2013 IEEE Security and Privacy Workshops

Steganography in OFDM Symbols of Fast IEEE 802.11n Networks

Szymon Grabski, Krzysztof Szczypiorski
Institute of Telecommunications
Warsaw University of Technology
Warsaw, Poland
e-mail: s.grabski@divegate.pl, ksz@tele.pw.edu.pl

***Abstract* — This paper presents a proposal of covert steganographic channels in high-speed IEEE 802.11n networks. The method is based on the modification of cyclic prefixes in OFDM (Orthogonal Frequency-Division Multiplexing) symbols. This proposal provides the highest hidden transmission known in the state of the art. This paper includes theoretical analysis and simulation results of the presented steganographic system performance. The simulation performance was compared with other known approaches in the literature.**

Keywords – IEEE 802.11n, network steganography, OFDM, wireless networks

I. INTRODUCTION

The increased interest in networks based on the IEEE 802.11 standards' family, and consequently the growing demand for fast and reliable wireless transmission, have forced standardization units to improve the WLAN standards. Limitations of the existing solutions have related primarily to the security aspects and offered throughput. While the first issue was solved by the IEEE 802.11i extension, significant "acceleration" was given after a few years with the approval of the standard IEEE 802.11n [10]. 802.11-based networks protect users' privacy with advanced cryptographic solutions. However, that users are 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.

This paper aims to present a new method of information hiding which is based on OFDM modulation, typically for IEEE 802.11n networks. This approach is adopted because steganographic channels based on high-speed networks enable more reliable and secure secret communications than older and slower systems.

Additionally, this paper presents an assessment of the proposed channel quality parameters. For this aim and in order to implement the system, we used a modified model of the 802.11n physical layer [8] [9]. That model works with *Simulink* software, which is a part of *The MathWorks' MATLAB* suite and provides reliable communication simulation. Moreover, the proposed system was assessed for its security and detection possibilities.

Finally, based on the results obtained, we compared the properties of the proposed channel with other existing concepts of information hiding.

II. STATE OF THE ART

Network steganography and the problem of hiding information in local area networks were the subject of studies even before the exact definition of network steganography. Therefore, the existing bibliography is vast (almost 200 entries [1]) and the majority is about new hidden channel proposals.

For example, Szczypiorski presented the system HICCUPS [12] assumes information hidding in the intentionally corrupted packets. Moreover, the proposals [3] and [7] are based on the frames headers modifications and hiding secrets in the modified fields. Other, selected major works and techniques were briefly discussed in [14].

From the point of view of this work, it should be recalled that hidden channels can be created on the basis of different layers of the network model [5]. Usage of network or transport layers is therefore very popular. However, the quintessence of network steganography is rather proposals based on medium access control (MAC) sub-layer or physical layer (PHY) because, theoretically, they can provide maximum safety

A steganographic system fully dedicated to IEEE 802.11n networks has not been presented until now. We have some proposals based on OFDM symbols – particularly WiPad [13], were information is hiding in the padding. However, none of existing proposals have been examined in the context of 802.11n networks. Of course, that does not mean that these proposals could not be adapted for such networks.

III. OFDM IN IEEE 802.11N

OFDM modulation is a method that allows simultaneous transmission of independent data streams (e.g. from different users) in a radio channel

As in the case of frequency division multiplexing (FDM), resources are shared by the division of the available bandwidth to a sufficient number of radio channels. In each of these channels, the data streams of each user are transmitted. In the case of OFDM, channel subcarriers are orthogonal to each other. Thanks to that, despite the fact that spectrums of adjacent channels overlap, we do not observe interference among them.

In the radio environment of wireless local area networks, the problem of multipath propagation is common [2]. In such case, the receiver receives not only the signal propagated

DOI 10.1109/SPW.2013.20

directly from the transmitter but also delayed copies of that signal – as a result of reflections from obstacles. Consequently, transmitted OFDM symbols could be affected by such reflected signals, called inter-symbol interferences (ISI). In order to reduce ISI, in OFDM modulation, a special guard interval (GI) is inserted between each pair of symbols [2].

The GI can be formed three in different ways. However, IEEE 802.11 standards implement filling that protection gap with the cyclic prefix. This method involves copying the ending part of each OFDM symbol and adding that copy in front of that symbol – as a GI (Figure 1). 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. In the case of 802.11, it is also the duration of the cyclic prefix (T_{CP}).

