A New Method for Authentication Based on Covert Channel

Yanan Sun, Xiaohong Guan, and Ting Liu

Ministry of Education Key Lab for Intelligent Networks and Network Security,
School of Electric and Information Engineering, Xian Jiaotong Uinversity

Abstract. Authentication is of great importance in information security. Traditional method only focus on encryption of the content itself, which is the same with the later proposed methods named information hiding and digital watermark. Since data transmission is in the open network, it can easily be detected and intercepted by the malicious party. In this paper, we put forward a new method which utilize the communication channel, not the content, as the data carrier, and guarantee the validation of the user's identity during the common data transmission. Specifically, by manipulating the inter-packet delays, we implement a prototype system for authentication and embed the authentication tag within the packet intervals based on network covert channel. By conducting a series of experiments, we prove that our method performs well in LAN and Campus Network.

Keywords: Network security, network covert channel, authentication, time intervals.

1 Introduction

With the development of modern technology, Internet is deeply involved with our daily life, the flaws and attacks within the network will lead to potential huge loss. As a result, information security is of great importance in order to maintain the security of the whole network, in which authentication plays an important part.

Authentication is critical for network security. Traditional authentication method is based on modern cryptography, which lay great emphasis on the study of the complexity of algorithm. It can be divided into symmetric and asymmetric key cryptography. Symmetric key cryptography is easy for encryption, but is not secure in key distribution; Asymmetric key cryptography introduce the new concept for PKI, which provide a new field and technical support for information security, but has a high requirement for system overhead. Relied on asymmetric key cryptography, digital signature is brought out as a new way to validate user's identity. Later, with the development of digital media, information hiding and digital watermark is proposed as a new thread to protect the copyright of digital media and also the validity and integrity of its content.

Traditional methods and the later proposed information hiding and digital watermark both make use of the content transmitted to do encryption and authentication. They are restricted in the information transmitted and appear to be vulnerable. Since

E. Altman and W. Shi (Eds.): NPC 2011, LNCS 6985, pp. 160–165, 2011.

the communication is in the open network, the transmitting data is easy to be intercepted by malicious middleman or third party, and if there is enough information, he can modify and fake the data, which emerge as a huge threat to information security. Thus, we propose a new scheme to do authentication from the respective of the communication channel, namely covert channel, which utilize the packet stream to indicate the cipher text. In this way, even though the malicious middleman intercept the packets for data transmission, he cannot determine if there is cipher text only from the overt communication, therefore covert channel can be a much more stealthy and secure way for authentication, which can be a supplement for the traditional methods.

2 Theory

2.1 Covert Channel

Covert channel is a communication channel that violates a security policy by using shared resources in ways for which they were not initially designed[2], which makes use of sharing resources to bypass the security policy to establish malicious communication for sensitive information leakage. Fig 1 shows the simple structure of covert channel.

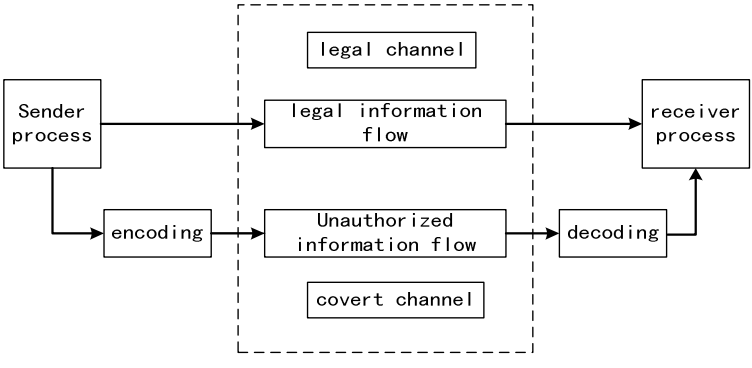

Fig. 1. Simple structure of Covert Channel

2.2 Categories of Covert Channel

Basically covert channels can be classified into two categories according to the type of the shared resources, namely storage covert channel and timing covert channel.
Storage covert channel means "the indirect or direct writing of a storage location by one process and the indirect or direct reading of the storage process by another process" [1].

Timing covert channel means "a sender process which signals information to another by modulating its own use of system resources in such a way that the response time observed by the second process is changed" [1].

2.3 Comparison between Storage and Timing Covert Channel

In the real network environment, timing covert channel is much more difficult to be detected compared with the storage one [3]. The reason for which is that sometimes the modification of TCP / IP header is illegal and quite obvious, but for the timing covert channel, it can hardly be recognized unless analyzing the characteristics of traffic stream during the whole communication process. However, on the other hand, the synchronization of the clock and the sequence of the packet order have a significant influence on the accuracy of decryption. So considering this, storage covert channel can be much more accurate. What's more, storage covert channel is more effective than the timing one due to the packet delay.

