Paper

Network Management in Non-classified Data Hiding System Using Master Resident over Hidden Layer

Krzysztof Sawicki and Zbigniew Piotrowski

Military University of Technology, Warsaw, Poland

Abstract—The paper presents a practical implementation of the non-classified data hiding system (NDHS) understood as a military platform for information warfare that takes advantage of the hidden data transmission for voice connections in order to gain informational lead over a potential enemy. The NDHS performs here as a botnet network that is managed by the hidden transmission controller referred to as the master resident. Research studies are dedicated to investigation of various connections in heterogeneous links as well as functionalities of such components as hidden protocol bridges and the master resident.

Keywords—hidden protocol bridge, hidden protocol interpreter, master resident, non-classified data hiding system, steganography, voice over IP, watermarking.

1. Introduction

Telecom IT networks present an important component of the contemporary telecom world. Safeguarded circulation of information with its continuous supervision pose substantial challenges for contemporary science. From the military point any attack to the national IT network (along with the entire telecom infrastructure) is the first step to initial warfare actions. In case of public IT networks one has to be aware that such networks may be used as reserved communication means between military troops to substitute, when necessary, commonly used communication means operated regularly by the army. Total destruction of public IT networks is extremely difficult as these networks are really extensive and incorporate great number of protecting measures to preserve their integrity when one or several their components are disrupted.

Beside cryptographic methods the safeguarding measures use also techniques of information hiding that are complementary to cryptographic ones.

This paper deals with the mechanism of the master resident (MR), the possibility to remote control network devices using hidden layer and implementation of those concepts. As stated in [1] "*Network Management normally has 4 components: The component that supervises (...); The component that is supervised (...); A protocol that transfers the information between the agent and the server. (...); A list of possible things to manage*". In non-classified data hiding system (NDHS) the component that supervises is the master resident, components that are supervised are hidden protocol interpreters (HPI), simple protocol used to communicate between master resident and hidden protocol interpreters is transmitted over hidden layer and allows to send commands to HPIs thus NDHS is network management mechanism that is designed to work on hidden networks.

The master resident makes it possible to control heterogeneous IT networks using hidden and confidential transmission of commands and data that takes advantage of the digital watermark technology and encoding with use of the variably modified permutation composition (VMPC) key scheduling algorithm (KSA) [2]. That mechanism is a part of the NDHS [3], [4]. NDHS can be classified as the mechanism of electronic defence (ED) [5], [6] and uses information hiding techniques to transmit information between NDHS functional elements (hidden protocol interpreter and master resident) [3], [7] and allows the NDHS operator to remote control every hidden protocol interpreter using commands transmitted in hidden layer. In case of a hostile conflict such a mechanism, if widely applied in public networks, makes it possible to take control over selected components of public IT networks and then continuous operation of the overall telecom systems is conducive to gain an informational lead.

The remaining part of the paper is structured in the following way: the second part presents the historical solutions that have been developed so far related to the issues of making the information hidden whilst the third part describes the mechanism to be implemented. Finally, the fourth part outlines how the intended mechanism was implemented.

2. Related Works

Continuously more and more research efforts of scientific circles are targeted to the application opportunities of hidden transmissions via IT network. The past interest was focused on data transmission itself via individual segments of the network. Some examples of proposed solutions can be found in studies [8]–[11], where stress is put onto hidden transmission exclusively by one type of channels. Some attempts towards application of hidden transmission were undertaken in studies related to: the steganographic router [12] as well as to the system for hidden transmission of information [4]. There are also other solutions that can be used for authentication procedures in networks. For

wireless networks to IEEE 802.11 such a mechanism is described in [13]. A similar mechanism is also applied to RF communication within the VHF bandwidth [14], [15].
The mechanism that is outlined in this paper combines various approaches to the issues how to apply hidden transmission to manage IT networks and was purposefully designed thus it would be operated in a heterogeneous environment and use the hidden layer to supervise the network infrastructure which is the unique feature.

