ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

A Study on Network Steganography Methods

Amritha Sekhar[1], Manoj Kumar G.[2], Prof. (Dr.) M. Abdul Rahiman[3]

Student, Department of CSE, LBS Institute of Technology for Women, Thiruvananthapuram, India [1]

Associate Professor, Department of CSE, LBS Institute of Technology for Women, Thiruvananthapuram, India [2]

Pro Vice Chancellor, Kerala Technological University, Thiruvananthapuram, India [3]

Abstract: Steganography is a technology used since years for the communication of messages secretly. These secret messages are put inside honest carriers. Carriers can be digital images, audio files, video files and so on. The limitation in sending concealed longer messages has been overcoming by the inclusion of video files as carriers. Popular internet services such as Skype, BitTorrent, Google Suggest, and WLANs are targets of information hiding techniques. Nowadays, plotters are not only using the carriers but also the protocols for communication that regulate the path of the carrier through the Internet. This technique is named Network Steganography.

Keywords: Protocol Steganography, Network Steganography, Cryptography.

I. INTRODUCTION

The term Steganography originates from the ancient Greek words steganos – covered, concealed or protected and graphein – writing. Likewise, the term cryptography originates from kryptos – hidden or secret and graphein [1]. Steganography and cryptography can be applied in combination; both are orthogonal [2]. Both the terms have closer meaning. But both need to be considered as different techniques for hiding information.

Network steganography is a fast developing field and immature branch of information hiding [3]. Krzysztof Szczypiorski at Warsaw University of Technology introduced network steganography and a steganographic method for wireless local area networks (WLANs) - Hidden Communication System for Corrupted Networks, HICCUPS. The gist of network steganography is the exploitation of Open System Interconnection Reference Model (OSI RM) protocols. Wojciech Mazurczyk and Krzysztof Szczypiorski published the first paper about network steganography in Internet Protocol telephony, introducing the concept of Lost Audio Packet Steganography, LACK.

The classification of network steganography methods can be based on the protocol functions associated with the OSI RM layers. These methods utilize one or more protocols simultaneously. The steganographic method that utilizes single network protocol is termed Intra-protocol network steganography and the one which utilizes more than one network protocol is termed Inter-protocol network steganography [1]. Padding Steganography (PadSteg) is one of the inter-protocol steganographic methods.

The classification of intra-protocol network steganographic methods is based on the type of modification of Protocol Data Unit (PDU) and modification of time- relations between PDUs. There exists methods which encompass the modification of PDUs as well as the modification of time-relations between PDUs, such methods are considered ”hybrid” [10] e.g. LACK, and Retransmission Steganography (RSTEG). Modification of PDUs includes either modification of payload, modification of protocol specific fields (e.g. Wireless Padding (WiPad), specific methods of Stream Control Transmission Protocol (SCTP)) or both (hybrid , e.g. HICCUPS), while the modification of time-relations between PDUs includes either reordering of the PDUs by SCTP multistreaming based methods, intentional losses of PDUs or modification of inter-PDU time delay.

The information transfer over the internet is always vulnerable to attacks. Hackers or intruders are always listening to the transmission channels to tap the information and make use of it. Cryptographic algorithms always could protect information from such malicious users to a greater extent. But encrypting the information, does not make it hidden. It becomes unreadable, but it exists as data itself. This limitation is overcome by the introduction of Steganography. Steganography is the act of concealing and thus protecting the information. It could hide the existence of the information. The information can be made hidden in carriers. These carriers can be text, audio, image, video files and protocol header fields.

Covert channel is the channel used in Steganography for the anonymous transfer of information. It is not a planned channel, but is a carrier of the secret information. Covert channel has a critical role in the area of information hiding or hidden communication. It allows the transmission of information by an unauthorized process. Covert channel is designed in such a way that it is hidden within the normal communication traffic of authorized logical channel. The violation of the security policies of the network system is the basis for enabling hidden communication [16]. Numerous network protocols can be made a vehicle to carry out covert communication [17].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

Covert channel is not an anticipated channel for the communication process. It makes use of the bandwidth of other legitimate channels for the transmission of secret data. The application of Steganography in network protocol headers also succeed in hiding the existence of the data rather than making the data impossible to read. Packets act as the cover object in this scenario.

