ISBN: 978-981-18-1791-5
2021 the 11th International Workshop on Computer Science and Engineering (WCSE 2021)
doi: 10.18178/wcse.2021.06.033

AEMT: An Analytic Hierarchy Process-based Evaluation Model for IP Traceback

Hongcheng Tian [1+] , Jinting Dai [2] and Shiyu Ji [1]

[1] Medical Supplies Center, Chinese PLA General Hospital, China
[2] Zhengzhou University, China

Abstract. Distributed denial of service attacks continue to pose major threats to the Internet. Attackers often forge source addresses to escape detection, how to effectively trace the attackers back is an important issue of Internet security. Researchers have proposed various IP traceback schemes, but for these schemes, there exist some shortcomings in the aspects of computation overhead, storage overhead, traceback accuracy, traceback time and so on. Furthermore, in the field of IP traceback, comparisons among different IP traceback methods are mainly ones of multiple evaluation indexes one by one, and there does not exist an evaluation model (or an evaluation method) to comprehensively evaluate different schemes. The paper has proposed an analytic hierarchy process-based evaluation model for IP traceback (AEMT). Subsequently, the paper takes the network supervision department (an evaluator) and selecting a method under all scenes for the random deployment (a model target) for example, and applies AEMT to evaluate four typical traceback methods based on unified simulation experiments. In the end, the evaluation result conforms to the design and application characteristics of traceback methods. AEMT can supply the traceback field with an evaluation model, which can comprehensively quantitatively evaluate different traceback schemes.

Keywords: IP traceback, evaluation model, analytic hierarchy process

1. Introduction

Due to the defects of TCP/IP protocol, Internet does not verify the authenticity of the source address of any packet, but only routes the packet according to its destination address, and attackers often forge source addresses to attack remote hosts or networks, avoiding being caught. How to effectively trace back the attackers is one of the important research contents in the field of Internet security. Although researchers have proposed a variety of methods for IP traceback, these methods have some defects in computing cost [1~15], storage cost [1~6], traceback accuracy [7~15], or traceback speed [7~15]. So far, there is no one traceback method, whose evaluation indexes are all the best. At present, there is a lack of an evaluation model (or a method) to make an overall and comprehensive evaluation on different traceback methods.

This paper summarizes five evaluation indexes of IP traceback methods: computation overhead, storage overhead, false positive ratio, false negative ratio, and traceback time, and establishes an analytical hierarchy process-based evaluation model for IP traceback (AEMT). And this paper takes the network supervision department (an evaluator) and selecting an optimal method under all scenes for the random deployment (Definition 1) (a model target) for example, and applies AEMT to comprehensively evaluate four typical traceback methods based on the unified simulation experiments: source path isolation engine (SPIE) [1], SampleTrace [2], compressed edge fragment sampling (CEFS) [7] and adaptive probabilistic marking scheme (APMS) [8]. In the end, the evaluation gives the ranking of these four methods, and the evaluation result also conforms to the design and application characteristics of the four traceback methods. AEMT can be used for comprehensive evaluation on different traceback methods.

2. An Analytic Hierarchy Process-Based Evaluation Model for IP Traceback

AEMT (Fig. 1) consists of three levels. And from top to bottom, there are the first, the second and the third levels. The model target A of the 1st level can be selected by a evaluator, for example, to select an

+ Corresponding author. Tel.: + 86 15201183281.
E-mail address: thc@pku.org.cn.

optimal traceback method; The 2nd level is the index level, which is composed of evaluation indexes, such as computation overhead (B_1), storage overhead (B_2), false positive ratio (B_3), false negative ratio (B_4), and traceback time (B_5); The 3rd level is the method level, which is composed of evaluation methods, for example, method 1, method 2, …, and method *p*; The model target A of the 1st level dominates the five factors B_i ($1<=i<=5$) of the 2nd level, and there exists a sub level between the 2nd and the 3rd levels, which is called the sub level of the 2nd one, and factors of the sub level are called the sub ones.

