Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **3**, May **2016**

A DWT-Based Covert Timing Channel of High Concealment

Ming-Qian Wang

School of Information Engineering
Changzhou Institute of Mechatronic Technology
No.26 Mingxin Road, Changzhou, Jiangsu, P.R.China
wmq1989219@126.com

Xian-Feng Liu and Wei-Jie Gu

School of Information Engineering
Changzhou Institute of Mechatronic Technology
No.26 Mingxin Road, Changzhou, Jiangsu, P.R.China
9755724@qq.com;gwjysu@163.com

Received September, 2015; revised February, 2016

Abstract. *Network covert channel exploits normal traffic as the carrier to transmit information secretly over the network. However, most of the existing covert timing channels can be detected since they may generate abnormal traffic or property. In this paper, a DWT-based covert timing channel is proposed to improve concealment. In order to preserve normal behavior and property, instead of being directly embedded into the normal traffic in spatial domain, the secret information is modulated into the wavelet coefficients of normal inter-packet delays (IPD). Experimental results show that our scheme can resist the existing popular detection methods.*
Keywords: Covert timing channel, Discrete wavelet transform, Information security

1. **Introduction.** Network covert channel is a hidden communication technique, which utilizes legitimate traffic as the vehicle to transfer secret information covertly over the network. In recent years, it has become a hot research topic in the field of information security. There are two broad types of network covert channel: covert storage channel and covert timing one. Covert storage channel embeds the secret information into the redundancies of network protocols [1, 2, 3, 4, 5]. Although it is simple and easy to implement, it can be easily detected by the existing methods.

Covert timing channel delivers the secret information by exploiting time-relevant events of network packets and it has better stealthiness than covert storage one. Generally, it can be divided into three sub-classes: On-Off covert channel [6], inter-packet delay (IPD) based covert channel [7, 8, 9, 10, 11], packet sorting [12, 13] and combination based ones [14, 15]. Synchronization is always a difficult problem to solve, since covert timing channel is susceptible to the unstable network condition, such as jitter and delay. To guarantee reliability, Luo [16] designed a mechanism by using TCP ACKs to synchronize the covert channel. Amir [17] and Archibald [18] used Error Correction Code to encode the secret information to increase accuracy, which sacrificed the bandwidth of covert channel and increase the transmission overhead.

Since IPD-based covert channel is one of the most common and effective method, it is mainly focused in this paper. However, most of the existing methods would either generate abnormal covert traffic or reveal distinct properties compared with the normal case, making it possible to be detected. This is because the embedding of secret information alters the normal carrier in some way. To overcome the drawbacks of the existing methods, a new Discrete Wavelet Transform (DWT) based covert timing channel is proposed in this paper, aiming to improve concealment. The main contribution of this paper is as follows:

(1) Instead of directly modifying the normal traffic in spatial domain, the secret information is modulated into the coefficients in wavelet domain. Via controlling the embedding position and strength, alteration of the normal carrier in spatial domain is reduced as possible. Thus, the covert traffic of our scheme preserves normal behavior and property, so as to resist detection.

(2) In our scheme, secret bits are embedded into the wavelet coefficients of normal traffic by using parity quantification. This is a quite simple way because the secret information can be decoded according to the parity of certain coefficients, without any additional template. Meanwhile, such method is noise-tolerated to some extent, making the proposed scheme more robust. The remainder of this paper is organized as follows. In section 2, some related works are reviewed in detail. In Section 3, the proposed scheme is introduced. In Section 4, experimental results are presented and analyzed. Finally, the whole paper is concluded in Section 5.

2. **Related work.**

2.1. **Review of IPD-based schemes.**

IPD-based covert channel is a notable branch of covert timing channel, which manipulates the timing intervals of adjacent network packets to transmit secret information. To achieve better understanding, four typical inter-packet delays based schemes are reviewed and analyzed, they are Jitterbug [11], TRCTC [13], MBCTC [14] and CTCDM [15] respectively.

Jitterbug [11] is a key board device that slowly leak typed information over network. It operates by deliberately inserting additional small delays into the original traffic. The sender transmits a bit 0 by adding certain delay to the original intervals such that the modified one module w milliseconds (ms) is 0. Similarly, a bit 1 is transmitted by increasing the original intervals to a value which module w ms is $w/2$. The timing window w limits the maximum delay that can be added, which determines the discrepancy between the legitimate and covert traffic. In our implementation, parameter w is set as 20 ms. Jitterbug modifies the normal traffic for information leaking without producing additional traffic, whereas the variation will cause anomaly.

To mitigate this problem, designers try to mimic the statistical feature of normal traffic. TRCTC [13] uses a sample of normal traffic captured from the overt network, and replays it later to transfer secret. The normal inter-packet delays are sorted and partitioned into two equal bins, with a value t_{cutoff} to distinguish them. Then the sender randomly picks up a value from the corresponding bin that matches the secret bit 1 or 0. Since the covert traffic of TRCTC is composed of scrambled normal inter-packet delays, its distribution is close to that of the normal one. However, the scrambled traffic may also raise suspicion of monitoring device.

MBCTC [14] provided an automated framework that fits the statistical model of normal traffic using parametric estimation, where the candidate distributions are Exponential, Weibull, Poisson and other common ones. The estimated distribution with the smallest root mean squared error (RMSE) is the best fit of normal traffic. To imitate the normal

distribution, covert traffic is generated using the inverse cumulative distribution function (ICDF) of normal traffic. In addition, the model is refitted to update its parameters every 100 packets. However, it should be noted that mathematical model of some network application may not exist, thus MBCTC is not applicable in some scenarios.

