SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2011)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.306

SPECIAL ISSUE PAPER

Steganography in IEEE 802.11 OFDM symbols†

Krzysztof Szczypiorski* and Wojciech Mazurczyk

Warsaw University of Technology, Institute of Telecommunications, ul. Nowowiejska 15/19, 00-665 Warsaw, Poland

ABSTRACT

This paper presents a new steganographic method called wireless padding (WiPad). It is based on the insertion of hidden data into the padding of frames at the physical layer of wireless local area networks (WLANs). A performance analysis based on a Markov model, previously introduced and validated by the authors, is provided for the method in relation to the IEEE 802.11 a/g standards. Its results prove that maximum steganographic bandwidth for WiPad is as high as 1.1 Mbit/s for data frames and 0.44 Mbit/s for acknowledgment frames. To the authors' best knowledge this is the most capacious of all the known steganographic network channels. Copyright © 2011 John Wiley & Sons, Ltd.

KEYWORDS

WLAN; IEEE 802.11; information hiding; OFDM; physical layer

***Correspondence**

Krzysztof Szczypiorski, Warsaw University of Technology, Institute of Telecommunications, ul. Nowowiejska 15/19, 00-665 Warsaw, Poland.
E-mail: ksz@tele.pw.edu.pl

1. INTRODUCTION

Network steganography is currently recognized as a new threat to network security that may be used, among others, to enable data exfiltration or also as the way of performing network attacks. Wireless Local Area Networks (WLANs) described in IEEE 802.11 standards were not recognized as a serious area for data hiding especially because of a limited range (for 802.11a/b/g the range is 30 m indoors and 100 m outdoors, for 802.11n the range is doubled). However, IEEE 802.11 was used to transmit secret data among Russian spies hunted down in the USA in June 2010 [1]. From military perspective WLAN is also one of the several ways of communications among soldiers in a battlefield.

In this paper we present and evaluate a new information hiding method based on bit padding of Orthogonal Frequency Division Multiplexing (OFDM) symbols at the physical layer (PHY) of IEEE 802.11 networks. Depending on the transmission data rate at the PHY layer the number of encoded bits per symbol spans from 24 up to 216, therefore as many as 27 octets can be embedded in each OFDM symbol. Due to the specific structure of a frame (described in detail in Section 3) up to 210 bits per frame (26¼ octets/frame) can be allocated for hidden communication. We named this steganographic method utilizing the principle of frame padding in the PHY of WLANs with the acronym Wireless Padding (WiPad).

This paper provides an evaluation of throughput for this method with the aid of our general, Markov-based model introduced and validated in Ref. [2]. This model is in line with the extensions of Bianchi's basic model [3] proposed in Refs. [2,4]. The essential difference with respect to the latter two is the consideration of the effect of freezing of the stations' backoff timer, as well as the limitation of the number of retransmissions and the maximum size of the contention window, and the impact of transmission errors. Results presented in Ref. [2] proved good accuracy of our model in the case of both: error-free and error-prone channels. In either case the proposed model is more accurate than other models presented in literature with which it was compared (including Refs. [2–4]), most notably, when large numbers of stations are under consideration.

This paper is organized as follows. Next section provides an overview of the state of the art with regard to information hiding techniques that utilize padding in

†This is the extended version of the authors' paper entitled ***Hiding Data in OFDM Symbols of IEEE 802.11 Networks*** presented at Second International Workshop on Network Steganography (IWNS 2010) co-located with The 2010 International Conference on Multimedia Information Networking and Security (MINES 2010), Nanjing, China, 4–6 November, 2010.

Table I. Parameters of 802.11 a/g OFDM PHY.

Rate R [Mbit/s]	Modulation	Code rate	Number of bits per symbol – N_{BpS}	Factorization of N_{BpS} into primes
6	BPSK	½	24	$2^3 3$
9	BPSK	¾	36	$2^2 3^2$
12	QPSK	½	48	$2^4 3$
18	QPSK	¾	72	$2^3 3^2$
24	16-QAM	½	96	$2^4 3$
36	16-QAM	¾	144	$2^4 3^2$
48	64-QAM	⅔	192	$2^6 3$
54	64-QAM	¾	216	$2^3 3^3$

WLANs. Section 3 contains a description of our method. Section 4 is a brief overview of the model presented in Ref. [2] and introduces a performance metric for the proposed method. Section 5 presents a performance analysis of the method based on the given model. Finally, Section 6 contains conclusions and suggestions for future work.

2. STATE-OF-THE-ART

Data padding can be found at any layer of the Open System Interconnection Reference Model (OSI RM), but it is typically exploited for covert communications only in the data link, network and transport layers. Wolf proposed in Ref. [5] a steganographic method utilizing padding of 802.3 frames. Its achievable steganographic capacity was maximally 45 bytes/frame. Fisk *et al*. [6] presented padding of the IP and transmission control protocol (TCP) headers in the context of active wardens. Each of these fields offers up to 31 bits/packet for covert communication. Jankowski *et al*. [7] developed a steganographic system, PadSteg, which is based on Ethernet frames' padding and is used in conjunction with address resolution protocol (ARP) and TCP. Padding of IPv6 packets as means for information hiding was described by Lucena *et al*. [8] – offers a couple of channels with a steganographic bandwidth reaching 256 bytes/packet.

Steganography for IEEE 802.11 was proposed by Szczypiorski [9], who postulated the usage of frames with intentionally corrupted checksums to establish covert communication. The system was evaluated by Szczypiorski [10]. Krätzer *et al.* [11] developed a storage channel based scenario (employing header embedding) and a time channel based scenario for IEEE 802.11. Krätzer *et al.* [12] reconsidered the approach presented in Ref. [11].

3. THE METHOD

IEEE 802.11 a/g standards exploit OFDM at the PHY. 802.11 network's PHY layer consists of two sublayers: PHY Layer Convergance Procedure (PLCP) and PHY Medium-Dependent. Selection of a specific transmission data rate at the PHY layer implies functioning with a predefined number of bits corresponding to each OFDM symbol. The number of bits per symbol may vary from 24, for 6 Mbps, up to 216, for 54 Mbps (Table I). Three fields are liable to padding: SERVICE, Physical layer Service Data Unit (PSDU), TAIL (Figure 1). The lengths of SERVICE and TAIL are constant (16 and 6 bits, respectively), while the PSDU is a medium access control (MAC) frame and its length varies depending on user data, ciphers and network operation mode (ad hoc vs. infrastructure).

For each rate R, the number of bits per symbol can be factorized into primes (Table I) and then, using this knowledge, a least common multiple can be calculated as $2^6\ 3^3 = 1728$. This means that the maximum number of padding bytes (octets) that may be used for all rates is:

$$L_\alpha = \frac{2^6 3^3}{8}\alpha - 2 = 216\alpha - 2 \qquad (1)$$

where α is a positive integer.

Please note that padding is present in all frames, therefore frames that are more frequently exchanged, like ACKs may become an interesting target for covert communication.

Typically all padding bits are set to zero [13], but in this paper we assume that all of them could be used for steganographic purposes.