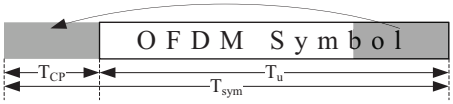

Figure 1. Cyclic prefix generation

Typically, it is assumed that in order to ensure complete orthogonal subcarriers and ISI minimization, the GI duration should be greater than the maximum signal delay caused by multipath propagation. However, in practice, in the case of using OFDM modulation in IEEE 802.11 networks, the GI is assumed to be a constant value $T_{CP} = 0.8$ μs. Optionally, 802.11n allows the shortening of the GI duration to $T_{CP} = 0.4$ μs in the case of good propagation conditions.

IV. PROPOSED SYSTEM

Operation of the proposed steganographic system is based on the existence of a cyclic prefix in the OFDM modulation. In the normal network its implementation improves the quality of the transmission. However, the cyclic prefix is not read or interpreted by radio receivers. The GI is, therefore, relevant only in terms of radio propagation but its content is completely ignored.

In order to hide information, the proposed steganographic system changes the cyclic prefixes of the chosen OFDM symbols and turns them into fragments of the secret message. In the standard network, the prefix is added before symbol transmission but after its modulation. A steganographic transmitter placed in the right place could, therefore, easily modify prefixes. While 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). The currently used MCS depends on the number of antennas and the conditions in the radio channel. It is chosen in such a way as to obtain the maximum possible bandwidth in a given environment at a given moment. The proposed system modifies the cyclic prefix at the physical layer. Therefore, fragments of the secret message must also be modulated. Intuitively, it seems that the safest method is to use the modulation in accordance with the MCS currently used in the network. However, due to the fact that the hidden channel has a much smaller bandwidth available in relation to the standard channel, from the point of view of the steganographic channel, it is better to skip error coding of hidden information.

With such a specified general formula of the steganographic transmitter operation, there is the problem of choosing antennas and transmitted OFDM symbols whose prefixes are to be modified. Additionally, the need to finding and read these modified symbols in the steganographic receiver must be taken into account. For this purposes, both the transmitter and the 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 the proposed system, both the transmitter and the receiver need to use a secret private key as an input of their generators. This allows system dependency on a secret, that is known only to the hidden transmission parties, and increases security of that system. Randomly generated numbers are from 0 to T_{max} and determine the distance between symbols scheduled to have modified cyclic prefixes (Figure 2). When sending hidden information, modified symbols carrying secret fragments are therefore distributed randomly in time.

An important element of the proposed system in terms of 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 (number of fragments). This information may be sent to an open channel or to the hidden steganographic channel of another type. 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.

In the case of selection the antenna that currently transmits modified symbols – similar solution could be implemented. However, the IEEE 802.11n standard limits the number of antennas to four, so such a solution would be an unnecessary complication. Of course, this is an additional protection for the hidden channel. Nevertheless, this solution is optional and is not examined in later work as it has no effect other than on the steganographic system's security parameters.

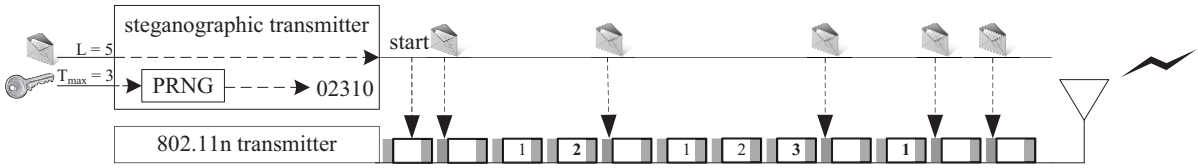

Figure 2. Proposed steganographic system operation

V. SYSTEM'S PARAMETERS

The most basic MCS specified in the standard is MCS-0. It uses BPSK modulation, code rate 1/2, a single transmitting antenna and the 20 MHz channels [6]. In this case, if the GI T_{CP} = 0,8 μs (i.e. T_{sym} = 4 μs) there are S_R = 250,000 OFDM symbols per second transmitted. Each symbol carries 52 coded bits (N_{CBPS}) and half of them are data bits (N_{DBPS}). Then, the achieved network throughput is 6.5 Mb/s.

