A Novel Network Flow Watermark Embedding Model for Efficient Detection of Stepping-stone Intrusion Based on Entropy

Yonghong Chen[1], **Shan Wang**[2]
[1]*College of Computer Science and Technology, Huaqiao University, Xiamen, China*
[2]*College of Computer Science and Technology, Huaqiao University, Xiamen, China*

Abstract - *Network flow watermarking schemes have been used to detect stepping stones, which including watermark embedding scheme and detection scheme. Among them, watermark embedding scheme plays a vital part in a watermarking scheme. Most existing watermark embedding schemes are based on using a randomly select the operation time interval and then generated watermark sequence in carrier flow. However, the randomness of watermark operating may cause watermark easily exposed to attacks. We herein propose a novel watermark embedding scheme based on entropy (NWESBE) to solve this problem. We firstly pre-process the carrier traffic by using entropy analysis and then determine optimum time intervals for embedding watermark. Secondly, we randomly embed watermark in these determined time intervals. Our analytical and empirical results demonstrate that our proposed scheme is robust for embedded watermark to timing perturbation, while invisible to attacks. And also it can greatly improve the detection rate and requiring fewer observation packet.*

Keywords: Network Flow Watermark; Entropy; Stepping-stone Intrusion Detection; Active Traffic Analysis

1 Introduction

In order to hide identity, Internet attackers commonly relay their traffic through a number of compromised hosts, called stepping stones [1]. Detecting such hosts is an important problem in computer security [2]. There are a lot of researches on the detection method of stepping stone, but most of it is passive traffic analysis method. More recently, comparing with traditional approaches [3-5], an active approach called watermarking has been more considered [6], with higher accuracy and detection efficiency, which traffic characteristic of an incoming flow are actively perturbed as they traverse some router to create a distinct pattern, which can later be recognized in outgoing flows.

A watermarking scheme is composed of the watermark embedding module and the detection module. The watermark embedding module is responsible for embedding the watermark by modulating the target flow. It not only affects the robustness and invisibility of embedded watermark, but also directly affects detection efficiency of the corresponding detection module. Therefore, a watermark embedding scheme plays a vital part in a watermarking scheme. Recently, many watermark embedding schemes have been proposed. ICBW [7], DICBW [8], IBW [9], where watermark embedding by manipulating packet counts of preselected interval pairs. In [10-12], authors developed packet-based watermarking by inflating or deflating an inter-packet delay (IPD). References [13-15] provided based on speed of traffic watermark embedding schemes. Among them, most existing watermark embedding schemes subdivide the network flow into short fixed-length intervals and perform transformative operations on an entire interval of packets for the purpose of modifying flow characteristics [16]. Unfortunately, the operation time interval is determined randomly, with the uncertainty of traffic information, such watermark embedding techniques will cause watermark easily expose to attackers and resulting in watermark effective weakened. We herein propose a novel watermark embedding scheme based on entropy (NWESBE) to solve this problem.

Entropy is the description of uncertainty of the random variable in information theory, which can be used as a metric of the amount of information [17]. In this paper, we firstly sample a fixed time interval T and statistic the packet bit entropy in per T, and then determine appropriate time interval for embedding watermark by comparing with the determined entropy threshold. It is well know that the greater entropy value of variables, indicating the greater the random degree of the variable, that is the greater the amount of contained information. We select time interval containing a large amount of information, namely a large entropy value to manipulate the inter-packet delays. Therefore, watermark information can be ignored when a few special watermark all are embedded in the time interval of a large amount of traffic information instead of the time interval of uncertain information.

The contribution of this paper is to use entropy to pre-process the carrier flow qualitatively and quantitatively, and select the appropriate time interval instead of the random selection of time interval to embed watermark information. Analytical and experimental results show that our proposed NWESBE is very effective, which not only can improve the invisibility and robustness of embedded watermark, but also can directly affect detection rate of watermark and detection efficiency of a watermarking scheme, with requiring fewer observation packets.

