Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 1107–1111

DOI: 10.15439/2015F88
ACSIS, Vol. 5

A Random Traffic Padding to Limit Packet Size Covert Channels

Anna Epishkina, Konstantin Kogos
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
Cybernetics anf Information Security Department,
31 Kashirskoe shosse, 115409, Moscow, Russia
Email: {avepishkina, kgkogos}@mephi.ru

***Abstract*—This paper observes different methods for network covert channels constructing and describes the scheme of the packet length covert channel. The countermeasure based on random traffic padding generating is proposed. The capacity of the investigated covert channel is estimated and the relation between parameter of covert channel and counteraction tool is examined. Practical recommendation for using the obtained results are given.**

I. Introduction

THE IDEA of covert channel was introduced by Lampson in 1973. The covert channel is a communication channel that was not intended for information transfer at all, such as the service program's effect on the system load [1]. It is obvious that covert channel may lead to information leakage and it cannot be eliminated by techniques to detect network anomalies [2], malware activities [3], etc. TCSEC postulates that the covert channel is a communication channel which allows the transfer of data and violation of security policy [4].

Presently, the most popular covert channels are built on packet switching data networks because of some features available in the TCP/IP protocol suite [5]. Moreover, traditional security measures based on traffic encryption also permit the design of different types of covert channels.

Covert channels are divided by the data transfer technique into two classes such as, timing and storage channels [4]. Storage channel allows the direct or indirect storage recording by one process and the direct or indirect reading of it by another. Timing channel allows one process to signal information to another process by modulating of system resources (e. g. CPU time) usage so that the change in response time observed by the second process would provide information.

The first technique to design a storage channel in the IP network is to modulate packet header fields, e. g. TTL [6], IP ID [7], ToS [8]. The second technique is based on the modification of the packet length. Different timing channels in the IP networks use alteration of the inter-packet delays [9], [10], e. g. by JitterBug [11] and packet transfer rate [12]. In addition, the packet reordering could be used to build a timing channel [13]. Timing channel is a channel with noise since a packet timing is a random variable whose distribution depends on the network load [14].

A capacity of undetectable packet size covert channels can be higher than a capacity of timing channels, therefore these channels can lead to a serious security breach. The authors of the paper research this type of covert channels and propose the technique to estimate and limit their capacity which can be useful in different types of information systems, e.g. in data storage system in a cloud [15].

Our Contribution. Since a technique to choose the quantitative characteristics of countermeasures in order to keep balance between capacity of covert and communication channels has not yet been proposed, we offer an approach to gain it. This paper describes a technique to estimate and limit the capacity of a packet size covert channel based on random traffic padding generation. The investigation carried out is significant because such type of covert channels could be constructed even if data encryption is used. There are complicated undetectable covert channels which have no noise in contrast to timing channels.

This paper is organized as follows. It gives an analysis of different types of packet size covert channels. The investigated covert channel scheme and the counteracting technique are shown. Then the capacity of the covert channel is estimated and the technique to generate dummy packets is given. The main results and further research guidelines are summed up in the conclusion.

II. Related Work

For the first time Padlipsky [16] and Girling [17] suggested to modulate the length of data link layer frames in order to accomplish the hidden data transfer. The main idea of the technique is as follows: sender and receiver share the rule used to compose a byte of the covert message depending on the frame length. To describe any byte of the transmitted message, one should use 256 different frame lengths.

Yao constructed a covert channel in which a sender and a receiver shared the periodically updated matrix with elements representing unique unsorted packet lengths in 2008 [18]. The sender using the bits of hidden transmitted message determines the matrix row and randomly chooses a packet length from the row. The receiver finds the gained packet length in the matrix and reconstructs bits of the message according to the row number. Because packet length distribution given by covert channel is not equal to packet length distribution of normal traffic, this type of covert channel is detectable.

