Hindawi
Security and Communication Networks
Volume 2020, Article ID 8846230, 14 pages
https://doi.org/10.1155/2020/8846230

Research Article

VoNR-IPD: A Novel Timing-Based Network Steganography for Industrial Internet

Mingqian Wang, Shuai Cao, and Yunliang Wang

School of Information Engineering, Changzhou Vocational Institute of Mechatronic Technology, Changzhou 213164, China

Correspondence should be addressed to Mingqian Wang; 937565385@qq.com

Received 20 April 2020; Revised 27 May 2020; Accepted 4 June 2020; Published 28 June 2020

Academic Editor: Zhaoqing Pan

As the predominant trade secret of manufacturing enterprises, industrial data may be monitored and stolen by competitive adversaries during the transmission via open wireless link. Such information leakage will cause severe economic losses. Hence, a VoNR-IPD covert timing steganography based on 5G network is proposed in this paper, in which VoNR traffic is employed as the steganographic carrier of covert communication in Industrial Internet. Interference of network jitter noise is fully considered and the high-order statistical properties of jittered VoNR interpacket delays (IPDs) are imitated during the modulation of confidential industrial data. Thus, the generated covert VoNR IPDs can possess consistent statistical properties with the normal case in order to improve undetectability. Besides, the synchronization mechanism of steganographic embedding mode is designed to control the embedding density of industrial data flexibly. The experimental results show that our scheme can resist statistical-based detections and the network noise effectively, which outperforms the existing methods in terms of undetectability and robustness.

1. Introduction

Industrial Internet realizes the comprehensive sensing, dynamic transmission, and real-time analysis of industrial data by constructing a basic network connecting the machines, materials, human, and information systems. Thus, scientific decision and intelligent control can be achieved to improve the efficiency of manufacturing resource allocation and production management, among which the intelligent production management and supervisory control system are mainly engaged in the automatic acquisition, transmission, and analysis of crucial industrial data, such as the core parameters, the overall production data, and the running state of devices. Nevertheless, with the rapid development and wide application of Industrial Internet, it is difficult to resist the external attack due to the penetrability of network boundary and the openness of wireless transmission. The industrial data are confronted with severe security threats.

As the predominant trade secret of manufacturing enterprises, industrial data may be monitored and stolen by competitive adversaries during the transmission via open wireless link. Such information leakage will cause severe economic losses and affect the core competitiveness of an enterprise and even threaten its survival and development. Therefore, covert communication technique should be exploited to guarantee the secure transmission of industrial data. Network steganography is a hidden communication technique, which utilizes legitimate traffic as the vehicle to transfer confidential information covertly over the untrusted network.

There are two broad types of network steganography: covert storage steganography and covert timing one. Covert storage steganography embeds the secret information into the redundancies of network protocols [1–6]. Although it is simple and easy to implement, it can be easily detected by the existing steganalysis. Covert timing steganography delivers the secret information by exploiting time-relevant events of network packets and it has better concealment than covert storage one. Generally, it can be divided into four subclasses: on-off steganography [7], interpacket delay- (IPD-) based steganography [8–11], packet sorting [12, 13], and combination-based ones [14, 15]. Synchronization is always a difficult issue to solve, since covert timing steganography is susceptible to the unstable network circumstance, such as jitter and delay. To guarantee reliability, several studies [16–20] have utilized Error Correction Code to improve accuracy, which sacrifices the capacity and increases the transmission overhead.

Since IPD-based steganography is one of the most common and effective means, we mainly focus on it in this paper. However, most of the existing methods would either generate abnormal covert traffic or possess distinct properties compared with the normal case, making it vulnerable to be detected. Countering such deficiencies, network steganography tends to mimic the normal traffic by shape-fitting. The feature model is considered in the modulation process of the secret message to resist statistical detection tools [13, 21, 22]. Predominantly, appropriate and feasible network services with more popularity, reliability, and security are sought after as steganographic carrier.

Nowadays, mobile network has become a predominant means of data transmission, dynamically evolving network steganography subfield. Under this background, recent network steganography solutions exploit 4G service like VoLTE [12, 23, 24]. Since 5G communication technique based on New Radio (NR) standard possesses the advantages of high data rate, low cost, low power consumption, ultralow latency, and availability, it has gradually become the main means of data transfer in the Industrial Internet. Moreover, it will achieve more wide and comprehensive application in the future. In 5G network, VoNR (Voice over New Radio) is an IP-based voice calling scheme, which will be the most prevailing and popular telecommunication level-communication service. Therefore, the potential continuous and large amount of VoNR traffic provides chances of launching steganography in Industrial Internet. However, in the state of the art, there are few literature studies engaged in studying the mobile steganography of 5G network.

On the basis of the above analysis, in order to overcome the drawbacks of the current methods, a VoNR-IPD covert timing steganography based on 5G network is proposed in this paper, in which VoNR traffic is employed as the steganographic carrier of covert communication in Industrial Internet. The main contribution of this paper is as follows:

(1) Interference of network jitter noise is fully considered and the high-order statistical properties of jittered VoNR traffic are imitated during the steganographic process. Specifically, the cumulative distribution function (CDF) of jittered VoNR IPDs is fitted and utilized in the modulation of confidential industrial data. Thus, the generated covert VoNR IPDs can possess consistent statistical properties with the normal case in order to resist detection.

(2) The synchronization mechanism of steganographic embedding mode is designed to control the embedding density of industrial data flexibly. In this manner, our scheme can resist the network noise effectively, so as to improve the undetectability and robustness of covert communication in Industrial Internet.

The remainder of this paper is organized as follows. In Section 2, related works are reviewed. The basis of our scheme is described in Section 3. In Section 4, the proposed scheme is introduced in detail. In Section 5, experimental results are presented and analyzed. Finally, the whole paper is concluded in Section 6.

2. Related Work

IPD-based steganography is a notable branch of covert timing steganography, which manipulates the timing intervals of adjacent network packets to transmit secret information. To achieve better understanding, four typical interpacket-delays-based schemes are reviewed and analyzed; they are Jitterbug [25], TRCTC [10], MBCTC [26], and CTCDM [27], respectively.

Jitterbug [25] is a keyboard device that slowly leaks 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 such that 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 traffic 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 [10] uses a sample of normal traffic captured from the overt network and replays it later to transfer secret. Since the covert traffic of TRCTC is composed of scrambled normal interpacket delays, its distribution is close to that of the normal one. However, the scrambled traffic may also raise suspicion of monitoring device.

MBCTC [26] 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 [27] 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 a binary channel, where bit “0” is decoded when the observed timing interval is smaller than the center value α^* 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 achieves well undetectability and robustness. In this paper, under the scenario of Industrial Internet, a novel IPD-based covert timing steganography is proposed by modulating the confidential industrial data into VoNR traffic of 5G network.

3. Basis of Our Scheme

3.1. Application Scenario of 5G Network. Nowadays, 5G has been the latest mobile communication technique, which mainly contains three kinds of application scenarios: enhanced Mobile Broadband Communication (eMBB), massive Machine-Type Communication (mMTC), and Ultrareliable Low-Latency Communication (URLLC), among which eMBB refers to the direct evolution of the mobile broadband service, which can support larger amount of data traffic and further enhance the user experience, such as higher data rate in user terminal. mMTC represents a kind of service that supports massive terminals, for instance, the remote sensors, manipulators, device monitor, and so on. The critical requirements of this service comprise extremely low cost and energy consumption of terminals. In general, such kind of terminals only consumes and produces relatively small amount of data. Meanwhile, the services under URLLC demand extraordinary low latency and extremely high reliability, such as Traffic Safety Control System and Industrial Automated Control System. Hence, 5G network will become the major means of data transmission in Industrial Internet.

3.2. VoNR Traffic Analysis. NR (New Radio) is a novel standard of 5G communication, which is evolved from and compatible with LTE. NR networks provide greater data capacity and lower latency for mobile broadband. In order to make up for the lack of circuit-switched voice domain, VoNR, an IP-based NR voice calling scheme, has been adopted by the mobile industry, which can be integrated with low-level drivers and network interfaces. It is a globally interoperable solution and also progresses innovative communication services.

In order to improve the undetectability and security of covert communication in Industrial Internet, the normal traffic, as well as its properties of certain network service, should be preserved or mimicked as possible during the steganographic process. In other words, alteration of the original carrier should not reveal anomaly to raise suspicion. Thus, the characteristics of VoNR traffic are analyzed initially. The normal and jittered IPDs of VoNR traffic are compared in Figure 1, where the x-axis is the sequence number of IPD and y-axis represents the corresponding value. It can be found that the normal IPDs of VoNR mainly concentrate on 20 ms. Meanwhile the jittered IPDs reveal the regularity of a random distribution between 10 ms and 30 ms. Furthermore, jitters of the normal VoNR traffic are presented in Figure 2. It is observed that jitters of such service mainly vary from −10 ms to 10 ms. As is known, jitter is the amount of network delay variation, which is generated by any two adjacent packets during network transmission. Excessive jitter is usually a symptom of a network congestion or insufficient bandwidth to handle traffic [12].

