type of input data are the two criteria in which it is classified. By type of key used, the ciphers are divided into symmetric key algorithms (Secret- key cryptography), where the same key is used for cryptography and asymmetric key algorithms (Public-key cryptography), where two different keys are used for cryptography. There are different algorithms used in both type of cryptographies. In a symmetric key algorithm the sender and receiver uses the same key and the key is kept forbidden from the end users. Some of the popular algorithms are DES and AES algorithms. Where, in an asymmetric key algorithm two separate keys i) A public key is published and enables any sender to perform encryption and ii) A private key is kept secret by the receiver and enables only him to perform correct decryption. The widely used asymmetric key algorithm is RSA. Moreover Ciphers can be distinguished into two types by the type of input data they are Block ciphers, which encrypt block of data of fixed size, and Stream ciphers, which encrypt continuous streams of data.

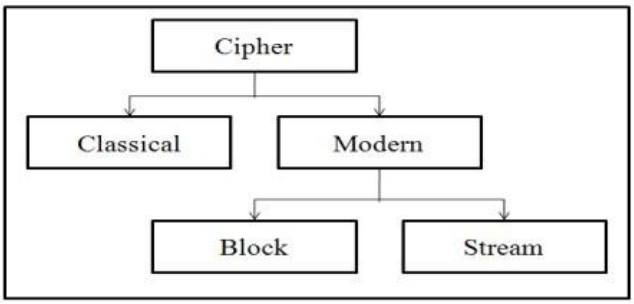

Figure-1 Classification of Cipher

Block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key. In the design of cryptographic protocols block ciphers are the important elementary components, which are widely used to implement encryption of bulk data. In block cipher for encryption it allows single data block of its cipher's block length. For a variable-length message, separate cipher blocks are used as it was done by partitioning the data. In this the message is split into separate blocks of the cipher's block size and then each block is encrypted and decrypted independently. If we use the block cipher in cognitive radio networking the block cipher will produce a key which can be easily hacked so, the security in code transferring is at high danger. Hence this method is generally insecure because equal plain text blocks will always generate equal cipher text
blocks (for the same key), so patterns in the plain text message become evident in the cipher text output.

To overcome this limitation, several block cipher modes of operation have been designed for encryption. To add security, the initialization vector passed along with the plaintext message must be a pseudo-random value, which is added in an elite manner to the first plaintext block before it is being encrypted. The resultant cipher text block is then used as the new initialization vector for the next plaintext block. AES algorithm is most preferred algorithm in the block cipher than DES.

AES algorithm:

AES is a substitution-permutation network based design principle. It uses the same key for both encrypting and

decrypting. It can have the key size of 128, 192, or 256 bits. The key size used for an AES cipher converts the input into the final output, called the cipher text by specifying the number of repetitions of transformation rounds. The number of cycles of repetition for 128-bit keys is of 10 cycles of repetition, for 192-bit keys it is of 12 cycles of repetition, for 256-bit keys it is of 14 cycles of repetition. Even though there are more cycles of repetition the overall time taking place in the ciphering the text is longer so to overcome delay time and to overcome the use of same key which can be easily traced out by common user the stream ciphers are used. There are many disadvantages of block cipher such as it is easy to insert or delete blocks. In block cipher to be easily modified by the common user identical block of plain text yield identical blocks of cipher text. To overcome all this disadvantages Stream Cipher is preferred instead of Block Cipher[4].

Stream Cipher:

Stream cipher is of a symmetric key cipher and each plaintext digit is encrypted one at a time to produce the cipher output. An alternate name for the stream cipher is state cipher, as each digit data encryption is dependent on the current state only, by encrypting each digit the security is added and the time for processing is minimized. Stream ciphers typically execute at a higher speed than block ciphers and have lower hardware complexity.

While encrypting in the block cipher if there is mess up in one part of the data the rest of the data is unrecoverable so by using stream cipher the each burst is encrypted as the stream of the burst data which requires less process time and adds more security to the data. Stream ciphers are finest in network streams where the amount of data is either unknown, or continuous[5][6].

Stream ciphers are really suitable for hard ware implementation that uses one bit data at a time for the encryption and the decryption. Stream cipher is less than to vulnerable to insertion or deletion of block. It can be mathematically analyzed easily. The key in the stream cipher is generated independently of the message stream. Thus Stream cipher is well suited for networking compared to the block cipher.

In data networks, authentication is done using RC4 and the symmetric key for the stream cipher is generated using the Pseudo Random Key Generation.

The already recommended algorithm is of AES which has some sort of disabilities which have been discussed above so, to overcome the AES disadvantages[7], the RC4 algorithm is recommended for the secure cognitive radio network and the key generation for the ciphering is done with Pseudo Random Key Generation[8].

way, so as not to cause harmful interference to PUs (ii) In cognitive radio network, SUs or **Secondary** users (without license) are allowed to access the licensed spectrum if primary users (having license) are not present.