3. Mechanism Description

Operation principle of the mechanism is based on use of voice transmission (phone conversation). Transmission of voice signals is carried out with use of various technologies: voice over IP (VoIP), phone calls within public switched telephone networks (PSTN) as well as connections with use of a military VHF radio stations.
The transmitted voice signal is considered as the transport layer for the binary signature of the watermark. Boundary components of the network (take-over points) that switch voice signals to subscribers can be furnished with suitable software HPI [3], [7] that make it possible to carry out actions on those components in remote manner. Remote commands with instructions to initiate required actions can be transmitted in a hidden manner by means of the voice signal.
The research studies employed three options of voice signals: male speech in English (track no. 1), male speech in German (track no. 2) as well as pop music (track no. 3). The watermarked records that had been processed with use of one of the two following methods: orthogonal frequency-division multiplexing (OFDM) [16] with its information capacity $P = 21$ bits as well as the method of drift correction modulation (DCM) [17] with two options of data payload $P = 84$ and $P = 147$ bits. Parameters of the records were the following: sampling frequency $f_S = 48000$ Hz, 16 bits per sample, mono mode.

3.1. Examination of Transmission Channels

In order to carry out the experiments it was necessary to examine individual transmission channels. The test consisted in transmission of a voice signal with an embedded digital watermark with further reception of the signal and recording it at the other end of the network segment. The recorded signal was then delivered to the watermark extractor where the binary signature of the watermark was obtained at the extractor output. In addition the binary signature bit error rate (BSBER – bit error rate of the binary signature embeded in watermark) was determined for the extracted binary signature of the watermark. The examination procedure covered the following types of transmission channels: RF channel of the NDHS-WiFi type where the voice signal was transmitted as VoIP phone call, PSTN telephone line as well as VHF radio channel. The aim of tests the performed tests was to find out whether a hidden transmission is feasible via such channels and to select optimum transmission parameters. Figure 1 presents

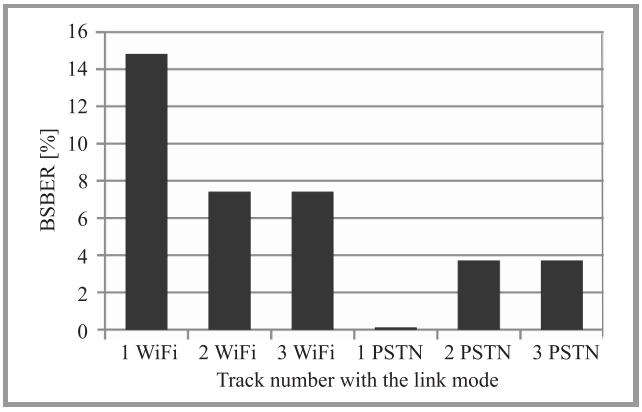

Fig. 1. Measurement results for the binary signature bit error rate when the OFDM method was used.

results for measurements of the bit error rate for the digital signature of transmitted watermarked tracks for signals determined with use of the OFDM method, transmitted via RF channels of the NDHS WiFi type as well as via a PSTN channel. Figure 2 shows corresponding results for

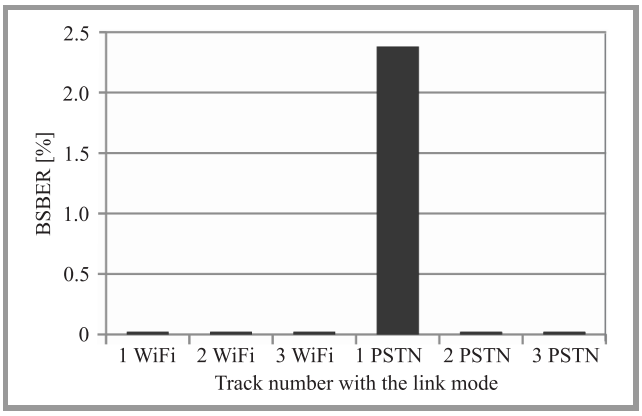

Fig. 2. Measurement results for the bit error rate when the DCM method was used ($P = 84$ bits).