Above all, since the IPDs of network traffic are independent identical distribution (i.i.d), it can be concluded that the normal or jittered IPDs of VoNR traffic are limited to a small range and possess distinct and obvious regularity. The direct modification of normal IPDs might generate abnormal properties, making such scheme detectable. Therefore, in this paper, the interference of network jitter is considered and imitated in the modulation of secret information. In that, the statistical properties of the covert IPDs can be almost consistent with those of the jittered normal ones.

4. The Proposed Scheme

In order to improve the undetectability and robustness of covert communication in Industrial Internet, interference of network jitter noise is fully considered and the high-order statistical properties of jittered VoNR traffic are imitated during the steganographic process. Specifically, the CDF of jittered VoNR IPDs is fitted and utilized in the modulation of confidential industrial data. Thus, the generated covert traffic can possess consistent statistical properties with the normal case. In addition, the synchronization mechanism of steganographic embedding mode is designed to control the embedding density of covert VoNR IPDs.

4.1. System Model. The proposed system model of VoNR-IPD for covert communication in Industrial Internet is presented in Figure 3, which is implemented as follows:

(1) VoNR link of 5G network is constructed between the steganographic sender and receiver; then, the legitimate service is performed.

(2) The confidential industrial data are modulated into the covert VoNR IPDs by utilizing the encoder of our scheme.

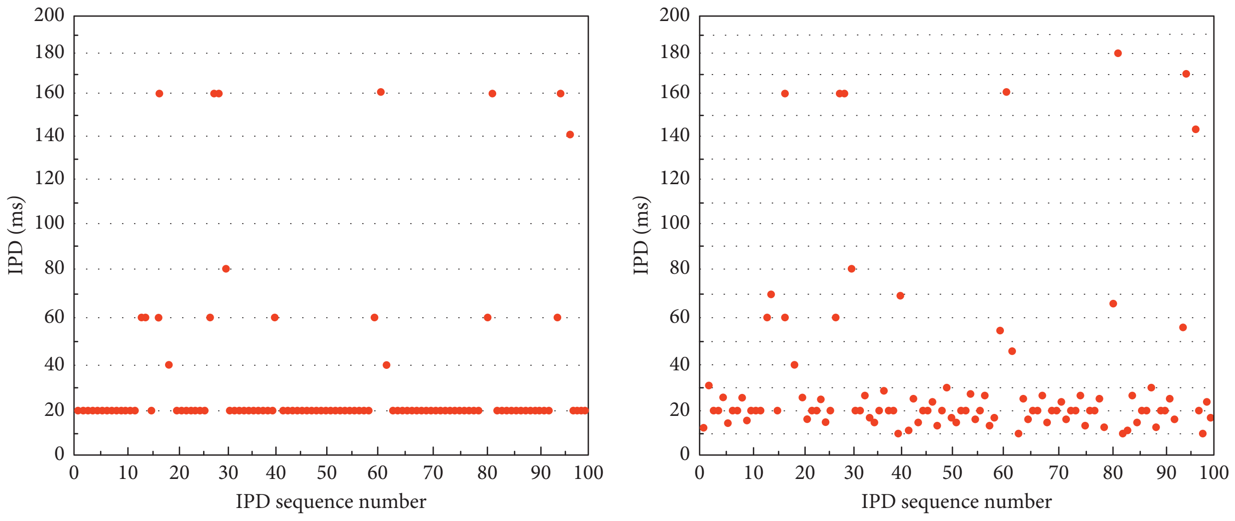
(3) The steganographic embedding mode is selected according to the comprehensive assessment of the transferred data size and Quality of Service (QoS). Thus, the generated covert IPDs can be inserted into the normal ones intensively or sparsely.

(4) The VoNR traffic is initially sent according to the synchronization IPD of the selected mode and then the normal or covert IPDs successively.

(5) The noised VoNR IPDs are obtained by the steganographic receiver, from which the steganographic embedding mode is recovered according to the synchronization IPD.

(6) The covert IPDs are extracted from all IPDs, and the confidential industrial data are retrieved by the decoder.

4.2. Steganographic Process. The VoNR traffic will inevitably suffer from network noise, such as jitter, packet loss, or disorder, during the transmission via the overt wireless



(a)

(b)

FIGURE 1: IPDs of the normal VoNR traffic. (a) The normal VoNR IPDs. (b) The jittered normal VoNR IPDs.

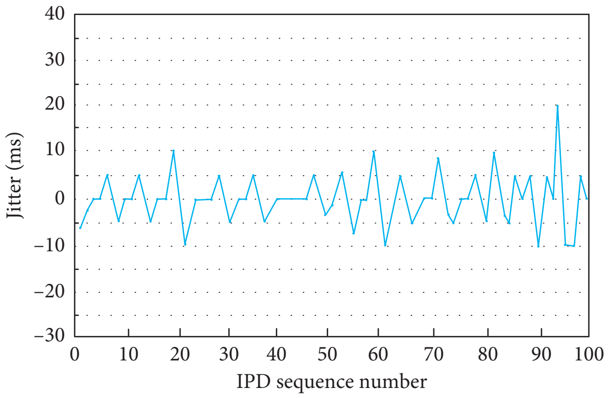


FIGURE 2: Jitter of the normal VoNR traffic.

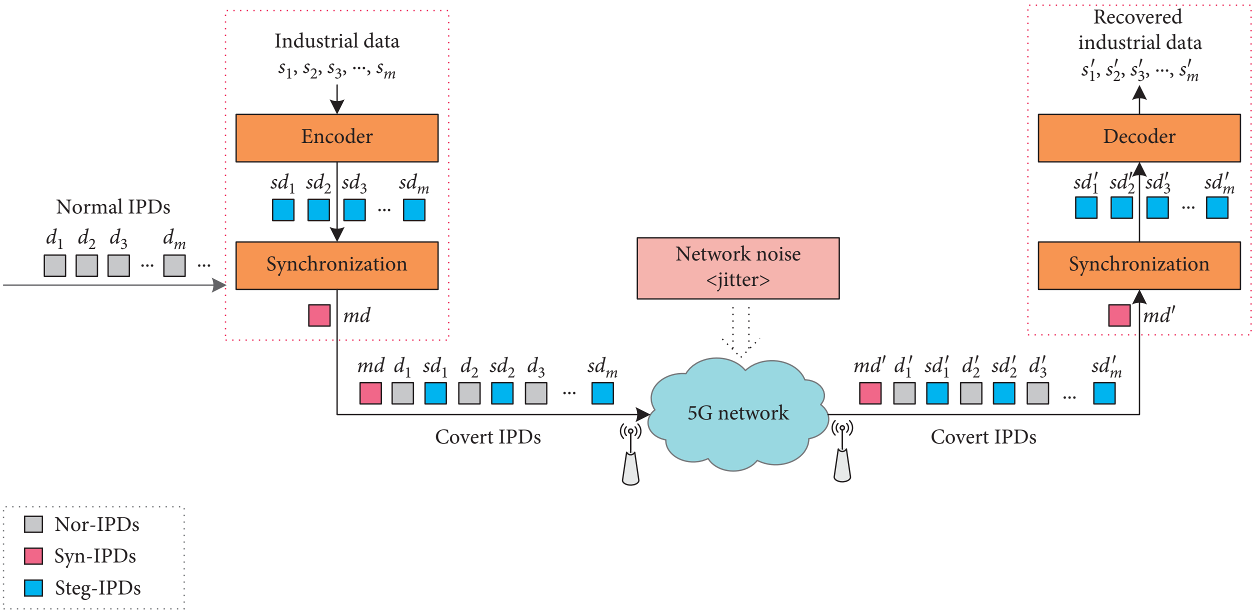

Industrial data
$s_1, s_2, s_3, \cdots, s_m$
Encoder
sd_1 sd_2 sd_3 ··· sd_m
Normal IPDs
d_1 d_2 d_3 ··· d_m ···
Synchronization
md
md d_1 sd_1 d_2 sd_2 d_3 ··· sd_m
Covert IPDs
Network noise
<jitter>
5G network
md' d_1' sd_1' d_2' sd_2' d_3' ··· sd_m'
Covert IPDs
Recovered
industrial data
$s_1', s_2', s_3', \cdots, s_m'$
Decoder
sd_1' sd_2' sd_3' ··· sd_m'
Synchronization
md'
Nor-IPDs
Syn-IPDs
Steg-IPDs

FIGURE 3: The system model of our proposed scheme.

channel. Moreover, only the noised VoNR traffic may be captured and analyzed by the network monitor device or an adversary. Thus, it should be noted that only the jittered case of normal or covert traffic is considered in this paper.

