An Optimized Recognition Algorithm for SSL VPN Protocol Encrypted Traffic

Kehua Xian
Sichuan College of Architectural Technology, Deyang, Sichuan 618000, China
E-mail: ak3161@126.com

Keywords: secure sockets layer virtual private network, fingerprint recognition, encrypted traffic, capsule neural network

Received: September 3, 2021

With the widespread use of Virtual Private Networks (VPNs), the identification of Secure Sockets Layer (SSL) VPN encrypted traffic has become an important issue. This paper first introduces SSL VPN encrypted traffic and analyzes the flow of its handshake protocol. Then, an improved fingerprint recognition algorithm is designed to identify SSL streams. Capsule Neural Network (CapsNet), an optimized convolutional neural network, was used to recognize SSL VPN. An experimental analysis was carried out on the ISCXVPN2016 dataset. It was found that the recognition accuracy of the proposed method reached up to 99.98% for SSL streams, and the convergence speed was high; the recognition precision reached 98.16%, and the recall rate reached 99.98% for SSL VPNs, both of which were better than the algorithms such as random forest (RF) and C4.5. The experimental results verify the effectiveness of the optimized recognition algorithm for SSL VPN recognition and make some contributions to its application in practice.

Povzetek: Predstavljen je algoritem za prepoznavanje prometa v privatnih omrežjih, preizkušen na podatkovni bazi SCXVPN2016.

1 Introduction

With the development of economy and society, people's living standard has been improving, and the use of the network has become more and more popular[1]. While people use various resources and services of network, problems such as network viruses [2], malicious codes [3], and hacker attacks [4] frequently appear, which bring great threats to network security. Network traffic refers to the amount of data transmitted on the network. Encrypted traffic refers to the network traffic generated by the encryption algorithm. Secure sockets layer virtual private network (SSL VPN), a new secure transmission technology, effectively ensures data security by transmitting data in the form of a password, which has been applied in more and more enterprises and organizations. At the same time, there are some illegal applications hidden in the SSL VPN encrypted traffic; therefore, how to achieve the identification of SSL VPN encrypted traffic is gradually becoming an important issue in network security. But most of the current research focuses on the recognition of SSL traffic but pays little attention to recognizing VPN traffic. Niu et al. [5] designed a heuristic statistical test (HST) method that combined statistics with machine learning. The experiments found that the method had better performance and higher recognition accuracy for traffic than traditional coding-based and entropy-based methods. Muhammad et al. [6] designed a system to analyze the communication between users and servers, divided the traffic into VPN traffic and standard traffic, and analyzed and classified network traffic by Domain Name System (DNS) packets and Hypertext Transfer Protocol Secure (HTTPS)-based traffic. They found that 329 out of 729 connections established by different users were classified as legitimate activities, and the remaining 400 connections were marked as VPN-based connections, indicating that the method was able to detect VPN traffic effectively. Yoon et al. [7] proposed a system for analyzing encrypted traffic and found through experiments that the method could effectively detect malicious behavior in enterprise networks. This paper studied the recognition of SSL VPN traffic using an improved fingerprint recognition algorithm and the Capsule Neural Network (CapsNet) algorithm. Experiments were carried out on the ISCXVPN2016 dataset to demonstrate the reliability of the method. This work provides some theoretical bases for better recognition of encrypted traffic.

2 SSL VPN protocol

VPN is a kind of private network that connects different networks by encryption, etc. [8]. It combines access control, encryption audit, etc. [9] and can encapsulate and encrypt data transmission to avoid data leakage. Most of the current VPNs have a dual network card structure. First, the external network card is connected to the Internet. After the public network finds the internet protocol (IP) address of the intranet, the packet is sent through the tunnel, the VPN gateway receives the packet and verifies it. After confirmation, it is encrypted and encapsulated, and a new packet is returned to the extranet gateway and sent to the Internet first and then the intranet gateway

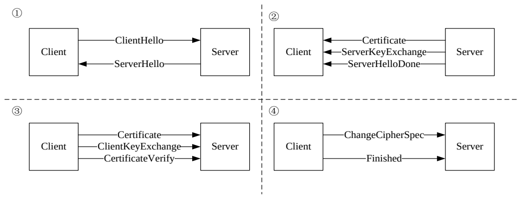

Figure 1The flow of SSL handshake protocol.

through the route. After confirmation, the packet is decrypted, and the intranet gateway sends the data to the intranet.