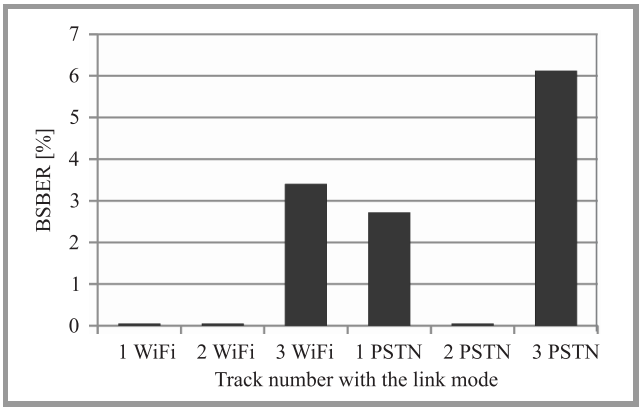

Fig. 3. Measurement results for the binary signature bit error rate when the DCM method was used ($P = 147$ bits).

signals where watermarks had been embedded with use of the DCM method and with the watermark data payload $P = 84$ bits. Similarly, Fig. 3 presents results for the DCM method and information capacity $P = 147$ bits. The analysis covered 30 seconds of a signal recorded at the other end of the examined transmission channel. The test demonstrated that the DCM method is less vulnerable to degradation of voice signals introduced by the IT networks under tests.

3.2. Examination of Bridges

For needs of the experiments the term of hidden protocol bridge (HPB) was introduced. The bridge is a hardware or software unit that is capable to handle the watermark embedded into a voice signal and to forward it between transmission channels of different types. Two bridge types were distinguished, i.e., the hardware bridge HPB-H that is incapable to process hidden information and merely forwards voice signals as well as the software bridge HPB-S that extracts binary signatures from voice signals transmitted via networks and uses corrective code extractors to recover information represented by the signatures. For that purpose two types of extractors can be used: the BCH type in case of the DCM method or the Reed-Solomon (RS) type when the OFDM method is used. Finally, the recovered information is recoded back into the watermark of the voice signal that is forwarded to that second network. In that way information to be forwarded in the hidden layer is refreshed. The completed experiments involved the following corrective codes: the BCH type ($n = 84$, $k = 28$, $t = 7$), where n – length of the code vector, k – length of the information vector and t – correction capacity of the code, another BCH type ($n = 147$, $k = 91$, $t = 7$) as well as the Reed-Solomon (RS) type ($n = 21$, $k = 9$, $t = 3$).

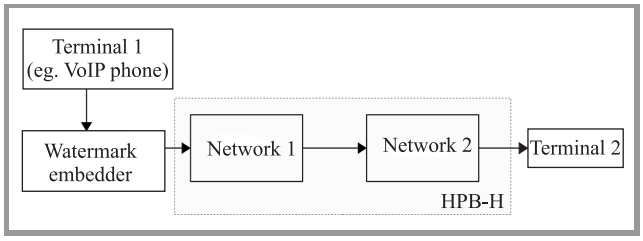

Fig. 4. General diagram of the hardware bridge HPB-H.

Figures 4 and 5 present general diagrams for individual bridge types. The following types of bridges were set up for the experiments: PSTN-NDHS WiFi as well as VHF-NDHS WiFi. Investigation of bridges included verification of their information bit error rates (IBER) for information recovered from the BCH and RS extractors. The calculated error rate served as the criterion to assess whether hidden transmission of commands to boundary appliances is possible or not.

Figure 6 presents measurement results for the bit error rate calculated for the hidden information (a control command) recovered from BCH and RS extractors for the hardware bridge PSTN-NDHS WiFi. One can clearly see that path no. 3 (pop music) is incapable to efficiently transmit control commands via such a bridge. In other cases corrective codes could recover the original form of information. Similar results were obtained for the software bridge (with information refreshment) of the PSTN-NDHS WiFi type. The obtained results can be seen in Fig. 7.

Experiment results for the software bridge VHF-NDHS WiFi are shown in Fig. 8. The graph contains only those paths that were substantially deteriorated so that extraction of the watermark binary signature proved infeasible. The next picture (Fig. 9) presents measurements results for the hardware implementation of the VHF-NDHS WiFi bridge. In such a case the OFDM method proved incapable to extract the watermark binary signature. On the other hand, the second path (male speech in German) with the watermark embedded by means of the DCM method proved sufficiently invulnerable to transmission degradation factors and recovery of the original command was possible.