The main notations and symbols of our scheme are presented in Table 1.

4.2.1. *Steganography Encoding*

Step 1: the jittered VoNR IPDs are collected during the normal communication in 5G network, which is denoted as Jit < NorIPD > . Jit<•> refers to the interference of network jitter, and NorIPD represents the normal VoNR IPDs. Then, the distribution of network jitter in VoNR is analyzed, which is denoted as $[-\varepsilon, +\varepsilon]$, satisfying $\varepsilon > 0$.

Step 2: the CDF of Jit < NorIPD > is fitted and its corresponding IPD interval with larger probability is defined as $\Delta D|p_{\max}$. Then $\Delta D|p_{\max}$ is divided into two portions utilized in the steganographic encoding, which is represented as $\Delta D_k^{\hat{e}} = [d_k^{\hat{e}}, \overline{d}_k^{\hat{e}}]\,(k = 0, 1)$, where $\Delta D_k^{\hat{e}}$ is the mapping interval of IPDs to the secret bit "0" or "1." $d_k^{\hat{e}}$ and $\overline{d}_k^{\hat{e}}$ refer to the upper and lower limits of the corresponding IPD interval, respectively, which is required to satisfy the following condition:

$$d_1^{\hat{e}} - \overline{d}_0^{\hat{e}} \geq 2\varepsilon. \tag{1}$$

Figure 4 presents the fitted CDF of Jit < NorIPD > and its corresponding mapping intervals of IPDs. In our case, ε is set to 5 and the IPD interval with larger probability is $\Delta D|p_{\max} = [10, 30]$. The effect of network noise should be taken into consideration in order to guarantee the robustness of covert communication. Therefore, in our implementation, the mapping interval of secret bit is set to $\Delta D_0^{\hat{e}} = [10, 15]$ and $\Delta D_1^{\hat{e}} = [25, 30]$.

Step 3: the confidential industrial data is converted into its binary form, denoted as $S = \{s_i \,|\, i = 1, 2, \ldots, m\}$, where $s_i \in \{0,1\}$. For the i^{th} secret bit s_i, the encoding function $E(s_i)$ is defined as

$$sd_i = E(s_i) = \text{rand}\lfloor d_{s_i}^{\hat{e}}, \overline{d}_{s_i}^{\hat{e}} \rfloor, \quad i = 1, 2, \ldots, m, \tag{2}$$

where sd_i is the i^{th} steganographic IPD and $\text{rand}\lfloor\bullet\rfloor$ represents a predefined function used to select a value from the given set randomly.

4.2.2. *Steganography Synchronization.*

In order to further enhance the detection-resistance and reliability of our scheme, a synchronization mechanism of steganographic embedding mode is designed in this paper. In this mode, Steg-IPDs is embedded into Nor-IPDs according to certain density. In our case, there are four modes set as $M \in \{0, 1, 2, 3\}$, and the embedding interval of Steg-IPDs is denoted as $\text{Interv} = 2^M$, which is depicted in Figure 5.

Step 1: for the CDF of Jit <NorIPD>, its corresponding IPD interval with relatively smaller probability is defined as $\Delta D|p_{\min}$. Then $\Delta D|p_{\min}$ is divided into four portions utilized in the steganographic synchronization, which is represented as $\Delta D_j^{\hat{s}} = [d_j^{\hat{s}}, \overline{d}_j^{\hat{s}}]\,(j = 0, 1, 2, 3)$, where $\Delta D_j^{\hat{s}}$ is the mapping interval of IPDs to the embedding mode. $d_j^{\hat{s}}$ and $\overline{d}_j^{\hat{s}}$ refer to the upper and lower limits of the corresponding IPD interval, respectively, which should satisfy the following condition:

$$d_{j+1}^{\hat{s}} - \overline{d}_j^{\hat{s}} \geq 2\varepsilon, \quad (j = 0, 1, 2). \tag{3}$$

In our case, ε is set to 5 and the IPD interval with smaller probability is $\Delta D|p_{\min} = \{[40, 80], [140, 180]\}$. In our implementation, the mapping interval of steganographic embedding mode is set to $\Delta D_0^{\hat{s}} = [45, 55]$, $\Delta D_1^{\hat{s}} = [65, 75]$, $\Delta D_2^{\hat{s}} = [145, 155]$, and $\Delta D_3^{\hat{s}} = [165, 175]$, respectively, as shown in Figure 4.

Step 2: the synchronization IPD md is generated according to the selected mode M, by using the steganography synchronization function $F(\bullet)$, which can be represented as

$$md = F(M) = \text{rand}\lfloor d_M^{\hat{s}}, \overline{d}_M^{\hat{s}} \rfloor. \tag{4}$$

Step 3: as presented in Figure 5, the VoNR traffic is initially sent according to the synchronization IPD md. Then it is delivered according to the normal IPDs $d_i\,(i = 1, 2, \ldots)$ or the generated steganographic IPDs $sd_i\,(i = 1, 2, \ldots, m)$ successively.

4.2.3. *Steganography Decoding*

Step 1: the covert VoNR traffic is captured on the receiver side. Firstly, all the covert IPDs are calculated according to the timestamp, which may not be equivalent to the original one owing to the impact of network noise. Secondly, the initial IPD is extracted as the synchronization md'. The steganographic embedding mode M'can be recovered by

$$M' = \widetilde{F}(md') = j, \quad \text{if } d_j^{\hat{s}}(1 - \sigma_1) \leq md' \leq \overline{d}_j^{\hat{s}}(1 + \sigma_2), \ (j = 0, 1, 2, 3), \tag{5}$$

where $\widetilde{F}(\bullet)$denotes a predefined function used to attain the steganographic embedding mode. σ_1 and σ_2 refer to the intensity factor of antinoise, which can be set according to the distribution of network jitter $[-\varepsilon, +\varepsilon]$. The better capability of noise-resistance will be achieved by our scheme with larger σ_1 and σ_2, which should simultaneously satisfy the following conditions:

$$\begin{aligned} &\overline{d}_j^{\hat{s}}(1 + \sigma_2) \leq d_{j+1}^{\hat{s}}(1 - \sigma_1), \quad (j = 0, 1, 2), \\ &\overline{d}_j^{\hat{s}}\sigma_2 \geq \varepsilon, d_j^{\hat{s}}\sigma_1 \geq \varepsilon, \quad (j = 0, 1, 2, 3). \end{aligned} \tag{6}$$

Table 1: The main notations and symbols.

Notation	Description
Nor-IPDs	The normal VoNR IPDs
Syn-IPDs	The synchronization IPDs
Steg-IPDs	The steganographic IPDs
Jit < NorIPD >	The jittered normal VoNR IPDs
$[-\varepsilon, +\varepsilon]$	The main distribution of VoNR jitter
$\Delta D\vert p_{\max}$	The IPD interval with larger probability
$\Delta D\vert p_{\min}$	The IPD interval with smaller probability
$\Delta D_k^{\hat{e}}$	The mapping interval of IPDs to secret bit "0" or "1"
$d_k^{\hat{e}}, \overline{d}_k^{\hat{e}}$	The upper or lower limit of the corresponding IPD interval
s_i	The ith secret bit of industrial data
sd_i	The ith steganographic IPD
d_i	The ith normal VoNR IPD
M	The steganographic embedding mode
Interv	The interval of embedding sd_i into d_i
$\Delta D_j^{\hat{s}}$	The mapping interval of IPDs to embedding mode
$d_j^{\hat{s}}, \overline{d}_j^{\hat{s}}$	The upper or lower limit of the corresponding IPD interval
md	The generated synchronization IPD
σ_1, σ_2	The intensity factor of antinoise

