Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **4**, July **2015**

A Detection Method for Cloak Covert Channel Based on Distribution of TCP Burst Size

Hao Wang, Guang-Jie Liu and Yue-Wei Dai
School of Automation
Nanjing University of Science and Technology
No.200 Xiaolingwei Street, Xuanwu District, Nanjing, China
whaanog@gmail.com; gjieliu@gmail.com; daiywei@163.com

Jin Shi
Center of Software
North Information Control Group Co., Ltd
No.528 Jiangjun Road, jiangning District, Nanjing, China
shijin1011@163.com

Received November, 2014; revised April, 2015

Abstract. *Cloak is a new class of network covert timing channel relied on multilink with high reliability and enhanced data rate. The existing detection schemes are less effective to detect this kind of covert channel. In this paper, the detection method for Cloak covert channel based on burst size distribution is proposed. The statistical distribution of burst size is calculated and Chi-Squared test is utilized to judge whether the network traffic obeys the theoretical distribution generated by Cloak. Further, the influences of detection performance caused by the RTT variation and packet loss are also discussed. Experimental results show that the proposed method achieves high detection performance.*

Keywords: Cloak covert channel; Burst size; Chi-Squared goodness-of-fit test; Covert channel detection.

1. **Introduction.** Network covert channel is a stealthy communication technique that utilizes the redundancies of network protocols or packet-sequence characteristics to transfer secret message. It also can be named network steganography referred to the field of image steganography [1, 2]. Similar to the covert channel in multi-level security (MLS) systems, Network covert channel can also be divided into two types: storage and timing channels [3]. Network covert storage channel is constructed by modifying some unused or insensitive bits of protocol header in network packets. Network covert timing channel is constructed by modulating secret message bits via setting packet rates/inter-packet delays. Besides the time sequence, other covert channels based on characteristics of packet-sequence are usually considered as the timing case.

Padlipsky et al. [4] firstly described the principle of the so-called on/off timing channel. It is that the sender either transmits or stays silent in each time interval to represent 0 or 1. Girling [5] also proposed a covert timing channel which can transmit secret message by particular delays between successive transmissions imposed by a sender. On this basis, Shah et al. [6] implemented a timing channel named Jitterbug by encoding information within inter-keystroke timings. The delay-based timing channel does not require synchronized clock while an on/off timing channel needs synchronization mechanism to ensure accurate decoding. Thus, Cabuk et al. [7, 8] implemented the on/off timing channel which introduces SOF (Start of frame) and silent intervals to synchronize between sender and receiver. The modulation of inter-packet delays may change overt communication pattern and made itself more exposed. To solve this problem, Gianvecchio et al. [9] proposed a model-based covert timing channel called MBCTC. In the scheme, the channel mimics the observed behavior of legitimate network traffic to evade detection. Liu et al. [10] proposed a simple binary covert timing channel based on Gianvecchio's framework, this method is more practical in encoding/decoding and has lower bit error rate. Although these covert channels can resist detection based on statistical properties, the algorithms are usually complicated with low data rate and not easy to be deployed in a real network.

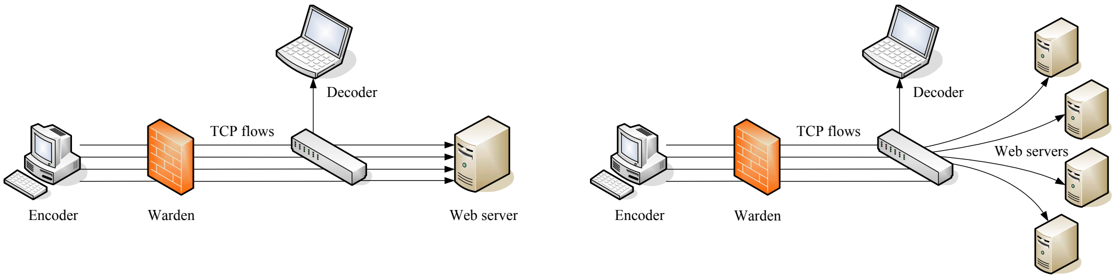
It is obvious making the detection against the covert timing channel is also an important problem, the researchers have made a lot of endeavor. Cabuk et al. [7] proposed a detection method for on/off covert timing channel. The authors defined two measures, Regularity (i.e. patterns in the variance) and -Similarity (i.e. similarity between adjacent inter-arrival times), to judge whether the traffic was a covert one. Gianvecchio et al. [11] proposed an entropy-based detection approach which makes use of entropy (EN test) and corrected conditional entropy (CCE test) to against abnormal shape or abnormal regularity separately. The approach is able to detect most existing covert timing channels successfully, the limitation is that legitimate traffic samples need to be utilized to determine bin ranges in the modeling stage. While, in practice, due to the large variation of network traffic, it is hard to choose proper traffic samples and the detection performance may discount.

