Journal of Information Hiding and Multimedia Signal Processing ©2009 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **3**, May **2015**

SkyLen: a Skype-based length covert channel

Jiangtao Zhai and Mingqian Wang

School of Electronics and Information
Jiangsu University of Science and Technology
No.2 Mengxi Road, Zhenjiang, Jiangsu, P.R.China
jiangtaozhai@gmail.com, wmq1989219@126.com

Guangjie Liu and Yuewei Dai

School of Automation
Nanjing University of Science and Technology
No.200 Xiaolingwei Street, Nanjing, Jiangsu, P.R.China
gjieliu@gmail.com, dywjust@163.com

Received December, 2014; revised January, 2015

Abstract. *Network covert channel is a technology that transfers information secretly through the computer network. The length-based covert channel is one of the most popular covert channels. Most of the existing length-based schemes are vulnerable to detections due to the abnormal statistical features of the covert traffic. In this paper, a Skype-based length covert channel SkyLen is proposed. The proposed method is based on the popular software Skype. The model of the Skype traffic is built first and then the encoding method is based on the built model. This will make the covert traffic has consistent high-order statistical feature with the normal case. Finally, for further improving the method's stealth, the Monte Carlo sampling method is used in the encoding process. The capacity of the proposed method is 4bits/packet, and the detection experiments show that the proposed method is much stealthier than the existing one.*
Keywords: Network covert channel, Skype traffic, Covert channel built, Information hiding

1. **Introduction.** Edward Snowden is an American computer professional from the National Security Agency (NSA). The documents he leaked revealed numerous global surveillance programs. In the surveillance environment, how to transfer information secretly is a very interesting problem. Network covert channel is one of the potential methods to solve this problem. It is a hidden communication technique that protects the security of the messages transmitted trough open network. Different from the principle of cryptography, it conceals the very existence of the communication itself in order to prevent the unauthorized party from getting access to the secret messages. Network covert channel utilizes the redundancies of network protocols as the vehicle to transfer secret messages covertly. It is similar to but superior than the manners of information hiding in multimedia such as image, audio or video. Since the massive and dynamic network communications are better candidates as the secret carrier, it is difficult for an attacker to detect and track the covert sessions between two arbitrary remote entities.

There are two broad categories of covert channels: covert storage channel and covert timing one. The covert storage channels which modify the protocol-specific header fields for data hiding are easily manipulated and abundant literatures on this topic have been reported by researchers [1, 2, 3] . Although these schemes have considerable bandwidth,

they are easily be detected by the existing methods. The covert timing channels conceal the secret information by modulating the time-dependent information of the transmitted network packets [4, 5, 6, 7]. These methods under this technique are relatively hard to be detected but they are sensitive to the changes of network environment [8], which may greatly degrade the performance of this covert channel.

In recent years, length-based covert channel has been popular among researchers due to the better property that it is not susceptible to network conditions. In the length-based schemes, the packet length gets adjusted for embedding secret messages. Here, some of the notable works are reviewed. The concept of length-based covert channel was first proposed by Padlipsky in [4] and his idea was realized by Girling [9]. The authors modulated the length of link layer frames and employed 256 different frame lengths to represent the secret bytes. It can be easily detected as it produces abnormal traffic. Yao et al. [10] proposed another model-based packet length covert channel. The sender and the receiver both share a secret matrix which consists of 256 rows and each cell in the matrix represents the unique length. The sender fetches a secret byte and randomly selects a length from the corresponding row. As it inevitably generates abnormal to the overt traffic, it is still detectable.

Later, Ji et al. [11] proposed a length covert channel that shows substantial improvement over the past ones. In its method, both parties share a set of normal packet length collected beforehand as a reference. The sender takes certain bits from the secret flow and uses the agreeable algorithm to select a length pseudo-randomly in the reference. After that, the decimal number of the secret bits is added to this length. Then a packet of the new length is transmitted. Finally, the reference gets updated when a new length is formed. This method tries to imitate the normal traffic and shows good performance when the packet length varies abundantly. However, in other cases, it produces abnormal traffic.

Recently, Omar [12] proposed a length-based scheme called DNS reference covert channel (DRCC). An analysis on standard DNS queries within their campus network showed that the packet length was between 24 and 63 Bytes. Thus, 16 different packet lengths of normal DNS request which occurred most frequently were used to represent 4-bits secret data. Anand [13] proposed a length covert channel using UDP protocol. It is observed that the packet length of the chat application based on UDP protocol is randomly distributed. This attribute is utilized to hide the secret information by adjusting the length of UDP payload. The above two schemes have made progress in mimicking the normal flow, but their features of packet length are distinct compared with the normal one.

