WLAN Steganography: A First Practical Review

Christian Krätzer Jana Dittmann Andreas Lang Tobias Kühne

Department of Computer Science, Research Group Multimedia and Security
Otto-von-Guericke-University of Magdeburg, Germany
{kraetzer, dittmann, alang} @iti.cs.uni-magdeburg.de
tobiaskuehne@yahoo.com

ABSTRACT

Two different approaches for constructing a steganographic channel in an IEEE 802.11 (WLAN) network are introduced in this paper. First test results on the reliability, undetectability and capacity of a prototypical implementation of both approaches are described and discussed.

Categories and Subject Descriptors: H.4.3 [Communications Applications] - Computer conferencing, teleconferencing, and videoconferencing; E.4 [Coding and Information Theory] - Formal models of communication

General Terms: Algorithms, Measurement, Performance, Design, Reliability, Experimentation, Security

Keywords: Steganography, WLAN

1. INTRODUCTION

Many approaches to network-based steganography can be found in literature. Some publications, like [5], [9] and [12] are focused on storage channel based hidden communication mostly using header modification; others, like [10] are focused on timing channel based steganography. Some publications like [11] are using both paradigms for constructing hidden channels. Most of these publications are concerned with higher level protocols based on Ethernet; only one publication could be found which is focused on the IEEE 802.11 standard [7] (WLAN). The publication [13] proposes a theoretical description of a steganographic system using the characteristics of a wireless network. Generating corrupted packets, which are discarded automatically by all receivers, which do not participate in the hidden communication, does the embedding in this system. When this paper was published in 2003 the author met obstacles provided by the hardware and drivers for the WLAN equipment used, which prevented him from implementing his theoretical scenario.

Motivated by the theoretical framework, in our paper we present and discuss two practical concepts and first test results for a prototypical implementation of these two steganographic scenarios which go further than [13] by moving from the storage channel approach to the usage of a covert timing channel. The *cover* in our case is a sequence of packets of the IEEE 802.11 protocol. Figure 1 is showing a classic passive steganography scenario as it is described in [8] and its adaptation to WLAN steganography. The basic principle here is to use a WLAN communication between two communication partners *A* and *B* as *cover* for the construction of a hidden channel between two other communication partners *C* and *D*. Furthermore the existence of an attacker E in the scenario is assumed.

MM&Sec'06, September 26–27, 2006, Geneva, Switzerland.

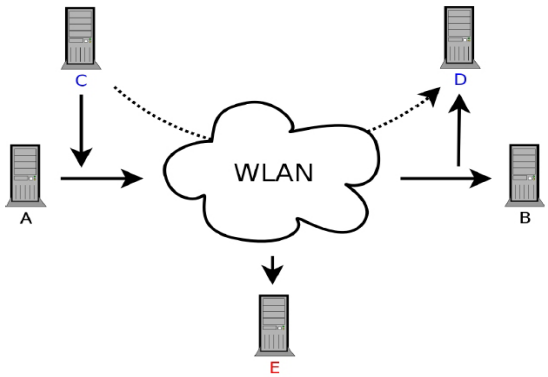

Figure 1: Basic principle

In our paper we want to compare the approach of a storage channel based scenario (using header embedding) and a time channel based scenario and discuss the advantages and disadvantages of both approaches.
Section 2 describes our application scenario; in section 3 an analysis of the WLAN protocol for possibilities for construction on a packet based steganographic channel is performed. Section 4 describes our two scenarios for a hidden communication; section 5 describes briefly the prototypical implementation, while section 6 describes our tests and the test results. The paper is completed by a summary and references for future work.