The rest of this paper is arranged as follows. In Section 2, we design a novel watermark embedding scheme, called NWESBE. Experimental results and discussion are given in Section 3. Finally, this paper is concluded in Section 4.

2 A Novel Network Flow Watermarking Model

In this section, we present a design of the NWESBE network watermark embedding scheme, which is an innovation of previous research work about network watermark embedding scheme.

2.1 Background of entropy

The definition of entropy is assumed to be, herein, the one introduced into the information theory [18], which describes entropy as a measure of the degree of uncertainty of a given random variable [19]. In this content, the entropy value is greater, indicating that the more amount of information transmitted by the variable of information source. Conversely, the smaller the entropy value, indicating that the amount of information that the variable transmission source is less. Therefore, entropy can be used as a metric for the amount of information, can effectively response the distribution of information content of network traffic.

The formal description of Entropy is given by expression (1) and denoted by $H(x)$ where x represents the number of values in the observation pool, and $p(x_i)$ denotes the probability of occurrence of a given valuex_i,

$$H(X) = -\sum_{i=1}^{n} p(x_i) log p(x_i) \tag{1}$$

2.2 A novel watermark embedding scheme

We take advantage of the entropy in information theory and watermark generated based on inter-packet delays (IPD) to propose our watermark embedding scheme. In our watermark embedding scheme, mainly including two key steps.

Step 1: Determine the appropriate time period for embedding watermark

In our approach, we first acquire carrier flow and real-time calculate bit entropy of per packet within the unit time interval. The concrete calculation procedures are as follows:

(1) The probability of packet size $P_{i,j}$ is given by

$$P_{i,j} = \frac{p\_size(i,j)}{p\_size\_sum(i)} \tag{2}$$

Where $p\_size(i,j)$ denotes per packet size in a time interval T, $p\_size\_sum(i)$ denotes the sum of packet size in this time interval.

(2) According to formula (1), we can get the bit entropy of packet within the unit time interval：

$$H_i = -\sum_{j=1}^{N_i} p_{i,j} log p_{i,j} \tag{3}$$

(3) In this paper, we derive the appropriate time interval for embedding watermark by finding the entropy value that it can reflect the amount of information. The particular entropy value is selected by the following equation (4). If H_i satisfies equation (4), there is an appropriate time interval, which showing the large amount of information content.

$$H_i > H_{threshold} \tag{4}$$

Where $H_{threshold}$ denotes entropy threshold. We using a statistical method involving the mean to obtain an entropy threshold before embedding watermark.

Step 2: Watermark generating

From Step 1, we obtain the appropriate time interval for watermark embedding. Then we will embed watermark in this time interval. The way of generating watermark information similar to the RAINBOW [6] watermark embedding scheme, which insert a watermark value by delaying some packets.

Suppose that the determined time interval from the carrier flow with the packet timing information $\{t_1^u, t_2^u, \dots, t_n^u\}$. Before embedding watermark, the inter-packet delays (IPDS) of the carrier flow $T_i^u = t_{i+1}^u - t_i^u$ .The watermark is subsequently embedded by delaying the packets by an amount such that the IPD of ith watermarked packet is $\{ T_i^w = T_i^u + w_i \}$. At the same time, we record the IPDS sequence of watermarked packets in a database, used as a special pattern for detecting stepping stone intrusion by comparing with the time delay pattern from the watermark detector.

The watermark components $\{w_i\}_{i=1}^n$ take values $\mp$a with equal probability:

$$w_i = \begin{cases} +a & w \cdot p \cdot \frac{1}{2} \\ -a & w \cdot p \cdot \frac{1}{2} \end{cases} \tag{5}$$

The value a is chosen to be small enough so that the artificial jitter caused by watermark embedding is invisible to ordinary users and attackers. We present our watermark embedding scheme in Fig.1.

