ICIC Express Letters
Volume **10**, Number **10**, October **2016**

 ISSN 1881-803X
pp. **2421–2427**

MULTICAST COVERT TIMING CHANNELS WITH UNEQUAL ERROR PROTECTION

Lihua Zhang[1], Guangjie Liu[1], Weiwei Liu[1], Jiangtao Zhai[2] and Yuewei Dai[2]

[1]School of Automation
Nanjing University of Science and Technology
No. 200, Xiaolingwei Ave., Nanjing 210094, P. R. China
zlh6013@163.com; {gjieliu; lwwnjust5817}@gmail.com

[2]Department of Electronics and Information
Jiangsu University of Science and Technology
No. 2, Mengxi Road, Zhenjiang 212003, P. R. China
jiangtaozhai@gmail.com; dywjust@163.com

Received March 2016; accepted June 2016

Abstract. *Covert timing channels exploit timing information of packets for data exfiltration. In recent years, multicast communication has been applied in many applications, such as IPTV, video conference and other multimedia services. Deploying covert timing channels on multicast traffic can disseminate secret messages to a group of receivers simultaneously. Traditional fountain codes provide equal error protection to all the secret message symbols. In this paper, we introduce expanding window fountain codes to provide unequal error protection for original information symbols in some scenarios. Encoding symbols are embedded into the inter-packet delays of traffic at the compromised server system. Simulation results are presented to illustrate the performance of the proposed algorithm.*

Keywords: Covert timing channel, Multicast, Unequal error protection, Expanding window fountain codes

1. **Introduction.** With the rapid development of Internet, a great deal of data and various protocols in the Internet make network traffic an ideal carrier for covert communications. Network covert channels embed secret messages into normal network traffic and provide a novel way for the data exfiltration. Fisk et al. [1] calculated that a large site which sends out 500 million packets each day could lose 26 GB of data annually when a malicious software inside only embeds one bit into a packet. Compared with traditional information hiding methods that embed data into digital media files, network covert channels have two evident advantages [2]. First, secret messages can be transferred to receivers stealthily during long periods of time. Second, it is more difficult to analyze the covert communication process for the forensics experts unless all the exchanged traffic is captured.

Up to present, there are two main types of network covert channels: storage channels and timing channels [3]. Covert storage channels write secret messages into some unused or optional fields of packet headers, such as IP checksum, IP TTL [4], and TCP initial sequence number [5]. This kind of covert channel is eliminated easily by traffic normalization that standardizes the relative fields of packet headers [6]. Covert timing channels are a class of advanced covert channels that embed secret messages into the transmission time of packets [7], which is more difficult to detect and handle. However, exiting schemes of CTCs can only achieve the transmission of secret messages to a single destination [8].

Recently, multicast communications that distribute content to multiple subscribers with minimal server and network loads are widely used for real-time applications, such as

IPTV, video conference and other multimedia services. Exploiting multicast traffic as the carriers of covert timing channels can implement the transmission of secret messages to a group of authorized receivers. However, packet losses caused by network congestion and physical layer impairments will lead to the erasure of some secret message symbols [9]. This paper focuses on the problem of how to enable the data of secret message with a higher importance to be recovered prior to other parts.

In this paper, we propose a multicast covert timing channel (CTC) with unequal error protection based on expanding window fountain (EWF) codes that are a class of rateless codes [10]. EWF coding is applied over secret message data in the encoding process performed by the sender of multicast CTC. Authorized receivers extract secret message from the inter-packet-delays (IPDs) of multicast traffic by using the iterative belief-propagation (BP) decoding algorithm. The usage of EWF codes allows the separation of secret message data into multiple importance classes [11].

The rest of this paper is organized as follows. In Section 2, the covert communication scenario is depicted and a multicast CTC scheme with unequal error protection is presented. Section 3 investigates the bit error performance of the proposed scheme. Finally, the paper is concluded and future directions are pointed out in Section 4.