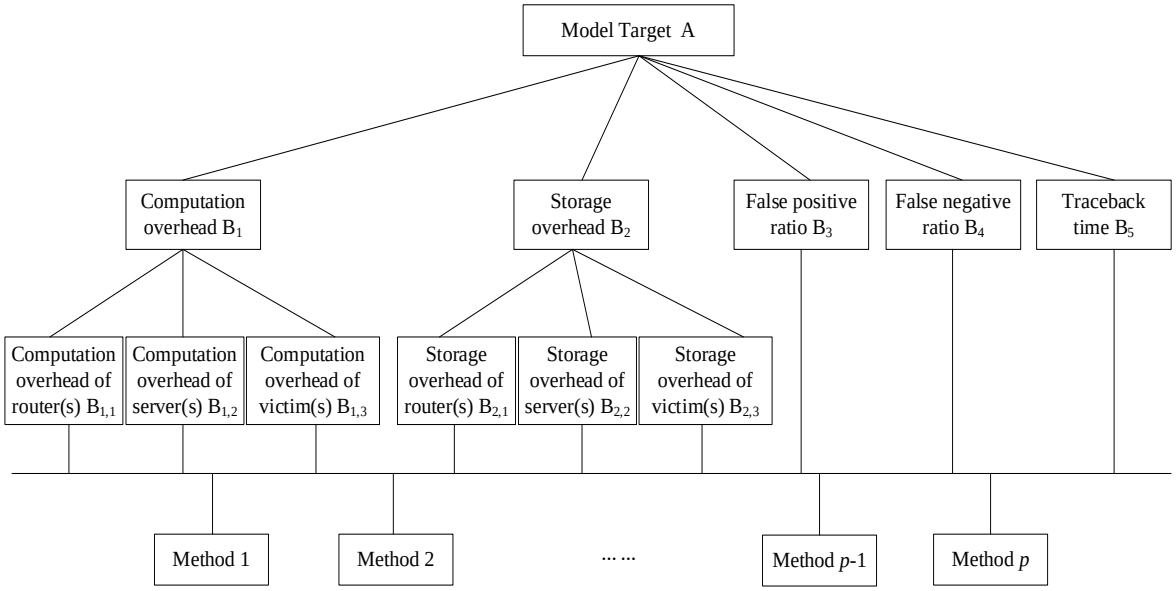

Fig. 1: An analytic hierarchy process-based evaluation model for IP traceback (AEMT).

Computation overhead (B_1) measures the computational cost of traceback methods. B_1 dominates the following three sub factors: computing overhead of a router ($B_{1,1}$), computing overhead of a server ($B_{1,2}$), computing overhead of a victim ($B_{1,3}$), and the above three factors are in milliseconds. Storage overhead (B_2) weighs the storage cost of traceback methods. B_2 dominates the following three sub factors: storage overhead of a router ($B_{2,1}$), storage overhead of a server ($B_{2,2}$), storage overhead of a victim ($B_{2,3}$), and the above three factors are in bits. False positive ratio (B_3) and false negative ratio (B_4) measure traceback accuracies of traceback methods. Traceback time (B_5) weighs the traceback speed of traceback methods, which is in milliseconds.

3. Evaluating 4 Traceback Methods based on AEMT

The difference of evaluators will affect the following two weight vector values of single hierarchical arrangement: the former is the one that the 2nd level is relative to the 1st level, and the latter is the one that the sub factors of the 2nd level is relative to the corresponding father factors. And this will ultimately influence the ranking that the evaluation methods of the 3rd level are relative to the model target. This paper chooses the network supervision department as the evaluator.

3.1. Simulation Experiment

We make simulation experiments of four traceback methods under all scenes for the random deployment, and we make statistics on 9 experimental values: $B_{1,1}$, $B_{1,2}$, $B_{1,3}$, $B_{2,1}$, $B_{2,2}$, $B_{2,3}$, B_3, B_4 and B_5. Furthermore, each experimental value is represented by a 2-dimensional vector [mean value, mean square deviation]. mean values and mean square deviations of 9 experimental values are smaller, 9 experimental values better, so the best 2-dimensional vector, *OPT*, used in the simulation experiments is O, which is [0 0]. Moreover, λ_1=1, λ_2=0.9.

