

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Reduction Mechanism of Eavesdropping Attack in Cognitive Radio Network

A. KARTHIK SAGAR N. NARESH

Electronics and Communication Engineering Dept,

TKR College of Engineering and Technology, Hyderabad, Telangana, India

Abstract- *In the last decade, cognitive radio (CR) has emerged as a major next generation wireless networking technology, which is the most promising candidate solution to solve the spectrum scarcity and improve the spectrum utilization. However there are some security issues and layered attacks encounter in these networks through some malicious nodes and Eavesdropping attacks that provide insecure communication between and data loss between two ends of the system So in order to defend this mechanism we have to design an Encryption and Decryption algorithm that protects the data from these eavesdropper attacks by using some key generation technique that uses both private and public key using Cryptographic research methodology.*

KeyWords: *Cognitive Radio Network (CRN), Eaves Dropping attack, Symmetric Key Cryptography, Asymmetric Key Cryptography, Secret Key, Public Key.*

1. INTRODUCTION

Cognitive radio network is a data communication network, which consist of intelligent devices. Intelligence means that they are aware of everything happening inside the device and in the network they are connected to. Using this awareness they can adjust their operation to match current and near future network conditions. 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 also improve radio operating behaviour. A novel idea was proposed by Mitola for the opportunistic use of the under-utilized portions of the spectrum, using novel devices called Cognitive Radios (CRs). When interconnected, CRs form Cognitive Radio Networks (CRNs). CRs are devices that are capable of sensing the spectrum and use its free portions in an opportunistic manner. The free

spectrum portions are referred to as “white spaces” or “spectrum holes”. A spectrum hole can be formally defined as a band of frequencies assigned to a primary user (PU), but, at a particular time and specific geographic location, the band is not being utilized by that user.

The issue of spectrum under-utilization in wire-less communication can be solved in a better way using Cognitive radio (CR) technology. Since Cognitive Radio Networks (CRN's) are basically wireless networks, they inherit most of the well-known security threats of wireless systems. The main objective of this project is to detect malicious nodes and provide secure transmission between two legitimate members of cognitive radio network. Cognitive Radio Technology is one of the strong candidate technology to solve the spectrum scarcity problems. In this project, there exists the problem of secure data transmission between the secondary user transmitter and a receiver in the presence of eavesdropper in cognitive radio network. A new model is proposed which combines various security parameters. There exist various security models in modern cryptography. However there still exist various security threats. A new model is proposed which overcomes various security active and passive attacks. This Method presents a symmetric and asymmetric key cryptography which uses both public key and private key.

The methodology of cryptography does not allow many people to actually understand the motivations in communication system. Cryptography methodology allows security at various level of network which focuses on basic attributes of information security i.e. confidentiality, integrity and availability. The reason that lacks the security are efficiency, fault-tolerance and security. Public shared symmetric key is used in symmetric/secret method where a common key is shared between the encryption and decryption mechanism. It includes Data Encryption standard(DES) ,3-DES, Advance encryption standard(AES) for encryption and decryption with different key lengths and ddepending

on the techniques various authentication protocols are evolved challenge response protocol, public key protocol, symmetric key protocol(which uses Kerberos distribution) and diffie Hellman key exchange protocol .Depending on the security levels various keys are used over network to increase the security level. Hence, different research that has done toward text encryption and decryption in the cipher text.

1.1 PROPOSAL SYSTEM

In the proposed technique, we are using encryption and decryption standard that uses both symmetric and asymmetric key cryptography with public key and private key. It uses the combination of both private and public key. The positive thing of our proposed algorithm is that it is very hard to break through encryption and decryption process without knowing the exact secret key.

2. MODULES USED

1. Plain Text, 2. Encryption Standard
3. Secret Key, 4. Cipher Text
5. Decryption standard, 6. Symmetric Key Cryptography
7. Asymmetric Key Cryptography

SOFTWARE USED

MATLAB

2.1 PLAIN TEXT

This is the original message or data that is fed into the algorithm as input. In cryptography data that can be read and understood without any special measures is called plaintext or clear text.

2.2 ENCRYPTION STANDARD

The method of covering up of plaintext in such a way as to hide its substance is called encryption. Encryption is a well-known technology for protecting sensitive data. The encryption algorithm performs various substitutions and transformations on the plaintext.

2.3 SECRET KEY

The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.

2.4 CIPHER TEXT

Encrypting plaintext results in unreadable data called cipher text. This is the scrambled message produced as output. It depends on the plaintext and the secret key. Thus, encryption is used to protect the information in hidden from anyone for whom it is not projected, even those who can see the encrypted data.

2.5 DECRYPTION STANDARD

The process of reversing cipher text to its original plain text is called decryption. This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key, and produces the original plaintext.