According to the brief review of some previous length covert channels, it can be found that most schemes are vulnerable to detections owning to the abnormal features generated during the embedding process. Besides, a particular network application is generally protocol-specific which results in its unique features. If the statistical features of the normal flow are altered after embedding, they might be judged anomaly. Thus, the latent covert channel will be exposed to an attacker. In this paper, a Skype-based length covert channel called SkyLen is proposed to overcome this flaw. Firstly, the Parzen Kernel Estimation is employed to fit the model of Skype packet length. Secondly, to make the covert channel hard to be detected, the Monte Carlo sampling technique is adopted in the embedding scheme to preserve the high-order statistical feature-the cumulative distribution function(CDF) of Skype traffic.

The remainder of this paper is organized as follows: in the next section, the statistical model of Skype traffic is constructed. In section 3, the proposed scheme is introduced in detail. In section 4, experimental results are presented and analyzed. Finally, the paper is concluded in section 5.

2. The statistical model of Skype traffic.

2.1. **A brief introduction to Skype.** Before elaborating our scheme, a brief introduction to the widely used network service-Skype is given firstly. It is a proprietary IP telephony service based on peer-to-peer (P2P) technique, which was originally developed by the organization that created Kazaa in 2003. It is a real-time service which enables users to make phone calls using IP protocol through the network. Skype utilizes the 32 kbps voice coding to ensure the quality of connection and AES (Advanced Encryption Standard) encryption method to protect the privacy of the communication. Typically, the preferred transport protocol for Skype to transmit the voice messages is User Datagram Protocol (UDP). In March 2012, it was reported that there were 35 million users online simultaneously. It has also been estimated that in 2011, Skype had acquired about 33 percent of the world's international telephone market.

As discussed in [14], the most favorable carrier for secret messages should have two features: widely used and confused, which means that the usage of such carrier should not be regarded as anomaly itself and the massive confused traffic could be the mask for the hidden communication. From this point, Skype is an ideal candidate to achieve the above goals, so it is employed in our scheme.

2.2. **Model fitting for Skype.** In the network communication, the packet length of particular services is different and their features are also unique. Hence, it is motivated to construct the length model of Skype in order to acquire its high-order statistical feature. In this paper, one of the most popular non-parametric estimation methods-Parzen Kernel Estimation is utilized to fit the Probability Distribution Function (PDF) of Skype traffic.

In the preparing period, a set of the normal Skype traffic which contained 100,000 packets was collected. The Skype traffic was captured by WinpCap software during the conversation between two Skype clients (Skype for Windows v.6.10) which are located in the city of Zhenjiang and Nanjing respectively. The distance between the two cities is 70km, and the ISP of the two clients is China Telecom.

After that, the PDF of the normal Skype traffic is estimated using Parzen Kernel method. The collected Skype set is denoted as $S = \{x_1, x_2, \cdots, x_N\}$, where N refers to the size of the collected set. From the collected set, it can be found that the range of Skype packet length is between 1 and 200.

The Normal Window Function employed in the Parzen Kernel method is shown in Eq. (1)

$$\phi(u) = \frac{1}{\sqrt{2\pi}} \exp(-\frac{1}{2}u^2), u = \frac{x - x_i}{h_N} (i = 1, 2, ...N) \tag{1}$$

Where x_i represents the value of the packet length in the sample set S and h_N represents the window width which is set to $1/\sqrt{N}$, thus, Eq.(2) has been achieved.

$$\phi(u) = \phi(\frac{|x - x_i|}{h_N}) = \frac{1}{\sqrt{2\pi}} \exp[-\frac{1}{2}(\frac{|x - x_i|}{h_N})^2](i = 1, 2, ...N) \tag{2}$$

According to Eq.(2), the estimated PDF $\hat{f}(k)$ can be got from Eq.(3), which is shown in Fig.1.

$$\hat{f}(k) = \frac{1}{N} \sum_{i=1}^{N} \frac{1}{h_N} \varphi(\frac{|k - x_i|}{h_N}), k = 1, 2, \cdots, 200 \tag{3}$$

And, the theoretical Cumulative Distribution Function (CDF) can further be obtained as Eq.(4)