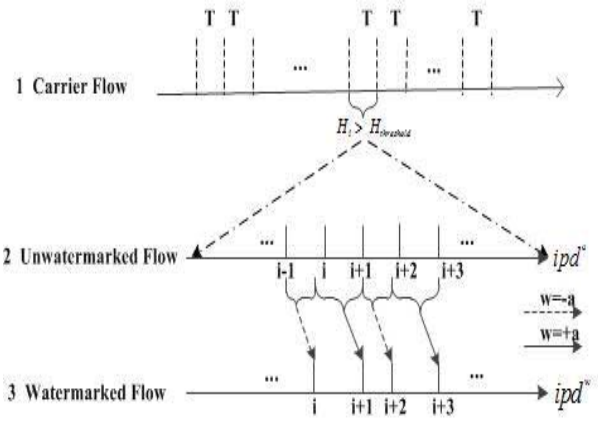

Fig.1 NWESBE watermark embedding scheme

2.3 Watermark detecting

The watermark detection works is a non-blind manner and therefore the detector had access to the database where the watermarked flow are recorded. Similar to the RAINBOW detector, normalized correlation as a detection scheme for watermark. First, we receive a flow detector subtracts its inter-packet delays (IPD). Then calculated correlation metric by comparing with the IPD pattern from the database and the detector decide whether the candidate flows is watermarked. Finally the detector decide whether the two flows are linked or not, so as to determine whether the host is a stepping-stone. A normalized correlation is defined as:

$$\mathrm{N}(a,b) = \frac{< a, b >}{\|a\| \cdot \|b\|} = \frac{\sum_{i=1}^{n} a_i b_i}{\sqrt{(\sum_{i=1}^{n} a_i^2)(\sum_{i=1}^{n} b_i^2)}} \quad (6)$$

3 Experimental result and analysis

In this section, we display our experimental results after applying our proposed watermark embedding scheme. We implemented a real-time watermark scheme consist of four sections as shown in Fig.2 to evaluate the performance of the novel watermark embedding scheme and compare the results with the previous work [11]. We simulated the RAINBOW and NWESBE schemes in NS2 platform [20].

In our experiments, the network flows are generated at the *Client* by injecting real dataset "The CAIDA Anonymized Internet Traces 2015" [21] into the NS2. Then watermark information was embedded at the *Watermarker*. The watermarked flow was perturbed with random delays at *Perturber* to simulate the timing perturbation. The *Detector* extracted the watermark from the received flow. The same set of experiments was conducted to test the RAINBOW watermark embedding scheme, which is recently a good watermark scheme. We choose average used packet numbers, detection rate, invisibility and robustness of watermark as measures to consistently compare watermark embedding scheme *Watermarker*.

There needs to be mentioned is that we have done a lot of repeated experiments, each experiment is run for more than 20 times. The experimental data obtained in this paper are the average of the 20 times repeated experiments. In the following, we evaluate the performance of the proposed watermark embedding schemes by detection rate, Robustness against timing perturbation, invisibility of watermark and expenditure of time.

