A Comparative Study of Different Encryption Methods Applied to CDMA to Enhance Security

Allamprabhu V. Kolaki and Dr.G.A. Bidkar

Abstract--- The paper presents a comparison of different encryption methods applied to Code Division Multiple Access to enhance security, in terms of performance, applications and implementation. The focus is mainly on direct sequence spread spectrum PN sequence security. The advantages and limitations of the different techniques are discussed.

Keywords--- DS-CDMA, PN Sequences, Encryption Algorithm, Authentication Algorithm, Performance Analysis.

I. INTRODUCTION

THE Wireless and cellular network arena have been developing rapidly as the user request grows. The existing communication systems such as TDMA and FDMA are becoming insufficient for some applications in today's communication demands. To fulfil the today's communication demands a system called DSCDMA used to replace the above-mentioned systems. This system transmits signals concurrently without inter symbol or inter channel interference. This system follows the spread spectrum technique in which the message signal occupies both time and frequency domains at the same time, thus the system capacity increases significantly. When designing multi-channel transmission we must concentrate to reduce cross talk between adjacent channels[1]. Generally the data communication system used today is spread spectrum communication. In Spread spectrum transmission, the signal occupies excess bandwidth than the minimum is necessary to send the information. It is necessary to give up this excess bandwidth as it offers secure communication in unpromising environment. The spreading of spectrum has achieved through a code that is independent of the data whereas at the receiver the same code has to use for despreading in order to recover data. The purpose of coding is to transform a narrow spectrum signal in to noise like wide spectrum. Due to the spreading energy, spread spectrum system results in several advantages like short-range interferences and resistance to interference.

II. MULTIPLE ACCESS TECHNIQUES

Multiple access is a technique in which many users share the communication channel at the same time from different places. In multiple access method, the radio spectrum divided into channels and allocated to various users of the system. As there are multiple users transmitting over the same channel, so

that individual users will not be interrupt with one another [15]. There are three basic schemes

1. Frequency Division Multiple Access (FDMA)
2. Time Division Multiple Access (TDMA)
3. Spread Spectrum Multiple Access (SSMA)
 - a) Frequency Hopped Multiple Access (FHMA)
 - b) Code Division Multiple Access (CDMA)

A. Frequency Division Multiple Access (FDMA)

A unique frequency band or channel has assigned to every user as shown in figure 1. The channels are assigned to subscribers only on request. In Frequency Division Duplexing, two frequencies are used—one for forward channel & another for reverse channel. At the time of call, other user cannot share the same frequency band. In FDMA if channel is not in use, and it goes idle and other users cannot use it. While at the receiver has to tune in to the know frequency in order to receive the transmitted signal.

B. Time Division Multiple Access (TDMA)

In TDMA, a limited amount of time allows to access entire frequency bandwidth. All senders can share the entire bandwidth but in different time as shown in figure 2. If two transmissions overlap that is known co-channel interference. The sender and receiver clock synchronization is required.

C. Spread Spectrum Multiple Access (SSMA)

Figure 1: FDMA Channel Allocation

Spread spectrum multiple access uses transmission signal bandwidth that is several orders greater than the minimum bandwidth required. A pseudo-noise (PN)

Allamprabhu V. Kolaki, Assistant Professor Dept. of ECE, KLS's Vishwanathrao Deshpande Rural Institute of Technology, Haliyal, India. E-mail: allamvk28@gmail.com

Dr.G.A. Bidkar, Professor and Head, Dept. of ECE, Shri Dharmastala Manjunatheshwar College of Engineering and Technology, India. E-mail: gabidkar@rediffmail.com

DOI:10.9756/BIJRCE.8205

Figure 2: TDMA Time Slot Allocation

sequence transforms a narrowband signal in to a wideband noise-like signal before its transmission. SSMA also provides immunity to multipath interference and robust multiple access capability. When a single user uses SSMA the nit is not a bandwidth efficient. However, when many users use the same spread spectrum bandwidth without interfering with one another Spread spectrum system becomes bandwidth efficient. There are two types of spread spectrum multiple access techniques; frequency hopped multiple access (FH) and direct sequence multiple access (DS) and it is also known as code division multiple access.

a) Frequency Hopping (FH)

The signal will pseudo-randomly switches between different frequencies within the hopping bandwidth and the receiver knows PN code to find the signal at any given time.

b) Direct Sequence (DS or CDMA)

The pseudo-random code generated and that has used to code the digital data directly at a higher frequency. The receiver also knows to generate the pseudo-random code. By using this code, receiver extracts the data from the received signal.