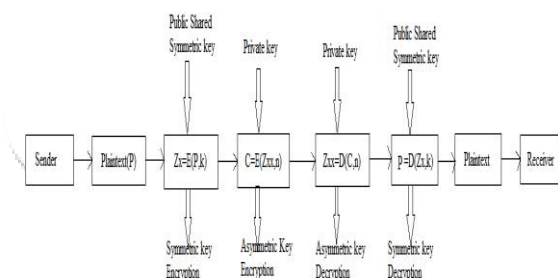
2.6 SYMMETRIC KEY CRYPTOGRAPHY

It uses a single key for both encryption and decryption. Same key is used both for the sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt that data. Because a single key is used for both functions, symmetric key cryptography is also called secret key cryptography.

2.7 ASYMMETRIC KEY CRYPTOGRAPHY

It uses one key for encryption and another for decryption. This cryptographic method makes use of two different algorithms for encryption and decryption respectively, a public key for encryption and a private key for decryption. The public key of the sender is used to encrypt the message by the sender. The receiver decrypts the cipher text with the help of a private key.

The proposed framework has focused on random combination of keys which is used for security enhancement.



Z=E-Encrypted message with public shared symmetric key
 C=E-Cipher text Encrypted with private key
 Z=C=Decrypted message with private key
 P=D-Plaintext decrypted with public shared symmetric key

Encryption and Decryption Algorithms to obtain Secure Communication

3. PROPOSED ENCRYPTION ALGORITHM

The step by step Encryption procedure is shown below

STEP1: Data is taken as input as plain text in the proposed algorithm.

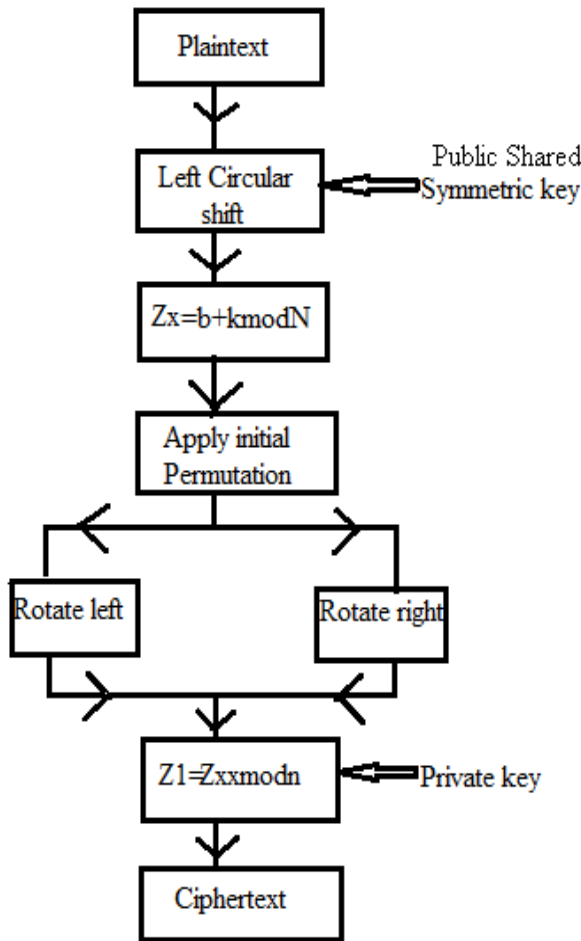
STEP2: Apply left circular shift on plain text.

STEP3: Then it is encrypted using symmetric key 'k' to produce Z1.

STEP4: Initial permutation is applied according to IP Values 2,6,3,1,4,8,5,7

STEP5: Divide it into two blocks and apply left shift on first block of data and apply right shift on the second block of data to produce Zxx.

STEP6: Cipher text is produced by applying application of asymmetric key 'n' on Zxx say Z1.



Proposed Encryption Algorithm

4. PROPOSED DECRYPTION ALGORITHM

The step by step Decryption procedure is shown below

STEP1: Cipher text is converted back to Zxx with the help of private key 'n' say Z11.

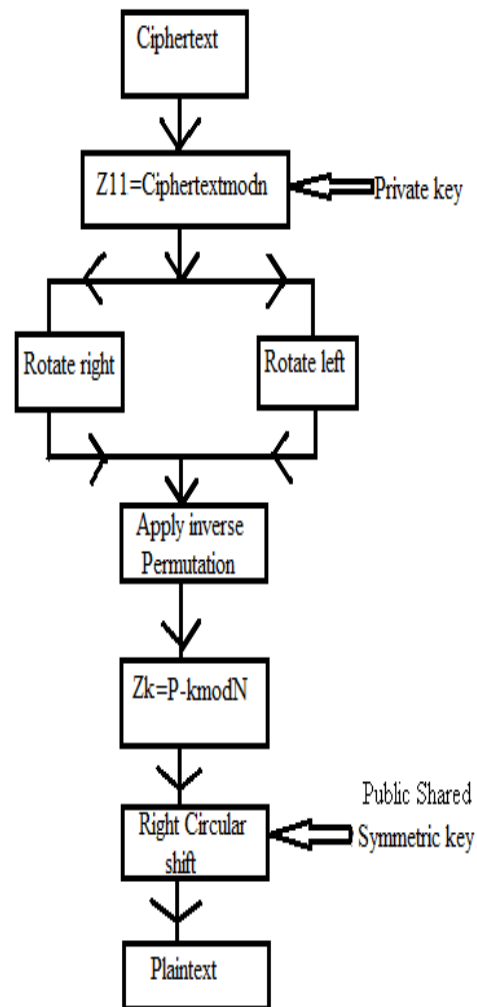
STEP2: Data Z11 is divided into two blocks and right shift is applied on first block and left shift is applied on second block.