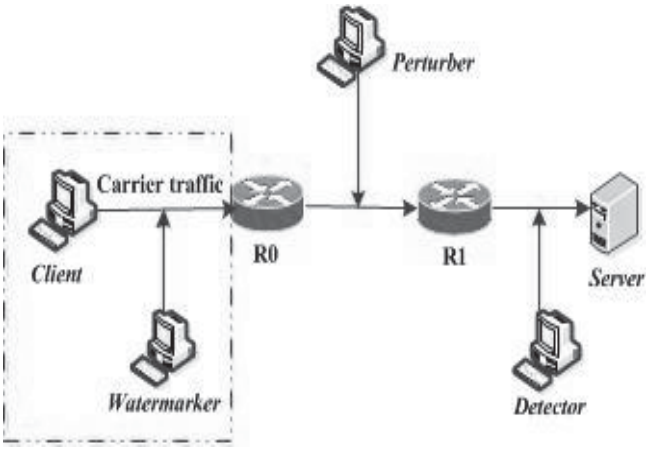

Fig.2 Experiment setup

3.1 Accuracy without timing perturbation

This experiment measured the detection rate of our proposed method and RAINBOW (recently an advanced watermarking scheme), respectively, without timing perturbation. The result in Fig.3 shows that the watermark detection rate of the RAINBOW watermark embedding scheme and NWESBE watermark embedding scheme change as the embedded watermark length increases. And the final watermark detection result using the RAINBOW scheme has great randomness, reflecting in the unstable watermark detection rate, while the watermark detection result using the NWESBE scheme is relatively stable. From Fig.3, compared to the RAINBOW, our proposed scheme to achieve higher watermark detection rate at same experiment sets. It means that using entropy to determine the appropriate time interval can guarantee the validity of embedded watermark and improve the accuracy of watermark detection. Hence, we can know that there is a significant advantage in using entropy to embed watermark over the RAINBOW under ideal conditions.

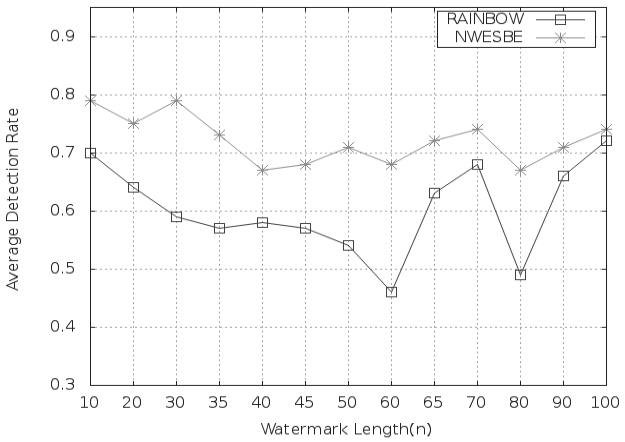

Fig. 3 Detection rate comparison between the two watermark embedding schemes

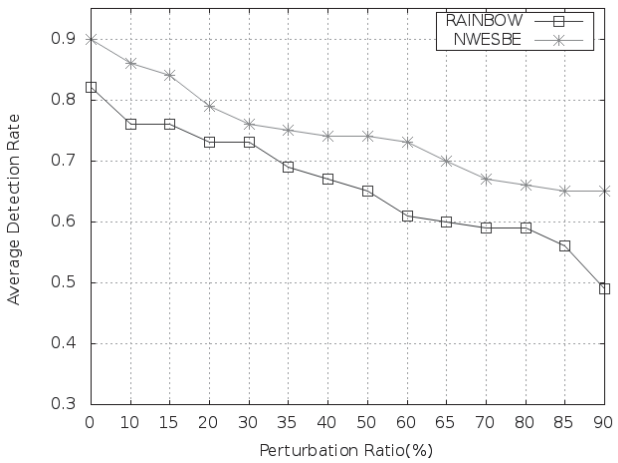

Fig. 4 A comparison of detection rate under timing perturbation

3.2 Robustness against timing perturbation

We also observe that active robustness is likely to be impossible to achieve at the same time. To demonstrate the robustness of our method against active time perturbation, which was modeled using uniformly random delays, we measured the detection rates of the NWESBE and RAINBOW, respectively, for different perturbation ratio as shown in Fig.4. From Fig.4, with the increase of perturbation ratio, the watermark detection rate based on two different watermark embedding method presenting a trend of downward, indicating that the robustness of watermark is affected by the timing perturbation. But, compared to the RAINBOW, the NWESBE scheme always achieve higher detection rate in the same perturbation ratio condition. Therefore, in our watermark embedding scheme, watermark are more resilient to an adversary who actively tries to remove them from the carrier flow, which they still alive after the interference by timing perturbation. We select the time interval contained a large amount of information for embedding watermark in our scheme. By this way, we find that watermark will introduce little distortion, in that they will not significantly impact the performance of the flows. The analysis results illustrated that the NWESBE based entropy analysis for watermark embedding is more robust against timing perturbation compared with the RAINBOW scheme.

3.3 Average number of packets used

Given a fixed detection rate (80%), Fig.5 gives a comparison of the packet numbers needed by the two watermark embedding methods as watermark length increase, which including 20 times repeated experiments. Compared to the RAINBOW, when fixed same watermark length, the NWESBE scheme only requires less than 10000 packets to achieve same detection rate, while the RAINBOW requires far more than 10000 packets under the same watermark detection framework.