Information hiding methods have been using network protocol header fields as covert channels. The term 'Network Steganography' was first introduced in 2003 by Krzysztof Szczypiorski[13]. The information hiding in TCP/IP protocols was illustrated by Craig Rowland [18]. Few fields in the TCP header can be used for covert communication.

Section II of this paper discusses the evolution of Steganography. Section III discusses the recent developments in the field of network steganography. Section IV discusses various network steganography methods. Section V deals with the various TCP/IP header fields that can be made use for covert communication. Section VI briefs the future possible applications and Section VII concludes the discussion.

II. EVOLUTION OF STEGANOGRAPHY

Steganography, meaning hidden writing, has been used to mask secret messages. In olden days, physical or ordinary objects were selected as carriers for hidden information [9]. The first written report of the Steganography use is imputed to the Greek historian Herodotus. It involved disguising the secret message within a hare corpse. The physical object or the carrier had to be shifted from one communication party to the other without arising any hunch.

Histiaeus tattooed secret message on the shaved head of his slave and waited for the hair to grow. The slave is sent to the intended receiver and the head was shaved off to read the message. Another noteworthy method used is the use of wooden tablets for the communication of secret messages [3], [9]. These were coated with a layer of wax. The woods were the carrier of the stenograms. Only the cognizant receiver would be able to read the message by removing the wax coated. Pliny the Elder invented the sympathetic ink or invisible ink which is nothing but the milk of the tithymalus plant. The messages written by this ink would appear only when it is heated. Other steganographic methods used in ancient days include Cardano Grille − a stiff sheet perforated with rectangular holes, Vexierbild − picture puzzle, Eggs, Beer barrel − by smuggling messages inside the stopper, Musical notes − each note corresponds to a letter, Newspaper code − by punching holes above letters, combination of invisible ink and musical notes and Microdots − by shriveling text down to a dot [3], [9]. In the 1980s, user identities were encoded in the spaces between words, termed watermarking. Today's steganographic methods make use of computers and networks. The most popular trends in digital steganography are digital media Steganography, linguistic Steganography and network Steganography [9]. Digital media steganography includes image Steganography, video Steganography and streaming Steganography. Alongside these, the one target of increased interest is the network Steganography.

III. RECENT DEVELOPMENTS

Recent information hiding solutions exploit popular P2P services like Skype, P2P file sharing systems like BitTorrent, search features like Google Suggest, multimedia and real-time services like IP telephony, new network protocols like SCTP, wireless network environments and many more [2].

Steganographers exploit services if it has large volume of traffic that can be altered to bring forth a covert channel (e.g. IP telephony). Transcoding Steganography (TranSteg) is a steganographic method which targets IP telephony services. Another steganographic method, Skype Hide (SkyDe) targets P2P services like Skype. A steganographic method has been introduced for P2P file sharing services, StegTorrent. The StegSuggest steganographic method targets the feature, Google Suggest.

Wireless networks are very popular, dynamically evolving network steganography sub-field. Information hiding tech- niques target wireless networks also. WiPad, a stegano- graphic method for WLANs, was introduced by Mazurczyk and Szczypiorski.

IV. NETWORK STEGANOGPRAPHIC METHODS

The following are the existing network steganograhic methods.

A. HICCUPS

HICCUPS stands for Hidden Communication System for Corrupted Networks. It is the steganographic system ded- icated to shared medium networks including WLANs. The freshness of HICCUPS is the use of procure communications network fortified with cryptographic mechanisms to provide steganographic system and proposal of a new protocol with bandwidth allocation based on corrupted frames [13]. It is a steganographic system for hidden group with common knowledge. A station sends a corrupted frame, i.e., a frame with an incorrect checksum. Remaining hidden stations change their mode of operation to the corrupted frame mode. To transmit steganograms, HICCUPS replaces payload of intentionally corrupted frames at the transmitter [10].

B. LACK

LACK stands for Lost Audio Packet Steganography. It is the steganographic method which targets IP telephony. There exists a fact that in typical multimedia communication protocols (e.g. Real-time Transport Protocol (RTP)), overly detained packets are not used by the receiver to rebuild the transmitted data. Those packets are reckoned useless and did cast away [14]. To transmit

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

steganograms, LACK replaces payload of intentionally delayed voice packets at the transmitter. And those packets will be recognized as lost and dropped at the receiver [10].

