A Hybrid Covert Channel with Feedback over Mobile Networks

Xiaosong Zhang[1], Linhong Guo[1], Yuan Xue[2], Hongwei Jiang[2], Lu Liu[2], and Quanxin Zhang[2](✉)

[1] Department of Computer Science and Technology,
Tangshan University, Tangshan 063000, China
[2] School of Computer Science, Beijing Institute of Technology University,
Beijing 100081, China
zhangqx@bit.edu.cn

Abstract. In the existing network covert channel research, the transmission of secret messages is one-way, lacking confirmation feedback on whether the secret message is successfully accepted. However, VoLTE has real-time interactive features, and the data packets between the sender and the receiver are transmitted in both directions, which facilitates the construction of a two-way covert channel with feedback. Therefore, we propose a hybrid covert channel over mobile networks, which includes a sender-to-receiver covert timing channel that modulates covert message through actively dropping packets during the silence periods and a reverse covert storage channel that hides the acceptance of the covert message as feedback information into the feedback control information field of the RTCP packet. The sender evaluates the current attack severity according to the feedback and adjusts the real-time parameters of the covert timing channel to weigh the robustness and other performance. Experimental results show that this solution can effectively feedback the transmission of the covert message while keeping undetectable and robust.

Keywords: Covert channel · VoLTE · Mobile networks · Feedback

1 Introduction

The concept of covert channels was first proposed by Lampson [1], who saw covert communication as a process of communicating data through a transmission channel that is neither designed nor expected. The emergence of information theory, coding theory, and high-performance systems interconnected by high-speed networks has led to the development of covert channels, especially covert timing channels, from conceptual ideas to potential practical tools. The network covert channels that use the network communication medium to transmit information in a covert manner have become the focus of covert channel research.

Covert channels are generally classified into two types: covert storage channels (CSCs) and covert timing channels (CTCs) [2]. The storage covert channel

W. Meng and S. Furnell (Eds.): SocialSec 2019, CCIS 1095, pp. 87–94, 2019.
https://doi.org/10.1007/978-981-15-0758-8_7

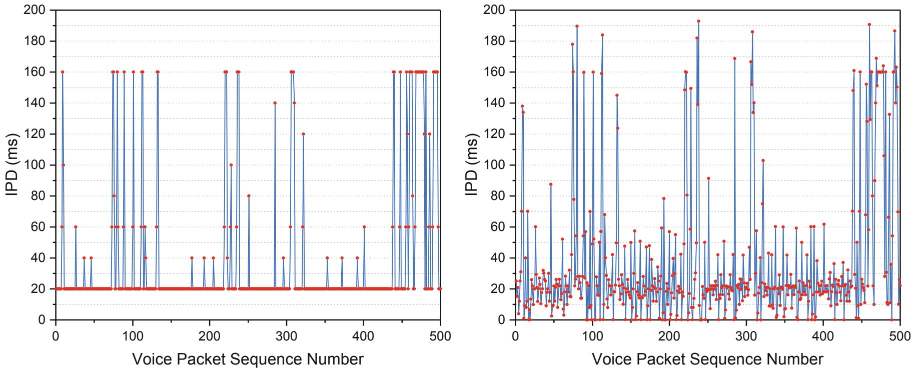
means that the sender directly or indirectly writes information to certain storage locations (memory unit, resource status, network data packet, etc. [3–8]), and the receiver restores the information from the sender by observing the storage location. The covert timing channel means that the influence of the sender on system events (performance, behavior, etc. [9–15]) can be observed by the receiver, and the two parties use the sequence of events, interval, frequency and other time factors to transmit covert message. Covert channels have both legitimate and malicious applications. An example of a malicious use of a covert channel is that criminals use it to leak the secret information of a business.

