Security of OFDM through Steganography

Nikita Agrawal
M.Tech Scholar, (D.C.), Department of Electronics & Communication Engineering
Truba Institute of Engineering & Information Technology, Bhopal

Neelesh Gupta
Professor in Electronics & Communication Engineering
Truba Institute of Engineering & Information Technology, Bhopal

ABSTRACT
Communication through wireless medium is widely used in today's world. Orthogonal frequency-division multiplexing (OFDM) is a multiplexing method in which data transmission is done over the equally spaced, overlapped carrier frequencies. Transmission of data through OFDM has the advantage that it can achieve high data rate with greater bandwidth and flexible underlying modulations. It can easily eliminate intersymbol interference (ISI). Therefore OFDM has become a leading choice for data transmission. .So it becomes important to secure data that is transferred through wireless OFDM communication systems. Different techniques have been used for secure data transmission like cryptography, watermarking etc. In this paper, literature studies of various techniques are discussed. Enhanced security using steganography is proposed.

Keywords
OFDM, cryptography, ciphering, encryption, steganography

1. INTRODUCTION
Orthogonal frequency-division multiplexing (OFDM) is a multiplexing technique for digital data encoding over multiple subcarriers. These subcarriers are orthogonal to each other which carry data over the channel. Orthogonality of subcarriers eliminates requirement of intercarrier guard band and also reduces crosstalk. OFDM advantages include high spectral efficiency, robustness against co-channel interference, fading caused by multipath propagation and inter-symbol interference. Implementation of modulators in OFDM is done by IFFT algorithm at sender station and FFT algorithm at the receiving station. These make OFDM a leading choice for communication over air interfaces. Although, OFDM is resistant to adverse effects of propagation, reflection and modulation, it requires inherent security measures. Multimedia information that is communicated by wireless network is not safe as compared to the wired technology. Hence, security of OFDM becomes an essentiality.

Major techniques are applied over OFDM security that include cryptosystems ,watermarking, encryption, coding etc. which rely over physical layer for implementation .Cryptography uses a key for encryption and decryption of data. At the sending station, data is encrypted using a key and decryption at receiver is not possible without the key. Cryptographic algorithms include RSA, ECC, PGP, DES etc. Watermarking techniques involve separation of embedded system from audio video signals for authentication. Original digital signal is embedded with watermark signal to create a digital watermark symbol. These methods are applied over multimedia data in OFDM transmission of which some methods prove efficient for the safety of data. In this paper, methods applied for OFDM secure communication is discussed.

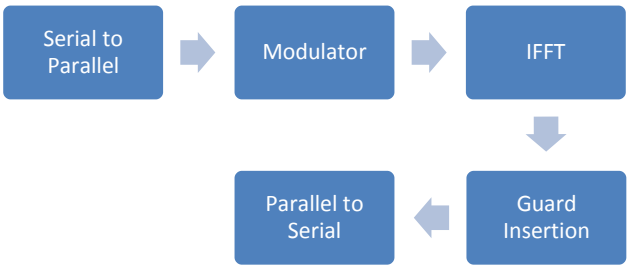


Fig.1.Block diagram of OFDM transmitter

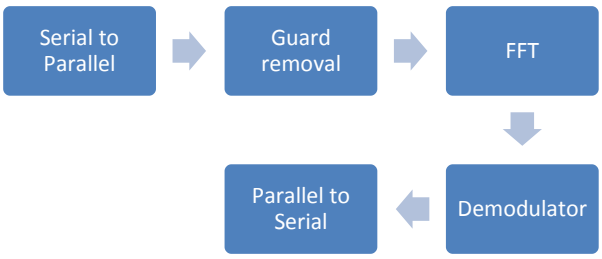


Fig.2. Block diagram of OFDM receiver

The organization of the remaining section of the paper is done in this manner: The section II deals with the literature of the previous work done. Section III deals with the problem statement .Next section deals with various techniques used for OFDM security. Section V deals with the proposed work. Last section gives overall conclusion of this paper to prevent the data to be attacked by an eavesdropper in OFDM wireless communication.

2. LITERATURE REVIEW
Various encryption, decryption and watermarking techniques have been applied over OFDM for security and better system performance. Some of the significant work is discussed.