4. THE MODEL

4.1. Assumptions

We considered saturation conditions: stations have non-empty queues and there is always a frame to be sent. The number of stations competing for medium access is n (for $n = 1$ there is one station sending frames to another station which may only reply with an ACK frame). Errors in the transmission medium are fully randomly distributed; this is the worst-case scenario in terms of *frame error rate* (FER). All stations experience the same bit error rate (BER) and all are within each other's transmission range and there are no hidden terminals. Stations communicate in ad hoc mode (basic service set) with basic access method. Every station employs the same PHY. The transmission data rate R is the same and constant for all stations. All frames are of constant length L. The

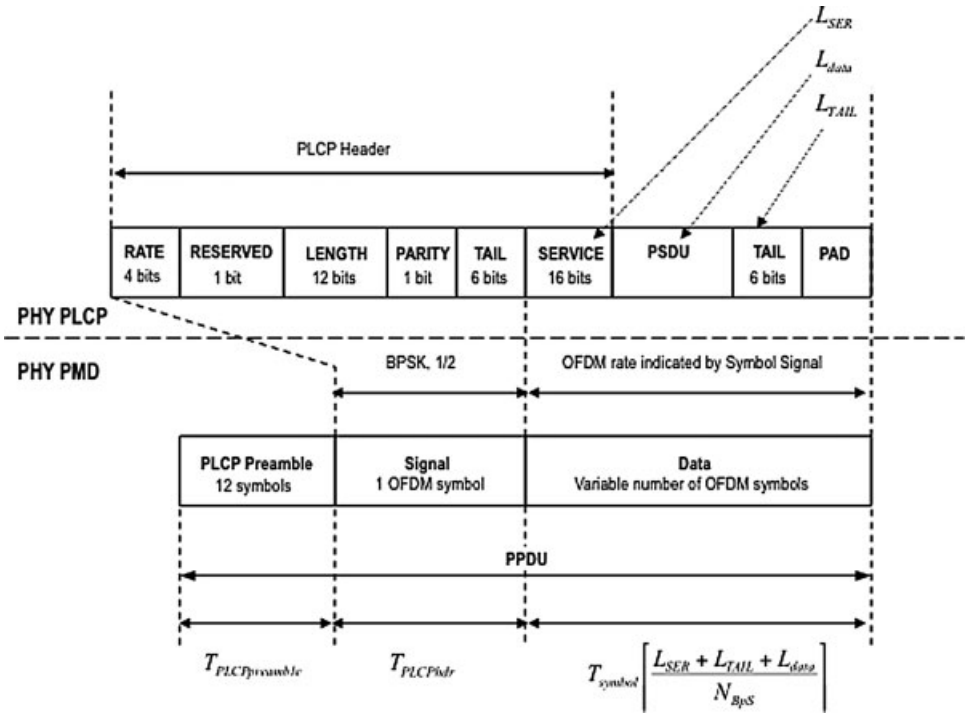

Figure 1. The structure of 802.11a/g PPDU for ERP-OFDM networks.

only frames that are exchanged are data frames and ACK frames. Collided frames are discarded – the capture effect [14] is not considered.

4.2. Saturation throughput *S* expressed through characteristics of the physical channel

The saturation throughput S is defined as in Ref. [2]:

$$S = \frac{E[\text{DATA}]}{E[T]} \tag{2}$$

where E[DATA] is the mean value of successfully transmitted payload, and $E[T]$ is the mean value of the duration of the following *channel states*:

T_{I} – idle slot,
T_{S} – successful transmission,
T_{C} – transmission with collision,
$T_{\text{E\_DATA}}$ – unsuccessful transmission with data frame error,
$T_{\text{E\_ACK}}$ – unsuccessful transmission with acknowledgement (ACK) error.

Figure 2 illustrates dependence of the above channel states on: T_{PHYhdr} – duration of a PLCP preamble and a PLCP header,

T_{DATA} – data frame transmission time,
T_{ACK} – ACK frame duration,
T_{SIFS} – duration of SIFS (short interframe space),
T_{DIFS} – duration of DIFS (DCF interframe space),
T_{EIFS} – duration of EIFS (extended interframe space).

The relation of the saturation throughput to physical channel characteristics is calculated similarly as in Ref. [4]:

$$\begin{cases} T_{\text{I}} = \sigma \\ T_{\text{S}} = 2T_{\text{PHYhdr}} + T_{\text{DATA}} + 2\delta + T_{\text{SIFS}} + T_{\text{ACK}} + T_{\text{DIFS}} \\ T_{\text{C}} = T_{\text{PHYhdr}} + T_{\text{DATA}} + \delta + T_{\text{EIFS}} \\ T_{\text{E\_DATA}} = T_{\text{PHYhdr}} + \delta + T_{\text{DATA}} + T_{\text{EIFS}} \\ T_{\text{E\_ACK}} = T_{\text{S}} \end{cases} \tag{3}$$

where σ is the duration of an idle slot (aSlotTime [13]) and δ is the propagation delay.

For 802.11a/g OFDM PHY (Figure 1):

$$T_{\text{ACK}} = T_{\text{symbol}} \left\lceil \frac{L_{\text{SER}} + L_{\text{TAIL}} + L_{\text{ACK}}}{N_{\text{BpS}}} \right\rceil \tag{4}$$

$$T_{\text{DATA}} = T_{\text{symbol}} \left\lceil \frac{L_{\text{SER}} + L_{\text{TAIL}} + L_{\text{DATA}}}{N_{\text{BpS}}} \right\rceil \tag{5}$$

where:

T_{symbol} – duration of a transmission symbol,
L_{SER} – OFDM PHY layer SERVICE field size,
L_{TAIL} – OFDM PHY layer TAIL field size,
N_{BpS} – number of encoded bits per symbol,
L_{ACK} – size of an ACK frame,
L_{DATA} – size of a data frame.

Values of σ, T_{PHYhdr}, T_{SIFS}, T_{DIFS}, T_{EIFS}, T_{symbol}, N_{BpS}, L_{SER}, and L_{TAIL} are defined in accordance with the 802.11 standard [13].

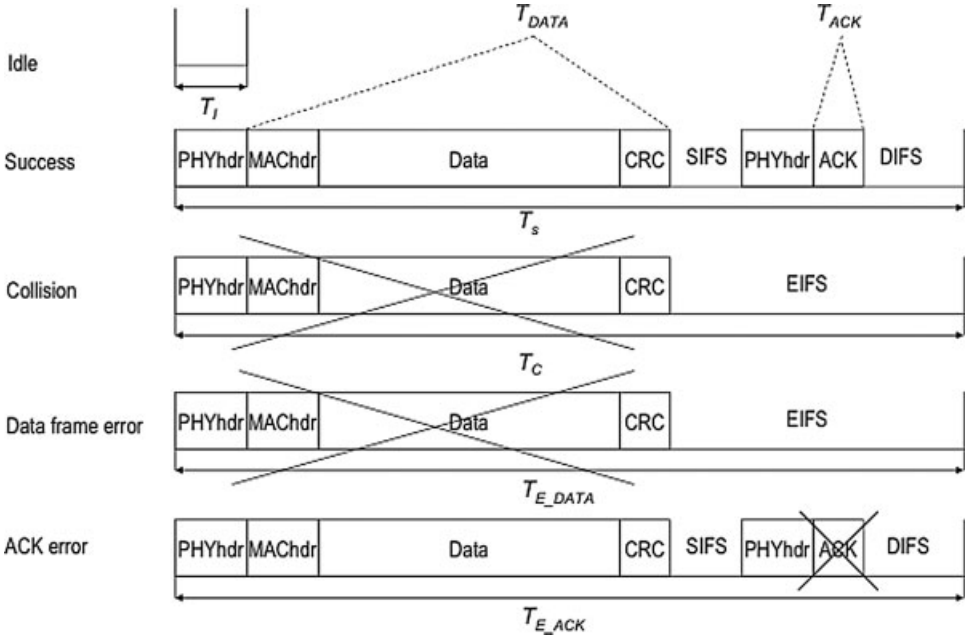

Figure 2. Channel states.