Cognitive Radios have to vacate the specific spectrum band, whenever a primary signal is detected. The main functionalities of CR networks are spectrum sensing, spectrum mobility, spectrum sharing and spectrum management. The cognitive cycle comprises of the following mechanisms:

Spectrum Sensing is one of the most significant components of a CR and it performs the detection of incumbent signals. There are two types of spectrum sensing (i) fast sensing, i.e.1ms/channel, and (ii) fine sensing, which is determined dynamically by the BS, dependent on the fast sensing result, and senses the spectrum more precisely. The BS collects the observations made by SUs and makes the final decision about the presence or absence of incumbent signals. Energy detection approach is used by IEEE 802.22 to sense an incumbent signal because of the simplicity and low computational overhead of this technique. Other than energy detection, there are various other methods such as cyclostationary based sensing, waveform based sensing, matched filtering and radio identification based sensing.

Spectrum Analysis is a process is based on the available information of spectrum holes from spectrum sensing. It analyzes various channel and network features such as capacity, bit error rate, delay, etc for each spectrum hole and later provides this analysis to the spectrum decision process.

Spectrum Decision process selects the best spectrum hole for transmission. This method can be the result of various cooperating cognitive radios or can be performed by a single cognitive radio.

Rivest Cipher 4:

In 1987 RC4 stream cipher was designed by Ron Rivest. It is legitimately termed as "Rivest Cipher 4". For real time processing stream ciphers are the most efficient. In stream cipher the key size is variable with byte oriented operations. This algorithm is based on the use of a random permutation[10]. According to the various analyses, the cipher run very quickly in software because eight to sixteen machine operations are required per output byte. The algorithm is simple, fast and easy to explain. It can be efficiently implemented in both software and hardware .

In Cognitive Radio Networks for providing the security the stream cipher is used which works on the RC4 algorithm. In cryptography, the most widely used cipher having remarkable simplicity and speed of processing is RC4 it may also be known as ARC4 meaning Alleged RC4. The key generation is by using pseudo random key generation, thus authenticated[9][10].

Following confidentiality and Authentication the next major domain is Integrity. Integrity is the ability to prevent an active attacker to modify the information without the end users notice. When the information is getting modified, its invalidity is proved. Certain algorithms have been emphasized to prove integrity. The two popular algorithms are SHA-0 and SHA-1[11].Though these algorithms have certain special features but these algorithms are more prone to linear and nonlinear attacks. SHA-2 algorithm has been lighted to prevent these attacks. The performance of SHA-2 is better secured when compared with SHA-1. Though SHA-1is analyzed and carved only after MD4, it creates a hash which has a length of 160 bits instead of 128 bits.SHA-2 is classified into four different types, known as SHA-224,SHA-256, SHA-384, and SHA-512.SHA 2 algorithm has overcome the drawbacks in SHA-0 and SHA-
1 algorithm. The SHA-2 algorithm has led to 24 step attacks against SHA 256 and SHA 512 for making the CRN secured from these attacks. Despite SHA 512 making it compatible, there are certain compression features that make it open for
attacks.

Table-1 Comparison of various integrity algorithms

Characteristics	MD5	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Block size	512	512	512	512	1024	1024
Message digest size	128	160	224	256	384	512
No. of rounds	64	80	64	64	80	80

4. Proposed security frameworks for PUEA attacks:

In the first proposed method which is shown in figure-2 authentication code which is to be transmitted to secondary user is given as an input to the key stream generator through which an secured key stream is obtained. This key stream is embedded along with the authentication code and provided to the legitimate secondary user.

Whereas, at the receiver end, if the secondary user is legitimate then the authentication code and the key stream is estranged. From which the key stream is generated using authentication code .If the both the key stream are identical then the primary user is legitimate else malicious.

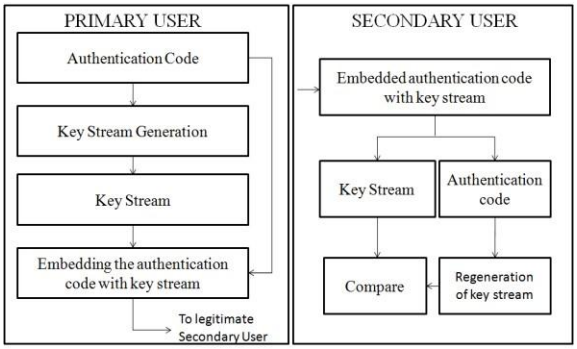

Figure- 2 Proposed Framework 1

The second framework is revealed in the figure- 3 in which the seed is used to generate the digest using hash algorithm. Further the seed is combined with the digest using logical operation and finally encrypting it before passing it on to the secondary user.

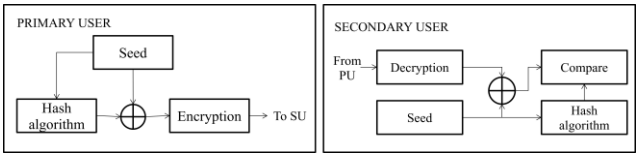

Figure- 3 Proposed Framework 2

The yield from the primary user is decrypted and a logical operation is performed with the seed to obtain the transmitted digest, which is compared with the digest generated from the hash algorithm at the secondary user. The secondary user has to abandon the spectrum if both the digest are alike.

