IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 9, 2019, accepted September 23, 2019, date of publication October 3, 2019,
date of current version October 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2945320

An Enlarging-the-Capacity Packet Sorting Covert Channel

LEJUN ZHANG[1], TIANWEN HUANG[1], WAQAS RASHEED[1], XIAOYAN HU[1], AND CHUNHUI ZHAO[1,2]

[1]College of Information Engineering, Yangzhou University, Yangzhou 225127, China
[2]College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China

Corresponding author: Chunhui Zhao (zhaochunhui@hrbeu.edu.cn)

This work was supported in part by the Natural Science Foundation of Heilongjiang Province of China under Grant LC2016024, the Natural Science Foundation of the Jiangsu Higher Education Institutions under Grant 17KJB520044 and Six Talent Peaks Project in Jiangsu Province XYDXX-108.

ABSTRACT The construction method of the covert channel has always been a topic of research and exploration in the field of information security, and the use of IP data packets for covert channel construction is also an important method. Based on the above content, this paper proposes an enlarging-the-capacity packet sorting covert channel. We establish enlarging-the-capacity packet sorting covert channel model and derive the functional relationship between the total number of covert information transmitted and the number of ports. This method can send more secret information when the network status is not ideal. The simulation results show that the covert channel of the extended packet sorting has high performance in different packet loss rates and delays, and is superior to other IP covert channel.

INDEX TERMS Information security, information hiding, inter-packet interval covert channel, packet sorting covert channel.

I. INTRODUCTION

A covert channel in a network refers to the transmission of secret information using a portion of the system that is not transmitting data. In 1973 [1], Lampson proposed the concept of covert channels originally. In 1996, Handel et al. introduced covert channels into computer networks [2], [3].

Unlike traditional secret information transmission methods, covert channels not only hide the content of the transmission but also protect transfer path. Existing network covert channels are divided into covert storage channel [4]–[9] and covert timing channel [10]–[14].

This paper mainly studies the covert timing channel, which means that the sender embeds information into time-related parameters. Both parties send and receive secret messages through preset rules, such as rate of change, sequence, interval, and other time parameters [15]–[20].

Tan *et al.* [21] proposed using packet interval in mobile networks to construct covert channel in IoT. Kro?sche *et al.* [22] analyzed the OpenFlow workflow and found that the OpenFlow controller can implement the timing covert channel and solve the time synchronization problem in the model. El-Atawy *et al.* [23] proposed a novel covert channel technique by using the packet reordering phenomenon, dynamically manipulate packet order into sending secret information.

By studying the data packet arrival sequence, when the packet sequencing packet losses or packet arrives at the wrong ordering, it will not express any secret information. As when the packet is lost, the remaining packet sorting will not be able to express the correct secret information. When an error occurs in the order in which the packets arrive, the remaining packet sorting will not be able to express the secret information accurately.

This paper proposes an enlarging-the-capacity packet sorting covert channel. When using packet sorting to transmit secret information, another set of secret information is carried using the time interval in these packets. When using the packet sorting secret transmission information without changing the order of transmission of packets, the time interval between each data packet is modified, and the purpose of transmitting the secret information at the time interval of using the data packet is achieved.

The proposed method in this paper can increase the total amount of secret information transmitted when there is no error in the order of arrival of the data packet and can transfer

The associate editor coordinating the review of this manuscript and approving it for publication was Aniello Castiglione.

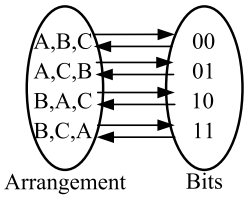


FIGURE 1. A mapping of packet arrangement and data in a covert channel based on packet sorting.

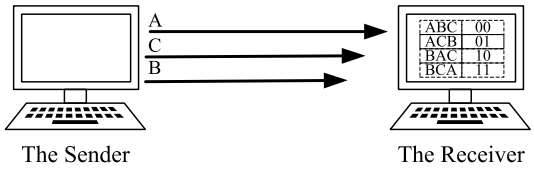


FIGURE 2. An example of a covert channel transmission based on packet sorting.

part of the secret information when the order of appearance of the data packet is wrong.

II. RELATED WORKS

A. IP COVERT CHANNEL MODEL BASED ON PACKET INTERVAL

The principle of data transmission based on the IP covert channel of the inter-packet interval is as follows. When there are $m + 1$ data packets in the communication process, there are time intervals of $T_1, T_2, \cdots, T_m$. Among them, M various values represent M different bits of information [24]. The receiver can judge the time difference between data arrival before and after arrival within a certain error to obtain the secret information.

If the communicating parties have agreed on two different time intervals S_1 and S_2, respectively, the bit "0" and the bit "1" are indicated. In four-time intervals T_1, T_2, T_3, and T_4, select S_1 or S_2 to transmit secret data in different time intervals.