Probabilities corresponding to the states of the channel are denoted as follows:

P_{I} – probability of an idle slot,
P_{S} – probability of successful transmission,
P_{C} – probability of collision,
$P_{\mathrm{E\_DATA}}$ – probability of unsuccessful transmission due to data frame error,
$P_{\mathrm{E\_ACK}}$ – probability of unsuccessful transmission due to ACK error.

Let τ be the probability of frame transmission, $p_{\mathrm{e\_data}}$ the probability of data frame error, and $p_{\mathrm{e\_ACK}}$ the probability of an ACK error. These are related to channel state probabilities as follows:

$$\begin{cases} P_{\mathrm{I}} = (1-\tau)^n \\ P_{\mathrm{S}} = n\tau(1-\tau)^{n-1}(1-p_{\mathrm{e\_data}})(1-p_{\mathrm{e\_ACK}}) \\ P_{\mathrm{C}} = 1-(1-\tau)^n - n\tau(1-\tau)^{n-1} \\ P_{\mathrm{E\_DATA}} = n\tau(1-\tau)^{n-1}p_{\mathrm{e\_data}} \\ P_{\mathrm{E\_ACK}} = n\tau(1-\tau)^{n-1}(1-p_{\mathrm{e\_data}})p_{\mathrm{e\_ACK}} \end{cases} \quad (6)$$

The saturation throughput S equals:

$$S = \frac{P_{\mathrm{S}}L_{\mathrm{pld}}}{T_{\mathrm{I}}P_{\mathrm{I}} + T_{\mathrm{S}}P_{\mathrm{S}} + T_{\mathrm{C}}P_{\mathrm{C}} + T_{\mathrm{E\_DATA}}P_{\mathrm{E\_DATA}} + T_{\mathrm{E\_ACK}}P_{\mathrm{E\_ACK}}} \quad (7)$$

where L_{pld} is MAC payload size and $L_{\mathrm{pld}} = L - L_{\mathrm{MAChdr}}$, where L_{MAChdr} is the size of the MAC header plus the size of a frame checksum sequence.

The data rate R is defined as:

$$R = \frac{N_{\mathrm{Bps}}}{T_{\mathrm{symbol}}} \quad (8)$$

As a result, saturation throughput S is expressed as a function of τ, $p_{\mathrm{e\_data}}$ and $p_{\mathrm{e\_ACK}}$. In the following sections these probabilities are evaluated.

4.3. Probability of frame transmission τ

Let $s(t)$ be a random variable describing DCF backoff stage at time t, with values from set $\{0, 1, 2, \ldots, m\}$. Let $b(t)$ be a random variable describing the value of the backoff timer at time t, with values from the set $\{0, 1, 2, \ldots, W_i\text{-}1\}$. These random variables are correlated because the maximum value of the backoff timer depends on the backoff stage:

$$W_i = \begin{cases} 2^i W_0, & i \le m' \\ 2^{m'} W_0 = W_m, & i > m' \end{cases} \quad (9)$$

where W_0 is the initial size of the contention window (CW) and m' is (the boundary stage above which the contention widow will not be enlarged further); m' can be either greater, smaller or m. W_0 and $W_{m'}$ depend on $\mathrm{CW}_{\min}$ and $\mathrm{CW}_{\max}$ [13]:

$$W_0 = \mathrm{CW}_{\min} + 1 \quad (10)$$

$$W_{m'} = CW_{\max} + 1 = 2^{m'} W_0 \quad (11)$$

The two-dimensional process $(s(t), b(t))$ will be analyzed with the aid of an embedded Markov chain (steady state probabilities), whose states correspond to the time instants at which the channel state changes. Let (i,k) denote the current state of this process. The conditional, one-step, state transition probabilities will be denoted by $P = (\cdot,\cdot|\cdot,\cdot)$.

Let p_f be the probability of transmission failure and p_{coll} the probability of collision. The non-null transition probabilities are determined as follows:

$$\begin{array}{ll}
\text{(a) } P(i,k|i,k+1) = 1-p_{coll}, & 0 \le i \le m,\ 0 \le k \le W_i-2 \\
\text{(b) } P(i,k|i,k) = p_{coll}, & 0 \le i \le m,\ 1 \le k \le W_i-1 \\
\text{(c) } P(0,k|i,0) = (1-p_f)/W_0, & 0 \le i \le m-1,\ 0 \le k \le W_0-1 \\
\text{(d) } P(i,k|i-1,0) = p_f/W_i, & 1 \le i \le m,\ 0 \le k \le W_i-1 \\
\text{(e) } P(0,k|m,0) = 1/W_0, & 0 \le k \le W_0-1
\end{array} \tag{12}$$

Ad (a): The station's backoff timer is decremented from $k+1$ to k at a fixed, i-th backoff stage, i.e., the station has detected an idle slot. The probability of this event *Pr{channel is idle}* = 1 − *Pr{one or more stations are transmitting}*. We consider saturation conditions, so *Pr{one or more stations are transmitting}* equals p_{coll}.

Ad (b): The station's backoff timer is frozen at a fixed, i-th backoff stage, i.e., the channel is busy. *Pr{channel is busy}* = *Pr{one or more stations are transmitting}* = p_{coll}.

Ad (c): The station's backoff timer is changed from 0 to k and the backoff stage reinitialized from i to 0. The probability of this event equals: *Pr{transmission is successful and number k was randomly chosen to initiate the backoff timer at stage 0}* = *Pr{transmission is successful}* · *Pr{number k was randomly chosen to initiate the backoff timer at stage 0}*. The probability of successful transmission is equal to $1-p_f$ and the probability that number k was randomly chosen to initiate the backoff timer at stage 0 equals $1/W_0$.

Ad (d): The station's backoff timer is changed from 0 to k and the backoff stage is increased from $i-1$ to i. Probability of this event equals: *Pr{transmission is unsuccessful and number k was randomly chosen to initiate the backoff timer at stage i}* = *Pr{transmission is unsuccessful}* · *Pr{number k was randomly chosen to initiate the backoff timer at stage i}*. The probability of unsuccessful transmission equals p_f and the probability that number k was randomly chosen to initiate the backoff timer at stage i equals $1/W_i$.

Ad (e): The station's backoff timer is changed from 0 to k and the backoff stage is changed from m to 0, i.e., the station has reached the maximum retransmission count. The probability of this event equals the probability that number k was randomly chosen to initiate the backoff timer at stage 0, i.e., $1/W_0$.