3 Methodology

Taking stealth, effectiveness and accuracy into consideration, we decide to utilize timing covert channel [4] [5] [6] which embeds the authentication tag within the packet intervals.

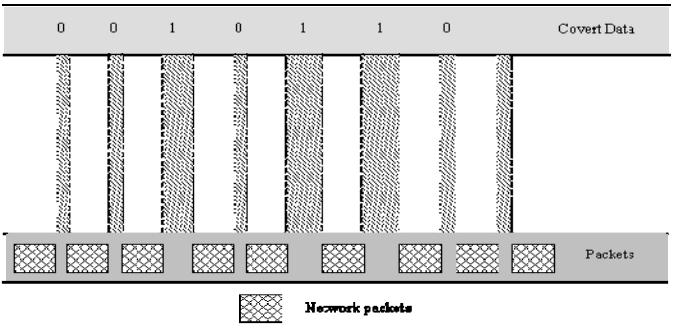

Fig. 2. A diagram to illustrate timing covert channel by manipulating the packet interval

In our design, the sender manipulate the interval between the two packets which is sent during the overt communication ,then use a certain kind of algorithm to encode these interval to represent certain information. And after these packets are received, the receiver decodes and obtains the information according to the "Key" which has been predetermined before. As Fig 2 illustrates, the sender process manipulates the inter-packet delays, and use the long intervals to indicate "1", the short intervals to indicate"0". And after the receiver process receives these packets, it records their arrival time and calculates the packet intervals, then decode and obtain the covert information the sender process transmit.

By using Winsock2 SPI and Winpcap interface, we implement a prototype system to do authentication as Fig 3 illustrates. In our proposed system, we exploit a module for FTP client to monitor the network traffic packets and embed the authentication tag within the packet intervals through encoding, and also a module for FTP server to decode the covert information and validate the client's identity, which is the authentication process.

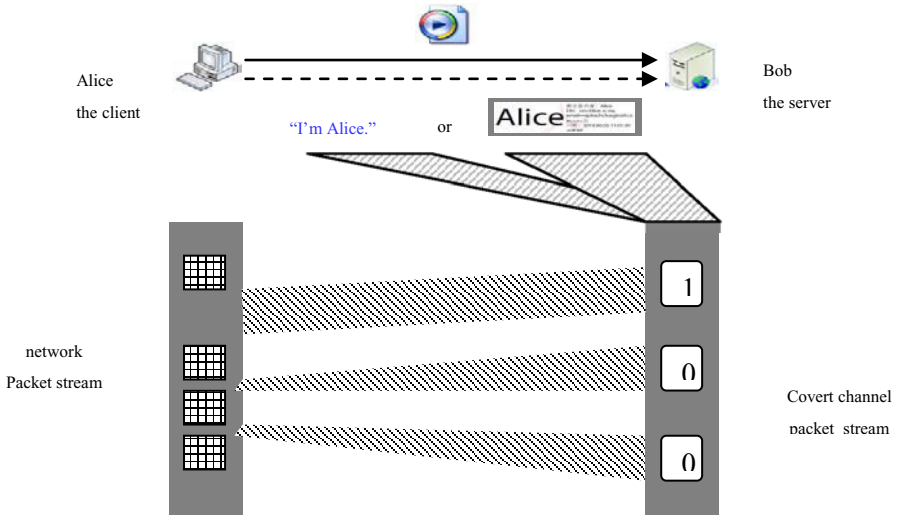

Fig. 3. The infrastructure of the model for authentication using timing covert channel

4 Result

From Fig 4, we can find that traffic stream distribution of covert channel is quite different from the legal one, no matter in LAN or Campus Network, the covert traffic stream shows an alternating long and short packet intervals, especially at the beginning of the communication process, the reason for which is that the sender process manipulate the inter-packet delays in order to transmit the authentication information. While the statistical charts are similar with each other, and this is because the packets used to transmit authentication tag is only a small portion of the total packets for the whole communication process, and most of the packets still belong to the overt channel.