B. IP COVERT CHANNEL MODEL BASED ON PACKET SORTING

The principle of the IP covert channel model of packet sorting is that based on the time sequence of the data packets arriving at the port, the corresponding secret information is converted [25], [26]. The sender and the receiver first specify multiple transmit ports and one receive port, and they establish a connection in turn. The receiver will sort the corresponding ports based on the order in which the data packets arrive, and it will read the secret data through the lookup mapping table.

If n bits of data are transmitted in each round, and the communication parties establish m connections, there are $m!$ different possible situations, and to be able to completely transmit data in the order of arrival of the data packets, $m! \geq 2^n$ must be satisfied. If the two parties establish three connections in turn, they can form 6 possible cases according to the order of transmission. However, to ensure the integrity of the total amount of data, only two possible cases can be used to represent 2 bits of data. If three ports are used to transmit data packets to represent 3 bits for each round, some data will not be represented. Fig. 1 is a mapping of packet arrangement and data in IP covert channel based on packet sorting.

Fig. 2 shows an example of the IP covert channel transmission based on packet sorting. It can be seen that the receiver obtains the data to be acquired by retrieving the mapping table according to the order in which the port data arrive.

III. SCHEME

A. BASIC IDEA OF THE SCHEME

This paper designs an enlarging-the-capacity packet sorting covert channel, modifying the time interval of packet transmission in IP covert channel based on packet sorting and using different time intervals to transmit data. Packet sorting is used to transmit secret information, but there is also an interval between each packet. Thus, these intervals can be used to transmit a set of data so that when the number of ports is constant, more hidden information can be transmitted.

B. THE SENDER DESIGN

Supposed that n is the number of sender ports and that the receiver has a port. When transmitting secret information, n ports of the sender are sorted according to the secret information, and then the data packet is sent to the receiving port. The receiver listens to the receiving port, receives the packets sent by n ports, and gets the secret information according to the sequence of packets sent by different ports.

During the data transmission, it is necessary to determine the secret information bit value m', corresponding to a port arrangement at the sender's end, and the total number of ports n and the bit value m' should meet at $n! \geq 2^{m'}$, which can be summarized as:

$$m' = \lfloor log_2 n! \rfloor \tag{1}$$

The sender has n ports, communicating with receiver's ports in turn, and n time intervals are used to transmit secret information (there is a starting data packet). It is necessary to determine the secret information bit value m'', corresponding to a time interval in the transmitting end, and the total number of time intervals n and the bit value m'' need to satisfy $n \geq 2^{m''}$, which can be summarized as:

$$m'' = \lfloor log_2 n \rfloor \tag{2}$$

After determining the port number n, the secret information bit value m' corresponding to the port arrangement mode and the secret information bit value m'' corresponding to a time interval, it is necessary to confirm the relationship tables, and finally, the secret data can be transmitted.

For improved covert channel based on packet sorting, the different secret information represents different interval time,and each interval time is $t_2, 2t_2, \cdots, 2^{\lfloor log_2 n \rfloor} \cdot t_2$.

When sending a message, the sender first processes the secret message *serectmessage*1 and the secret message *serectmessage*2 respectively, and determines that the secret message *serectmessage*1 transmits m' bits per round and the secret message *serectmessage*2 transmits nm'' bits per round. Then the sender establishes the port sequence and the corresponding relationship table *rel1* for each round of transmission bit m' and establish the time interval and the corresponding relationship table *rel2* for each round of transmission bit m''.

The encoding method of *rel1* is that n sending ports are $P_1, P_2, \cdots, P_n$, and the secret information sent in each round is $\underbrace{00\cdots0}_{m'} \sim \underbrace{11\cdots1}_{m'}$. Therefore, the correspondence between the port arrangement order and the secret information can be established, that is, $P_1P_2\cdots P_{n-1}P_n = \underbrace{00\cdots0}_{m'}$, $P_1P_2\cdots P_nP_{n-1} = \underbrace{00\cdots1}_{m'}, \cdots, P\cdots P = \underbrace{11\cdots1}_{m'}$.

The specific encoding mode of *rel2* is: the secret information sent by each round is $\underbrace{00\cdots0}_{m''} \sim \underbrace{11\cdots1}_{m''}$, corresponding to the interval time of $t_2, 2t_2, \cdots, 2^{m''}t_2$. Therefore, the correspondence between interval time and secret information can be established, denoted as $t_2 = \underbrace{00\cdots0}_{m''}$, $2t_2 = \underbrace{00\cdots1}_{m''}, \cdots, 2^{m''}t_2 = \underbrace{11\cdots1}_{m''}$,.

Pseudo-code of the sender is given in Algorithm 1.