2. THE APPLICATION SCENARIO

The notation briefly introduced in section 1 is concretised at this point. In the context of this paper the following general notation is used: *A* is an element of the set of transmitting entities in a WLAN (since it is considered to use more than one connection for the steganographic embedding to make it more transparent *A* itself is a set of sending entities $A_1, A_2, ..., A_n$ with *n* being the maximum number of sending entities in the WLAN; this principle is shown in figure 2), *B* element of the set of receiving entities in a WLAN (like *A B* is also to be considered a set of receivers; with *d* being

the maximum number of receiving entities in the WLAN), *C* sender of the steganographic message, *c* number of communicating entities within the WLAN ($c=n+d$), *D* is the receiver of the steganographic message, *E* attacker on the steganography scenario (a global observer capable of steganalytical analysis), *H* the hidden steganographic channel, *m* the steganographic message (which is assumed to be the same at *C* and *D*), *p* a captured (sniffed) WLAN packet, p_{mod} a modified WLAN packet, *s* key shared by *C* and D for the initialisation of *H*, *v* number of connections within the WLAN. Furthermore it is assumed that: The communication between *A* and *B* is not disturbed by *H*, all concepts for the hidden communication have to be non-impairing; furthermore no entirely new network packets (fake contents) are created, only (duplicated and modified) existing packets are part of the *cover*, using features provided by the IEEE 802.11 protocol.

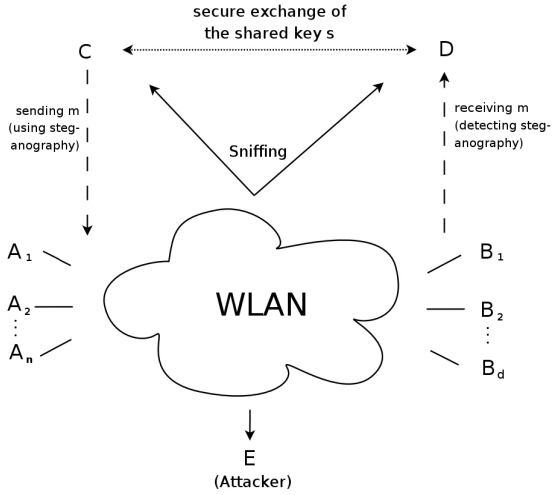

Figure 2: Application Scenario

The WLAN considered is a limited network ($c < \infty$), with more than two active communication partners ($c \geq 2,\ c \in N$; WLAN access points (APs) which act as a gateway between WLANs and other networks have to be considered also as active communication partners in this context; the maximum number of connected entities per AP is restricted to 2007 [6] but the number of APs in a wireless network cannot be restricted) in concept one and more than one active communication in concept two. The message *m* is any binary message (hidden message), for the embedding of *m* only fields in the header are used and only fields are selected for the embedding of *m* where a modification is not obvious to *E*. It exists an attacker *E* who is capable of using steganalytical methods to evaluate the communications in the WLAN; *E* is a global observer regarding the communication between *A* and *B* as well the hidden communication between *C* and *D* (i.e. *E* is capable of receiving all radio signals emitted by *A* and *C* and received by *B* and *D*), and the hard- and software configuration of *C*, *D* and *E* enables them to perform their assigned tasks (use the monitor mode of the NICs, the packet modification or packet duplication).

3. Analysis of the WLAN protocol and the infrastructure used for testing

For any application of steganographic techniques the characteristics of the cover chosen for embedding have to be investigated thoughtfully in advance. In the focus of this document the behaviour of an IEEE 802.11 (WLAN) network in "normal operation" and the influence of a steganographic embedding in the network have to be analysed. Based on a preceding theoretical analysis and [13] the IEEE 802.11 MAC header is reviewed for possible places for header modification as a means of steganographic embedding. As criteria for this analysis the impact of a modification on the communication between *A* and *B* and the transparency of the modification are chosen. The results of this analysis with regards to the cover protocol (WLAN) and the cover itself (a sequence of network packets) as well as the tests performed are discussed here to act as a base of knowledge for the steganographic concepts.