Let $b_{i,k}$ be the steady-state occupancy probability of state (i,k). It can be shown that:

$$b_{i,0} = p_f \cdot b_{i-1,0} \tag{13}$$

$$b_{i,0} = p_f^i \cdot b_{0,0} \tag{14}$$

and

$$b_{i,k} = \begin{cases} \frac{W_i-k}{W_i(1-p_{coll})} p_f^i \cdot b_{0,0}, & 0 < k \le W_i-1 \\ p_f^i \cdot b_{0,0}, & k = 0 \end{cases} \tag{15}$$

From the normalization condition:

$$\sum_{i-0}^{m} \sum_{k=0}^{W_i-1} b_{i,k} = 1 \tag{16}$$

and

$$\sum_{i=0}^{m} b_{i,0} = b_{0,0} \frac{1-p_f^{m+1}}{1-p_f} \tag{17}$$

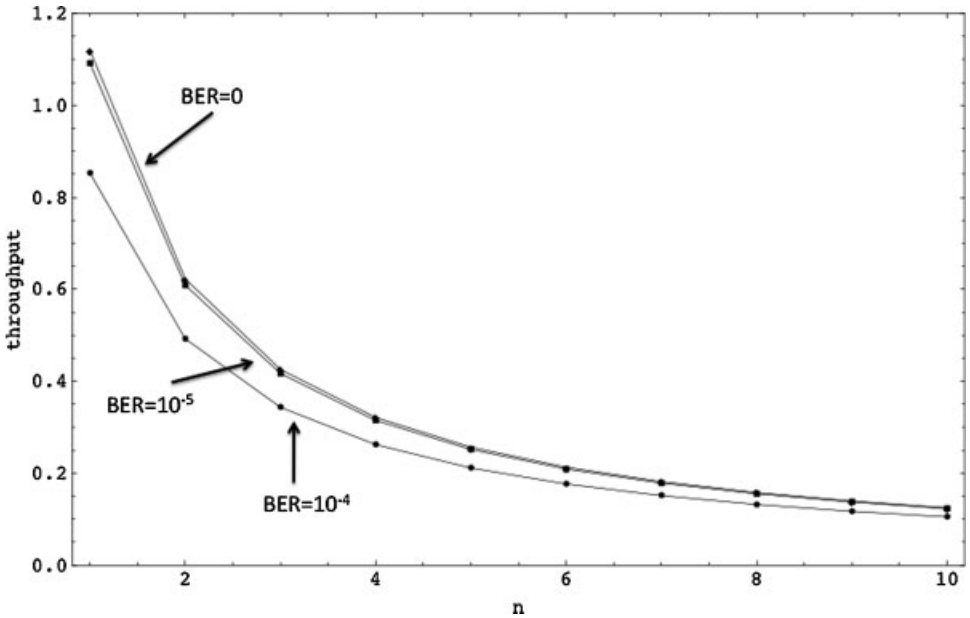

Figure 3. S_{DATA} as a function of n – for $L = 214$ octets and different values of BER.

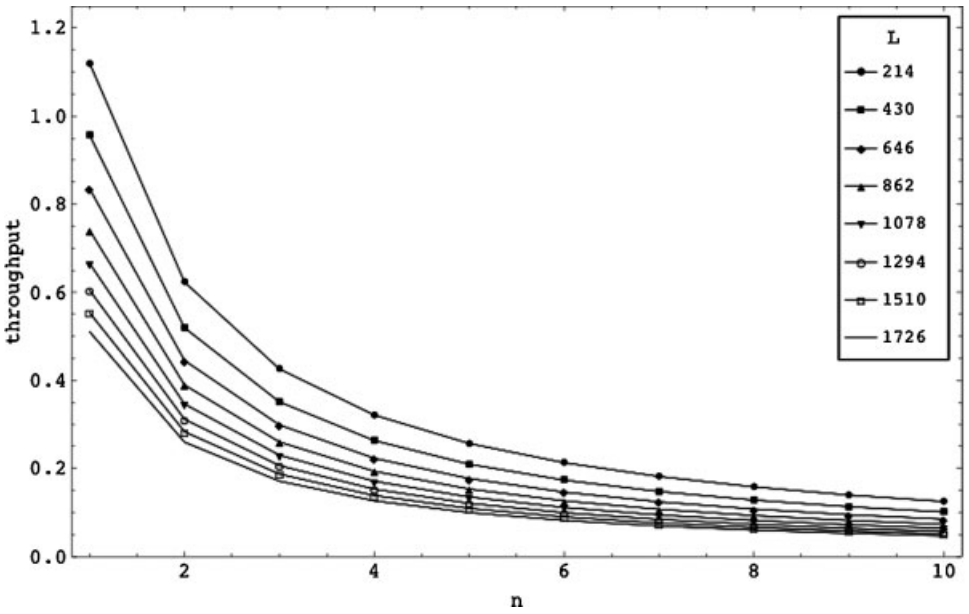

Figure 4. S_{DATA} as a function of n – for different values of frame length and $BER = 0$.

we get:

$$b_{0,0}^{-1} = \begin{cases} \frac{(1-p_{\mathrm{f}})W_0(1-(2p_{\mathrm{f}})^{m+1})-(1-2p_{\mathrm{f}})(1-p_{\mathrm{f}}^{m+1})}{2(1-2p_{\mathrm{f}})(1-p_{\mathrm{f}})(1-p_{\mathrm{coll}})} + \frac{1-p_{\mathrm{f}}^{m+1}}{1-p_{\mathrm{f}}}, & m \le m' \\ \frac{\psi}{2(1-2p_{\mathrm{f}})(1-p_{\mathrm{f}})(1-p_{\mathrm{coll}})} + \frac{1-p_{\mathrm{f}}^{m+1}}{1-p_{\mathrm{f}}}, & m > m' \end{cases} \quad (18)$$

where

$$\psi = (1-p_{\mathrm{f}})W_0(1-(2p_{\mathrm{f}})^{m'+1})-(1-2p_{\mathrm{f}})(1-p_{\mathrm{f}}^{m+1}) + W_0 2^{m'} p_{\mathrm{f}}^{m'+1}(1-2p_{\mathrm{f}})(1-p_{\mathrm{f}}^{m-m'}) \quad (19)$$

The probability of frame transmission τ is equal to *Pr{backoff timer equals* 0*}* and thus:

$$\tau = \sum_{i=0}^{m} b_{i,0} = \begin{cases} \left(\frac{(1-p_f)W_0(1-(2p_f)^{m+1})-(1-2p_f)(1-p_f^{m+1})}{2(1-2p_f)(1-p_f)(1-p_{coll})} + \frac{1-p_f^{m+1}}{1-p_f}\right)^{-1} \frac{1-p_f^{m+1}}{1-p_f}, & m \le m' \\ \left(\frac{\psi}{2(1-2p_f)(1-p_f)(1-p_{coll})} + \frac{1-p_f^{m+1}}{1-p_f}\right)^{-1} \frac{1-p_f^{m+1}}{1-p_f}, & m > m' \end{cases} \quad (20)$$

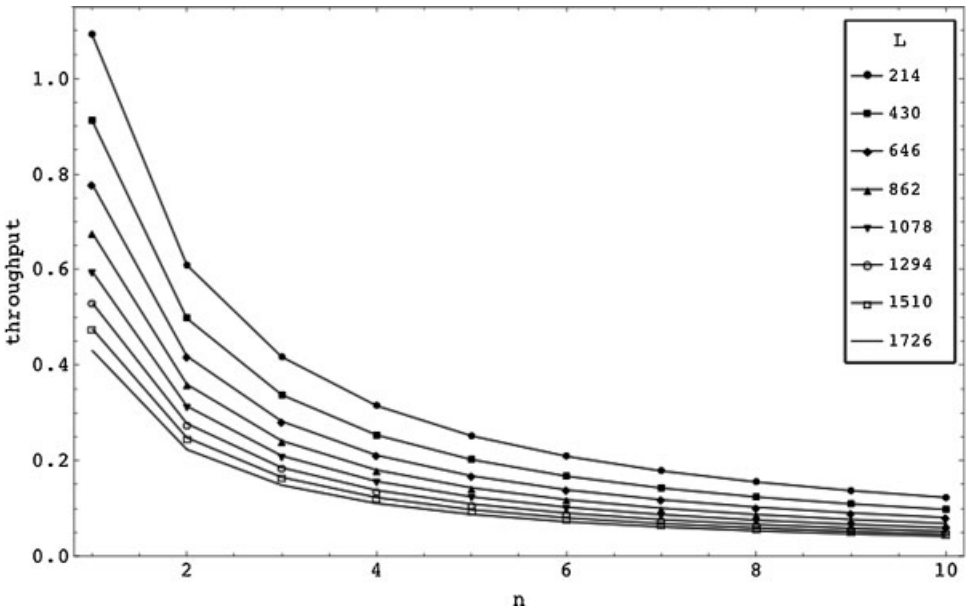

Figure 5. S_{DATA} as a function of n – for different values of frame length and $BER = 10^{-5}$.

