Designing Rich-Secure Network Covert Timing Channels Based on Nested Lattices

Weiwei Liu[1*], Guangjie Liu[1], Xiaopeng Ji[1], Jiangtao Zhai[2] and Yuewei Dai[1,2]
[1] School of Automation, Nanjing University of Science and Technology
Nanjing, Jiangsu 210094 - P.R.China
[e-mail: lwwnjust@njust.edu.cn, gjieliu@njust.edu.cn, jixiaopeng@njust.edu.cn]
[2] School of Electrical and Computer Engineering, Jiangsu University of Science and Technology
Zhenjiang, Jiangsu 212003 - P.R.China
[e-mail: jiangtaozhai@gmail.com, dywjust@163.com]
*Corresponding author: Weiwei Liu

Received January 12, 2018; revised October 27, 2018; accepted November 21, 2018;
published April 30, 2019

Abstract

As the youngest branch of information hiding, network covert timing channels conceal the existence of secret messages by manipulating the timing information of the overt traffic. The popular model-based framework for constructing covert timing channels always utilizes cumulative distribution function (CDF) of the inter-packet delays (IPDs) to modulate secret messages, whereas discards high-order statistics of the IPDs completely. The consequence is the vulnerability to high-order statistical tests, e.g., entropy test. In this study, a rich security model of covert timing channels is established based on IPD chains, which can be used to measure the distortion of multi-order timing statistics of a covert timing channel. To achieve rich security, we propose two types of covert timing channels based on nested lattices. The CDF of the IPDs is used to construct dot-lattice and interval-lattice for quantization, which can ensure the cell density of the lattice consistent with the joint distribution of the IPDs. Furthermore, compensative quantization and guard band strategy are employed to eliminate the regularity and enhance the robustness, respectively. Experimental results on real traffic show that the proposed schemes are rich-secure, and robust to channel interference, whereas some state-of-the-art covert timing channels cannot evade detection under the rich security model.

Keywords: Covert timing channel, inter-packet delays, rich security model, nested lattice, undetectability.

This work was supported by The National Natural Science Foundation of China(Grant No. 61602247, 61702235, U1536104, U1636117, 61472188), Natural Science Foundation of Jiangsu Province(Grant No. BK20160840, BK20150472), National Key Technology Research and Development Program of the Ministry of Science and Technology of China(Grant No. 2014BAH41B01), Fundamental Research Funds for the Central Universities (30920140121006, 30915012208).

http://doi.org/10.3837/tiis.2019.04.007 **ISSN : 1976-7277**

1. Introduction

Network covert timing channel is a timing channel that transfers covert information over a network [1], it conceals the very existence of secret messages by hiding them in open overt communication channels [2]. As the youngest branch of information hiding, covert timing channels have no limit on the amount of cover information, and allow for covert information to be transmitted over long periods of time when compared to information hiding in media files [3]. Thus, finding the starting and ending times of the covert timing channel are difficult and further detection is more challenging. Network covert timing channels can be carried out by adjusting the transmission rate or manipulating the inter-packet delays (IPDs) [4-6]. The secret messages are modulated into the timing information of overt traffic, predominantly into the IPDs. Advances in the coding theory and high-speed networks have spurred interest in the development of various types of covert timing channels.

As the goal of network covert timing channel is to transmit information between the sender and receiver without being detected by the warden, the fundamental design principle is to alter the characteristics of IPDs as slightly as possible while preventing the channel disruptions, such as timing perturbation or packet loss. Undetectability and robustness are two main performance metrics of covert timing channels. The undetectability means that the warden cannot distinguish between legitimate and covert traffic using statistical detection tools such as Kolmogorov-Smirnov (K-S) test [7], Kullback-Leibler divergence (KLD) test [8], and entropy test [9]. Robustness refers to the ability of the covert timing channel to cope with the network jitter inherent in the communication channels.

IPDs have been regarded as the common carriers of network covert timing channels as they are basic units of traffic timing information. Earlier IPD-based scheme modulates the secret message by adding different delays to each IPD according to the secret message bits [10], which results in the significant degradation of normal communication. Later, the distribution of IPDs of cover traffic is considered in the design of covert timing channels [11, 12]. A model-based covert timing channel is proposed to mimic the statistical properties of legitimate traffic, which modulates the secret message based on the empirical cumulative distribution function (CDF) of the IPDs of the cover traffic [12]. It is regarded model-secure though the security model is very rough. To consider robustness in the design of covert timing channels, many studies have employed various types of coding schemes to improve the robustness of covert timing channels. In [13, 14], spreading codes are used to strengthen the robustness of the covert timing channel with the assumption that IPDs are independent and identically distributed (*i.i.d.*). Later on, different error-correcting codes are used incorporated with model-based modulation in CoC [15], and Fountain codes are used to generate encoded symbols continuously until the receiver sucessfully demodulates the secret message [16]. Furthermore, trellis-based adaptive modulation [17] and analog fountain timing channels [6] are proposed to achieve the tradeoff between robustness and undetectability.

Model-based covert timing channels typically consider *i.i.d.* IPDs. Nevertheless, IPDs of most real traffic are not *i.i.d.* which makes the covert timing channel vulnerable to regularity or entropy test. To avoid detection based on regularity, Mimic scheme is proposed to learn about shape and regularity properties to resist regularity test [18]. Liquid scheme is proposed to smooth out the shape distortion to resist entropy test [19]. However, the modeling parameters need to be shared frequently and they can only realize model-fitting within limited order.

The main motivation of this study can be described as follows: In the design of existing covert timing channels, undetectability is usually studied based on the security model established from one-order statistics of IPDs (e.g., cumulative distribution function or probability distribution function), whereas high-order statistics of IPDs are always discarded completely. In actual fact, this inchoate security model works under the assumption that the IPDs of network traffic are *i.i.d.*. Meeting the goal of undetectability still remains challenging, as the multi-order statistics of the IPDs of cover traffic cannot be retained after modulation. To design secure covert timing channels under a more general security criterion, we discuss a novel security model that exploits the correlation of IPDs, and study the message modulation methods under this model.

In this study, we first construct a rich security model of covert timing channel based on IPD chains, which can be used to measure the multi-order statistical distortion of IPDs. To achieve undetectability under the rich security model, we then propose two rich-secure covert timing channel schemes based on nested lattices. The dot-lattice and interval-lattice are constructed to quantize the secret messages, respectively. We also employ compensative quantization and guard band strategy to enhance the quantization performance. At the sender, the secret message bits are first encoded into *Q*-ary symbols. Then, the empirical CDF of the IPDs of the legitimate traffic is established from the captured traffic samples, which can be used to generate *Q* coarse lattices. Each encoded symbol can be modulated based on the corresponding coarse lattice according to its symbol value. We construct two types of nested lattices including dot-lattice and interval-lattice. Compensative quantization and guard band strategy are incorporated with dot-lattice quantization and interval-lattice quantization, respectively. The former aims to remove the quantization regularity and the latter aims to enhance the robustness.

The following are the key contributions of this study:

1) We propose a new general security model which can measure the multi-order statistical distortion of covert timing channels. It can be viewed as the development of polynomial security model and KLD for multi-order IPD chains.
2) We propose a new framework to design covert timing channels that are rich-secure, two types of nested lattices are constructed to quantize secret messages based on the CDF of the IPDs, and they can be easily combined with existing robustness-enhancing strategies.
3) We present detailed comparative analysis of the proposed covert timing channel schemes with several types of state-of-the-art covert timing channels.