III. SECURITY REQUIREMENTS

Each organization intended to protect their confidential data from tampering and access to authorized users. One requirement is when confidential data that is stored or transmitted over public networks must be encrypted using professional algorithms. Other requirement is for users to authorize themselves, is achieved using a security token (e.g., one time password or Password). Biometric approaches used as one of the authentication factors [2]. Some of the security requirements are as follows.

A. Importance of Digital Signature

The digital signature using asymmetric key cryptography considered to achieve information security. It provides non-repudiation of message, message authentication and data integrity.

B. Message Authentication

The receiver receives the data and validates it by using symmetric key that assures that only my intended sender who possesses the similar key and no one else. Therefore, this kind of communication provides the authorization.

C. Data Integrity

When two authorized users communicating each other, an attacker access to that data and changes it; at receiver, the verification of digital signature fails. The has hof modified data and the output provided by the verification algorithm will not match. The data integrity has breached thus the receiver can deny the message.

D. Non-repudiation

We considered that only the sender and receiver have the knowledge of the digital signature key. The sender can only create digital signature on a given data. Thus, receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future. Here no one can deny either the transmission or reception of message.

IV. SECURITY THREATS TO WIRELESS COMMUNICATION

The transmission of confidential data over wireless networks means prevent from attacks like confidentiality, integrity and availability. Possible threats due to weaknesses in the security protocols. This section describes various types of security attack techniques. Different types of security attacks are as follows[14].

A. Attack Based on Traffic Analysis

This technique enables the attacker to access types of information. The information related to identification of activities on the network. The important information to the attacker is identifying the physical location of access point in its surroundings. The information an attacker can get by analysing the traffic flow. An attacker needs to gather the information about the size and number of the package over a certain period.

B. Eavesdropping

An attacker secretly listens to the personal conversation of others without their permission. Eavesdropping attacks are classified in to passive eavesdropping, active eavesdropping.

a) Passive Eavesdropping

The attacker watches over a wireless session and able to read the data during encrypted transmission. By surveying, the packages gather the data indirectly. The Passive eavesdropping attack violates confidential information. The gathered information may use for more insecure kinds of attacks.

b) Active Eavesdropping

The attacker not only gathers the information by watching wireless session but also inserts own messages in order to modify the content of the messages in the session. The active eavesdropping attack violates confidential and integrity of information.

C. Attack that can cause Denial of Service (DOS)

The denial of service attack is due to wrong or misleading information. The attacker disables the network or jamming network availability in order to degrade the performance. Due to this, attack legitimate users are unable to access the communication network.

V. CRYPTOGRAPHY

Cryptography is the art of science for hiding information to retain its privacy. Based on the keys used in encryption and decryption process the cryptosystem classified in to Symmetric Key Encryption and Asymmetric Key Encryption, [14].

A. Symmetric Key Encryption

In symmetric key encryption, process same keys are used for encrypting and decrypting the information. Examples of symmetric key encryption methods are Advanced Encryption Standard (AES), Triple-DES (3DES), IDEA, and Digital Encryption Standard (DES).

B. Asymmetric Key Encryption

The encryption process in which different keys are used for encrypting and decrypting the information is referred as asymmetric key encryption. However, the keys are different, but they are mathematically related and hence extracting the plaintext by decrypting cipher text is feasible. Examples are Diffie Hellman, RSA and Elgamal Cryptosystem.

VI. RELATED WORK

In one of the related work, the flow of the spread voice signal in the CDMA system is monitored through forward traffic channel by the FCM protocol. The possibility of monitoring one-way channel of CDMA system by the FCM protocol[3] Show the system architecture of the test instrument to monitor the forward channel in CDMA. In the future, based on the result, new system architecture for the secure CDMA system may be designed.