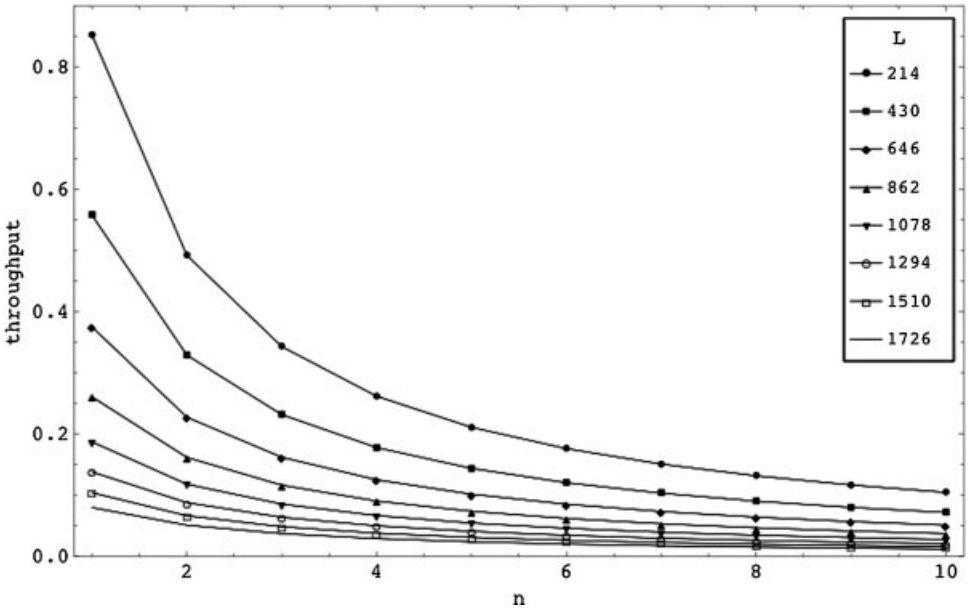

Figure 6. S_{DATA} as a function of n – for different values of frame length and $BER = 10^{-4}$.

For $p_{coll} = 0$ the above solution is the same as presented in Ref. [4].

4.4. Probability of transmission failure p_f and probability of collision p_{coll}

We use a channel model with random distribution of errors, i.e., without grouping of errors. The probability of transmission failure

$$p_f = 1-(1-p_{coll})(1-p_e) \tag{21}$$

where p_e is the frame error probability:

$$p_e = 1-(1-p_{e\_data})(1-p_{e\_ACK}) \tag{22}$$

where p_{e_data} is FER for data frames and p_{e_ACK} is FER for ACK frames. p_{e_data} and p_{e_ACK} can be calculated from bit error probability (i.e., BER), p_b:

$$p_{e\_data} = 1-(1-p_b)^{L_{data}} \tag{23}$$

$$p_{e\_ACK} = 1-(1-p_b)^{L_{ACK}} \tag{24}$$

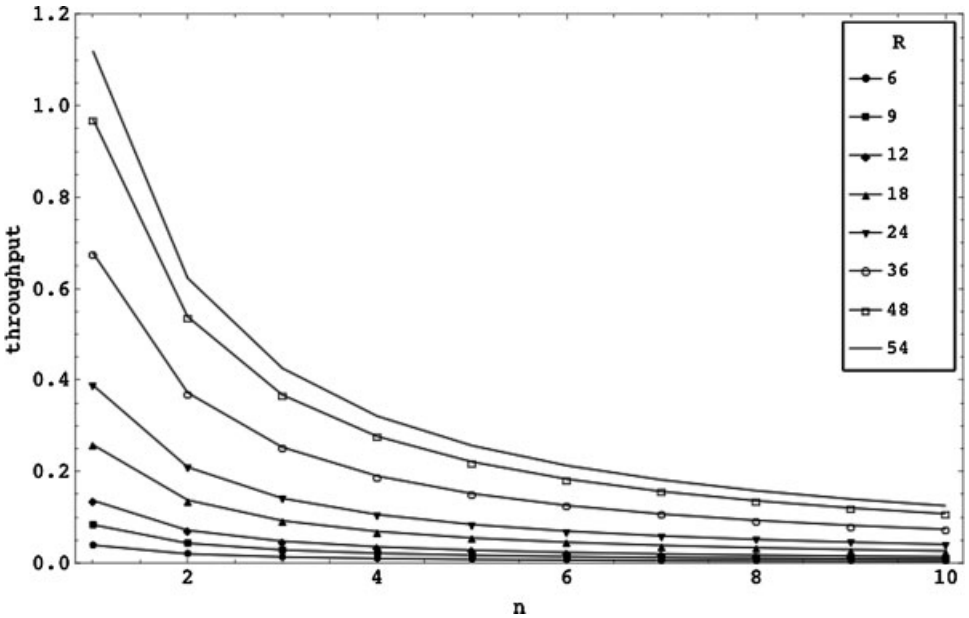

Figure 7. S_{DATA} as a function of n – for $L = 214$ octets, BER = 0 and different values of R.

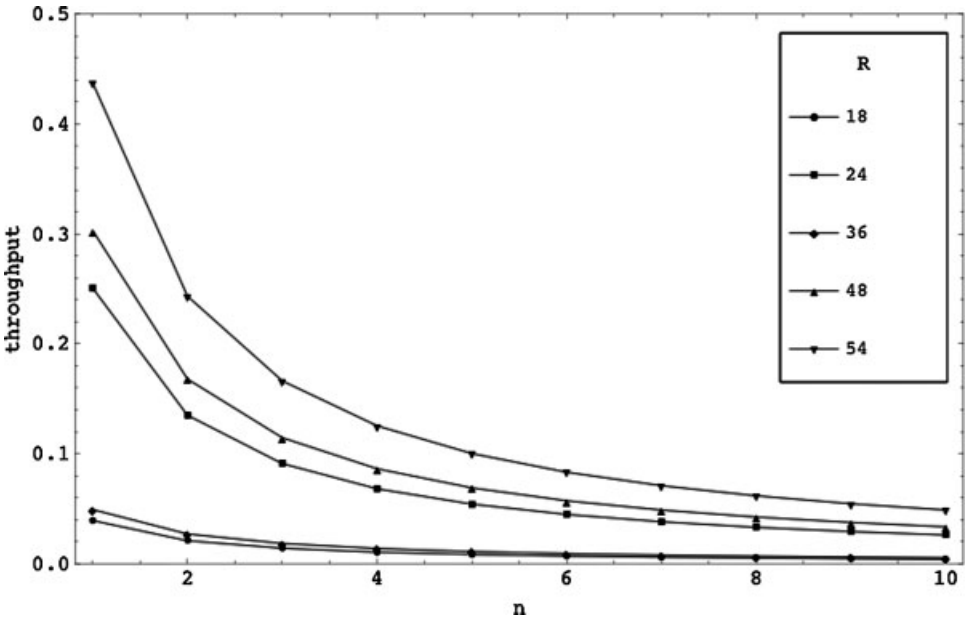

Figure 8. S_{ACK} as a function of n – for $L = 214$ octets, BER = 0 and different values of R.