The construction or detection of covert timing channel is aimed to be more practical. Luo et al. [12] designed the network covert timing channel named Cloak which transmits secret message by a unique distribution of N TCP packets over X TCP flows. Cloak offers ten different encoding methods which are based on whether packets/flows are distinguishable or not. While the Cloak utilizes TCP traffic as a cover and its reliability is ensured by TCP's reliable transmission mechanism, the decoding accuracy will not be affected by packet losses, delay jitters, and so on. Due to the cooperative transmission in multiple flows, data rate of Cloak is several times faster than the other channels mentioned above and the threat of information leaking grows as well. Therefore, it is especially important to exploit detection scheme against Cloak covert channel. In this paper, the detection method for Cloak covert channel based on burst size distribution is proposed. The statistical distribution of burst size is calculated and Chi-Square testing is utilized to judge whether the network traffic obeys the theoretical distribution generated by Cloak. Experimental results show that the proposed method achieves high detection performance.

The remainder of this paper is organized as follows. Section 2 introduces the principle of Cloak and corresponding analysis. Section 3 gives our detection scheme. Section 4 presents the experimental results. Section 5 concludes the whole paper.

2. **Review of Cloak Covert Channel.** Cloak covert channel [12] encodes message with a unique distribution of N TCP packets over X TCP flows which is the most important deviation from the existing timing channels. Based on the combination of distinguishable or indistinguishable packets/flows and restriction of packet number in a TCP flow (i.e. at most one packet, at least one packet, no restriction), ten types of Cloak covert channel can be constructed (for details, see Table 1 in Ref. [12]), denoting Cloak^c, $c \in [1, 10]$. For the decoder and encoder, the values of N and X are agreed on beforehand. After sending N packets over X flows, the encoder waits for the acknowledgements (ACKs) of these packets, then will do the next sending only after receiving all ACKs of N packets. Meanwhile, the decoder extracts secret message according to the packets distribution

in flows as soon as collecting N packets sent by encoder. Cloak is implemented using a normal TCP stack and its reliability is ensured by TCP's reliable transmission mechanism. Then comparing with other timing channels, not encoding by exact time interval makes Cloak resist most adverse network conditions, thus Cloak can keep high data rate and low bit error rate in a worse network condition. There are two scenarios for the Cloak encoder and decoder to communicate, as shown in Figure 1. In Figure 1(a), the encoder only establishes HTTP sessions with a remote server. While in Figure 1(b), the encoder establishes HTTP sessions with different remote servers. Although in the second scenario the communication is more covert, the decoder should be located on the gateway which all sessions pass through and the suitable gateways are usually near to the encoder, so the covert communication distance is restricted. Taking it into consideration, the detection scheme in this paper for Cloak is based on the first scenario.



(a)All flows connect to the same Web server (b)All flows connect to different Web server

FIGURE 1. Two communication scenarios for Cloak

Considering the changes of the values of (c, N, X) and potential huge encoding space, it is unrealistic to use a table-lookup encoding/decoding approach to exchange every explicit codebooks between encoder and decoder. The authors use ranking and unranking algorithms [13] referenced to the field of Enumerative Combinatorics to fulfill encoding/decoding. For instance, the number of unique packet-flow distribution (i.e. combination number) for Cloak^6 (indistinguishable packets, distinguishable flows, at least one packet in a flow) is C_{N-1}^{X-1}, then each unique packet-flow distribution can maximally encode an L-bit word, where $L = \left\lfloor \log_2(C_{N-1}^{X-1}) \right\rfloor$. The encoder transforms L-bit word to a decimal number R when starting every sending. Then R is regarded as the rank for corresponding packet-flow distribution and unranking algorithm will give the exact packet numbers sent in each flow. On the other hand, the decoder decrypts the value of R based on the observed packet-flow distribution, then getting L-bit secret message. The distinguishable packets/flows increase the channel capacity. To make the TCP packets distinguishable, additional markers are usually added to them, which could reduce the channel's camouflage capability. While the TCP flows are distinguishable in most situations. Therefore Cloak^6 and Cloak^4 have a better tradeoff between channel capacity and camouflage capability compared with other types. Due to the limited space, we only describe the detection scheme for Cloak^6. However, the proposed method can also detect other types of Cloak by few modifications. The cloak mentioned below is referred to Cloak^6 unless otherwise stated.

