Jestr

Journal of Engineering Science and Technology Review 15 (6) (2022) 28 - 34

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Research Article

A Hybrid Traceback based Network Forensic Technique to Identifying Origin of Cybercrime

Rachana Patil[1,*] , Yogesh H. Patil[2], Renu Kachhoria[1], Savita Kumbhare[1] and Sheetal U. Bhandari[2]

[1]Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India
[2] Institute of Technology, Pimpri, Pune, Maharashtra, India

Received 20 June 2022; Accepted 31 October 2022

Abstract

Protecting the critical infrastructure is crucial task when the cybercrime and cyber-threats are on the rise. The internet is vulnerable to packet tampering, as it does not have any safeguards in place. While initiating an attack, attackers use vulnerabilities to alter the source IP address. As a result, cybercrime investigations are becoming increasingly challenging. The network is the backbone of cybercrime, and it is important to develop a network forensic investigation system to determine the true origin of cybercrime. The purpose of this study is to propose a hybrid source identification system for network forensic investigations, which could identify the source of the attack with a single packet with minimal computational capacity and high storage. The CAIDA topology database estimates that each route requires just 320KB of storage. Finally, we simulate and compare our system to other similar systems in terms of storage requirements, processing, and logging time.

Keywords: Network forensic, traceback, evidence, cyber crime, packet logging, packet marking

1. Introduction

As the number of cybercrimes are on rise, so does the need for forensic investigation arises frequently, and the most crucial phase in any investigation is gathering evidence and determining where the attack originated [1]. Even though spoofing the originating IP address is easy, this information cannot be used as evidence against an attacker because it may be easily spoofed. The category of techniques known as "trace back based network forensics" can be used to pinpoint the point of origin of an attack [2].

The traceback mechanisms can be utilized to locate the real origin of attack as well as the attack path. The method of identifying the real origin of the attack is difficult because the source IP address field in the IPV4 packet header is generally spoofed by the attackers.

The detection of the origin of packets in a network is called traceback. It is used to ascertain the source from where packets are originated by identifying the origin of an attack [3]. Traceback is an appropriate forensic network method used to identify the source of the packets by examining the attack method primarily for IP spoofing-based attacks[4].

The two main phases of any traceback techniques are, embedding evidences on packet and Reconstruct the attack graph/path.

To find the actual source of the attack packet even in the situation of IP spoofing, the exact information about the origin of the packet and the path followed by it should be embedded in the packets. As shown in figure 1, the evidence generation and embedding mechanism needs to be deployed on the intermediate routers. The intermediate routers are responsible for selecting the packets and embedding evidences in it.

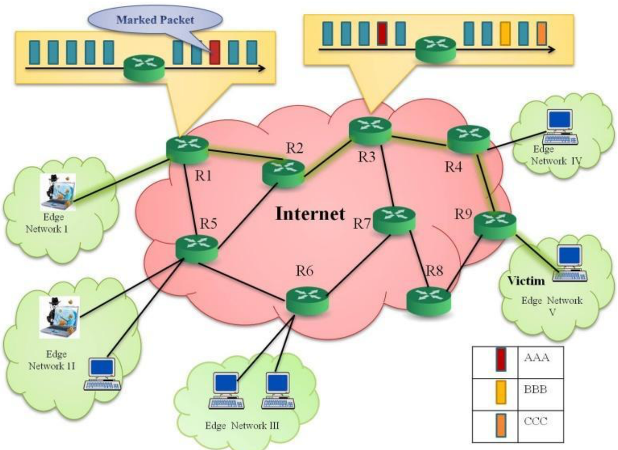

Fig. 1. Evidence generation and embedding mechanism.

The second stage of any traceback method is to rebuild the graph / attack path. As shown in figure 2, the victim is responsible for collecting and verifying evidence. With the help of this evidence gathered and analyzed, victims can reconstruct the attack path followed by packets. The root node of this attack graph is the actual source of the attack

2. Review of traceback based Source Identification Approaches

In the years since 1999, several researchers have worked to discover the origin of the attack, with the goal of tracking the package behind its source. The strategy of finding network objects that can be applicable as evidence in the process of court of law in the opposition of attackers is known by multiple different names. The authors in [5] provided a real-time approach to cyber attacks. IP trace back

[*] E-mail address: rachana.patil@pccoepune.org

ISSN: 1791-2377 © 2022 School of Science, IHU. All rights reserved.
doi:10.25103/jestr.156.04

is a term used by the authors of [6]. Although [7] on the other hand, it uses the term to produce evidence and a validation strategy. The most commonly used tracking term used in this project.

