IJIREEICE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

NCIET- 2020

National Conference on Innovations in Engineering & Technology

Govt., Polytechnic College, Palakkad, Kerala

Vol. 8, Special Issue 1, February 2020

Dynamic Key Based Encryption Scheme in Wireless Communication System

Vismaya M[1], Job Chunkath[2]

Department of Electronics and Communication Engineering, Government Engineering College, Thrissur, India[1,2]

Abstract: Cryptography plays a key function in protecting data, integrity, and confidentiality in the data system. Mainly cryptography is classified as symmetric and asymmetric. The combination of both is known as sessional keys. The dynamic key has the advantage over the sessional key as the session duration problem will not be affecting it and there is no key exchange between the sender and receiver in each session. The dynamic key can be symmetric or asymmetric and the symmetric dynamic key is used in this project. The dynamic key-based phase and permutation encryption scheme are analyzed in 4G technology which uses an OFDM based communication system. The encryption is applied to post-IFFT in OFDM based 4G technology. Performance is analyzed in terms of BER of both dynamic key-based encryption scheme.

Keywords: OFDM, Dynamic Key, Permutation Encryption, Phase Encryption, BER.

I. INTRODUCTION

Cryptography plays a key function in securing data, integrity, and confidentiality. The word cryptography came from the ancient Greek words 'crypt' means 'hidden' and 'graphy' means 'writing'. Hence cryptography is the technique of securing the facts and communication device in which the usage of a few mathematical standards and set of rule-primarily based calculations known as algorithm unique messages or statistics are converted to another shape called encrypted data which can be decrypted at the receiver side the usage of the right decryption method. The key is a secret password that is used for encryption and decryption. There are two sorts of key in cryptography, symmetric and uneven keys. In symmetric-key cryptography, the keys can be equal on the sender and receiver aspect and it is the oldest and only form of encryption. The main disadvantage of symmetric key encryption is that they have to exchange the key between the sender and receiver. In asymmetric key cryptography, both the keys will be different and it is also known as public-key since anyone can send the message but they can be only decrypted by the one who is known as the receiver. The asymmetric key uses longer keys than the symmetric key cryptography to provide better security which causes slower encryption and decryption.

Session keys are the combination of these two keys wherein each session the keys will be changing and its performance depends on the session duration. Key exchange will be occurring in the session keys, hence degrades its security. For these demerits, there is a need for dynamic key encryption technique which is almost similar to session key but there will not be any key exchange. The system performance in terms of BER in the 4G system is analyzed. Dynamic phase and dynamic permutation encryptions are applied in the 4G OFDM system. Dynamic encryption schemes can be applied either post or pre IFFT. The key generation scheme for dynamic key includes 2 steps: Initial key generation and repeated key generation. In an initial key generation, the first set of N dynamic keys are generated and can be used for encryption and decryption process. The repeated key generation will be generated only if an attacker is trying to generate the dynamic keys or receiver itself is trying to generate the dynamic key for the second time. In such a case a new set of N dynamic keys will be generating and using that encryption or decryption will not be successfully occurred.

II. OFDM SYSTEM MODEL

4G is the fourth generation of broadband cellular network technology, succeeding 3G[11]. Even though the first-release Long Term Evolution (LTE) standard was commercially deployed in Oslo, Norway, and Stockholm, Sweden in 2009, and has since been deployed throughout most parts of the world, It has been debated whether first-release versions should be considered 4G LTE[11]. In 2005, OFDMA transmission technology is chosen as a candidate for the HSOPA downlink, later renamed 3GPP Long Term Evolution (LTE) air interface E-UTRA[11].

The system model of the OFDM transmitter is shown in Fig.1[1]. The input data is first split into Mxr data bits, upon which IFFT is applied and again converted back to the serial bitstream. Each r bit data is known as sub-channels in which they are orthogonal to each other. After converting back to serial data stream cyclic prefix is added to reduce the effect of ISI since it acts as a guard band. Then the data is converted to an analog signal which can be modulated with suitable modulation technique. Adequate power can also be allocated for the signal before transmission to reduce fading.