Luo et al. also proposed a D-limited codeword scheme [12] to solve HoLB (A Head-of-Line Blocking) problem existing in Cloak. However, according to the result of Figure 5 in Ref. [12], the gain of throughput is slight. Although the scheme mitigate the influences of adverse network conditions, the channel capacity also decreases with the reducing of encoding space (the maximum number of packets sent in a flow is limited to D), thus it is not necessary to take consideration of the D-limited codeword in our detection scheme. Paper [14] gives two improvements for Cloak considering the channel's undetectability. The first one is mimicking the behavior of normal HTTP flows to evade detection. The second one is a flow-size-based method to evade detection (i.e. encoding by flow sizes instead of packets). These two improvements make the implementation more complicated and less practical, so we still focus on the original Cloak.

3. The Proposed Method.

3.1. **Analysis of the burst size distribution.** The burst size of a TCP flow refers to the number of packets sent out together [14], the upper bound number of bytes for these packets is determined by send window size. According to the encoding scheme of Cloak, each flow sends corresponding number of packets for every L-bit word, these packets can be sent out in a burst in most situations and the number of packets sent in each flow is calculated by combinatorial generation algorithm (i.e. unranking algorithm) [13]. Therefore, the distribution of burst size represents the theoretical distribution of packet number of Cloak, then we can design detecting method based on the distribution of burst size. Paper [14] also mentioned TCP burst size can be a characteristic for detection, but without implementation details of detection scheme and experimental verification. Moreover, the authors simply judge the burst size of Cloak is uniformly distributed and we consider it is an incomplete conclusion (the distribution is uniform only when $X = 2$). For a given value of (N, X), taking all the integer values in interval $\left[0,\ C_{N-1}^{X-1}\right)$ for R, then the theoretical distribution of packet number sent in each flow can be obtained by combinatorial generation algorithm. For instance, Figure 2 shows the theoretical distribution of packet number for each flow when $(N, X) = (10, 4)$, while Figure 3 shows the theoretical distribution of packet number for one flow when (N, X) taking different values.

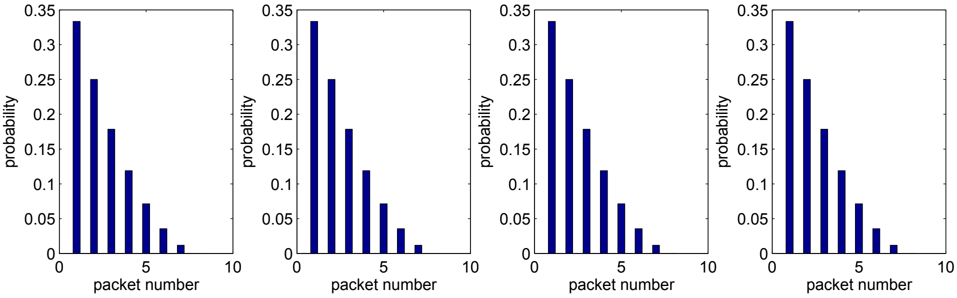


FIGURE 2. Packet number distribution of each flow when $(N, X) = (10, 4)$

As shown in above two Figures, for a given value of (N, X), there is same theoretical distribution in each flow. For different values of (N, X), the packet number is uniformly distributed only when X=2 while distributions of other values are similar to each other. Then we use theoretical distribution as a feature to judge whether the traffic contains a Cloak covert channel.

There is an important design issue about how to identify a burst in a flow. For a specific bidirectional communication, the traffic can be analyzed manually which packets belong to a burst. While it is not easy to identify a burst by a computer program only according to the inter-packet intervals (IPIs) because of the various type of normal traffic. After deeply investigating on plenty traffic, an identification method is given as follows. Firstly, we randomly choose B (300 is a proper value) consecutive packets from a detection window, calculating the inter-packet intervals and sorting these values denoted

