



Implementing security to OFDM symbols of 802.11n networks

¹SANTOSH, ²VINOD B DURDI

^{1,2} Department of Telecommunication Engineering,
Dayananda Sagar College of Engineering, VTU, Bangalore, India

Abstract: This paper mainly deals with the steganographic channels in high speed 802.11n networks. Here the modification of cyclic prefix in OFDM has been discussed. This is the highest hidden transmission technique known till date. Here the main focus is on the theoretical analysis and simulation results of the steganographic system performance.

Keywords: OFDM, network Steganography, IEEE 802.11n

I. INTRODUCTION

Since there is a great demand for fast and reliable wireless transmission there is a need to extend the standardization limit of WLAN standards. In the existing solution the main focus is on the security and offered throughput. The former has been solved by the IEEE 802.11i extension, significant “acceleration” was given after a few years with the approval of the standard IEEE 802.11n. 802.11 [1] based networks protect users’ privacy with advanced cryptographic solutions. However, that user is still vulnerable to steganographic systems that could be implemented in their wireless network. Fast 802.11n networks are, therefore, potentially a great hidden transmissions carrier.

The main objective of this paper is to analyze the cyclic prefix information hiding technique which is based on OFDM modulation [2] specifically for IEEE 802.11n networks. In order to implement this system modified model of the 802.11n physical layer is used. The system requirements are MATLAB 7.10, Microsoft Windows 7.

II. EXISTING SYSTEM

Steganography for 802.11 was proposed by Szczypiorski according to him information has been hidden in the intentionally corrupted packets HICCUPS. Also as discussed in [3] and [4] the information has been hidden in the intentionally corrupted packets where secret information will be in the modified fields of the frame headers. WiPad, where information is hiding in the padding [5].

Disadvantages of existing methods:

- The existing system is not fast as the cyclic prefix steganographic system system.
- Existing system is having more cost.

III. OFDM IN 802.11N

OFDM (Orthogonal Frequency-Division Multiplexing) means simultaneous transmission of independent data streams in single radio channel. In OFDM subcarriers will be orthogonal to each other. In FDM resources are shared according to the available bandwidth to a radio channels. In each of these channels the data streams of each user are transmitted.

In the radio environment there is problem of multipath propagation where the receiver receives not only the signal propagated but also the delayed copies of that signal which is the main reason for ISI (Inter symbol Interference). In order to reduce ISI [6], in OFDM modulation, a special guard interval (GI) is inserted between symbols as shown in Fig.1.

The IEEE 802.11 standards implement the guard interval by copying the ending part of each OFDM symbol and adding it in front of that symbol. The total single symbol transmission time (T_{sym}) is then the sum of the useful part of the symbol (T_u) and the duration of the GI as shown in Fig.1.



Fig.1 Cyclic prefix generation

In the case of OFDM modulation in IEEE 802.11 networks, the GI is assumed to be a constant value $T_{CP} = 0.8\mu\text{s}$. Optionally, 802.11n allows the shortening of the GI duration to $T_{CP} = 0.4\mu\text{s}$ in the case of good propagation conditions.

IV. DISCUSSION

The cyclic prefix technique is based on the existence of the cyclic prefix in the OFDM modulation. It improves the quality of transmission in the standard network. The cyclic prefix has to be introduced at the right place i.e. before its transmission and after the modulation. The duration of the GI remains unchanged the described modification does not affect the correct operation of the wireless network.

The IEEE 802.11n standard distinguishes several modulation and coding schemes (MCSs) and allows the usage of one from the four modulations (BPSK, QPSK, 16-QAM or 64-QAM). It is chosen in such a way as to obtain the maximum possible bandwidth in a given environment at a given moment.

The cyclic prefix technique modifies the cyclic prefix at physical layer. There is a problem of choosing antennas and the transmitters whose prefixes are to be modified. The need to finding and read these modified symbols in the steganographic receiver [7] must be taken into account.

In order to accomplish this transmitter and receiver should have identical pseudo random number generators (PRNGs). This type of generator allows the creation of a sequence of numbers that is similar to random. The most important feature is that such a sequence is created in the deterministic manner that is based on the input source. In other words, in the case of two identical generators with the same input, both output random sequences are the same.

