Telecommun Syst (2012) 49:161–162
DOI 10.1007/s11235-010-9361-8

Toward network steganography detection

Krzysztof Szczypiorski · Wojciech Mazurczyk

Published online: 23 June 2010

Network steganography is a recently introduced, general term which describes all information hiding methods that may be used to hide secret data in the normal data transmissions of users. While sending encrypted information, enabled by some cryptographic algorithm, protects messages from being captured by unauthorized parties, steganographic techniques enable concealing the fact that a message is being sent, and if not detected, make the sender and receiver "invisible".

Network steganography methods may be viewed as a threat to network security, as they may be used as a tool for confidential information leakage, for example. For this reason, it is important to identify possibilities for covert communication, as knowledge of information hiding procedures may be used to develop countermeasures. To detect existence of hidden data inside the network traffic steganalysis methods are used. Steganalysis tools identify suspected network communication and try to determine whether or not it carries hidden information. If it is possible they should also recover hidden information

Steganographic techniques arise and evolve with the development of network protocols and mechanisms, and are expected to be used in secret communication or information sharing. Now, it becomes a hot topic due to the wide spread of information networks, e.g., multimedia services in networks and social networks.

K. Szczypiorski · W. Mazurczyk (✉)
Faculty of Electronics and Information Technology,
Institute of Telecommunications,
Warsaw University of Technology, 15/19 Nowowiejska Str.,
00-665 Warsaw, Poland
e-mail: wmazurczyk@tele.pw.edu.pl

K. Szczypiorski
e-mail: k.szczypiorski@tele.pw.edu.pl

The First International Workshop on Network Steganography (IWNS 2009) which was co-located with International Conference on Multimedia Information Networking and Security (MINES 2009) is intended to integrate the researchers and practitioners focused on such areas of research as steganography, steganalysis (steganology), and digital forensics. We aim at investigate the potential applications of such solutions, their detection, and discuss the future research topics.

The first edition of the IWNS took place on November 18–20, 2009 in Wuhan, Hubei, China. We are delighted to present in this special issue a selection of 11 papers resulting from the workshop.

It is important to identify new information hiding methods that may be utilized in communication networks to develop countermeasures. Wojciech Mazurczyk and Krzysztof Szczypiorski in their paper "Evaluation of Steganographic Methods for Oversized IP Packets" propose new steganographic methods that may be applied to mechanisms for handling oversized IP packets for both version of IP protocol: 4 and 6. In "Covert Timing Channel with Distribution Matching" Guangjie et al. design a reliable and undetectable covert timing channel with distribution matching. The approach processes the traffic as fixed-length fragment and obtains the histogram of the delays, then use the binary coding method to embed the message bits.

Hiding information within multimedia stream like video stream is a recent new trend. The paper by Ke Liao et al. "Lightweight Information Hiding in H.264/AVC Video Stream" deals with this topic by proposing new interesting real-time information hiding algorithm on latest H.264/AVC video coding standard. The information is embedded into the Trailing Ones of 4×4 blocks during the Contextbased Adaptive Variable Length Coding (CAVLC) process. They

prove that this algorithm is efficient with low computational complexity.

Xinpeng Zhang and Shuozhong Wang in their paper "Efficient Data Hiding with Histogram-Preserving Property" describe a novel efficient data hiding scheme with a histogram-preserving property is proposed in this work that may be used for improving the steganographic security.

The paper "Lightweight Secure Multimedia Distribution Based on Homomorphic Operations" by Shiguo Lian and Xi Chen introduces a secure media distribution scheme, which distributes different media copy to different customer in a secure and efficient manner and is able to trace illegal redistribution.

The paper by Krzysztof Szczypiorski "A Performance Analysis of HICCUPS—A Steganographic System for WLAN" presents efficiency and the cost of HICCUPS (HIdden Communication system for CorrUPted networkS) in WLANs (Wireless Local Area Networks). The analysis relies on the original CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) 802.11 Markov chain-based model.

Hongjie He and Jiashu Zhang in their paper "Cryptanalysis on Majority-Voting Based Self-Recovery Watermarking Scheme" examined the security of the Wang-Chen self-recovery watermarking scheme and show that it is vulnerable to the XOR-equivalent attack.

Amit Phadikar, Santi P. Maity and Claude Delpha in the paper "Image Error Concealment and Quality Access Control Based on Data Hiding and Cryptography" showed a data hiding scheme that integrates the dual purpose of error concealment and quality access control of digital images in a single platform.

The paper "A Reliable Watermarking Algorithm Based on Wavelet Transform for Satellite Images" by Mehdi Abolfathi and Rasoul Amirfattahi turns around novel algorithms, building systems with higher performance using multiresolution decomposition especially includes a new watermarking scheme for satellite images.

In "Spectrum-estimation based lossless information recovery for sparse array patterns" Guorui Feng, Zhenxing Qian and Xinpeng Zhang proposed a simple and efficient approach to predict high-similar interpolation image from its sparse pattern and spectral expansion.

Santi P. Maity, Seba Maity, and Jaya Sil describe in their paper "Multicarrier Spread Spectrum Watermarking for Secure Error Concealment in Fading Channel" a novel multicarrier spread spectrum watermarking scheme for the application of image error concealment using multicarrier-code division multiple access (MC-CDMA) with binary phase shift keying (BPSK) transmission in Rayleigh fading channel.

We believe that this Special Issue will contribute to enhancing knowledge in information hiding techniques applications as well as their detection possibilities. In addition, we also hope that the presented results will stimulate further research in the important areas of information and network security.

Krzysztof Szczypiorski holds an M.Sc. (1997) and a Ph.D. (2007) in telecommunications both with honours from the Faculty of Electronics and Information Technology, Warsaw University of Technology (WUT), and is an Assistant Professor at WUT. He is the founder and head of the International Telecommunication Union Internet Training Centre (ITU-ITC), established in 2003. He is also a research leader of the Network Security Group at WUT (secgroup.pl). His research interests include network security, steganography and wireless networks. He is the author or co-author of over 110 publications including 65 papers, two patent applications, and 35 invited talks.

Wojciech Mazurczyk holds an M.Sc. (2004) and a Ph.D. (2009) in telecommunications from the Faculty of Electronics and Information Technology, Warsaw University of Technology (WUT, Poland) and is now an Assistant Professor at WUT and the author of over 40 scientific papers and over 25 invited talks on information security and telecommunications. His main research interests are information hiding techniques, network security and multimedia services, and he is also a research leader of the Network Security Group at WUT (secgroup.pl). Personal website: http://mazurczyk.com.