Similar to MBCTC, CTCDM [15] fits the histogram distribution property of normal traffic. The fitted histogram is utilized in the encoding of secret information, in order to make the distribution of covert traffic more natural and similar to the normal one. CTCDM is designed as an binary channel, where bit 0 is decoded when the observed timing interval is smaller than the center value $\alpha^\star$ of the histogram, otherwise a bit 1 is retrieved. However, the normal pattern of transmission is also overlooked in this scheme. Hence, we are motivated to design a method that make less modification on the normal traffic as possible when embedding the secret information. In this paper, a DWT-based covert timing channel is proposed by embedding the secret bits into the coefficients in wavelet domain, minimizing the alteration of normal traffic in spatial domain.

2.2. **A brief introduction of DWT.** The Wavelet Transform (WT) is a technique for analyzing signals. It outperforms other transforms due to its excellent time and frequency resolution properties. The multi-scale analysis of signals is conducted by expansion and translation operations. WT is self-adaptive to the requirement of time-frequency analysis for signals, which can focus on any detail of signals. Discrete wavelet transform (DWT) is a special case of WT that processes discrete signals. Thus, DWT is chosen in this paper. DWT of a signal x is calculated by passing it through a low pass filter h and a high pass filter g, which is denoted by Eq.(1) and Eq.(2):

$$y_{low}[n] = \sum_{k=-\infty}^{\infty} x[k]h[2n-k] = (x * h) \downarrow 2 \tag{1}$$

$$y_{high}[n] = \sum_{k=-\infty}^{\infty} x[k]g[2n-k] = (x * g) \downarrow 2 \tag{2}$$

Where the approximation coefficients y_{low} and detail coefficients y_{high} are the outputs of low pass (h) and high pass (g) filters respectively, after sub-sampling by 2. The above processes can also be represented in the form of convolution, as shown in Eq.(1) and (2). This decomposition has halved the time resolution since only half of each filter output characterizes the signal. The one-level wavelet decomposition of signal x is depicted in Fig.1. The signal can be analyzed at different frequency bands with different resolution by further decomposing the approximation coefficients using the same step.

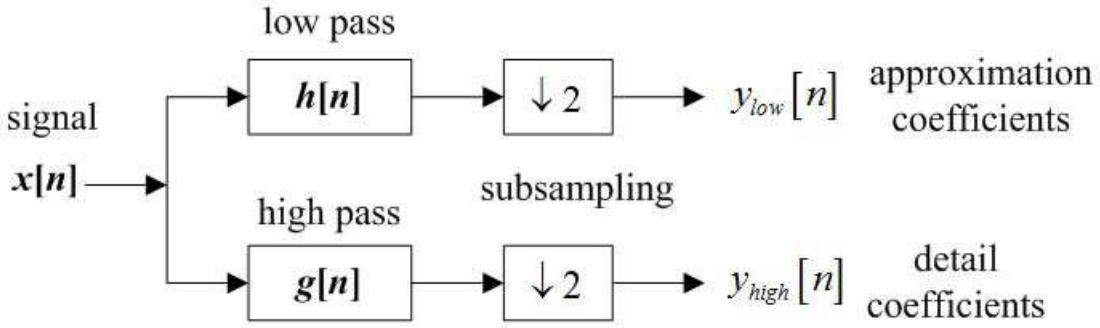

FIGURE 1. Wavelet decomposition of signal x

3. **The proposed scheme.** The model of our scheme is demonstrated in Fig.2. Initially, a sample of normal traffic is collected, and the delays of adjacent packets are extracted. Then, the normal IPDs are divided into several segments for processing. Let ΔT be one of the segments and l be the size of it, where $\Delta T = \{\Delta t_1, \Delta t_2, \cdots, \Delta t_l\}$. The secret information S_e in binary form is encoded by the following procedures:

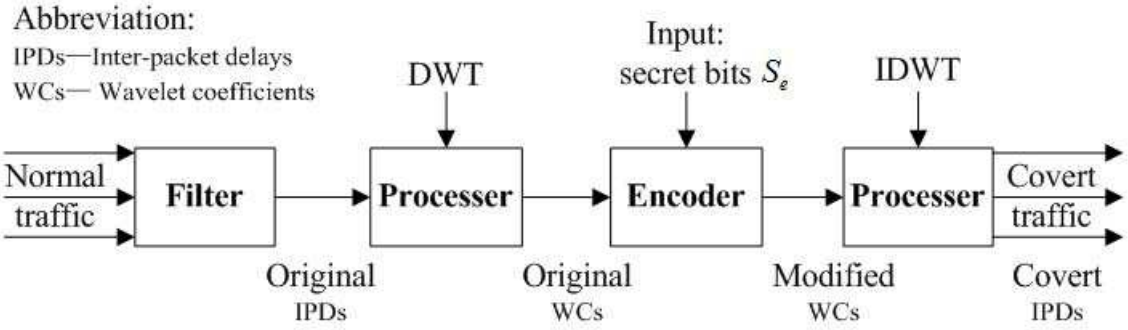

FIGURE 2. The model of our proposed covert channel

Step I: three-level wavelet decomposition is performed on the normal traffic ΔT according to Eq.(1) and Eq.(2) as illustrated in subsection 2.2. The result can be denoted as Eq.(3), where $ca3$ represents the approximation coefficients of third-level wavelet decomposition, and it is defined as $ca3 = \{ca3(1), ca3(2), \cdots, ca3(n)\}(n = l/2^3)$; $cd1$,$cd2$ and $cd3$ are the corresponding detail coefficients.

$$ca3 \oplus cd3 \oplus cd2 \oplus cd1 = DWT3(\Delta T) \tag{3}$$

For better understanding, DWT of the normal traffic is presented in Fig.3 as an example. In this case, YY-audio is selected as the normal carrier and the segment size l is set to 500. It is intuitive that $ca3$ are larger than the coefficients of other frequencies. Hence, it can be found that the energy of normal traffic is mainly concentrated on the low-frequency area, which is chosen as the embedding area.