2. **Problem Statement and Proposed Scheme.** We consider a scenario where a normal stream is transmitted from a server to a number of heterogenous receivers over a lossy packet networks according to the modulated IPDs, as illustrated in Figure 1. The carrier channels from the server to each receiver have potentially different erasure probabilities. At the server side, confidential information is periodically broken into several source blocks, and each source block is separately encoded by an EWF encoder.

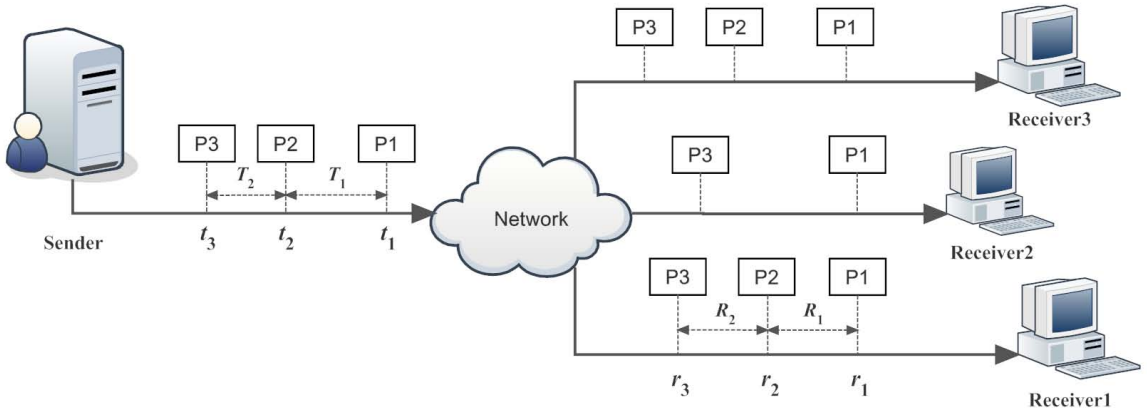

FIGURE 1. Diagram of a multicast covert timing channel

2.1. **Encoding and embedding of secret message.** Suppose that the secret message is partitioned into r parts $S_1, S_2, \ldots, S_r$ of size $m_1, m_2, \ldots, m_r$ such that $\sum_{i=1}^{r} m_i = K$. The importance of symbols in each part decreases with the part index. If $i < j$, then the ith part is more important than the jth part. A generating polynomial is defined to describe the partition process, $\Pi(x) = \sum_{i=1}^{r} \Pi_i X^i$, where $\Pi_i = m_i/K$ is the percentage of symbols in S_i.

The encoding window is defined as the set of information symbols that the input symbols of LT code are chosen from. The ith encoding window denoted as W_i consists of the first $n_i = \sum_{j=1}^{i} m_j$ information symbols, as illustrated in Figure 2. Circles represent information symbols while squares represent the encoding symbols. The percentage of symbols in W_i is denoted as $\Theta_i = n_i/K$. Each encoding symbol is assigned to a randomly chosen encoding window. The window selection distribution is $\Gamma(x) = \sum_{i=1}^{r} \Gamma_i X^i$, where

Γ_i is the probability that the ith window is chosen. The probability of the information symbol selection from different windows can be adjusted by varying Γ_i. For the extreme case of Γ_i $(i = 1, 2, \ldots, r-1)$, equal error protection is provided for all of the information symbols, whereas the protection to the most important part is added by increasing Γ_1. Therefore, Γ_i should be determined according to the practical requirements by the sender of multicast CTC.