Algorithm 1 Pseudo Code of the Sender

```
1:  function main( )
2:      read n, m', m'', rel1, rel2
3:      socketconnet(n)
4:      send(startframe)
5:      message1 ← openfile("serectmessage1")
6:      message2 ← openfile("serectmessage2")
7:      while *message1 ≠ ' \ 0' do
8:          strncpy(smsg1, message1, m')
9:          strncpy(smsg2, message2, nm'')
10:         sendInf(smsg1, smsg2, rel1, rel2)
11:         message1 ← message1 + m'
12:         message2 ← message2 + nm''
13:     end while
14:     closeallconnect(n)
15: end function
16:
17: function sendInf(smsg1, smsg2, rel1, rel2)
18:     port[n] ← findfrommap(smsg1, rel1)
19:     sleeptime[n] ← findfrommap(smsg2, rel2)
20:     for i ← 0 to n do
21:         sleep(sleeptime[i])
22:         sendtoserver(port[i])
23:     end for
24: end function
```

The encoding hiding process of the sender is as follows:

1)The sender establishes socket connections with the designated port of the receiver on n ports, and divides each m' bits of secret information *message*1 into a group of message *smsg*1, and each nm'' bits of secret information *message*2 into a group of message *smsg*2. The two groups of information to be sent are sliced and prepared for sending.

2) According to relational table *rel*1, we can find that the arrangement of n sends ports which correspond to *sendmessage*1, and sends time interval which correspond to *sendmessage*2. Then sleep for a specified time before specifying the sending port to send a packet.

C. THE RECEIVER DESIGN

The process received by the receiver is the inverse of the sender's hidden process.

A correspondence table *rel3* of the interval time and the transmission bit nm'' of each round is established. As the network has a delay, the time corresponding to the receiving end should be a time range. The solution has high requirements for delay jitter in the network, and the average delay jitter is t_d. The time range of the receiving end is set to $t - t_d \le t < t + t_d$.

The relationship table *rel3* is set to $[0, t_2 + t_d) = \underbrace{00\cdots0}_{m''}$, $[2t_2 - t_d, 2t_2 + t_d) = \underbrace{00\cdots1}_{m''}, \cdots, [2^{\lfloor \log_2 n \rfloor} \cdot t_2 - t_d, 2^{\lfloor \log_2 n \rfloor} \cdot t_2 + t_d) = \underbrace{11\cdots1}_{m''}$.

Pseudo-code of the receiver is given in Algorithm 2.

The decoding process of the receiver is as follows:

1) The receiver monitors n socket connections at specified ports and decodes after receiving the start frame.

2) The receiver forms a port sequence *port*[n] according to the time the packet arrives, then find *rel*2 and convert it into m' bits secret information *recvmsg*1.

3) The time interval *intervaltime* exists in each sorting port, and the receiver finds *rel*3 and converts it to m'' bits secret message *recvmsg*2.

IV. COMPARISON

A. TRANSFER OF SECRET INFORMATION AND PACKETS USED

Fig. 3 shows the relationship between the numbers of ports and packets used to transmit the secret information before and after the secret information is added.

When no improvement is made, the relation between the number of ports and the secret information bit m_1 is to satisfy $n! \ge 2^{m_1}$. In other words, the hidden information that can be expressed by this set of ports is $m_1 = \lfloor \log_2 n! \rfloor$, and the improved time between different packets can represent different information. For a set of ports to fully express information, the relationship between the number of ports n and the secret information bit m_2 of the packet interval should be $n \ge 2^{m_2}$, that is, the secret information transmitted during a time interval is $m_2 = \lfloor \log_2 n \rfloor$, and the secret information

Algorithm 2 Pseudo Code of the Receiver

```
function main
    read n, rel1, rel3
    bind(listeningport)
    if recvmessage(startframe) then
        starttime ← gettimenow()
        while 1 do
            recvfrom(clientport)
            handlemessage1(clientport, rel1, n)
            handlemessage2(rel3)
        end while
    end if
end function

function handlemessage1(clientport, rel1, n)
    strcat(port, clientport)
    if strlen(port) = n then
        recvmsg1 ← findfrommap(port, rel1)
        savemessage(recvmsg1)
        port ← ′ \ 0′
    end if
end function

function handlemessage2(rel3)
    intervaltime ← gettimenow()−starttime
    recvmsg2 ← findfrommap(intervaltime, rel3)
    savemessage(recvmsg2)
    starttime ← gettimenow()
end function
```