Researchers in this area have proposed a blind, robust and secure watermarking technique based on DS-CDMA [4]. By using this technique, a watermark can be extracted at very high PSNR value with very low BER. An adaptive approach selects the coefficients in the DCT domain, where the watermark is to hide. This significantly reduces BER. Multiple spreading codes can be used to make this scheme secure and more robust against JPEG compression, scaling and cropping.

Instead of using the long-code sequences generated by the LFSR directly, the scrambling sequences generated through AES operations are proposed. As a result, the physical layer built-in security of the CDMA system is significantly increased with very limited complexity load. Scrambling the training sequence and the message sequence separately with two independent scrambling sequences, both information privacy and system performance can be further improved. Finally, decryption can be achieved through secure scrambling [5]. This Scheme is very feasible and it can be implemented for security enhancement in wireless networks.

Researchers in this area have proposed the encryption algorithm to spreading code in order to improve the security of CDMA. The security produced in this way is primarily associated with the complexity of the employed encryption algorithm. Because the encryption algorithms security is highly reliable, it is suitable for any kind of data communications. The combination of encrypted and decrypted M-sequence is used as a spreading code to mitigate the system

performance, and the advantage of this combination is considered from the interference level and the security point of view. A compatible algorithm for the key exchange is produced [6].

In this paper researchers have proposed, chaotic spreading codes for MIMO MC DS/CDMA considered for the analysis [7]. A NPG algorithm based on pricing performs better by effectively mitigating the MAI in MIMO MC DS-CDMA system. Also, the use of chaotic codes performs better than the system with classical codes in exterminating MAI. Numerical results of analysis shows that employing chaotic code with good cross correlation properties can minimizes the interference in a multiuser MIMO MC DS CDMA system. It also achieves significant improvement in the utility factor compare to the conventional system without pricing.

Time-hopping CDMA network architecture supports point-to-point and point-to multipoint communication up to 128 ONUs with a worst-case rate of 12 Mbps. The related work provides security at the physical layer and VPNs between ONUs can be set up without additional higher-level protocols [8]. They also showed that there is a low penalty due to physical layer impairments, such as transmitter extinction ratio, fiber, splitter, and splice losses. This opens the door to the design of a larger secure CDMA network, covering longer distances and capable of servicing more end users.

The researchers have proposed CDMA air interface security mechanisms includes data encryption technology, based on AES and ECC hybrid cryptosystem [9]. It can be achieved based on the design and implementation of CDMA IX wireless access technology centralized control of air defence and disaster warning system. It solves the data transfer security issues of the CDMA IX public network channel access schemes in the Internet. Not only encryption and even decryption is quick and secure, but for digital signatures and authentication, and real-time transmission of data has less influence.

The concept of physical encoding to provide optical layer security OCDMA systems are proposed and analysed possible ways to compromise the OCDMA systems and intercept the transmitted data [10]. They also illustrated some approaches to improve the confidentiality of OCDMA systems. Finally, they discussed physical encoding in optical steganography, and a wireless-CDMA optical transmission system for confidentiality enhancement. This field is still at its early research stage. More research efforts on this field, both theoretical and experimental, are expected in the near future.

The OCDMA performs encoding and decoding through an optical signature code, in order to allow the selection of a desired signal so that different users can share the same bandwidth [11]. In such a systems, data signal overlap in both time and wavelength. The researchers have proposed Confidentiality against eavesdropper interception strategies for optical CDMA. The Coherent detection with combining signals shows better confidentiality than the incoherent one. In the network system if one user is active, the optical CDMA scheme cannot guarantee physical layer any more. If the network capacity is increased, that will lead to eavesdropper to

detect high SNRs, higher SNRs will increase the eavesdropper possibility of attack. The wide bandwidth enhances SNRs for authorized user and eavesdropper. To prevent the information data from the eavesdropper the signal to noise ratio SNRs must be reduced without effecting the system performance

The Authentication and Key Agreement (AKA) protocols are proposed to solve two known vulnerabilities of UMTS security: identity catching and secret key exposure. It protects the messages exchanged during the Authentication and Key Agreement protocol. The first phase of the solution consists of a secure key generation. The secure key generation phase is called AKA (Authentication and Key Agreement) -phase. The second phase of the solution is able to solve the problem of redirection attacks, man-in-the-middle attack, sequence number depletion attack, and roaming attack. This phase includes a User Confidentiality for UMTS (EMSUCU) protocol[12]. It solves the vulnerabilities through eliminating it and improves the security and efficiency. The enhanced SHAI technique solve redirection attacks: sequence number depletion attack, man in-the-middle attack and roaming attack.