Step II: the secret information S_e is partitioned into several bit-strings which size is indicated as m $(m \leq n)$, and s_e represents a secret bit. Then, parity quantification is employed to modulate the secret bit s_e into the approximation coefficient $ca3$, which is defined in Eq.(4):

$$ca3'(i) = f_{encode}(s_e) = \begin{cases} [ca3(i)] & [ca3(i)]\%2 = s_e \\ [ca3(i)] + (-1)^m & [ca3(i)]\%2 = s_e \end{cases} \quad (1 \leq i \leq m) \tag{4}$$

Where f_{encode} denotes the encoding function, and $ca3'$ refers to the modified approximation coefficients after injecting the secret bits. $[ca3(i)]$ indicates the half-adjust operation on $ca3(i)$. Additionally, the variable m is set to 1 if $ca3(i)$ is less than $[ca3(i)]$, otherwise it is set to 0.

Step III: inverse DWT is conducted on the modified coefficients to reconstruct the covert traffic ΔT_s, which can be represented as:

$$\Delta T_s = IDWT3(ca3' \oplus cd3 \oplus cd2 \oplus cd1) \tag{5}$$

On the receiver side, it is quite simple to extract the secret bits without any additional template shared in advance. Inter-packet delays ΔT_r are extracted according to the timestamp of packets. It should be noted that ΔT_r may not be equivalent to ΔT_s, since the impact of network noise is taken into account. The secret bit can be retrieved by using

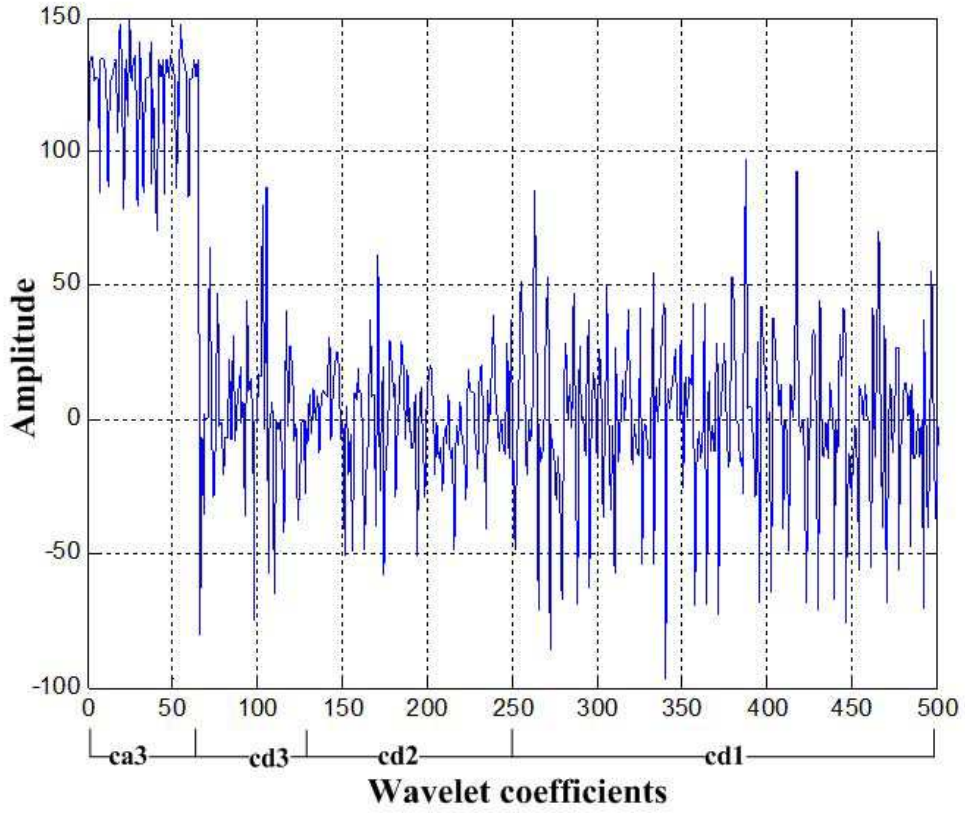

FIGURE 3. Three-level DWT of the original traffic

the decoding function f_{decode}, as shown in Eq.(6). Where $c\hat{a}3$ refers to the corresponding approximation coefficient of covert traffic.

$$\hat{s}_e = f_{decode}(c\hat{a}3) = [c\hat{a}3(i)]\%2(1 \leq i \leq m) \tag{6}$$

A bit 0 is decoded when $c\hat{a}3$ module 2 equals 0, or a bit 1 is recovered if $c\hat{a}3$ module 2 is identical to 1.

4. **Experimental results.** The proposed scheme is protocol-independent, which means that any network application can be used as its carrier. Therefore, it is widely applicable in different scenarios. As we know, an ideal carrier should possess two properties: popularity and complexity. Since the massive communication traffic and complex pattern of such carrier can improve the concealment of covert channel. YY audio a network service based on P2P, do satisfy the above requirement, therefore it is adopted as the normal carrier in the implementation of this paper.

In our experiment, the normal traffic of YY audio is captured from an intermediate router within the campus network of Jiangsu university of science and technology during the communication of two hosts. Then the secret information is inserted into such carrier using the aforementioned steps. The normal and covert traffic of our scheme after three-level wavelet decomposition are compared in Fig.4. Meanwhile, the comparison of normal and covert traffic in spatial domain is also presented in Fig.5. It is manifest that the covert traffic of our scheme is quite similar to the normal one whenever in spatial or wavelet domain.