In order to build an effective covert channel, many research solutions have been proposed [16–18]. However, the existing covert channel construction scheme based on inter-packet delay (IPD) cannot be directly applied to VoLTE because the IPDs of VoLTE traffic is limited to a small range and has strong regularity, which makes the modulation of IPDs easy to detect, and it is difficult to hide covert message into the IPDs of VoLTE traffic. Therefore, based on the research of VoLTE traffic characteristics, we propose a VoLTE two way covert channel, which includes a sender-to-receiver covert timing channel that modulates covert message through actively dropping packets during the silence periods and a reverse covert storage channel that hides the acceptance of the covert message as feedback information into the feedback control information field of the RTCP packet. In order to verify the effectiveness of the covert channel created, we conducted experiments and analysis in the real VoLTE environment, and gave the test results. In this paper, the research on the construction method of VoLTE covert channel will provide useful reference for construction and detection technology of covert channels over mobile networks.

2 Preliminaries

With the in-depth deployment of LTE networks and the popularity of smartphones, data services are beginning to emerge. LTE has successfully penetrated into the cellular communication market and has become the mainstream of communication technology. As an all-IP technology, LTE has many advantages, including robustness, low latency, and high bandwidth. However, since all-IP networks are inherently incompatible with voice processing and cannot utilize traditional circuit-switched-based voice services, there are many challenges in providing voice services based on an all-IP architecture. To compensate for the shortcomings of circuit-switched voice, VoLTE is widely used in the mobile industry as an IP-based LTE voice and video calling solution.

In order to analyze the characteristics of VoLTE traffic, we developed packet capture software for mobile devices to capture packets in the VoLTE video calling. Two Samsung A5108 mobile phones that support VoLTE calling are selected, where Android system version is 5.1.1 and the kernel version is 3.10.61. The network environment is China Mobile 4G network. Figure 1 shows the IPDs of VoLTE voice traffic. Comparing (a) and (b), we can see the difference between the IPDs of the sender and the receiver. For voice traffic, as shown in Fig. 1, the



(a) The sender

(b) The receiver

Fig. 1. The IPDs of VoLTE voice traffic

IPDs of the voice packets sent by the sender are basically 20 ms. The IPDs of the voice packet at the receiver vary greatly from the IPDs at the sender, and the regularity is not obvious. Jitter is the amount of network delay variation. It is generated by any two adjacent packets of the same application during network transmission.

By analyzing the IPD and jitter of VoLTE traffic, it can be seen that the IPDs of VoLTE traffic are limited to a small range and have obvious regularity, and both video traffic and voice traffic have a large jitter variation. According to the characteristics analysis of VoLTE traffic, since the IPDs of VoLTE traffic are obviously regular when the sender sends, if the traditional IPD-based covert timing channel construction method is used, the modulation and modification of the IPDs of the VoLTE traffic will be easily detected by the opponent. At the same time, due to the large variation of the jitter of VoLTE traffic, the IPD-based covert timing channel construction scheme will also face challenges in decoding and accurate secret information cannot be obtained, which will result in high bit error rate. These features make the IPD-based hidden channel construction method not suitable for VoLTE traffic. Therefore, this paper proposes a covert channel construction method by packet rearrangement for VoLTE traffic, which can ensure the constructed covert channel undetectable and robust.

3 The Hybrid Covert Channel

The hybrid covert channel is composed of a covert timing channel from the sender to the receiver and a reverse covert storage channel. On one hand, the covert timing channel from the sender to the receiver is implemented by actively dropping packets during the silence periods, and the covert message is modulated into the numbers of silence insertion descriptor (SID) packets in the silence periods. The silence period is a normal phenomenon in a voice call, and a moderate change in the silent period is not easily detected. At the same time, the use of Gray coding ensures the robustness of the covert channel against the adversary's intentional packet loss attack. The changes of silent periods may affect the covert channel undetectability and reduce the voice quality of the conversation, so the variable length coding is employed to meet the undetectability and voice quality requirements. On the other hand, a covert storage channel is built for feedback from the receiver to the sender, and it hides the acceptance of the covert message as feedback information into the feedback control information field of the RTCP packet back to the sender. These certain bits of the fields are selected to serve as acknowledgment bits for the covert message transmission. The sender evaluates the current attack severity according to the feedback and adjusts the real-time parameters of the covert timing channel to weigh the relationship between the robustness of the adversary's active attack and other performance of the covert timing channel. After many rounds of feedback, the security confrontation against the active attack of the adversary is finally realized. The two-way feedback covert channel is shown in Fig. 2.