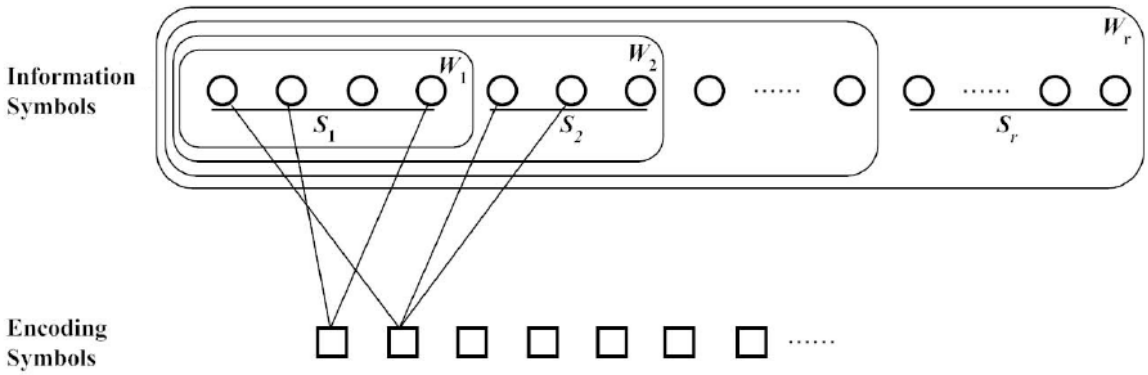

FIGURE 2. Expanding window fountain codes

LT code is performed on the chosen encoding window W_i with degree distribution $\Omega^{(i)}(x) = \sum_{j=1}^{k_i} \Omega_j^{(i)} X^j$. An EWF code that assigns each output symbol to the ith window with probability Γ_i and encodes the chosen window using LT code with distribution $\Omega^{(j)}$ can be denoted as $F_{EW}\left(\Pi,\ \Gamma,\ \Omega^{(1)},\ \ldots,\ \Omega^{(r)}\right)$. $\Omega_j^{(i)}$ denotes the probability that the value j is chosen as degree when the encoding symbol is assigned to W_i.

In order to ensure that the expected size of ripple is large enough at each point in the decoding process, $\Omega_j^{(i)}$ is designed to follow the robust soliton distribution [12], which is defined as

$$\Omega_j^{(i)} = \frac{\rho_j^{(i)} + \tau_j^{(i)}}{\beta^{(i)}}, \quad \text{for } j = 1, 2, \ldots, n_i \tag{1}$$

where $\rho_j^{(i)}$ is an ideal soliton distribution and $\tau_j^{(i)}$ is the supplement to make LT code practically decodable. $\rho_j^{(i)}$ and $\tau_j^{(i)}$ are defined as

$$\rho_j^{(i)} = \begin{cases} 1/n_i & \text{for } j = 1 \\ \frac{1}{j(j-1)} & \text{for } j = 2, 3, \ldots, n_i \end{cases} \tag{2}$$

$$\tau_j^{(i)} = \begin{cases} \frac{R}{jn_i} & \text{for } j = 1, \ldots, \frac{n_i}{R} - 1 \\ \frac{R}{jn_i} \ln\left(\frac{R}{\sigma}\right) & \text{for } j = \frac{n_i}{R} \\ 0 & \text{for } j > \frac{n_i}{R} \end{cases} \tag{3}$$

where $R = \lambda \cdot \ln\left(k_i/\sigma\right) \sqrt{k_i}$ for some suitable constants $\lambda > 0$, and σ denotes the allowable failure probability of the decoder to recover the data for a given number k_i of encoding symbols.

The normalized factor $\beta^{(i)}$ is defined as

$$\beta^{(i)} = \sum\nolimits_{j=1}^{k_i} \rho_j^{(i)} + \tau_j^{(i)} \tag{4}$$

The degree of an encoding symbol is defined as the number of information symbols connected to it. Each encoding symbol can be independently generated from information symbols by the following encoding process. First, a window index j is determined randomly according to the window selection distribution $\Gamma(X)$. Second, the degree of current encoding symbols d is generated according to $\Omega_j^{(i)}$. Third, d distinct information

symbols are selected from W_i uniform randomly. Last, perform bitwise XOR operations on the selected information symbols to get the encoding symbols. The encoding process is iterated until all the encoding symbols are generated.

Assume that each encoding symbol denoted by c_t represents α bits and the symbol set size is 2^α, the encoding symbols are transformed into IPDs as

$$T_t = F^{-1}\left(\left(\frac{c_t}{2^\alpha} + v_t\right) \bmod 1\right) \tag{5}$$

where $F^{-1}(\cdot)$ is the inverse function of cumulative distribution function. Random numbers v_t that make the possible values of generated IPDs cover the whole range of legitimate IPDs are generated by a cryptographically secure pseudo random number generators (CSPRNG). Packets of carrier stream are sent out according to the generated IPDs.