The rest of the paper is organized as follows. In the next section, we give a brief review of existing network covert timing channels. In Section 3, we give the description of the proposed rich security model of covert timing channels. Then, in Section 4 and Section 5, we introduce the design of the covert timing channel based on dot-lattice and that based on interval-lattice, respectively. Experimental results and analysis are presented in Section 6. Finally, in Section 7, we give a conclusion for this paper and discuss the future work.

2. Related Work

The basic requirements of a network covert timing channel are undetectability and robustness. Undetectability implies that the warden cannot identify the existence of a covert timing channel by distinguishing between the legitimate and covert traffic. If there exists a negligible function $\upsilon(\delta)$ such that $\left|T(\mathbf{d})-T(\mathbf{d}_s)\right|\le\upsilon(\delta)$ for some probabilistic polynomial-time statistical test T [13], a covert timing channel can be termed *Polynomial Undetectable* regarding a security parameter δ, where $\mathbf{d}$ and $\mathbf{d}_s$ denote arbitrary N samples of IPDs of the legitimate traffic and covert traffic, respectively. On the other side, a covert timing channel may be exposed to both inherent and intentional channel noise. Robustness refers to the capability of correctly receiving the secret message at the receiver in spite of the inherent and maliciously added interference. It is usually measured in terms of bit error rate (BER) for a given covert transmission rate under channel noise including the common additive white Gaussian noise (AWGN) and real channel noise [14]. The covert transmission rate is defined as the average number of message bits transmitted per packet.

Due to their application scenarios, undetectability has been regarded as the most important performance metric of covert timing channels since the birth of this technique. Covert timing channels can be categorized as three types: rate-based [4, 20], packet-reordering-based [21, 22], and IPD-based [6, 17]. Among them, IPD-based covert timing channel is the main focus of the theoretical and implemention studies on covert timing channel. Therefore, we only discuss IPD-based covert timing channel in this study.

To achieve undetectability, a TCP-based covert timing channel called *TCPScript* first takes the TCP's normal burstiness patterns into consideration. It embeds secret messages into the TCP burst size [11]. The capacity as well as robustness are evaluated, whereas no solution to improve them can be given. Another IPD-based covert timing channel targeting interactive SSH traffic considers a two-state Markov Modulated Possion Process (MMPP) model of the legitimate traffic to guarantee the designed covert timing channel satisfying the requirement on undetectability [23]. Time-replay strategy is also employed to maintain the property of the legitimate traffic. A time-replay covert timing channel utilizes a previously recorded sequence of timing intervals to transmit secret messages [24]. The recorded sequence is partitioned according to the size of the message alphabet, and each partition is then associated with a message symbol. A secret message symbol is modulated by randomly choosing a timing interval from the corresponding partition.

To further improve the undetectability, a general model-based framework to design undetectable covert timing channels was proposed to mimic the statistical properties of the legitimate traffic [12], predominantly to mimic the empirical CDF of the IPDs of the legitimate traffic. The framework consists of filter, analyzer, encoder, and transmitter. The filter and analyzer are designed to characterize the features of the legitimate traffic and adjust the model to fit with the features. Then the encoder and transmitter are used to generate the covert traffic with IPD distribution which is consistent to the model. This framework has been employed in many subsequent schemes [5, 15-17]. However, the requirement for the adjusted model to be shared between the sender and the receiver limits the sender's ability to adapt to changes in the IPD distribution of the application traffic.

In our prior work [6], we have addressed the problem of model updating based on a general model-fitting framework using analog fountain codes (AFC), which allows the sender to change the target model without synchronizing with the receiver. Analog fountain timing channel based on symbol transition and that based on symbol split were proposed to achieve both undetectability and robustness. In our another prior work [25], a covert timing channel with distribution matching was proposed. The legitimate traffic is partitioned into fixed-length fragements and all IPDs in a fragements are used to derive the IPD histogram, then the histogram is matched after the secret messages are encoded into IPDs. Later, a model-based covert timing channel with a trellis structure at the modulation stage of the sender and at the iterative demodulation stage of the receiver was proposed in [17]. It provides an adaptive modulation scheme to improve the robustness without any loss of undetectability.

Due to the inherent channel noise (e.g., timing perturbation, packet loss) and maliciously added network jammers, achieving robustness along with undetectability is a challenging task. Many studies have employed various of coding schemes to improve the robustness of covert timing channels. In [18], a simple Geometric code in conjunction with pseudo random generators is employed to establish a provable undetectable timing channel scheme for *i.i.d.* traffic [26]. However, the protection level of the secret message needs to be further enhanced as it can only operate under a strong assumption that the network jitter is bounded in a reasonable scope. In [13, 14], an IPD-based covert timing channel using spread codes was proposed to make the covert timing channel robust under no assumption of the network jitter, whereas the capacity is low and a *Cryptographically Secure Pseudo Random Number Generator* (CSPRNG) is required to guarantee model security. Next, a serial of error correcting codes are employed incorporated with model-based framework to achieve undetectability and robustness in CoCo scheme [15], and the performance of different codes are comparatively analyzed. Besides the finite codes, LT codes are also employed to improve the robustness of covert timing channels [16, 27], the encoded message bits are then modulated into the IPDs based on empirical CDF of the IPDs of the legitimate traffic, which can continually generate code symbols until the secret message is decoded correctly at the receiver. In addition, some entropy coding such as Huffman coding is also applied to compress the covert timing channel, whereas the robustness analysis is not given in their work [28].

Above all, there have been many state-of-the-art studies that achieve undetectability and robustness. However, the undetectability usually relies on the security model established from cumulative distribution function (CDF) or probability mass function (PMF) of the IPDs of the legitimate traffic. The statistical model is used to generate an *i.i.d.* IPD sequence which is distributed in constitent with the empirical CDF or PMF. As we know, in a generic covert timing channel system, the source and the destination are two end-points of some overt application. The source is the overt sender which generates a packet stream (referred to as legitimate traffic) which is transmitted to the destination (overt receiver) over a multihop network. The covert sender and the covert receiver are the end-points of the timing channel. They can be implemented in network elements in the path between the source and the destination or they can be integrated with the source and the destination. Therefore, in a covert timing channel constructed with a empirical CDF or PMF model, the timing sequence of the overt traffic will be manipulated according to the model, whereas no high-order property can be reserved. These covert timing channels are indeed cover-irrelevant but only related to a first-order statistical model of the IPDs of the legitimate traffic. This limitation on security model has led to the vulnerability to some high-order statistical tests such as the entropy test [9].

Consequently, the problem of maintaining multi-order property of IPDs of the legitimate traffic is still a challenging task. A feasible solution to this problem is to design cover-relevant covert timing channel which can reserve multi-order property as much as possible, while ensuring the secret messages being correctly received. In this study, we first establish a rich security model of covert timing channels, which can measure the multi-order statistical distortion of the IPD sequence. Next, we propose a new general framework to design covert timing channels considering multi-order security.

3. Rich Security Model Based on IPD Chains

The undetectability of a covert timing channel is closely relevant to the security model. Most of existing model-secure covert timing channels are indeed only undetectable under a very weak security model, e.g., to measure the KLD between the CDF of the IPDs of the covert traffic and the modeled CDF. To the best of our knowledge, there still exist no work to give a generic security model of covert timing channels which covers each order statistic of the IPDs. Therefore, we give a rich security model for covert timing channels based on IPD chains in this section, which can measure the capability of maintaining multi-order statistical property of the IPDs of the overt traffic.