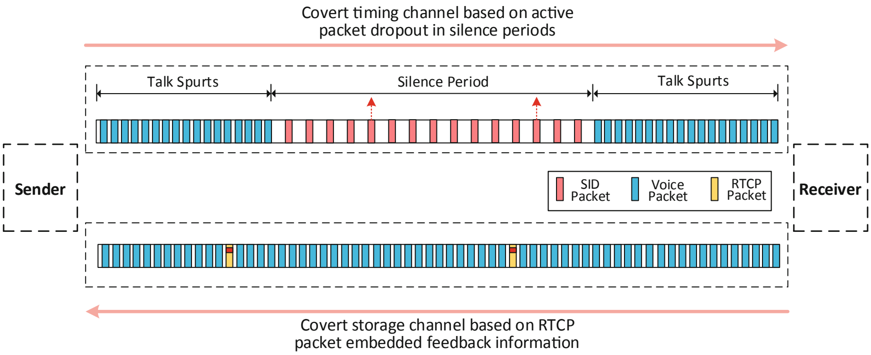

Covert timing channel based on active packet dropout in silence periods
Talk Spurts
Silence Period
Talk Spurts
Sender
Receiver
SID Packet
Voice Packet
RTCP Packet
Covert storage channel based on RTCP packet embedded feedback information

Fig. 2. The two-way feedback covert channel

4 Covert Channel Construction

4.1 Encoding

We use Gray code to mitigate channel noise since Gray code is characterized by two consecutive values that differ only in one bit resulting in robustness to packet reordering and packet loss. The covert message is encoded by the Gray code according to the variable length bl determined by the number of SID packets in the silence period. The covert information bits are encoded into code symbols with a variable length of bl, where each silent period carries one piece of information bits of length bl. The larger the average bit length of the symbol, the higher the transmission efficiency of the covert message. Therefore, if you want to increase the capacity of the covert channel, you can select the voice traffic with a longer average silence period as the carrier.

4.2 Modulation

In our covert timing channel, the encoded covert information is modulated into the numbers of SID packets in the silence period. We consider a one-to-one mapping as the conversion of a symbol s_i to the numbers of SID packets n_i must be invertible: $n_i := G(s_i)$ where $G(\cdot)$ is an invertible function. Correspondingly, $n_i^{'} := G^{-1}(s_i^{'})$ represents that the demodulation is done at the receiver, where $n_i^{'}$ is the received numbers of SID packets, and $s_i^{'}$ denotes the symbols which the numbers of SID packets demodulated into.

The first SID packet is used as a synchronization identifier to mark the beginning of the covert timing channel. At the end of the silence period, the sender calculates the number of SID packets in the silence period to determine how many covert information bits can be transmitted. According to the number of SID packets n_i and covert message, the maximum bl can be found that satisfies $GraytoDec(Getmessage(bl)) \leq n_i - 2 < GraytoDec(Getmessage(bl + 1))$. If the number of SID packets n_i is not equal to the symbol value, the sender will actively discard the extra SID packets to make the two values equal. Moreover, the sender will modify the tail SID packet so that the time interval between the tail packet and the previous SID packet is $bl * 20$. In this way, the size of bl can be judged by the tail packet interval.

