An Anonymous Network Website Fingerprinting Attack Method Based on Wavelet Transformation

Qi Lai and Jie Ling
Faculty of Computer, Guangdong University of Technology, 100 West Ring Road, Higher Education Mega Centre, Panyu District, Guangzhou, Guangdong, China.
Email: 2902173773@qq.com

Abstract. The anonymous network in protecting user privacy information, but also for the use of criminals, for its illegal acts, and increase the cover monitoring, tracking and obstacle of the government organs forensics, Aiming at the problem of anonymous network, this paper proposes a website fingerprinting attack method for TOR anonymous network. Wavelet transform is introduced to deal with the traffic generated by visiting the website. SVM algorithm is used to learn and generate classifiers, establish fingerprint feature library, and then compare the data generated by the target visiting website with the feature library to confirm its visiting website. In this way, the experimental results show that the average recognition accuracy of target visited websites is 96.7% under all known features of websites, which is superior to literature [17].

1. Introduction

With the rapid development of the Internet, people pay more and more attention to the protection of personal privacy. In e-commerce, online surfing and other network services, the security of users' personal information is becoming a new disaster area. Past security based on cryptography aims at the protection of information content, and can’t effectively hide the identity and communication mode of both sides of communication.

In order to protect users ‘freedom of speech and personal privacy from disclosure, Anonymous network has become an effective means to protect the identity of both sides of communication. A variety of anonymous networks have emerged, such as Crowds, Tor and Anonymizer and so on. Among them, Tor anonymous network has become one of the most widely used anonymous networks on the Internet due to its low latency, easy configuration and use, and stable and reliable services. However, while providing privacy protection for users, anonymous networks are also used by illegal elements to increase the cover for their illegal acts and hinder government agencies from monitoring, tracking and forensics. In order to protect the right of users to use the Internet normally and to strengthen the crackdown on online crime, and to strengthen the control of anonymous networks, literature [1-3] and literature [8-20] proposed attacks against anonymous networks. The attack methods based on traffic analysis are stream watermarking attack method [1-3] and Web Fingerprinting attack method (WFP) [4-6]. The core idea of stream watermarking method is to intercept the traffic between client and entrance, add marking features to the traffic, and determine the communication between sender and receiver by detecting the marking of the traffic of the exit node. The core idea of WFP is to analyze the traffic characteristics generated by anonymous communication and infer the relationship between anonymous network users. The existing work [7-19] to prove the feasibility of WFP on the anonymous Internet website of recognition, but how to choose the flow characteristics in order to improve the accuracy of the attack needs further research.
This paper presents a method of WFP on Tor anonymous network. The main idea is to use wavelet transform to extract features of traffic and improve the accuracy of identifying website.

2. Related Works in Wfp

In recent years, WFP has become a hot research topic. Literature [8] introduced WFP into anonymous networks such as JAP, Tor, Open SSH, Open VPN, Stunnel and CISCO IPsec-VPN. Using polynomial naive Bayesian classifier, the accuracy rate of identifying websites on 775 sites achieved 90% for single-hop anonymous systems. However, the multi-hop anonymous system is not ideal. Literature [9] According to the characteristics of Tor and other anonymous systems, it was proposed to generate fingerprint features by using the size, time and direction of traffic, and classify them by using Support Vector Machine (SVM). The experimental results showed that WFP was feasible in multi-hop low-delay communication system. Later, research on WFP on Tor anonymous networks has emerged. Researchers have found that converting data packets into cells for feature extraction can improve accuracy. Literature [10] rounded the packet size to a multiple of 600, and extracted sorting and numbers as features. The best string alignment distance is used as the SVM kernel function. Similarly, literature [11] reconstructed the transport layer security (TLS) record from the data packet, rounded the length to the nearest multiple of 512, designed a heuristic algorithm to delete Sendme units, and used a new distance-based measure in SVM, the accuracy reached 91%.

Literature [12-14] further improved WFP by selecting fingerprint feature processing methods and appropriate classifiers. Literature [12] used KNN to extract six types of features and iteratively adjust feature weights. Literature [13] used the cumulative method to sample features, which was robust to the dynamics of bandwidth, congestion and page loading time. Literatures [14] extended random forest technology, choose appropriate features, and carried out experiments on standard web pages and Tor hiding services.

Literature [15] has pointed out that the assumption of WFP on websites will have an impact on fingerprint attacks under real conditions. In order to solve this problem, literature [16] proposed several methods to make up for the gap between the laboratory environment and the actual conditions of fingerprint identification.