As can be seen in the above example, in the case of BPSK modulation, the useful part of the OFDM symbol (T_u = 3.2 μs) carries 52 bits. Therefore, as in 0.8 μs 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. In general, this can be determined from the equation:

$$C_{max} = N_{CBPS} \cdot \frac{T_{CP}}{T_u} \cdot S_R . \qquad (1)$$

Depending on the used modulation, the proposed steganographic system allows for a maximum capacity of:

- 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.

For the safety reasons and according to the proposition assumptions, the system should modify the prefixes of randomly selected OFDM symbols. The hidden channel capacity is therefore determined by the number of modified symbols in time (N_{MSPS}). These values are dependent on the range of random numbers (T_{max} parameter) and the random variable.

When generating the random sequence using the uniform distribution, where each number is equally probable, the expected value of such a lot is simply the arithmetic average of the draw limits. The expected value of the modified number of symbols in time is independent of modulation and equals:

$$N_{MSPS} = \left\lceil \frac{S_R}{\frac{T_{max}}{2}+1} \right\rceil , \qquad (2)$$

where ⌈x⌉ is a ceiling of x.

The expected throughput (C_{EX}) of the hidden channel is, however, dependent on the number of bits that can be transmitted in the single cyclic prefix. Therefore, the applied modulation scheme affects the reached throughput and equals:

$$C_{EX} = N_{MSPS} \cdot N_{BPCP} = \left\lceil \frac{S_R}{\frac{T_{max}}{2}+1} \right\rceil \cdot N_{BPCP}, \qquad (3)$$

where N_{BPCP} is the number of bits which can be transmitted in the single cyclic prefix for the given modulation.

With the increase in the T_{max} parameter, in time a significant (exponential) decrease in the expected number of prefixes modified can be seen and, in consequence, the expected throughput. At the same time, increasing the parameter makes the steganographic system safer as the distribution of OFDM symbols with modified prefixes seems to be more "casual".

In the same way, two extreme cases can be shown – optimistic, in which each drawing gives a zero gap between the modified symbols; and the pessimistic, where the gap has the maximum possible value (T_{max}). Of course, in this case "optimism" and "pessimism" should be understood in terms of the hidden channel's capacity, rather than its safety.

It should be kept in mind that optimistic system capacity is also a particular case where T_{max} = 0 so each OFDM symbol has a modified cyclic prefix.

From the perspective of the ordinary network users, the steganographic system implementation may involve an additional cost. It results from the interference of the hidden system (which is not specified in the standard) implemented in the network. In the proposed case, users do not lose their available bandwidth as the secret information is carried in parts of the OFDM systems that are ignored anyway. In addition, modification of the cyclic prefix should not expose transmitted symbols to interferences as the duration of the GI is maintained. Therefore, the proposed hidden channel does not influence the public channel and does not involve any additional cost. This is an advantage of the hidden channel which characterizes only a very small group of steganographic systems.

Security of the proposed system is ensured by the implementation of a randomized selection of modified symbols that is based on a secret key. Detection (without knowing the key) of the steganographic channel created in the proposed way 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. HIDDEN CHANNEL SIMULATION

To test the IEEE 802.11n network, its behaviour under the influence of the steganographic system and the parameters of that system, dedicated simulations were prepared. Each simulation is based on a model [9] which was prepared by Ogunfunmi and Paul from Santa Clara University, California. It is also an improved version of the model [8] by the same authors. All model simulations and modifications have been developed in *Simulink 7.0* which cooperates with the numerical package *MATLAB version R2007b* (7.5.0.342).

The model used allows simulation of the physical layer (PHY) of the IEEE 802.11n network in various configurations. The model is simplified by assumptions that are discussed in detail in [10], as well as by the theoretical basis.

In order to test the performance of the proposed steganographic system in simulation, a standard network model was appropriately modified by implementing additional elements responsible for steganography.

In the implementation of the presented steganographic system and in further simulations, we used a radio channel model with additive white Gaussian noise (AWGN).

VII. SIMULATION RESULTS

The most interesting relation is the dependency of expected steganographic system capacity on the T_{max} parameter. Such an observation allows the hidden channel configuration to be adjusted to individual needs, taking into account the trade-off between secret transmission speed and hidden channel security.

The simulation was prepared in the channel without noise in order to imitate ideal propagation conditions. Such an approach allows the results of theoretical analysis and simulation to be compared. The relation between the capacity of the system and the T_{max} parameter was examined for the T_{max} range of 0 to 30.