2.2. **Decoding and extracting of secret message.** When packets are transmitted over network, small jitters denoted by δ_t that are the variations of end-to-end delays between two consecutive packets will be added to the modulated IPDs. The arriving IPDs denoted by R_t can be expressed as

$$R_t = T_t + \delta_t \tag{6}$$

Receivers in a multicast group may be dispersed over the Internet and each of them may encounter specific network conditions. Each receiver recovers the encoding symbols from the arriving IPDs as

$$\hat{c}_t = \lfloor 2^\alpha \cdot [(F(R_t) - v_t) \bmod 1] + 0.5 \rfloor \tag{7}$$

The decoder finds out the neighbors of each encoding symbol by generating random linear combinations synchronized with the transmitter. Information symbols are recovered by the following three-step process. Firstly, all the encoding symbols of degree one are released to cover their unique neighbor information symbols. Secondly, the covered but not processed information symbols are sent to ripple that is a set of covered unprocessed information symbols gathered through the previous step. And then, each information symbol in the ripple is chosen to be processed. The edges connecting the information symbol to its neighbor encoding symbols are removed and the values of the encoding symbols change according to the information symbol. The processed information symbols are removed from the ripple. The three-step process iterated until all information symbols are covered.

3. **Experimental Results.** Simulation experiments are performed to evaluate the performance of the scheme proposed in this paper. First, the performance of CTC with UEP is compared with the traditional scheme where EEP is exploited. Then, some experiments are conducted to report the relationship between the performance and serval parameters. Without loss of generality, two receivers will be considered in our experiment. The secret message data is divided into two importance classes, the class of more important bits (MIB) and less important bits (LIB). We employed an EWF code $F_{EW}\left(\Pi_1 X + (1-\Pi_1)X^2,\ \Gamma_1 X + (1-\Gamma_1)X^2,\ \Omega^{(1)},\ \Omega^{(2)}\right)$. The robust soliton distribution with $\lambda = 0.2$ and $\sigma = 0.3$ is applied on both windows. 226, 432 IPDs that are extracted from the traffic of YY voice application are used as legitimate samples. Covert IPDs that carry secret message are generated based on the CDF of legitimate samples.

The bit error rates (BER) of MIB and LIB for CTC with UEP are compared with the BER of CTC with EEP over different reception overheads in Figure 3 for the case of $\Pi_1 = 0.2$ and $\Gamma_1 = 0.15$. The MIB block contains 200 bits input symbols and the LIB block contains 800 bits input symbols. The BER of MIB is reduced significantly while the BER of LIB is degraded slightly when the reception overhead is identical for these two schemes. Since the number of information symbols is small, high reception overhead is necessary to the reliable recovery of all the information symbols.