3.1 Cover Protocol Analysis

Since it is not possible in a radio based network to block the transmission of sent packets, the duplication of packets has to be considered as the only remaining way to construct a hidden channel in a packet based approach (different approaches might use other features like a variation of the signal strength for sending, but this is outside the focus of this document). IEEE 802.11 features a sender side retransmission mechanism, which uses for signalling the "Retry" bit to be discussed in more detail in section 3.2.1. Preliminary tests were performed in the WLAN infrastructure to be found on the campus of the Otto-von-Guericke University Magdeburg, Germany. Since WLAN is a radio network and therefore highly dynamic in regards of participants and traffic, detailed descriptions of the network at the time of every test is spared out at this point. Instead we give an impression how the behaviour of selected components in this dynamic and strongly inhomogeneous network could influence a possible steganographic communication. Our tests result in the knowledge that a manual duplication of packets of certain WLAN packet types provokes a reaction from certain participants in the network. For example the duplication of packets of the type/subtype "Probe Request" or "Probe Response" resulted in retransmitting of the original packet 10 times by certain APs which detected their MAC address in the header of the duplicated packet (obviously a security feature of the APs concerned against spoofing). To guarantee a reliable performance in a steganographic application, parts of the protocol protected by such security mechanisms should be excluded from usage in the construction of *H* (i.e. packet types should be chosen which can be duplicated without causing side effects, e.g. Beacon Frames).

3.2 Cover Packet Analysis

Here an analysis of packets used as cover is performed. For this the IEEE 802.11 MAC frame provided by the protocol has to be evaluated for possible points of transparent modification, where an embedding has no impact on the overall functionality of the underlying network traffic (the *cover*). This frame, which contains all IEEE 802.11 protocol data as well as the payload and consists of the nine fields, is shown in figure 3 [7].

Bytes 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

Figure 3: IEEE 802.11 MAC Frame [7]

The possibility to use one of those fields is defined by its function since the modification of a special field must not have an impact on the overall functionality of the WLAN or the WLAN

connection it belongs to. Also the probability of the detection by *E* of a modification in a field has to be considered. Therefore the fields of the frame have to be analysed for their functionality and their usefulness as a carrier for the steganographic message.

3.2.1 The Frame Control Field

The Frame Control field (FCF) of the IEEE 802.11 MAC header is a 16 Bit field containing status information about the frame type, the fragmentation, WEP encryption and other protocol relevant data. Therefore it can be found in all possible types of WLAN packets making this field an interesting place for steganographic embedding. Its composition is shown in figure 4.

Bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

Figure 4: Frame Control Field of the WLAN header [7]

At this point only the "Retry" bit is described in some detail, since it is important for both steganographic scenarios described in section 4 of this paper. This bit is set if the sender considers it necessary to retransmit a packet (assuming that the first transmission did not succeed). Such a retransmission has no influence on the Sequence Control field of the resent packet – it has the same value like the original. In any packet duplication based approach the "Retry" bit should be set; otherwise the necessary requirement of a high transparency for the steganographic channel is violated. Table 1 concludes the results of preceding tests for the FCF, marking fields where data could be embedded without disturbing the protocol or being too obvious for an assumed attacker *E*.

Table 1: Fields of the FCF and their usefulness for steganographic embedding

Field	Usefulness in steganography
Protocol Version, Type, Subtype, To DS, From DS, WEP, Order	-
More Frag, Retry, PwrMgt, More Data	+

In a field test at the Otto-von-Guericke University of Magdeburg, a first statistic of the occurrence of the bits identified as possible carriers of hidden information has been prepared. In this field test about 500,000 data packets within a WLAN infrastructure ($c \approx 100$) have been analysed for the fields identified as possible places for embedding (due to the lacking impact on the functionality of the WLAN network) in table 1.

Table 2: Selected fields of the FCF and their occurrence in practise

Bit	Number of packets	Percentage
More Frag	0	0 %
Retry	40,814	7.916 %
PwrMgt	1,467	0.285 %
More Data	12,328	2.391 %

As indicated in table 2 from these preliminary tests about 8% of all packets in a WLAN infrastructure are marked as retransmitted packets ("Retry" set). Also with 2.4% the occurrence of packets with the "More Data" flag set considered high enough for the usage for constructing *H*. In the environment used for testing the fields "More Frag" and "PwrMgt" were used too seldom to be of interest for the steganographic scenarios described in section 4.