978-83-60810-66-8/$25.00

Ji suggested a protocol-independent covert channel in 2009 [19]. Before the transmission starts, sender and receiver form the dynamically updated reference of packet lengths by fixing packets lengths in normal traffic. In order to transfer a hidden message the sender transmits a special packet. The length of the special packet is chosen from the reference using the algorithm known to the sender and receiver. The length of the next packet is a sum of lengths of the previous packet and the number corresponding to the message bits. The reference is updated by adding the length of the transmitted packet. The receiver recovers the message bits by evaluating the difference of the packets length gained. The disadvantage of the covert channel is as follows: the lengths of hidden messages are added to the reference, therefore the packet length distribution with the covert channel is not equal to packet length distribution of the normal traffic and this type of covert channels is detectable in case of the large data volume.

Ji worked out another protocol-independent covert channel in 2009 [20]. Before the transmission starts, sender and receiver form a non-updating reference of packet lengths by fixing packets lengths in the normal traffic. The main advantage of the technique is a small space and time complexity of the decoding, since the sender stores the whole reference and receiver saves only the lower and upper bound of each basket. To transmit the hidden data the sender randomly chooses the packet length from the basket, the receiver determines the number of the basket and restores the message bits. The regularity in the distribution of the transmitted message bits could cause a highly probable detection of the channel.

Hussain improved the technique and designed high capacity covert channel based on the alteration of packets lengths and information content in 2011 [20]. Sender and receiver share periodically updated matrix with elements representing unsorted packet lengths in normal traffic. The sender using bits of hidden message determines the matrix row and randomly chooses the packet length from the row. If the chosen length belongs to the stego-column, then the data is transferred in the information content of the packet, otherwise the data is transferred in the number of matrix row. The receiver finds the length of gained message in the matrix, detects the transfer method using the matrix row and recovers bit of the message. The disadvantage of the channel is that information content of the packet has to be used as the hidden container and is more complicated in comparison with the other techniques.

Edekar improved the method in 2013 [22] and realized it using TCP. Packets lengths in the shared matrix are unique. Each matrix element a is associated with the binary vector (v, y), where $v = 1 \Leftrightarrow a$ belongs to the stego-column and $y = 1 \Leftrightarrow a$ belongs to the stego-row. Then if $(v, y) = (1, 1)$ the packet is ignored; if $(v, y) = (1, 0)$ data is transferred in the packet information content; if $(v, y) = (0, 0)$ data is transmitted in the number of the matrix row; if $(v, y) = (0, 1)$ data is transferred in the number of the matrix row and the packet information content.

The way to eliminate covert channels based on length of transferred packets modulation is to equalize packets lengths and send packets with maximum length. However, the technique essentially diminishes the capacity of a communication channel. To limit a covert channel capacity, the random increase of packet lengths and generation of dummy packets can be used. Kiraly suggested the realization of the methods based on IPsec in 2008 in order to make traffic nontraceable [23].

However, a technique to choose the quantitative characteristic of the methods in order to keep balance between capacity of covert and communication channels has not yet been proposed. The authors of this paper offer an approach to gain it.

III. The Covert Channel Scheme

Let the lengths of transferred packets possess the values from l_{fix} to $l_{fix} + L$. The disjoint sets L_0 and L_1 are given and

$$\begin{cases} L_0 \cup L_1 = N_{L+l_{fix}} \backslash N_{l_{fix}-1}, \\ \mid L_0 \mid = \mid L_1 \mid \end{cases} \tag{1}$$

where N_a stands for the set of positive integers from 1 to a.

Further, we consider a method to build a binary covert channel. In order to transfer «0» the sender communicates a packet with length $l \in L_0$, to transfer «1» the sender communicates a packet with length $l \in L_1$. It is obvious that the capacity of such a channel without counteraction is equal to 1 bit per packet. A large-scale site loses about 26 Gb of data annually if there is a covert channel with such a capacity [24].