To further evaluate the performance of our proposed scheme, it is compared with two existing methods jitterbug [11] and ctcdm [15] regarding some significant properties, such

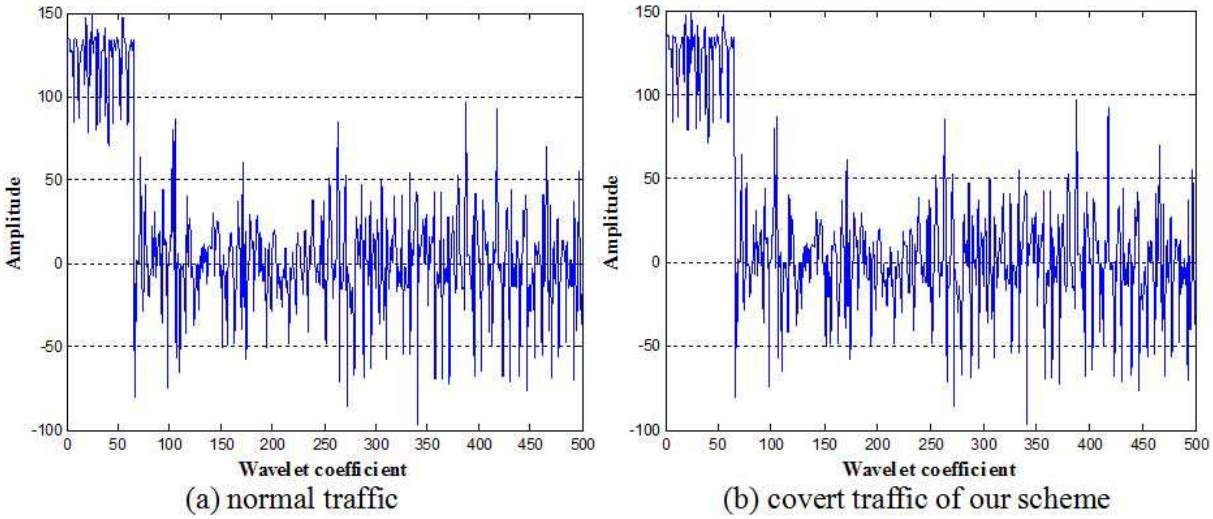

FIGURE 4. The comparison between normal and covert traffic of our scheme in Wavelet domain

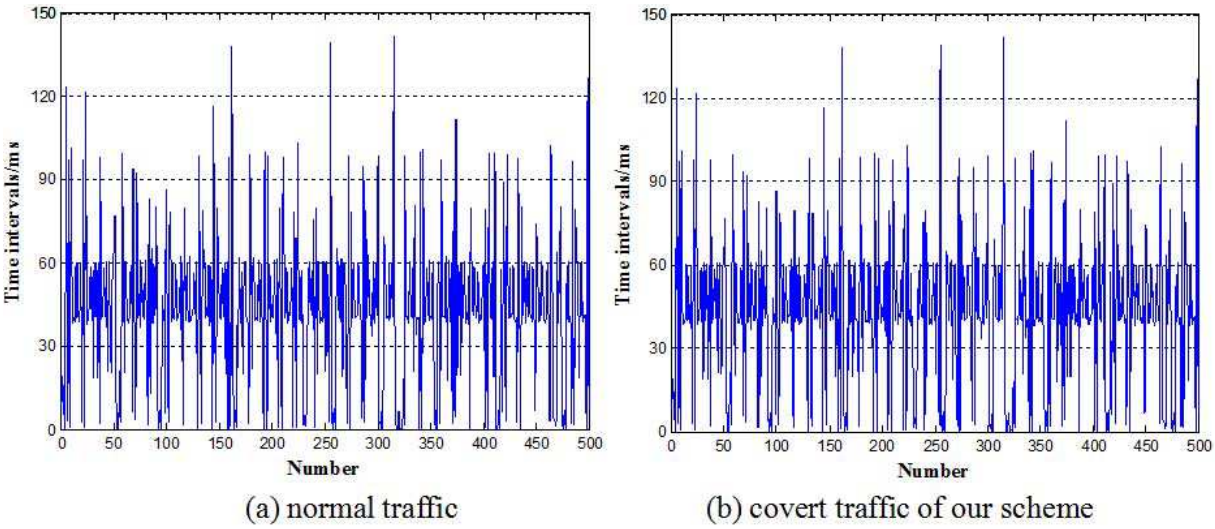

FIGURE 5. The comparison between normal and covert traffic of our scheme in spatial domain

as concealment and robustness. The whole size of normal or covert traffic is 10000 in the following experiment.

4.1. **Robustness analysis.** Most timing covert channel is easily affected by network noise, such as jitter and delay. In the experiment, noises of different power are injected into the covert traffic of our scheme. The additive white Gaussian noise is utilized to simulate channel noise in our case. The power of noise is measured by signal-to-noise ratio (SNR) when the power of signal is fixed. In other words, the power of noise increases as SNR decreases. The comparison of bit error rate (BER) between our scheme and jitterbug is demonstrated in Fig.6, given different SNR ranging from 0 to 70db. From the result, it can be seen that distortion raised by such noise can be tolerated in our scheme when the SNR is larger than 40db. And it achieves relatively well accuracy when the SNR is above 30db. As for jitterbug, its BER is larger than that of our scheme when the SNR locates under 50db. However, it becomes totally disabled as the SNR decreases to 35db.