3.2.2 Other fields in the WLAN MAC header

For a detailed description of all fields in the IEEE 802.11 MAC header see [7]. Table 3 displays the results of preceding tests for the WLAN MAC header, marking fields where data could be embedded without disturbing the protocol or being too obvious to *E*. It is shown that the "Duration/ID" field (the duration value is used for the Network Allocation Vector (NAV) calculation) and the "FCS/CRC" (containing a 32-bit Cyclic Redundancy Check) are considered possible places for a steganographic embedding due to their lacking impact on the operation of the network. The "Data" field containing the information that is transmitted or received is not considered for embedding. The modification of the data in this field (the payload of the packet) might have influence on the transparency or reliability of the communication between *A* and *B* and is therefore beyond question.

Table 3: Fields of the IEEE 802.11 header and their usefulness for steganographic embedding

Field	Usefulness in steganography
Frame Control Field	See section 3.2.1
Duration/ID, FCS/CRC	+
Addr. 1-4, Sequence Cont., Data	-

Concluding can be stated that there exist fields in the WLAN header which fulfil the necessary requirements (no impact of a modification on the network or the communication and an acceptable degree of transparency in the case of an embedding) for becoming part of a hidden channel.

4. Concepts for constructing *H*

In this section two different concepts based on packet duplication/modification for constructing the hidden channel are introduced (in the following those two concepts are referred to as scenario I and II). The first scenario is based on header modification, using original network packets as *cover* and embedding the data into the fields identified as possible places for embedding in section 3. It uses a covert storage channel [5] for both synchronisation and payload (message) transmission. This approach is derived from the methods applied in [9], [11] and [12], and can be considered an intuitive way of construction *H*. Additionally an adequate capacity for this scenario can be assumed. The second scenario is aimed for a very high level of transparency. It also duplicates original network packets to act as *cover*, making them look like a sender side retransmission (setting the "Retry" bit and correcting the CRC/FCS is in our context not considered a modification of the packet, since these two operations would also occur in the case of a resending invoked by the original sender). While a covered time channel is used to transmit the payload (the message *m*). The synchronisation is done by using sequences in of network traffic on selected connections. Additionally to the assumptions made in section 2 we have to establish for both scenarios that: *A, B, C*, and *D* have access to the same communication medium (the same WLAN) and that *C* is capable of identifying packets send from *A* to *B* and the resending can be managed by *C* in a tolerable amount of time.

4.1 Scenario I - Packet modification

This packet modification based approach is based on the knowledge that p_{mod} modified by *C* are considered corrupted by *B*. These packets are therefore discarded by *B* at a very early stage of the processing and *D* is capable of identifying the p_{mod} send by *C*

and successfully extract from them *m*. From the results of the preliminary tests presented in section 3 it is obvious that a header modification based scheme could only consider certain fields for embedding. Table 2 shows that the usage of the "More Fragments" bit has to be excluded from any steganographic approach since it would be to obvious for *E* that an hidden channel is constructed including this bit. With an occurrence of about 8 % in a normal WLAN network it can be assumed that basing *H* on the embedding in the "Retry" bit is the most transparent option when only considering embedding in the Frame Control Field. Additionally the "Retry" bit should be set in any resend WLAN packet, otherwise the duplication of the packet would be too obvious. Furthermore a delay between the sending of two p_{mod} is introduced to generate more transparency and prevent *C* from duplicating its own generated packets. The potential usage of the "More Data" bit is also considered transparent enough for the composition of *H* since it was set in about 2.4 % of all packets evaluated. For the first prototypical implementation of this scenario we decided to use the "Retry" and "More Data" bits for synchronisation and "Duration/ID" field for transmitting the actual payload, assuming (based on the initial analysis made in section 3) this has no impact on the overall functionality of the network, is transparent and provide a capacity of 2 byte for each packet chosen for embedding. Whether these assumptions are justified is evaluated in section 6.