IJIREEICE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

NCIET- 2020

National Conference on Innovations in Engineering & Technology

Govt., Polytechnic College, Palakkad, Kerala

Vol. 8, Special Issue 1, February 2020

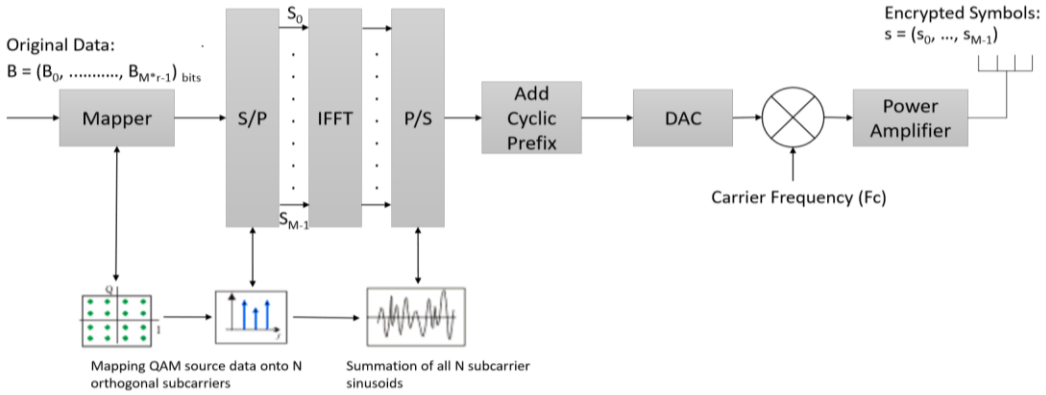

Fig. 1 OFDM Transmitter[1]

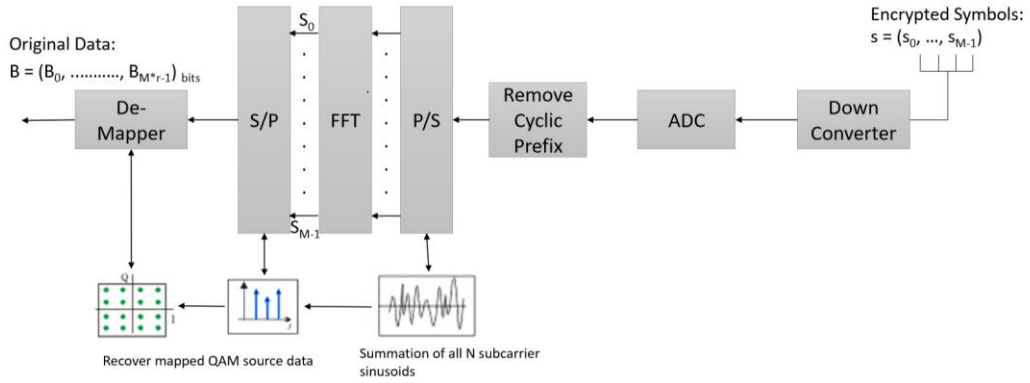

Fig. 2 OFDM Receiver[1]

The block diagram of the OFDM receiver is shown in Fig. 2. Here the received signal is demodulated, converted to the parallel data stream and FFT is applied to it. Then the signal is converted back to serial. For removing cyclic prefix, suitable equalization has to be done.

III. INITIAL DYNAMIC KEY GENERATION

The dynamic key generation process includes two steps: the initial dynamic key generation and the repeated dynamic key generation. The initial dynamic key generation can be divided into four following steps as in Fig. 3.