3.1.1. Experimental Design

Each experimental scenario (defined by seven parameters) is determined by the deployment scenarios (defined by five parameters) and the attacking scenarios (defined by two parameters). In the experiments, all

network attacks simulate DDoS attacks, and one experiment scenario corresponds to one DDoS attack one by one.

1) The deployment scenarios. The deployment scenario is specified by five parameters: the experimental topology, the victim AS, deployment strategy, deployment rate and sampling rate (marking probability).

a. The experimental topology and the victim AS. This paper uses BRITE to generate 5 topologies for each scale of 100, 400, 1000 and 3000 ASes. Furthermore, the BA model is chosen as the model paremeter to generate the topologies. Thus, there are 20 topologies in total. In this paper, from each of these 20 topologies, 5 ASes are randomly selected to do experiments respectively so that there are 100 cases.
b. Deployment strategy. Random deployment is that a number of ASes in the experimental topology are randomly selected as deployed ones, while the strategy deployment is to sort the degrees of ASes in the experimental topology from high to low, and the ASes with higher degrees will be deployed first.
c. Deployment rate. The optional values of the deployment rate are 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% and 100%. In addition, it is assumed that the victim ASes are deployed.
d. Sampling rate (marking probability).

The marking probability of deployed ASes in CEFS is the same as the sampling probability of deployed AS in SampleTrace.

2) The attacking scenarios. The attacking scenarios are specified by 2 parameters: the attacking scale and the attacking flow characteristic.

a. The attacking scale. A certain proportion of ASes in each topology are randomly chosen as the attacking sources to send attacking packets to the victim AS, which is the attack scale. The same AS can be selected to send attacking packets to the victim AS multiple times. In this experiment, the optional values of the attack scale are 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% and 100%.
b. The attacking flow characteristic. The attacking flow characteristic is the number of attacking packets contained in an attack flow. In the experiments, the attack flow characteristic has six values: 1, 10, 50, 100, 200 and random number of attacking packets from 1 to 200.

Definition 1 All scenes for the random deployment: In the seven parameters which determines an experimental scenario, the deployment method is random deployment, and the other six parameters randomly select all the values in their own value ranges to get the set of experimental scenarios.

3.1.2. Experiment Results

Based on the experimental results under all scenes for the random deployment, according to [18], we can obtain the weight vectors of single hierarchical arrangement, that the 3rd level is relative to the factors and sub factors of the 2rd level (Fig. 2).

3.2. Evaluation on 4 Traceback Methods

In this paper, from the viewpoint of the network supervision department (the evaluator), we choose an optimal method under all scenes for the random deployment as the model target to comprehensively evaluate four traceback methods based on AEMT.

Under the premise of not wronging people, the network supervision department hopes to find the people who do bad things. If the false positive ratio and the false negative ratio of a traceback method is lower and the traceback speed is faster, the network supervision department considers that the traceback method is better.

As the user of traceback service, the network supervision department is most concerned about the false positive ratio, the false negative ratio and traceback speed, not about the storage and computing overheads of traceback service providers. According to [18], by pairwise comparison of B_i ($1 \le i \le 5$), the weight vector of single hierarchical arrangement, that B_i ($1 \le i \le 5$) is relative to the model target, is

$$\boldsymbol{V}_2^{(1,1)} = [0.0415\ 0.0415\ 0.4555\ 0.2862\ 0.1753]^{\mathrm{T}} \quad (1)$$

The network supervision department cares about its own computing overhead, but not about the computing overheads of traceback service providers. According to [18], by pairwise comparison of $B_{1,i}$ ($1 \le i \le 3$), the weight vector of single hierarchical arrangement, that $B_{1,i}$ ($1 \le i \le 3$) is relative to B_1, is