The values obtained during the simulation (Figure 3b) agree with the theoretical, calculated values (Figure 3a). Slight variations in the simulation results from the theoretical values are caused by a random variable implemented in the system. According to the theory of probability, with an infinite simulation time, those two graphs would be the same.

As mentioned before, simulations that allow determination of the expected throughput were carried out for the perfect radio environment. In order to take radio channel noise into account, we also examined the dependency of the hidden channel's goodput on the signal-to-noise ratio (SNR). These simulations were carried out on the two cases. In the first case, we assumed $T_{max} = 0$ (Figure 4a), which is the extreme where each OFDM symbol is modified. In the second case, $T_{max} = 5$ was assumed (Figure 4b). That value of the T_{max} parameter seems to be the optimal from the point of view of the trade-off between security and the hidden transmission speed.

It is easy to see that the results obtained during both mentioned simulations correspond to each other (Figure 3 and Figure 4). In the case of the good conditions in the radio channel, the effective capacity of the steganographic channel equals its expected capacity for the given T_{max}.

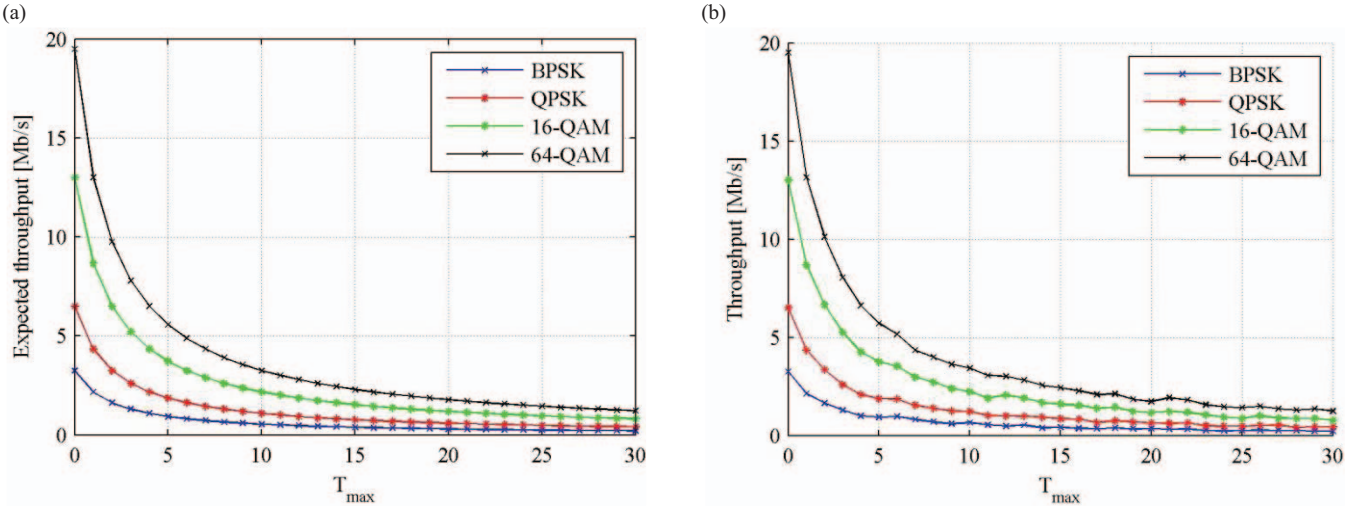

Figure 3. Hidden channel throughput as a function of T_{max} parameter – theoretical (a) and as a simulation result (b)