SSL protocol connection is authenticated by password. Data are encrypted by encryption algorithms to guarantee the validity of the data. SSL VPN is a VPN technology implemented based on SSL protocol. SSL VPN uses a browser/server (B/S) architecture and has a variety of flexible authentication methods. It can control resources, has a host detection function, and is convenient to use. SSL VPN has a functional module called virtual gateway, providing SSL VPN access service to users. After users log in to the virtual gateway, they request to establish an SSL connection, and then the virtual gateway sends certificates to users for authentication. After passing the authentication, users can connect to SSL successfully. At the same time, the virtual gateway will query user rights and classify users with the same rights into the same group to facilitate access to related resources.

The core of SSL VPN is the SSL protocol, and the handshake protocol is the most important part of the SSL protocol [10]. The flow of the handshake protocol is shown in Figure 1.

According to Figure 1, the handshake protocol can be divided into four phases.

(1) Both parties exchange Hello messages to negotiate the follow-up password suite.

(2) The server sends a certificate, key exchange, and ServerHelloDone.

(3) Upon receiving a certificate request, the client sends its certificate and sends a message of key exchange.

(4) The cipher suite is changed, and the handshake protocol ends.

3 Optimized recognition algorithm

3.1 SSL traffic recognition

In the recognition of SSL VPN encrypted traffic, the SSL traffic needs to be recognized first. In a complete handshake protocol, there must be several types of messages, such as ClientHello, ServerHello, ServerHelloDone, ClientKeyExchange, and ChangeCipherSpec. The traditional method of identifying SSL traffic is to test the above types of messages in sequence. If not all type information is detected, the traffic will be judged as a non-SSL stream, but this may be due to unsuccessful handshake protocol establishment or missed packets when capturing packets; therefore, it may miss the recognition of SSL stream. Thus, this paper adopts an improved fingerprint recognition method to identify SSL streams.

Content-type	Version		Length	
Byte 1	Major	Minor	Byte 4	Byte5

Table 1Format of the first five bytes of the SSL stream.

Hex	Dec	Type
0×14	20	ChangeCipherSpec
0×15	21	Alert
0×16	22	Handshake

Table 2Content type correspondence information.

Major version	Minor version	Version type
3	0	SSLv3
3	1	TLS 1.0
3	2	TLS 1.1
3	3	TLS 1.2

Table 3Version correspondence information.

The format of the first five bytes in the SSL stream is fixed, as shown in Table 1, which can be treated as a 5-tuple. The content type and version correspondence information is shown in Tables 2 and 3. The improved fingerprint recognition method determines whether the current packet is SSL encrypted traffic by identifying this 5-tuple.

The process of recognizing SSL by the improved fingerprint method is as follows.

(1) Whether the selected packet is the first 20 packets of the stream is determined. If not, whether the major version is smaller than three. If it is smaller than three, the current stream is not an SSL stream; if it isn't, the current stream is an SSL stream.

(2) For the first 20 packets of the stream, whether the value of the first byte of TCP data is 21, 22, 23, or 24 is determined. If it isn't, return to the first step; if it is, go to the next step.

(3) Whether the value of the second byte of TCP data is three is determined. If it isn't, return to the first step; if it is, go to the next step.

(4) Whether the value of the second byte of TCP data is zero, one, two, or three is determined. If it isn't, return to the first step; if it is, go to the next step.

(5) Whether the length of the SSL data is smaller than that of the TCP data is determined. If it isn't, return to the first step; if it is, the next stream is determined in the same way.

3.2 Capsule neural network recognition algorithm

CapsNet is based on a convolutional neural network. It replaces the sampling layer with two new layers. The first layer of its network is the convolutional layer, the second layer is the basic capsule layer, and the third layer is the

Category	Content
Traffic	Content
Web Browsing	Firefox and Chrome
Email	SMPTS, POP3S and IMAPS
Chat	ICQ, AIM, Skype, Facebook and Hangouts
Streaming	Vimeo and Youtube
File Transfer	Skype, FTPS and SFTP using Filezilla and an external service
VoIP	Facebook, Skype and Hangouts voice calls (1h duration)
P2P	uTorrent and Transmission (BitTorrent)

Table 4ISCXVPN2016 dataset.