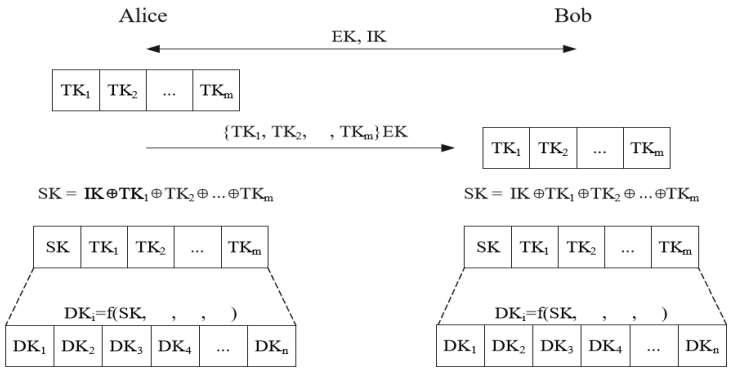

Fig. 3 Initial Dynamic Key Generation[10]

- Step 1: Alice and Bob alternate keys EK and IK via a secure channel[10].
- Step 2: Alice randomly generates m initial temporary keys $TK_1, \ldots, TK_m$ and sends the message to Bob, encrypted by using EK[10].

$$A \rightarrow B: \{TK_1, \ldots, TK_m\}EK, h\{TK_1 \oplus TK_2 \oplus \ldots \oplus TK_m \oplus EK\}$$

- Step 3: Both Alice and Bob compute a seed key SK from the initial key IK and the temporary keys $TK_1, \ldots, TK_m$ using bit-wise exclusive or operation[10]. $SK = IK \oplus TK_1 \oplus \ldots \oplus TK_m$

IJIREEICE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

NCIET- 2020

National Conference on Innovations in Engineering & Technology

Govt., Polytechnic College, Palakkad, Kerala

Vol. 8, Special Issue 1, February 2020

- Step 4: All the dynamic keys can be generated by using the below equation[10].

$$DK_1 = f(SK, TK_1 \ldots, TK_{m-1}, TK_m)$$
$$DK_2 = f(SK, TK_2 \ldots, TK_m, DK_1)$$
$$DK_3 = f(SK, TK_3 \ldots, DK_1, DK_2)$$
$$\ldots..$$
$$DK_n = f(SK, DK_{n-m} \ldots, DK_{n-2}, DK_{n-1})$$

IV. REPEATED DYNAMIC KEY GENERATION

Once the initial dynamic key generation process is executed then only the repeated dynamic key generation process will be processing, ie if the attacker tries to retrieve the dynamic key sequence. The steps for the repeated dynamic key generation are listed below.

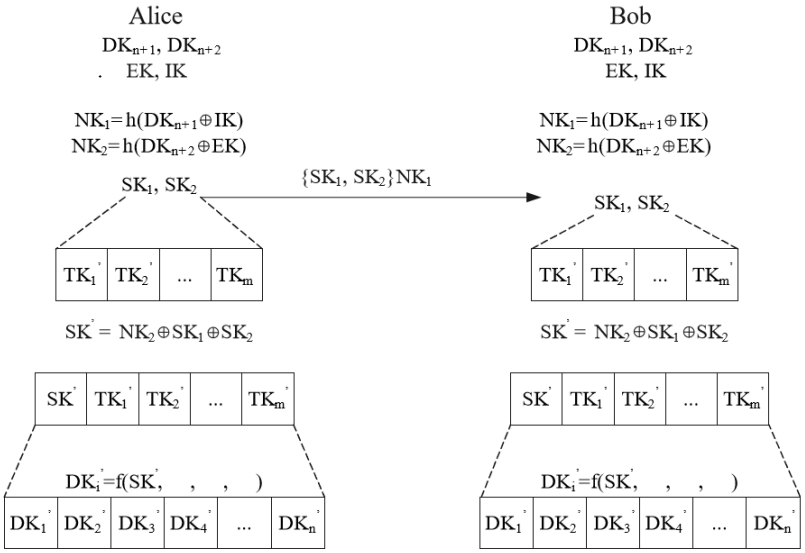

Fig. 4 Repeated Dynamic Key Generation[10]