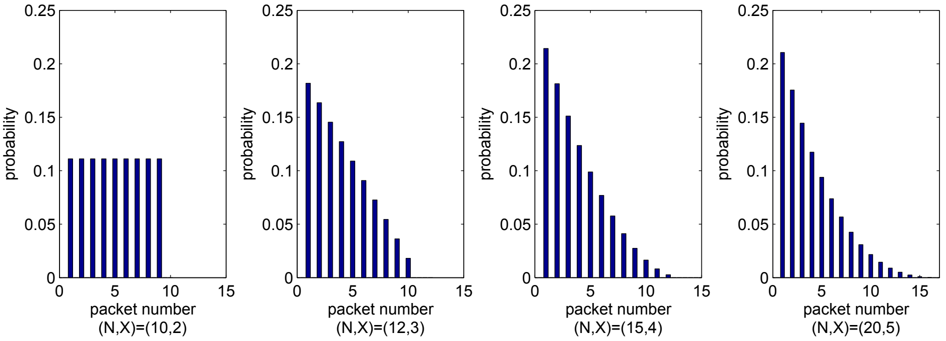


Figure 3. Packet number distribution of one flow when $(N,\ X)$ taking different values

by IPI_i. Secondly, we then calculate the difference between adjacent IPIs, $DIFF = \frac{IPI_{i+1}-IPI_i}{IPI_i}$ $(i = 1, 2, \cdots, 298)$. Thirdly, we seek the maximum value in sequence of $DIFF$ and get the position p, if $IPI_p > 0.5ms$ and $IPI_p < 15ms$, then $T = \frac{IPI_{p+1}+IPI_p}{2}$ is accepted as a threshold (i.e. the consecutive packets whose IPIs are all less than T belong to a burst). At last, if IPI_p can not meet the conditions, we will seek the second largest value of $DIFF$ and check. After 5 times, if we do not obtain proper IPI_p, that means all 300 packets belong to a burst and B need to be added for recalculation (for $IPI_p \leq 0.5ms$) or each packet belong to a burst (for $IPI_p \geq 15ms$).

3.2. **Chi-Squared test.**

After identifying bursts of flows, Chi-Squared test is utilized to judge whether the burst size distribution obeys the theoretical distribution generated by Cloak. Chi-Squared Goodness-of-Fit test [15] can be used to test a null hypothesis stating that the frequency distribution of certain events observed in a sample is consistent with a particular theoretical distribution.

Suppose the distribution of population X' is unknown, $x_1, x_2, \cdots, x_n$ is the sample of X', $F(x)$ is a known distribution function, the hypothesis need to be tested is

$$H_0 : \ distribution\ function\ of\ X'\ is\ F(x) \tag{1}$$

For χ^2 test, the real axis is divided into m disjoint intervals $-\infty = t_0 < t_1 < \cdots < t_m = +\infty$. Let n_i be the frequency of sample $x_1, x_2, \cdots, x_n$ belonging to $[t_{i-1},\ t_i)$, then $\sum\limits_{i=1}^{m} n_i = n$ which is the sample size. Let p_i be the probability of X' belonging to $[t_{i-1},\ t_i)$, $p_i = F(t_i) - F(t_{i-1})$ when H_0 is true. The theoretical frequency of sample belonging to $[t_{i-1},\ t_i)$ is f_i, where $f_i = n \times p_i$. So the test statistic of H_0 created by Pearson is

$$\chi^2 = \sum_{i=1}^{m} \frac{(n_i - f_i)^2}{f_i} \tag{2}$$

When H_0 is true, Pearson statistic obeys χ^2 distribution whose df(degree of freedom) is $m-1$. For a given level of significance α, the rejection region R' for H_0 can be obtained by table-lookup, $R' = [\chi^2(m-1),\ \infty)$. Thus, whether Pearson statistic belongs to R' can be used to reject or not reject hypothesis H_0.

When we use rejection region to judge whether the traffic contains Cloak covert channel, the result is sensitive to the sample size n. Therefore we divide both side of Formula (2) by n, the new statistic is denoted by χ_n^2 and a threshold Th is set for judgment.

$$\chi_n^2 = \frac{\chi^2}{n} = \sum_{i=1}^{m} \frac{(n_i/n - p_i)^2}{p_i} \tag{3}$$

Let M be the maximum burst size observed from flows, then the real axis will be divided into M disjoint intervals and each burst size belongs to an interval. For determining values of p_i, parameter N and X need to be estimated at first. Cloak is a multilink-based covert channel, so the detector needs to maintain a list of link-info for monitoring concurrent communication which has the same source/destination IP address, then the flow number of concurrent communication can be consider as X. Theoretically, N is the total number of packets from all flows in a sending period, however it is difficult to judge which bursts from each flow are in the same period, we utilize maximum burst size M to infer the value of N. After analyzing above, the procedure of detection method is illustrated as follows.

Step 1: If the concurrent communication exists, value of X will be determined. Burst size is counted from the flow within detection window W, then we get an n-length sequence and the maximum burst size M.