STEP3: After then inverse permutation is applied according to values 4,1,3,5,7,2,8,6.

STEP4: Then it is decrypted using symmetric key 'k' to produce Zk.

STEP5: Apply right circular shift on data Zk.

STEP6: The resultant decrypted text is the plain text say P1



Proposed Decryption Algorithm

5. KEY GENERATION

Select two prime numbers such that p & q are kept confidential and $p \neq q$

$$n = p * q$$

$$\phi(n) = (p - 1)(q - 1)$$

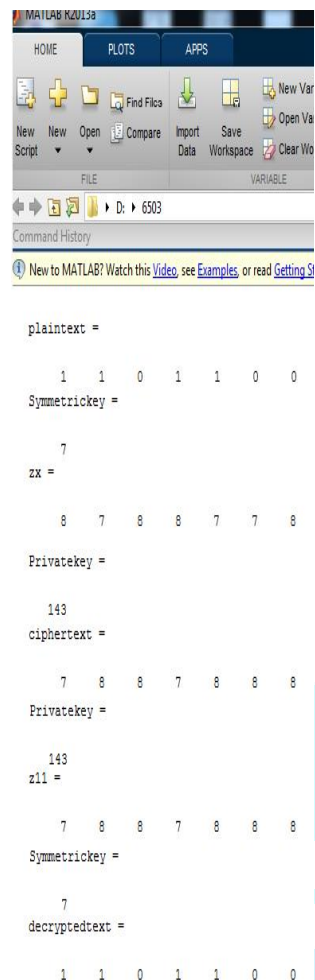
Select an integer e such that $\text{gcd}(e, \phi(n)) = 1$ & $1 < e < \phi(n)$

$k = \text{mod}(e, \phi(n))$ where k is the public shared symmetric key and n is the private key

Initial permutation values are 2,6,3,1,4,8,5,7

Inverse permutation values are 4,1,3,5,7,2,8,6

6. RESULT ANALYSIS



```

MATLAB R2018a
HOME PLOTS APPS
New Script New Open Compare Import Data Save Workspace Clear Workspace
Find Files New Variable Open Variable
FILE VARIABLE
D:\6503
Command History
New to MATLAB? Watch this Video, see Examples, or read Getting Started

plaintext =
    1    1    0    1    1    0    0
Symmetrickey =
    7
zx =
    8    7    8    8    7    7    8
Privatekey =
    143
ciphertext =
    7    8    8    7    8    8    8
Privatekey =
    143
z11 =
    7    8    8    7    8    8    8
Symmetrickey =
    7
decryptedtext =
    1    1    0    1    1    0    0
  
```

Result obtained through Proposed model

7. CONCLUSION

Cryptography is a particularly interesting field because of the amount of work done in secrecy. Regardless of the mathematical theory and statistical tools behind an algorithm, the best algorithms are those that are well-known, well documented and are also well-tested. Data Security is the most important aspect for any encryption and decryption algorithm. The positive thing of the proposed algorithm is that it is very hard to break through encryption and decryption process without knowing the exact secret key that is kept confidential throughout the algorithm. This algorithm describes the cryptographic concepts of symmetric key and asymmetric key encryption.

REFERENCES

[1]. Natasha Saini, Nitin Pandey & Ajeet Pal Singh International Conference on Communication and Signal Processing, April 6-8, 2016, India "Implementation of Security Model in Cognitive Networks."

[2]. IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 61, NO. 12,

DECEMBER 2013, "Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks."

[3]. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis

[4] Cryptographic Algorithms: Applications in Network Security Saurabh Sindhu Department of Computer Science, CRM Jat College, Hisar, Haryana, India Divya Sindhu Department of Computer Science, CRM Jat College, Hisar, Haryana, India.

[5] Ari Juels, RFID Security and Privacy: A Research Survey, IEEE journal, vol 24, No 2, february 2006.

AUTHORS BIODATA



A.KARTHIK SAGAR

received his B. Tech degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University in 2016 and he completed his M. Tech from Jawaharlal Nehru Technological University in 2018. He is presently working as Assistant Professor in TKR college of Engineering and Technology, HYD.



N.Naresh received his B. Tech degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University in 2011 and he completed his M.Tech in Communication Systems from Jawaharlal Nehru Technological University in 2014, currently he is working as Assistant professor in TKR College of engineering and technology, Hyd.