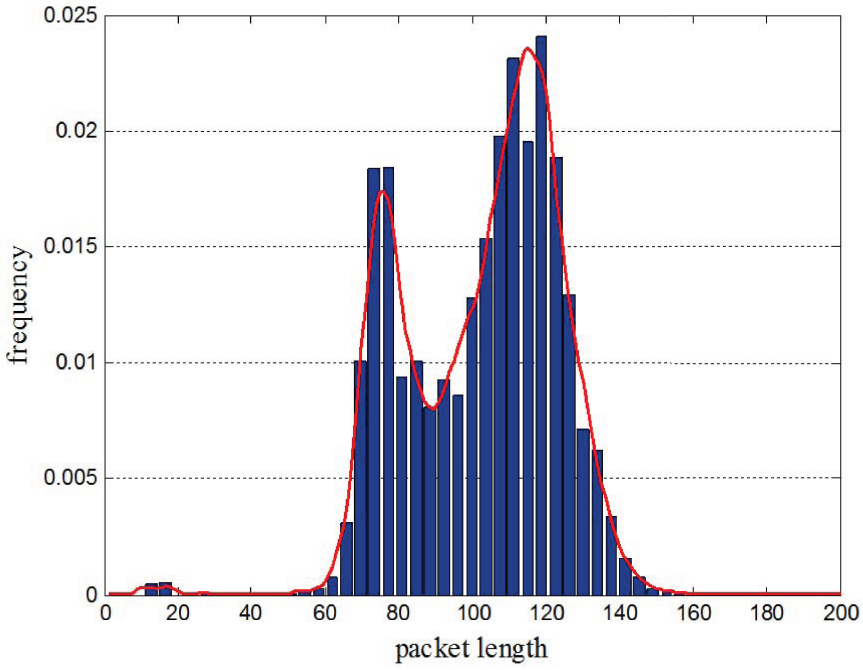

FIGURE 1. The estimated PDF of Skype traffic

$$\hat{F}(k) = \sum_{i=1}^{k} \hat{f}(k), k = 1, 2, \cdots, 200 \tag{4}$$

The frequency distribution histogram (FDH) of the sample set is also demonstrated in Fig.1, and it is easily observed that the estimated PDF fits the actual FDH well. Further more, the actual and the theoretical CDF are compared in Fig.2. It is manifest that they are aligned with each other.

In order to verify the validity of our built model, the Kolmogorov-Smirnov test (K-S test) is exploited to measure the goodness of fit. It is assumed that $H_0 : \hat{F}(k) = F(k)$ and $H_1 : \hat{F}(k) \neq F(k)$. Suppose $\hat{F}(k)$ is the theoretical CDF and $F(k)$ is the actual CDF of Skype traffic, which are calculated as follows:

Let $L = \{l_1, l_2, \cdots, l_m\}$ be a group that contains all the valid packet length in the sample set S. From the above analysis, it is easily known that l_i is between 1 and 200. The actual relative frequency of each packet length is represented by the following discrete function.

$$f(k) = \frac{n(k)}{N}, k = 1, 2, \cdots, 200 \tag{5}$$

In Eq.(5), $n(k)$ is the number of packets whose length are k and N is the total number of elements in the sample set. Then the actual CDF is able to be obtained.

The deviation between the actual and theoretical CDF can be achieved by calculating a certain statistic D_n, which is given as

$$D_n = \sup_x \left| \hat{F}(k) - F(k) \right| \tag{6}$$

According to Eq.(6), D_n is calculated in our case, whose value is 0.000922. It can be proved that the statistic D_n follows the limiting distribution of $K(\lambda)$, hence we look up in the critical value table of K-S test when the significance level α is 0.05.