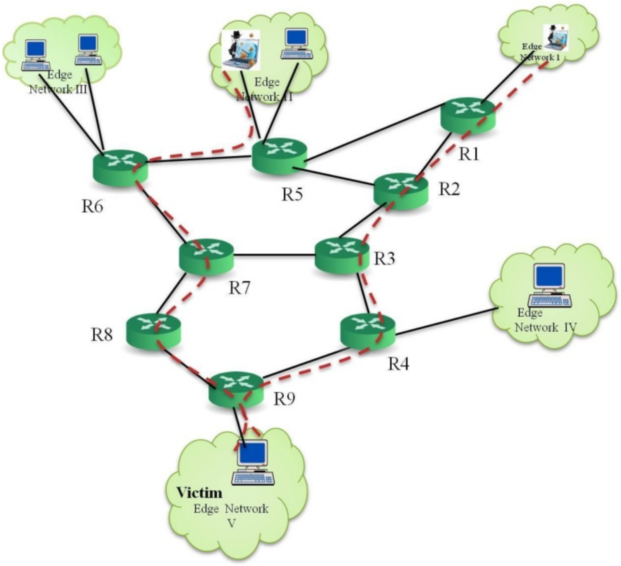

Fig. 2. Find the actual source of the attack packet.

2.1 Link Testing

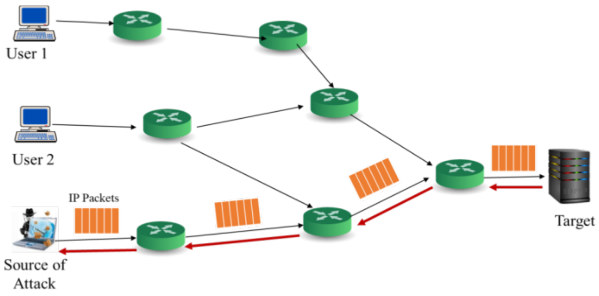

Fig. 3. Link Testing based Traceback Method.

Link-based analysis methods link all the growing links between victims and perpetrators to control the origin of the attack. Most of the time starts at the victim's nearest route and ends until the attacker's route is identified as shown in figure 3. The authors of [8-10] have proposed follow-up schemes based on link speculation. The main disadvantage of this method is that the analysis of the transmission attack is not possible and can only be done during the attack. Link testing methods are not suitable for forensic investigations. There are two types of link testing methods.

2.2 Input Debugging

Once the target realizes it's being attacked, input debugging is a viable option. For an attack to be successful, it must be able to collect the incoming traffic and analyse it for specified features. Upstream routers are informed of this signature by the victim. To find an attacker, this attack signature is repeatedly passed on to the rising warriors for re-examination. However, an important feature of the debugging installation method requires high ISP involvement and visual management.

2.3 Control Flooding

The first IP traceback was proposed by Burch [11] in 1999 for flood control. In the process, the victim repeatedly floods the pockets of his legs up and down the river and at the same time decides to differentiate between the magnitude of the attack. This algorithmic process will determine the flow flow of each level rising up the river. However, early understanding of network topology is an important aspect of flood control. These methods also generate network traffic by filling additional packets.

2.4 Marking

Marking is basically an idea of tagging a package or how to detect embedding route information in the package itself. The mid router will see the packets or set the route information into a pocket and at the side of the victim extract the dotted information to recreate the attack method and observe and note the real source of an attack. Pots with dots can be set in all attack lines or edge routers based on the package acquisition method. The tag-based method uses three methods depending on the strategy and the type of data recorded in the package. However, the key features of the marking systems track the number of packages required for reconstruction. Package marking required modification of existing network protocols and overloading in IP-based fields may cause problems.

The commonly used methods for packet marking in research are Probabilistic Packet Marking (PPM) or deterministic packet marking (DPM) & Flow-based marking[12].

2.5 Logging

The purpose of the package cutting method is defined to collect the hash value in the middle rows. Rugs keep track of the IP subject fields of the packets they pass through as shown in figure 4. The network route can be built using the information stored on these routers. Gun-based practice can track the attack method using a single package [14] proposed tracking-based tracking method, SPIE (source source method). Their strategy makes use of a space-efficient data framework which is named as a bloom filter to notably lessen the amount of storage capacity for packing alarms. However, the critical aspects of logging-based processes are a huge burden on integrated storage for routers. It requires high processing power and memory. As routers constantly update to track pre-installed information it needs to be done on time. Therefore, it is a challenging task to implement such techniques.

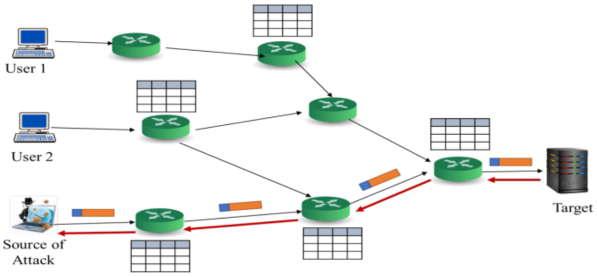

Fig. 4. Logging based Traceback Method.