3.3. Collaboration between Master Resident and Hidden Protocol Interpreter

The master resident is a specific component of the NDHS system as it is intended to supervise operation of individual stations that make up components of a hidden network (botnet) as it is the station where hidden protocol interpreters are installed. The hidden protocol interpreter enhances the forwarding station (router) with the functionality of a network-centric router [12]. The HPI unit analyzes streams of voice packages that pass through the specific router with the aim to detect hidden transmission or embeds a watermark into the forwarded voice signal. The master resident communicates with HPI units operated within the existing network in a hidden or open manner (depending on available possibilities and importance of information transmitted). The master resident makes the decision on the basis of information about data streams forwarded by every specific HPI unit and provides that HPI unit with relevant commands. The commands are always encrypted with use of the symmetric VMPC code. Encryption keys that are used to encode communication sessions between MR and HPI are stored in the MR database (repository) and are unique for each specific HPI unit. After receiving the command the HPI unit undertakes the required action. There are many possible actions, starting from simple recording of the voice signals through modification of these signals (injection of an additional content or extraction of some fragments of the voice package) up to disabling the entire voice signal or forwarding the latter to another subscriber. In extreme cases the entire components of the network infrastructure where the specific HPI is installed can be eliminated or some functions attributable to these components can be disabled.

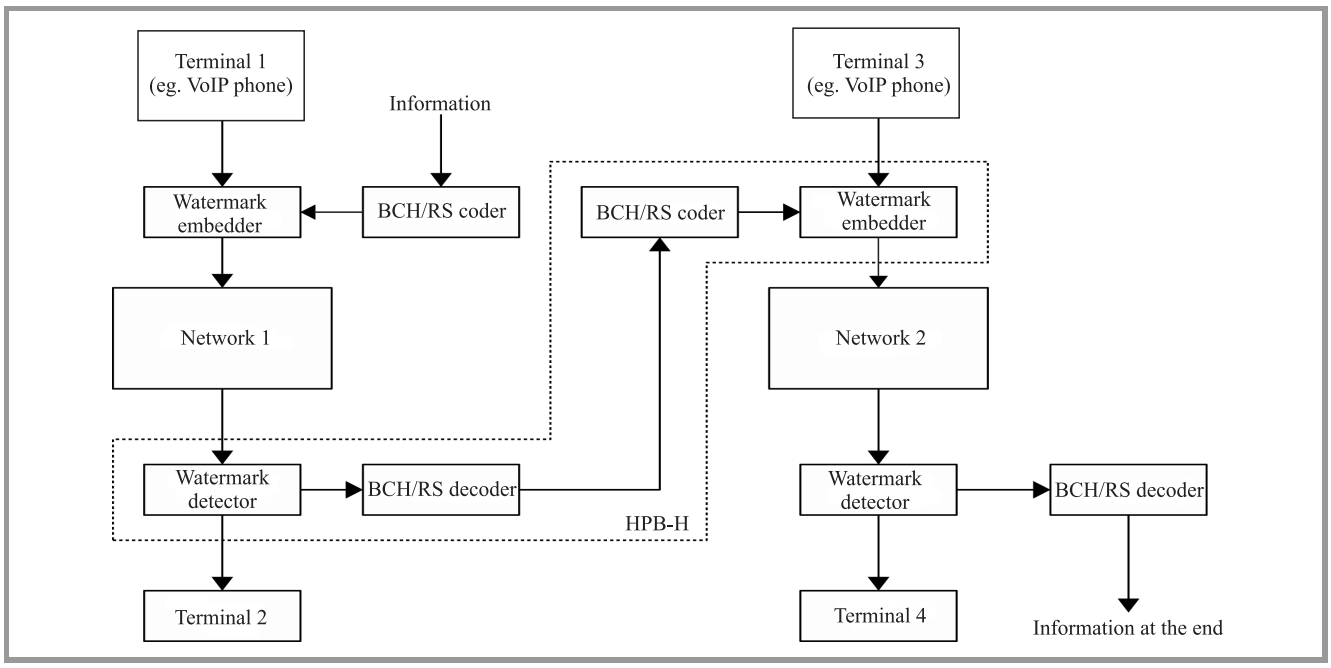

Fig. 5. General diagram of the software bridge HPB-S.