In order to increase the security of this system both the transmitter and the receiver should use secret private key as the input to their generators [8]. Randomly generated numbers are from 0 to T_{max} and determine the distance between symbols. Scheduled to have modified cyclic prefixes this allows system dependency on a secret that is known only to the hidden transmission parties.

The synchronization between the transmitter and the receiver is the time of the pseudo-random number sequence and the beginning of the hidden transmission. For this purpose, the transmitter must notify the steganographic receiver of setting-up the hidden channel and the message length [9] (number of fragments). After receiving the starting information, both parties generate a random sequence of the desired length and gradually, with an appropriate spacing between modified symbols (prefixes), send fragments of the secret message.

V. SYSTEM PARAMETERS

In case of BPSK modulation the code rate is $1/2$, for a single transmitting antenna of 20 MHz [10] channels. Here if the $GI_{TCP} = 0.8 \mu s$ (i.e. $T_{sym} = 4 \mu s$) there are symbol rate = 250,000 OFDM symbols per second transmitted. Each symbol carries 52 coded bits (NCBPS) and half of them are data bits (NDBPS). From the above example in BPSK modulation, the useful part of the OFDM symbol ($T_u = 3.2 \mu s$) carries 52 bits. Therefore, as in $0.8 \mu s$ of the GI it is possible to carry 13 bits, in the case of the modification of each OFDM symbol and avoiding using error correction coding, it is possible to achieve 3.25 Mb/s capacity of the hidden channel. The capacity can be determined from below mentioned equation[10].

$$C_{MAX} = N_{CBPS} \cdot (T_{CP} / T_u) \cdot S_R \quad (1)$$

Based on the modulation used the maximum capacity is [10]:

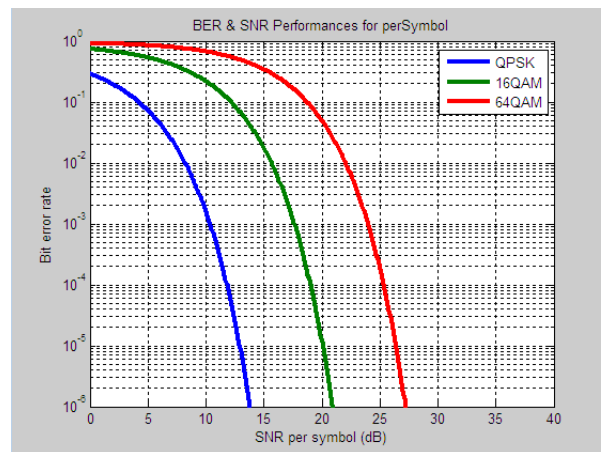
- 3.25 Mb/s when using BPSK modulation.
- 6.5 Mb/s when using QPSK modulation.
- 13.0 Mb/s when using 16-QAM modulation.
- 19.5 Mb/s when using 64-QAM modulation.

In the case of ordinary network users the steganography system user includes an additional cost which results from the interference of the hidden system implemented in the network. In the cyclic prefix technique user don't lose their available bandwidth since the secret information is carried in parts of the OFDM system which are ignored anyway.

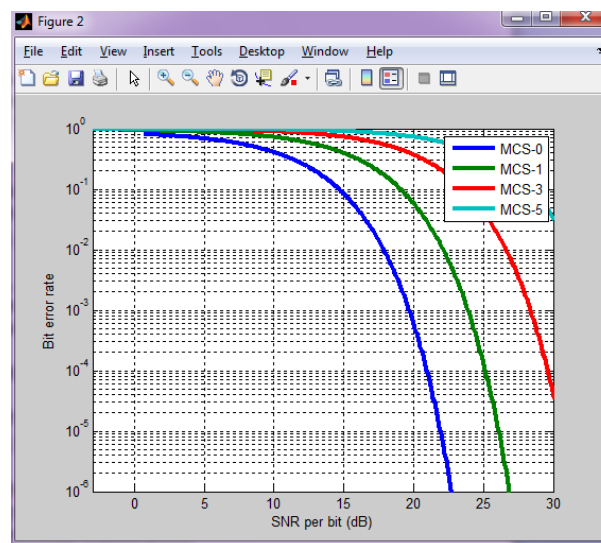
Security is accomplished by the randomized selection of modified symbols that is based on a secret key. Detection (without knowing the key) of the steganographic channel created in the cyclic prefix technique requires observation and study of the cyclic prefixes in every single OFDM symbol in the network. Moreover, such an unauthorized observer should be able to separate and compare the two extremes of the already modulated OFDM symbol. For the casual user, who does not feel the presence of a hidden channel, this task is impossible, especially when the secret message is additionally encrypted.