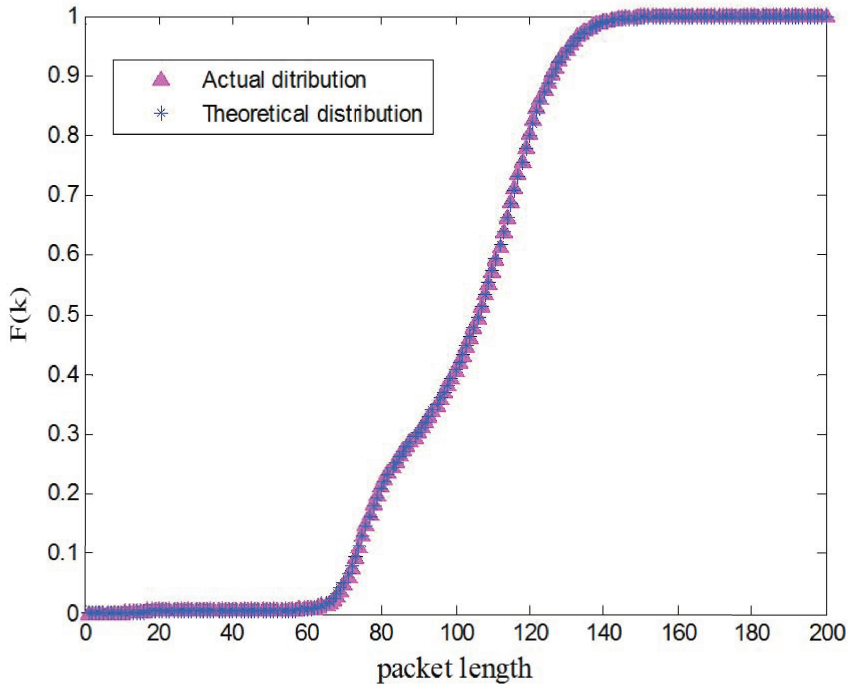

FIGURE 2. The comparison of CDF between the actual and theoretical cases for Skype traffic

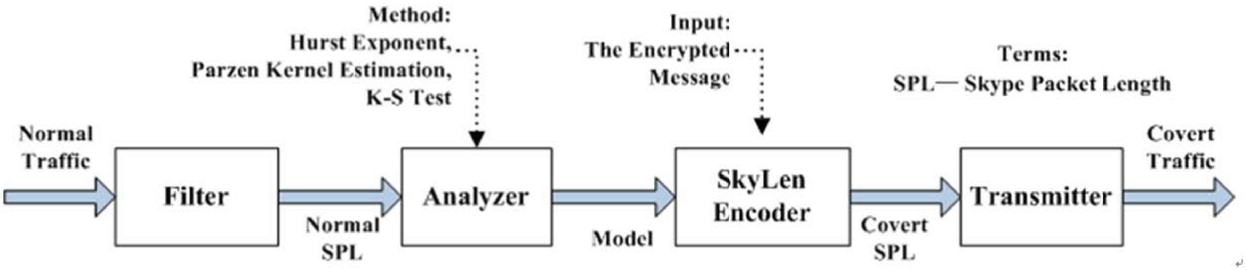

FIGURE 3. The scheme of SkyLen

$$P(D_n \geq D_{n,\alpha}) = \alpha \tag{7}$$

As a result, $D_{n,\alpha} = 0.00435 > D_n = 0.00092$, which indicates that the null hypothesis $H_0 : \hat{F}(k) = F(k)$ should be accepted.

3. **The proposed scheme:SkyLen.** The proposed scheme of our method is shown in Fig.3.

According to the length model built in section 2, the estimated Cumulative Distribution Function (CDF) is exploited during the encoding process. In order to make our scheme undetectable, Monte Carlo sampling technique-a classical approach to preserve the raw CDF is adopted in the embedding algorithm.

Initially, the y axis is divided into several segments equally and then the corresponding intervals along with the x axis [0, 200] are obtained. In our case, the y axis is divided into 16 segments to guarantee that there is at least one packet length in each corresponding interval of the x axis. The 16 segments represent the secret data from "0000" to "1111"

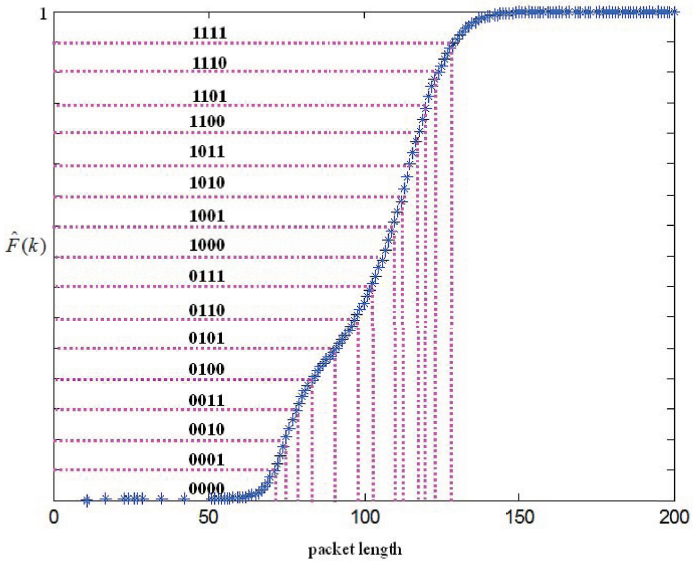

FIGURE 4. The mapping from the secret data to the interval of packet lengths of CDF