If the symbol distribution in a transmitted message simulates a uniformly distributed random sequence (e.g. cryptographic keys sending), a random equiprobable choice of packets lengths from L_0 and L_1 leads to equally probable random distributed lengths of transmitted packets. Moreover, L_0 and L_1 could be periodically changed multisets so that a random choice of packets lengths from L_0 and L_1 induces the distribution of packets lengths to be close to the empirically obtained distribution of normal traffic.

To build such a covert channel, the sender must have one of the following possibilities:

- to modify lengths of transmitted messages;
- to form packets with undefined lengths;
- to buffer packets to be sent and transfer them to a channel at a specified moment.

The investigation proposes a technique to limit the capacity of covert channel based on random traffic padding. After i data packets have been sent, random length dummy packets are created, the number of packets i between dummy packets is the value of random variable that is uniformly distributed at the N_k, $k \in N$ where k is the parameter of a counteraction tool. Let μ be the capacity of a communication channel, then a counteraction tool decreases the capacity of a communication channel and it equals

$$\frac{k+1}{k+3}\mu. \tag{2}$$

The countermeasure using traffic padding generation after equal number of packets passed is not resistant against the attack of traffic padding tracing. If the violator detects traffic padding ones, data transmitting via covert channel has no

errors and can be processed without synchronization. The investigated countermeasure is resistant to this type of attack.

After a dummy packet is received, the mismatch between the hidden sender and hidden receiver takes place. To negotiate this fact SOF packets [25] are utilized after transferring $T-1$ packets within a covert channel. A receiver fixes $T-1$ packets gained after SOF packet and waits for the next SOF packet. Thus, T is the parameter of a covert channel which estimates the synchronization frequency.

IV. The Capacity of the Covert Channel

In 1987 Millen was the first to suggest the use of information theory to estimate a capacity of covert channels with noise [26]. The investigation was continued by Ventakraman [27]. The authors determine network covert channels and analyze techniques to audit and limit a capacity of covert channels utilizing indirect routing.

The capacity C of the investigated covert channel is

$$C = \max_X I(X,Y) \tag{3}$$

where $I(X,Y)$ is the mutual information of random variables describing the input and output properties of the covert channel properly, the dimensionality of covert channel capacity is one bit per packet.

Let us consider the case when synchronization is done more rarely than a dummy packet sending, i. e. $T > k$. After a dummy packet is received, mismatch between sender and receiver occurs, therefore identification of the following received bits would be wrong until the next synchronization happens. Consequently, in order to build a covert channel the inequality $T < k+1$ is required.

Let the synchronization be not less frequent than dummy packet sending, i. e. $T < k+1$. Corresponding choice of parameters is explained in Fig. 1.

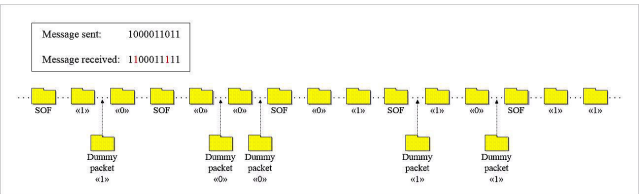

Fig. 1. The scheme of data transfer in the covert channel ($T = 3$, $k = 5$)

Since each T-th packet sent via a covert channel is not a data packet but a synchronization packet, the mutual information can be calculated using the following formula

$$I(X,Y) = \frac{T-1}{T} I^*(X,Y) \tag{4}$$

where $I^*(X,Y)$ is a mutual information of random variables describing the input and output properties of a covert channel without synchronization accordingly.