4.2 Scenario II - Packet duplication

Additionally to the general notation introduced in section 2 we have to define for scenario II the following: *K* is the communication matrix, K_C communication matrix of station *C*, K_D communication matrix of station *D*, *P* the key-matrix, t_a time marking the begin of the construction of *K*, *x* number of elements in *K*, *y* number of elements in *P*, ε as the tolerance threshold in the steganographic transmission. Generally it is assumed for this scenario that t_a, the dimension of *K* (and *P*), as well as the key used for generating *P* are shared secrets between *C* and *D*.

The scenario is built on the idea of sending *m* without modifying a WLAN packet. This is done by packet duplication for embedding and the usage of two matrices *K* (communication matrix) and *P* (key-matrix) for synchronisation. The values in the rows and columns of the matrix *K* contain communication identifiers (MAC addresses for sender and receiver) for WLAN communications detected by the generator of the matrix. Both *C* and *D* start at t_a with the generation of such a communication matrix of a predefined size (resulting in K_C and K_D). For the rest of the paper it is assumed that $K_C = K_D = K$. The second matrix needed for synchronisation is the *P*. It has the same size like *K* ($x=y$ and the numbers of rows and columns are equal) and is filled with by *C* and *D* with a pseudo-randomised sequence of "0" and "1". Here the fact is used, that a PRNG initialised with the same seed (which is a shared secret between *C* and *D*) always returns the same sequence. The following two subsections describe the sending and receiving of one bit of *m*.

4.2.1 Sending of a bit

After *K* and *P* are initialised, the sending of one bit (m_f) of *m* by *C* requires the following steps: first all fields in *P* are identified where the value equals m_f, for all these fields the corresponding fields (same position in the matrix) in *K* are selected. The WLAN connections represented by the connection identifiers selected are used for the composition of the hidden channel. By duplicating the next WLAN packet on all the selected connections one bit is send in this scenario.

4.2.2 Receiving of a bit

D as the receiver of one bit of the hidden message listens on the connections identified in *K* for duplicated packages. If he detects duplicated packets on all connections containing the same value ("0" or "1") in *P*, a bit with this value is considered received. The threshold value ε is introduced into the system to prevent other duplicated WLAN packets to desynchronise *H*.

5. IMPLEMENTATION

For the prototypical implementation of the introduced concepts WLAN NICs with an Atheros [1] chipset were chosen. These cards can be addressed under Linux using the "madwifi" device driver [2]. For this driver a patch enables packet injection in raw format. Using this driver the CRC/FSC field of the resend packet is automatically corrected. As a software for handling the packets (sniffing, creation, modification, and sending) the Python based Scapy [3] was used under Linux.

For the tests described here scenario I is fully implemented (except for the functionality of *s*), while scenario II was only partially implemented (the synchronisation of K_C and K_D is done manually). The simulation of the functionalities used for testing of scenario II therefore allows no evaluation the reliability.

6. FIRST TEST RESULTS

In this section first tests are described regarding the impact of the steganographic embedding on the availability and reliability of the communication between *A* and *B*, the reliability (robustness; probability of correct decoding) of *H* as well as the transparency or detectability and capacity of the steganographic embedding. To allow for comparability of the result, first some more measurements of the normal behaviour of the WLAN infrastructure used for testing are presented. Since a WLAN infrastructure is a highly dynamic formation, the normal behaviour of the *cover* for during each test performed has to be described separately to match the actual configuration. The tests in sections 6.1 and 6.2 as well as the preliminary tests were made in different environments. This results in slightly different statistical behaviour of the *cover* noticeable in the following tables.