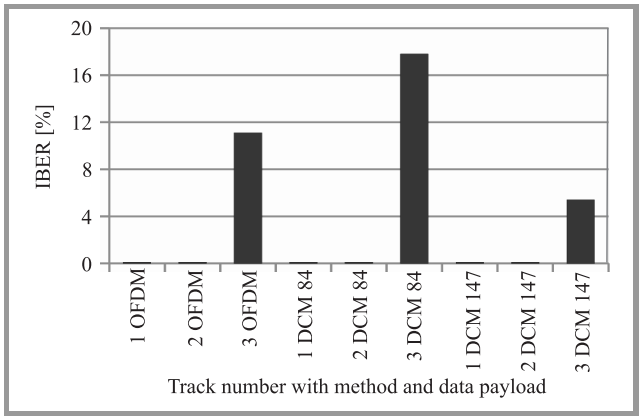

Fig. 6. Results for measurements of information bit error rates (IBER) for information recovered from the PSTN-NDHS WiFi bridge implemented as HPB-H.

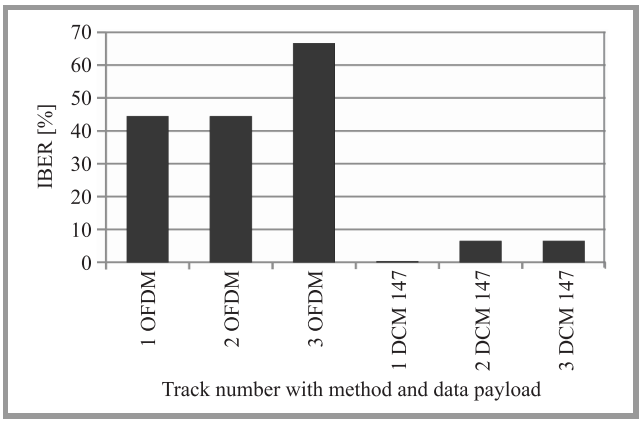

Fig. 8. Results for measurements of information bit error rates (IBER) for information recovered from the software bridge VHF-NDHS WiFi.

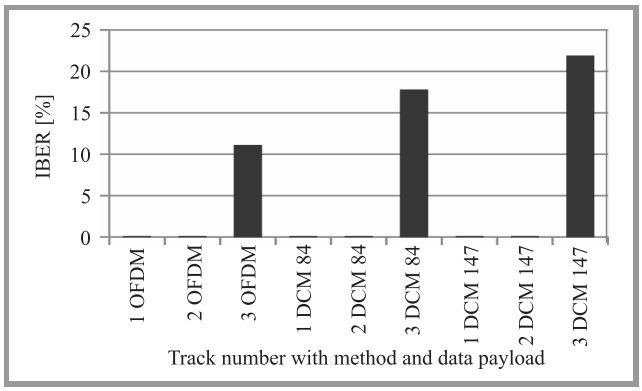

Fig. 7. Results for measurements of information bit error rates (IBER) for information recovered from the software bridge PSTN-NDHS WiFi.

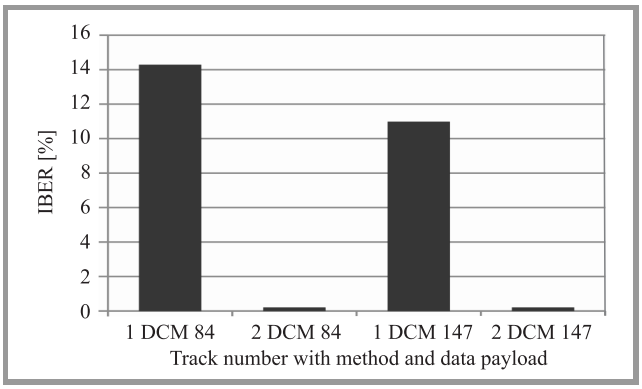

Fig. 9. Results for measurements of information bit error rates (IBER) for information recovered from the hardware bridge VHF-NDHS WiFi.

