Steganography in Long Term Evolution Systems

Iwona Grabska, Krzysztof Szczypiorski
Institute of Telecommunications
Warsaw University of Technology
Warsaw, Poland
e-mail: {i.grabska, ksz}@tele.pw.edu.pl

Abstract — **This paper contains a description and analysis of a new steganographic method, called LaTEsteg, designed for LTE (Long Term Evolution) systems. The LaTEsteg uses physical layer padding of packets sent over LTE networks. This method allows users to gain additional data transfer that is invisible to unauthorized parties that are unaware of hidden communication. Three important parameters of the LaTESteg are defined and evaluated: performance, cost and security.**

Keywords – 4G, LTE, Steganographic Algorithm, Steganographic Channel, Steganography

I. INTRODUCTION AND STATE OF THE ART

LTE technology is currently enjoying huge popularity in wireless networking and helps in introducing services that could not be previously offered in cellular systems like high definition video transmission or VoD (Video on Demand) ([8], [15], [19]). With growing popularity of these services and the possibility of very fast wireless transmission, LTE systems are becoming the perfect carriers for steganography [12].

There are many proposals for steganographic systems designed for different types of networks. Most methods are based on the most popular and commonly used protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol) or VoIP (Voice over Internet Protocol), which can be combined with standard networks like WiFi (Wireless Fidelity) [17]. One can observe first proposals of steganographic systems dedicated for LTE as can be found in [14], where usage of padding was used to develop additional covert channels. However, that steganographic systems where not evaluated well, especially by network simulations.

The idea of using the padding is also presented in this paper, however, padding-based steganographic system for LTE were additionally tested and assessed for performance and efficiency. The presented system was also implemented in the simulation environment.

The idea of using padding for covert channels was also presented for other types of wireless networks: WiFi (method called WiPAD) [18] and for WiMAX [13]. Moreover, first implementation of LTE physical layer in FPGA was presented [11] and gives the opportunity for further work to implement presented steganographic system in the real network and make them evaluated not only in simulation environment.

II. LTE STANDARD

The presented steganographic system uses the frequency division duplex (FDD) mode of LTE, where downlink and uplink transmission takes place at the same time in a separate frequency channel. Each FDD transmission frame (T_{frame} = 10 ms) consists of two time slots (T_{slot} = 0.5 ms). In the frequency domain such an FDD frame is divided into 15 kHz subcarriers. The maximum number of subcarriers is, therefore, not a constant value but depends on the width of the available bandwidth ([2], [1]).

Every single time slot consists of 7 OFDM (Orthogonal Frequency-Division Multiplexing) symbols with the useful duration of 66.7 μs. In the frequency domain, such a slot contains exactly 12 subcarriers with a total width of 180 kHz (12 * 15 kHz). This slot – resource block (RB) – is the basic unit for the allocation of the transmitted data. The network assigns to its users not a single RB unit but a pair of units belonging to one subframe. Therefore, N_{RB} as used in this paper stands for the number of allocated RB pairs, rather than their total number.

Depending on the size of resources allocated to the user, the base station places data for that user in appropriate RBs. Information about the localization of those RBs is sent via another physical channel so that the user's receiver is able to locate and read these blocks.

The data size that the user can send using the resources assigned to him is well defined. 3rd Generation Partnership Project (3GPP) standardization documents contain a list of available modulation and coding schemes (MCSs). Twenty-eight out of 31 defined proposals of these schemes are used. Each MCS with the index I_{MCS} has an I_{TBS} parameter assigned. That parameter defines the size of a data block that can be sent in the channel – depending on the size of resources allocated to the user (N_{RB}). Such a defined data block is called a transport block (TB) [3].

III. THE PROPOSAL OF LATESTEG

During the normal operation of the LTE system, padding fields consist of sequences of zeroes. Immediately after receiving the frame, these sequences are rejected by the receiver as unnecessary bits without relevant user information. The principle of the presented steganographic system is to create a hidden transmission channel by placing an additional amount of information in the padding field – instead of the zeroes.

DOI 10.1109/SPW.2014.23

The LTE system is based on packet transmission with the use of an IP protocol [4]. Each of the IP packets (of a variable length) that should be delivered to users is properly formatted in the transmitter of the base station. Each IP packet is, therefore, processed by the packet data convergence protocol (PDCP) [7], radio link control (RLC) [6] and medium access control (MAC) [5] layers, having an important impact on the final size of the padding.

Estimations of the effectiveness of the presented steganographic system were based on a number of assumptions:

- the LTE system works in the unacknowledged mode (UM) and acknowledged mode (AM);
- there is no IP header compression in the PDCP layer;
- fragmentation in the RLC layer is used only when the total size of the MAC protocol data unit (MAC PDU) is larger than the available TB;
- concatenation of the RLC service data units (RLC SDU) is used only in cases where adding the whole next SDU unit (without its fragmentation) does not cause the unit to exceed the available TB size.