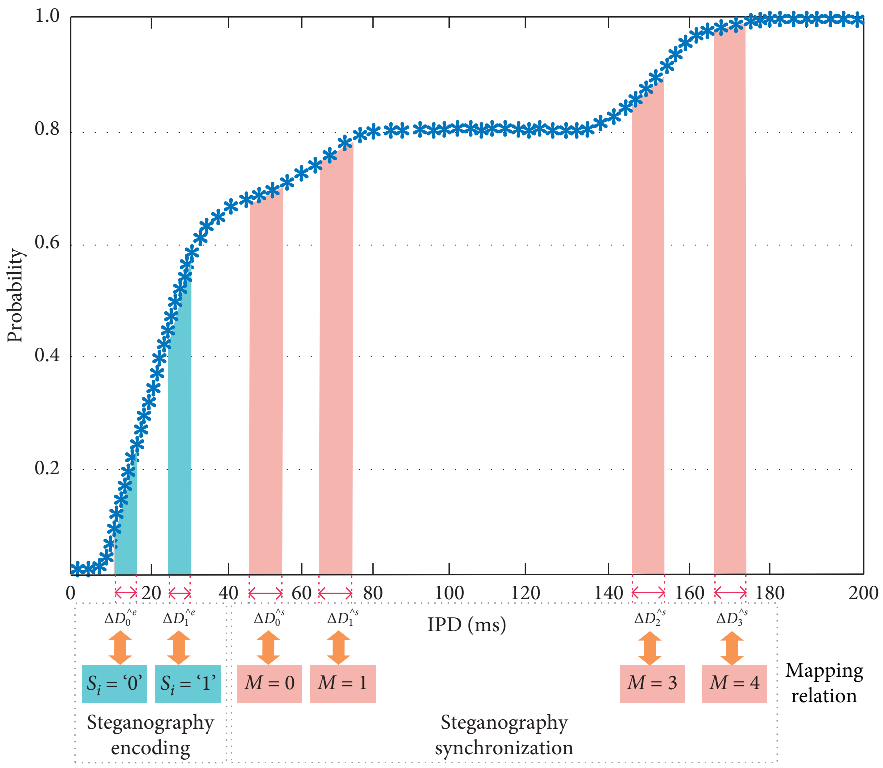


Figure 4: The CDF of Jit < NorIPD > and its corresponding mapping intervals of IPDs.

Step 2: the steganographic IPDs $sd_i'(i = 1, 2, \ldots, m)$ are extracted from the whole covert IPDs according to the interval $2^{M'}$. For the i^{th} steganographic IPD, the decoding function $D(sd_i')$ is defined in

$$s_i' = D(sd_i') = \begin{cases} 0, & \text{if } d_0^{\hat{e}}(1-\sigma_1) \le sd_i' \le \overline{d}_0^{\hat{e}}(1+\sigma_2), \\ 1, & \text{if } d_1^{\hat{e}}(1-\sigma_1) \le sd_i' \le \overline{d}_1^{\hat{e}}(1+\sigma_2). \end{cases} \quad (7)$$

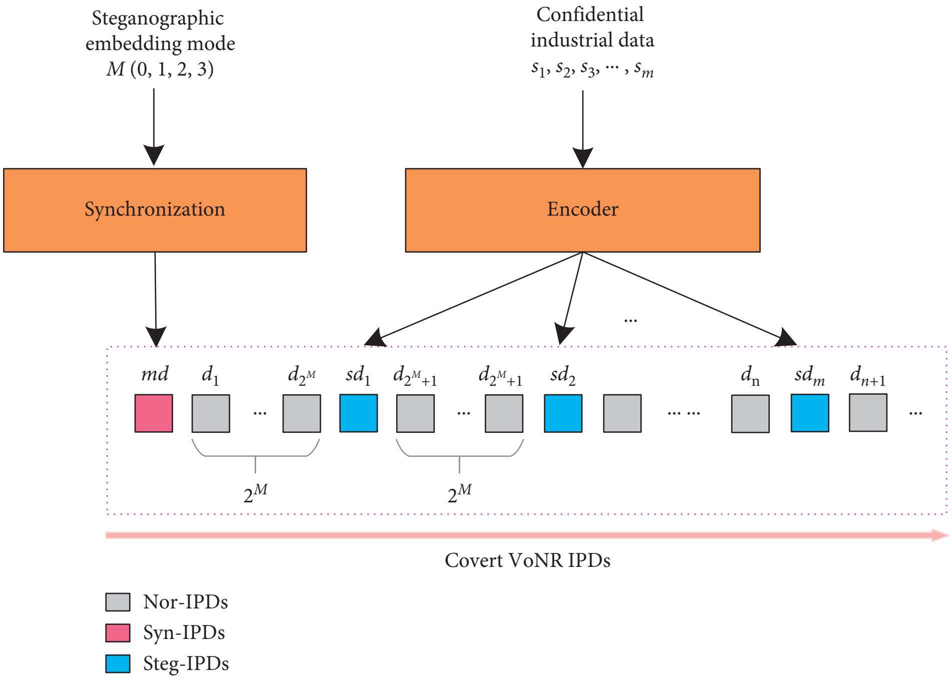


Figure 5: The covert VoNR IPDs generated by our scheme.

The confidential industrial data can be retrieved as $S' = \{s_i' \mid i = 1, 2, \ldots, m\}$.

5. Experiment Results and Analysis

5.1. Data Set and Implementation. In the experiment, our proposed scheme is implemented in a manufacturing enterprise under the scenario of Industrial Internet. The proprietary steganography software of our scheme is developed and deployed in the SCADA (Supervisory Control and Data Acquisition) system, where 5G network is utilized as the means of industrial data transmission. The normal VoNR traffic is captured during the legitimate 5G communication by using Huawei Mate30. The total number of the captured normal VoNR IPDs is 20,000. Then the confidential industrial data is modulated into the covert VoNR IPDs under four steganographic embedding modes, respectively, according to the aforementioned steps. From Figures 6–9, the original and jittered covert IPDs of our scheme are compared with those of the normal case under different modes. It can be seen that the original covert IPDs of our scheme slightly differ from those of the normal one, which seem like the noise-added normal IPDs. Meanwhile, it is manifested that the jittered covert IPDs of our scheme and the normal ones are mixed with each other, which can hardly be differentiated. Meanwhile, the covert IPDs become closer to the normal ones when the value of M is larger. The alteration of normal IPDs declines as the decrement of Steg-IPD embedding density. The VoNR traffic will inevitably suffer from network noise, such as jitter, packet loss, or disorder, during the transmission via the overt wireless channel. Moreover, only the noised VoNR traffic may be captured and analyzed by the network monitor device or an adversary. Thus, it should be noted that only the jittered case of normal or covert traffic is considered in this paper.

Further experiments are performed to evaluate the main performance metrics of the proposed scheme, which contain the undetectability, robustness, and capacity analysis.

5.2. Undetectability. As the core property, undetectability refers to the fact when the covert traffic cannot be differentiated from the normal one, which is all dependent on the similarity between the two. Therefore, in order to improve undetectability, the modulation of secret information cannot generate abnormal traffic or properties. Statistical-based steganalysis is the most common and popular method to detect the potential covert traffic, in which statistical properties such as traffic regularity or distribution function are exploited to distinguish the normal traffic and covert traffic.

In the experiment, the high-order statistical property-CDF of normal and covert IPDs are compared in Figure 10 under different steganographic embedding modes, where the x-axis shows the value of IPD ranging from 0 to 200 ms and y-axis represents the corresponding probability. It can be noticed that the CDF of our scheme is deviated slightly from the normal case when $M = 0$. Meanwhile, with the increase of embedding interval, the CDF of our scheme becomes closer to the normal one. In addition, it is obvious that the CDF of our scheme matches the normal one quite well when $M = 3$.

Meanwhile, two notable detection methods are employed to reckon the detection resistance of our scheme compared with Jitterbug [25] quantitatively, which are entropy test [5] and Kolmogorov-Smirnov test [28]. For normal and covert IPDs, they are both divided into 20 consecutive windows, the size of which is 1000. Certain

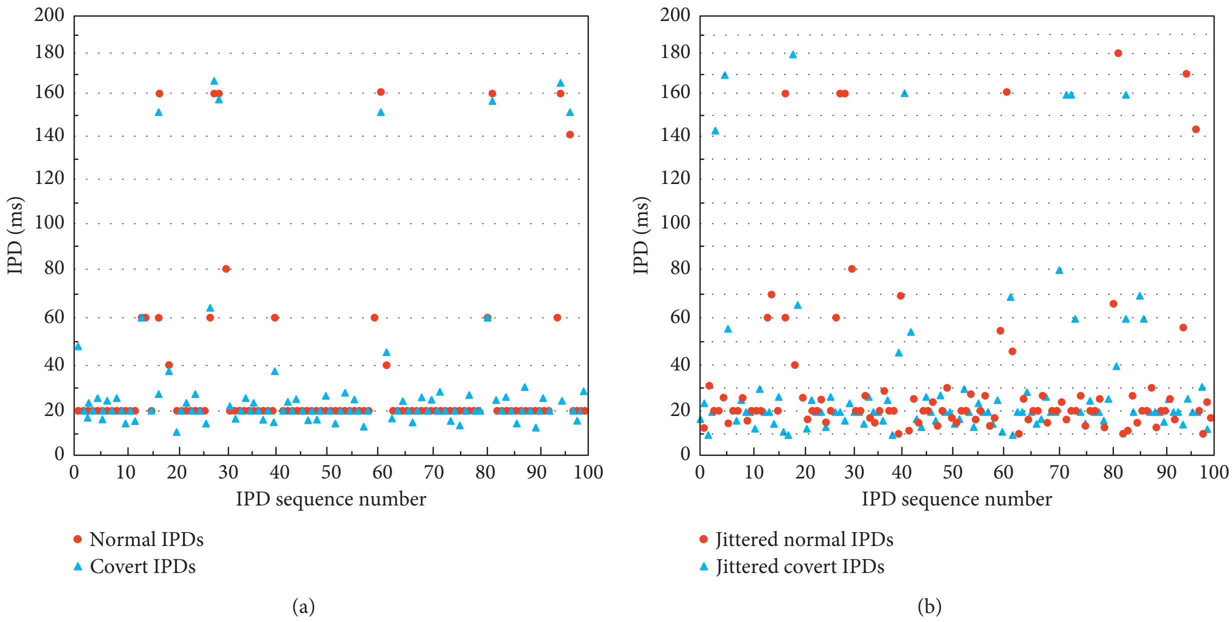


Figure 6: The comparison of VoNR IPDs between normal traffic and covert traffic of our scheme when $M = 0$. (a) VoNR IPDs. (b) Jittered VoNR IPDs.