Gill R. Tsouri and Dov Wulich [1] proposed method in which overloading of subcarriers is done by multiple transmitters in wireless time-varying channels. The method applied is based on superposition modulation, reverse piloting and joint decoding. It also uses channel reciprocity, randomness and de-correlation in space to secure OFDM with low overheads on encryption, decryption, and key distribution. Other implementing methods are also derived that include generating robust joint constellations and mitigating the effects of imperfections due to power control errors, mobility and synchronization errors.

A. Al-Dweik and M. Mirahmadi[2] proposed a method which developed a new OFDM symbol structure by the use of symmetric key cryptography by use of a secret key. Data detection without the use of secret key results in a distorted noise like data. This type of system has enhanced security and reduced computational complexity. The secret key must be chosen such that it cannot be guessed by the attackers, and the data lost due to the absence of knowledge of the secret key is maximized, the data sequence can then be considered safe. Approach is to use permutation matrices, which change the order of samples and mix with the samples of other OFDM blocks. The permutation matrix can be realized as a random block or convolution interleaver. Security analysis is done by the probability of estimating the permutation matrix and the loss of data due to inaccurate knowledge of permutation matrix. For moderate frequency selective channels, this method is highly robust and useful. Performance evaluation of the system using nonlinear functions is required for this proposed method. The derivation of analytical BER using different methods is to be considered.

John E. Kleider and Steve Gifford[3] proposed the method of digital watermarking in which embedded signals are separated from audio and video signal. This allows distribution tracing, copyright protection and authorized access control. Watermarking is applied to the physical layer of modulation waveform which improves efficiency of the process of authentication. Two major watermarking process are constellation dithering (CD) and baud dithering (BD) which are applied to OFDM. The advantage of BD includes higher detection robustness and CD includes flexibility. Generation of CD signal is done by mapping watermarking information bits on symbols and spreading symbols with Gaussian distributed code.BD signal can be represented by time controlled jitter process induced on OFDM symbols after the insertion of cyclic prefix.CD reconstructed image has no perpetual degradation and no statistical or visual difference.BD technique was is more robust. The robustness of CD technique is low as compared to the BD technique and also has less capacity.BD technique is robust and provides better capacity but it needs attention to the operational performance in the tracking circuit of the receiver so as the interoperability is maintained with non-informed receivers.

D. Rajaveerappa and Abdelsalam Almarimi [4] proposed cryptosystem with combination of both the symmetric key mono alphabetic shift ciphering and the public key RSA (Rivest, Shamir, and Adleman) ciphering. This was then combined with multimedia wireless systems of IFFT/FFT based OFDM. The merits of both SKC and PKC were considered and eliminated the demerits of both SKC and PKC. This technique is able to encrypt/decrypt signals which include text, audio and image signals (multimedia) in very short duration of time and for the same time it is difficult for hackers to get the information which is being transmitted. [5][6] Hadamard transform is used for Walsh code generation and AWGN channel is modeled. This method encrypts and decrypts data but the overall message transmission process is not hidden in the process.

3. PROBLEM STATEMENT

The methods that are studied allow encryption and decryption of data. The data to be send is secured, but attacker is always attracted by an encrypted data. So, it is important that the data that is being transferred is hidden and secured. Also, the data should be properly encrypted. So a complete methodology for data encryption and data hiding is required for secure transmission of data through OFDM.

4. VARIOUS TECHNIQUES USED FOR OFDM SECURITY

4.1. Cryptography

Cryptography is a method of securing information such that only intended person can retrieve that information. Algorithms are applied over data to encrypt or decrypt it for secure transmission. Data being transferred is converted to cipher text and at the receiving station it is decrypted back to plain text [7].Basically there are two ways to apply cryptography. They are symmetric cryptography and non symmetric cryptography.

4.1.1. Principle of Cryptography

Data or plain text to be transferred is converted into cipher text with help of a key. This process is called encryption process. This is sent over the channel. At the receiving station cipher text is converted back to plain text again with the help of a key. This process is called decryption process.

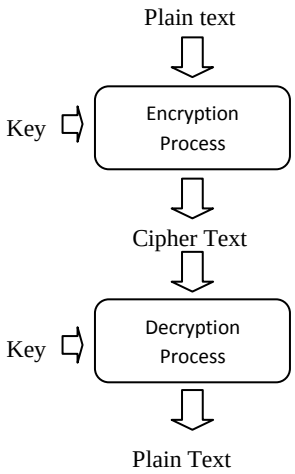


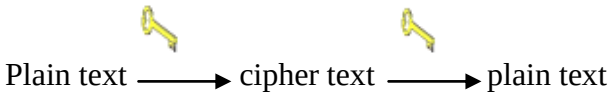
Fig.3.Cryptographic process

4.1.2. Symmetric Cryptography

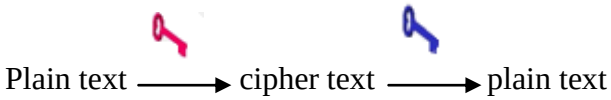
It uses a single secret key which is used both for encryption and decryption. Key is changed timely. This algorithm is fast and efficient. This works well for large volume of data.