The steps are:

- The voice packets stream is generated at the transmitter.
- One of the voice packets is chosen to be intentionally delayed.
- Chosen voice packet's payload is replaced with steganogram and it is delayed.
- After the delay timer expires, delayed voice packet is sent to the receiver.
- Usual receiver treats excessively delayed voice packet as lost and it drops such packet.
- LACK-aware receiver extracts steganogram from delayed voice packet.

C. RSTEG

RSTEG stands for Retransmission Steganography. RSTEG is a new steganographic method which is meant for a wide class of protocols that uses retransmission mechanisms. The main novelty in RSTEG is that it does not acknowledge a packet which is received successfully, thereby intentionally invoking its re-transmission. Instead of user data in the payload field, the retransmitted packet carries a steganogram [12]. In RSTEG, to transmit steganograms, the receiver intentionally does not acknowledge received packets to invoke retransmission. The sender replaces the payload with the secret message which is recognized as a steganogram by the receiver.

One possible detection method is statistical steganalysis based on the network retransmission rate. RSTEG is very hard to detect, if it is used reasonably [10].

D. SCTP Multistreaming-based Method

SCTP is Stream Control Transmission Protocol. SCTP improves by mixing components of TCP and UDP. In this method, subsequent chunks are transmitted within streams determined by bits of steganogram. Let the steganogram be 10011100 and let there be 4 streams - Stream 1, 2, 3 and 4 [10]. The steps are:

- Sender wants to transmit following hidden bits: 10011100.
- First two hidden bits are 10, so a chunk within stream 3 is sent.
- Next a chunk within stream 2 is sent in order to transmit bits 01.
- Then a chunk within stream 4 - bits 11.
- Finally a chunk within stream 1 - bits 00.

E. PadSteg

PadSteg stands for Padding Steganography. It is the steganographic system for LANs. PadSteg is known to be the first inter-protocol steganography solution. By the term inter-protocol, it means the usage of relation between two or more protocols from the TCP/IP stack to enable secret communication [10].

PadSteg replaces padding bits of the short Ethernet frames with steganograms. The known Etherleak vulnerability makes PadSteg not trivial to detect. Etherleak is caused by ambiguous standardization that makes implementation of padding mechanism vary. In result, some NIC drivers handle frame padding incorrectly and fail to fill it with zeroes [4].

PadSteg utilizes Address Resolution Protocol (ARP) to identify all PadSteg-capable hidden nodes and also to perform so called carrier-protocol hopping during hidden exchange. Carrier-protocol hopping is an ability to negotiate carrier-protocol of the steganograms during hidden communication.

PadSteg actually exchanges data with short frames of protocols such as Transmission Control Protocol (TCP), ARP, User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP).

F. TranSteg

TranSteg (Trancoding Steganography) is a middlingly new IP telephony steganographic method.

It functions by compressing open data to make space for the steganogram. This is achieved by means of transcoding. It offers high steganographic bandwidth. TranSteg retains good voice quality. It is harder to detect than any other VoIP steganographic methods that exist today. In TranSteg, the hidden information is extracted and the speech data is practically restored to what was originally sent, after the steganogram reaches the receiver. This is a brobdingnagian advantage when TranSteg is compared with the existing VoIP steganographic methods. In all other methods, hidden data can be extracted and removed, but the original data cannot be restored because it was previously erased due to a hidden data insertion process [15].

TranSteg is intended for a broad class of multimedia and real-time applications e.g. IP telephony. TranSteg can be exploited in other applications or services like video streaming, wherever a possibility exists to efficiently compress the overt data. The typical approach to steganography is to compress the covert data in order to limit its size, because it is reasonable in the context of a limited steganographic bandwidth [10]. TranSteg utilizes compression of the overt data to make space for the steganogram. TranSteg for IP telephony is using transcoding of the voice data from a higher bit rate codec - overt codec to a lower bit rate codec - covert codec with the least possible degradation in voice quality.

TranSteg operates as follows:

- For a chosen RTP voice stream, find a codec that will result in a similar voice quality but smaller voice payload size than the originally selected.

Then, transcode the voice stream.

At this step, the original voice payload size is intentionally unaltered and the change of the codec is not indicated.