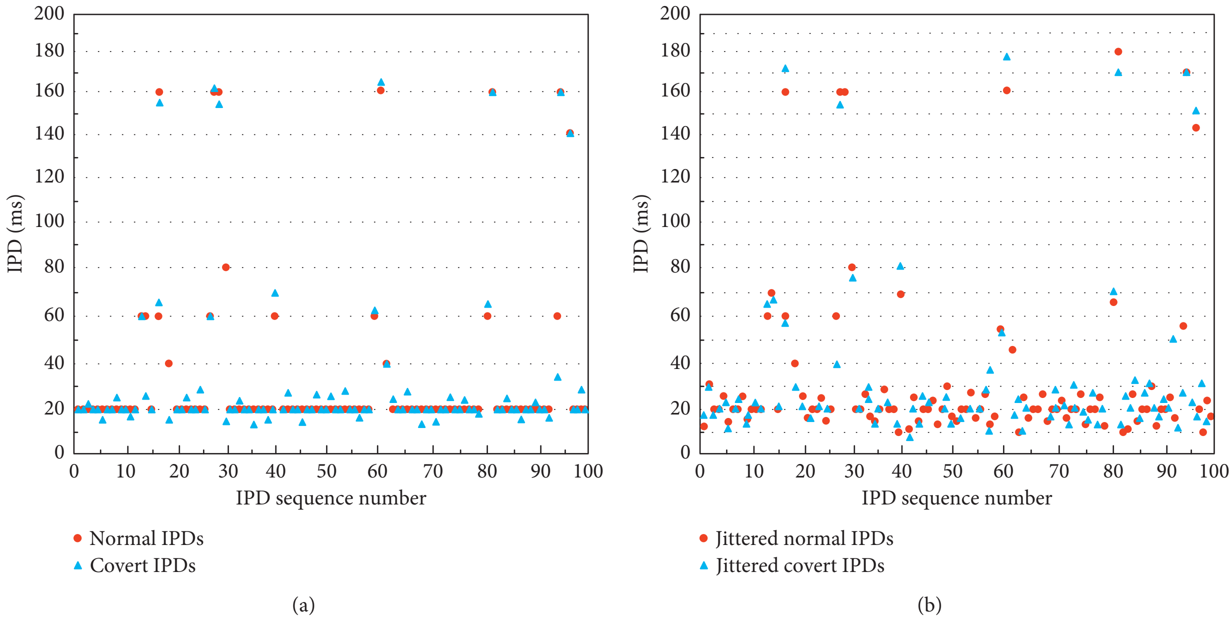


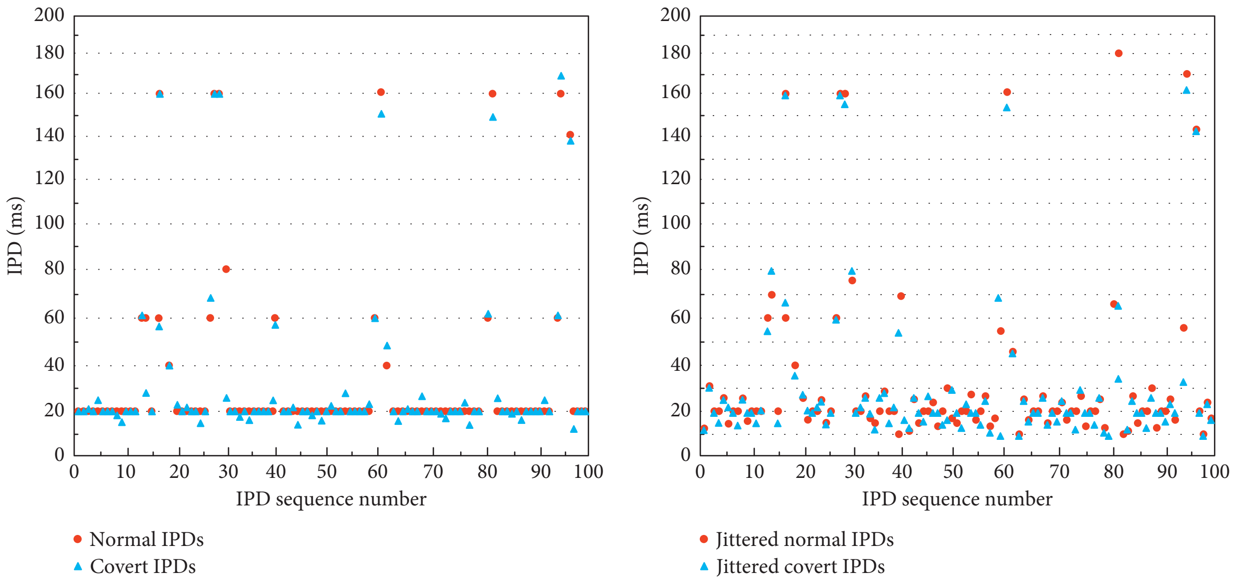
Figure 7: The comparison of VoNR IPDs between normal traffic and covert traffic of our scheme when $M = 1$. (a) VoNR IPDs. (b) Jittered VoNR IPDs.

statistical feature of each window is calculated and used during the detection process, as depicted in Figure 11.

5.2.1. Kolmogorov–Smirnov Test. The K-S test [28] 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 (K-S test value) is attained by taking the supremum of absolute difference between two empirical distribution functions for all x, which can be defined as

$$\text{KS} - \text{test} = \sup\left|S_1(x) - S_2(x)\right|, \tag{8}$$

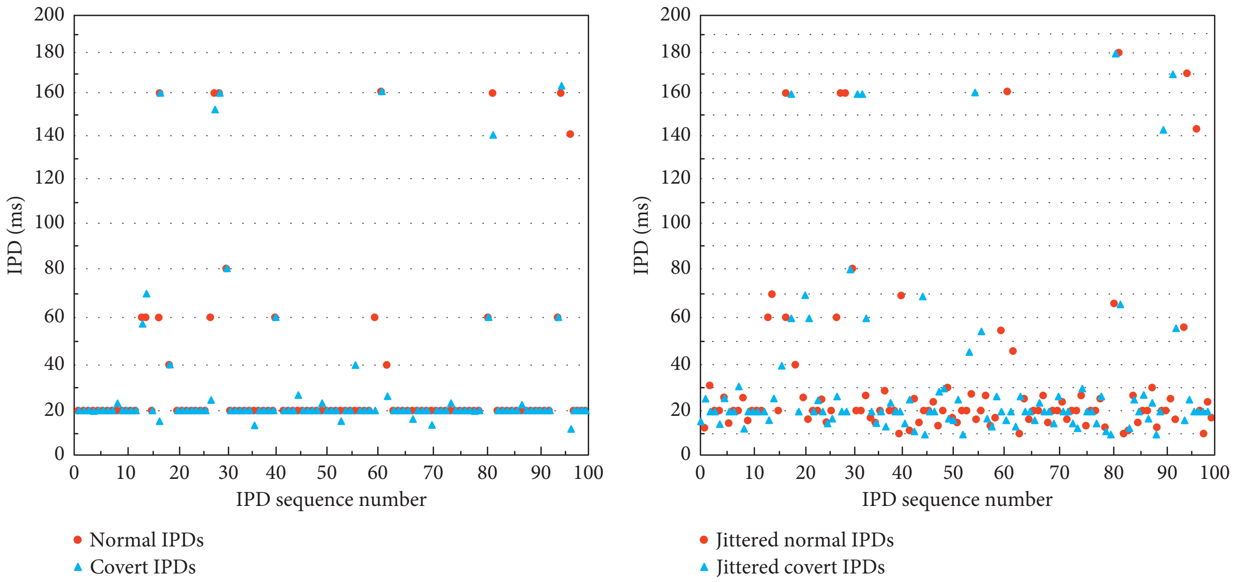
where $S_1(x)$ and $S_2(x)$ refer to the empirical distribution functions of two samples. The comparison of K-S test values between the normal and covert IPDs is shown in Figure 12.