4.1.3. Asymmetric Cryptography

This requires two keys public and private. Encryption is done by the public key but decryption is possible only with the private key. Advantage of asymmetric cryptography is that it can be widely used by many people with help of public key. Data security using asymmetric key cryptography is better because of using two different keys.



A) Secret key (symmetric cryptography) uses single key for both encryption & decryption.



B) Public (asymmetric) key cryptography uses two keys. One for encryption, other for decryption.

Fig.4.Types of cryptography

4.2. Steganography

Steganography is a method of information hiding. Data can be secretly hidden in the media file like image, audio, video etc. Information hiding through steganography has application of higher security, robustness and capacity. For the detection of data from hidden files, special algorithm is required. Steganography takes cryptography one step further as encrypted data is hidden and hackers scanning the data will not be able to know that it contains an encrypted data. Even if data is decrypted, it still remains hidden.

5. PROPOSED METHOD

To safeguard the data that could be attacked by eavesdropper, a method is proposed in which data is encrypted using RSA technique. Then Steganography is applied over the data to ensure hidden and secure data transmission. The method proposed allows encryption of data so that attacker is not able to read the message. It also hides the data so that data is not visible to the eavesdropper. This ensures that the message being transferred is visible and can be read, only by the intended users. So, a combination of cryptography and steganography can provide the highest level of security in data transmission.

5.1. Expected Outcome

Proposed system will enhance the security of data that is transmitted. Proposed method is expected to increase robustness and capacity of the transmitted data. The performance analysis of the proposed work is to be done by PSNR and BER. Expected results include better PSNR and higher reliability with lower values of BER.

6. CONCLUSION

Wireless network communication is most popularly used for data transfer. To guard the data being transferred, various techniques has been proposed. In this paper literature study of the proposed methodology is summarized. Some methods are efficient for secure transfer of information through cryptographic and watermarking techniques. In proposed work, we need to design methodology which enhances the security of data transmission through OFDM by hiding the encrypted data being transmitted. Steganography is proposed for enhancing security of data transmission through OFDM.

7. REFERENCES

[1] Gill R. Tsouri, Dov Wulich, "Securing OFDM over Wireless Time-Varying Channels Using Subcarrier Overloading with Joint Signal Constellations." Hindawi Publishing Corporation. EURASIP Journal on Wireless Communications and Networking. Volume 2009, Article ID 437824, doi:10.1155/2009/437824

[2] A. Al-Dweik, M. Mirahmadi, A. Shami, Z. Ding and R. Hamila , "Joint Secured and Robust Technique for OFDM Systems" ,Western University, Canada,IEEE ICC 2013

[3] John E. Kleider, Steve Gifford, Scott Chuprun, and Bruce Fette, "RADIO FREQUENCY WATERMARKING FOR OFDM WIRELESS NETWORKS", General Dynamics, Decision Systems, Scottsdale, Arizona, USA 85257.

[4] D. Rajaveerappa and Abdelsalam Almarimi, "RSA/SHIFT SECURED IFFT/FFT BASED OFDM WIRELESS SYSTEM" ,Department of Communications Higher Institute of Electronics Baniwalid, Libya, 2009 Fifth International Conference on Information Assurance and Security.

[5] Bewley, William L, 1983, The Origins of Spread Spectrum Communications. In IEEE Transactions on Communications, Vol. 22, No.5, pp. 637-648.

[6] Esmael H., et al, 1998, Spreading Codes for Direct Sequence CDMA and Wideband Cellular Networks. *In IEEE Communications Magazine.* Vol. 36, pp. 88-95.

[7] Ranjan Bose, "Information theory & coding, cryptography", second edition.

[8] Fei Huo and Guang Gong, "A New Efficient Physical Layer OFDM Encryption Scheme", Department of Electrical and Computer Engineering, University of Waterloo, Ontario N2L 3G1, CANADA.