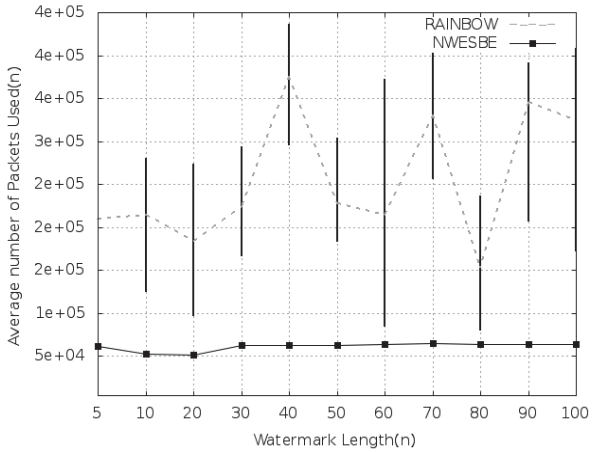

Fig. 5 Average number of packets under watermark length

From Fig.5, we also found that average number of packets required changes fluctuate widely as the change of the watermark length if watermark are embedded using the RAINBOW scheme, while it maintains a steady state using the NWESBE scheme. The result demonstrates that the randomness of watermark embedding may increase the burden of the watermark detection module and reduce the efficiency of detection.

Table 1 demonstrates that the average number of packets needed by the two watermark embedding methods, with achieved different detection rate. We can see that there is a significant advantage in using our proposed scheme, which seems to reduce packet number up to 60% compared to RAINBOW. The results show that RAINBOW requires longer observation duration leading to low efficiency of detecting stepping stones. Therefore, our proposed scheme are more efficient, with shorter observation periods necessary.

Table 1: Average number of packets required under achieved same detection rate

Detection rate	Average number of packets used	
	NWEBSBE	RAINBOW
20	78476	232970
40	63058	314474
60	63538	300164
80	64195	298934
100	63402	451946

3.4 Invisibility of watermark

Watermark are embedded in the time interval of randomly selected by the RAINBOW scheme, which may result in the exposure of the embedded watermark and causing the attacker to malicious operation of the watermark. We propose a watermark embedding scheme that selecting the appropriate time interval with a large amount of information by using entropy to preprocess the carrier flow before embedding watermark. In our scheme, all watermark information are embedded in the larger amount of information and watermark information almost can be ignored, compared to RAINBOW, the embedded watermark can only introduce minute changes to the carrier flow, which ensuring invisibility of the embedded watermark.

4 Conclusions and future work

In this paper, we propose a novel watermark embedding scheme by using entropy to determine time intervals of watermark operating, which can help to detect intrusions in the network more accurately and efficiently.

The essence of our proposed method is to hide information in the network flow characteristics. In our watermark embedding scheme, all watermark information will be embedded in these time intervals of a large amount of information by using entropy preprocessing the carrier flow instead of embedding in the time interval of randomly determined. Experiments confirm that our proposed watermark embedding technology is effective and can help watermarking scheme more effectively detect stepping-stone intrusion.

Entropy presents different forms in different scenarios, our future work is to apply different forms of entropy to the watermarking schemes, thus providing more effective watermarking scheme.

Acknowledgement

We would like to thank the anonymous reviewers for their insightful comments. This paper is supported by the National Natural Science Foundation of China (No. 61370007) and Natural Science Foundation of Fujian Province of China (No. 2013J01241).

5 References

[1] Houmansadr A, Borisov N. "SWIRL: A Scalable Watermark to Detect Correlated Network Flows." *NDSS*. 2011.

[2] Yang J, Woolbright D. Correlating TCP/IP Packet Contexts to Detect Stepping-stone Intrusion [J]. Computers & Security, 2011, 30(6): 538-546.