(a)

(b)

Figure 8: The comparison of VoNR IPDs between normal traffic and covert traffic of our scheme when $M = 2$. (a) VoNR IPDs. (b) Jittered VoNR IPDs.



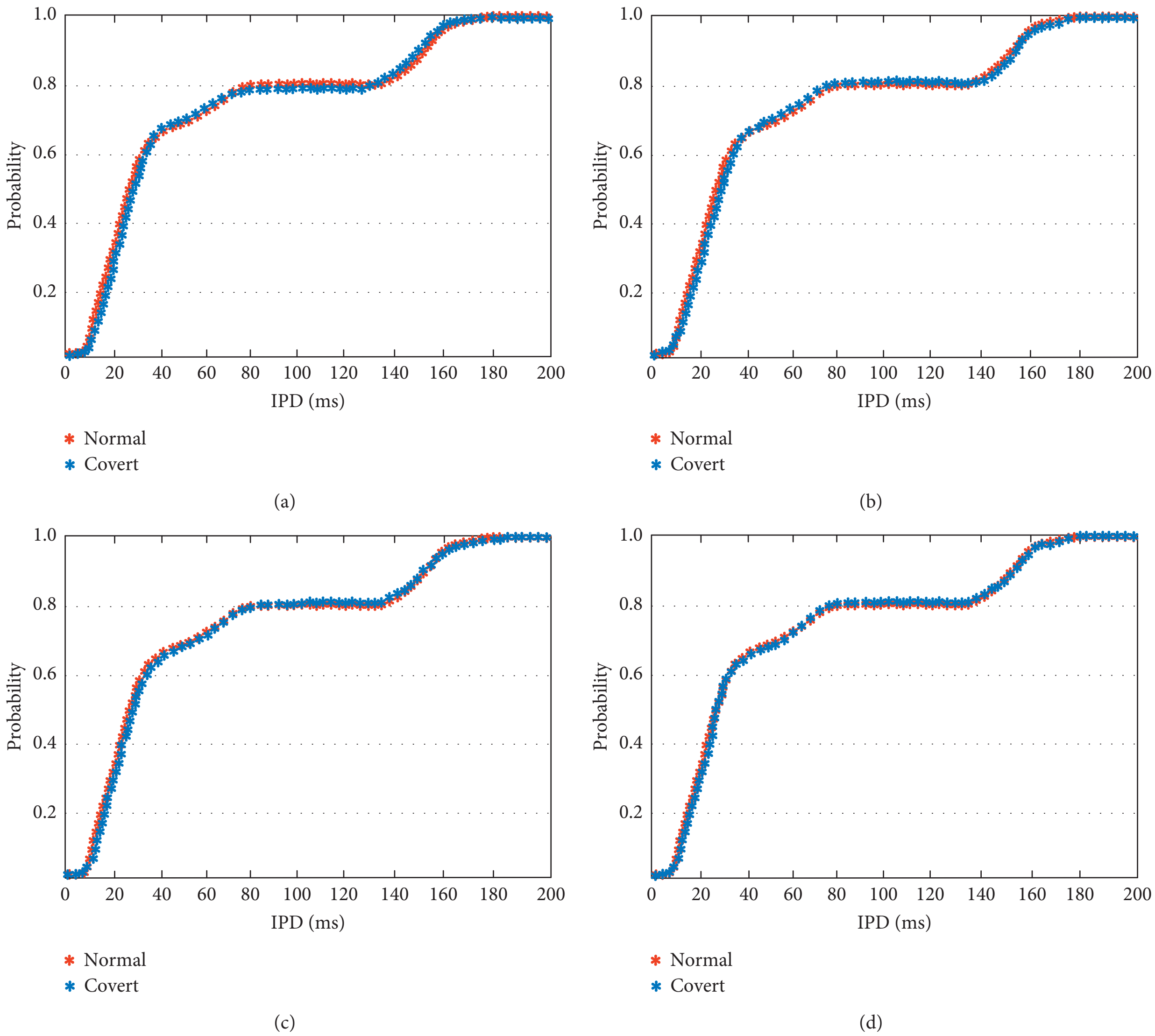
(a)

(b)

Figure 9: The comparison of VoNR IPDs between normal traffic and covert traffic of our scheme when $M = 3$. (a) VoNR IPDs. (b) Jittered VoNR IPDs.

Likewise, 20 windows of normal and covert traffic are tested in the experiment. The x-axis is the window number and y-axis shows the corresponding K-S test value. It is found that the K-S test values of our scheme are all below 0.15 under different modes and are 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 occur from 0.13 to 0.25, which are deviated from the normal case.

Then, the covert traffic is detected using the K-S test and the detection results are shown in Table 2, where the detection threshold is denoted as THD. It is observed that the false negative (FN) rate of the normal traffic declines when the threshold increases. FN refers to the normal sample



(a)

(b)

(c)

(d)

FIGURE 10: The comparison of CDF between the normal and covert IPDs of our scheme under different steganographic embedding modes. (a) $M = 0$. (b) $M = 1$. (c) $M = 2$. (d) $M = 3$.

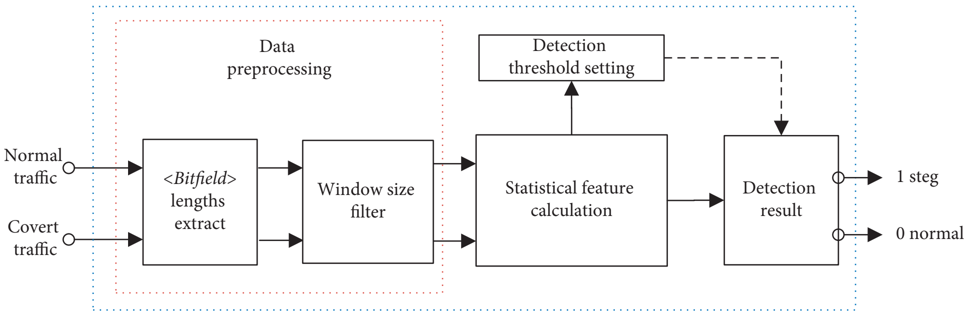


FIGURE 11: Block diagram of statistical-based detection process.

which is misclassified as the covert one. Hence, the detection threshold is set appropriately from 0.13 to 0.15 in order to guarantee that the false negative rate remains under 1%. Meanwhile, the true positive (TP) rates of covert samples are presented in the table. In this paper, the detection rate is represented by TP. From the results, it is easily seen that the detection rate of Jitterbug is more than 93% when tested with different thresholds. But in our case it is located under 3% for

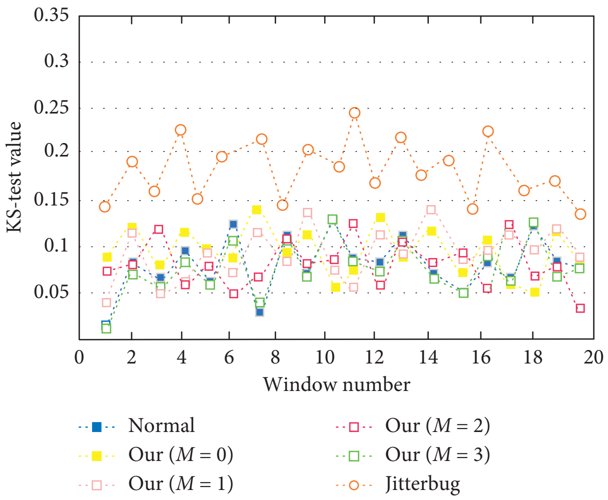


Figure 12: The comparison of K-S test values between normal traffic and covert traffic.

Table 2: The detection result of Kolmogorov–Smirnov test under different thresholds.

Detection result	TP (%)	FN (%)	TP (%)	FN (%)	TP (%)	FN (%)
Detection threshold	THD = 0.13		THD = 0.14		THD = 0.15	
Our scheme ($M = 0$)	0.03	0.01	0.02	0.00	0.01	0.00
Our scheme ($M = 1$)	0.02	0.01	0.01	0.00	0.00	0.00
Our scheme ($M = 2$)	0.02	0.01	0.01	0.00	0.00	0.00
Our scheme ($M = 3$)	0.01	0.01	0.00	0.00	0.00	0.00
Jitterbug	0.98	0.01	0.96	0.00	0.93	0.00

different modes, indicating that the Kolmogorov–Smirnov test cannot effectively detect the covert traffic generated by our scheme.