VI. SIMULATION RESULTS

From Fig.2. It shows that, while using 64-QAM, with SNR = -10 dB and $T_{max} = 0$, gained throughput is greater than 10Mb/s. However, in this case, the BER is too high to read the entire message properly.

Fig. 2 BER as a function of SNR in the hidden channel for the AWGN radio channel model

From Fig.3. We can say that BER as a function of SNR for chosen MCS in the ordinary channel with and without the steganographic system implemented will generate same result. which means the steganographic system hidden transmission uses part of the OFDM symbol which will not uses extra bandwidth which will not demands extra cost.

Fig. 3 BER as a function of SNR with steganographic system implemented.

VI. CONCLUSION

The cyclic prefix steganographic system does not generate any additional cost that ordinary users would incur. The secret private keys, introduced in the system generate random spaces between transmitted hidden message fragments which increases security of the system.

In this system there is a need to set an additional signaling channel that would be used to agree the value of private keys and provide information about the start of transmission.

V. References

- [1] Cho Y., Kim J., Yang W., Kang C., "MIMO-OFDM Wireless Communications with MATLAB", John Wiley & Sons Ltd., 1996.
- [2] Anibal Louis Intini, "OFDM multiplexing for wireless networks", University of California.
- [3] Frikha L., Trabelsi Z., El-Hajj W., "Implementation of a Covert Channel in the 802.11 Header", Proc. Wireless Communications and Mobile Computing Conference (IWCMC 08), 6–8 Aug. 2003, pp. 594–599, doi: 10.1109/IWCMC.2003.103.
- [4] Szczypiorski K., "A Performance Analysis of HICCUPS – a Steganographic System for WLAN", Proc. International Conference on Multimedia Information Networking and Security (MINES 2010), –20 Nov. 2010, vol. 1, pp. 569–572, doi: 10.1109/MINES.2010.248. 28–54, First Quarter 2009, doi: 10.1109/MCAS.2009.915504.
- [5] Szczypiorski K., "HICCUPS: Hidden Communication System for Corrupted Networks", Proc. 10th International Multi-Conference on Advanced Computer Systems (ACS'2003), 22–24 Oct. 2010, pp. 31–40.
- [6] IEEE Standard 802.11n-2008, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment
- [7] Krätzer C., Dittman J., Lang A., Kühne T., "WLAN Steganography: A First Practical Review", Proc. 8th Workshop on Multimedia and Security, 26–27 Sept. 2009, pp. 17–22, doi: 10.1145/1161366.1161371.

- [8] Paul T., Ogunfunmi T., “Wireless LAN Comes of Age: Understanding the IEEE 802.11n Amendment”, Circuits and Systems Magazine, IEEE, vol. 8, no. 1, pp.
- [9] Title “Fundamentals of wireless communication”. David Tse. Publisher. Cambridge university press 2005.
- [10] Szymon Grabski, Krzysztof Szczypiorski. “Steganography in OFDM Symbols of Fast IEEE 802.11n Networks”, IEEE 2013.

Author profile

¹Santosh, received B.E Degree in Electronics and Communication from Visvesvaraya Technological University in 2011, Currently Pursuing M.Tech Degree in Digital Communication and Networking from Visvesvaraya Technological University in 2014, Department of Telecommunication Engineering, Dayanand Sagar College of Engineering, Bangalore India.

²Vinod B Durdi received BE (Electronics and Communication) from Karnataka University, Dharwad, in 2000. He obtained M.Tech (Digital Communication) from Visvesvaraya Technological University (VTU), Belgaum, in 2003. He is presently pursuing Ph.D from Visvesvaraya Technological University (VTU), Belgaum, India. His research interest includes video processing, wireless networks, network security and chaos communication. He has authored and coauthored the various research papers in major national and international conference proceeding. He is currently Associate Professor in Dayananda Sagar College of Engineering, Bangalore, India.