respectively, shown in Fig.4. Hence, 4 bits secret data can be transmitted per packet. The intervals of packet length are generated as follows:

$$\frac{i-1}{16} < \hat{F}(k) \leq \frac{i}{16} \ (i = 1, 2, \cdots, 16 \ \ k = 1, 2, \cdots, 200) \tag{8}$$

$$T_i = \{l_{(i,1)}, l_{(i,2)}, \cdots, l_{(i,j)}, \cdots, l_{(i,ni)}\} \ (i = 1, 2, \cdots, 16) \tag{9}$$

Where $\hat{F}(k)$ in Eq.(8) is the estimated CDF of the Skype packet length given in section 2.2. The symbol T_i represents the i^{th} interval of packet length corresponding to the i^{th} segment of $\hat{F}(k)$ and $l_{(i,j)}$ is the j^{th} element of the i^{th} interval of the packet lengths. T_i in Eq.(9) which can be acquired by Eq.(8), and n_i denotes the number of the whole elements in the i^{th} interval which satisfies the following conditions:

$$\begin{cases} n_i \geq 1, \ \ i = 1, 2, \cdots, 16 \\ \sum_{i=1}^{16} n_i = 200 \end{cases} \tag{10}$$

Thus, in this manner each segment represents the secret message from "0000" to "1111" is mapped to a few packet lengths in the corresponding interval.

(1) Encoding

Step I: Since Monte Carlo sampling requires the input to be uniformly distributed, the secret message is first encrypted with the agreeable algorithm to meet this demand. Let S_e be the encrypted format of the secret message S to be sent. Then S_e is the binary form of S and it is divided into m blocks. Each block contains 4 bits secret data, which can be described $S_e = s_1 s_2 s_3 ... s_m, s_i = s_{i_1} s_{i_2} s_{i_3} s_{i_4} (i = 1, 2, \cdots, m)$, where s_i refers to the i^{th} block of S_e.

Step II: For the i^{th} sending, the encoding function $E(s_i)$ is defined as:

$$len = E(s_i) = rand(T_{[s_i]_d+1}) \ ([s_i]_d + 1) \in [1, 16] \tag{11}$$

Where $[s_i]_d$ in Eq.(11) ranges from 0 to 15, which indicates the decimal form of s_i. The symbol $T_{[s_i]_d+1}$ in Eq.(11) refers to the $([s_i]_d + 1)^{th}$ interval of packet length mentioned

in Eq.(9). It should be noticed that, the input of the function $rand()$ is a set of packet length $T_{[s_i]_d+1}$, and $rand(\bullet)$ is a pre-defined function that used to select a value from the given set $T_{[s_i]_d+1}$ randomly. The symbol len indicates the packet length carrying the secret data. For example, if $T_2 = \{12, 13, 14\}$, the value of the packet length '12','13' or '14' in set T_2 has the equal probability to be picked out using the function $rand(T_2)$.

Step III: A stegnographic packet with the length len is sent to the receiver.

Step IV: Steps II and III are repeated until the whole secret message has been sent.

(2) Decoding

On the receiver side, the covert flows are captured first. Then their packet length len_{recev} is extracted to retrieve the stealth by judging the interval to which len_{recev} is belonged to. As such, after all the secret data are decoded, they should be decrypted to recover the final secret message.

4. **Experimental Results.** To evaluate the performance our scheme, an experiment is done to compare the proposed SkyLen with Liping's method [11]. The experiment is performed in the same situation mentioned in section 2.2. Both of them work in Windows XP SP3. The secret message is encrypted by AES cipher algorithm with a shared key.

In the experiment, the high-order statistical features-CDF of the normal and the covert traffic are compared considering the impact of different encoding window sizes. Four groups of SkyLen covert traffic with the encoding window sizes range from 50 to 1,000 are shown in Fig.5 concerning their CDF. Meanwhile, the total number of the packet length in each group is 10,000 and we represent each group as $G(50, 200)$, $G(100, 100)$, $G(500, 20)$ and $G(1000, 10)$. The CDF of covert traffic (the total number of the packets are 10,000) for Liping's method is also present in Fig.5.