digital capsule layer. The basic unit is capsule, which contains multiple neurons. The activation function of the network is the squashing function, and its formula is:

$$V_j = \frac{\|s_j\|^2}{1+\|s_j\|^2}\frac{s_j}{\|s_j\|},$$

where V_j refers to the total output of j capsules and S_j refers to the total input of j capsules. Its training process is:

$$S_j = \sum_i C_{ij}\hat{u}_{j|i},$$

$$\hat{u}_{j|i} = W_{ij}u_i,$$

where C_{ij} refers to the weight between the low-layer and high-layer capsules, $C_{ij} = \frac{exp(b_{ij})}{\sum_k exp(b_{ik})}$, b refers to the prior probability that the capsules are coupled to each other, u_i refers to the i-th capsule of the l-th layer, $\hat{u}_{j|i}$ is the overall information prediction result of the j-th capsule of the $l+1$-th layer under the i-th capsule of the l-th layer, and W_{ij} is the weight matrix.

The loss function of CapsNet is:

$$L_k = T_k max(0, m^+ - \|v_k\|)^2 + \gamma(1 - T_k)max(0, \|v_k\| - m^-)^2,$$

where T_k refers to the classification indicator function (it is 1 if class k exists and 0 if it does not exist), v_k refers to the output of the network, m^+ and m^- are the upper and lower bounds, respectively (they take the empirical values in this paper, $m^+ = 0.9$, and $m^- = 0.1$), γ refers to the scale factor (it takes the initial value in default, $\gamma = 0.5$).

4 Experimental analysis

The experiments were conducted in a Linux system with a computer processor of AMD Ryzen 7-1700, a graphics card of GTX 1080TITAN, and 16GB RAM, and CapsNet used the open source Keras module to conduct experiments on the identification of SSL streams first, and then SSL VPN encrypted traffic, published in Lashkari et al. [11] on the VPN-nonVPN dataset (ISCXVPN2016), in which there are 28G data containing eight categories, the contents of which are shown in Table 4.

The stream features used for recognition are derived from the 23 features proposed by Lashkari et al. [11], which are:

(1) duration: the duration of the flow;

(2) FLAT: forward inter-arrival time, including mean, maximum, minimum, and variance, four in total;

(3) BLAT: backward inter-arrival time, including mean, maximum, minimum, and variance, four in total;

(4) Flow-IAT: flow inter-arrival time, including mean, maximum, minimum and variance, four in total;

(5) active: the time to change from active stream to silent stream, including mean, maximum, minimum, and variance, four in total;

(6) Idle: the time to change from a silent flow to an active flow, including mean, maximum, minimum, and variance, four in total;

(7) FB-psec: the number of bytes per second transferred by the flow;

(8) FP-psec: the number of packets per second transmitted by the flow.

First, the performance of the improved SSL stream recognition method designed in this paper was analyzed. The recognition results of the traditional method were compared with the improved method, as shown in Figure 2.

It was seen from Figure 2 that the improved method was significantly better than the traditional method in recognizing SSL streams. Taking AIM as an example, the recognition accuracy of the improved method was 98.67%, which was 12.19% higher than the traditional method; the accuracy of the improved method was always above 95%, with a maximum of 99.98%, while the highest and lowest accuracy of the traditional method was only 93.61% and 82.56%. In comparison, the performance of the improved method was better in SSL stream recognition.

The results of CapsNet's recognition of SSL VPN encrypted traffic were represented by a confusion matrix, as shown in Table 5.

In Table 5, TP means that traffic that belongs to class i is recognized as belonging to class i; FN means that traffic that belongs to class i is recognized as belonging to non-class i; FP means that traffic that does not belong to class i is recognized as belonging to class i; TN means that traffic that does not belong to class i is recognized as belonging to non-class i.

The evaluation indicators used in this paper are:

$$\text{Precision} = \frac{TP}{TP+FP},$$

$$\text{Recall} = \frac{\mathrm{TP}}{\mathrm{TP+FN}}.$$

First, the convergence rate of CapsNet was analyzed. The training period was set as 1000. The variation of the loss rate is shown in Figure 3.

It was seen from Figure 3 that the loss rate of the algorithm dropped rapidly in the early training period; when training times reached 200, the loss rate of the algorithm has dropped to below 0.1, and the loss rate also continued to drop afterward and finally stabilized. Figure 3 shows that the CapsNet optimized recognition algorithm had a high convergence speed.