5. Conclusion

Cognitive radio is one the intelligent network that is autonomously and dynamically adapts its operation from the previous experience. This paper highlights the advantages of CR in the aspects of spectrum sharing and the security vulnerabilities associated with CR. The paper mainly focuses the PUEA. The proposed frameworks give the better security solutions against PUEA in CR. In the future better security algorithms have been chosen for our proposed frameworks that it will be suitable for real time scenarios in cognitive radio networks.

References

[1] Alexandros G. Fragkiadakis, Elias Z. Tragos and Ioannis G. Askoxylakis "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks" IEEE communications surveys & tutorials, Vol. 15,No. 1,2013.

[2] L. B. Wang and K. J. Ray Liu, "Advances in Cognitive Radio Networks: A Survey," IEEE Journal of Selected Topics in Signal Processing, Vol. 5, No. 1,2011, pp. 5- 23.

[3] A.C. Sumathi , R. Vidhyapriya and C. Kiruthika, "A Proactive Elimination of Primary User Emulation

Attack in Cognitive Radio Networks Using Intense Explore Algorithm", International Conference on Computer Communication and Informatics (ICCCI -2015), Jan. 08 – 10, 2015.

[4] Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, and Tongtong Li" ,"Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard", in proc IEEE Transactions on Information Forensics and Security, vol. 9, no. 5, MAY 2014.

[5] Elminaam Diaa Salama Abdual, Kader Hatem Mohamed Abdual & Hadhoud Mohiy Mohamed 2008, 'Performance Evaluation of Symmetric Encryption Algorithms', IJCSNS International Journal of Computer Science and Network Security, vol.8, no.12, pp. 280-286.

[6] Elminaam Diaa Salama Abdual, Kader Hatem Mohamed Abdual & Hadhoud Mohiy Mohamed, 2010, 'Evaluating the Performance of Symmetric Encryption Algorithms', International Journal of Network Security, vol.10, no.3, pp.213-219.

[7] Nidhi Singhal & Raina JPS 2011, 'Comparative Analysis of AES and RC4 Algorithms for Better Utilization', International Journal of Computer Trends and Technology, pp. 177-181.

[8] Paul, S & Preneel, B 2004, 'A new weakness in the RC4 key stream generator and an approach to improve the security of the cipher', Fast Software Encryption, Lecture Notes in Computer Science, vol. 3017, pp.245-259.

[9] Mousa, A & Hamad, A2006, 'Evaluation of the RC4 algorithm for data encryption', International Journal of Computer Science and Applications, vol. 3, no. 2, pp. 44-56.

[10] Balamurugan, AM, Sivasubramanian, A & Parvathavarthini, B 2016, "Secured Hash Based Burst header Authentication Design for Optical Burst Switched Networks" Journal of Optical Communications. ISSN (Online) 2191-6322, ISSN (Print) 0173-4911, DOI: 10.1515/joc-2015-0097, July

[11] S.V.Vidhya Harini and Dr.Mrs.T.Aruna "A Mitigation Strategy for Primary User Emulation Attacks in Cognitive Radio Networks" Intelligent Systems and Control (ISCO), 2016 10th International Conference 2016

[12] Kapil M. Borle, Biao Chen, and Wenliang (Kevin) Du Physical Layer Spectrum Usage Authentication in Cognitive Radio: Analysis and Implementation IEEE Transactions on information forensics and security,Vol.10,No,10,October 2015

[13] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in Proc. IEEE ICASSP, May 2013, pp.2935–2939.

[14] Elham Hosseini, Abolfazl Falahati "Transmission over Cognitive Radio Channel with Novel Secure LT Code" Communications and Network, 2013, 5, 198-203

AUTHOR

P.S Dinesh is pursuing his Bachelor's degree in Electronics and Communication from St.Joseph's College of Engineering, Anna University, Chennai-600025.

S. Dinesh is pursuing his Bachelor's degree in Electronics and Communication from St.Joseph's College of Engineering, Anna University, Chennai-600025.

S.Tephillah is a Research Scholar and pursuing a Doctoral Degree in Information & Communication Engineering at the Department of Electronics and Communication Engineering at Anna University, Chennai-600025, India. She Received her B.E in Electronics and Communication Engineering (2003) from Madras University, Chennai, Tamilnadu, India. She received her M.E in Applied Electronics (2006) from Anna University, Chennai, Tamilnadu. She has 8 years of experience in teaching and guiding projects for undergraduate and postgraduate students. Her research area is Security issues in Cognitive radio networks.

Dr. A.M.Balamurugan has received B.E. degree in ECE from Madurai Kamaraj University, Madurai, 2002and M.E. in Digital Communication and Network Engineering 2005 from Anna University, Chennai and Ph.D degree in Optical Communication Networks from Anna University Chennai in 2016. Currently he is working as an Associate Professor, in the department of Electronics and communication engineering at St. Joseph's College of Engineering, Chennai, India. He has 13 years of experience in teaching and guiding projects for undergraduate and postgraduate students. He has added 13 international and national publications to his credit. His areas of interests include optical communication, optical networks, network security, Wireless sensor and computer networks..