The probability of collision:

$$p_{coll} = 1-(1-\tau)^{n-1} \tag{25}$$

Finally

$$p_f = 1-(1-p_{coll})(1-p_e) = 1-(1-\tau)^{n-1}(1-p_e) \tag{26}$$

Equations (20) and (26) form a nonlinear system with two unknown variables τ and p_f, which can be solved numerically.

4.5. Capacity and saturation throughput of steganographic channels

Let the capacity of a steganographic channel based on data frames be:

$$C_{DATA} = N_{BpS}\left|\frac{L_{SER} + L_{TAIL} + L_{DATA}}{N_{BpS}}\right| - (L_{SER} + L_{TAIL} + L_{DATA}) \tag{27}$$

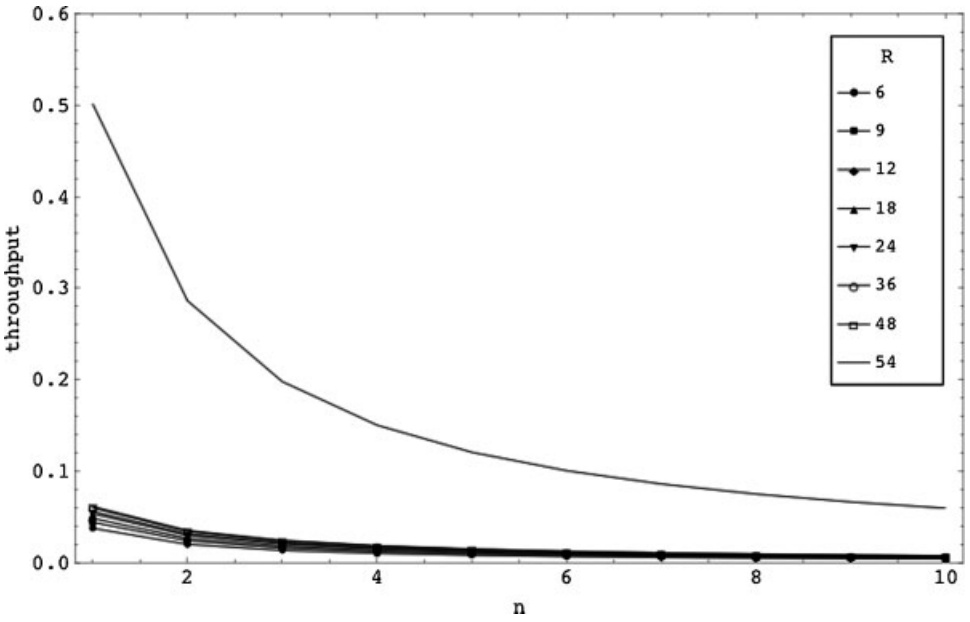

Figure 9. S_{DATA} as a function of n – for $L = 68$ octets, BER = 0 and different values of R.

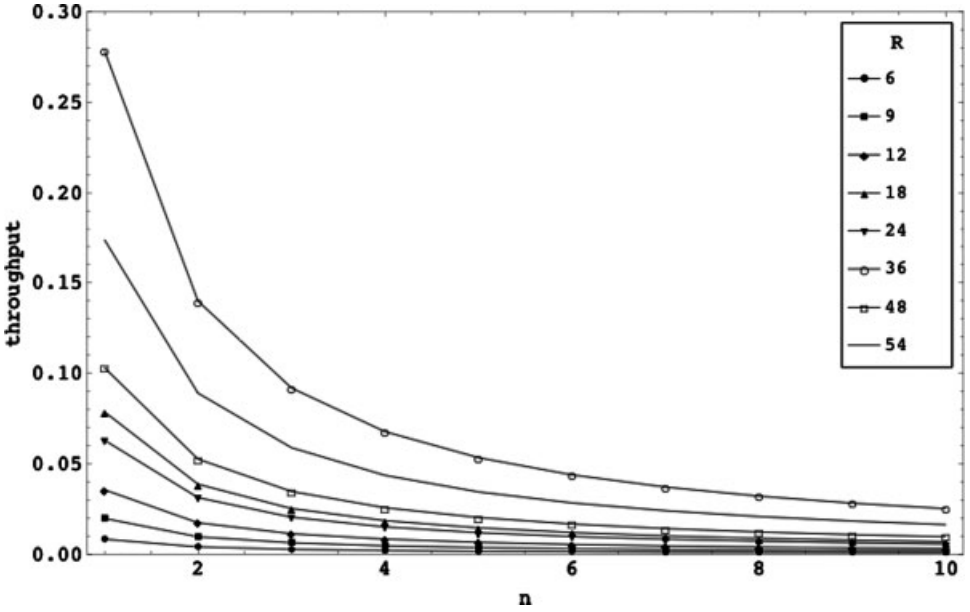

Figure 10. S_{DATA} as a function of n – for $L = 1528$ octets, BER = 0 and different values of R.

Let the capacity of a steganographic channel based on ACK frames be:

$$C_{\mathrm{ACK}} = N_{\mathrm{BpS}} \left| \frac{L_{\mathrm{SER}} + L_{\mathrm{TAIL}} + L_{\mathrm{ACK}}}{N_{\mathrm{BpS}}} \right| - (L_{\mathrm{SER}} + L_{\mathrm{TAIL}} + L_{\mathrm{ACK}}) \tag{28}$$

Therefore the saturation throughput of a steganographic channel based on data frames may be defined as:

$$S_{\mathrm{DATA}} = \frac{C_{\mathrm{DATA}} \cdot S}{n \cdot L_{\mathrm{pld}}} \tag{29}$$

And, finally, the saturation throughput of a steganographic channel based on ACK frames equals:

$$S_{\mathrm{ACK}} = \frac{C_{\mathrm{ACK}} \cdot S}{n \cdot L_{\mathrm{pld}}} \tag{30}$$