From Fig.5, it is noticed that the CDF of SkyLen with different encoding window size is quite closer to that of the actual case. And, our method fits the normal distribution better than Liping's. And then, the K-S method is used to give the fitting deviation of our method and Liping's. The results are shown in Table 1.

Table 1. The comparison of K-S values between the scheme of ours and Liping's

Method	$G(20, 500)$	$G(100, 100)$	$G(500, 20)$	$G(1000, 10)$
Our scheme	0.00312	0.00311	0.00315	0.00309
Liping's scheme	0.0156	0.0181	0.0165	0.0158

From Table 1, it is intuitively found that the K-S value of our method is less than that of Liping's. From the description in section 2.2, it can be seen that the anomaly threshold of K-S method is 0.00435 when the confidence level α is 0.05. From the data shown in Table 1, it is noted that Liping's scheme will be judged abnormal by the K-S method, but our method will be not. That is to say, our method has better undetectable ability than Liping's method. The reason is that the new length inserted into the carrier of Liping's method will leads to abnormal traffic but our method fits the carrier traffic itself instead of inserting new length to the carrier. Thus, the statistical distribution of our method is closer to that of the normal Skype traffic. At the same time, from the results shown in Fig.5 and Table 1, it can be seen that the encoding window size makes no difference to the CDF of SkyLen traffic. Therefore, it has been proved the proposed method has a flexible utility of delivering various sizes of secret messages without affecting its performance.

5. **Conclusions.** In this paper, a Skype-based length covert channel which is named as SkyLen has been proposed. In order to imitate the high-order statistical feature of the normal Skype traffic, we construct the statistical model of Skype traffic by utilizing Parzen