For given samples of overt traffic C, let $\mathbf{d}=\{d_i\}_{i=1}^{n}$ be the IPDs, where n is the number of the IPDs, $d_{\max}$ and $d_{\min}$ denote the maximal and minimal IPD value, respectively. Let $F(x)=\Pr\left(d_i<x\,|\,x\in[d_{\min},d_{\max}],\,i=1,2,...,n\right)$ denote the CDF of the IPDs, and $F^{-1}(\cdot)$ is the inverse CDF. Then, we divide the interval $[d_{\min},d_{\max}]$ into N subintervals $\Omega_1,\Omega_2,...,\Omega_N$ by

$$\Omega_i=\begin{cases}\left[d_{\min},\,F^{-1}\left(\frac{1}{N}\right)\right], & i=1\\ \left(F^{-1}\left(\frac{i-1}{N}\right),\,F^{-1}\left(\frac{i}{N}\right)\right], & i=2,...,N\end{cases} \tag{1}$$

We define a function G, which can map arbitrary real-value in a subinterval Ω_i to the corresponding subinterval index i. The index sequence $\mathbf{g}=\{G(d_i)\}_{i=1}^{n}=\{g_i\}_{i=1}^{n}$ can be obtained from the function G and the IPD sequence, where $g_i\in\{1,2,...,N\}$.

To establish a multi-order security model of covert timing channels, we regard IPD chains as the basic units in the measurement of multi-order property of the IPDs. In fact, conditional entropy based on IPD chains have proven to be an effective characteristic to detect the existence of some model-based covert timing channels in entropy test scheme. Arbitrary successive M IPDs $\{d_k\}_{k=i}^{i+M-1}$ can form a M-order IPD chain. Similar to the first-order statistics such as CDF or PMF, the multi-order statistics of the IPDs of the legitimate traffic have the property of shape-stability in large time scale and irregularity in small time scale.

In our proposed security model, joint distribution probabilities of the corresponding indices of IPD chains are incorporated with accumulated KLD to measure the multi-order statistical distortion of the IPD sequence of a covert timing channel. The joint distribution probability of the corresponding indices of IPD chains is defined by

$$\mathrm{P}(K_1,K_2,...,K_M)=\Pr\left(G(d_j)=K_1,G(d_{j+1})=K_2,...,G(d_{j+M-1})=K_M\right) \tag{2}$$

where $K_i\in\{1,2,...,N\}$, $j=1,...,(n-M+1)$. Based on polynomial security model and KLD, the rich security model of covert timing channels can be defined as follows:

Rich security model: For arbitrary IPD sequence $\mathbf{d}^C=\{d_i^C\}_{i=1}^{n}$ of legitimate traffic, and arbitrary IPD sequence $\mathbf{d}^S=\{d_i^S\}_{i=1}^{n}$ of covert traffic with enough large length n, a covert timing channel can be regarded as rich secure with respect to security parameter vector

$\boldsymbol{\delta} = (\delta_1, \delta_2, ..., \delta_T)$ when (3) is satisfied, T denotes the maximal order of the rich security model.

$$Q_q = \sum_{K_1, K_2, ..., K_q \in \{1,2,...,N\}} P_S(K_1, K_2, ..., K_q) \log \frac{P_S(K_1, K_2, ..., K_q)}{P_C(K_1, K_2, ..., K_q)} \le \delta_q, \ 1 \le q \le T \tag{3}$$

where P_C and P_S denote the joint distribution probability of the indices of IPD chains in the legitimate and covert traffic, respectively. Q_q denotes the q-th order accumulated distortion, specifically, Q_1 denotes the KLD between the distribution of the IPDs of the legitimate traffic and that of the covert traffic. It is apparent that the rich security model can be employed to detect most existing model-based covert timing channels.

4. Covert Timing Channels Based on Dot-Lattice

According to the above rich security model, a critical criterion to design undetectable covert timing channels is to ensure the accumulated distortion as imperceptible as possible. Therefore, cover-relevant covert timing channels have significant superiority when compared with cover-irrelevant ones that generate IPD using an empirical CDF. Nested lattice codes are a family of codes which can asymptotically achieve the Wyner-Ziv limit [29]. There exists duality between Wyner-Ziv coding and information embedding [30]. Thus, we design two types of nested lattices using CDF of IPDs of the legitimate traffic to operate rich-secure covert timing channels: dot-lattice and interval-lattice. Compensative quantization and guard band strategy are employed to remove the regularity and to enhance the robustness, respectively.

In this section, we give the general framework to design a rich-secure covert timing channel. A dot-lattice is constructed by choosing serials of structured dot sets according to the CDF of the IPDs of the legitimate traffic. The framework of the proposed covert timing channel scheme based on dot-lattice is shown in Fig. 1, which depicts the example of nested dot-lattices when the coarse lattice number $K = 2$. It mainly consists of dot-lattice constructor, quantizer, and decoder.

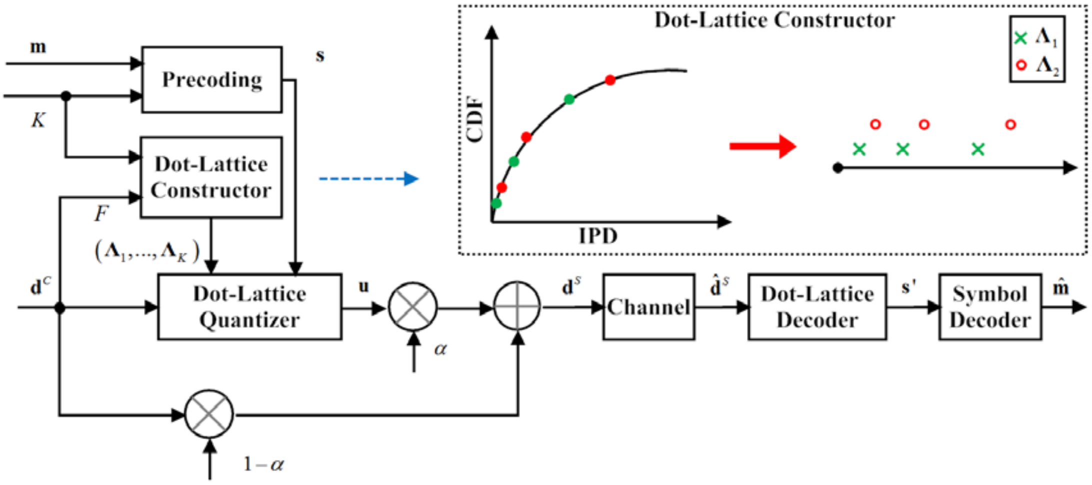


Fig. 1. Covert timing channel framework based on dot-lattice

For a given CDF $F(\cdot)$ of the IPDs of the legitimate traffic and the number of the coarse lattices K, the coarse lattice set $(\mathbf{\Lambda}_1,...,\mathbf{\Lambda}_K)$ can be constructed through a dot-lattice constructor, and the fine lattice $\mathbf{\Lambda}=\bigcup_{i=1}^{K}\mathbf{\Lambda}_i$, each coarse lattice $\mathbf{\Lambda}_i=\{\tau_{i,j} \mid j=1,...,n_i\}$ contains n_i lattice dots.