4. Implementation of the Mechanism

The described mechanism was implemented in practice on the basis of the GNU/Linux operating system. HPI units were developed as kernel modules whilst the MR represented an independent application developed in C programming language.

To confirm operability of the mechanism two hardware bridges were set up, namely VHF-NDHS WiFi as well as PSTN-VHF (in that way a heterogeneous network was developed) where two HPI were operated. The network layout with the established bridges is shown in Fig. 10.

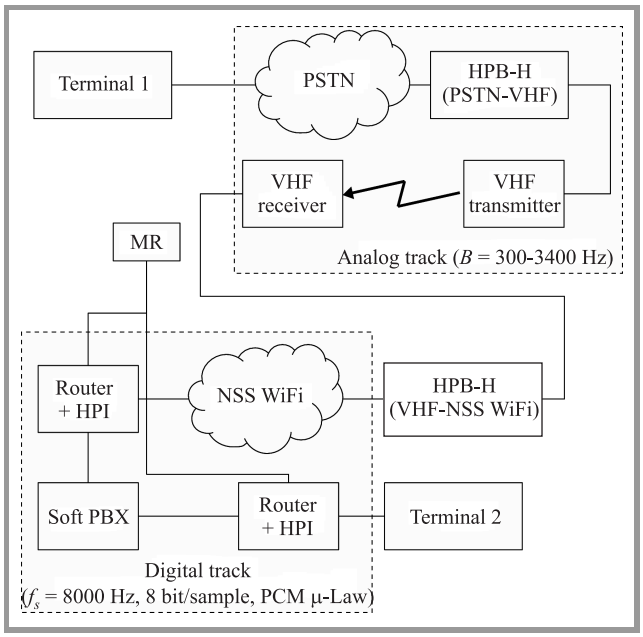

Fig. 10. Diagram of examined heterogeneous network (PSTN-VHF-NDHS WiFi).

The network was used to transmit voice packages with embedded watermarks equivalent to encrypted commands. The record no. 2 was selected for experiments (male speech in German) with the watermarks embedded with use of the DCM method (where the both information capacities were applied). The command was encrypted and then encoded with use of the BCH code. HPI units, after having the command decoded and decrypted, were forced to perform the specific operation, namely to have the voice message "conversation monitored, conversation monitored" introduced into the voice package transmitted between terminal 1 and terminal 2. The completed experiments confirmed the assumption that IT networks can be managed with use of hidden and confidential information transmitted via heterogeneous environment with use of HPI units, the master resident and HPB.

5. Conclusion

Nowadays none of the voice telephone systems (VoIP, PSTN, GSM) fails to be invulnerable to hidden transmission, which enables wide application of hidden transmission systems similar to the described one. Therefore there is the potential risk that the unauthorized hidden transmission shall be used to control components of network infrastructures. Consequently, development of mechanisms intended to safeguard the network against such an unintended use is an urgent must.

Acknowledgements

This paper has been co-financed from science funds granted within the years 2008–2010 as a research project of the Ministry of Science and Higher Education of the Republic of Poland no. 0018/B/T00/2008/34.

References

[1] http://sodaphish.com/files/ebks/try2innovate.com/downloads/E-books/Networking/Network%20Management.pdf

[2] B. Żółtak, "VMPC – One way function and stream cipher", in *Proc. 11th Int. Worksh. Fast Software Encryption 2004 FSE'2004*, Delhi, India, 2004.

[3] Z. Piotrowski, "The national network-centric system and its components in the age of information warfare", in *Safety and Security Engineering III*, M. Guarascio, C. A. Brebbia, And F. Garzia, Eds. Southampton, Boston, WIT Press 2009, pp. 301–309.