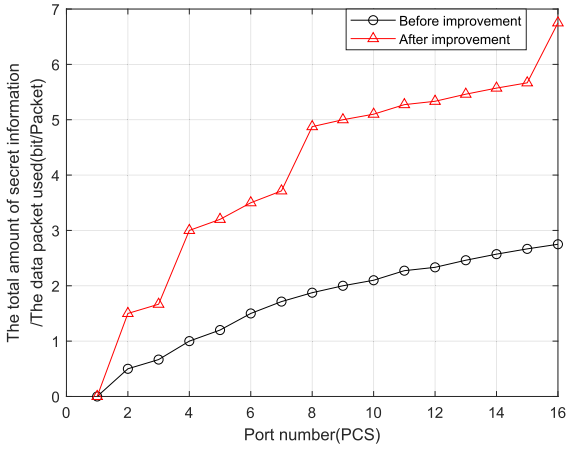


FIGURE 3. The ratio of the total amount of secret information and the data packet used before and after the secret information is added to the packet interval.

expressed by a time interval in a set of ports is $n\lfloor\log_2 n\rfloor$. Therefore, the total amount of transmitted secret information:

$$m = n * \lfloor\log_2 n\rfloor + \lfloor\log_2 n!\rfloor \tag{3}$$

It can be obtained that the ratio of the transmitted secret information before adding the secret information to the packet interval is $\lfloor\log_2 n!\rfloor/n$. From (3), the ratio of the transmitted

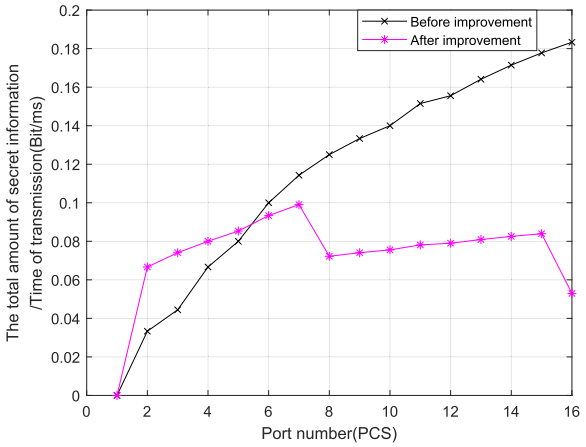


FIGURE 4. The ratio of the total amount of secret information and time of transmission before and after the secret information is added to the packet interval.

secret information after adding the secret information to the packet interval is:$\left(n\lfloor\log_2 n\rfloor + \lfloor\log_2 n!\rfloor\right)/n$.

Overall, it can be seen that the total number of secret information transmitted after improvement is much higher than that without improvement. After improvement, when the result $\log_2 n$ is rounded down, the performance becomes better.

B. THE RATIO OF TRANSMITTED SECRET INFORMATION TO TRANSMISSION TIME

Fig. 4 shows the relationship between the number of ports and the transmission time of secret messages transmitted at different packet intervals.

Before the improvement, while the interval between the data packets does not represent the secret information, the interval between the data packets is fixed.

After the improvement, the interval between the packets is used to represent the secret information. To distinguish different secret information, it is necessary to set different time into equal difference series in this paper. Due to the transmitted information, the probability of occurrence of the bit '0', '1' is the same. Therefore, the time spent on the improvement in the above figure is the average of all possible times.

Different information is indicated due to the use of different inter-packet intervals. When the difference between different time sets is small, the ratio of the secret information transmitted to the transmission time at different packet intervals is higher, which means that less time is required to transmit a certain amount of secret information.

The IP covert channel based on packet sort sets the time interval of sending packets to each port as t_1, and the time T' is the time it takes to transmit a set of secret information:

$$T' = n \cdot t_1 \tag{4}$$

The improved IP covert channel based on packet sorting. Different secret information represents different interval time, and each of them is t_2, $2t_2$, $\cdots$, $2^{\lfloor log_2 n\rfloor} \cdot t_2$. Assuming that each interval has the same probability,

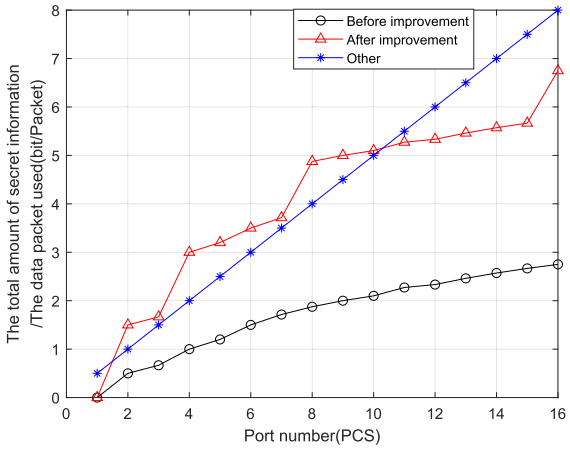


FIGURE 5. Comparison with another covert channel.