The scheme of the creation of the TBs in the transmitter, with the padding field marked, is presented in Figures 1 and 2.

In this paper the following designations are used:

- L_{IP} – the size of the currently transmitted IP packet (in bytes);
- $L_{H\text{-}PDCP}$ – the size of header added to the PDCP SDU in PDCP layer ($L_{H\text{-}PDCP} = 2$ bytes);
- $L_{H\text{-}RLC}$ – the size of the header added in the RLC layer:

$$L_{H-RLC} = \begin{cases} 2, & \text{for } k = 1 \\ 2{,}5 + 1{,}5 * k, & \text{for } k = \{3, 5, 7, \dots\}, \\ 2 + 1{,}5 * k, & \text{for } k = \{2, 4, 6, \dots\} \end{cases} \quad (1)$$

where k is the number of RLC SDU units included in one RLC PDU unit;

- $L_{H\text{-}MAC}$ – the size of the header added in the MAC layer. It consists of MAC subheaders designed for individual MAC SDU units contained in the MAC PDU unit and padding field (if there is one):

$$L_{H-MAC} = \begin{cases} 1, & \text{for } n = 1, L_{PAD} = 0 \\ L_{SH-MAC} * (n-1) + 1, & \text{for } n > 1, L_{PAD} = 0, \\ L_{SH-MAC} * n + 1, & \text{for } n \geq 1, L_{PAD} \neq 0 \end{cases} \quad (2)$$

where n is the number of MAC SDU units included in one MAC PDU unit and the size $L_{SH\text{-}MAC}$ of the subheader depends on the current MAC SDU size:

$$L_{SH-MAC} = \begin{cases} 2 \text{ bytes}, & \text{for } L_{MAC\ SDU} \leq 128 \text{ bytes} \\ 3 \text{ bytes}, & \text{for } L_{MAC\ SDU} > 128 \text{ bytes} \end{cases}; \quad (3)$$

- L_{PAD} – the size of the padding field in the MAC PDU unit (in bytes);
- BR – hidden channel capacity;
- TB_{SIZE} – the size of the TB. It depends on the resources assigned to the user and on the currently used MCS (in bytes);

Depending on the size L_{IP} of the currently transmitted IP packet, that packet is appropriately formatted so it can be transmitted in the radio channel and delivered to the receiver.

If the following condition is satisfied:

$$L_{IP} + L_H \leq TB_{SIZE}, \quad (4)$$

where:

$$L_H = L_{H-PDCP} + L_{H-RLC} + L_{H-MAC} \quad \text{for } n = 1, l = 1, L_{PAD} = 0,$$

so the length of IP packet with all basic headers added in each layer does not exceed the available TB, then fragmentation of the IP packet is not needed.

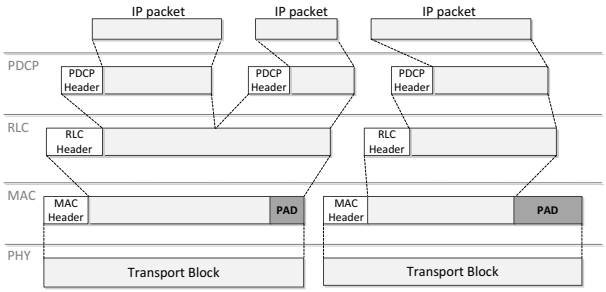

Figure 1. Construction of the transmitted TBs – using RLC SDU concatenation (source: [8])

The maximum number of IP packets N_{MAX} that are included in the given TB equals:

$$N_{MAX} = \left\lfloor \frac{TB_{SIZE} - L_{H-MAC} - L_{H-RLC}}{L_{IP} + L_{H-PDCP}} \right\rfloor, \quad (5)$$

where $\lfloor X \rfloor$ is the floor of X.

It is necessary to verify the obtained N_{MAX} value. If the size of the newly received unit $L_{IP} + L_H$ is equal to TB_{SIZE}:

$$L_{IP} + L_H = TB_{SIZE}, \quad (6)$$

where:

$$L_H = N_{MAX} * L_{H-PDCP} + L_{H-RLC} + L_{H-MAC} \text{ for } n = 1, k = N_{MAX}, L_{PAD} = 0$$

the assumption of simultaneous transmission of N_{MAX} packets is maintained and:

$$L_{PAD} = 0. \quad (7)$$

However, if: $L_{IP} + L_H < TB_{SIZE}$

where:

$$L_H = N_{MAX} * L_{H-PDCP} + L_{H-RLC} + L_{H-MAC} \text{ for } n = 1, k = N_{MAX}, L_{PAD} \neq 0$$

the number of simultaneously transmitted packets is also N_{MAX}, but the size of the padding is not zero and:

$$L_{PAD} = TB_{SIZE} - [N_{MAX} * (L_{IP} + L_{H-PDCP}) + L_{H-RLC} + L_{H-MAC}] \quad (8)$$

In other cases the N_{MAX} value is decreased by 1:

$$N_{MAX} = N_{MAX} - 1, \quad (9)$$

until in the newly formed unit (made as in the previous case of the IP packet and additional headers from each layer) Equation (6) or (8) is satisfied. Then, the size of padding reaches (7) or (9).