Instead, after placing the transcoded voice payload, the remaining free space is filled with hidden data. If Secure Real-time Transport Protocol (SRTP) is utilized for RTP streams, TranSteg detection is very difficult to perform.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

Group of methods	Pros	Cons
Methods that modify protocol PDU/PCI	–High steganographic bandwidth –Easy implementation –No sender-receiver synchronization required	–Potential loss of some of the protocols' functionality –Easy to detect
Methods that modify protocol PDU/SDI	–Harder to detect than PCI-based methods –No sender-receiver synchronization required	–Lower steganographic bandwidth than PCI-based methods –Harder to implement than PCI-based methods –Potential deterioration of quality of user data
Methods that modify protocol PDU/Mixed	–High steganographic bandwidth –Hard detection –No sender-receiver synchronization required	–Harder to implement than PCI-based and SDI–based methods –Potential increased transmission error rate
Methods that modify time-relations between PDUs	–Easy implementation –Hard detection	–Very low steganographic bandwidth –Sender-receiver synchronization required –Increased transmissions' delays
Hybrid methods	–Hard to detect –No sender-receiver synchronization required –High steganographic bandwidth –Easy implementation	–Potential deterioration of quality of user data

Table 1. Comparison of steganographic methods groups [22]

G. SkyDe

SkyDe stands for Skype Hide which is a new steganographic method. SkyDe uses Skype-encrypted silent packets to provide means for secret communication. Skype does use any silence suppression mechanism. Therefore, it is possible to reprocess those packets that have no voice signal, for steganographic purposes. SkyDe experiments prove that the method is viable. Also, results show that SkyDe offers high steganographic bandwidth.

Voice over IP (VoIP) or IP telephony is a real-time service. It enables users to make phone calls through data networks that use an IP protocol. One of the most popular of the IP telephony systems is Skype. It is a proprietary P2P telephony service. Skype is owned by Microsoft [5].

Because of Skype traffic encryption, SkyDe can replace the encrypted silence with encrypted secret data. This makes SkyDe hard to detect. Packets with silence have low impact on Skype conversation quality. To provide undetectability and low voice quality distortion SkyDe that utilizes 30% of all packets with silence is advised [10]. This gives almost 2 kbits steganographic bandwidth.

H. StegTorrent

StegTorrent is a new network steganographic method. It is intended for the popular P2P file transfer service - BitTorrent. StegTorrent is developed for encoding classified data or information in transactions via BitTorrent. It works on the basis of reordering data packets in the peer to peer data exchange protocol. Some of the existing steganographic methods also reorder packets, but they need synchronization. StegTorrent doesn't.

BitTorrent is a P2P file sharing system that allows its users to distribute large amounts of data over IP networks [6]. A BitTorrent user shares a file or part of a file with so many recipients at once. This is the advantage taken up by StegTorrent. [7].

In the clandestine communication scenario, both the secret data senders and receivers are in control of a number of BitTorrent clients and their IP addresses are known to each other. It is not at all necessary to have any knowledge about the topology of the network. The hidden data sender uses the modified BitTorrent client, i.e., the StegTorrent client. This client then shares a resource downloaded by another StegTorrent client. And that consists of a controlled group of BitTorrent clients [6].

I. StegSuggest

StegSuggest is the steganography method that targets Google Suggest. Google Suggest service's suggestions within Google search are utilized as a hidden data carrier.

Google Suggest was created to aid a user bump the right phrase by suggesting and completing popular phrases automatically while typing. StegSuggest is another approach to attack Google searches. Google Suggest is based on Asynchronous JavaScript and XML (Ajax) technology. It brings up a list of 10 most popular related search phrases as the user types. It integrates Document Object Model (DOM), HTML/XHTML, Cascading Style Sheets (CSS), Extensible Markup Language (XML), JavaScript etc. Web applications that uses Ajax can retrieve data from the server asynchronously. This retrieval will neither disrupt the display nor behavior of the page which is loaded currently.

One attack intercepts the suggestions from Google server. It adds a word to the end of each of the suggested phrases [11]. The hidden receiver extracts these appended words and then converts it into a meaning message with the aid of a pre-shared lookup table.Google Suggest uses HTTP and TCP protocols. Both of them have been used for exchanging web pages. StegSuggest works as follows:

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

When user begins typing a search phrase into the search field, once in a while, these characters are sent to the Google server in HTTP GET message [8]. Google server returns a list of the most popular search phrases in HTTP OK message. The list is then presented to the user in a drop-down list. While the user is typing, HTTP GET messages are sent frequently. This means that during search for particular phrase, numerous HTTP messages will be exchanged. Each HTTP request may carry at least one or more characters of the search phrase.