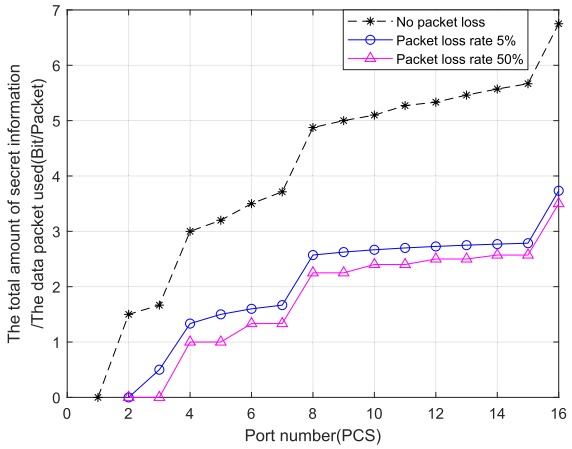


FIGURE 6. The ratio of the total amount of secret information and the data packet used in different packet loss rate.

the average time for transmitting a set of secret information is $\left[2^{\lfloor log_2 n \rfloor} \cdot t_2 + 2^{\lfloor log_2 n \rfloor}(2^{\lfloor log_2 n \rfloor} - 1) \cdot t_2/2\right]/2^{\lfloor log_2 n \rfloor}$, and the simplification is $\left[1 + \left(2^{\lfloor log_2 n \rfloor} - 1\right)/2\right] \cdot t_2$, then the time T for transmitting a set of secret information is:

$$T = \left[1 + \frac{\left(2^{\lfloor log_2 n \rfloor} - 1\right)}{2}\right] \cdot t_2 \cdot n \tag{5}$$

From (4), before adding confidential information between packets, the ratio of the secret information transmitted to the port number and the different packet interval time is $\lfloor \log_2 n! \rfloor/(n \cdot t)$. From (3) and (5), after the secret information is added between the packets, the number of ports and the interval between different packets are transmitted. The ratio of the hidden information to transmission time is $\left(n \lfloor \log_2 n \rfloor + \lfloor \log_2 n! \rfloor\right) / \left(n \cdot t \cdot [1 + (2^{\lfloor \log_2 n \rfloor} - 1)/2]\right)$.

C. COMPARISON WITH ANOTHER COVERT CHANNEL

Another covert channel is to obtain secret information by determining whether or not a packet arrives to identify a bit "1" or a bit "0" within a fixed time interval [10], [16]. The authors think that the bit "1" and the bit "0" in the secret information are randomly appear. while the port transmission packet indicates the bit "1", the port does not transmission packet indicates that the bit "0", so each packet can represent 0.5 bit hidden information. As can be seen in Fig. 5, an enlarging-the-capacity packet sorting covert channel is superior to the method described above. When the number of ports is 2-10, the number of hidden information carried by one data packet in the method is larger than that of the method presented above.

To sum up, this model transmits a group of secret information by using the sorting of ports and transmits another group of secret information by using packet time interval. These two different channels only use a set of data packets, so its carrier utilization is higher. However, because different time intervals are used to represent different secret information, when the number of ports is increased, the number of time intervals is increased, which can represent more secret information. In order to represent different secret information, different time intervals are needed, which will increase the time of transmitting a group of secret information and reduce the bandwidth of this model.

V. PERFORMANCE ANALYSIS

A. PACKET LOSS RATE

Fig. 6 shows the relationship between the number of ports and the ratio of secret information transmitted at different packet loss rates to the total number of packets used.

The ratio of the number of ports and the secret information transmitted when the packet is lost to the total number of packets used is $\left[\lfloor \log_2 n \rfloor \cdot (\lfloor n(1-p) \rfloor - 1)\right]/[n(1-p)]$, where p is packet loss rate, and the packet loss rate is set to a specific probability for each port to be lost. When transmitting confidential information, it is agreed that the port where the packet loss occurs is continuous, that is, if there are 8 ports to send, and 5 ports have lost packets, the 5 ports are continuous, so there are still two ports that can represent the secret information. It is also agreed that even if packet loss occurs, the time taken by the packets and sent by this group of ports does not change (using UDP).

When a port generates lost packets, the port arrangement cannot indicate hidden information. However, the port interval can still indicate a part of the secret information. It can be seen from the figure that the higher the packet loss rate is, the lesser confidential information can be transmitted.

Fig. 7 shows the relationship between the number of ports and the ratio of hidden information to transmission time transmitted at different packet loss rates.

The ratio of the number of ports and secret information that is lost to the total number of packets used is $\left(\lfloor \log_2 n \rfloor\right) \cdot (\lfloor n(1-p) \rfloor - 1)/\left(n \cdot t \cdot [1 + (2^{\lfloor \log_2 n \rfloor})]\right)$, where p is the rate of packet loss.