Step 2: Let intervals be $(T, T+1]$, $T = 0, 1, \cdots, M-1$, frequency n_i of each interval is counted. If $n_i < 5$, merging intervals is made to keep detection accuracy.

Step 3: As mentioned above, probability of burst size distribution p_i can be calculated according X and M, moreover for theoretical frequency $f_i = n \times p_i$, if sample intervals is merged, f_i need to be merged correspondingly.

Step 4: Calculate Statistic χ_n^2, for a given threshold Th, if $\chi_n^2 < Th$, the traffic within W is considered to be a Cloak covert communication. Slide W and begin next calculation.

4. **Experimental Results.**

4.1. **Datasets.**

We have implemented Cloak covert channel based on TCP socket (SOCK_STREAM) in Windows XP platform, then the communication traffic generated by Cloak is the object for detection. Typical test environment of detection for Cloak is shown in Figure 4, the sender and receiver are connected by a switch which has port mirroring function, then the detector connected to the switch can monitor all the traffic passed through. To simulate the network conditions of WAN, a host running Linux with double NICs (Network Interface Card) is joined to the link, then the function module Netem of Linux is used to simulate packet losses, delays and so on. The detection scheme described in Figure 4 is an online real-time one, we can also dump the communication traffic and use it for an offline detection.

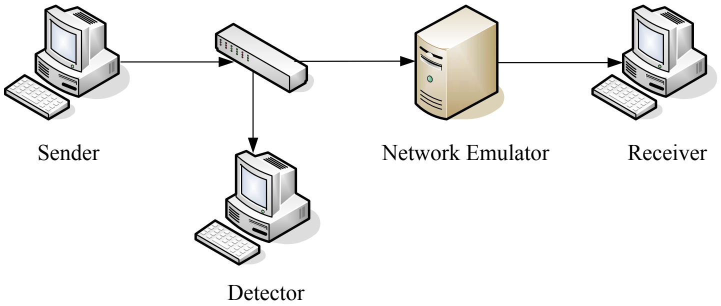


Figure 4. Typical test environment of detection for Cloak

In test environment of Figure 4, the Cloak traffic set for testing is obtained by changing the values of N and X. Meanwhile we prepared two groups of normal traffic sets, one is from WIDE project [16] and the traffic is captured from its sample point-F, we choose HTTP flows during March 20, 2013-March 26, 2013 as normal traffic set. The other is the HTTP traffic obtained in our laboratory's gateway (about 20 hosts connected to Internet) during 24 hours.