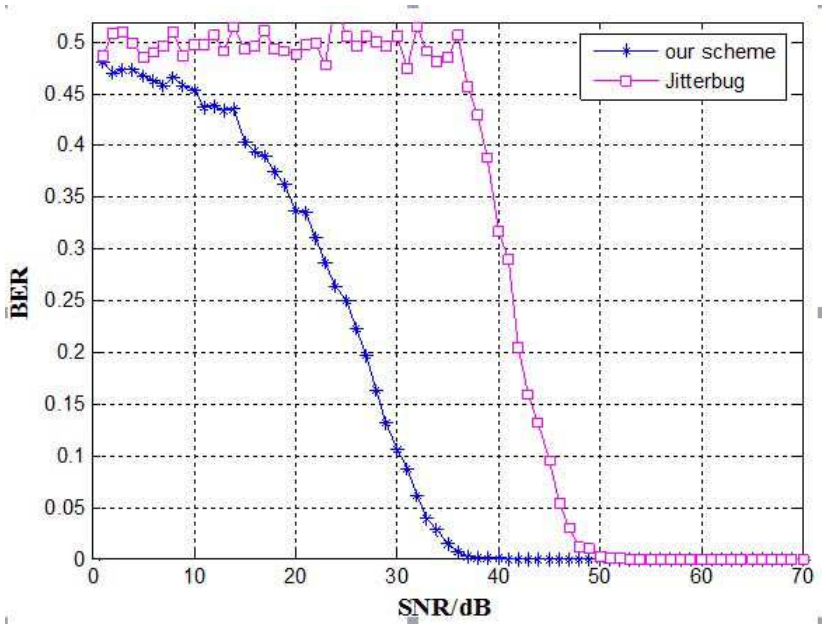

FIGURE 6. The comparison of BER between our scheme and Jitterbug under different SNR

Thus, it is indicated that our proposed scheme is robust when the power of noise is less than of the signal, which outperforms jitterbug in terms of robustness.

4.2. **Concealment analysis.** As we know, histogram is a significant property which can reveal the statistical distribution feature of traffic. Therefore, the histograms of normal and covert traffic are compared in Fig.7. Where the x-axis shows inter-packet delays ranging from 0 to 150ms and the y-axis indicates the number of delays occurred within each bin (the x-axis is divided into ten bins). It is easily found that, inter-packet delays of normal traffic occur most between 15 and 60ms. But for jitterbug it turns out to be a distinct distribution deviated from the normal one. It can also be noted that the distribution of ctcdm only differs slightly from the normal case when between 75 and 105ms, since ctcdm aims to imitate the normal histogram property. Hence, the histogram of our scheme matches the normal one better than jitter or ctcdm.

Meanwhile, two notable detection methods are employed to reckon the detection resistance of our scheme compared with jitterbug [11] and ctcdm [15] quantitatively, which are ϵ-similarity test [6] and Kolmogorov-Smirnov test [19]. Each method tries to find abnormal property or regularity of covert traffic.

The normal traffic obtained from an intermediate router is used for training in the detection tests. Then the covert traffic is detected when the window size is 500 or 1000 respectively. In addition, the number of training or detection window is 100 in each case. For each test, detection rate of covert traffic is calculated under different thresholds, when the false positive rate is less than 0.1.

(1)ϵ-similarity test

ϵ-similarity test [6] reckons the self-similarity within certain traffic. Firstly, for each window, the IPDs are sorted from smallest to largest, as shown in Fig.8. The x-axis is the packet number, and the y-axis represents the IPDs which vary from 0 to 150ms. It can be seen that the sorting result of normal traffic is a step function varying slowly with about six smooth steps, and so is that of our scheme. The shape of ctcdm resembles the normal case, but its steps are jagged. For Jitterbug, there are more sharp steps.