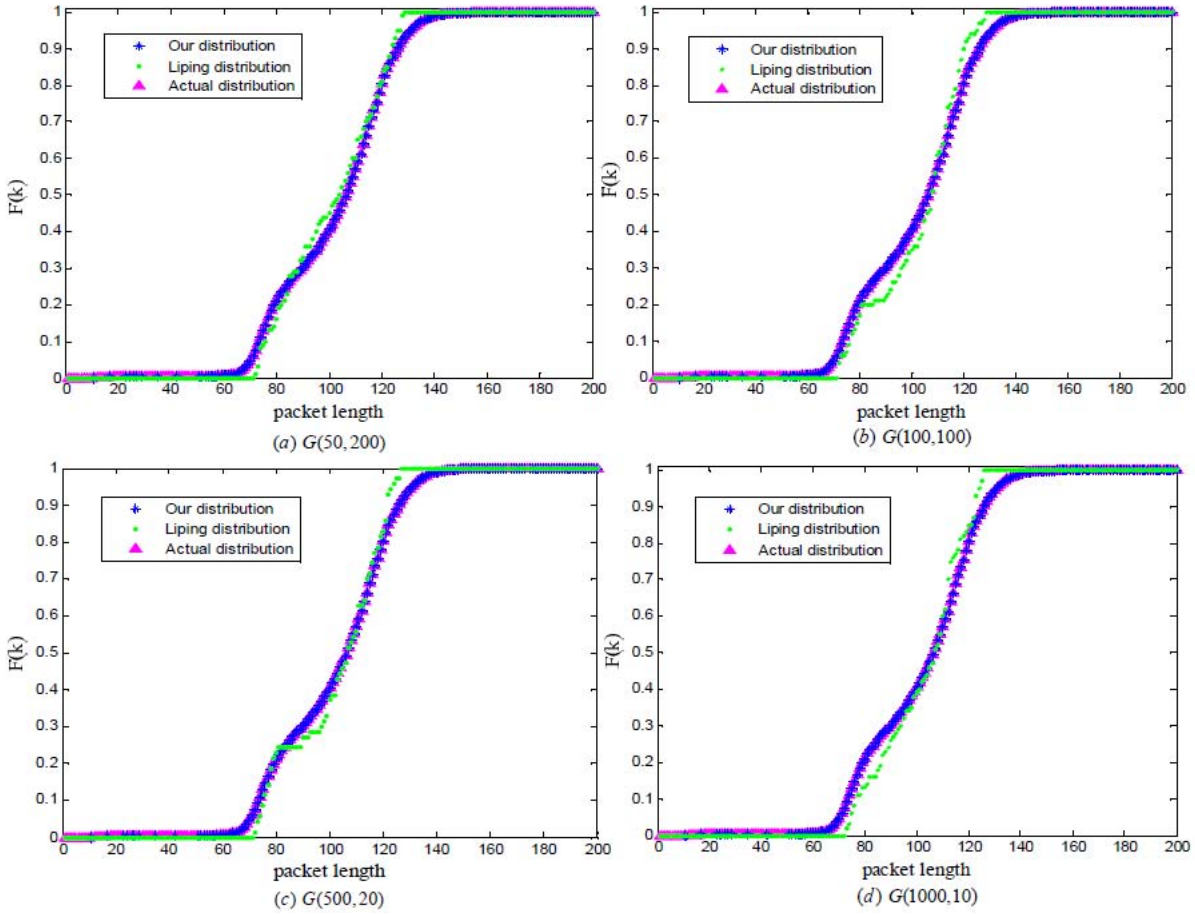

FIGURE 5. The comparison of CDF between the actual and SkyLen covert traffic in respect of different encoding window sizes

Kernel Estimation. Further, the Monte Carlo sampling technique is employed to preserve the normal CDF during the embedding process of the secret information. Experimental results show that the CDF of the covert traffic generated by the SkyLen is quite similar to that of the normal one. Hence, SkyLen is superior to the previous length-based methods in this respect and it is a suitable approach to communicate covertly and securely.

Acknowledgment. The authors are grateful to the anonymous reviewers for their insights and fruitful comments during the reviewing process, which greatly contributed to improving the quality of the original manuscript.

This work is supported by the NSF of China (Grant No.: 61170250, 61472188) and the project of college advantage subject construction of Jiangsu province.

REFERENCES

[1] W. Mazurczyk and K. Szczypiorski, Evaluation of steganographic methods for oversized IP packets, *Telecommunications Systems*, vol.49, no. 2, pp.207-217, 2012.

[2] J. Gimbi, D. Johnson, P. Lutz and B. Yuan, A Covert Channel Over Transport Layer Source Ports, July, 2012, http://hdl.handle.net/1850/15924.

[3] J. Zhai, G. Liu and Y. Dai. An Improved Retransmission-based Network Steganography: Design and Detection, *Journal of Networks*, vol. 8, no.1, pp.182-188, 2013.

[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, MitreCorporation, 1978, http://stinet. Dtiemi/cgibi/GetTR.Doc.

[5] R. Archibald and D. Ghosal, A Covert Timing Channel Based on Fountain Codes, *Proc. of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* , pp. 970-977, 2012.

[6] P. Dong, H. Qian, Z. Lu and S. Lan, A Network Covert Channel Based on Packet Classification, *International Journal of Network Security*, vol. 14, no. 1, pp. 147-154, 2012.

[7] T. Callahan, M. Allman and M. Rabinovich, Pssst, over here: Communicating without fixed infrastructure, *Proc. of IEEE INFOCOM* , pp. 2841-2845, 2012.

[8] L.X. Yang and X.F. Yang, The spread of computer viruses under the influence of removable storage devices, *Applied Mathematics and Computation*, vol. 219, no. 8, pp. 3914-3922, 2012.

[9] C.G. Girling. Covert channels in LAN's, *IEEE Trans. on Software Engineering*, vol. 13, no. 2, pp. 292-296, 1987.

[10] Q. Yao and P. Zhang, Coverting channel based on packet length, *Computer Engineering*, vol. 34, no.3 , pp. 183-185, 2008.

[11] L. Ji, W. Jiang, B. Dai and X. Niu, A Novel covert channel based on length of messages, *Proc. of International Symposium on Information Engineering and Electronic Commerce*, pp. 551-554, 2009.

[12] S. N. Omar and M. A. Ngadi, DNS request for normal minima length distribution based on reference matrix, *Proc. of International Conference on Information Engineering and Information Science*, pp. 248-258, 2011.

[13] A. S. Nair and A. Kumar, Length Based Network Steganography using UDP Protocol, Proc. of IEEE 3rd International Conference on Communication Software and Networks, pp. 726-730, 2011.

[14] W. Mazurczyk, M. Karas and K. Szczypiorski, SkyDe: a Skype-based Steganographic Method, *International Journal of Computers, Communications and Control*, vol. 8, no. 3, pp. 389-400, 2013.