For simplicity, we assume that each coarse lattice $\mathbf{\Lambda}_i$ is composed of L lattice dots, namely, $n_i=L$, $i=1,...,K$. In order to guarantee the distribution of the lattice dots similar to that of the IPDs of the legitimate traffic and maximize the minimum distance between arbitrary two coarse lattices, each coarse lattice $\mathbf{\Lambda}_i$ is constructed by choosing L sampling points from the CDF curve, $(x_{i,1},y_{i,1}),...,(x_{i,L},y_{i,L})$, where $y_{i,j}=F(x_{i,j})$, $i=1,...,K$, $j=1,...,L$. Each sampling point is determined by

$$\begin{cases} y_{i,j}=(j-1)/L+(i-1)/(L\cdot K) \\ x_{i,j}=F^{-1}(y_{i,j}) \end{cases} \tag{4}$$

Each coarse dot-lattice contains L sampling values, $\mathbf{\Lambda}_i=\{x_{i,1},...,x_{i,L}\}$. With the nested dot-lattice, the secret message bits $\mathbf{m}\in\{0,1\}^m$ are first encoded into *K*-ary symbols $\mathbf{s}\in\{0,1,...,K\text{-}1\}^t$, $t=m/\log_2 K$, and when encoded symbol $s_i=k$ ($0\le k\le K$-1), $\mathbf{\Lambda}_k$ will be chosen as the quantization lattice, the corresponding *i*-th IPD d_i^C is quantized to the nearest lattice dot u_i through dot-lattice quantizer.

$$u_i=\arg\min_{\sigma\in\mathbf{\Lambda}_k}\left|\sigma-d_i^C\right| \tag{5}$$

In order to remove the regularity of the IPDs of covert channels introduced by dot-based quantization, compensative quantization strategy is employed to achieve the tradeoff between undetectability and robustness. $\alpha\in(0,1)$ denotes the quantization parameter and $1-\alpha$ denotes the compensative parameter, the resulting *i*-th IPD of the covert timing channel can be obtained by

$$d_i^S=\alpha u_i+(1-\alpha)d_i^C \tag{6}$$

At the receiver, the received IPDs $\hat{\mathbf{d}}^S=\{\hat{d}_i^S\}_{i=1}^n$ is a noisy version of the IPDs $\mathbf{d}^S=\{d_i^S\}_{i=1}^n$ and is given by

$$\hat{\mathbf{d}}^S=\mathbf{d}^S+\boldsymbol{\delta} \tag{7}$$

where $\boldsymbol{\delta}$ denotes the channel noise. The nested dot-lattice is reconstructed with the shared parameter L and the CDF of IPDs of the legitimate traffic. The estimated encoded symbols

$\mathbf{s}'=\left\{s_i^{'}\right\}_{i=1}^{n}$ can be extracted through dot-lattice decoder by finding the lattice dot in the fine lattice $\mathbf{\Lambda}$ that is nearest to the observed IPD. The index of the corresponding coarse lattice which contains the finding lattice dot is regarded as the estimated encoded symbol

$$s_i^{'}=\sigma\left(\arg\min_{y\in\mathbf{\Lambda}}\left|y-\hat{d}_i^S\right|\right) \tag{8}$$

where $\sigma(\cdot)$ denotes the index querying function for dot-lattice, namely, $\lambda\in\Lambda_{\sigma(\lambda)}$. The final estimated secret message bits $\hat{\mathbf{m}}$ can be determined through the K-ary decoder.

5. Covert Timing Channels Based on Interval-Lattice

The covert timing channel based on dot-lattice (CTC-DL) is designed to be rich-secure while maintaining well tradeoff between undetectability and robustness. The compensative quantization strategy needs to be employed to remove the inherent regularity. In this section, we present a covert timing channel based on interval-lattice (CTC-IL). This scheme divides the CDF curve of IPDs of the legitimate traffic into distinct parts to construct lattice instead of choosing sampling points from the curve, guard band strategy is employed to separate the lattice intervals to reduce the bit error rate (BER) of the received message bits. Fig. 2 shows the framework of the CTC-IL, the example of the interval-lattice is constructed with the coarse lattice number $K=2$.

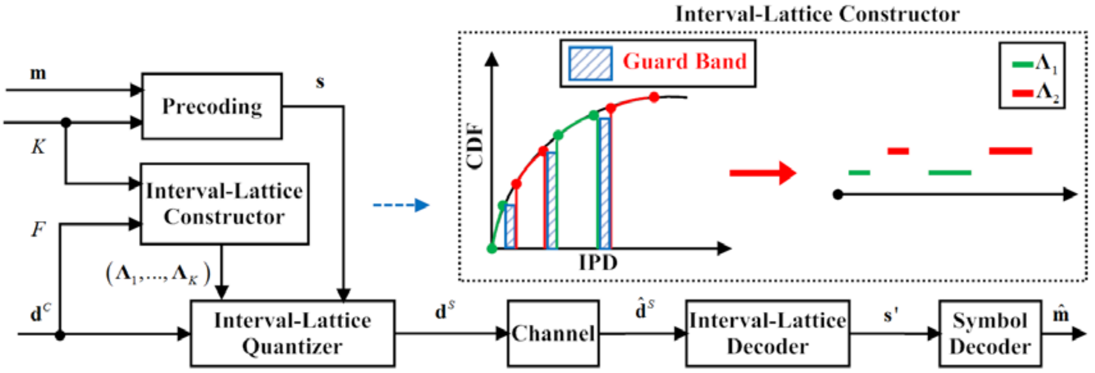


Fig. 2. Covert timing channel framework based on interval-lattice

With the given CDF $F(\cdot)$ of the IPDs of the legitimate traffic and the number of the coarse lattices K, the coarse lattice set $(\mathbf{\Lambda}_1,\ldots,\mathbf{\Lambda}_K)$ can be constructed through an interval-lattice constructor.

Similar to the dot-lattice, we denote the coarse lattice set and fine lattice as $(\mathbf{\Lambda}_1,\ldots,\mathbf{\Lambda}_K)$ and $\mathbf{\Lambda}=\bigcup_{i=1}^{K}\mathbf{\Lambda}_i$, respectively. Each coarse lattice $\mathbf{\Lambda}_i=\left\{B_{i,1},\ldots,B_{i,L}\right\}$ contains L lattice intervals, $B_{i,j}=\left[L_{i,j},R_{i,j}\right]$, where $L_{i,j}$ and $R_{i,j}$ denote the lower bound and upper bound of $B_{i,j}$, respectively.

The interval-lattice constructor divides the CDF curve of IPDs of the legitimate traffic into $L\cdot K$ distinct parts, guard band is reserved between the parts belonging to different coarse lattice to enhance the robustness of the covert timing channel. The interval-lattice can be constructed by

$$\begin{cases} l_{i,j} = (j-1)/L + (i-1)/(L \cdot K) \\ r_{i,j} = l_{i,j} + 1/(L \cdot K) - S \\ L_{i,j} = F^{-1}(l_{i,j}) \\ R_{i,j} = F^{-1}(r_{i,j}) \end{cases} \tag{9}$$

where S denotes the width of guard band. It is apparent that $L \cdot K - 1$ guard bands are required in an interval-lattice.