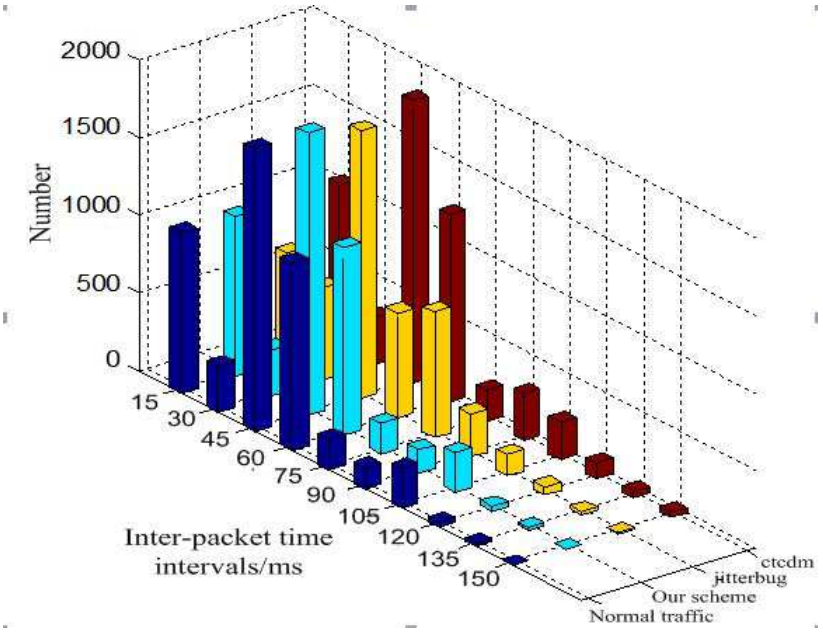

FIGURE 7. The comparison of histogram between normal and covert traffic

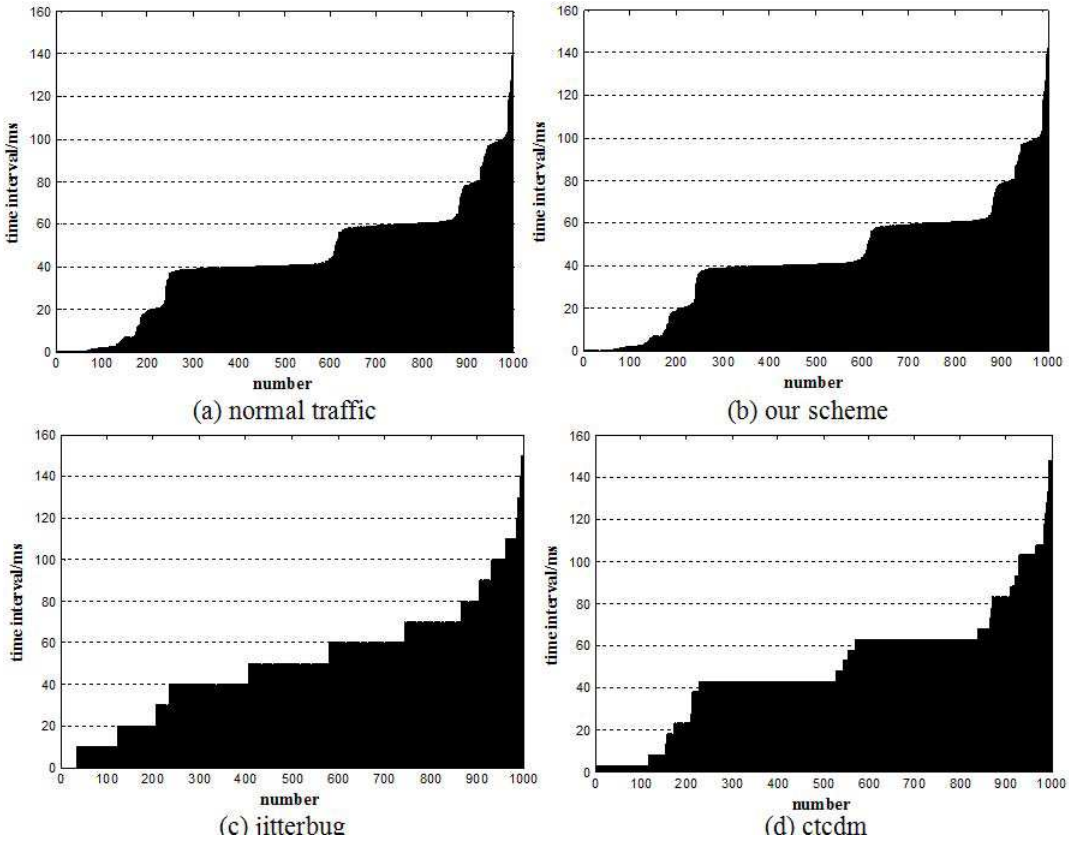

FIGURE 8. The sorting results of normal and covert traffic

Secondly, the relative difference between each pair of consecutive points is calculated as $|P_i - P_{i+1}|/P_i(i=1,..., w)$, where w refers to the window size. Finally, a measure of similarity called ϵ-similarity is obtained by computing the percentage of relative differences that are less than ϵ. The ϵ-similarity values of normal and covert traffic under different

ϵ are given in Tab.1. As ϵ varies from 0.01 to 0.02, the ϵ-similarity value rises because more relative differences fall into the region. For a single window, the ϵ-similarity value of our scheme ranges from 0.8448 to 0.9029, which is quite close to that of the normal case. However, such value of jitterbug or ctcdm is all above 0.95 for each ϵ.

TABLE 1. The ϵ-similarity values of normal and covert traffic under different ϵ

ϵ	0.010	0.012	0.014	0.016	0.018	0.020
normal	0.8488	0.8609	0.8799	0.8959	0.9039	0.9099
our scheme	0.8448	0.8559	0.8699	0.8849	0.8949	0.9029
jitterbug	0.9510	0.9510	0.9510	0.9510	0.9510	0.9510
ctcdm	0.9750	0.9750	0.9750	0.9750	0.9750	0.9750

By utilizing the steps mentioned above, the ϵ-similarity values of 100 windows for normal and covert traffic are compared in Fig. 9, when ϵ is set to 0.01. From the results, it is found that the ϵ-similarity value slightly increases as the window size becomes larger, because the traffic turns to be more regular. Most similarity values of normal traffic appear under 0.9, whereas those of the covert traffic generated by ctcdm concentrate on 0.95 or 0.97. For jitterbug, the values range approximately from 0.9 to 0.97. But the values of our scheme mix with those of the normal traffic, which can hardly be differentiated.