- Step 1: Both Alice and Bob calculate two extra dynamic keys from the old sequence[10].

$$DK_{n+1} = f(SK, DK_{n-m+1} \ldots, DK_{n-1}, DK_n)$$
$$DK_{n+2} = f(SK, DK_{n-m+2} \ldots, DK_n, DK_{n+1})$$

Using them to compute two new initial key using the use of a one-way hash function $h(.)$[10].

$$NK_1 = h(DK_{n+1} \oplus IK)$$
$$NK_2 = h(DK_{n+2} \oplus EK)$$

- Step 2: To generate the new sequence of the dynamic key, Alice and Bob need m new temporary keys which can be generated using the below equation:

$$TK_1' = h(DK_{n-m+4} \oplus SK_1)$$
$$TK_2' = h(DK_{n-m+5} \oplus SK_1)$$
$$\ldots..$$
$$TK_{m-1}' = h(DK_{n+2} \oplus SK_1)$$
$$TK_m' = h(DK_{n+1} \oplus SK_1)$$

- Step 3: Both Alice and Bob compute a new seed key SK' from the key $NK_2$and the session keys SK_1,SK_2 using bit-wise exclusive or operation[10].

$$SK' = NK_2 \oplus SK_1 \oplus SK_2$$

- Step 4: Generate a series of dynamic keys - this step is the same as Step 4 in the initial dynamic key generation scheme[10]. The new seed key $SK'$and the new set of temporary keys $TK_1', \ldots, TK_m'$are used to calculate the brand new series of dynamic keys $DK_1', \ldots, DK_m'$

$$DK_1' = f(SK', TK_1', \ldots, TK_{m-1}', TK_m')$$
$$DK_2' = f(SK', TK_2', \ldots, TK_m', DK_1')$$
$$DK_3' = f(SK', TK_3', \ldots, DK_1', DK_2')$$
$$\ldots..$$
$$DK_n' = f(SK', DK_{n-m}', \ldots, DK_{n-2}', DK_{n-1}')$$

IJIREEICE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

NCIET- 2020

National Conference on Innovations in Engineering & Technology

Govt., Polytechnic College, Palakkad, Kerala

Vol. 8, Special Issue 1, February 2020

V. DYNAMIC KEY ENCRYPTION SCHEME

A. *Dynamic Permutation Encryption Scheme*

Algorithm 1: Dynamic Permutation Encryption

while i = *1 to* α **do**
  $t[2i-1]$ =Re$(X[i])$;
  $t[2i]$ =Im$(X[i])$;
end
while i = *1 to* 2α **do**
  $temp = t[i]$;
  $t[i] = t[\pi[i]]$;
  $t[\pi[i]] = temp$;
end
while i = *1 to* α **do**
  $D[i] = t[2i = 1] + j \times t[21]$;
end

Permutation encryption is an encryption technique where a simple swapping operation is introduced in-turn to achieve a random permutation/interleaving. The random perturbation depends on the CSI between legitimate users. To implement the dynamic behavior, in each instance the real and imaginary terms are splits and introduce the swapping operation. Afterward, they will combine to get the dynamic key sequence. The algorithm for the same is described in algorithm 1.

B. *Dynamic Phase Encryption Scheme*

The pseudo-code for dynamic phase encryption is described in algorithm 2. Two pseudo-random sequences a and b are generated using secure stream ciphering, where a is multiplied by the real part of the time domain signal, and b is multiplied by the imaginary part[1]. Both a and b should be transformed to bipolar. To implement the dynamicity, real and imaginary terms are swapped before multiplying with the a and b sequence.