The researchers have proposed two methods are called Nested DSSS and Interleaved DSSS[13]. In the nested method, the variance of multi-user interference that corresponds to the interference power is reduced significantly, so this method can provide high level of security while a better BER performance is also achieved, compared with a common DSSS system. The interleaved DSSS that exploits a key-based permutation cipher to interleave the M-sequence bits within the encrypted code bits leads to a higher level of security compared with the nested DSSS and hidden DSSS methods.

VII. CONCLUSION

In this paper, we reviewed the different approaches for DS CDMA security by using cryptographic algorithm. After reviewing some papers, it is noticed that we need to prevent the PN sequences from the eavesdroppers that fulfils the user data confidentiality and authentication. There is a further Scope in enhancing the mutual authentication and security of the data in DSCDMA.

REFERENCES

- [1] V.K. Kakade "Implementation of DS-CDMA Transmitter and Receiver in VHDL for FPGA", IJLTETIDEAS, Pp.158-166, 2013.
- [2] U. Kumar and S. Gambhir, "A Literature Review of Security Threats to Wireless Networks", IJFGCN, Vol.7, No.4, Pp.25-34, 2014.
- [3] D.H. Ryu and S. Jang, "A Security Weakness of the CDMA Cellular Service", IJCSNS, Vol.6, No.5, Pp.218-227, 2006.
- [4] M.K. Samee and J. Gotze, "Increased robustness and security of digital watermarking using DS-CDMA", IEEE International Symposium on Signal Processing and Information Technology, Pp.185-189, 2007.
- [5] T. Li, Q. Ling and J. Ren, "Physical Layer Built-In Security Analysis and Enhancement Algorithms for CDMA Systems", EURASIP Journal on Wireless Communications and Networking, Pp.1-7, 2007.
- [6] M. Tafaraji and A. Falahati, "Improving code division multiple access security by applying encryption methods over the spreading codes", IET Communication, Vol.1, No.3, Pp.398-404, 2007.
- [7] V. Nagarajan and P. Dananjayan, "Performance Analysis of MIMO MC-DS/CDMA System Using Chaotic Spreading Sequence", International Journal of Computer and Electrical Engineering, Vol.2, No.2, Pp. 329-333, 2010.
- [8] A.A. Ortega, V.A. Bettachini, J.I. Alvarez-Hamelin and D.F. Grosz, "Point-to-point and Point-to-multipoint CDMA Access Network with

- Enhanced Security", Advanced Photonics, OSA Technical Digest (CD), 2011.
- [9] C. Dan, L. Yijun and T. Jiali, "Analysis of Security Based on CDMA Air Interface System", Energy Procedia, Vol.16, Pp.2003-2010, 2012.
- [10] Z. Wang, M.P. Fok and P.R. Prucnal, "Physical encoding in optical layer security", J Cyber Secur Mobility, 2012.
- [11] M.M. Shukra, A.K. Jaiswal, M. Kumar, "Security Based Performance Analysis in Optical CDMA Network Systems", Vol. 8, No.6, Pp.70-74, 2013.
- [12] V. Vijayakumar and Dr.R. SamsonRavindran, "Enhanced Security Framework For Authentication And Integrity (ESFAI) in CDMA Networks", Journal of Theoretical and Applied Information Technology, Vol.69 No.3, Pp.503-513, 2014.
- [13] A. Falahati and N. Sanandaji, "Nested and interleaved direct sequence spread spectrum to enhance CDMA security and bit error rate performance", 2016.
- [14] A. Kahate, "Cryptography and network Security", Tata McGraw Hill, 2006.
- [15] S. Haykin, "Communication Systems", 4th edition, Tata McGraw Hill, 2005.