5.2.2. Entropy Test. Entropy can describe the degree of chaos in a process. In the entropy test (EN test), it is utilized to measure the regularity of data traffic [5]. If the traffic is less regular, the entropy value will be larger, and vice versa. Since the less regularity indicates more randomness, the big amount of information is contained in the traffic. The entropy value is obtained by calculating the statistical average of all possible self-information, which is denoted as

$$H(X) = E[I(x_i)] = -\sum_{i=1}^{n} p(x_i)\log p(x_i), \quad (9)$$

where X represents a one-dimensional discrete random variable, the set of values of which is $\Omega = \{x_i | i = 1, 2, \ldots, n\}$. The self-information of x_i is $I(x_i)$ and the probability of x_i is denoted as $p(x_i) = P\{X = x_i\}$. The entropy values of 20 windows for normal and covert IPDs are compared in Figure 13. From the result, it can be seen that most entropy values of normal IPDs range approximately from 0.45 to 1.24, whereas those of the covert IPDs generated by Jitterbug vary from 0.82 to 1.47. But the values of our scheme mix with those of the normal case under different modes, which can hardly be differentiated.

Subsequently, 20 windows of normal and covert IPDs are tested using theentropy test, respectively, when the window size is 1000. The results are presented in Table 3, where the detection threshold is denoted as THD. It is observed that the false negative rate of normal IPDs declines when the threshold increases. Meanwhile, the detection rates (true positive rates) of covert samples are shown in the table. We can see that the detection rate of Jitterbug ranges from 92% to 99%, while that of our scheme is only below 7%. Hence, the entropy test fails to distinguish the covert IPDs of our scheme from the normal ones. Therefore, it is indicated that our scheme possesses better undetectability than the existing methods.

5.3. Robustness. Robustness requires the covert communication to keep working with relatively high accuracy and low bit error rate (BER), resisting the perturbation of natural or malicious network noise. In the experiment, the robustness of our proposed scheme is reckoned in terms of network jitter, packet loss, and packet disorder, respectively. When suffered from network jitter, the BERs of the proposed scheme are attained under different intensity factors of antinoise (σ_1 and σ_2), compared with those of Jitterbug, as shown in Figure 14, where σ_1 and σ_2 are set to 2 to 5, respectively, satisfying the aforementioned condition. Since the BERs will remain consistent under different modes of our scheme, when the jitter noise of different power is injected into the covert traffic, the proposed scheme is implemented only when M is 0. 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

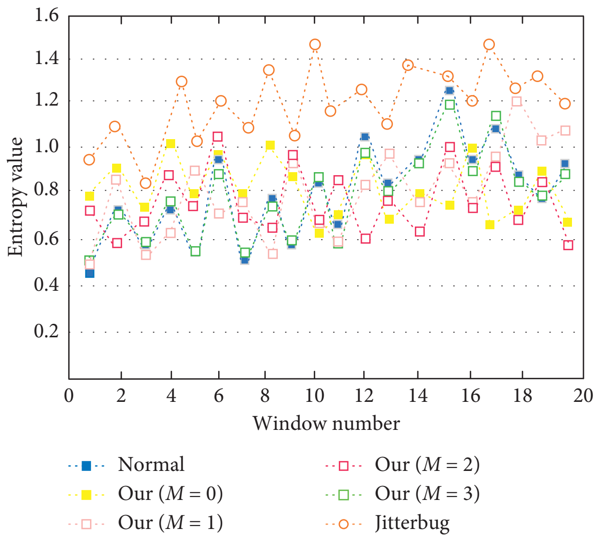


Figure 13: The comparison of entropy values between normal traffic and covert traffic.

Table 3: The detection result of the entropy test under different thresholds.

Detection result	TP (%)	FN (%)	TP (%)	FN (%)	TP (%)	FN (%)
Detection threshold	THD = 0.95		THD = 0.98		THD = 1.03	
Our scheme (M = 0)	0.07	0.09	0.04	0.07	0.02	0.04
Our scheme (M = 1)	0.06	0.09	0.02	0.07	0.01	0.04
Our scheme (M = 2)	0.04	0.09	0.01	0.07	0.00	0.04
Our scheme (M = 3)	0.02	0.09	0.00	0.07	0.00	0.04
Jitterbug	0.99	0.09	0.93	0.07	0.92	0.04

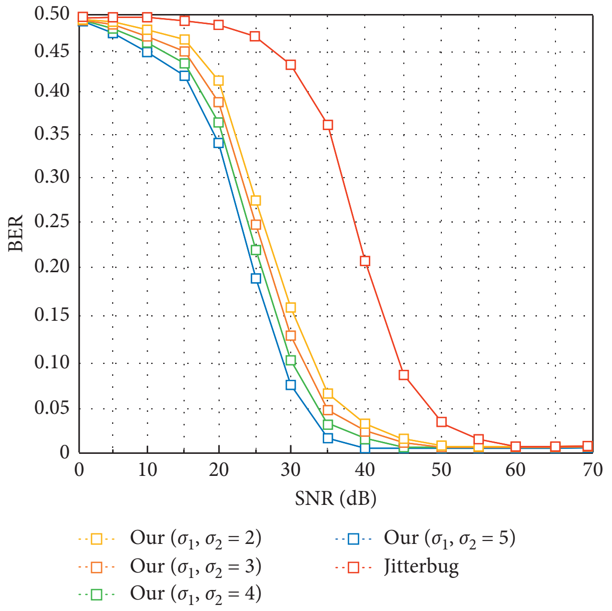


Figure 14: The comparison of BERs between our scheme and Jitterbug under different SNR.

SNR decreases. From the results, it can be seen that the BERs of our scheme decline with the increment of σ_1 and σ_2, as they become more noise-resistant. The SNR in our experiment ranges from 0 to 70 dB, while the natural SNR of VoNR in 5G network is about 40 to 45 dB. Under this circumstance, when σ_1 and σ_2 are set to 5, distortion raised by such jitter noise can be thoroughly tolerated in our scheme. Besides, it can also be observed that the BERs of our scheme vary from 2.1% to 3.6% when σ_1 and σ_2 are set to 2. Hence, our scheme can achieve relatively well accuracy when the SNR is above 40 dB. However, as for Jitterbug, the BER reaches up to 20%, which is much larger than that of the proposed scheme.

Then, the comparison of BERs between our scheme and Jitterbug is demonstrated in Figure 15 under different rates of packet disorder/loss when σ_1 and σ_2 are fixed to 5. It is obvious that the proposed scheme is more reliable with the increase of embedding interval. The confidential industrial data can be almost accurately obtained by our scheme under different modes when packet disorder rate is less than 3%. In addition, the BERs entirely locate under 6% in our scheme when 20% of the packets are lost. Meanwhile, the BER of Jitterbug increases sharply with the increment of packet disorder rate. The BER of Jitterbug reaches up to 12% when 20% of packets are lost, which will degrade the reliability of covert communication in Jitterbug (Figure 16).

5.4. Capacity. Capacity is the maximum data size that can be reliably transmitted over the covert channel per second or packet. In other words, capacity refers to the transfer rate of

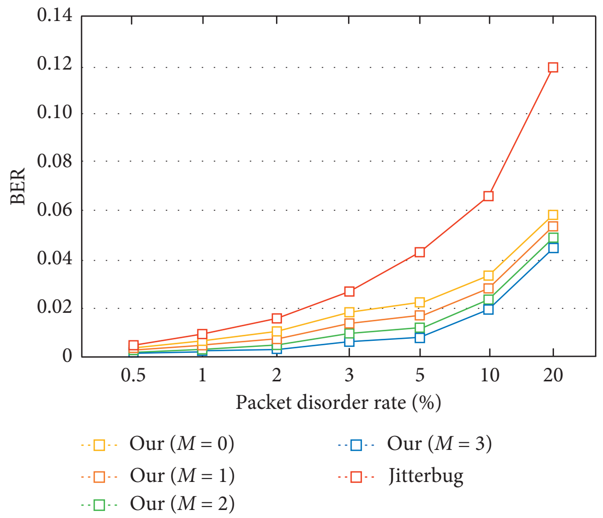


Figure 15: The comparison of BERs between our scheme and Jitterbug under different rates of packet disorder (σ_1 and $\sigma_2 = 5$).