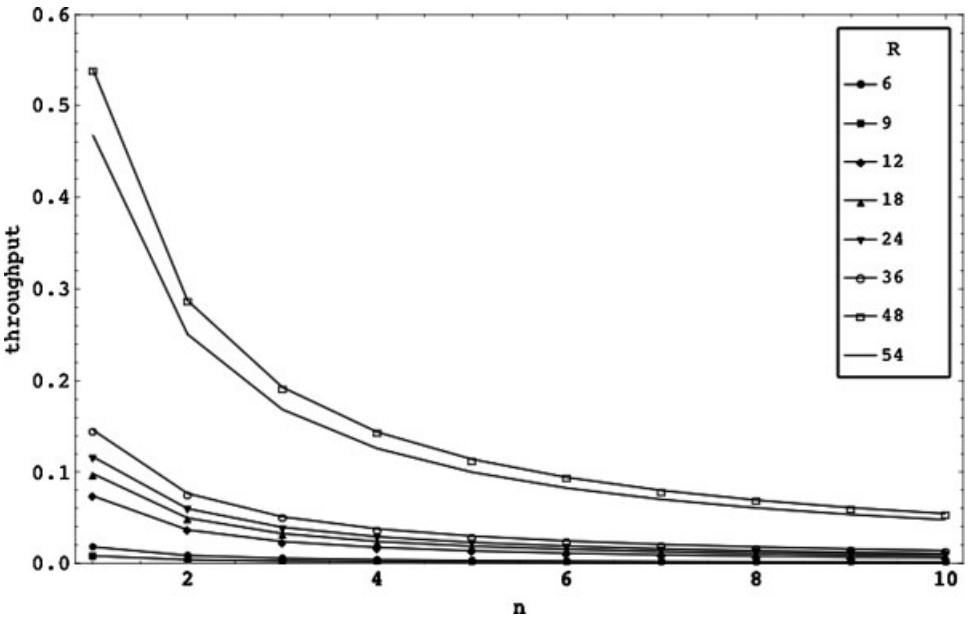

Figure 11. S_{DATA} as a function of n – for $L = 604$ octets, BER = 0 and different values of R.

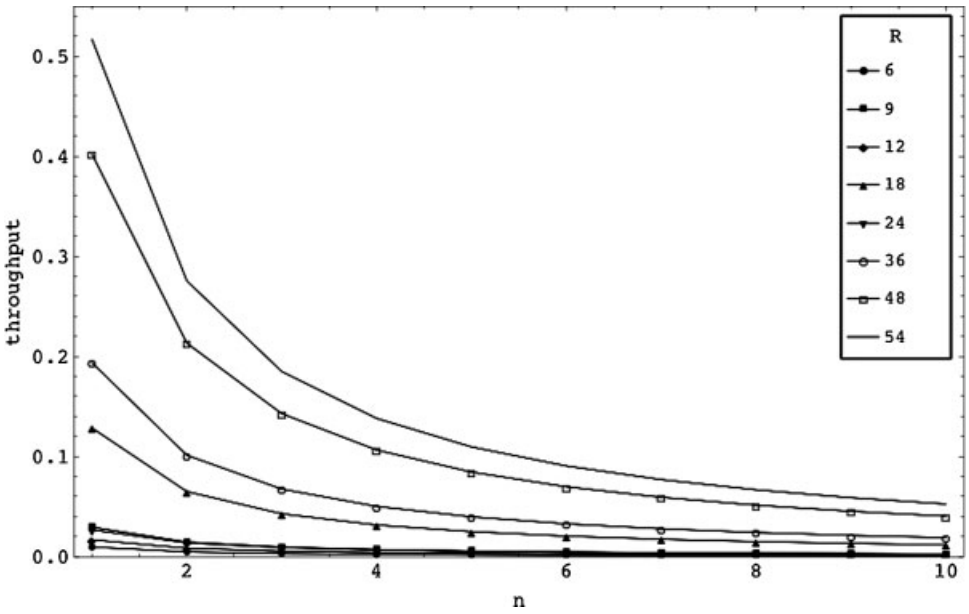

Figure 12. S_{DATA} as a function of n – for $L = 656$ octets, BER = 0 and different values of R.

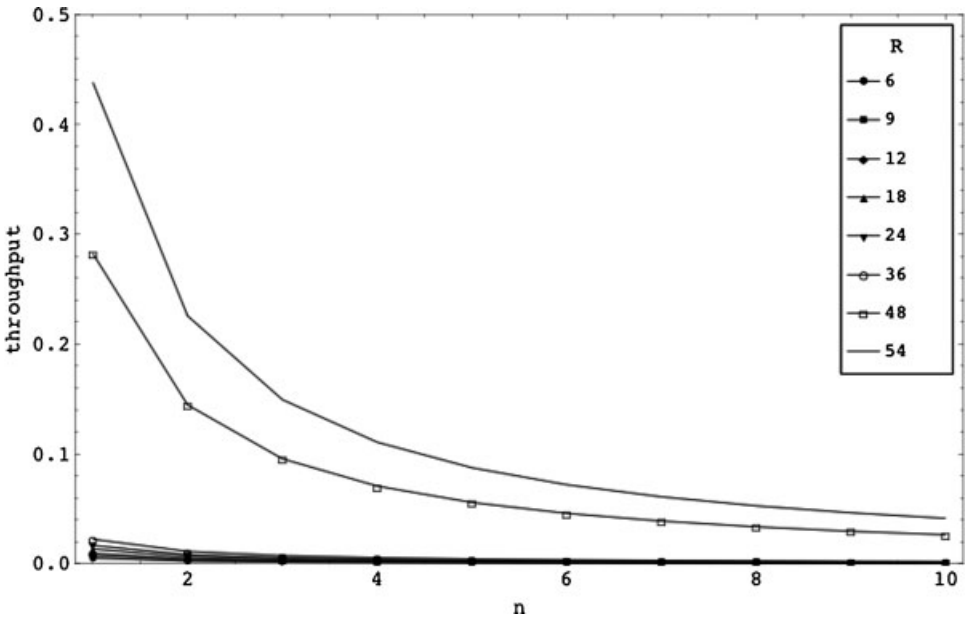

Figure 13. S_{DATA} as a function of n – for $L = 1328$ octets, BER = 0 and different values of R.

5. ANALYSIS

5.1. Frames with a maximum number of padding octets

All diagrams presented in this section display values of the saturation throughput of the proposed steganographic method (WiPad) based on the data frame variant. All calculations were made for $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. For $L = 214$ octet frames ($\alpha = 1$; 186 bytes at IP layer) the following values of BER were used $\{10^{-4}, 10^{-5}, 0\}$, and for $L \in \{214, 430, 646, 862, 1078, 1294, 1510\}$ octet frames ($\alpha \in \{1, 2, \ldots, 7\}$) the correspondent BER$\in \{10^{-4}, 10^{-5}, 0\}$. We considered the IEEE 802.11g – ERP-OFDM i.e., 'g'-only mode and a data rate of $R = 54$ Mbps (with an exception for the last diagram, which provides an evaluation of the impact of R on S_{DATA}).

Figure 3 presents S_{DATA} as a function of n for $L = 214$ octet frames and different values of BER. Along with an

increasing value of BER the steganographic throughput, S_{DATA}, declines. The maximum value reaches 1.12 Mbps for BER = 0 and $n = 1$. Along with an increasing value of BER the presented curves flatten out. For a given BER, the decrease of S_{DATA} together with an increase of n is related to a growing number of collisions in the medium. The observed decline in the value of S_{DATA} between BER = 0 and BER = 10^{-5} is very small.

Figure 4 presents S_{DATA} as a function of n for different values of frame length and BER = 0. For a given n, an increasing frame length leads to a fall in the attainable S_{DATA}.

Figure 5 represents the correlation between S_{DATA} and n, for different values of frame length and BER = 10^{-5}, while Figure 6 displays S_{DATA} as a function of n for different frame lengths and BER = 10^{-4}. Compared to the values obtained for BER = 0, we observe a reduction in the value of S_{DATA} due to the influence of channel errors.