6.1 Scenario I

Table 4 displays the results of the test for normal behaviour for the scenario I. The value of selected fields in the network is recorded for a time of 5 minutes and evaluated in 10 windows of 30 seconds. At the time of the testing the network had the following configuration: $c = 15$, one *C*, two *D* (distance to *C* 0.3 and 20 meters), *m*="UniversityOfMagdeburg", one *E*. All participants in *H* were configured to use the same WLAN channel. Based on the knowledge presented in the cover protocol analysis (section 3.2) it was decided to use packets of the type 8 ("Beacon Frame") for the embedding. The delay between the sending of two stego-packets was set to 0.5 seconds. The results in table 4 show for the "Retry" bit very similar results like table 2. For the "More Data" bit the results differ from the figures computed in the preliminary tests (which show very well how different the "normal behaviour" of the same WLAN

infrastructure at different times can be). Unfortunately we found in none of the 10 windows a case where the "Retry" and "More Data" bits were both set. The results for the "Duration/ID" field show that this field was set in more than 41% to a value larger than 0.

6.1.1 Reliability

The tests performed had no impact on the communication between *A* and *B*. For the measurement of the reliability of *H* we could transmit *m* 15 times in the 5 minutes. In two of these 15 transmissions *m* was corrupted (letters were duplicated). The source of this corruption could not be determined and has to be a goal for further research. From these first tests we can assume a reliability of about 87%.

6.1.2 Undetectability

If *E* (who is assumed to be capable of receiving the packets send by *A* and *C*) compares all duplicated packets within the WLAN with their originals he would detect in scenario I the communication (between *A* and *B*) selected by *C* as cover and also the message embedding itself by identifying the stream of modified packets. If he refuses this informed approach he could also use a analysis on the statistical occurrence of values in selected fields in the WLAN MAC header to detect the embedding by its impact on the distribution of values. This steganalytical approach is strongly depending on reliable evaluations on the "normal operation" within the network analysed which is slightly difficult with WLANs for which a high degree of variability must be assumed. Table 4 displays the results of a statistical evaluation of the relevant field for scenario I in "normal operation". Table 5 displays the results of the same analysis on the same network with an *H* present. From the comparison of both tables it is obvious that the message embedding has no visible influence on the behaviour of the "Retry" bit and the "Duration/ID" field. But the embedding leaves a strong mark in the "More data" field and it is really obvious when considering all packets where "Retry" and "More Data" are set.

A second useful indicator for the embedding is gained by an evaluation of the delays caused by *C* during the processing and retransmitting. Figure 5 shows the delays of "normal" retransmitted packets (in black) in comparison to the delays in a WLAN with (additional) steganographic traffic (in grey). It is noticeable that the modification of the packets has a strong impact to the delay between original and retransmitted packet. Concluding has to be stated that the detectability rate of scenario I has to be assumed to be very high. The statistics presented in table 4 and 5 indicate that the usage of the "Retry" and "More Data" bits for synchronisation is disadvantageous. Future work will have to propose a different synchronisation scheme for this scenario, since *H* is considered not transparent enough against the observation from *E*.

6.1.3 Capacity

With the chosen configuration scenario I has a capacity of 2 byte payload per modified packet. In our tests the delay between two p_{mod} was set to 0.5 seconds, therefore we have a theoretical capacity of 4 byte per second (1200 byte in 5 minutes) with the selected parameters. In our tests we were able to transmit *m* 15 times (15*21*2 byte = 630 byte) in 5 minutes resulting in a practical capacity of 2.1 byte per second. The difference between the theoretical and practical transparency results from the effect that *C* must wait for an appropriate packet for duplication and from the computation time *C* needs for processing and retransmission.