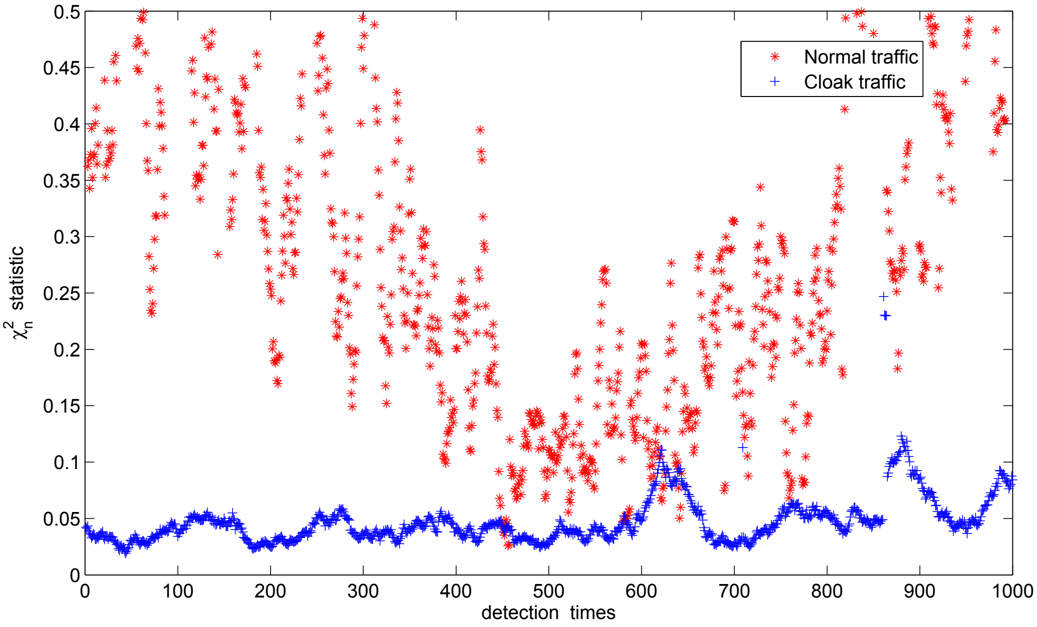


Figure 5. χ_n^2 statistic of normal traffic and Cloak traffic

4.2. **Results and analysis.** χ_n^2 statistic of normal traffic and Cloak traffic are calculated separately. The distribution of χ_n^2 is shown in Figure 5 (for a distinct display, the values greater than 0.5 have not been drawn in this figure). The statistics of two types of traffic have few overlaps, then we can choose a threshold Th to identify these two kinds of traffic. After plenty of experiments, 0.08 was chosen as detection threshold in this paper. Detection window W is a significant parameter for detection rate, when W is small, the sample size of counted burst size is not enough to infer population distribution. The detection rate under different values of (N, X) is shown in Figure 6, we can see that the

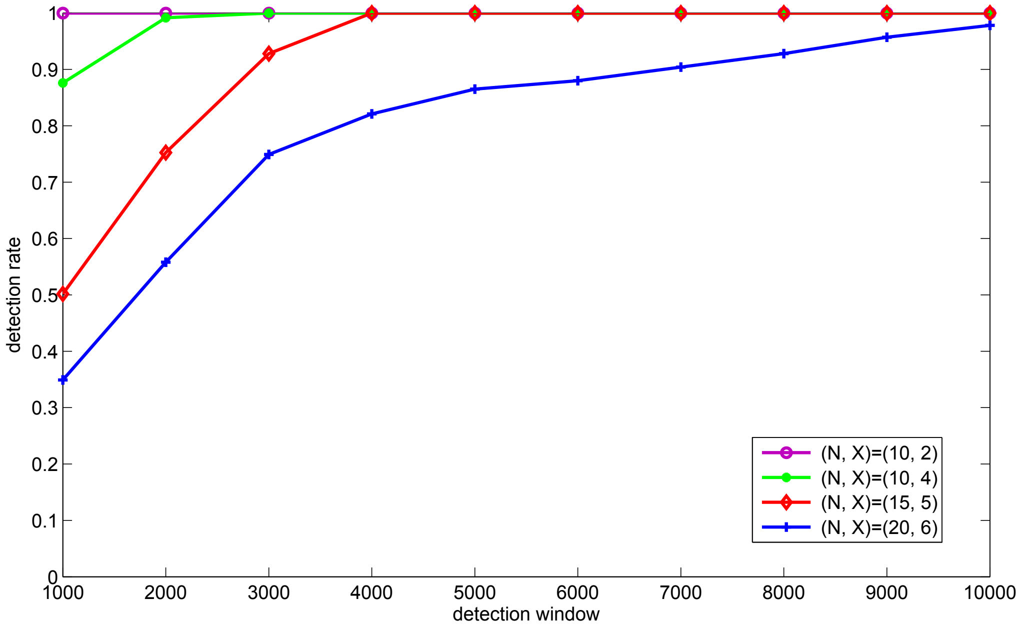


Figure 6. detection rate under different values of (N, X)

detection rates approach 1 as the growing of W. Therefore, a flexible detection window is considered in our scheme and W may increase step by step with the increase of observed maximum burst size M.

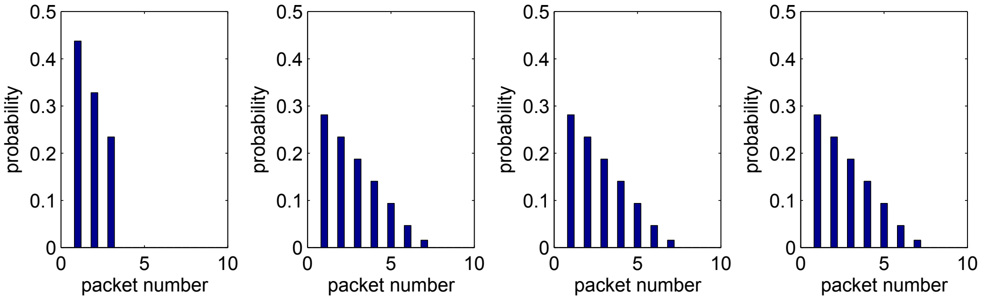


FIGURE 7. Packet number distribution of each flow when $(N, X) = (10, 4)$ under binary encoding

From the experiment we further find only X-1 flows can be detected as abnormal one in most cases while Cloak has X flows. The reason of this phenomenon is the usage of binary encoding for Cloak. For L-bit word, only 2^L types of combination are used from the whole combinatorial generation space. Take $(N, X) = (10, 4)$ for instance, all the possible combination number is $C_{N-1}^{X-1} = C_9^3 = 84$, but only 64 types is utilized to encode. Distribution of packet number for each flow when $(N, X) = (10, 4)$ under binary encoding is shown in Figure 7. Compare with Figure 2, one of the flow's distributions has a large deviation while the other ones keep similar. Hence, for a concurrent communication, if most flows obey theoretical distribution, we could judge all the flows belong to a Cloak covert channel.