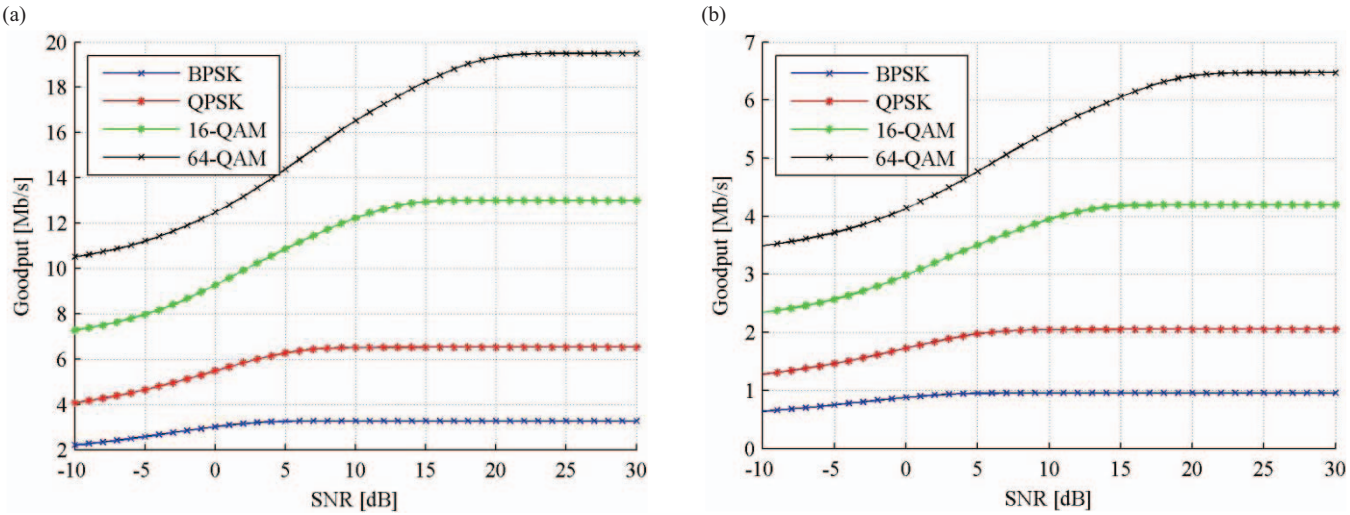

Figure 4. Hidden channel goodput as a function of SNR for T_{max} = 0 (a) and T_{max} = 5 (b)

Depending on the modulation used in the hidden channel, its resistance to radio interference is different. The secret transmission with the maximum possible for that system speed is available for 64-QAM modulation. However, that requires very good conditions of propagation and SNR ≥ 20 dB. Several times slower BPSK modulation allows correct data receiving with SNR = 4 dB. However, keep in mind that, in accordance with the proposed steganographic system assumptions, the hidden data should be modulated with the same modulation as specified in the current MCS used in the network, avoiding, of course, correction coding.

Notice that there is a high risk of misinterpretation of the dependency between the hidden channel and SNR (Figure 4). In low radio propagation conditions, the bit error rate (BER) is very high; hence the possibility of the correct signal detection decreases. The presented graph indeed shows a large number of correctly received bits in time. However, in the case of such a high error rate and data stream as in a series of ones and zeros, each correct bit is the result of a 50% chance of a correct "hit". In fact, an interpretation of the whole steganogram in this case would, of course, be impossible.

To illustrate the problem more accurately it is better to use another relationship – dependency between BER and SNR (Figure 5). For example, while using 64-QAM, with SNR = -10 dB and T_{max} = 0, gained throughput is greater than 10 Mb/s (Figure 4). However, in this case, the BER is too high to read the entire message properly (Figure 5).

In order to confirm the lack of theoretical cost resulting from the implementation of the steganographic system in the network, we compared dependency on BER from SNR in the ordinary channel in two cases – with (Figure 6a) and without (Figure 6b) the hidden channel implemented. Both graphs are the same, it is impossible to discern any difference. That fact confirms that the proposed steganographic channel has no influence on the wireless network. Since, according to the proposition, hidden transmission uses the part of the OFDM symbol that is rejected in the receiver anyway, there is also no mention of the cost associated with the loss of normal users' bandwidth. Additional simulations are, therefore, unnecessary.

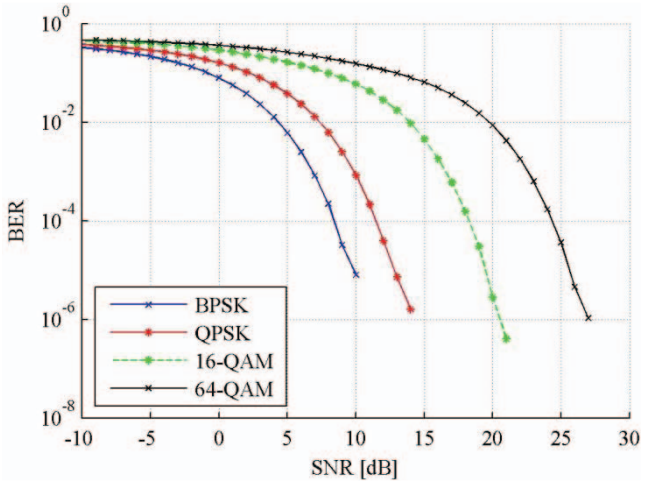

Figure 5. BER as a function of SNR in the hidden channel for the AWGN radio channel model