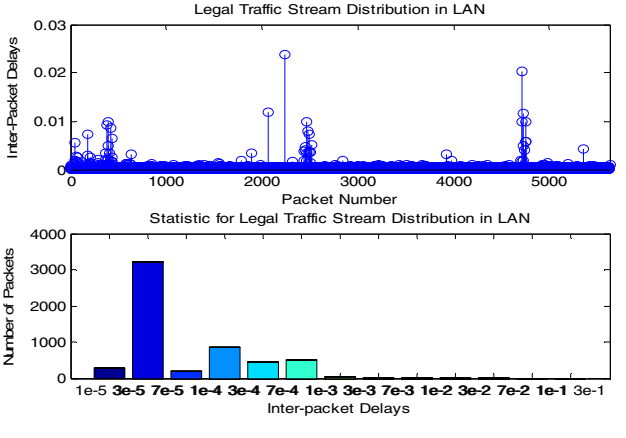

Fig. 4. Traffic Stream for legal and Covert Communication

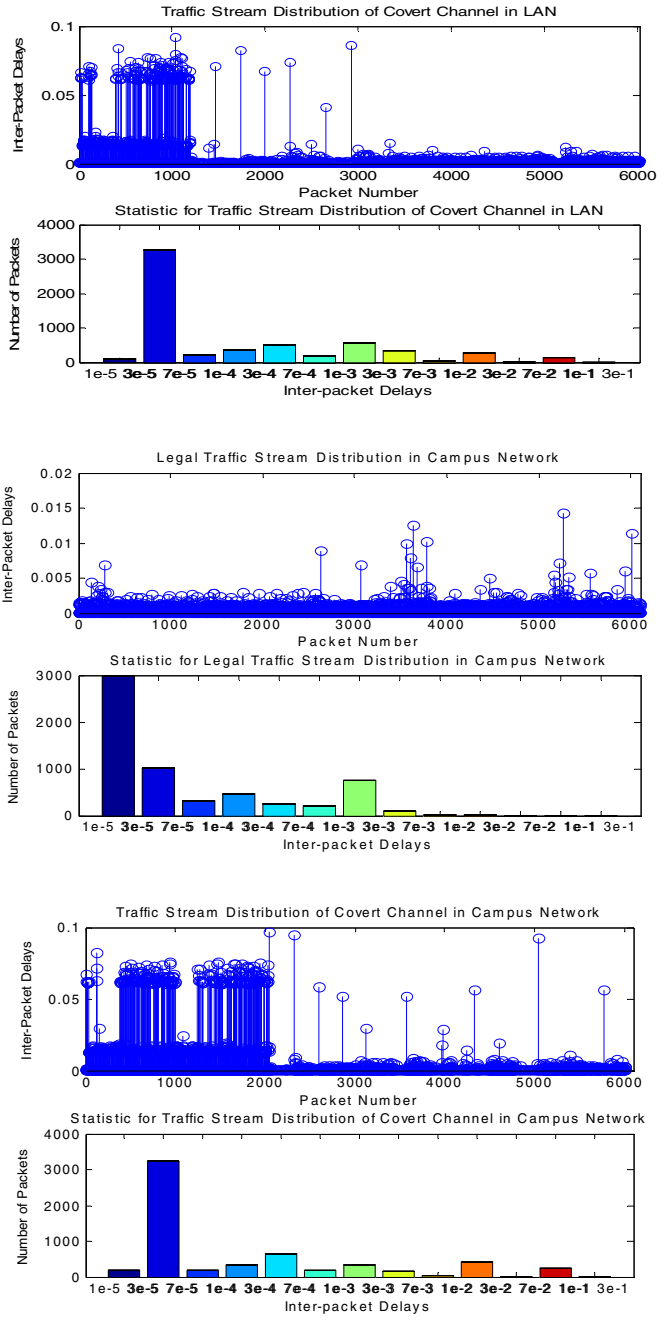

Fig. 4. (*continued*)

5 Conclusion and Future Work

In this paper, a new method for authentication by using communication channel—timing covert channel is proposed, and by conducting a series of experiments in LAN and Campus Network, we find timing covert channel may lead to certain delays and the packet stream is not similar to the regular ones, but it still proves to be a much more secure and stealthy way for authentication. Our future work is focus on evaluating the performance of the proposed system and further analyzing the difference of the traffic stream between legal and covert communication.

References

[1] Cabuk, S.: Network Covert Channels: Design, Analysis, Detection, and Elimination, Ph.D. thesis (2006)
[2] Lampson, B.W.: A Note on the Confinement Problem. Communications of the ACM 16(10), 613–615 (1973)
[3] Ahsan, K., Kundur, D.: Practical Date Hiding in TCP/IP, MMSec. (2002)
[4] Cabuk, S., et al.: IP Covert Timing Channels: An Initial Exploration. In: CCS 2004, Washington, DC, USA, October 25-29 (2004)
[5] Cabuk, S., Brodley, C.E., Shields, C.: IP Covert Timing Channels: Design and Detection. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004 (2004)
[6] Sellke, S.H., Wang, C.-C., Bagchi, S.: TCP/IP Timing Channels: Theory to Implementation. In: Proceedings of the 28th, Conference on Computer Communications, INFOCOM (April 2009)