When a packet is lost on a port, the port arrangement can not indicate hidden information, but the port interval can still represent some secret information. It can be seen from the figure that the higher the packet loss rate is, the lesser hidden information can be represented within a certain period of time.

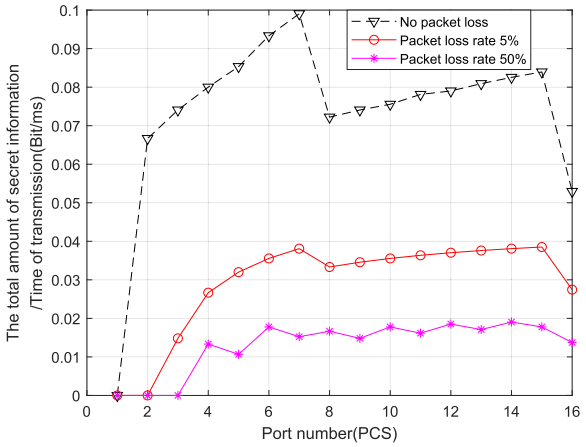


FIGURE 7. The ratio of the total amount of secret information and time of transmission in different packet loss rates.

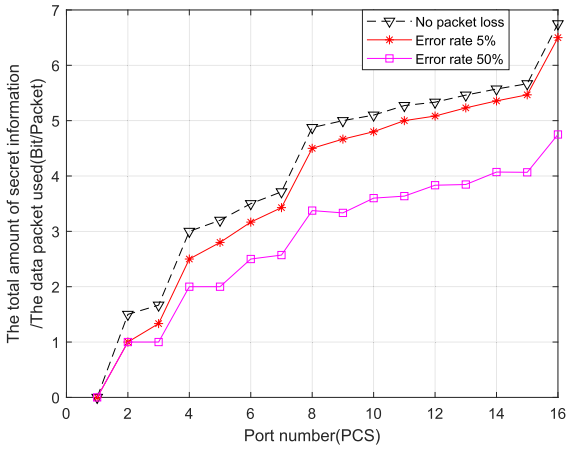


FIGURE 8. The ratio of the total amount of secret information and the data packet used due to delay jitter.

B. DELAY JITTER

Fig. 8 shows the influence of delay jitter on the transmission of secret information in the network. Delay jitter refers to the change of delay. When the time of the transmitted data packet is lower than or higher than the threshold set by the receiver, it will lead to error in receiving the secret information. Taking this error into account and setting the error rate as d, the influence of delay jitter can be obtained [27].

The ratio of the total amount of secret information and the data packet used when the delay jitter occurs: $\left(\lfloor \log_2 n \rfloor \cdot [n(1-d)] + \lfloor \log_2 n! \rfloor\right)/n$, where d is the error rate due to excessive or too little time jitter.

Due to the time jitter being too large or too small, the port arrangement can completely represent the secret information. The port interval can indicate some secret information. The figure shows that the higher the packet loss rate is, the lesser confidential information can be transmitted.

C. UNDETECTABILITY

Undetectability is the most basic characteristic of covert channels. By analyzing the principle of the covert channel used in this paper, it can be found that since the content of the data packet is not modified, the packet capture software is used to analyze the data packet in the model, which is similar to the normal data packet transmitted in the network. In the process of covert communication, the contents of the data packet can withstand the review of the security device.

The existing detection algorithms for the covert timing channel are usually rule-based and statistics-based [28], and the receiver has regular data traffic for a period of time as a basis for detecting the covert timing channel. The regular data traffic in this model is dispersed in multiple connections of the receiving parties. In order to detect whether the data traffic existing in multiple connections is related to each other, large performance and time overhead are required.

VI. SUMMARY

In this paper, based on the IP covert channel of packet sorting, a covert channel for packet expansion is proposed. The relationship between the number of ports in the IP covert channel based on the packet sorting, the number of IP covert channel packet intervals based on the packet interval, and the different time intervals in the IP covert channel based on the packet interval are used to represent the relationship. In analyzing the transmission efficiency and the performance of the proposed method, it can be seen that it optimizes the IP covert channel of packet sort, and increases the total amount of data transmitted in the covert channel of packet sort.

However, some limitations should be noted. First, setting the time range t of the receiving end is determined by the average delay jitter t_d in the network. In practice, the generation of jitter is random and unpredictable. Therefore, the determination of this value is difficult [29]–[31]. It is necessary to set a value that needs to be larger than the average delay of the network to ensure the correctness of the transmitted data.

Second, as the packet loss rate and the bit error rate are random events, the normal distribution model is needed to calculate the packet loss rate and the bit error rate [32]–[34]. In this paper, the randomness of events is not considered when calculating the packet loss rate and bit error rate, which will lead to errors in the results.

The concealment and improvement measures of the method will be further studied in the future.