V. USING PROTOCOL FIELDS

Fig. 1 shows the TCP header. The Options field is used to provide additional functionality or optional parameters that may be used by the sender or the receiver, whereas the 32 bit Sequence number field is used to identify the current position of the data byte in the segment.

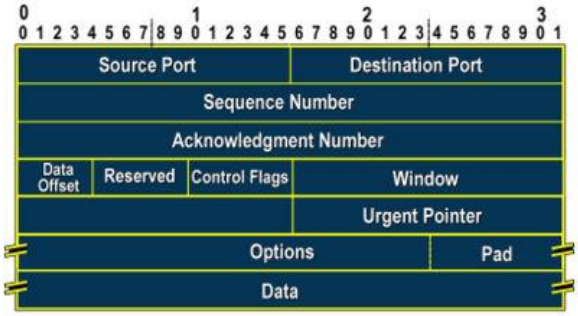

Figure 1. TCP Header.

Fig. 2 shows the IP header. In the IP header, the 8 bit ToS field is not used by many of the network systems. The 16 bit ID field helps the receiver in reassembling the datagram fragments. The value in the ID field is copied to all fragments when a fragmentation occurs. The Flag field has 3 reserved bits – X (Reserved), DF (Do not Fragment) and MF (More Fragments). The use of DF bit in covert communication requires prior knowledge about the MTU [18]. In [19], a method of covert communication by manipulating the lower order bits of the TCP timestamp field has been presented.

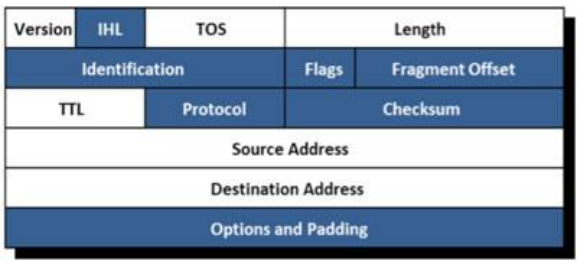

Figure 2. IP Header.

From the analysis made in [6], it is concluded that the use of most of these header fields in carrying out network steganography, can be easily detected. Therefore, it is necessary to have new systems that are capable for the effective transmission of secret information across the network.

VI. FUTURE APPLICATIONS

Network Steganography has a lot of future applications for malicious software. The application of the aforementioned network steganographic methods leads to more sophisticated malware. The covertness of malevolent programs on smart phones can be increased in the future. This possibility is dra- matically doubled in smart phones because the multimedia capability lets to create and use a video range of carriers e.g. audio, video, images or Quick-Response (QR) codes. Another reason is the availability of a full featured TCP/IP stack. It gives the possibility to interact with desktop-class services, thereby completely utilizing all the already available network methods for computing devices. Also, covert channels can be made exploitable based on VoIP and P2P, since the plethora of the adopted OS allows developing sophisticated applications. Network Steganography has been emerging into new and new domains. The stealthiness of illegal data exchange can be increased. Network Steganography can have tremendous influence to industrial espionage when it comes to data leakage.

VII. CONCLUSION

Network Steganographic methods are getting more so-phisticated. They are becoming harder to detect. New and new data carriers could be developed. It must be highlighted that as new and popular steganographic methods evolve, the data traffic of genuine internet users will also be utilized by network steganograhers. The network steganography threat can affect all internet users. This would lead to legal as well as ethical problems. Recently, there has been a significant increase in the development and application of network steganographic methods for malicious purposes.

This in turn has increased the qualities, capabilities and covertness of the network steganography. Network steganography would be applied in an increasing manner in each and every future malware or malicious activities. But, there lacks effective countermeasures. Therefore, an additional research is a critical need in the field of network steganography which would formulate universal countermeasures.

Network steganography is the art of concealing information inside protocol headers i.e., the secret information is made hidden in the unused fields of headers of the protocols such as TCP/IP. The need for secure hidden communication welcomes new and new reliable methods using which the purpose can be fulfilled.

Though several methods have been introduced in this area of security, some of them fail to meet the goal, while others pave a way for the effective communication of the covert information.

In this method, by the introduction of time as the critical factor, we succeed in achieving an extended security by reducing the effect of malicious attacks and thereby the recovery of the hidden information becomes more or less infeasible.