[3] Huadong Wang, Jiang Zhong, Ang Li, Network Intrusion Detection Based on Artificial Immune Clustering [J], Journal of Information and Computational Science, 10(10), 2013, 3003-3012

[4] Laia Q, Linb Y., A Novel Network Intrusion Detection System Based on Bayesian Inference: IDS-BI [J], Journal of Information and Computational Science, 12(11), 2015, 4369-4376

[5] Xie K, Yang Y, Zhang L, et al. Research of Hierarchical Intrusion Detection Model Based on Discrete Cellular Neural Networks [J], Journal of Information and Computational Science, 10(17), 2013, 5569-5578

[6] Houmansadr A, Borisov N. Towards Improving Network Flow Watermarks Using the Repeat-accumulate Codes [C], IEEE/ACM Transactions on Networking, Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on, IEEE, 2011, 1852-1855

[7] Luo J, Wang X, Yang M. An Interval Centroid Based Spread Spectrum Watermarking Scheme for Multi-flow Traceback [J], Journal of Network and Computer Applications, 35(1), 2012, 60-71

[8] Wang X, Luo J, Yang M. A Double Interval Centroid-based Watermark for Network Flow Traceback [C], Computer Supported Cooperative Work in Design (CSCWD), 14th International Conference on, IEEE, 2010, 146-151

[9] Pyun Y J, Park Y, Reeves D S, Interval-based Flow Watermarking for Tracing Interactive Traffic [J], Computer Networks, 56(5), 2012, 1646-1665

[10] Wang X, Chen S, Jajodia S, Network Flow Watermarking Attack on Low-latency Anonymous Communication Systems [C], Security and Privacy, SP' 07, IEEE Symposium on, IEEE, 2007, 116-130

[11] Houmansadr, A., Kiyavash, N., Borisov, N., Non-blind Watermarking of Network Flows, IEEE/ACM Transactions on Networking (TON), 22(4), 2014, 1232-1244

[12] Gong, X., Rodrigues, M., Kiyavash, N., Invisible Flow Watermarks for Channels with Dependent Substitution, Deletion, and Bursty Insertion Errors [J], Information Forensics and Security, IEEE Transactions on, 8(11), 2013, 1850-1859

[13] Huang J, Pan X, Fu X, Long PN Code based DSSS Watermarking [C], INFOCOM, 2011 Proceedings IEEE, IEEE, 2011, 2426-2434

[14] Yu W, Fu X, Graham S, DSSS-based Flow Marking Technique for Invisible traceback [C], Security and Privacy, SP' 07, IEEE Symposium on, IEEE, 2007, 18-32

[15] Jia, W., Tso, F. P., Ling, Z., Fu, X., Xuan, D., Yu, W., Blind Detection of Spread Spectrum Flow Watermarks [J], Security and Communication Networks, 6(3), 2013, 257-274

[16] Wang X, Yang M, Luo J., A Novel Sequential Watermark Detection Model for Efficient Traceback of Secret Network Attack Flows [J], Journal of Network and Computer Applications, 36(6), 2013, 1660-1670

[17] Ma, X., Chen, Y., DDoS Detection Method Based on Chaos Analysis of Network Traffic Entropy [J], Communications Letters, IEEE, 18(1), 2014, 114-117

[18] Shannon C E., A mathematical theory of communication [J], ACM SIGMOBILE Mobile Computing and Communications Review, 5(1), 2001, 3-55

[19] Gomes J V P, Inácio P R M, Freire M M, et al. Analysis of Peer-to-peer Traffic Using a Behavioural Method Based on Entropy [C], Performance, Computing and Communications Conference, 2008, IPCCC 2008, IEEE International. IEEE, 2008, 201-208

[20] Issariyakul T, Hossain E. Introduction to Network Simulator NS2, Springer Science & Business Media, 2011

[21] The CAIDA UCSD Anonymized Internet Traces 2015, Downloadable from http://www.caida.

[22] The CAIDA UCSD Anonymized Internet Traces 2015, Downloadable from http://www.caida.org/data/passive/passive_2015_dataset.xml/