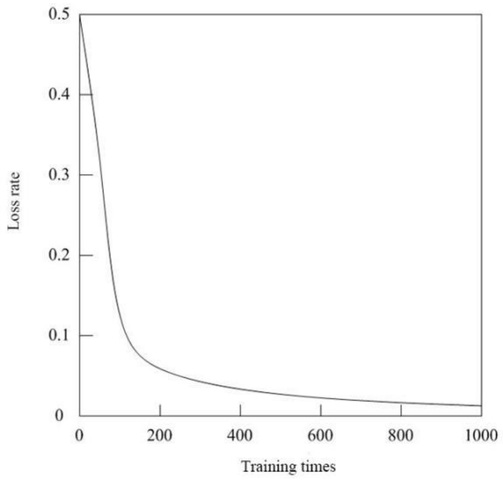

Figure 2Change in loss rate.

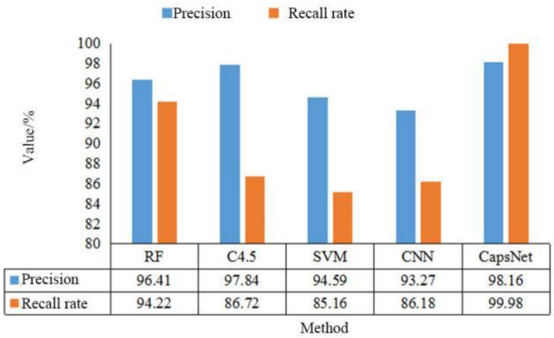

Figure 3Recognition results of SSL VPN encrypted traffic.

The CapsNet optimized recognition algorithm was compared with other algorithms, including Random Forest (RF) [12], C4.5 [13], Support Vector Machine (SVM) [14], and Convolutional Neural Network (CNN) [15], and the results are shown in Figure 4.

It was seen from Figure 4 that the CapsNet optimized recognition algorithm showed the best performance. First, the precision of the five methods was 96.41%, 97.84%, 94.59%, 93.27%, and 98.16%, respectively, and the precision of the CapsNet optimized recognition algorithm was the highest, which was 4.89% higher than CNN. Secondly, the recall rates of the five methods were 94.22%, 86.72%, 85.16%, 86.16%, and 99.98%, respectively; the recall rate of the CapsNet optimized recognition algorithm was the highest, which was 14.82% higher than SVM. The results verified that the CapsNet optimized recognition algorithm was effective in recognizing SSL VPN encrypted traffic, which can be further promoted and applied in practice.

5 Conclusion

This paper mainly analyzed the recognition of SSL VPN encrypted traffic and designed an improved fingerprint recognition method to identify SSL streams. The recognition algorithm was optimized by CapsNet to achieve the recognition of SSL VPN encrypted traffic. An experimental analysis was carried out on the

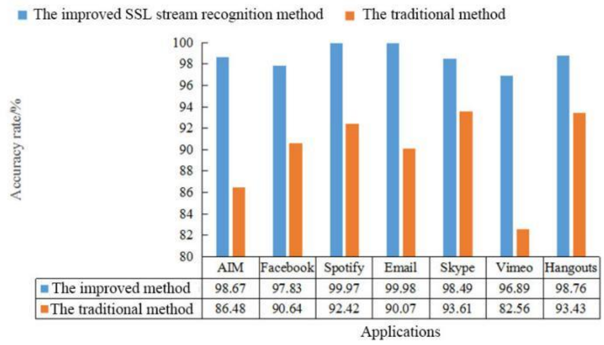

Figure 4The recognition results of SSL stream.

	Recognized as P	Recognized as N
Actually P	TP	FN
Actually N	FP	TN

Table 5Confusion matrix.

ISCXVPN2016 dataset. The results showed that the improved method had good recognition performance for SSL streams, with the highest accuracy (99.98%); it also had a good recognition performance for SSL VPN encrypted traffic, with a precision of 98.16% and a recall rate of 99.98 %, which were superior to the other algorithms. The CapsNet optimized recognition algorithm can be well applied in the recognition of practical network encrypted traffic.

References

[1] Saša Nikolić, and Jurij Šilc. Drupal 8 modules: translation management tool and paragraphs. *Informatica*, 40(1):145-152, 2016. https://doi.org/

[2] Yonghong Xu, and Jianguo Ren. Propagation Effect of a Virus Outbreak on a Network with Limited Anti-Virus Ability. *PLoS ONE*, 11(10):e0164415, 2016. https://doi.org/10.1371/journal.pone.0164415.