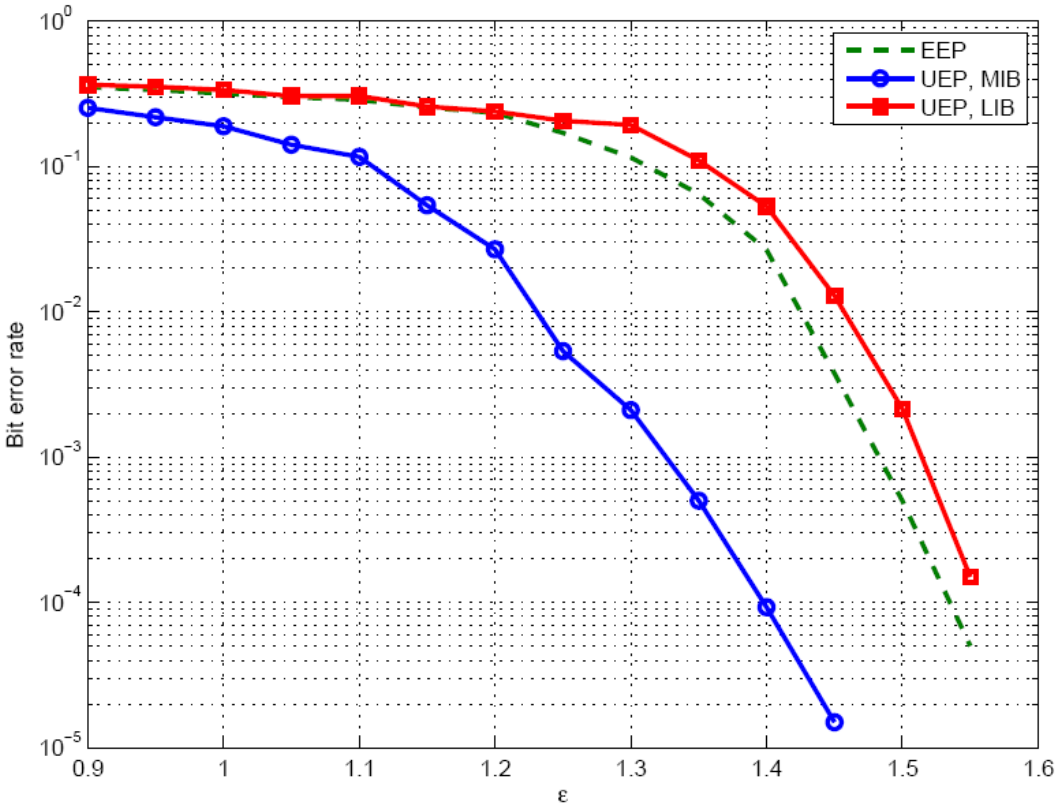

FIGURE 3. Comparison of BER for CTCs with UEP and EEP

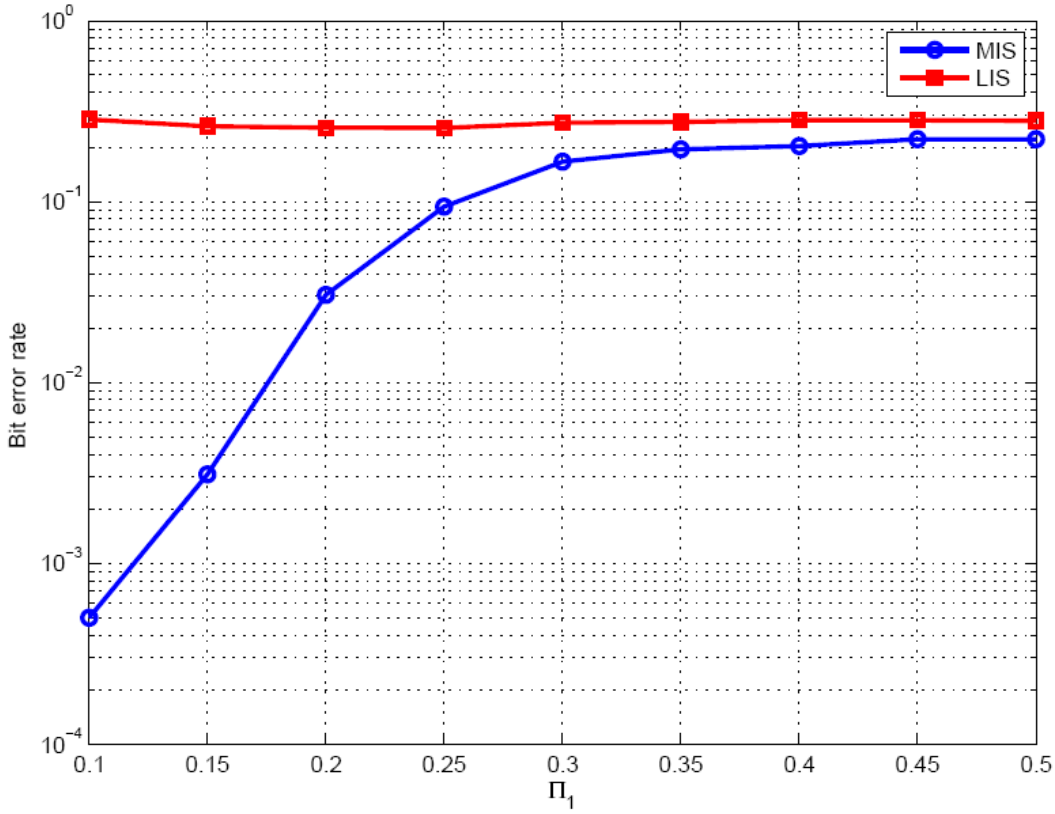

FIGURE 4. BER versus the percentage of bits in MIB class Π_1

The bit error performance against the percentage of bits in the class of MIB Π_1 is presented in Figure 4. The selection probability of the first window Γ_1 is set to 0.15 and the reception overhead is equal to 0.2. It can be noted that the BER of MIB increased with Π_1, while there is slight deterioration on the BER of LIB. This is because MIB are given higher priority to be decoded correctly under the limited reception overhead. However, the protection to MIB is weakened as the number of MIB is increased.

Figure 5 shows the dependence of BER on the first window selection probability Γ_1 for the reception overhead $\varepsilon = 0.1$. The percentage of symbols in the first class Π_1 is equal to 0.2. The MIB class contains 200 bits of secret message symbols, while the total number of symbols is 1000. As it can be observed, the choice of Γ_1 significantly influences the BER both for MIB and LIB. For the case of $\Gamma_1 = 0$, all the encoding symbols are generated from the second window and the protections for MIB and LIB are the same. As the increasing of Γ_1, protection of input symbols in the MIB class is added progressively. The BER of MIB is reduced significantly while there is slight deterioration on the BER of LIB.