DOI 10.17148/IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)
International Conference on Recent Trends in Computing and Communication (ICRTCC 2015)
Cochin College of Engineering & Technology
Vol. 4, Special Issue 1, June 2015

ACKNOWLEDGEMENT

The author would like to thank her guide, **Mr. Manoj Kumar G.,** Associate Professor, LBS Institute of Technology for Women, Thiruvananthapuram and Prof. (Dr.) M. Abdul Rahiman who encouraged her throughout the preparation of this paper.

REFERENCES

[1] J. Lubacz, W. Mazurczyk and K. Szczypiorski, Principles and Overview of Network Steganography, IEEE Communications Maga- zine, vol. 52, no.5, May 2014.
[2] S. Wendzel, W. Mazurczyk, L. Caviglione and M. Meier, Hidden and Uncontrolled - On the Emergence of Network Steganography Threats, ISSE, Brussels, Belgium, 2014.
[3] E. Zieliska, W. Mazurczyk and K. Szczypiorski, Trends in Steganogra- phy, In: Communications of the ACM, 57(2), pp. 86-95, March 2014.
[4] B. Jankowski, W. Mazurczyk, K. Szczypiorski, PadSteg: Introducing inter-protocol steganography, In: Telecommunication Systems: Mod- elling, Analysis, Design and Management, Vol. 52, Iss. 2, pp. 1101-1111, 2013
[5] W. Mazurczyk, M. Kara, K. Szczypiorski, SkyDe: a Skype-based Steganographic Method, Int'l J. Computers, Communications & Con- trol, 8(3), pp. 389-400, June 2013.
[6] P. Kopiczko, W. Mazurczyk and K. Szczypiorski, StegTorrent: a Steganographic Method for the P2P File Sharing Service, IEEE Security and Privacy Workshops, 2013.
[7] J. Lubacz, W. Mazurczyk and K. Szczypiorski, 4 New Ways to Smuggle Messages across the Internet, IEEE Spectrum, 2013
[8] P. Biaczak, W. Mazurczyk and K. Szczypiorski, Sending Hidden Data via Google Suggest, ICTSM, 2011, Prague, Czech Republic, pp. 121-131.
[9] J. Lubacz, W. Mazurczyk and K. Szczypiorski, Vice over IP, IEEE Spectrum, pp. 40-45, February 2010.
[10] URL: www.stegano.net
[11] URL:http://www.technologyreview.com/view/529071/the-growing-threat-of-network-based-steganography/
[12] W. Mazurczyk, M. Smolarczyk and K. Szczypiorski, Retransmission steganography and its detection, Soft Comput. 15(3): 505-515 (2011).
[13] K. Szczypiorski, HICCUPS: Hidden Communication System for Cor- rupted Networks, In Proc. of The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, pp. 31-40, October 22-24, 2003 - Midzyzdroje, Poland.
[14] W. Mazurczyk, Lost audio packets steganography: the first practical evaluation, Security and Communication Networks 5(12): 1394-1403, 2012.
[15] A. Janicki, W. Mazurczyk and K. Szczypiorski, Steganalysis of transcoding steganography, Annales des Tlcommunications 69(7-8): 449-460,2014.
[16] R.M. Goudar, Pankaj Joshi, "Information Security through Steganography using TCP/IP Header Fields", Intl. Journal of Next Generation Computer Applications, vol.1, issue 4, Dec. 2012.
[17] S. Zander, G. Armitage and P. Branch, "A survey of covert channels and countermeasures in computer network protocols" IEEE communication surveys, 3rd Quarter 2007, vol. 9, no. 3, pp. 44-57.
[18] C. Rowland. Covert Channels in the TCP/IP Protocol Suite. First Monday, Peer Reviewed Journal on the Internet, 2(5), January 1997.
[19] J. Giffin, R. Greenstadt, P. Litwack, and R. Tibbetts, "Covert Messaging Through TCP Timestamps." Massachusetts Institute of Technology - MIT, USA, 2002.
[20] S. J. Murdoch and S. Lewis. Embedding Covert Channels into TCP/IP. In Information Hiding: 7th International Workshop, volume 3727 of LNCS, pages 247–261. Springer, 2005.
[21] Abdel-Karim Al Tamimi, Performance Analysis of Data Encryption Algorithms, aa7@wustl.edu.
[22] J. Lubacz, W. Mazurczyk, K. Szczypiorski, "Principles and Overview of Network Steganography", IEEE Communication Magazine, vol. 52, no. 5, May 2014