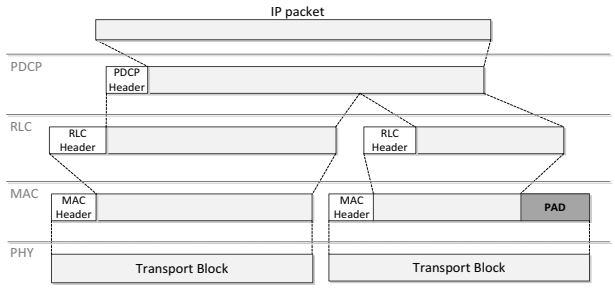

Figure 2. Construction of the transmitted TBs – using IP packet fragmentation (source: [8])

If however, condition (4) is not satisfied, so the IP packet along with its headers is greater than the resources allocated to the user, it is necessary to fragment the transmitted packet on the level of the RLC layer (Figure 2). For this purpose, the received unit (IP packet with PDCP layer header) is divided into q parts. As a result, q TBs are needed to transmit one IP packet:

$$q = \left\lceil \frac{L_{IP}+L_{H-PDCP}}{TB_{SIZE}-L_{H-MAC}-L_{H-RLC}} \right\rceil, \quad (11)$$

where $\lceil X \rceil$ is the ceiling of X.

Using q TBs, there are two possible variants of the network operation. The first corresponds to the following condition satisfying:

$$L_{IP} + L_H = q * TB_{SIZE}, \quad (12)$$

where:

$L_H = L_{H-PDCP} + q * L_{H-RLC} + q * L_{H-MAC}$ for $n = 1, k = 1, L_{PAD} = 0$.

This is the situation, where exactly q TBs are needed in order to transmit an IP packet of the length of L_{IP}. Therefore,

$$L_{PAD} = 0. \quad (13)$$

The second case corresponds to the condition:

$$L_{IP} + L_H < q * TB_{SIZE}, \quad (14)$$

where:

$$L_H = L_{H-PDCP} + q * L_{H-RLC} + q * L_{H-MAC}$$

for

$$\begin{cases} n = 1, k = 1, L_{PAD} = 0, & \text{in case of first } q-1 \text{ TBs} \\ n = 1, k = 1, L_{PAD} \neq 0, & \text{in case of } q^{th} \text{ TB'} \end{cases}$$

which corresponds to the situation where the last used TB is not fully filled with the bits from the IP packet and attached headers. Therefore, a newly created transmission unit must be appropriately padded. Padding obtained in that way (counted as the number of padding bytes per TB) has the length of:

$$L_{PAD} = \frac{TB_{SIZE}-L-L_{H-RLC}-L_{H-MAC}}{q}, \quad (15)$$

where L is the number of bytes from the given IP packet and the attached PDCP layer header that were transmitted in the q^{th} TB. Therefore:

$$L = L_{IP} + L_{H-PDCP} - (q-1) * (TB_{SIZE} - L_{H-MAC} - L_{H-RLC}) \quad (16)$$

The derivation of the relationships (7), (9), (13) and (15) enables the size of padding that corresponds to one TB to be calculated. In addition to the size of the padding, another important parameter that determines the efficiency of the steganographic system is the hidden channel capacity. In this case, the capacity of the proposed steganographic channel is:

$$BR = \frac{L_{PAD}}{T_{frame}}, \quad (17)$$

where L_{PAD} is the size of padding calculated on the basis of (7), (9), (13) and (15), and T_{frame} is the duration of the transmission frame.

IV. The Efficiency of LaTEsteg

Dependencies obtained in the above analysis were used to determine the theoretical efficiency of the LaTEsteg. According to the research [16], the most common IP packets in the network are packet sizes 40 and 1 500 bytes. Therefore, in this work we focus on the analysis of these types of packets.

The results confirm the significant impact of external factors as well as conditions in the network on the size of padding. Therefore, the efficiency of the steganographic system is not constant. Hidden channel capacity depends on:

- the size of IP packet which is to be sent to the user;

- how the packet is formatted in each network layer – the size of the headers of each layer (PDCP, RLC and MAC);
- segmentation usage in the RLC layer;
- the size of the TB, which depends on the MCS used, the conditions of the radio environment and the resources assigned to the user.