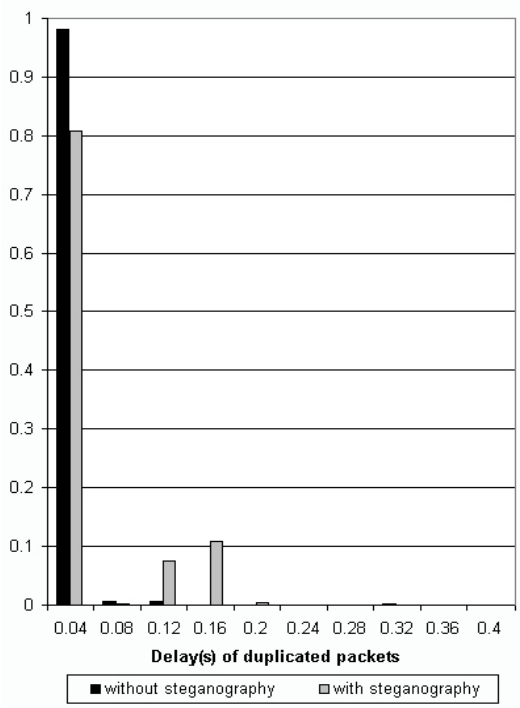

Figure 5: Distribution of delays of duplicated packets in scenario I

6.2 Scenario II

Due to problems with the synchronisation scheme encountered during the implementation of scenario II (the assumption $K_C = K_D = K$ could not be met by the implementation), the behaviour of this scenario had to be simulated. Therefore no statements on the reliability can be made.

6.2.1 Undetectability

This scenario was designed to be less detectable than scenario I. This goal is achieved by abstaining from a packet modification. For a successful attack *E* requires here the two matrices *K* and *P*. Without the knowledge of these two matrices he can neither identify the connections used for the communication, nor can he determine which of the duplicated packets is associated with which meaning (representing a "0" or "1"). Since we assume that t_a is shared between *C* and *D*, in this case *E* can only use the statistics of the WLAN (the probability for the occurrence of packet duplication in "normal operation" and in the case of message embedding) for the detection of the hidden communication *H*. The impact on the statistics is depending on the used capacity (bytes or duplicated packets per second) and the ratio between the size of *K* and *c*. If these parameters are chosen by *C* with the aim of a high transparency and the "Retry" bit for the duplicated packets is set to avoid collusion with the WLAN protocol we can assume that this goal is reached.

Table 6 and 7 show the results for a computation of the relevant fields (in this case only the "Retry" bit). When comparing both tables no impact of the embedding on the "Retry" bit can be seen. By chance the results for most windows are even lower in table 7

than in 6. From the tests it can be confirmed that even the delays for the duplication cannot be diminished from the delay in genuine retries. From these results it can be assumed that the transparency goal for this scenario can be met.

6.2.2 Capacity

For the second scenario the capacity is far smaller than with scenario I and it is depending on more parameters. Under the best circumstances (K is a 1*2 matrix, P=[0 1] and ideal traffic) the capacity (with the selected 0.5 second delay between two p_{mod}) is 1 bit per packet (0.2 byte per second).

7. SUMMARY AND FUTURE WORK

In this paper we introduced two steganographic scenarios for the IEEE 802.11 network standard. From the first test results presented the potential of both scenarios (high capacity for scenario I and high transparency for scenario II) are obvious. Necessary modifications on both scenarios, mainly on the synchronisation schemes and varied parameters used will provide a good basis for further testing (e.g. to achieve the necessary increase of the reliability to 100%).

ACKNOWLEDGMENTS

The results from the preceding tests mentioned in the document and the prototypical implementation of the steganographic embedder are results of the Diploma thesis of Tobias Kühne.

The work about transparency evaluation described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

REFERENCES

[1] Atheros Consumer Products, http://www.atheros.com/

[2] MadWifi, Linux kernel driver for Wireless LAN chipsets from Atheros, http://madwifi.org/

[3] Scapy, Philippe Biondi, phil@secdev.org, interactive packet manipulation programme, http://www.secdev.org/projects/scapy/

[4] Ethereal, network protocol analyzer, http://www.ethereal.com

[5] Pukhraj Singh, *Whispers on the Wire - Network Based Covert Channels*, Proceedings of the Symposium on Security for Asia Network (SyScAN'05), 1st and 2nd of September 2005, Bangkok, Thailand.