	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$	$B_{2,1}$	$B_{2,2}$	$B_{2,3}$	B_3	B_4	B_5
SPIE	0.0086	0.3333	0.3333	0.0236	0.3333	0.2500	0.2788	0.2789	0.3333
SampleTrace	0.3331	0.0000	0.3333	0.3333	0.0000	0.2500	0.2766	0.2875	0.3333
CEFS	0.3333	0.3333	0.1252	0.3239	0.3333	0.2500	0.2057	0.2135	0.1252
APMS	0.3250	0.3334	0.2082	0.3192	0.3334	0.2500	0.2389	0.2201	0.2082
	$V_3^{(2,1,1)}$	$V_3^{(2,1,2)}$	$V_3^{(2,1,3)}$	$V_3^{(2,2,1)}$	$V_3^{(2,2,2)}$	$V_3^{(2,2,3)}$	$V_3^{(2,3)}$	$V_3^{(2,4)}$	$V_3^{(2,5)}$

Fig. 2: The weight vectors of single hierarchical arrangement, that the 3rd level is relative to the factors and sub factors of the 2rd level under all scenes for the random deployment, respectively.

$$\boldsymbol{V}^{(2,1)}= [0.0909\ 0.0909\ 0.8182]^{\mathrm{T}} \tag{2}$$

The network supervision department are concerned about its own storage overhead, but not about the storage overheads of traceback service providers. According to [18], by pairwise comparison of $B_{2,i}$ ($1\leq i\leq 3$), the weight vector of single hierarchical arrangement, that $B_{2,i}$ ($1\leq i\leq 3$) is relative to B_2, is

$$\boldsymbol{V}^{(2,2)}= [0.0909\ 0.0909\ 0.8182]^{\mathrm{T}} \tag{3}$$

According to [18] and Fig. 2, the weight vectors of single hierarchical arrangement, that the 3rd level is relative to B_1 of the 2nd level, is

$$\boldsymbol{V}_3^{(2,1)}=[0.3038\ 0.3030\ 0.1630\ 0.2302]^{\mathrm{T}} \tag{4}$$

According to [18] and Fig. 2, the weight vector of single hierarchical arrangement, that the 3rd level is relative to the factor B_2 of the 2nd level, is

$$\boldsymbol{V}_3^{(2,2)}=[0.2370\ 0.2348\ 0.2643\ 0.2639]^{\mathrm{T}} \tag{5}$$

Thus, the weight matrix of single hierarchical arrangement, that the 3rd level is relative to the 2nd level, is

$$\boldsymbol{M}_3^{(2)}= \begin{bmatrix} 0.3038 & 0.2370 & 0.2788 & 0.2789 & 0.3333 \\ 0.3030 & 0.2348 & 0.2766 & 0.2875 & 0.3333 \\ 0.1630 & 0.2643 & 0.2057 & 0.2135 & 0.1252 \\ 0.2302 & 0.2639 & 0.2389 & 0.2201 & 0.2082 \end{bmatrix} \tag{6}$$

Thus, according to [18], the weight vector of overall hierarchical arrangement of the 3rd level is

$$\boldsymbol{W}_3^{(1)}= [0.2877\ 0.2890\ 0.1945\ 0.2288]^{\mathrm{T}} \tag{7}$$

From the perspective of the network supervision department (the evaluator), the optimal method is selected under all scenes for the random deployment (model objective), and among the 4 traceback methods, SampleTrace is the best, SPIE is the second best, APMS is the second, and CEFS is the lowest. In the packet marking methods for IP traceback, there are legal marks, forged marks and original domain semantic information in the marking areas of packets received by the victim, which is difficult for the victim to distinguish from each other. But As the collected path information, they participate in the reconstruction of attacking paths, which not only brings a large false positive ratio, but also brings a large computational overhead, and this results in a long traceback time. SPIE and CEFS do not consider incremental deployment, and their performance is poor under incremental deployment. Moreover, SampleTrace is specially designed for incremental deployment, and APMS also designs the operation mechanism under incremental deployment. Therefore, under all scenes for the random deployment, SampleTrace performs better than SPIE, and APMS better than CEFS.