After encoding the message and choosing lattice using the same strategies in Section 4, we quantize the i-th IPD d_i^C to d_i^S using the following equation.

$$\begin{cases} \hat{\Upsilon} = \arg\min_{\Upsilon \in \mathbf{\Lambda}_k} D(\Upsilon, d_i^C) \\ d_i^S = \delta(\hat{\Upsilon}) \end{cases} \tag{10}$$

where $\delta(\hat{\Upsilon})$ denotes a random value in the interval $\hat{\Upsilon}$, and the function $D(B, p)$ denotes the distance between the interval B and the value p, which is given by

$$D(B,p) = \begin{cases} 0, \ p \in B \\ \min\{|p - L_B|, |p - R_B|\}, \ p \notin B \end{cases} \tag{11}$$

where L_B and R_B denote the lower bound and upper bound of B, respectively.

At the receiver, the nested interval-lattice can be reconstructed with the shared parameter L and the CDF of the IPDs of the legitimate traffic. The estimated encoded symbols $\mathbf{s}' = \{s_i^{'}\}_{i=1}^{t}$ can be extracted through interval-lattice decoder by

$$s_i^{'} = \theta\left(\arg\min_{B \in \mathbf{\Lambda}} D(B, \hat{d}_i^S)\right) \tag{12}$$

where function $A = \theta(B)$ denotes the index querying function for interval-lattice, namely, $B \in \Lambda_A$. The final estimated secret message bits $\hat{\mathbf{m}}$ can be determined through the K-ary decoder.

6. Experimental Results and Analysis

6.1 Experimental Setup

In this section, we benchmark the proposed covert timing channel schemes (CTC-DL, CTC-IL) by examining the undetctability and robustness. We compare them with three schemes including the popular model-based covert timing channel incorporated with analog fountain precoding (MB-AFTC) [6, 12], fountain timing channel (FTC) based on LT codes proposed in [16], analog fountain timing channel based on symbol transition (ST-AFTC) proposed in our prior work [6]. As MB-AFTC, FTC, and ST-AFTC use rateless codes to enhance robustness, in order to make a fair comparison, we also employ forward error correcting codes to precode the secret message bits in the proposed schemes, while maintaining the same covert transmission rate to benchmark performance on robustness for all schemes. The utilized forward error correcting codes are punctured binary BCH codes [31].

In this paper, we analyze the performance of the covert timing channel schemes based on the network traffic generated by TeamViewer IP voice, the most popular remote control software with more than 200 million users which can also supply Voice over IP (VoIP) service, VoIP is one of the most important types of packet streams used for covert timing channels. The samples of the traffic are the same with that we used in our prior work [6]. The destination was implemented in a host in the Computer Science Department at the University of California, Davis (UCDavis), which was connected to the Internet using wired Ethernet. The source was a laptop which was connected to the Internet via public WiFi in the UCDavis campus. For this case, the end-to-end connection was over multiple hops. For this type of traffic, we captured the IPDs both at the source and the destination. The statistical characteristics of the filtered IPDs and the channel noise are shown in **Table 1**. The channel noise are obtained by comparing the difference between the IPDs with the same identification at two ends of the connection. As we can locate the lost packets through packet identification and the packet loss rate is only 0.12%, the pattern of packet loss has no influence on the performance. Thus, we do not discuss the packet loss in this paper.

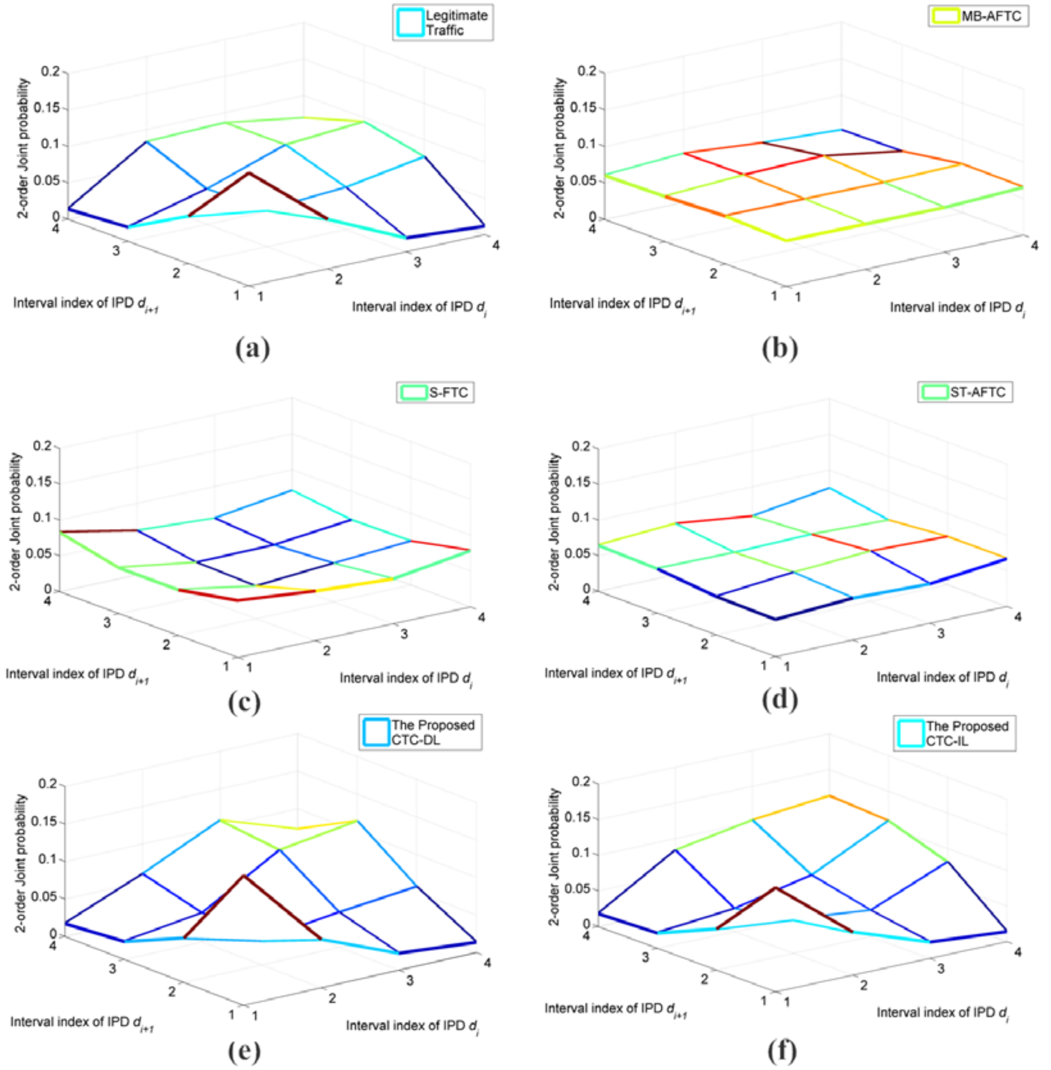
Table 1. Timing statistical characteristics of the captured traffic

Data type	Maximun	Minimum	Mean	Standard Deviation
IPDs	89.9ms	0.064ms	57.1ms	31.3ms
Channel noise	215.6ms	-93.5ms	0.002ms	15.3ms

6.2 Undetectability

We model the legitimate traffic of the channels with the captured 10^4 samples, the empirical CDF of IPDs is acquired from filtered legitimate traffic. The filter is adopted to remove outlier data with value $\hat{d}$ which satisfies $\Pr(\mathbf{d} \le \hat{d} \mid \hat{d} \ge \mu + \eta) \ge 0.995$, where μ and η are the mean and standard deviation of the captured samples, respectively.