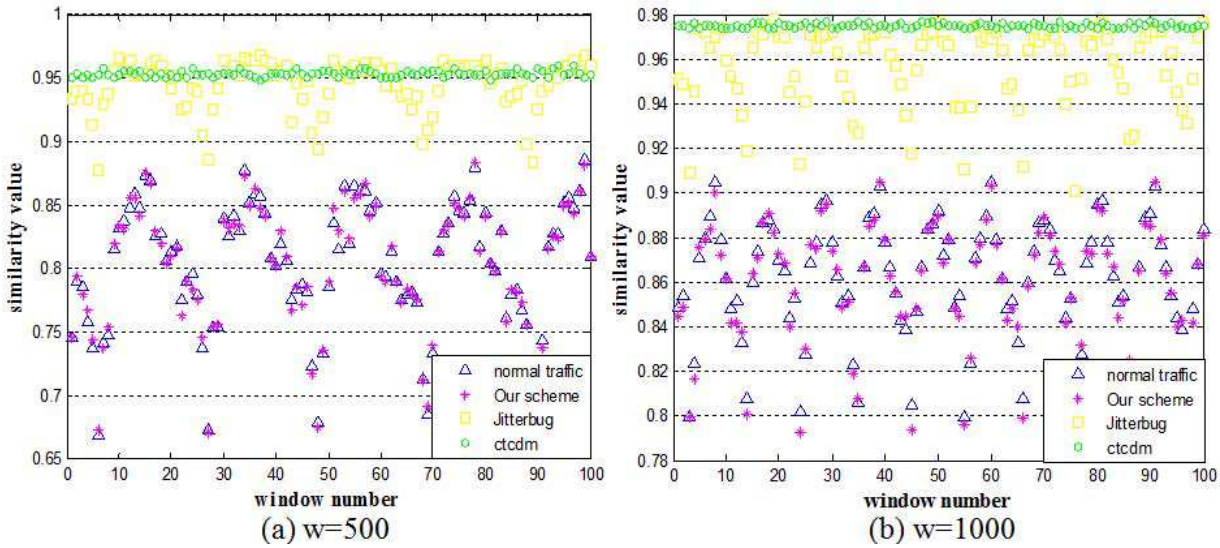

FIGURE 9. The comparison of similarity values between normal and covert traffic (ϵ=0.01)

100 windows of covert traffic are tested using ϵ-similarity test when the window size w is 500 or 1000 respectively, and the results are presented in Tab.2. Where the detection threshold is denoted as t. It is observed that the false positive rate of normal traffic declines when the threshold increases. Meanwhile, the detection rates of covert traffic are shown in the table, and we can see covert traffic of ctcdm is completely detected. The detection rate of jitterbug ranges from 0.94 to 1, while that of our scheme is only from 0.02 to 0.04. Hence, ϵ-similarity test fails to distinguish the covert traffic of our scheme from the normal one.

(2)Kolmogorov-Smirnov test

TABLE 2. The detection results of covert traffic using ϵ-similarity test under different thresholds and window sizes (ϵ=0.01)

	t=0.895		t=0.900		t=0.905	
	w=500	w=1000	w=500	w=1000	w=500	w=1000
false positive	0.01	0.06	0.01	0.04	0.00	0.00
our scheme	0.02	0.04	0.00	0.03	0.00	0.00
jitterbug	0.99	1.00	0.98	1.00	0.94	0.99
ctcdm	1.00	1.00	1.00	1.00	1.00	1.00

Kolmogorov-Smirnov test [19] measures the maximum distance between two distributions. A small value indicates that two distributions are close to each other. Conversely, a large value means one distribution does not fit the other one. The Kolmogorov-Smirnov test value (KS-test value) is attained by taking the supremum of absolute difference between two empirical distribution functions for all x, which can be defined in Eq.(7):

$$KSTEST = sup|S_1(x) - S_2(x)| \tag{7}$$

Where $S_1(x)$ and $S_2(x)$ refer to the empirical distribution functions of two samples. The comparison of KS-test values between the normal and covert traffic is shown in Fig.10. Likewise, 100 windows of covert traffic are tested in the experiment. The x-axis is the window number and y-axis shows the corresponding KS-test value. It can be found that, KS-test value drops as window size increases, since the traffic becomes more stable and regular. The KS-test values of our scheme are under 0.15, confused with those of the normal traffic. Thus, the distribution of our scheme is close to that of the normal one. Nevertheless, the corresponding values of jitterbug and ctcdm occur from 0.15 to 0.3 and 0.35 to 0.45 respectively, which are both deviated from the normal case.

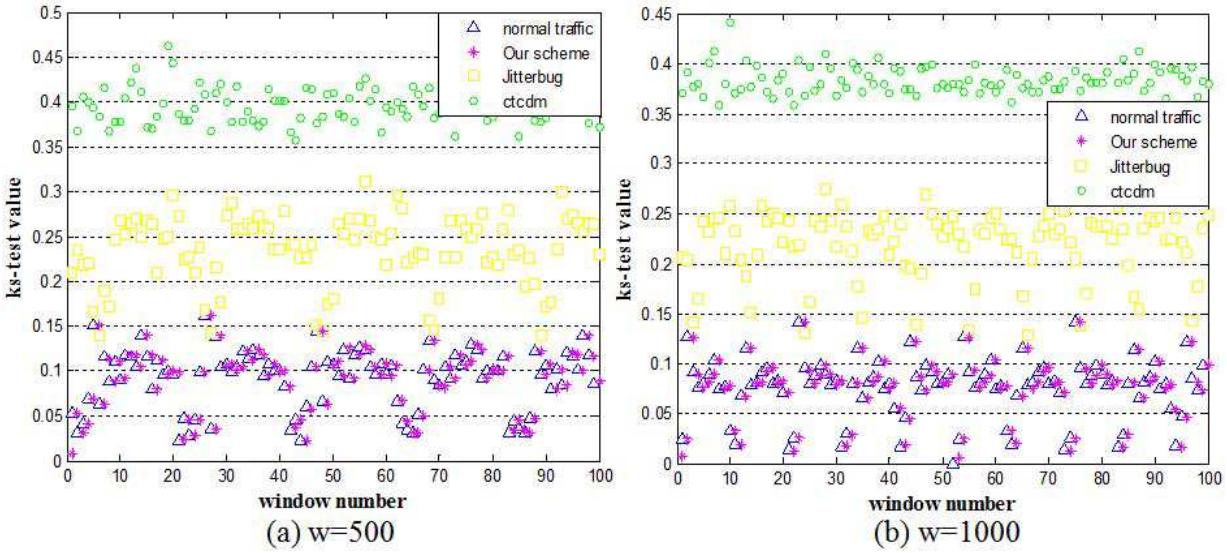

FIGURE 10. The comparison of KS-test values between normal and covert traffic

Then, 100 windows of covert traffic are detected using Kolmogorov-Smirnov test and the detection results are shown in Tab. 3. It is observed that the false positive rate of the normal traffic declines when the threshold increases. From the results, it is easily seen that covert traffic of ctcdm can be detected thoroughly by this method. The detection rate of Jitterbug is more than 0.9 when tested with different thresholds. But in our case it

is located under 0.06, indicating that Kolmogorov-Smirnov test cannot effectively detect the covert traffic generated by our scheme.