Finally, it needs to be said that there is a difference in dependencies on BER from SNR in the case of the ordinary channel (Figure 6) and the hidden channel (Figure 5). It is easy to see that the hidden channel is more sensitive to interferences in the radio channel. It is an obvious consequence of the resignation of error coding in the steganographic system. Nevertheless, keep in mind that even error coding with the lowest possible ratio R = 1/2 would result in a two times lower hidden channel goodput.

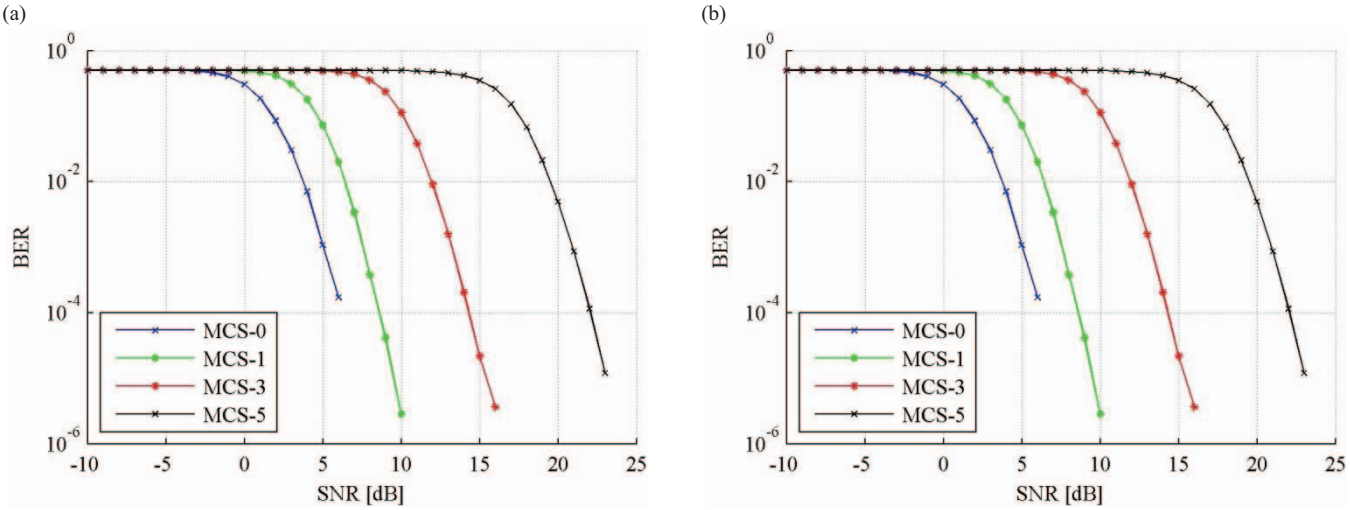

Figure 6. BER as a function of SNR for chosen MCS in the ordinary channel with (a) and without (b) the steganographic system implemented

VIII. CONCLUSIONS

The parameters of the proposed steganographic system were compared to the most important systems known to the authors that are based on the wireless networks of the IEEE 802.11 standards. A summary of the performance parameters for all of these systems is presented in Table I below.

TABLE I. PARAMETERS' COMPARISON OF 802.11-BASED STEGANOGRAPHIC SYSTEMS

Steganographic system	Parameter		
	Capacity	*Cost*	*Detection*
Frikha et al. [3]	max. 24 b/packet	nd	very easy [4]
Krätzer et al. [7] (Scenario I)	16.8 b/s (with delay between modified packets d=0.5 s)	nd	easy [4]
Krätzer et al. [7] (Scenario II)	1.6 b/s	nd	nd
HICCUPS [11][12]	1.27 Mb/s (in IEEE 802.11g, for ΔFER = 0.05)	1.28 Mb/s (in IEEE 802.11g, for ΔFER = 0.05)	theoretically hard [4]
WiPad [13]	1.65 Mb/s (in IEEE 802.11g)	0	theoretically hard
Cyclic prefix	from 3.25 Mb/s to 19.5 Mb/s for T_{max} = 0, depending on modulation	0	theoretically hard

The most distinct difference is the capacity of the hidden channel. According to current knowledge and the literature known to the authors, the proposed system is the fastest steganographic system to date. Its throughput is greater even than WiPad [13], which can offer up to 1.65 Mb/s of secret capacity in an IEEE 802.11g network.