Figure 3 illustrates the relationship between the MCS (I_{TBS}) and the obtained padding size and hidden channel capacity for selected sizes of resources assigned to the user (N_{RB} = {30, 90}) and for 40-byte IP packets. A similar relationship for the transmission of 1 500-byte IP packets is presented in Figure 4.

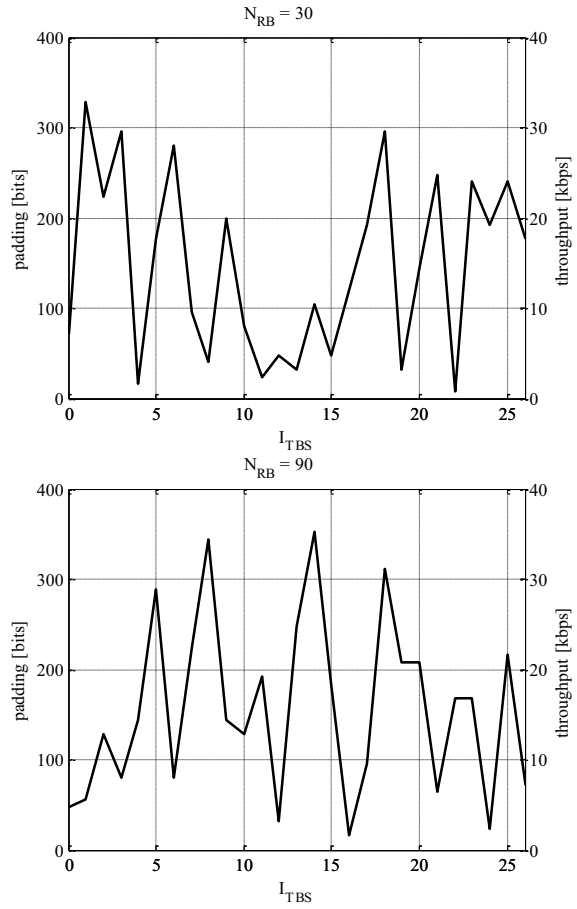

Figure 3. The size of padding and hidden channel capacity as a function of MCS (I_{TBS}) and available resources (N_{RB} ={30,90}) for L_{IP} = 40 bytes

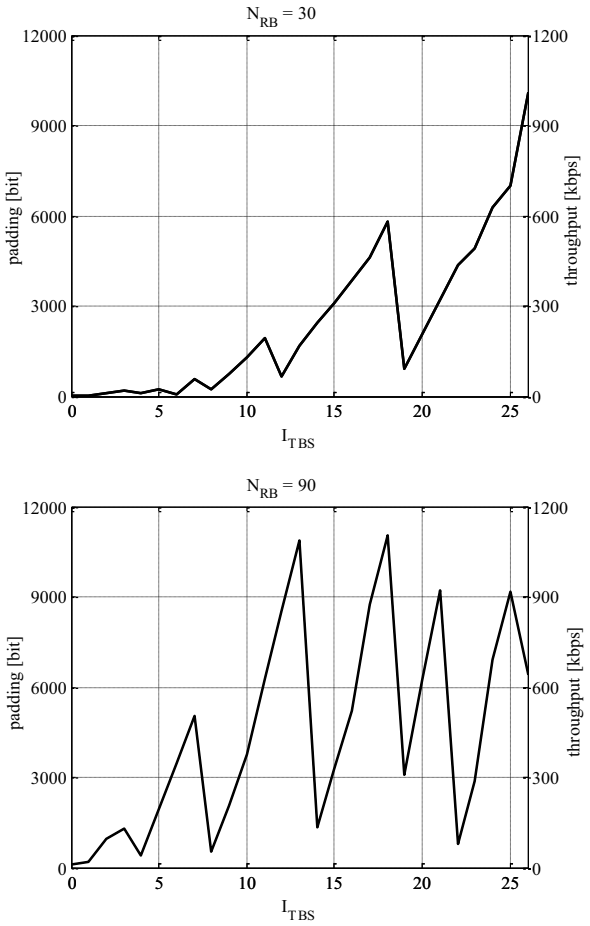

Figure 4. The size of padding and hidden channel capacity as a function of MCS (I_{TBS}) and available resources (N_{RB} ={30, 90}) for L_{IP} = 1 500 bytes

The graphs presented are characterized by significant and dynamic volatility – depending on I_{TBS} (Figures 3 and 4) and N_{RB} (Figure 5). However, regardless of the amount of resources assigned to the user, the size of padding varies considerably and in some cases takes the value 0. Therefore, a large amount of resources does not guarantee high capacity in the hidden channel. Moreover, the size of padding changes with the improvement in the radio environment condition and the MCS used, which influences the TB size. Therefore, the current conditions of the radio channel have a significant impact on the efficiency of the LaTEsteg. Table I presents the results of analyses for significant, specific network conditions and confirms the number of factor affections on the obtained hidden channel capacity.