TABLE 3. The detection results of covert traffic using K-S test under different thresholds and window sizes

	t=0.13		t=0.14		t=0.15	
	w=500	w=1000	w=500	w=1000	w=500	w=1000
false positive	0.08	0.04	0.03	0.02	0.02	0.00
our scheme	0.06	0.03	0.02	0.01	0.02	0.00
jitterbug	1.00	0.99	0.98	0.95	0.95	0.92
ctcdm	1.00	1.00	1.00	1.00	1.00	1.00

From the above results, it is manifest that both of jitter [11] and ctcdm [15] can be detected by existing methods [6, 19]. Since the behavior or property of normal carrier is altered in their encoding process. But our scheme is superior to the current methods in detection resistance, because the normal traffic in wavelet domain is modified to embed the secret information, preserving its spatial regularity and property. Therefore, it can be concluded that our scheme possesses better concealment and robustness.

5. **Conclusions and future work.** In this paper, a DWT-based covert timing channel of high concealment is proposed. The legitimate traffic is exploited as a sample to maintain the normal regularity and behavior. For the normal sample, approximation coefficients of the third-level wavelet decomposition are modulated to deliver the secret information by using parity quantification. The reconstructed covert traffic is able to keep the normal spatial property. From the experimental result, it is indicated that the covert traffic of our scheme is quite close to the normal one, which can successfully evade detection. Hence, the proposed scheme outperforms the existing methods in terms of detection resistance.

In the future, the robustness of our scheme will be further studied and improved. Specifically, conditions of packet loss and disorder will be considered.

Acknowledgment. This work is supported by the NSF of China (Grant No.: 61170250) and NSF of Jiangsu Province (Grant No.:BK20150472).

The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

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

[2] 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. 1841–1847, 2013.

[3] R. Rios, J. A. Onieva, and J. Lopez, HIDE DHCP: Covert Communications Through Network Configuration Messages, *Proc. of 27th Information Security and Privacy Conference*, pp. 162-173, 2012.

[4] 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.

[5] W. Mazurczyk, and K. Szczypiorski, Evaluation of steganographic methods for oversized IP packets, *Telecommunications Systems*, vol. 49, no. 2, pp.210-217, 2012.

[6] S. Cabuk, C. Brodley, and C. Shields, IP covert timing channels: Design and detection, *Proc. of the 2004 ACM Conference on Computer and Communications Security*, pp. 55-74, 2004.

[7] G. Shah, A. Molina, and M. Blaze, Keyboards and covert channels, *Proc. of the 2006 USENIX Security Symposium*, pp. 59-75, 2006.

[8] X. Zi, L. Yao, and L. Pan, Implementing a passive network covert timing channel, *Computers and Security*, vol.29, no.6, pp.686C696, 2010.
[9] S. Cabuk, *Network Covert Channels: Design, Analysis, Detection and Elimination*, Ph.D. Thesis, Purdue University, USA, 2006.
[10] S. Gianvecchio, H. Wang, and D. Wijesekera, Model-Based Covert Timing Channels: Automated Modeling and Evasion, *Lecture Notes In Computer Science*, no.5230, pp. 211-230, 2008.
[11] G. J. Liu, J. T Zhai, Y. W Dai, Covert Timing Channel with Distribution Matching, *Proc. of International Conference on Multimedia Information Networking and Security*, pp. 565-568, 2009.
[12] A. Galatenko, A. Grusho, and A. Kniazev, Statistical Covert Channels Through PROXY Server, *Proc. of 3rd International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security*, pp.424C29, 2005.
[13] A. El-Atawy, and E. Al-Shaer, Building Covert Channels over the Packet Reordering Phenomenon, *Proc. of IEEE INFOCOM*, pp.2186-2194, 2009.
[14] X. Luo, E. Chan, and R. Chang, Cloak: A Ten-Fold Way for Reliable Covert Communications, *Proc. of. European Symposium Research in Computer Security*, 2007.
[15] X. Luo, W. W. Edmon, and P. Zhou, Robust Network Covert Communications Based on TCP and Enumerative Combinations, *IEEE Transaction on Dependable and Secure Computing*, vol.9, no.6, pp. 890-902, 2012.
[16] X. Luo, E. Chan, and R. Chang, TCP covert timing channels: Design and detection, *Proc. of IEEE International Conference on Dependable Systems and Networks With FTCS and DCC*, pp.420-429, 2008.
[17] A. Houmansadr, and N. Borisov, CoCo: coding-based covert timing channels for network flows, *Proc. of 13th International Conference on Information Hiding*, pp. 314-328, 2011.
[18] R. Archibald, and D. Ghosal, A Covert Timing Channel Based on Fountain Codes, *Proc. of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp.970-977, 2012.
[19] P. Peng, P. Ning, and D. Reeves, On the Secrecy of Timing-Based Active Watermarking Trace-Back Techniques, *Proc. of IEEE Symposium on Security and Privacy*, 2006.