4.3 RTCP Feedback

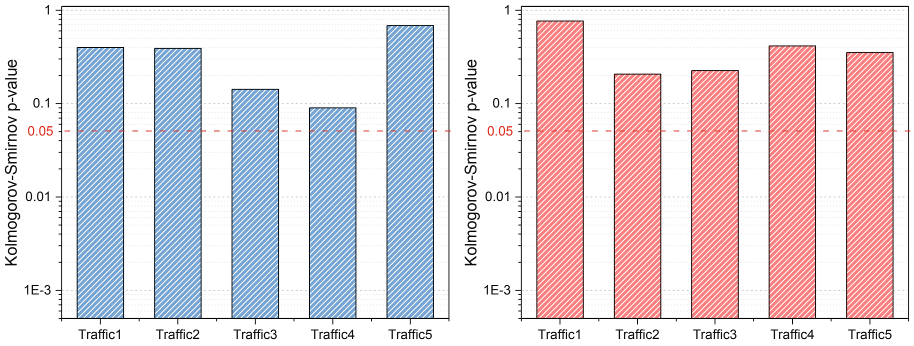
A covert storage channel is built for feedback from the receiver to the sender, and it hides the acceptance of the covert message as feedback information into the feedback control information field of the RTCP packet back to the sender. We use the 16 bits of the bitmask of the lost packet in the feedback control information field to feed back the receiver's confirmation of the covert message. Among them, 8 bits are used to indicate the number of received covert information bits, and the other 8 bits are used to store the last eight bits of the received covert message. Moreover, in order to ensure undetectability of the covert storage channel, not all RTCP packets are used to feedback the reception of covert message, and the interval frequency of the selected RTCP is determined according to the capacity of the sender-to-receiver covert timing channel.

5 Experimental Results and Analysis

To analyze the performance of the proposed covert channel, we used VoLTE traffic between two mobile phones. As long as the devices and systems support VoLTE, our solution can be successfully implemented on different mobile devices and different versions of android. We chose two Samsung A5108 phones, of which the Android version is 5.1.1 and the kernel version is 3.10.61. We test our solution by the two phones as sender and receiver. We capture the VoLTE voice traffic of the sender and receiver in the experiment. Due to that the existing software cannot capture the VoLTE voice packets processed by the baseband program, we have developed a capture program based on the Android kernel. According to our solution, covert traffic is generated by encoding and modulating overt traffic.

5.1 Undetectability

We use KS test, a standard statistical test, to visualize and verify undetectability. In Fig. 3(a), the KS p-values are all greater than 0.05 for the number of SID packets in the silence period of the five overt traffic, which indicates that the number of SID packets of these traffics fit the same distribution. On the other hand, Fig. 3(b) shows that KS p-values are all greater than 0.05 for the number of SID packets of the five corresponding covert traffics which represents that the covert traffics fit the same distribution with the overt traffic.



(a) Overt traffics

(b) Covert traffics

Fig. 3. KS test for the number of SID packets in the silence period

5.2 Robustness

We measure the robustness of covert channels with BER of the decoded covert message. In Fig. 4, the BER of the proposed covert channel reaches 10^{-3} when R_l is less than 0.2%, whereas the BER increases to 10^{-1} when R_l is greater than 5%. The sort of performance for all covert traffics are similar in different network conditions. In summary, the proposed covert channel remains valid even under high network jitter. Specifically, the covert channel with larger average number of SID packets can achieve better robustness.

At the same time, the receiver-to-sender covert storage channel feedbacks the transmission of the covert message through RTCP packets. If the feedback information indicates that the current bit error rate is high, the sender will adjust the covert timing channel modulation parameters or even suspend the delivery of the covert message to resist the active attack of the adversary.

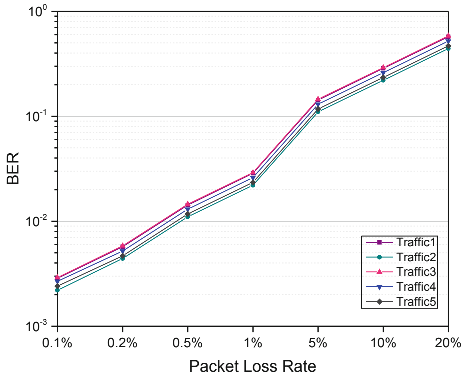


Fig. 4. BER of our covert channels under different packet loss rate

6 Conclusion

The existing covert channel solution based on IPD cannot be applied to VoLTE due to the limited and regular IPDs. Therefore, we proposed a VoLTE two-way covert channel, which includes a sender-to-receiver covert timing channel that modulates covert message through actively dropping packets during the silence periods and a reverse covert storage channel that hides the acceptance of the covert message as feedback information into the feedback control information field of the RTCP packet. To improve the robustness, we employ Gray code to encode the covert message for mitigating the packet loss. To remain undetectable, we employ controllable active packet dropout to fit the distribution of overt traffic. Our scheme implements a covert channel with feedback while considering robustness and undetectability. An interesting future direction for this work is employing silence periods to hide covert message by different modulation algorithm to increase the capacity of covert channels.