Most importantly, the hidden channel based on cyclic prefixes does not generate any additional cost that ordinary users would incur. It is also characterized by a very high level of security that can even be configured by the user with the parameter T_{max}.

An important aspect of the hidden channel's security is secret private keys, introduced in the algorithm, which generate random spaces between transmitted hidden message fragments.

The disadvantage of the presented system is the need to set an additional signalling channel that would be used to agree the value of private keys and provide information about the start of transmission.

The basic conclusion based on the presented comparison is the supremacy of low-level steganography that operates on the lowest layers of the network model. Covert channels assembled at the physical layer appear to be the essence of the concept of network steganography.

IX. FURTHER WORK

Further diverse work on steganography in IEEE 802.11n should be carried out. First of all, work should focus on the further development and improvement of the proposals presented so far.

In addition, an important aspect of research is the implementation of the proposed steganographic channel in the existing network and the investigation of the actual performance of this system in the real environment. With the current knowledge on network steganography, we can see the need to build a real (not theoretical) and secure steganographic system that allows hidden data transmission. Such a system should be based on a number of concepts to create steganographic channels simultaneously and also on cryptographic techniques.

REFERENCES

[1] http://www.stegano.net/bibliography.html

[2] Cho Y., Kim J., Yang W., Kang C., "MIMO-OFDM Wireless Communications with MATLAB", John Wiley & Sons Ltd., 2010

[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. 2008, pp. 594–599, doi: 10.1109/IWCMC.2008.103

[4] Grabski S., Szczypiorski K., “Steganography Detection in Wireless Local Area Networks”, in Polish, The National Symposium Telecommunications and Teleinformatics (KSTiT 2012), Warsaw, 12–14 Sept. 2012, Telecommunication Review and Telecommunication News, vol. LXXXV, no. 8–9/2012, 2012, pp. 809–820

[5] Handel T., Sandford M., “Hiding Data in the OSI Network Model”, In Information Hiding, vol. 1174 (1996), pp. 23–38, doi: 10.1007/3-540-61996-8_29

[6] IEEE Standard 802.11n-2009, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 5: Enhancements for Higher Throughput”, 2009

[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. 2006, pp. 17–22, doi: 10.1145/1161366.1161371

[8] Ogunfunmi T., “Simulink Model of the IEEE 802.11n PHY Layer Model”, http://www.mathworks.com/matlabcentral/fileexchange/22137-simulink-model-of-the-ieee-802-11n-phy-layer-model, 17 Nov. 2008

[9] Ogunfunmi T., “IEEE 802.11n WLAN File Update”, http://www.mathworks.com/matlabcentral/fileexchange/26232-ieee-802-11n-wlan-file-update, 31 Dec. 2009

[10] Paul T., Ogunfunmi T., “Wireless LAN Comes of Age: Understanding the IEEE 802.11n Amandment”, Circuits and Systems Magazine, IEEE, vol. 8, no. 1, pp. 28–54, First Quarter 2008, doi: 10.1109/MCAS.2008.915504

[11] Szczypiorski K., “A Performance Analysis of HICCUPS – a Steganographic System for WLAN”, Proc. International Conference on Multimedia Information Networking and Security (MINES 2009), 18–20 Nov. 2009, vol. 1, pp. 569–572, doi: 10.1109/MINES.2009.248

[12] Szczypiorski K., “HICCUPS: Hidden Communication System for Corrupted Networks”, Proc. 10th International Multi-Conference on Advanced Computer Systems (ACS’2003), 22–24 Oct. 2003, pp. 31–40

[13] Szczypiorski K., Mazurczyk W., “Hiding Data in OFDM Symbols of IEEE 802.11 Networks”, Proc. International Conference on Multimedia Information Networking and Security (MINES 2010), 2010, pp. 835–840, doi: 10.1109/MINES.2010.177

[14] Szczypiorski K., “Steganography in Local Wireless Networks”, in Polish, PhD Thesis, Warsaw University of Technology, Warsaw, Sept. 2006