For false positive investigation, 50 HTTP flows were chosen from WIDE set and lab set separately, detection window W=5000, threshold $Th = 0.08$, the average false positive of each set is shown in Table 1.

TABLE 1. Average false positive of two normal sets

	http flows from WIDE set	http flows from lab set
average false positive	2.3%	1.7%

The detection schemes for covert timing channel are usually designed as a special method against one covert channel while entropy-based test is a general detection scheme effecting on most existing covert timing channels [17]. Thus, we compare the proposed method with entropy-based test. The entropy-based test contains two parts, EN test for detecting abnormal shape and CCE test for detecting abnormal regularity. We have implemented these two algorithms and utilized the same parameter settings suggested in the original paper [11]. 200 HTTP flows (over 2,000,000 packets) were chosen from lab set, half of them are used as training set to obtain bin ranges of entropy-based test, the other half is the legitimate HTTP set for test. The Cloak traffic is obtained under the setting $(N, X) = (15, 5)$ and then we get 5 flows for test. The detection results are shown in Table 2 under fixed detection window W=5000. From the Table we can find the CCE test is invalid for detecting Cloak. It is because CCE test uses a coarse-grain binning and can not distinguish Cloak traffic from legitimate HTTP traffic. EN test uses a fine-grain binning, so it can detect tiny changes of inter-packet delays (IPDs) distribution, however, the detection rates are still lower than our proposed method. It also should be noticed that EN test gets much better detection rate for Flow-1 than other flows. It is caused by Cloak's encoding scheme (as above discussion, binary encoding makes Flow-1 contain only small burst size) which makes a larger deviation of IPDs distribution in Flow-1.

Table 2. Comparison between proposed method and entropy-based test

test	HTTP (false positive)	Cloak (detection rate)				
		Flow-1	Flow-2	Flow-3	Flow-4	Flow-5
EN $\leq$ 8.7	0.01	0.95	0.85	0.88	0.83	0.82
CCE $\leq$ 1.6	0.01	0.07	0	0	0.01	0
$Th \leq 0.08$ (proposed method)	0.01	0.99				

For given parameters $(N, X) = (20, 6)$, $W = 8000$, $Th = 0.08$, the influence on detection rate cased by round-trip time(RTT) and packet loss rate(PLR) has been investigated. As shown in Figure 8, the increase of RTT has little influence on detection rate because our detection method isn't based on the analysis of exact time intervals and the change of RTT has little affect on the identification of the bursts. As shown in Figure 9, lower PLR also has little influence on detection rate, as the increase of PLR to a boundary, the detection rate drops to 0 rapidly. This phenomenon is cased by TCP retransmission mechanism, the enabled SACK (Selective Acknowledgment) option of TCP makes the sender only retransmit the lost packets and consecutive lost packets are allowed to perform repacketization, sending a bigger segment. For our detection method, that means the number of burst which contains one packet will increase a lot, when the number is big enough, the distribution of burst size will deviate from the theoretical one and the detection rate will reduce quickly. The experimental results show that there is little influence on proposed method when PLR is less than 5%. In fact, the PLR on Internet is much smaller than 5%.