Acknowledgment. This work has been supported by the National Natural Science Foundation of China under grant No. U1636213 and No. 61876019.

References

1. Lampson, B.W.: A note on the confinement problem. Commun. ACM **16**(10), 613–615 (1973)
2. Department of Defense Trusted Computer System Evaluation Criteria, pp. 69–72. Palgrave Macmillan UK, London (1985)
3. Mazurczyk, W., Szczypiorski, K.: Evaluation of steganographic methods for oversized IP packets. Telecommun. Syst. **49**(2), 207–217 (2012)
4. Sadeghi, A.-R., Schulz, S., Varadharajan, V.: The silence of the LANs: efficient leakage resilience for IPsec VPNs. In: Foresti, S., Yung, M., Martinelli, F. (eds.) ESORICS 2012. LNCS, vol. 7459, pp. 253–270. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33167-1_15

5. Rios, R., Onieva, J.A., Lopez, J.: Covert communications through network configuration messages. Comput. Secur. **39**(4), 34–46 (2013)
6. Muchene, D.N., Luli, K., Shue, C.A.: Reporting insider threats via covert channels. In: 2013 IEEE Security and Privacy Workshops, pp. 68–71, May 2013
7. Do, Q., Martini, B., Choo, K.K.R.: Exfiltrating data from android devices. Comput. Secur. **48**, 74–91 (2015)
8. Wu, Z., Cao, H., Li, D.: An approach of steganography in G. 729 bitstream based on matrix coding and interleaving. Chin. J. Electron. **24**(1), 157–165 (2015)
9. Cabuk, S.: Network covert channels: design, analysis, detection, and elimination. Ph.D. thesis, Purdue University, West Lafayette, IN, USA (2006)
10. Houmansadr, A., Borisov, N.: CoCo: coding-based covert timing channels for network flows. In: Filler, T., Pevný, T., Craver, S., Ker, A. (eds.) IH 2011. LNCS, vol. 6958, pp. 314–328. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24178-9_22
11. Tan, Y., Zhang, X., Sharif, K., Liang, C., Zhang, Q., Li, Y.: Covert timing channels for iot over mobile networks. IEEE Wirel. Commun. **25**(6), 38–44 (2018)
12. Tan, Y., Xinting, X., Liang, C., Zhang, X., Zhang, Q., Li, Y.: An end-to-end covert channel via packet dropout for mobile networks. Int. J. Distrib. Sens. Netw. **14**(5), 1–14 (2018)
13. Zhang, X., Liang, C., Zhang, Q., Li, Y., Zheng, J., Tan, Y.: Building covert timing channels by packet rearrangement over mobile networks. Inf. Sci. **445–446**, 66–78 (2018)
14. Zhang, X., Tan, Y., Liang, C., Li, Y., Li, J.: A covert channel over VoLTE via adjusting silence periods. IEEE Access **6**, 9292–9302 (2018)
15. Zhang, X., Zhu, L., Wang, X., Zhang, C., Zhu, H., Tan, Y.: A packet-reordering covert channel over VoLTE voice and video traffics. J. Netw. Comput. Appl. **126**, 29–38 (2019)
16. Luo, X., Chan, E.W.W., Chang, R.K.C.: TCP covert timing channels: design and detection. In: 2008 IEEE International Conference on Dependable Systems and Networks with FTCS and DCC (DSN), pp. 420–429, June 2008
17. Wu, J., Wang, Y., Ding, L., Liao, X.: Improving performance of network covert timing channel through huffman coding. Math. Comput. Model. **55**(1C2), 69–79 (2012)
18. Ahmadzadeh, S.A., Agnew, G.: Turbo covert channel: an iterative framework for covert communication over data networks. In: 2013 Proceedings IEEE INFOCOM, pp. 2031–2039, April 2013