4. Conclusions

This paper summarizes 5 evaluation indexes for IP traceback: computation overhead, storage overhead, false positive ratio, false negative ratio, and traceback time. And the evaluation model for IP traceback is

established based on the analytic hierarchy process (AEMT). In this paper, AEMT is applied to give an evaluation example: from the perspective of the network supervision department (the evaluator), an optimal traceback method is chosen under all scenes for the random deployment (model target). Based on the simulation experiments on the unified experimental platform, 4 traceback methods are comprehensively evaluated, and the relative advantages and disadvantages are comprehensively arranged, and the evaluation results conform to the design and application characteristics of traceback methods. AEMT can evaluate different traceback methods comprehensively, which greatly facilitates end-users, and This paper is of valuable reference for network researchers to make further studies for IP traceback.

5. References

[1] A. C. Snoeren, C. Alex, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, W. T. Strayer. Single-packet IP traceback. *IEEE/ACM Transactions on Networking*. 2008, 10 (6): 721–734.

[2] H. C. Tian, J. Bi. An Incrementally Deployable Flow-Based Scheme for IP Traceback. *IEEE COMMUNICATIONS LETTERS*. 2012, 16 (7): 1140-1143.

[3] M. M. Fadel, A. L. El-desoky, A. Y. Haikel, L. M. Labib. A low-storage precise IP traceback technique based on packet marking and logging. *Computer Journal*. 2016, 59 (11): 1581-1592.

[4] V. Murugesan, M. S. Selvaraj, M. H. Yang. HPSIPT: A high-precision single-packet IP traceback scheme. *Computer Networks*. 2018, 143 (8): 275-288.

[5] M. H. Yang, M. C. Yang. RIHT: A novel hybrid IP traceback scheme. *IEEE Transactions on Information Forensics and Security*. 2012, 7 (2): 789-797.

[6] S. Malliga, C. S. Kanimozhiselvi, S. V. Kogilavani. Low storage and traceback overhead IP traceback system. *Journal of Information Science and Engineering*. 2016, 32 (1): 27-45.

[7] S. Savage, D. Wetherall, A. Karlin, et al. Network support for IP traceback. *IEEE/ACM Transactions on Networking*. 2001, 20 (2): 226-237.

[8] H. C. Tian, J. Bi, X. K. Jiang, D. K. Wang, W. Zhang. Fast and secure probabilistic marking technology for IP traceback. *Journal of Tsinghua University*. 2011, 51 (4): 542-547.

[9] S. Yu, W. L. Zhou, S. Guo, M. Y. Guo. A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking. *IEEE Transactions on Computers*. 2016, 65 (5): 1418-1427.

[10] V. Aghaei-foroushani, A. N. Zincir-heywood. Autonomous system based flow marking scheme for IP-Traceback. *Proc. of 2016 IEEE/IFIP Network Operations and Management Symposium.* NJ: IEEE Press. 2016, pp. 121-128.

[11] S. Roy, A. S. Sairam. Distributed star coloring of network for IP traceback. *International Journal of Information Security*. 2018, 17 (3): 315-326.

[12] Y. Bhavani, V. Janaki, R. Sridevi. IP traceback through modified probabilistic packet marking algorithm using chinese remainder theorem. *Ain Shams Engineering Journal*. 2015, 6 (2): 715-722.

[13] N. Lu, J. W. Zhang, J. F. Ma, X. Cong, W. B. Shi, S. G. Wang. A Scalable IP Traceback Approach Employing Dynamic Deterministic Packet Marking in the Large-Scale Networks. *Chinese Journal of Computers*. 2020, 43 (8): 1493-1516.

[14] L. Cheng, D. M. Divakaran, W. Y. Lim, V. L. Thing. Opportunistic piggyback marking for IP Traceback. *IEEE Transactions on Information Forensics and Security*. 2016, 11 (2): 273-288.

[15] Y. N. Abdullah, E. T. Mehmet. Record route IP traceback: Combating DoS attacks and the variants. *Computers and Security*. 2018, 72 (8): 13-25.

[16] Boston University. BRITE Topology Generator version 2.1b. http://www.cs.bu.edu/fac/matta/Research/BRITE.

[17] B. H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Communications of Acm*. 1970, 13 (7):422–426.

[18] H. C. Zhao, S. B. Xu, et al. *Analytic Hierarchy Process- a Simple New Decision-making Method*. Beijing: Science Press, 1986.