[3] Yuancheng Li, Rong Ma, and Runhai Jiao. A Hybrid Malicious Code Detection Method based on Deep Learning. *International Journal of Software Engineering and its Applications*, 9(5):205-216, 2015. https://doi.org/10.14257/ijseia.2015.9.5.21.

[4] Nicole Perlroth, and Binyamin Appelbaum. Federal Reserve Bank of St. Louis Confirms a Hacker Attack. *New York Times*, 164(56872):B2-B2, 2015.

[5] Weina Niu, Zhongliu Zhuo, Xiaosong Zhang, Xiaojiang Du, Guowu Yang, and Mohsen Guizani. A Heuristic Statistical Testing Based Approach for Encrypted Network Traffic Identification. *IEEE Transactions on Vehicular Technology*, 68(4):3843-3853, 2019. https://doi.org/10.1109/TVT.2019.2894290.

[6] Muhammad Zain ul Abideen, Shahzad Saleem, and Madiha Ejaz. VPN Traffic Detection in SSL-Protected Channel. *Security and Communication Networks*, 2019(5):1-17, 2019. https://doi.org/10.1155/2019/7924690.

[7] Jihoon Yoon, Kangsik Shin, and Yoojae Won. *Encrypted Network Traffic Analysis Method via*

Secure Socket Layer Handshake Control. Springer, Singapore, 2017.
https://doi.org/10.1007/978-981-10-5041-1_11

[8] Muhamed Elezi, and Bujar Raufi. Conception of Virtual Private Networks Using IPsec Suite of Protocols, Comparative Analysis of Distributed Database Queries Using Different IPsec Modes of Encryption. *Procedia - Social and Behavioral Sciences*, 195:1938-1948, 2015.
https://doi.org/10.1016/j.sbspro.2015.06.206.

[9] Alexander Uskov, and Hayk Avagyan. *Fusion of Secure IPsec-Based Virtual Private Network, Mobile Computing and Rich Multimedia Technology*. Springer, Cham, 2015.
https://doi.org/10.1007/978-3-319-14645-4_3

[10] Ki-Seok Byun, and Jun-Cheol Park. SSLmTCP Handshake: Embedding the SSL Handshake into the TCP 3-Way Handshake. *Journal of Korean Institute of Communications & Information Sciences*, 42(3):595-603, 2017.
https://doi.org/10.7840/kics.2017.42.3.595.

[11] Gerard Drapper Gil, Arash Habibi Lashkari, Mohammad Mamun, and Ali A. Ghorbani. Characterization of Encrypted and VPN Traffic Using Time-Related Features. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy(ICISSP 2016)*, Rome, Italy, SCITEPRESS – Science and Technology Publications, Setúbal, 407-414, 2016.
https://doi.org/10.5220/0005740704070414

[12] Prayag Tiwari, Hari Mohan Pandey, Aditya Khamparia, and Sachin Kumar. Twitter-based opinion mining for flight service utilizing machine learning. *Informatica*, 43(3):381-386, 2019.
https://doi.org/10.31449/inf.v43i3.2615.

[13] Monalisa Jena, and Satchidananda Dehuri. Decisiontree for classification and regression: a state-of-the art revie. *Informatica*, 44(4):405-420, 2020. https://doi.org/10.31449/inf.v44i4.3023

[14] Daniel Rodríguez-Martín, Albert Samà, Carlos Pérez-López, Andreu Català, Joan M. Moreno Arostegui, Joan Cabestany, Àngels Bayés, Sheila Alcaine, Berta Mestre, Anna Prats, M. Cruz Crespo, Timothy J. Counihan, Patrick Browne, Leo R. Quinlan, Gearóid ÓLaighin, Dean Sweeney, Hadas Lewy, Joseph Azuri, Gabriel Vainstein, Roberta Annicchiarico, Alberto Costa, and Alejandro Rodríguez-Molinero. Home detection of freezing of gait using support vector machines through a single waist-worn triaxial accelerometer. *Plos One*, 12(2):e0171764, 2017. https://doi.org/10.1371/journal.pone.0171764.

[15] Mohammed Kamel Benkaddour. CNN based features extraction for age estimation and gender classification. *Informatica*, 45(5):697-703, 2021.
https://doi.org/10.31449/inf.v45i5.3262