In order to evaluate the undetectability of the five schemes, we employed the proposed rich security model in Section 3. The joint distribution probability of the corresponding indices of IPD chains for the legitimate traffic and the covert traffic generated from the five schemes are shown in **Fig. 3(a)-(f)**, respectively. In this figure, the order of IPD chains is set to $M = 2$ and the subinterval number is set to $N = 4$. As the practical covert channel detection requires small window-size, the number of the observed IPDs is set to $l = 2000$. In MB-AFTC [6, 12], the secret message bits are first encoded into message symbols with analog fountain codes (AFC) [32], and then mapped into IPDs with model-based modulation. In S-FTC [16], the guard band strategy is implemented at the sender, the width of guard band is set to 0.1. In ST-AFTC [6], we use AFC to encode the secret message bits and utilize symbol transition strategy to generate IPDs. The weight set of AFC in this paper is set to $W = \{1/2, 1/3, 1/5, 1/7, 1/11, 1/13, 1/17, 1/19\}$. In our proposed two schemes, the quantization parameter α in CTC-DL is set to 0.5 and the width of the guard band in CTC-IL is set to $S = 0.5/(L \cdot K)$. Both the coarse lattice number K and the number of sampling points L are set to 4. Hereinafter, we all employ above parameters in following experiments unless otherwise stated. **Fig. 3(a)** depicts the second-order joint probability of IPD chains of legitimate traffic and **Fig. 3(b)-(f)** depict that of the five schemes including MB-AFTC, S-FTC, ST-AFTC, the proposed CTC-DL and CTC-IL.



(a)

(b)

(c)

(d)

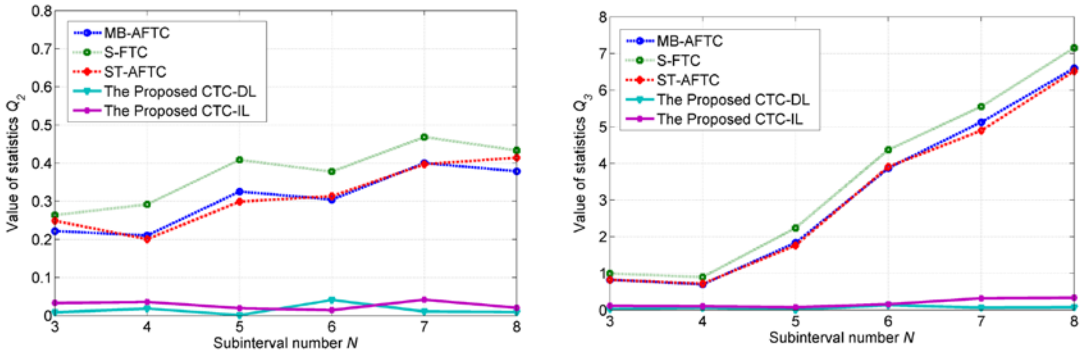
(e)

(f)

Fig. 3. The joint probability of the second-order IPD chains: (a) legitimate traffic (b) MB-AFTC (c) S-FTC (d) ST-AFTC (e) the proposed CTC-DL (f) the proposed CTC-IL

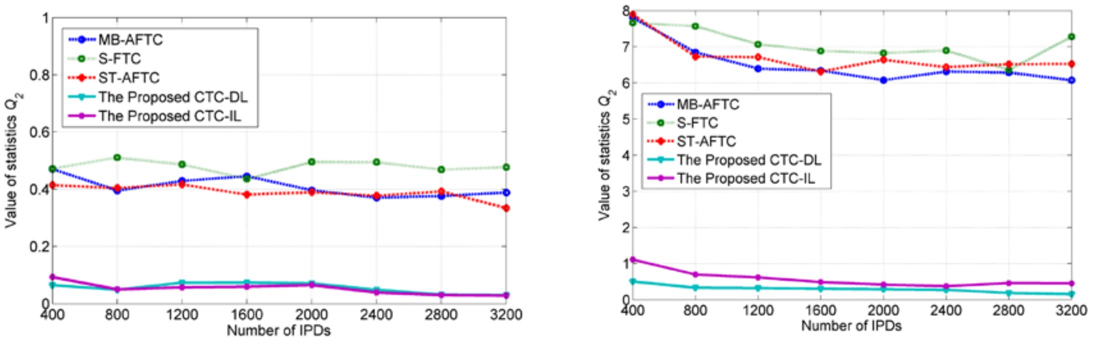
As we can see from **Fig. 3**, the proposed CTC-DL and CTC-IL schemes can mimic the joint distribution probability of the corresponding indices of IPD chains for legitimate traffic very well. In fact, as most network traffic is non-stationary, the statistical characteristics of legitimate traffic have stability in long time scale and dynamics in short time scale. In practical covert channel detection scenario, the inconspicuous gap between the joint distributions of the legitimate traffic and the covert traffic generated by the proposed schemes can be regarded as normal variation. However, there exist significant difference between the joint distribution probability of IPD chains of legitimate traffic and that generated by MB-AFTC, S-FTC and ST-AFTC, which shows the vulnerability of the existing three schemes to rich security model. The results in **Fig. 3** show that the proposed two schemes can achieve significantly better undetectability than the other three schemes when they are tested with the joint distribution of 2-order IPD chains.

Furthermore, we employ the statistics Q_q in Eq. (3) to evaluate the undetectability of the five schemes under rich security model. The statistics Q_2 with the order of IPD chains $M = 2$ and the statistics Q_3 with the order of IPD chains $M = 3$ for the five schemes are shown in **Fig. 4** and **Fig. 5**, respectively. Each point is obtained using the average of 10 samples. **Fig. 4** depicts the statistics with different interval numbers, the number of IPDs is set to $l = 2000$, the horizontal axis denotes the subinterval number and the vertical axis denotes the value of the statistics. **Fig. 5** depicts the statistics with different numbers of IPDs, the subinterval number is set to $N = 8$, the horizontal axis denotes the number of IPDs and the vertical axis denotes the value of the statistics.



(a) (b)

Fig. 4. The stastics Q_q with different subinterval number for covert traffic generated from the five schemes: (a) the value of statistics Q_2 (b) the value of statistics Q_3



(a) (b)

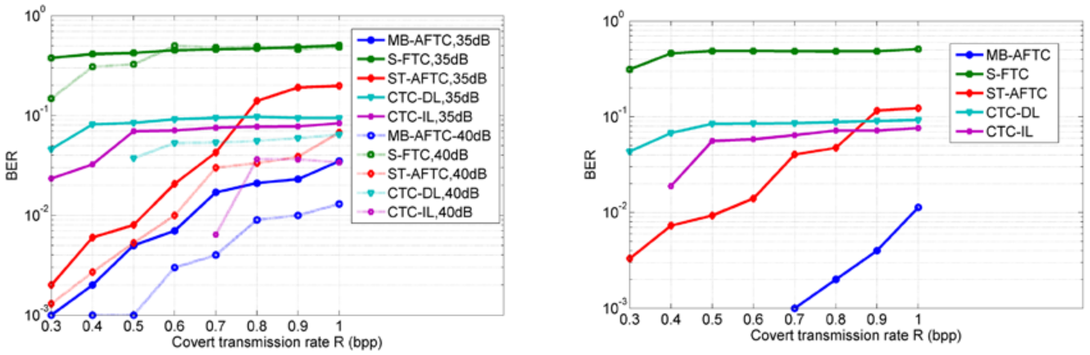
Fig. 5. The stastics Q_q with different number of IPDs for covert traffic generated from the five schemes: (a) the value of statistics Q_2 (b) the value of statistics Q_3

From **Fig. 4** and **Fig. 5** we see that the proposed CTC-DL and CTC-IL are model-secure under the rich security model and they can maintain very good undetectability for multi-order statistical test even when a small number of IPDs is used for the test. The results of statistical test tend to be stabilized gradually with increasing number of IPDs and subintervals. On the other hand, the values of statistics for MB-AFTC, S-FTC and ST-AFTC are all much larger than the proposed schemes. When the subinterval number $N = 8$ and the number of IPDs $l = 400$, Q_2 of the proposed two schemes are both lower than 0.1 and Q_3 of them are both lower than 1.1. Nevertheless, Q_2 and Q_3 of the other three schemes are all larger than 0.4 and 7, respectively. It means that we can easily distinguish between the legitimate traffic and the covert traffic generated by MB-AFTC, S-FTC and ST-AFTC even with very small number of IPDs under the proposed rich security model. In contrast, both the proposed two covert timing channel schemes can achieve good undetectability when they are tested with multi-order statistics.