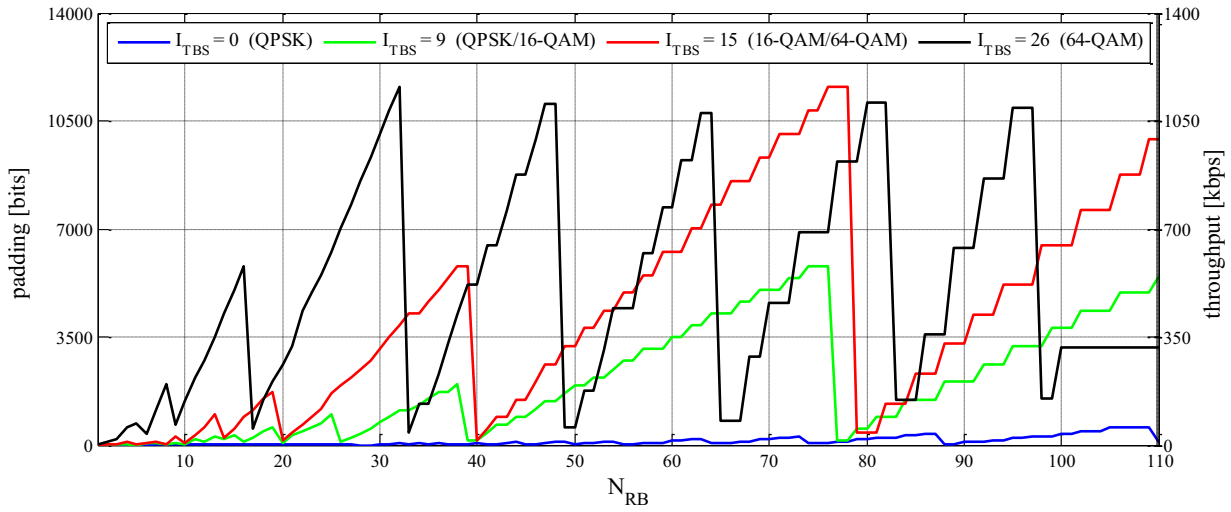

Figure 5. The size of padding and hidden channel capacity as a function of available resources N_{RB} for the chosen MCS (I_{TBS} = {0, 9, 15, 26}) for L_{IP} = 1 500 bytes

TABLE I. STEGANOGRAPHIC SYSTEM EFFICIENCY FOR SELECTED VALUES OF L_{IP}, I_{TBS} AND N_{RB}

	Hidden channel capacity (kb/s)									
	N_{RB} = 1		***N_{RB} = 15***		***N_{RB} = 30***		***N_{RB} = 45***		***N_{RB} = 60***	
L_{IP} [B]	40	1500	40	1500	40	1500	40	1500	40	1500
I_{TBS} = 0 QPSK	TB_{size} = 2 B		TB_{size} = 49 B		TB_{size} = 101 B		TB_{size} = 157 B		TB_{size} = 209 B	
	0.00	0.00	1.60	0.34	7.20	3.20	16.00	2.88	23.20	14.40
I_{TBS} = 9 QPSK 16-QAM	TB_{size} = 17 B		TB_{size} = 293 B		TB_{size} = 597 B		TB_{size} = 871 B		TB_{size} = 1 191 B	
	0.00	0.06	20.80	31.45	20.00	73.87	30.40	92.40	8.00	348.40
I_{TBS} = 15 16-QAM 64-QAM	TB_{size} = 35 B		TB_{size} = 573 B		TB_{size} = 1 143 B		TB_{size} = 1 692 B		TB_{size} = 2 292 B	
	8.00	0.00	0.80	54.67	4.80	310.00	26.40	147.20	19.20	627.20
I_{TBS} = 26 64-QAM	TB_{size} = 89 B		TB_{size} = 1 383 B		TB_{size} = 2 769 B		TB_{size} = 4 107 B		TB_{size} = 5 477 B	
	33.60	1.96	22.40	502.40	17.60	1 009.00	9.60	875.20	26.40	768.00

V. SIMULATION RESULTS

In order to verify and confirm the obtained theoretical results, a number of simulations were carried out. Moreover, such simulations allow the influence of the radio environment conditions on the hidden transmission quality to be checked and the hidden channel safety and the cost of the steganographic system's operation to be evaluated. Simulations were based on the modified LTE system model [9], [10] for Simulink.