The mutual information $I^*(X,Y)$ is equal to the form of

$$I^*(X,Y) = H(Y) - H(Y|X) \tag{5}$$

where the entropy of random variable Y is

$$H(Y) = -\sum_{y\in\{0,1\}} p(y)\log_2 p(y), \tag{6}$$

the conditional entropy of random variable Y comparatively to random variable X is expressed as

$$H(Y|X) = \\ = -\sum_{x\in\{0,1\}} \Big(p(x)\Big(\sum_{y\in\{0,1\}} (p(y|x)\log_2 p(y|x))\Big)\Big). \tag{7}$$

Since sizes of sets L_0 and L_1 are equal and lengths of passing through the covert channel dummy packets are chosen randomly and equiprobable, then

$$H(Y) = 1. \tag{8}$$

Whereas the values of conditional probabilities $p(x|y)$, $x, y \in \{0,1\}$ depend on the number of packets sent via a covert channel between the moment of synchronization and the moment of dummy packet receiving, the mutual information $I^*(X,Y)$ can be found using the following formula

$$I^*(X,Y) = \frac{\binom{k-T+2}{2} + \sum\limits_{i=0}^{T-2}\Big((k-i)(1-H_i(Y|X))\Big)}{\binom{k+1}{2}} \tag{9}$$

where $H_i(Y|X)$ is the conditional entropy of random variable Y compared to random variable X and it is evaluated when i packets received between a moment of synchronization and the dummy packet's arrival.

The mutual information $I(X,Y)$ could be estimated as

$$I(X,Y) = \frac{(T-1)\Big(\binom{k-T+2}{2} + kS_1(T) - S_2(T)\Big)}{T\binom{k+1}{2}} \tag{10}$$

where

$$S_1(T) = \sum_{i=0}^{T-2}(1-H_i(Y|X)), \tag{11}$$

$$S_2(T) = \sum_{i=0}^{T-2} i(1-H_i(Y|X)). \tag{12}$$

Since

$$H_i(Y|X) = -\left(\frac{T-1-i}{2(T-1)}\log_2\frac{T-1-i}{2(T-1)} + \right. \\ \left. + \frac{T-1+i}{2(T-1)}\log_2\frac{T-1+i}{2(T-1)}\right) \tag{13}$$

then

$$S_1(T) = -(T-1)\log_2(T-1) + \\ + \frac{1}{2(T-1)}\Big(\sum_{i=0}^{T-2} f^+(i) + \sum_{i=0}^{T-2} f^-(i)\Big), \tag{14}$$

$$S_2(T) = \frac{1}{2(T-1)}\Big(\sum_{i=0}^{T-2} f^{2,+}(i) - \sum_{i=0}^{T-2} f^{2,-}(i) + \\ +(T-1)\sum_{i=0}^{T-2} f^{+}(i) - (T-1)\sum_{i=0}^{T-2} f^{-}(i)\Big), \tag{15}$$

where

$$f^{+}(i) = (T+i-1)\log_2(T+i-1), \tag{16}$$

$$f^{-}(i) = (T-i-1)\log_2(T-i-1), \tag{17}$$

$$f^{2,+}(i) = (T+i-1)^2\log_2(T+i-1), \tag{18}$$

$$f^{2,-}(i) = (T-i-1)^2\log_2(T-i-1). \tag{19}$$

In order to analyze functions $f^{+}(i)$, $f^{-}(i)$, $f^{2,+}(i)$, $f^{2,-}(i)$ we will examine analogue variable $\tilde{i}$, $\tilde{i} \in [0, T-2]$ instead of discrete variable i, in which case $f^{+}(\tilde{i})$, $f^{2,+}(\tilde{i})$ are strictly increasing and $f^{-}(\tilde{i})$, $f^{2,-}(\tilde{i})$ are strictly decreasing defined and continuous functions in the interval $[0, T-2]$. Then the values of the following forms

$$\sum_{i=0}^{T-2} f^{+}(i), \sum_{i=0}^{T-2} f^{-}(i), \sum_{i=0}^{T-2} f^{2,+}(i), \sum_{i=0}^{T-2} f^{2,-}(i) \tag{20}$$

could be approximated by means of functions $f^{+}(\tilde{i})$, $f^{-}(\tilde{i})$, $f^{2,+}(\tilde{i})$, $f^{2,-}(\tilde{i})$ integrating in the interval $[0, T-2]$ accordingly.