We also find that the undetectability of the proposed CTC-IL is a little worse than CTC-DL, which is the result of the employed guard band strategy in CTC-IL. The gap can be reduced by decreasing the width of the guard band between coarse lattice intervals. The number of the IPDs has more significant influence on the value of statistics Q_q for the proposed two schemes than subinterval number. The results also show that ST-AFTC has similar performance on undetectability with MB-AFTC, whereas S-FTC is the worst one.

6.3 Robustness

In order to evaluate the robustness, two types of network noise are considered in our experiments. Firstly, we consider the real channel noise with statistical characteristics shown in **Table 1**. Secondly, we consider an additive white gaussian noise (AWGN), which is measured by the signal-to-noise ratio (SNR). Without loss of generality, we measure the robustness of covert timing channels using the BER of the decoded secret messages. The number of the secret message bits is set to $m = 3000$, the number of the sampling points L is set to 2, and the quantization parameter α is set to 0.6. **Fig. 6 (a)** shows the BER of MB-AFTC, S-FTC, ST-AFTC, and the proposed two schemes with AWGN. **Fig. 6(b)** shows the BER of them with real channel noise. The horizontal axis denotes the covert transmission rate R, which is defined as the average number of message bits transmitted per packet (bpp). The vertical axis denotes the BER of the decoded secret message. We test the five schemes with the covert transmission rate from 0.3bpp to 1bpp. The unmarked points in the figure means the corresponding BER is zero.



(a) (b)

Fig. 6. The BER of the five covert timing channels with different covert transmission rates. (a) AWGN (b) real channel noise

As shown in **Fig. 6(a)**, the performance of S-FTC is the worst of all as the BP algorithm in the decoder cannot converge in these cases. The robustness of the proposed covert timing channels schemes are both observably better than the other three schemes for low covert transmission rate and high SNR under AWGN. When SNR=40dB and the covert transmission rate $R \le 0.4$ bpp, CTC-DL and CTC-IL can both decode the secret message correctly, whereas the BER of MB-AFTC achieves 10^{-3} when $R = 0.4$ bpp and decreases to 0 when $R = 0.3$ bpp. The BER of ST-AFTC is about 3×10^{-3} and 10^{-3} with $R = 0.3$ bpp and $R = 0.4$ bpp, respectively. When SNR=35dB and $R \le 0.7$ bpp, the robustness of the proposed two schemes are worse than ST-AFTC and MB-AFTC, the BER of CTC-DL and CTC-IL are about 9×10^{-2} and 8×10^{-2} when $R = 0.7$ bpp, respectively. Nevertheless, the BER of MB-AFTC is about 2×10^{-2} and that of ST-AFTC is about 5×10^{-2}.

The comparison results of the five covert timing channel schemes with real channel noise are shown in **Fig. 6(b)**. We can find that the performance of MB-AFTC is the best and that of S-FTC is the worst. When the covert transmission rate $R > 0.8$ bpp, the performance of the proposed two schemes are a little better than that of ST-AFTC, whereas ST-AFTC can achieve stronger robustness when $R \le 0.8$ bpp. When $R = 0.3$ bpp, the BER of the proposed CTC-DL scheme is about 4×10^{-2} and that of the proposed CTC-IL scheme is 0. When $R = 1$ bpp, namely, there exist no precoding stage in the proposed schemes, the BER of CTC-DL and CTC-IL are about 9×10^{-2} and 8×10^{-2}, respectively. With the same covert transmission rate $R = 1$ bpp, the BER of MB-AFTC and ST-AFTC are about 1×10^{-2} and 1×10^{-1}, respectively.

In summary, MB-AFTC, ST-AFTC and the proposed two schemes can all perform efficiently on the channels with network jitter and for traffic which is not very well suited for establishing covert timing channels. In general, MB-AFTC can achieve the best performance on robustness due to the capacity-approaching analog fountain codes. The proposed CTC-DL and CTC-IL have better performance with high SNR and low transmission rate when compared with ST-AFTC and S-FTC. We also find that the robustness of the proposed CTC-IL is a little better than CTC-DL.

7. Conclusion

In this paper, we have established a general security model to measure the difference of the multi-order statistical characteristics between the legitimate and covert traffic. It can efficiently detect the existence of covert timing channels that use model-based modulation framework, and also can operate for some state-of-the-art covert timing channels. Moreover, nested lattice codes incorporated with the distribution of IPDs are utilized to design covert timing channels that not only meet the goals of rich security but are also robust. Two types of nested lattices including dot-lattice and interval-lattice are designed to quantize the secret messages. In addition, compensative quantization and guard band strategy are adopted to remove the regularity and enhance the robustness, respectively. Using experiments with real traffic we have demonstrated the effectiveness of the proposed covert timing channels with respect to undetectability and robustness.

Even though the proposed covert timing channel schemes have been shown to be robust enough for general network jitters when forward error correcting codes are employed, it inevitably limits the covert transmission rate as we have trade off the capacity for undetectability. Another issue is the dimension of the constructed nested lattices, we concentrate on one-dimensional lattices in this paper while the increasing dimension can further enhance the overall performance of the proposed covert timing channels. Covert timing channel schemes based on multi-dimensional nested lattices are also part of future work.

References

[1] A. K. Biswas, D. Ghosal, and S. Nagaraja, "A survey of timing channels and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 50, no. 1, 2017. Article (CrossRef Link).

[2] S. Wendzel, S. Zander, B. Fechner, and C. Herdin, "A pattern-based survey and categorization of network covert channel techniques," *ACM Computing Surveys (CSUR)* , vol. 47, no. 50, 2015. Article (CrossRef Link).

[3] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 2, pp. 221-234, 2016. Article (CrossRef Link).

[4] L. Yao, X. Zi, L. Pan, and J. Li, "A study of on/off timing channel based on packet delay distribution," *Computers & Security*, vol. 28, no. 8, pp. 785-794, 2009. Article (CrossRef Link).

[5] R. Archibald and D. Ghosal, "Design and performance evaluation of a covert timing channel," *Security & Communication Networks*, vol. 9, no. 8, pp. 755-770, 2016. Article (CrossRef Link).

[6] W. Liu, G. Liu, J. Zhai, Y. Dai, and D. Ghosal, "Designing analog fountain timing channels: Undetectability, robustness, and model-adaptation," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 4, pp. 677-690, 2016. Article (CrossRef Link).

[7] R. Archibald, and D. Ghosal, "A comparative analysis of detection metrics for covert timing channels," *Computers & Security*, vol. 45, no. 8, pp. 284-292, 2014. Article (CrossRef Link).