Figure 7 shows the hidden channel capacity achieved during the transmission of 1 500-byte IP packets in the standard way for three selected MCSs and depending on the noise power in the radio channel. According to the presented relations, I_{MCS} significantly affects the achieved hidden channel capacity. However, the use of the higher ratio MCS does not guarantee a higher result. For example, in Figure 7, the second case, where I_{MCS} = 15, gives higher hidden transmission throughput than in the case where I_{MCS} = 25.

The parameter which has a significant influence on the hidden transmission quality (the number of correctly received bits for all transmitted bits) is certainly the E_b/N_0 level. With worsening conditions in the radio channel, the number of correctly received bits gradually decreases, thereby the quality and capacity of the hidden transmission is lower.

Using the lower modulation and higher number of redundant bits, the noise in the radio environment has lower influence on the transmitted signal so the possibility of bit detection and correction is higher. In some cases it is possible to avoid any bit errors.

For MCSs with a higher I_{MCS} parameter, the bit error rate decreases much more slowly depending of E_b/N_0 than in the case of a lower I_{MCS}. This is due to the fact that MCSs with a lower index use lower modulations and a higher number of redundant bits. Therefore, in the worst condition of the radio environment, it is possible to detect and correct more errors.

Figure 8 presents the effect of the E_b/N_0 parameter on the bit error rate (BER) obtained in the hidden channel for the chosen MCSs. However, with the use of an MCS of a lower index (for example, I_{MCS} = 9 or I_{MCS} = 10, thus the QPSK and 16-QAM modulations) the BER increases for the same values of E_b/N_0. The reason for this is the difference in the number of redundant bits, which has a significant influence on the ability to detect errors and correct them. We can see a

similar relation in the case of I_{MCS} = 16 and I_{MCS} = 17, where 16-QAM and 64-QAM modulations are used.

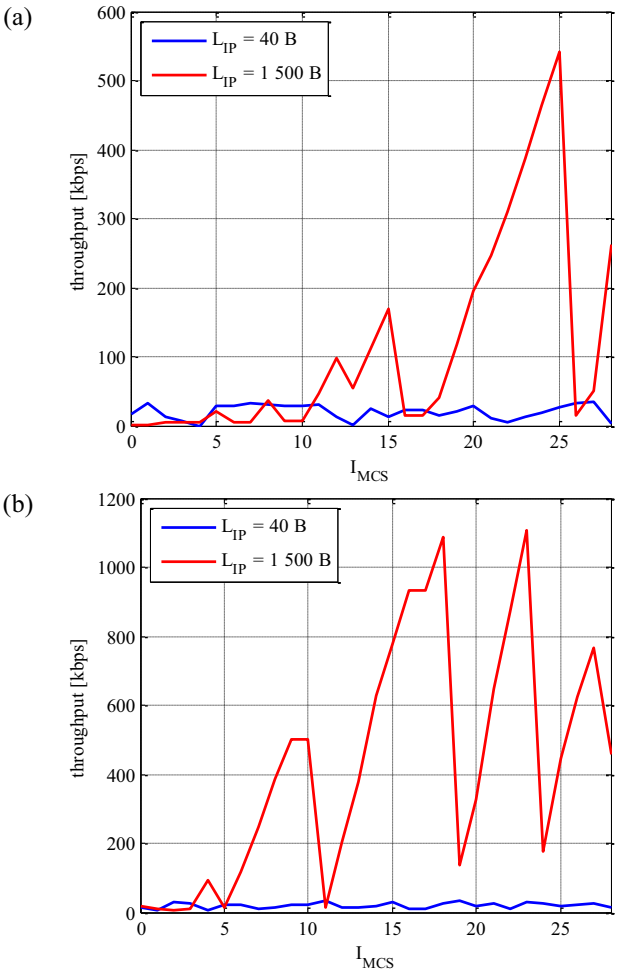

Figure 6. Influence of the MCS used (I_{MCS}) on the hidden channel capacity as a function of IP packet size and available resources – (a) N_{RB} = 20 and (b) N_{RB} = 70

A very necessary aspect of designing a steganographic system is the avoidance of that system's influence on the normal network operation. It is very desirable to have the lowest possible (or no) cost associated with the hidden channel's existence.

In the case of the presented steganographic system, the estimated cost is small. Additional, hidden data are stored in the ignored part of the transmitted frame. Therefore, the hidden transmission does not affect the normal operation of the network and does not generate additional errors. This is confirmed by figures presenting BER as a function of E_b/N_0 in the standard channel in the case of normal network operation (Figure 9a) and in the case of the steganographic system's existence (Figure 9b).