Now we explain how to gain the approximate value of the sum $\sum_{i=0}^{T-2} f^{2,+}(i)$ and the other sum can be estimated in a similar,

$$\sum_{i=0}^{T-2} f^{2,+}(i) \approx \int_0^{T-2} f^{2,+}(\tilde{i})d\tilde{i} + f^{2,+}(T-2) - \\ -\sum_{j=0}^{T-3}\frac{f^{2,+}(j+1) - f^{2,+}(j)}{2} = \int_0^{T-2} f^{2,+}(\tilde{i})d\tilde{i} + \\ +\frac{f^{2,+}(0) - f^{2,+}(T-2)}{2}. \tag{21}$$

Values of the integrals could be found using the variable substitution and integration by parts

$$\int_0^{T-2} (T+\tilde{i}-1)^2\log_2(T+\tilde{i}-1)d\tilde{i} = \\ =|\ T+\tilde{i}-1 = p\ |= \\ = \int_{T-1}^{2T-3} p^2\log_2 p dp = \frac{1}{3}\int_{T-1}^{2T-3}\log_2 p d(p^3) = \\ = \frac{1}{3}(p^3\log_2 p)\Big|_{T-1}^{2T-3} - \frac{1}{3}\int_{T-1}^{2T-3} p^3 d(\log_2 p) = \\ = \Big(\frac{1}{3}p^3\log_2 p - \frac{p^3}{9\ln 2}\Big)\Big|_{T-1}^{2T-3}. \tag{22}$$

It follows that

$$I(X,Y) \approx \frac{(T-1)\Big(\binom{k-T+2}{2} + kA(T) + B(T)\Big)}{T\binom{k+1}{2}} \tag{23}$$

where

$$A(T) = \frac{2T-3}{2}\log_2\frac{2T-3}{T-1} - \frac{T-2}{2\ln 2}, \tag{24}$$

$$B(T) = -\binom{T-1}{2}\log_2(T-1) - \\ -\frac{(T-1)^2\log_2(T-1)}{6} + \frac{(T-2)^2}{12\ln 2} - \\ -\frac{(2T-3)(2T^2-6T+3)\log_2(2T-3)}{12(T-1)}. \tag{25}$$

Graphs of function $I(X,Y)$ from k where $T \in \{2,3,4\}$ are illustrated in Fig. 2.

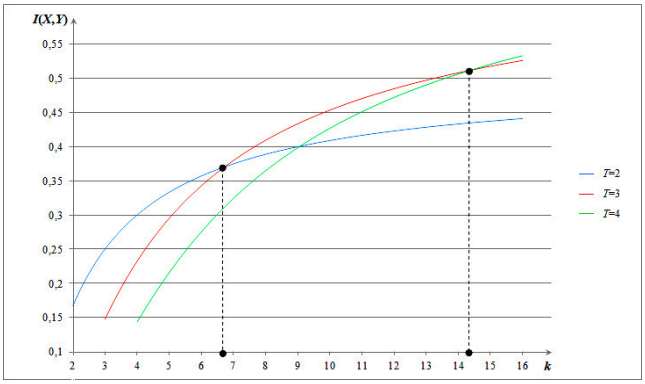

Fig. 2. $I(X,Y)$ function as a function from k graph, $T \in \{2,3,4\}$

To build a covert channel the parameter T is chosen while $I(X,Y)$ has a maximum value. Fig. 2 shows that when $k \in \{2,...,6\}$, parameter T should be equal to 2, when $k \in \{7,...,14\}$, parameter T should be equal to 3.