WFP is an attack method based on traffic analysis. This paper considers from the direction of traffic analysis. Literature [17] has proved that the feature sequence consisting of the size and direction of the data packet is self-correlated. A new method based on fast Fourier transform is introduced to calculate the similarity distance between the instance and the traffic pattern, so as to improve the efficiency and accuracy of feature extraction stage. Before that, no related research based on wavelet transform has been proposed. Inspired by this research, this paper introduces the way of wavelet transform to process data to extract features.

3. The Proposed Wfp

3.1. Process of the Method

The methods adopted in this paper are divided into feature collection and website recognition stages. The main task of feature collection is to collect traffic generated by visiting a large number of websites, process the traffic and extract fingerprint features. In this stage, wavelet transform is used to process data, and SVM algorithm is used to learn and generate classifiers to form fingerprint database. In the stage of website identification, the main task is to identify the website visited by the target host. In this stage, the purpose is achieved by the classifier generated in the first stage. As shown in the following figure 1:
The first stage of WFP is feature collection. When accessing anonymous networks, data packets can be obtained. Furthermore, the size and direction of the packet are obtained, so this method uses these two kinds of information to generate feature fingerprints.

3.2. The Steps and Instructions of the Method

Each instance of the datasets which is presented by $T_i$ in relation (1) is equivalent of vector of transmitting packets in a secure anonymous channel to load a website,

$$T_i = d_{i1}, d_{i2}, ..., d_{il}, \text{Where } d_{ik} = \pm s_{ik}$$  \hspace{1cm} (1)

In which $l$ is the number of packets in $i^{th}$ instance and it is considered as the actual length of $i^{th}$ instance; $d_k$ represents the $k^{th}$ packet; $s_k$ reflects the size of $k^{th}$ packet and $-$ or $+$ sign shows the direction of the packet:

- Fill in $T_i$ so that the length of each instance reaches L and the size of the filled data packet is 0. Experiments in literature [18] show that better results can be achieved when the number of data packets reaches 2048, so the value of L is 2048.
- Three-layer Mallat wavelet decomposition is carried out on each instance $T_i$ to get the approximate part $A_{i13}$. The experimental results show that choosing DB4 can improve the accuracy.
- Then the approximate part is reconstructed by Mallat algorithm to get $A_{i13}'$. Here the approximate component is taken as the feature of its visit to the website. Each of the same websites visits $n$ times, and there are $m$ websites. Machine learning is used to generate classifiers for $m*n$ features. Where $n = 40$.

To choose a machine learning algorithm in step C, according to the previous research results of [10] [11] show that the SVM algorithm has a better performance in the field, and chose to use the SVM algorithm to the training datasets. SVM is a typical two-class classifier, and the problem to be solved in experiments is multi-classification. When solving multi-classification problems with SVM algorithm, there are two common methods: One-against-one and one-against-all.

- One-against-one: The approach is to design a SVM between any two classes of samples, so $k(k-1)/2$ classifiers are needed for k-class samples. When classifying an unknown sample, the category that gets the most votes is the category of the unknown sample.
- One-against-all: it classifies the instances of one class against all the instances of the remaining classes. Therefore, it needs only $m$ distinct separators to classify all the different classes. Although this method is fairly fast, it has a low accuracy and asymmetric instances.

The advantage of the first method is that it does not need to retrain all SVM when adding a new website, so it is chosen. The proposed method uses SVM based on the Polynomial kernel with parameter $C = 10,000$ and the second strategy to solve the multiclass problem.
4. Results and Analysis

The dataset DS1 used in this experiment is to capture the traffic generated by users and entry nodes. The URLs are selected from Alexa global access list and the top 500 URLs are selected. Dataset DS2 is derived from literature [11].

The evaluation technology used is 10-fold cross validation, and the accuracy is used to measure the effectiveness of identifying the target website. The website detection effectiveness is measured by accuracy that is defined by (2).

\[
\text{accuracy} = \frac{TP}{TP + NP}
\]  

(2)

Where TP represents the number of instances correctly classified as True and NP represents the number of instances incorrectly classified as False.

Different wavelet functions have a certain impact on the accuracy rate. The experiment begins with DS1 to select the appropriate wavelet basis, with M = 100 as the fixed value. The experimental results are as follows:

| wavelet analysis | accuracy |
|------------------|----------|
| sym8             | 91.23%   |
| db4              | 97.91%   |
| haar             | 75.2%    |
| coif4            | 82.51%   |

The results showed that the treatment effect of db4 was better than the other three.

Figure 2 shows the change of the accuracy of website recognition in dataset DS1 with the increase of the number of training websites. It can be seen that this method has advantages in this dataset, and the average accuracy of calculation reaches 96.96%, which is higher than the results obtained in literature [17].