ACKNOWLEDGMENT

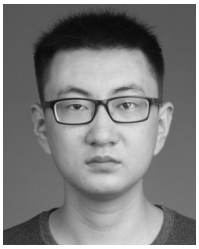
The authors would like to thank the reviewers for their detailed reviews and constructive comments, which helped in improving the quality of this paper.

REFERENCES

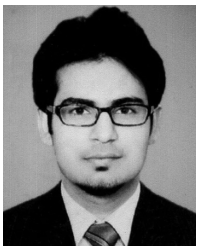
[1] B. W. Lampson, "A note on the confinement problem," *Commun. ACM*, vol. 16, no. 10, pp. 613–615, 1973.
[2] T. G. Handel and M. T. Sandford, "Hiding data in the OSI network model," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer, 1996, pp. 23–38.
[3] Z. Wang, R. Yang, X. Fu, X. Du, and B. Luo, "A shared memory based cross-VM side channel attacks in IaaS cloud," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2016, pp. 181–186.
[4] N. B. Lucena, J. Pease, P. Yadollahpour, and S. J. Chapin, "Syntax and semantics-preserving application-layer protocol steganography," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer, 2004, pp. 164–179.

[5] S. Burnett, N. Feamster, and S. Vempala, "Chipping away at censorship firewalls with user-generated content," in *Proc. USENIX Secur. Symp.*, Washington, DC, USA, 2010, pp. 463–468.
[6] R. Rios, J. A. Onieva, and J. Lopez, "HIDE_DHCP: Covert communications through network configuration messages," in *Proc. IFIP Int. Inf. Secur. Conf.* Berlin, Germany: Springer, 2012, pp. 162–173.
[7] Z. Trabelsi, H. El-Sayed, L. Frikha, and T. Rabie, "A novel covert channel based on the IP header record route option," *Int. J. Adv. Media Commun.*, vol. 1, no. 4, pp. 328–350, 2007.
[8] S. Taheri, M. Mahdavi, and N. Moghim, "A dynamic timing-storage covert channel in vehicular ad hoc networks," *Telecommun. Syst.*, vol. 69, no. 4, pp. 415–429, 2018.
[9] E. Jones, O. Le Moigne, and J.-M. Robert, "IP traceback solutions based on time to live covert channel," in *Proc. 12th IEEE Int. Conf. Netw.*, vol. 2, Nov. 2004, pp. 451–457.
[10] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels: Design and detection," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, Oct. 2004, pp. 178–187.
[11] X. Luo, E. W. W. Chan, and R. K. C. Chang, "TCP covert timing channels: Design and detection," in *Proc. IEEE Int. Conf. Dependable Syst. Netw. FTCS DCC (DSN)*, Jun. 2008, pp. 420–429.
[12] J. Wu, Y. Wang, L. Ding, and X. Liao, "Improving performance of network covert timing channel through Huffman coding," *Math. Comput. Model.*, vol. 55, nos. 1–2, pp. 69–79, 2012.
[13] J. Chen and G. Venkataramani, "CC-Hunter: Uncovering covert timing channels on shared processor hardware," in *Proc. 47th Annu. IEEE/ACM Int. Symp. Microarchit.*, Dec. 2014, pp. 216–228.
[14] X. Zhang, C. Liang, Q. Zhang, Y. Li, J. Zheng, and Y.-A. Tan, "Building covert timing channels by packet rearrangement over mobile networks," *Inf. Sci.*, vols. 445–446, pp. 66–78, Jun. 2018.
[15] R. Archibald and D. Ghosal, "A comparative analysis of detection metrics for covert timing channels," *Comput. Secur.*, vol. 45, pp. 284–292, Sep. 2014.
[16] G. Shah, A. Molina, and M. Blaze, "Keyboards and covert channels," in *Proc. USENIX Secur. Symp.*, vol. 15, Jul. 2006, pp. 59–75.
[17] X. Xue, Y.-M. Kou, S.-F. Wang, and Z.-Z. Liu, "Computational experiment research on the equalization-oriented service strategy in collaborative manufacturing," *IEEE Trans. Serv. Comput.*, vol. 11, no. 2, pp. 369–383, Mar./Apr. 2018.
[18] X. Zi, L. Yao, L. Pan, and J. Li, "Implementing a passive network covert timing channel," *Comput. Secur.*, vol. 29, no. 6, pp. 686–696, 2010.
[19] A. Houmansadr and N. Borisov, "Swirl: A scalable watermark to detect correlated network flows," in *Proc. NDSS*, 2011, pp. 1–15.
[20] A. Belozubova, A. Epishkina, and K. Kogos, "Dummy traffic generation to limit timing covert channels," in *Proc. IEEE Conf. Russian Young Res. Electr. Electron. Eng. (EIConRus)*, Jan./Feb. 2018, pp. 1472–1476.
[21] Y.-A. Tan, X. Zhang, K. Sharif, C. Liang, Q. Zhang, and Y. Li, "Covert timing channels for IoT over mobile networks," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 38–44, Dec. 2018.
[22] R. Krösche, K. Thimmaraju, L. Schiff, and S. Schmid, "I DPID it my way! A covert timing channel in software-defined networks," in *Proc. IFIP Netw. Conf. (IFIP Netw.) Workshops*, May 2018, pp. 217–225.
[23] A. El-Atawy, Q. Duan, and E. Al-Shaer, "A novel class of robust covert channels using out-of-order packets," *IEEE Trans. Depend. Sec. Comput.*, vol. 14, no. 2, pp. 116–129, Mar./Apr. 2017.
[24] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert channel detection," *ACM Trans. Inf. Syst. Secur. (TISSEC)*, vol. 12, no. 4, Apr. 2009, Art. no. 22.
[25] T. Huang, L. Zhang, X. Hu, and X. Lei, "A data validation method based on ip covert channel packet ordering," in *Proc. 14th Int. Conf. Comput. Intell. Secur. (CIS)*, Nov. 2018, pp. 223–227.
[26] X. Luo, P. Zhou, J. Zhang, R. Perdisci, W. Lee, and R. K. Chang, "Exposing invisible timing-based traffic watermarks with BACKLIT," in *Proc. 27th Annu. Comput. Secur. Appl. Conf.*, Dec. 2011, pp. 197–206.
[27] T. Wang, Y. Cao, Y. Zhou, and P. Li, "A survey on geographic routing protocols in delay/disruption tolerant networks," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 2, 2016, Art. no. 3174670.
[28] Q. Li, P. Zhang, Z. Chen, and G. Fu, "Covert timing channel detection method based on random forest algorithm," in *Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2017, pp. 165–171.
[29] U. Premaratne, "Empirical network jitter measurements for the simulation of a networked control system," in *Proc. 14th Int. Conf. Adv. ICT Emerg. Regions (ICTer)*, Dec. 2014, pp. 235–240.
[30] H. Dahmouni, A. Girard, M. Ouzineb, and B. Sanso, "The impact of jitter on traffic flow optimization in communication networks," *IEEE Trans. Netw. Service Manag.*, vol. 9, no. 3, pp. 279–292, Sep. 2012.
[31] A. Huremovic and M. Hadzialic, "Novel approach to analytical jitter modeling," *J. Commun. Netw.*, vol. 17, no. 5, pp. 534–540, Oct. 2015.
[32] R. Pauliks, I. Slaidins, K. Tretjaks, and A. Krauze, "Assessment of IP packet loss influence on perceptual quality of streaming video," in *Proc. Asia–Pacific Conf. Multimedia Broadcast.*, Apr. 2015, pp. 1–6.
[33] M. Terauchi, K. Watabe, and K. Nakagawa, "Model-less approach of network traffic for accurate packet loss simulations," in *Proc. IEEE 26th Int. Conf. Netw. Protocols (ICNP)*, Sep. 2018, pp. 251–252.
[34] L. Roychoudhuri and E. S. Al-Shaer, "Real-time packet loss prediction based on end-to-end delay variation," *IEEE Trans. Netw. Service Manag.*, vol. 2, no. 1, pp. 29–38, Nov. 2005.