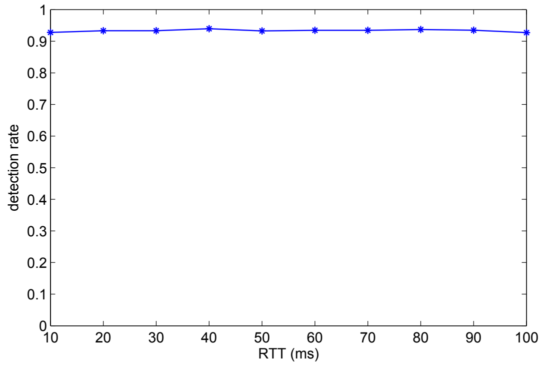


Figure 8. Influence of RTT

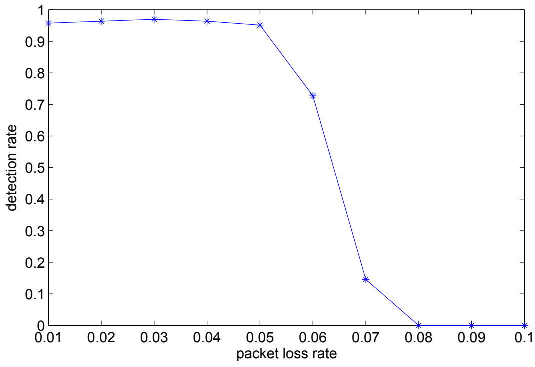


Figure 9. Influence of PLR

5. Conclusions.

In this paper, a detection method for Cloak covert channel based on burst size distribution and Chi-Squared test is proposed, experimental results show the high detection performance of our method. Meanwhile, the detection performance influence coming from RTT and packet loss is also discussed, experimental results show the well robustness of the proposed method. Although the detection method is illustrated by Cloak^6, it is effective to Cloak^{1,3,4}. While Cloak$^{7-10}$ is the type with indistinguishable flows, thus the distribution of burst size in a single flow is random and the burst size sequences from each flow need to be merged to analyze the total distribution for detection.

In the future, we will focus on further investigation on the improved Cloaks mentioned above which are more robust and undetectable.

Acknowledgment. This work was supported by the NSF of China (Grant No. 61170250, 61103201) and the Fundamental Research Funds for the central Universities (Grant No. 30920140121006).

REFERENCES

[1] E. Zielińska, W. Mazurczyk, and K. Szczypiorski, Trends in steganography, *Communications of the ACM*, vol. 57, no. 3, pp. 86–95, 2014.

[2] C. Patsakis and N. Aroukatos, LSB and DCT steganographic detection using compressive sensing, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 1, pp. 20–32, 2014.

[3] National Computer Security Center, US DoD, Trusted Computer System Evaluation Criteria, *Tech. Rep. DOD 5200.28-STD*, National Computer Security Center, Dec. 1985.

[4] M. A. Padlipsky, D. W. Snow, and P. A. Karger, Limitations of End-to-End encryption in Secure Computer Networks, *Tech. Rep. ESD-TR-78-158*, Mitre Corporation, Aug. 1978.

[5] C. G. Girling, Covert Channels in LAN's, *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 292–296, 1987.

[6] G. Shah, A. Molina, and M. Blaze, Keyboards and Covert Channels, *Proceedings of the 15th conference on USENIX Security Symposium*, pp. 59–75, Aug. 2006.

[7] S. Cabuk, C. E. Brodley, and C. Shields, IP Covert Timing Channels: Design and Detection, *Proceedings of the 11th ACM conference on Computer and communications security*, ACM, pp. 178–187, 2004.

[8] S. Cabuk, *Network Covert Channels: Design, Analysis, Detection, and Elimination*, Ph.D. Thesis, Purdue University, West Lafayette, USA, 2006.

[9] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, Model-based Covert timing Channels: Automated Modeling and Evasion, *RAID 2008, LNCS 5230*, pp. 211–230, 2008.

[10] G. Liu, J. Zhai, and Y. Dai, Network Covert timing Channel with Distribution Matching, *Telecommunication Systems: Modeling, Analysis, Design and Management*, vol. 49, no. 2, pp. 199–205, 2012.

[11] S. Gianvecchio and H. Wang, An Entropy-Based Approach to Detecting Covert Timing Channels, *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 785–797, 2011.

[12] X. Luo, E. Chan, and R. Chang, Cloak: A Ten-fold Way for Reliable Covert Communications, *ESORICS 2007, LNCS 4734*, pp. 283–298, 2007.

[13] D. Kreher and D. Dtinson, *Combinatorial Algorithms: Generation, Enumeration and Search*, CRC press, 1998.

[14] X. Luo, E. Chan , P. Zhou, and R. Chang, Robust Network Covert Communications Based on TCP and Enumerative Combinatorics, *IEEE Trans. on Dependable and Secure Computing*, vol.9, no.6, pp.890–902, 2012.

[15] P. E. Greenwood and M. S. Nikulin, *A guide to chi-squared testing*, Wiley, New York, 1996.

[16] "Packet traces from WIDE backbone", http://mawi.wide.ad.jp/mawi/, 2013.

[17] R. Archibald and D. Ghosal, A comparative analysis of detection metrics for covert timing channels, *Computers & Security*, vol. 45, pp. 284–292, 2014.