![Figure 2](image1.png)

**Figure 2.** Comparison of the accuracy of two kinds of WFP under DS1

![Figure 3](image2.png)

**Figure 3.** Comparison of the accuracy of two kinds of WFP under DS2

Figure 3 shows the change of site recognition accuracy in data set DS2 with the increase of the number of training websites. Data set DS2 comes from literature [8] removes all ACK packets from the data set and extracts Tor unit sequences. It can be seen that this method is superior to the Fourier transform-based WFP method. The average accuracy of calculation is 96.70%, which means that it is more accurate in identifying target websites.
5. Conclusion
In this paper, a method of WFP on Tor anonymous network is proposed. The collected data are decomposed by using multi-scale analysis of wavelet transform. The fingerprint feature database is generated by SVM algorithm, and the purpose of identifying the website visited by the target is achieved by using this feature library. The simulation experiments on DS1 and DS2 datasets show that the proposed method is more accurate than the fast Fourier transform based WFP method.

6. Acknowledgments
This work is supported by the science and technology project of Guangdong Province (No.2017B090906003) and the project of Guangzhou Science and Technology (No.201802010043, 201807010058).

7. References
[1] Yu W Fu X Graham S Xuan D and Zhao W 2007 May DSSS-based flow marking technique for invisible traceback 2007 IEEE Symposium on Security and Privacy (SP ’07) IEEE Symposium on pp 18-32
[2] Luo J Wang X and Yang M 2012 An interval centroid based spread spectrum watermarking scheme for multi-flow traceback. Journal of Network and Computer Applications 35(1) pp 60-71
[3] Wang X Chen S and Jajodia S 2007 May Network flow watermarking attack on low-latency anonymous communication systems 2007 IEEE Symposium on Security and Privacy (SP ) pp 116-130.
[4] Hintz A 2002 April Fingerprinting websites using traffic analysis International Workshop on Privacy Enhancing Technologies pp 171-178
[5] Sun Q Simon D R Wang Y M Russell W Padmanabhan V N and Qiu L 2002 May Statistical identification of encrypted web browsing traffic null p 19
[6] Bissias G D Liberatore M Jensen D and Levine B N 2005 May Privacy vulnerabilities in encrypted HTTP streams International Workshop on Privacy Enhancing Technologies pp 1-11
[7] Zhuo Z Zhang Y Zhang Z L Zhang X and Zhang J 2018 Website Fingerprinting Attack on Anonymity Networks Based on Profile Hidden Markov Model IEEE Transactions on Information Forensics and Security 13(5) pp 1081-1095
[8] Herrmann D Wendolsky R and Federrath H 2009 November Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naïve-bayes classifier Proceedings of the 2009 ACM workshop on Cloud computing security pp 31-42
[9] Panchenko A Niessen L Zinnen A and Engel T 2011 October Website fingerprinting in onion routing based anonymization networks Proceedings of the 10th annual ACM workshop on Privacy in the electronic society pp 103-114
[10] Cai X, Zhang X C, Joshi B and Johnson R 2012 October Touching from a distance: Website fingerprinting attacks and defenses Proceedings of the 2012 ACM conference on Computer and communications security pp 605-616
[11] Wang T and Goldberg I 2013 November Improved website fingerprinting on tor Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society pp 201-212
[12] Wang T, ai X, Niithyanand R, Johnson R and Goldberg I 2014 August Effective Attacks and Provable Defenses for Website Fingerprinting USENIX Security Symposium pp 143-157
[13] Panchenko A, Lanze F, Pennekamp J, Engel T, Zinnen A, Henze M and Wehrle K 2016 February Website Fingerprinting at Internet Scale Proc. 23 rd Internet Society (ISOC) Network and Distributed System Security Symp San Diego CA USA
[14] Hayes J and Danezis G 2016 August K-fingerprinting: A Robust Scalable Website Fingerprinting Technique USENIX Security Symposium pp 1187-1203.
[15] Juarez M, Afroz S, Acar G, Diaz C and Greenstadt R 2014 November A critical evaluation of website fingerprinting attacks Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security pp 263-274
[16] Wang T and Goldberg I 2016 On realistically attacking Tor with website fingerprinting Proceedings on Privacy Enhancing Technologies 2016(4) pp 21-36

[17] Jahani H and Jalili S 2016 A novel passive website fingerprinting attack on tor using fast fourier transform Computer Communications 96 pp 43-51

[18] Gu X, Yang M and Luo J 2015 May A novel website fingerprinting attack against multi-tab browsing behavior Computer Supported Cooperative Work in Design (CSCWD) 2015 IEEE 19th International Conference on pp 234-239

[19] Gu X, Yang M and Luo J 2015 Website Fingerprint Attack Method for SSH Anonymous Traffic Chinese Journal of Computers 38(4)