V. The Practical Using of the Obtained Results

Let functioning of a covert channel with capacity less than $v_{\max}$ has no influence upon security (the dimensionality of $v_{\max}$ is one bit per sec) and the capacity of communication channel is μ bits per sec. Hence if the average length of transmitted packets is $\bar{l}$ bits, then the residual communication channel capacity is

$$\frac{(k+1)\mu}{(k+3)\bar{l}} \tag{26}$$

packets per sec. In case of the full using of the communication channel by the sender and the receiver the capacity of the covert channel is

$$v = \frac{(k+1)\mu C}{(k+3)\bar{l}} \tag{27}$$

bits per sec, where C is the capacity of covert channel with the dimensionality bits per packet. Therefore when the allowable capacity of covert channel in limited, the following inequality is true

$$v \le v_{\max}. \tag{28}$$

For example, according to [4] the functioning of a covert channel with capacity less than $v_{\max} = 100$ bits per sec can be acceptable in some cases. Let the capacity of the communication channel be $\mu = 100$ Mbits per sec (standard 100Base-T). The maximum length of IP packet is 65535 bytes, from which 20 bytes is a header length ($l_{fix} = 20$ bytes and $L = 65515$ bytes). Then the average length of sending packets is $\bar{l} = 262220$ bits in case of random equipropable choice of packets lengths from equinumerous sets L_0 and L_1.

Table I presents the relation between parameters of the covert channel and the counteraction tool (the symbol «*» means that the value of v is round up to 2 digits).

TABLE I
RELATION BETWEEN PARAMETER OF COVERT CHANNEL, PARAMETER OF COUNTERACTION TOOL AND CAPACITY OF COVERT CHANNEL

k	*T*	*C*	*v*
2	2	0,17*	41
3	2	0,25	67
4	2	0,30	86
5	2	0,33*	100
6	2	0,36*	112
7	3	0,38*	122

Table I shows that in order to limit the capacity of covert channel up to 100 bits per sec the parameter of counteraction tool should be $k = 5$.

VI. CONCLUSION

In this work the capacity of a packet size covert channel was examined using the information theory statements. The counteraction tool based on random traffic padding generating was designed. We proposed selecting the parameter of the counteraction tool when an allowable covert channel capacity is given.

The topic of the further work is to estimate the residual capacity in multi-symbol covert channels with traffic padding and to investigate the technique to limit covert channel capacity by random increase of packets sizes.

REFERENCES

[1] Lampson, B.W. 1973. A Note on the Confinement Problem. Communications of the ACM, 16(10):613–615, http://dx.doi.org/10.1145/362375.362389

[2] Szmit, M., Szmit, A., Kuzia, M. 2013. Usage of RBF Networks in prediction of network traffic. Annals of Computer Science and Information Systems. Position Papers of the 2013 Federated Conference on Computer Science and Information Systems, 1:63-66.

[3] Jasiul, B., Sliwa, J., Gleba, K., Szpyrka, M. 2014. Identification of malware activities with rules. Annals of Computer Science and Information Systems. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, 2:101-110, http://dx.doi.org/10.15439/978-83-60810-58-3

[4] Department of defense trusted computer system evaluation criteria. Department of defense standard, 1985.

[5] Zander, S., Armitage, G., Branch, P. 2007. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications surveys and tutorials, 9(3):44–57, http://dx.doi.org/10.1109/COMST.2007.4317620

[6] Zander, S., Armitage, G., Branch, P. 2006. Covert channels in the IP time to live field. Proceedings of the 2006 Australian telecommunication networks and applications conference, 298–302.

[7] Ahsan, K., Kundur, D. 2002. Practical data hiding in TCP/IP. Proceedings of the 2002 ACM Multimedia and security workshop.

[8] Handel, T., Sandford, M. 1996. Hiding data in the OSI network model. Proceedings of the first International workshop on information hiding, 23–38, http://dx.doi.org/10.1007/3-540-61996-8_29

[9] Berk, V., Giani, A., Cybenko, G. 2005. Detection of covert channel encoding in network packet delays: Technical report TR2005-536. New Hampshire: Thayer school of engineering of Dartmouth College.

[10] Sellke, S.H., Wang, C.-C., Bagchi, S., Shroff, N.B. 2009. Covert TCP/IP timing channels: theory to implementation. Proceedings of the twenty-eighth Conference on computer communications, 2204–2212.