[4] Z. Piotrowski, "Effective method of the watermark embedding and decoding in the broadcast audio signal band", Ph.D. thesis, Military University of Technology, Warsaw, Poland, 2005.

[5] *NATO Glossary of Abbreviations Used in NATO Documents and Publications*, NATO Standardization Agency, 2010.

[6] *NATO MC 0064/10 – NATO Electronic Warfare Policy*, NATO Electronic Warfare Advisory Committee NEWAC, 2010.

[7] K. Wodecki, "Hidden protocol interpreter and its main features in the watermarking battle net", in *Proc. 2nd AFCEA Europe Student Conf.*, Brussels, Belgium, 2009.

[8] Z. Piotrowski, K. Sawicki, M. Bednarczyk, and P. Gajewski, "New hidden and secure data transmission method proposal for military IEEE 802.11 networks", in *Proc. Sixth Int. Conf. Intel. Inf. Hid. – Multim. Sign. Proces. 2010 IIHMSP 2010*, Darmstadt, Germany (submitted for publication).

[9] K. Szczypiorski, "HICCUPS: Hidden communication system for corrupted networks", in *Proc. 10th Int. Multi-Conf. Adv. Comp. Sys. ACS 2003*, Międzyzdroje, Poland, 2003.

[10] W. Mazurczyk and K. Szczypiorski, "Steganography in handling oversized IP packets", in *Proc. Int. Conf. Multime. Inf. Netwo. Sec. MINES 2009*, Wuhan, Hubei, China, 2009, vol. I, pp. 559–564.

[11] L. Frikha, Z. Trabelsi, and W. El-Hajj, "Implementation of a covert channel in the 802.11 header", in *Proc. Int. Wir. Commun. Mob. Comput. Conf. IWCMC 2008*, Crete Island, Greece, 2008, pp. 594–599.

[12] K. Szczypiorski, I. Margasiński, and W. Mazurczyk, "Steganographic routing in multi agent system environment", *J. Inf. Assur. Sec.*, vol. 2, iss. 3, pp. 153–154, 2007.

[13] T. E. Calhoun, R. Newman, and R. Beyah, *Authentication in 802.11 LANs Using a Covert Side Channel*, Atlanta, Georgia State University, 2009.

[14] Z. Piotrowski and P. Gajewski, "Novel method for watermarking system operating on the HF and VHF radio links", in *Computational Methods and Experimental Measurements XIII*, C. A. Brebbia and G. M. Carlomagno, Eds. Southampton, Boston, WIT Press 2007, pp. 791–800.

[15] Z. Piotrowski, L. Zagoździński, P. Gajewski, and L. Nowosielski, "Handset with hidden authorization function", in *Proc. Eur. DSP Educ. Res. Symp. EDERS 2008*, Tel Aviv, Israel, 2008, pp. 201–205.

[16] P. Gajewski, J. Łopatka and Z. Piotrowski, "A new method of frequency offset correction using coherent averaging", *J. Telecommun. Inf. Technol.*, vol. 1, pp. 142–146, 2005.

[17] Z. Piotrowski, "Drift correction modulation scheme for digital audio watermarking", in *Proc. Int. Conf. Multime. Inf. Netw. Secur. MINES 2010*, Nanjing, China (submitted for publication).

Krzysztof Sawicki received his M.Sc. degree in communications from the Military University of Technology (MUT Warsaw) in 2009. Currently he is a Ph.D. student at the Electronics Faculty at MUT. He is interested in information hiding technology especially wireless networks steganography.

e-mail: Krzysztof.Sawicki@wat.edu.pl
Military University of Technology
Kaliskiego st 2
01-489 Warsaw, Poland

Zbigniew Piotrowski received the M.Sc. and Ph.D. degrees in communications from the Military University of Technology (MUT), Warsaw, in 1996, and 2005 (with honours), respectively. At present he is a DSP engineer in the Telecommunication Institute (EF MUT). His main areas of interest are speech and audio processing, telecommunication systems engineering and information hiding technology.

e-mail: Zbigniew.Piotrowski@wat.edu.pl
Military University of Technology
Kaliskiego st 2
01-489 Warsaw, Poland