A VoLTE Covert Channel with Intelligent Confrontation

Linhong Guo1 and Xiaosong Zhang1

1 Department of Computer Science and Technology, Tangshan University, Tangshan 063000, China

*Corresponding author’s e-mail: zxs0224@163.com

Abstract. VoLTE (voice over LTE) is widely popular and the potential target for covert communications. The transmission of continuous and large amounts of data over VoLTE enables the construction of a covert channel. The existing covert channel construction scheme based on IPD (inter-packet delay) cannot be applied to VoLTE due to the particularity of the IPD of VoLTE traffics. In this paper, we propose a covert channel with intelligent confrontation for VoLTE traffic. It modulates messages in the relative relationship of voice and video packets based on learning of the characteristics of active attack traffic. The experimental results indicate that the proposed covert channel is undetectable and robust.

1. Introduction

Covert channels are generally classified into two types: covert storage channels (CSCs) and covert timing channels (CTCs) [1]. The storage covert channel means that the sender directly or indirectly writes information to certain storage locations (memory unit, resource status, network data packet, etc. [2-7]), 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, behaviour, etc. [8-15]) 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.

VoLTE is widely used in the mobile industry as an IP-based LTE voice and video calling solution. It is a global interoperability solution that provides the advanced and innovative communication service. 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. It is difficult to hide covert message into the IPDs of VoLTE traffic since the modulation of IPDs is easy to detect. Moreover, the adversary attacks the covert channel by means of active packet loss and out-of-order, making the security of the covert channel threatened. Therefore, we propose a VoLTE covert channel with intelligent confrontation, which modulates the message in the relative relationship of the voice/video packets. More critically, the range of position changes of voice and video packets will also intelligently change adaptively with the degree of disorder caused by active attacks.

2. VoLTE traffic capture and analysis

In order to verify the effectiveness of the VoLTE covert channel construction method proposed in this paper, it is necessary to obtain real VoLTE traffic data for testing. Currently, there is no universal VoLTE traffic dataset. Therefore, VoLTE packet capture is an important preparation. Due to the characteristics of VoLTE traffic, the capture needs to be implemented through the kernel or baseband.

Smartphones typically have a separate architecture of baseband processor (BP) and application processor (AP). This separation architecture provides the flexibility to properly distribute the various

...
software components between BP and AP when designing a VoLTE terminal solution. BP is used for the physical layer, while AP is used for user interfaces and various applications. AP and BP are connected via chip-to-chip interface technology. Video packets are generated in the AP and voice packets are created in the BP. However, both video and voice packets are sent over the baseband. Therefore, we used a self-developed crawler to capture video and voice packets at the baseband simultaneously.

Figure 1. The overall framework of the baseband packet capture scheme.

The overall framework of the baseband packet capture scheme is shown in Figure 1. The entire solution includes three aspects of BP and AP and serial port mechanism. The BP side is mainly responsible for capturing packet information, and the AP side is mainly responsible for receiving information. When a VoLTE calling is made, on the BP side, after the baseband captures the packet information and the physical layer forward, the captured information is transmitted to the AP side through the chip-to-chip link layer. At the same time, on the AP side, the captured information is received by the operating system process and the hardware abstraction layer. Finally, the AP side will call the USB transfer driver to send the captured information to the PC serial port data reader for display and storage.

In order to analyse the characteristics of VoLTE traffic, we developed packet capture software for mobile devices to capture packets in the VoLTE calling. Through traffic analysis, we can see the IPDs of the voice packets sent by the sender are basically 20ms and the regularity is obvious.

3. A covert channel with intelligent confrontation

The adversary increases the channel noise by increasing the delay, such as delay jitter, packet loss, and out-of-order, so that the IPDs obtained by the receiver are distorted, and the bit error rate in the decoding process is too high, resulting in the interruption of covert channel communication.

This work studies the identification and countermeasures of active attacks on covert channels in real-time voice and video services. It also studies real-time and efficient deep packet inspection technology, and recovers the network packet timestamp from the application layer payload. After identifying active attacks such as violent delay jitter, packet loss, and out-of-order, it eliminated noise by means of network packet reordering. The voice/video packet has continuity and position randomness. The positional relationship of the two types of network packets is used as the modulation object. The demodulation process does not depend on the interval between network packets, and can resist the active attack of network delay jitter.

The work utilizes the network characteristics of the real-time interactive service to restore the timestamp information of the voice and video network packets at the application layer, and modulate the message in the relative relationship of the voice/video packets in the video call. Under the condition of active attack introduced by the enemy, the receiver can eliminate channel noise and improve the
robustness of covert communication. The range of position changes of voice/video packets will also intelligently change adaptively with the degree of disorder caused by active attacks. The covert message encoding and modulation is showed in Algorithm 1.

At the same time, in the establishment and operation phase of covert communication, the delay statistical distribution of the transmitting and receiving sides is adjusted according to the network conditions, and the covert channel can intelligently adapt to network congestion, delay jitter, packet loss rate, signal strength, transmission path, etc. Such changes, against aggressive attacks such as violent delay jitter, packet loss, and out-of-order, to achieve a reasonable compromise between capacity and security.