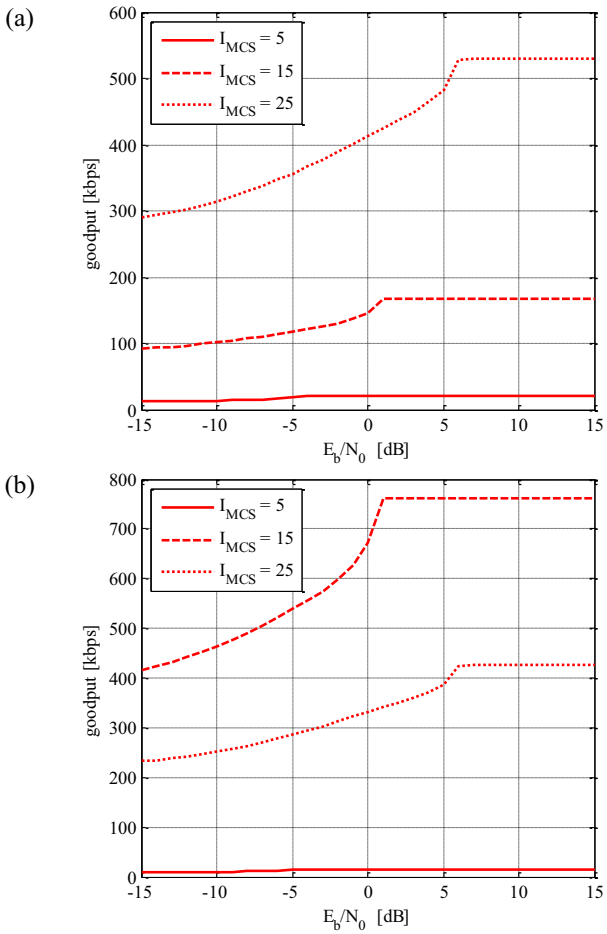

Figure 7. Influence of the radio channel condition (E_b/N_0) on the hidden channel capacity for 1 500-byte IP packets as a function of the MCS used and available resources – (a) N_{RB} = 20 and (b) N_{RB} = 70

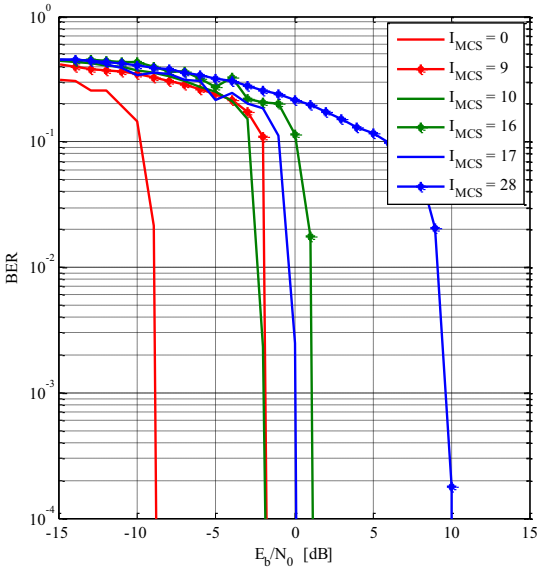

Figure 8. Influence of E_b/N_0 value on BER in the hidden channel for the chosen MCS (I_{MCS} = {0, 9, 10, 16, 17, 28})

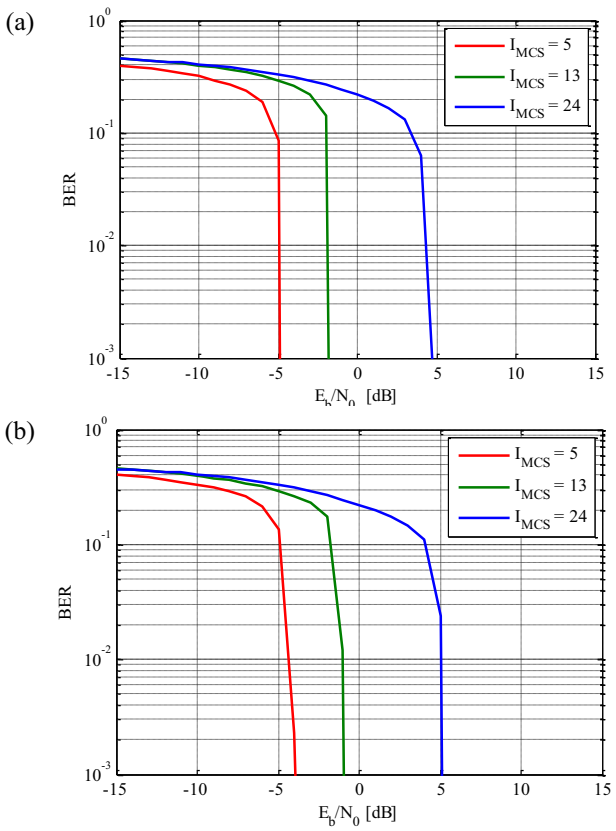

Figure 9. Influence of the E_b/N_0 value on BER in the standard channel – (a) for normal network operation, (b) for simultaneous network and steganographic system operation