Finally we evaluate (Figure 7) S_{DATA} as a function of n for different IEEE 802.11g data rates $R \in \{6, 9, 12, 18, 24, 36, 48, 54\}$ Mbps.

5.2. ACK frames

We evaluate (Figure 8) S_{ACK} as a function of n for different IEEE 802.11g data rates $R \in \{18, 24, 36, 48, 54\}$ Mbps. For $n = 1$ and $R = 54$, $S_{ACK} = 0.44$ Mbps (82 bits serve as a hidden channel). The throughput for 24 Mbps networks is higher than for 36 Mbps because of the different capacity of the hidden channel: 58 and 10 bits, respectively.

5.3. Typical IP packet sizes

The Refs. [15,16] show that most typical sizes for IP packets are 40 and 1500 bytes, and then 576, 628, and 1300 bytes. These values are in line with $L \in \{68, 1528, 604, 656, 1328\}$ octet frames. We consider $R \in \{6, 9, 12, 18, 24, 36, 48, 54\}$ and BER = 0.

For $L = 68$ octets (Figure 9), $n = 1$ for and $R = 54$ S_{DATA} is 0.50 Mbps (capacity of the hidden channel: 82 bits). For $R \in \{6, 9, 12, 18, 24, 36, 48\}$ the capacity of the hidden channel is only 10 bits and for $n = 1$ S_{DATA} is low (<0.06 Mbps).

For $L = 1528$ octets (Figure 10), $n = 1$ for and $R = 36$ S_{DATA} is 0.28 Mbps (capacity of the hidden channel: 138 bits) and for $R = 54$ S_{DATA} is 0.17 Mbps (66 bits). For other values of R S_{DATA} is from 0.01 to 0.1.

For $L = 604$ octets (Figure 11), $n = 1$ for and $R = 48$ S_{DATA} is 0.54 Mbps (capacity of the hidden channel: 138 bits), and for $R = 54$ S_{DATA} is 0.47 Mbps (114 bits). For other values of R S_{DATA} is from 0.01 to 0.15.

For $L = 656$ octets (Figure 12), $n = 1$ for and $R = 54$ S_{DATA} is 0.52 Mbps (capacity of the hidden channel: 130 bits). For $R = 48$ S_{DATA} is 0.40 Mbps (106 bits), for $R = 36$ S_{DATA} is 0.19 Mbps (58 bits), and $R = 18$ S_{DATA} is 0.13 Mbps (58 bits). For other values of R S_{DATA} is from 0.01 to 0.03.

Finally, for $L = 1328$ octets (Figure 13), $n = 1$ for and $R = 54$ S_{DATA} is 0.48 Mbps (capacity of the hidden channel: 154 bits) and for $R = 48$ S_{DATA} is 0.28 Mbps (106 bits). For other values of R S_{DATA} is from 0.01 to 0.2.

For evaluated lengths of IP packets the highest throughput is generally for 54 and 48 Mbps IEEE 802.11 networks. For 40, 576, 628, and 1300 bytes packets the maximal value of S_{DATA} is around 0.50 Mbps. For 1500 bytes IP packet S_{DATA} is below 0.3 Mbps.

6. CONCLUSIONS AND FUTURE WORK

In this paper we evaluated a new steganographic method called WiPad intended for IEEE 802.11 OFDM networks, whose functioning bases on insertion of bits into the padding of transmission symbols. The analysis for IEEE 802.11g 54 Mbps networks revealed that the capacity of WiPad equals 1.1 Mbit/s for data frames and 0.44 Mbit/s for ACK frames, which gives a total of almost 1.54 Mbit/s. To the authors' best knowledge this is the most capacious of all the known steganographic network channels.

Future work will include WiPad the estimation of achievable steganographic bandwidth in case of the IEEE 802.11n standard also with channel model with grouping of errors. Further studies should also involve pinpointing potential detection mechanisms of the proposed communication system. Experimental implementation as a proof-of-concept will be made similar to Ref. [17] in MATLAB and Simulink with Communication Toolbox.

REFERENCES

1. BBC News. *FBI allegations against 'Russian spies' in US*. http://www.bbc.co.uk/news/10442869 [29 June 2010].
2. Szczypiorski K, Lubacz J. *Performance Evaluation of IEEE 802.11 DCF Networks*. In *20th International Teleraffic Congress (ITC-20), Ottawa, Canada*, June 2007; Lecture Notes in Computer Science (LNCS) 4516, Springer-Verlag Berlin Heidelberg, 2007; 1082–1093.
3. Bianchi G. Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications* **18**(3): 2000; 535–547.
4. Ni Q, Li T, Turletti T, Xiao Y. Saturation throughput analysis of error-prone 802.11 wireless networks. *Wiley Journal of Wireless Communications and Mobile Computing (JWCMC)* **5**(8): 2005; 945–956.
5. Wolf M. *Covert Channels in LAN Protocols*. In *Proceedings of the Workshop of Local Area Network Security (LANSEC)*, 1989; 91–101.
6. Fisk G, Fisk M, Papadopoulos C, Neil J. Eliminating Steganography in Internet Traffic with Active Wardens. In *Proceedings of the 5th International Workshop on Information Hiding, Lecture Notes in Computer Science: 2578*, October 7–9, 2002, Noordwijkerhout, The Netherlands, Springer-Verlag: Heidelberg, Germany, 2003; 18–35.

7. Jankowski B, Mazurczyk W, Szczypiorski K. *Information hiding using improper frame padding*. In *Proceedings of the 14th International Telecommunications Network Strategy and Planning Symposium – Networks 2010*, September 2010, Warsaw, Poland.
8. Lucena NB, Lewandowski G, Chapin SJ. *Covert channels in IPv6*. In *Proceedings of the Privacy Enhancing Technologies (PET)*, May 2005; 147–166.
9. Szczypiorski K. *HICCUPS: hidden communication system for coruppted networks*. In *Proceedings of the Tenth International Multi-Conference on Advanced Computer Systems ACS'2003*. *Miedzyzdroje*, October 2003; 31–40.
10. Szczypiorski K. *A performance analysis of HICCUPS – a steganographic system for WLAN*. In *Proceedings of the 2009 International Conference on Multimedia Information NEtworking and Security (MINES 2009) – First International Workshop on Network Steganography (IWNS'09)*, Vol. I, Wuhan, Hubei, China, November 2009; 569–572.
11. Krätzer C, Dittmann J, Lang A, Kuhne T. *WLAN steganography: a first practical review*. In *Proceedings of the 8th ACM Multimedia and Security Workshop*. Geneve (Switzerland), September 2006.
12. Krätzer C, Dittmann J, Merkel R. *WLAN steganography revisited*. In *Proceedings of the SPIE Electronic Imaging 2008*, San Jose, CA, 2008.
13. IEEE 802.11, 2007 Edition, IEEE Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (2007).
14. Kochut A, Vasan A, Shankar A, Agrawala A. *Sniffing out the correct physical layer capture model in 802.11b*. In *Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP 2004)*, Berlin 2004.
15. John W, Tafvelin S. *Analysis of Internet backbone traffic and header anomalies observed*. In *Proceedings of the Internet Measurement Conference IMC'07*, San Diego, CA, August 2007.
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. Odor M, Babak N, Salmanian M, Mason P, Martin M, Liscano R. *A frame handler module for a side-channel in mobile ad hoc networks*. In *Proceedings of the 5th LCN Workshop on Security in Communications Networks (SICK 2009)*, Zürich 2009; 930–936.