Algorithm 2: Dynamic Permutation Encryption

while i = *1 to* α **do**
  $R[i]$ =Re$(X[i])$;
  $I[i]$ =Im$(X[i])$;
  if $c[i] == 0$ **then**
    $temp = R[i]$;
    $R[i] = I[i]$;
    $I[i] = temp$;
  end
  $R[i] = R[i] \times a[i]$;
  $I[i] = I[i] \times b[i]$;
  $D[i] = R[i] + j \times I[i]$;
end

VI. CONCLUSION

Cryptography plays a key function in securing data, integrity, and confidentiality. There are two sorts of keys in cryptography: Symmetric and Asymmetric. Session keys are a combination of these two. The dynamic key is almost similar to session keys but there will not be any key exchange between the sender and receiver. Dynamic key encryption techniques have better performance than symmetric, asymmetric and session key encryption schemes. Dynamicity can be implement in many encryption schemes. When dynamic phase and dynamic permutation encryption schemes were introduced in the MIMO 4G channel with the OFDM multiplexing technique, performance is found that at lower SNR value both encryption scheme shows almost similar BER rate. But on increasing the SNR value Phase encryption is dominating.

IJIREEICE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

NCIET- 2020

National Conference on Innovations in Engineering & Technology

Govt., Polytechnic College, Palakkad, Kerala

Vol. 8, Special Issue 1, February 2020

REFERENCES

[1] Reem Melki, Hassan N. Noura, Mohammad M. Mansour, Ali Chehab, "An efficient OFDM - Based Encryption Scheme Using a Dynamic Key Approach", IEEE Internet of Things Journal, 361 - 378, Volume: 6, Issue: 1, Feb. 2019

[2] Hikmet Sari, Ali Maatouk, Ersoy Caliskan, Mohamad Assaad, Mutlu Koca, Guan Gui, "On the foundation of NOMA and its application to 5G cellular networks",2018IEEEWirelessCommunicationsandNetworkingConference (WCNC), April 2018

[3] Zhang Wu, Kun Lu, Chengxin Jiang, Xuanbo Shao, "Comprehensive Study and Comparison on 5G NOMA Schemes", IEEE Access, 18511 - 18519, March 2018

[4] Bahubali Akiwate, Latha Parthiban, "A Dynamic DNA for Key-based Cryptography", International Conference on Computational Techniques, Electronics and Mechanical, Dec. 2018

[5] Asim Mazin, Kemal Davaslioglu, Richard D. Gitlin, "Secure key anagementfor5Gphysicallayersecurity",2017IEEE18thWirelessandMicrowave Technology Conference (WAMICON), April 2017

[6] Anass Benjebbour, Anxin Li, Keisuke Saito, Yuya Saito, Yoshihisa Kishiyama, TakehiroNakamura, "NOMA-Concepttostandardization", IEEE Conference on Standards for Communications and Networking (CSCN), October 2015

[7] Dr. Rupesh Singh, "Multiple Access Techniques For 4G Mobile Wireless Networks", International Journal of Engineering Research and Development, Volume 5, Issue 11 (February 2013), PP. 86-94

[8] Hassan N. Noura, Reem Melki, Ali Chehab, Mohammad M. Mansour, "Efficient and Secure Physical Encryption Scheme for Low-Power Wireless M2M Devices", 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018, 1267-1272, 2018

[9] Noura, Hassan N. Melki, Reem Chehab, Ali Mansour, Mohammad M., "A Physical Encryption Scheme for Low-Power Wireless M2M Devices: a Dynamic Key Approach", Mobile Networks and Applications, Vol. 24, Issue 2, 447-463, 2019

[10] Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, and Balasubramaniam Srinivasan," Dynamic Key Cryptography and Applications", InternationalJournalofNetworkSecurity, Vol.10,No.3,PP.161–174, May2010

[11] https://en.wikipedia.org/wiki/4G

[12] F. Huo and G. Gong, "A new efficient physical layer OFDM encryption scheme,"inProc.IEEEInt.Conf.ComputerCommun.(INFOCOM), Toronto, ON, Canada, Apr. 2014, pp. 1024–1032.