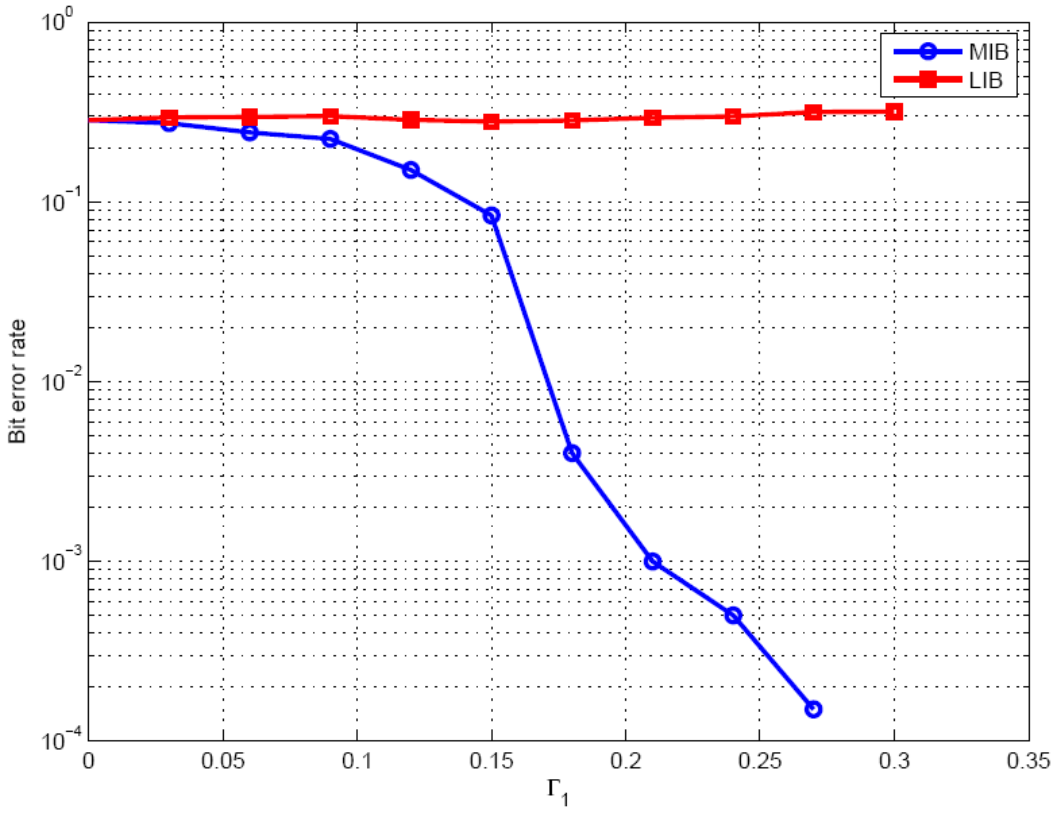

FIGURE 5. BER versus the first window selection probability Γ_1

4. **Conclusions.** In this paper, a multicast covert timing channel with unequal error protection based on a class of rateless codes named EWF codes is proposed. When the secret message is disseminated over multicast CTCs, symbols with different importance are provided with unequal error protection. Then, the improved error protection will facilitate reception of more important symbols over a carrier channel with limited capacity. The proposed scheme is also suitable to unicast scenario. Experimental results show that the bit error performance of more important bits is improved significantly with only a subtle loss on the performance of less important bits. Potential improvements of the proposed scheme by applying Raptor-like precoding is a promising direction for further investigation.

Acknowledgment. This work is partially supported by Natural Science Foundation of China (Grant Nos. 61170250, 61103201 and 61472188), the Fundamental Research Funds for the Central Universities (Nos. 30920140121006, 30915012208) and NSFC of Jiangsu Province (No. BK20150472). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] G. Fisk, M. Fisk, C. Papadopoulos and J. Neil, Eliminating steganography in Internet traffic with active wardens, *Proc. of the 5th International Workshop on Information Hiding*, Noordwijkerhout, The Netherlands, pp.18-35, 2002.

[2] E. Zieliska, W. Mazurczyk and K. Szczypiorski, Trends in steganography, *Communications of the ACM*, vol.57, pp.86-95, 2014.

[3] S. Wendzel, S. Zander, B. Fechner and C. Herdin, Pattern-based survey and categorization of network covert channel techniques, *ACM Computing Surveys*, vol.47, p.50, 2015.

[4] S. Zander, G. Armitage and P. Branch, Covert channels in the IP time to live field, *Proc. of Australian Telecommunication Networks and Applications Conference*, 2006.

[5] H. Zhao and Y. Shi, Detecting covert channels in computer networks based on chaos theory, *IEEE Trans. Information Forensics and Security*, vol.8, pp.273-282, 2013.

[6] Y. Qian, H. Song, F. Wang and Z. Wang, Network covert channel encoding by packet length: Design and detection, *Journal of Computational Information Systems*, vol.7, pp.1463-1471, 2011.

[7] N. Kiyavash, F. Koushanfar, T. Coleman and M. Rodrigues, A timing channel spyware for the CSMA/CA protocol, *IEEE Trans. Information Forensics and Security*, vol.8, pp.477-487, 2013.

[8] K. Kothari and M. Wright, Mimic: An active covert channel that evades regularity-based detection, *Computer Networks*, vol.57, pp.647-657, 2013.

[9] Y. Liu, D. Ghosal, F. Armknecht, A.-R. Sadeghi, S. Schulz and S. Katzenbeisser, Robust and undetectable steganographic timing channels for i.i.d traffic, *The 12th International Conference on Information Hiding Calgary*, AB, Canada, 2010.

[10] N. Rahnavard, B. N. Vellambi and F. Fekri, Rateless codes with unequal error protection property, *IEEE Trans. Information Theory*, vol.53, pp.1521-1532, 2007.

[11] D. Sejdinovic, D. Vukobratovic, A. Doufexi, V. Senk and R. J. Piechocki, Expanding window fountain codes for unequal error protection, *IEEE Trans. Communications*, vol.57, pp.2510-2516, 2009.

[12] M. Luby, LT codes, *IEEE the 54th Annual Symposium on Foundations of Computer Science*, pp.271-271, 2002.