VI. CONCLUSIONS

In the LaTEsteg, the maximum achieved hidden transmission speed reached 1.162 Mb/s. However, the effectiveness of the steganographic system depends on many factors which may not be controlled by the hidden-system user, for example, the size of the transmitted IP packet, MCS used or amount of assigned resources. Therefore, hidden channel capacity may be decreased to zero in some cases.

The advantage of the LaTEsteg is the fact that system does not generate any changes in the operation of the LTE system. Therefore, there is no cost of the hidden transmission which makes the proposed steganographic system very secure. Any additional anomalies do not raise suspicion among standard network users, thus hidden transmission is unnoticed. This means that the proposed steganographic system enables safe and effective hidden transmission and has potentially huge range of use.

After some modifications, the proposed steganographic system can be implemented in other types of networks that use padding. However, in such cases, the effectiveness of the system may be different than presented as there are several different factors that influence the parameters of hidden channel. Therefore, the presented steganographic system should be analysed for each type of network that implements that system.

Possible directions for further work and research may be different. The LaTEsteg can be modified in order to obtain even better performance – not only in an LTE system but also in other networks. What is more, that system should be implemented and tested in the environment of real network.

ACKNOWLEDGMENT

This research was partially supported by the Polish National Science Center under grant no. 2011/01/D/ST7/05054.

REFERENCES

[1] "LTE in a Nutshell: The Physical Layer", White Paper, Telesystem Innovations, Canada, 2010

[2] 3GPP TS 36.211, Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation (Release 9), March 2010

[3] 3GPP TS 36.213, Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Layer Procedures (Release 9), September 2010

[4] 3GPP TS 36.300, Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 9), December 2011

[5] 3GPP TS 36.321, Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) Protocol Specification (Release 9), March 2012

[6] 3GPP TS 36.322, Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) Protocol Specification (Release 9), September 2010

[7] 3GPP TS 36.323, Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) Specification (Release 9), December 2009

[8] Dahlman E., Parkvall S., Skold J., Beming P., "3G Evolution: HSPA and LTE Mobile Broadband", Academic Press, Burlington 2008

[9] Guo X., Song P., "Matlab Simulink Based LTE System Simulator", Göteborg, Sweden, 2010

[10] Guo X., Song P., "Simulink Based LTE System Simulator", M. Sc. Thesis, Göteborg, Sweden, 2010

[11] Lenzi, K.G.; Bianco F, J.A.; de Figueiredo, F.A.; Figueiredo, F.L., "Optimized rate matching architecture for a LTE-Advanced FPGA-based PHY" in Proc. IEEE International Conference on Circuits and Systems (ICCAS 2013), 2013 pp. 102-107, doi: 10.1109/CircuitsAndSystems.2013.6671636

[12] Lubacz J., Mazurczyk W., Szczypiorski K., "Network Steganography", Telecommunication Review and Telecommunication News, in Polish, no 4/2010, pp. 134–135

[13] Grabska I., Szczypiorski K.: "Steganography in WiMAX Networks", in Proc. 5th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT 2013), 10-13 September 2013,

[14] Rezaei, F.; Hempel, M.; Dongming Peng; Yi Qian; Sharif, H., "Analysis and evaluation of covert channels over LTE advanced" in Proc. Wireless Communications and Networking Conference (WCNC), 7-10 April 2013, pp. 1903-1908, doi: 10.1109/WCNC.2013.6554855

[15] Sauter M., "From GSM to LTE", John Wiley & Sons, UK, 2011

[16] Sinha R., Papadopoulos C., Heidemann J., "Internet Packet Size Distributions: Some Observations", University of Southern California, Los Angeles, CA, USA (web page released October 5, 2005 republished as ISI-TR-2007-643 May 2007)

[17] Szczypiorski K., "Steganography in Wireless Local Networks", in Polish, Ph. D. Thesis, Warsaw, September 2006

[18] Szczypiorski K., Mazurczyk W., "Hiding Data in OFDM Symbols of IEEE 802.11 Networks", in Proc. International Conference on

Multimedia Information Networking and Security (MINES 2010), 2010, pp. 835–840, doi: 10.1109/MINES.2010.177

[19] The Office of Electronic Communications “Long Term Evolution, the Next Step in the Evolution of Mobile Systems”, in Polish, Warsaw, May 2010