LEJUN ZHANG received the M.S. degree from the Harbin Institute of Technology and the Ph.D. degree from Harbin Engineering University, both in computer science and technology. He was a Professor with Yangzhou University. His research interests include computer networks, social network analysis, dynamic network analysis, and information security.



TIANWEN HUANG received the B.Eng. degree in Internet of Things engineering from the Huaiyin Institute of Technology. He is currently pursuing the master's degree in computer technology engineering with Yangzhou University. His research interest includes network security.



WAQAS RASHEED received the B.Eng. degree in software engineering from the University of Sindh, Pakistan. He is currently pursuing the master's degree in software engineering with Yangzhou University. His research interest includes network security.

XIAOYAN HU received the B.Eng. degree in computer science and technology engineering from the Huaiyin Institute of Technology. She is currently pursuing the master's degree in software engineering with Yangzhou University. Her research interest includes network security.

CHUNHUI ZHAO received the Ph.D. degree from the Department of Automatic Measure and Control, Harbin Institute of Technology, in 1998. He is currently with the College of Information Engineering, Yangzhou University, as a Professor, a Doctoral Supervisor, and a part-time Professor. He has published four works and more than 500 articles. His research interests include digital signal and image processing, mathematical morphology, and nonlinear filters. He is a Senior Member of the Chinese Electronics Academy.