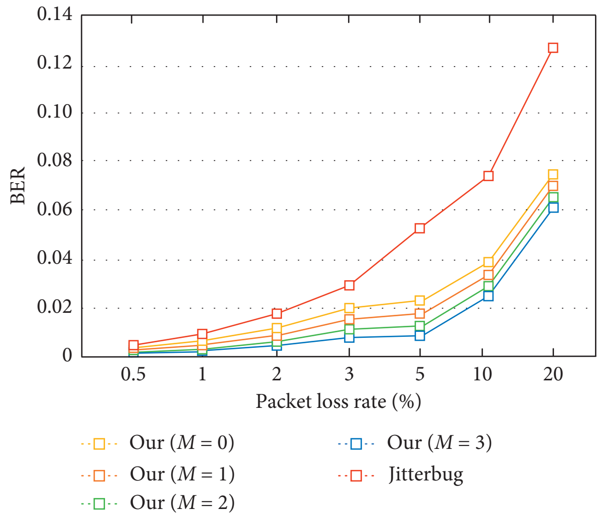


Figure 16: The comparison of BERs between our scheme and Jitterbug under different rates of packet loss (σ_1 and $\sigma_2 = 5$).

secret information. It is closely related to the bandwidth of normal carrier and the steganographic modulation algorithms. In this paper, capacity of our scheme under different steganographic embedding modes is measured by bit per packet (b/p), which can be calculated as

$$\mathrm{Cap}(M) = \frac{1}{(2^M + 1)}, \quad M = 0, 1, 2, 3. \tag{10}$$

Meanwhile, from the result presented in Figure 17, it is obvious that the capacity of our scheme declines when M becomes larger. However, better undetectability and robustness will be achieved under larger M. Since the embedding density of the secret information will be lower in the steganographic synchronization mode of larger interval, the modification of the normal carrier will be less. Thus, trade-off between the main performance metrics will be taken into

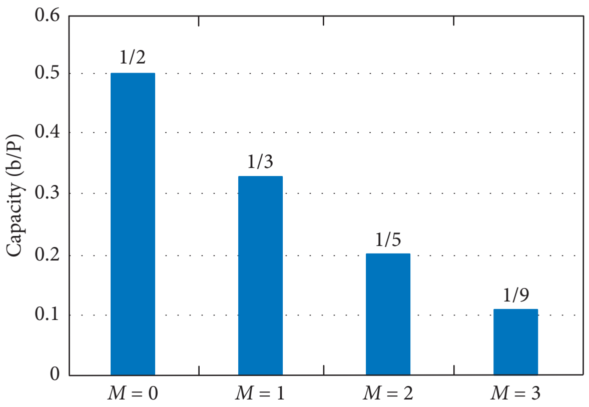


Figure 17: Capacity of the proposed scheme under different modes.

consideration in the future research. Then the optimal steganographic embedding mode can be analyzed and selected.

6. Conclusions

In this paper, under the scenario of Industrial Internet, a VoNR-IPD covert timing steganography based on 5G network is proposed in order to guarantee the secure transmission of confidential industrial data. The VoNR traffic is employed as the steganographic carrier to conduct covert communication in Industrial Internet. Interference of network jitter noise is fully considered and the high-order statistical properties of jittered VoNR traffic are imitated during the modulation of confidential industrial data. Thus, the generated covert IPDs can possess consistent statistical properties with the normal case in order to resist detection. Additionally, the synchronization mechanism of steganographic embedding mode is designed to control the embedding density of industrial data flexibly. Hence, our scheme has been proven to have better undetectability and robustness than the current methods. In the future work, another 5G-based steganographic algorithm will be designed and researched, in which trade-off between the main performance metrics will be taken into consideration. Then the optimal steganographic embedding mode can be analyzed and selected.

Data Availability

The software code data used to support the findings of this study are available from the corresponding author upon request (e-mail: wmq1989219@126.com).

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province under Grant no. 19KJB510019, Innovation and Entrepreneurship Training Program for College Students of Jiangsu Province under Grant no. 201913114004Y, Changzhou Key Laboratory of Industrial Internet and Data Intelligence under Grant no. CM20183002, and the Project of Changzhou Vocational Institute of Mechatronic Technology under Grant no. 2019-YBKJ-05.

References

[1] J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2386–2396, 2016.

[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] M. A. Elsadig and Y. A. Fadlalla, "Survey on covert storage channel in computer network protocols: detection and mitigation techniques," *International Journal of Advances in Computer Networks and Its Security*, vol. 6, no. 3, pp. 11–17, 2016.

[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] Y. Chen, J. Xiong, W. Xu, and J. Zuo, "A novel online incremental and decremental learning algorithm based on variable support vector machine," *Cluster Computing*, vol. 22, no. 8, pp. 7435–7445, 2019.

[6] Z. Zhang, Y. Li, C. Wang, M. Wang, Y. Tu, and J. Wang, "An ensemble learning method for wireless multimedia device identification," *Security and Communication Networks*, vol. 2018, no. 1, 9 pages, Article ID 5264526, 2018.

[7] Z. Pan, X. Yi, Y. Zhang, B. Jeon, and S. Kwong, "Efficient in-loop filtering based on enhanced deep convolutional neural networks for HEVC," *IEEE Transactions on Image Processing*, vol. 29, pp. 5352–5366, 2020.

[8] Y. Tu, Y. Lin, J. Wang, and J. Kim, "Semi-supervised learning with generative adversarial networks on digital signal modulation classification," *Computers Materials & Continua*, vol. 55, no. 2, pp. 243–254, 2018.

[9] W. Liu, G. Liu, J. Zhai, Y. Dai, and D. Ghosal, "Designing analog fountain timing channels: undetect-ability, robustness, and model-adaptation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 677–690, 2016.

[10] S. Gianvecchio, H. Wang, and D. Wijesekera, "Model based covert timing channels: automated modeling and evasion," *Lecture Notes In Computer Science*, Springer, vol. 5230, pp. 211–230, Berlin, Germany, 2008.

[11] R. Meng, S. G. Rice, J. Wang, and X. Sun, "A fusion steganographic algorithm based on faster R-CNN," *Computers Materials & Continua*, vol. 55, no. 1, pp. 1–16, 2018.

[12] X. Zhang, C. Liang, Q. Zhang, Y. Li, J. Zheng, and Y.-a. Tan, "Building covert timing channels by packet rearrangement over mobile networks," *Information Sciences*, vol. 445-446, pp. 66–78, 2018.

[13] X. Zhang, L. Zhu, X. Wang, C. Zhang, H. Zhu, and Y.-A. Tan, "A packet-reordering covert channel over VoLTE voice and video traffics," *Journal of Network and Computer Applications*, vol. 126, pp. 29–38, 2019.

[14] J. Liu, C. Gu, J. Wang, G. Youn, and J.-U. Kim, "Multi-scale multi-class conditional generative adversarial network for handwritten character generation," *The Journal of Supercomputing*, vol. 75, no. 4, pp. 1922–1940, 2019.

[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] A. Houmansadr and N. Borisov, "CoCo: coding-based covert timing channels for network flows," in *Proceedings of the 13th International Conference on Information Hiding*, pp. 314–328, Prague, Czech Republic, May 2011.

[17] J. Lei, J. Sun, Z. Pan, S. Kwong, J. Duan, and C. Hou, "Fast mode decision using inter-view and inter-component correlations for multiview depth video coding," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 4, pp. 978–986, 2015.

[18] J. Lei, D. Li, Z. Pan, Z. Sun, S. Kwong, and C. Hou, "Fast intra prediction based on content property analysis for low complexity HEVC-based screen content coding," *IEEE Transactions on Broadcasting*, vol. 63, no. 1, pp. 48–58, 2017.

[19] R. Sun, L. Shi, C. Yin, and J. Wang, "An improved method in deep packet inspection based on regular expression," *The Journal of Supercomputing*, vol. 75, no. 6, pp. 3317–3333, 2019.

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

[21] J. Yao, K. Zhang, Y. Dai, and J. Wang, "Power function-based signal recovery transition optimization model of emergency traffic," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 7003–7023, 2018.

[22] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based covert timing channels: automated modeling and evasion," in *Proceedings of the Conference on Recent Advances in Intrusion Detection*, pp. 211–230, Cambridge, MA, USA, September 2008.

[23] X. Zhang, L. Guo, Y. Xue, and Q. Zhang, "A two-way VoLTE covert channel with feedback adaptive to mobile network environment," *IEEE Access*, vol. 7, pp. 122214–122223, 2019.

[24] G. Shah, A. Molina, and M. Blaze, "Keyboards and covert channels," in *Proceedings of the 2006 USENIX Security Symposium*, pp. 59–75, San Jose, CA, USA, July 2006.

[25] J. Wang, C. Ju, Y. Gao, A. K. Sangaiah, and G.-j. Kim, "A PSO based energy efficient coverage control algorithm for wireless sensor networks," *Computers Materials & Continua*, vol. 56, no. 3, pp. 433–446, 2018.

[26] G. Liu, J. Zhai, and Y. Dai, "Covert timing channel with distribution matching," in *Proceedings of the International Conference on Multimedia Information Networking and Security*, pp. 565–568, Wuhan, China, November 2009.

[27] S. Gianvecchio and H. Haining 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.

[28] J. Wang, Y. Gao, W. Liu, W. Wu, and S. Lim, "An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks," *Computers, Materials & Continua*, vol. 58, no. 3, pp. 711–725, 2019.