[6] Jörg Rech, *Wireless LANs - 802.11-WLAN-Technologie und praktische Umsetzung im Detail*, 2004, ISBN 3-936931-04-6

[7] Institute of Electrical and Electronics Engineers (IEEE), *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11, 1997

[8] Dittmann, Jana; Hesse, Danny; Hillert, Reyk: *Steganography and steganalysis in voice over IP scenarios: operational aspects and first experiences with a new steganalysis tool set*, Delp, Edward J. (Hrsg.); Wong, Ping W. (Hrsg.): Security, steganography, and watermarking of multimedia contents VII (Electronic imaging science and technology San Jose, California, USA, 17-20 January 2005); Bellingham, Wash.: SPIE, 2005, pp. 607 - 618, ISBN 0-8194-5654-3, 2005

[9] Steven J. Murdoch, Stephen Lewis, University of Cambridge, *Embedding Covert Channels into TCP/IP*, Information Hiding Workshop, 2005

[10] Hans Georg Eßer, Felix C. Freiling, Universität Mannheim, *Kapazitätsmessung eines verdeckten Zeitkanals über HTTP*, Sicherheit 2006 Proccedings, Köllen Verlag, 2006, ISBN 3-88579-171-4

[11] Deepa Kundur, Kamran Ahsan, *Practical Internet Steganography: Data Hiding in IP*, Proceedings of the Texas Workshop on Security of Information Systems, April 2nd, 2003

[12] Craig H. Rowland, *Covert Channels in the TCP/IP Protocol Suite*, 1996, http://www.firstmonday.org/issues/issue2_5/rowland/

[13] Krzysztof Szczypiorski, HICCUPS: Hidden Communication System for Corrupted Networks, The 10th International Multi-Conference on Advanced Computer Systems ACS 2003, October 22-24th, 2003, http://krzysiek.tele.pw.edu.pl/pdf/acs2003-hiccups.pdf

Table 4: Distribution of selected fields of the IEEE 802.11 header in "normal operation" (test for scenario I)

Field \ T (in seconds)	0-30	30-60	60-90	90-120	120-150	150-180	180-210	210-240	240-270	270-300	Avg.
Retry (percent)	8.78	12.23	11.05	6.74	11.67	5.55	2.38	6.44	11.17	2.91	7.89
More Data (perc.)	0.00	0.13	0.23	0.39	0.16	0.15	0.24	0.05	0.37	0.14	0.19
Dur./ID (perc.)	43.63	55.93	56.50	41.04	59.16	41.16	45.74	51.23	55.76	41.07	49.12
Retry & M.Data (perc.)	0	0	0	0	0	0	0	0	0	0	0.00

Table 5: Distribution of selected fields of the IEEE 802.11 header with embedded m (test for scenario I)

Field \ T (in seconds)	0-30	30-60	60-90	90-120	120-150	150-180	180-210	210-240	240-270	270-300	Avg.
Retry (percent)	14.95	4.31	6.77	6.81	16.09	4.43	6.95	6.21	4.59	1.98	7.31
More Data (perc.)	0.61	1.41	1.50	2.84	0.58	1.55	1.68	1.39	1.35	0.38	1.33
Dur./ID (perc.)	69.75	37.65	45.49	31.74	64.60	44.98	44.57	40.79	50.45	59.99	49.00
Retry & M.Data (perc.)	0.35	1.37	1.06	2.84	0.42	1.55	1.36	1.35	1.31	0.36	1.20

Table 6: Distribution of selected fields of the IEEE 802.11 header in "normal operation" (test for scenario II)

Field \ T (in seconds)	0-30	30-60	60-90	90-120	120-150	150-180	180-210	210-240	240-270	270-300	Avg.
Retry (percent)	3.60	4.16	8.17	1.66	6.29	3.54	2.27	4.31	2.05	4.94	4.10

Table 7: Distribution of selected fields of the IEEE 802.11 header with embedded m (test for scenario II)

Field \ T (in seconds)	0-30	30-60	60-90	90-120	120-150	150-180	180-210	210-240	240-270	270-300	Avg.
Retry (percent)	3.18	2.89	7.08	2.06	4.60	2.66	3.21	4.27	2.81	3.79	3.65