Algorithm 1: Covert Message Encoding and Modulation
1: Enter(FirstInterval)
2: while !eof (CovertMessageFile) do
3:  pnum ← CountPacket(CurrentInterval)
4:  BlockValue ← Mod(pnum, Pow(bl, 2))
5:  if(Mod(inum,span)==1) then
6:    BalanceValue←TrafficLearning()
7:    GrayValue ← GraytoDEC(BalanceValue))
8:  else
9:    GrayValue ← GraytoDEC(GetCovertMessage(bl))
10:  end if
11:  if BlockValue < GrayValue then
12:    Move(Next(GrayValue-BlockValue),CurrentInterval)
13:  else
14:    Move(Current(BlockValue-GrayValue), NextInterval)
15:  end if
16:  inum++;
17:  Enter(NextInterval)
18: end while

4. Experimental results and analysis
To analyse the performance of the proposed covert channel, we used VoLTE traffic between the two Samsung A5108 phones, the Android version is 5.1.1, and the kernel version is 3.10.61. We tested our solution as a sender and receiver via two mobile phones.

We use standard statistical test KS tests to visualize and verify undetectability. For the number of video packets between voice packets of overt traffic, the KS p values are all greater than 0.05, indicating that the number of video packets for these traffic matches the same distribution. On the other hand, for the number of video packets between voice packets of covert traffic, the KS p value is greater than 0.05, which means that the covert traffic conforms to the same distribution as the overt traffic.

We use the BER of the decoded covert message to measure the robustness of the covert channel. When the packet loss and out-of-order rate is less than 1%, the proposed BER of the covert channel reaches $10^{-3}$, and when the packet loss and out-of-order rate are greater than 10%, the BER increases to $10^{-1}$. The performance of the proposed covert channel is similar under different network conditions. In summary, the proposed covert channel is still effective even under active attacks.

5. Conclusion
In this paper, we propose a covert channel with intelligent confrontation for VoLTE traffics. The proposed scheme is an alternative scheme of the existing packet arranging schemes, which modulates the message in the relative relationship of the voice and video packets based on the learning of the characteristics of the actively attacked traffic. We discuss on how to encode and modulate the covert message and employ the balance value to adjust the feature distribution of the covert traffic for the undetectability and robustness of the covert channel. The experimental results show that the scheme is stealthy and the channel BER is acceptable under the actively attacked network conditions.
Acknowledgments
This work has been supported by the National Natural Science Foundation of China under grant No.61876019.

References
[1] Department of Defense Trusted Computer System Evaluation Criteria, pages 69-72. Palgrave Macmillan UK, London, 1985.
[2] Z. Wu, H. Cao, and D. Li. An approach of steganography in g.729 bitstream based on matrix coding and interleaving. Chinese Journal of Electronics, 24(1):157-165, 2015.
[3] Quang Do, Ben Martini, and Kim Kwang Raymond Choo. Exfiltrating data from android devices. Computers & Security, 48:74-91, 2015.
[4] D. N. Muchene, K. Luli, and C. A. Shue. Reporting insider threats via covert channels. In 2013 IEEE Security and Privacy Workshops, pages 68-71, May 2013.
[5] Ruben Rios, Jose A. Onieva, and Javier Lopez. Covert communications through network configuration messages. Computers & Security, 39(4):34-46, 2013.
[6] Ahmad Reza Sadeghi, Steen Schulz, and Vijay Varadharajan. The silence of the LANs: Efficient leakage resilience for IPsec VPNs. In Computer Security C ESORICS 2012. Lecture Notes in Computer Science, volume 7459, pages 221-232. Springer Berlin Heidelberg, 2012.
[7] Wojciech Mazurczyk and Krzysztof Szczypiorski. Evaluation of steganographic methods for oversized ip packets. Telecommunication Systems, 49(2):207-217, 2012.
[8] Xiaosong Zhang, Liehuang Zhu, Xianmin Wang, Changyou Zhang, Hongfei Zhu, and Yu-an Tan. A packet-reordering covert channel over volte voice and video traffics. Journal of Network and Computer Applications, 126:29-38, 2019.
[9] Xiaosong Zhang, Yu-an Tan, Chen Liang, Yanzhang Li, and Jin Li. A covert channel over VoLTE via adjusting silence periods. IEEE Access, 6:9292-9302, 2018.
[10] Xiaosong Zhang, Chen Liang, Quanxin Zhang, Yanzhang Li, Jun Zheng, and Yu-an Tan. Building covert timing channels by packet rearrangement over mobile networks. Information Sciences, 445-446:66-78, 2018.
[11] S. A. Ahmadzadeh and G. Agnew. Turbo covert channel: An iterative framework for covert communication over data networks. In 2013 Proceedings IEEE INFOCOM, pages 2031-2039, April 2013.
[12] Jingzheng Wu, Yongji Wang, Liping Ding, and Xiaofeng Liao. Improving performance of network covert timing channel through huffman coding. Mathematical & Computer Modelling, 55(1C2):69-79, 2012.
[13] Serdar Cabuk. Network Covert Channels: Design, Analysis, Detection, and Elimination. PhD thesis, Purdue University, West Lafayette, IN, USA, 2006.
[14] Xiapu Luo, E. W. W. Chan, and R. K. C. Chang. TCP covert timing channels: Design and detection. In 2008 IEEE International Conference on Dependable Systems and Networks with FTCS and DCC (DSN), pages 420-429, June 2008.
[15] Amir Houmansadr and Nikita Borisov. Coco: Coding-based covert timing channels for network flows. In Proceedings of the 13th International Conference on Information Hiding, IH’11, pages 314-328, Berlin, Heidelberg, 2011. Springer-Verlag.