[11] Shah, G., Molina, A., Blaze, M. 2009. Keyboards and covert channels. Proceedings of the 15th USENIX Security symposium, 59–75.

[12] Yao, L., Zi, X., Pan, L., Li, J. 2009. A study of on/off timing channel based on packet delay distribution. Computers and security, 28(8):785–794, http://dx.doi.org/10.1016/j.cose.2009.05.006

[13] Kundur, D., Ahsan, K. 2003. Practical Internet steganography: data hiding in IP. Proceedings of the 2003 Texas workshop on security of information systems.

[14] Bovy, C.J., Mertodimedjo, H.T., Hooghiemstra, G., Uijterwaal, H., Mieghem, P. van. 2002. Analysis of end-to-end delay measurements in Internet, Proceedings of the 2002 ACM Conference Passive and Active Measurements.

[15] Shatilov, K., Boiko, V., Krendelev, S., Anisutina, D., Sumaneev, A. 2014. Solution for Secure Private Data Storage in a Cloud. Annals of Computer Science and Information Systems. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, 2:885-889, http://dx.doi.org/10.15439/978-83-60810-58-3

[16] Padlipsky, M.A., Snow, D.W., Karger, P.A. 1978. Limitations of end-to-end encryption in secure computer networks: Technical report ESD-TR-78-158. Massachusetts: The MITRE Corporation.

[17] Girling, C.G. 1987. Covert channels in LAN's. IEEE Transactions on software engineering, 13(2):292–296.

[18] Yao, Q., Zhang, P. 2008. Coverting channel based on packet length. Computer engineering, 34(3):183–185.

[19] Ji, L., Jiang, W., Dai, B., Niu, X. 2009. A novel covert channel based on length of messages. Proceedings of the 2009 Symposium on information engineering and electronic commerce, 551–554, http://dx.doi.org/10.1109/IEEC.2009.122

[20] Ji, L., Liang, H., Song, Y., Niu, X. 2009. A normal-traffic network covert channel. Proceedings of the 2009 International conference on computational intelligence and security, 499–503, http://dx.doi.org/10.1109/CIS.2009.156

[21] Hussain, Mehdi, Hussain, M. 2011. A high bandwidth covert channel in network protocol. Proceedings of the 2011 International conference on information and communication technologies, 1–6, http://dx.doi.org/10.1109/ICICT.2011.5983562

[22] Edekar, S., Goudar, R. 2013. Capacity boost with data security in network protocol covert channel. Computer engineering and intelligent systems, 4(5):55–59.

[23] Kiraly, C., Teofili, S., Bianchi, G., Cigno, R. Lo, Nardelli, M., Delzeri, E. 2008. Traffic flow confidentiality in IPsec: protocol and implementation. The International federation for information processing, 262:311–324, http://dx.doi.org/10.1007/978-0-387-79026-8_22

[24] Fisk, G., Fisk, M., Papadopoulos, C., Neil, J. 2002. Eliminating steganography in Internet traffic with active wardens. Proceedings of the fifth International workshop on information hiding, 18–35, http://dx.doi.org/10.1007/3-540-36415-3_2

[25] Cabuk, S., Brodley, C.E., Shields, C. 2004. IP covert timing channels: design and detection. Proceedings of the eleventh ACM conference on computer and communications security, 178–187, http://dx.doi.org/10.1145/1030083.1030108

[26] Millen, J.K. 1987. Covert channel capacity. Proceedings of the IEEE Symposium on Security and Privacy, 60–66, http://dx.doi.org/10.1109/SP.1987.10013

[27] Venkatraman, B.R., Newman-Wolfe, R.E. 1995. Capacity estimation and auditability of network covert channels. Proceedings of the IEEE Symposium on Security and Privacy, 186–198, http://dx.doi.org/10.1109/SECPRI.1995.398932