[8] C. Cachin, "An information-theoretic model for steganography," *Information & Computation*, vol. 192, no. 1, pp. 41-56, 2004. Article (CrossRef Link).

[9] 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. Article (CrossRef Link).

[10] G. Shah, A. Molina, and M. Blaze, "Keyboards and covert channels," in *Proc. of 15th USENIX Security Symposium*, pp. 59-75, 2006. Article (CrossRef Link).

[11]X. Luo, E. W. Chan, and R. K. Chang, "TCP covert timing channels: Design and detection," in *Proc. of IEEE Int. Conference on Dependable Systems and Networks with FTCS and DCC*, pp. 420-429, 2008. Article (CrossRef Link).

[12] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based covert timing channels: Automated modeling and evasion," in *Proc. of Recent Advances in Intrusion Detection*, pp. 211-230, 2008. Article (CrossRef Link).

[13] Y. Liu, D. Ghosal, F. Armknecht, A.-R. Sadeghi, S. Schulz, and S. Katzenbeisser, "Robust and undetectable steganographic timing channels for *iid* traffic," in *Proc. of Information Hiding*, pp. 193-207, Article (CrossRef Link).

[14] Y. Liu, D. Ghosal, F. Armknecht, A.-R. Sadeghi, S. Schulz, and S. Katzenbeisser, "Hide and seek in time—robust covert timing channels," *in Proc. of Computer Security–ESORICS 2009*, pp. 120-135, 2009. Article (CrossRef Link).

[15] A. Houmansadr, and N. Borisov, "CoCo: coding-based covert timing channels for network flows," in *Proc. of Information Hiding*, pp. 314-328, 2011. Article (CrossRef Link).

[16] R. Archibald, and D. Ghosal, "A covert timing channel based on fountain codes," in *Proc. of 11th Int. Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 970-977, 2012. Article (CrossRef Link).

[17] S. A. Ahmadzadeh, and G. Agnew, "Turbo covert channel: an iterative framework for covert communication over data networks," in *Proc. of INFOCOM*, pp. 2031-2039, 2013. Article (CrossRef Link).

[18] K. Kothari, and M. Wright, "Mimic: An active covert channel that evades regularity-based detection," *Computer Networks*, vol. 57, no. 3, pp. 647-657, 2013. Article (CrossRef Link).

[19] R. J. Walls, K. Kothari, and M. Wright, "Liquid: A detection-resistant covert timing channel based on IPD shaping," *Computer Networks*, vol. 55, no. 6, pp. 1217-1228, 2011. Article (CrossRef Link).

[20] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels:design and detection," in *Proc. of ACM Conference on Computer and Communications Security*, pp. 178-187, 2004. Article (CrossRef Link).

[21] H. Khan, Y. Javed, F. Mirza, and S. A. Khayam, "Embedding a covert channel in active network connections," in *Proc. of Global Telecommunications Conference*, pp. 4933-4938, 2009. Article (CrossRef Link).

[22] X. Luo, E. W. W. Chan, P. Zhou, and R. K. C. Chang, "Robust network covert communications based on TCP and enumerative combinatorics," *IEEE Transactions on Dependable & Secure Computing*, vol. 9, no. 6, pp. 890-902, 2012. Article (CrossRef Link).

[23] T. P. Coleman, and N. Kiyavash, "Sparse graph codes and practical decoding algorithms for communicating over packet timings in networks," in *Proc. of Information Sciences and Systems*, pp. 447-452, 2008. Article (CrossRef Link).

[24] C. E. Brodley, E. H. Spafford, and S. Cabuk, "Network covert channels: Design, analysis, detection, and elimination," *Dissertations & Theses, Purdue University*, 2006. Article (CrossRef Link).

[25] G. Liu, J. Zhai, and Y. Dai, "Network covert timing channel with distribution matching," *Telecommunication Systems*, vol. 49, no. 2, pp. 199-205, 2012. Article (CrossRef Link).

[26] S. H. Sellke, C. C. Wang, S. Bagchi, and N. Shroff, "TCP/IP timing channels: theory to implementation," in *Proc. of INFOCOM* , pp. 2204-2212, 2007. Article (CrossRef Link).

[27] R. Archibald, "Design and detection of covert communication: timing channels and application tunneling," *Dissertations & Theses, University of California, Davis*, 2013.

[28] J. Wu, Y. Wang, L. Ding, and X. Liao, "Improving performance of network covert timing channel through Huffman coding," *Mathematical & Computer Modelling*, vol. 55, no. 1–2, pp. 69-79, 2012. Article (CrossRef Link).

[29] L. Cong, G. Su, and J. C. Belfiore, "Wyner-Ziv coding based on multidimensional nested lattices," *IEEE Transactions on Communications*, vol. 60, no. 5, pp. 1328-1335, 2011. Article (CrossRef Link).

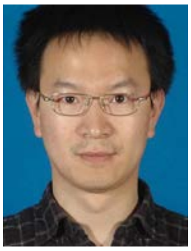
[30] R. J. Barron, B. Chen, and G. W. Wornell, "The duality between information embedding and source coding with side information and some applications," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1159-1180, 2003. Article (CrossRef Link).

[31] S. Lin, and D. J. Costello, *Error Control Coding, Second Edition*: Prentice-Hall, Inc., 2004. Article (CrossRef Link).

[32] M. Shirvanimoghaddam, Y. Li, and B. Vucetic, "Near-capacity adaptive analog fountain codes for wireless channels," *IEEE Communications Letters*, vol. 17, no. 12, pp. 2241-2244, 2013. Article (CrossRef Link).

Weiwei Liu received the B.S. degree in automation, and the Ph. D degree in control science and engineering, both from Nanjing Universuty of Science and Technology, Nanjing, in 2010 and 2015, respectively. From September 2014 through February 2015, he was a visiting scholar with the Department of Computer Science, University of California, Davis, CA, USA. He is currently an Assistant Professor in the School of Automation at Nanjing University of Science and Technology. His research interests include multimedia signal processing and network traffic analysis.

Guangjie Liu received the B.S. degree in electrical and computer engineering, and the Ph.D. degree in control science and engineering, both from Nanjing University of Science and Technology, Nanjing, in 2002 and 2007, respectively. He is presently an Associate Professor in the School of Automation at Nanjing University of Science and Technology. His research interests are multimedia systems and deep learning.



Xiaopeng Ji received the B.S. degree in electrical and computer engineering, and the Ph. D degree in control science and engineering, both from Nanjing Universuty of Science and Technology, Nanjing, in 2005 and 2010, respectively. He is presently an Assiatant Professor in Nanjing Universuty of Science and Technology, Nanjing. His research interests include multimedia signal processing and wireless sensor networks.

Jiangtao Zhai received the B.S. degree in electrical and computer engineering, and the M.S. and Ph.D. degrees in control science and engineering, from Nanjing University of Science and Technology, Nanjing, in 2007, 2009 and 2013, respectively. He is presently an Associate Professor in Jiangsu University of Science and Technology, Zhenjiang. His research interests include multimedia communication and wireless sensor networks.

Yuewei Dai received the B.S. and M.S. degrees in system engineering from East China Institute of Technology in 1984 and 1987, respectively, and the Ph.D degree in control science and engineering from Nanjing University of Science and Technology in 2002. He is presently a Professor in the School of Automation at Nanjing University of Science and Technology. His research interests are in multimedia security, system engineering theory and network security.