2.6 Messaging

The first message-based approach is proposed by the authors [15]. This method supports additional convenience through sending traceback-oriented information to the victim of the attack. In this process each mid router creates a tracking message, often an ICMP message that informs the tracking information.

The authors of [15] proposed a message-based IP tracking system using ICMP messages. In the given process, each router could generate an ICMP packet named as a tracking package or can be a iTrace signal, which is considered for handling data that will be used as input into the tracking process. R2 produces an additional message as shown in figure 5 which contains parameters similar to the previous hop or the next hop. It may contain information such as a timestamp or MAC address, etc. Thousands of these iTrace packages make it easy to track effective tracking during an attack. However, the chances of producing messages are below the tolerable limits to prevent the congestion of the network traffic generated by these messages.

2.7 Overlay

Stone [16] initially suggested a tracking concept based on the output network as shown in figure 6. In this sense a unique network of independent applications and a normal network are built. The overlay div is responsible for capturing the entire page. Then the routers monitor the traffic going through them and gather the required tracking information collected on the overlay network. Traceback strategy based on overlay network provides accurate tracking results. However, the critical aspects of these methods require high start-up costs and increasing shipping is a daunting task.

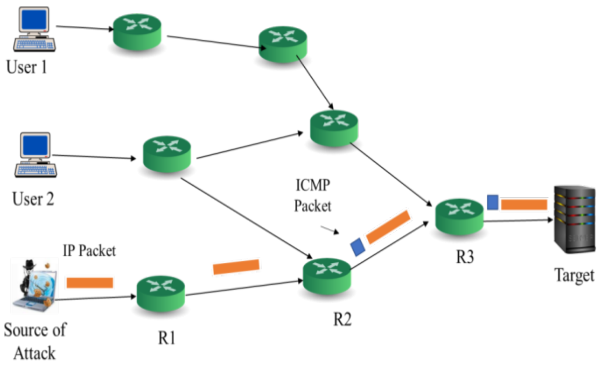

Fig. 5. Messaging based Traceback Method

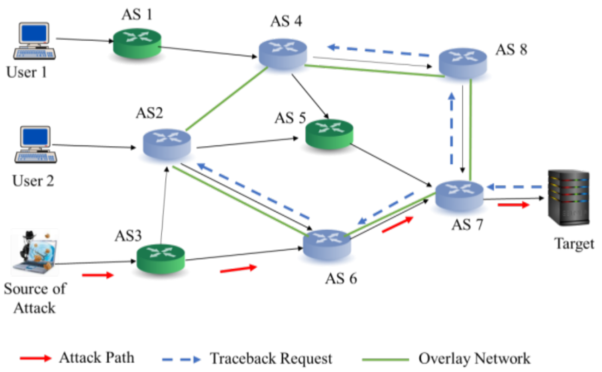

Fig. 6. Overlay Network based Traceback Method

2.8 Hybrid

The hybrid IP traceback approach integrates many different tracking schemes to work seamlessly. A combination of schemes can provide better results. The authors [18] of the package marker combined with packing cut and also called the hybrid traceback system.

3. Analysis of Existing Source Identification Techniques

The various source identification schemes can be evaluated using the criteria presented in this section. Several parameters required for analysing and comparing various traceback based source identification approaches have been proposed by the authors of [23]. In addition to these, we've taken into account a few other factors that forensic investigators should keep in mind.

- **Evidence Context (EC) -** The type of event used in the post-tracking source identification process is known as "evidence context." These scenarios cover the entire package, including the package title, and the network nodes. The package head contains the data needed to move it from A to point B. On cut-off and mixed-use routes, network nodes represent intermediate routers that capture the source identification information that can be used to reconstruct attack methods.
- **Processing Location (PL) -** Whether the network forensic investigation is conducted in a centralised or decentralised manner is represented by this attribute. The centralised processing is used by the vast majority of existing traceback approaches. Forensic traceback and path reconstruction are two separate processes that can only be carried out using distributed processing.
- **Execution Approach (EA)** – The forensic investigation approach to locating the underlying cause is represented by this attribute. Proactive and reactive are two broad categories of execution approaches. When an attack is detected, proactive measures are immediately put into action. Live forensic investigation can benefit from proactive approaches. Dead forensics is a post-incident investigation method that employs a reactive approach.
- **Packets Required (PR) -** In order to investigate each traceback-based identity scheme, a different number of packets was required. Ideally, one package should be required for investigation.
- **ISP involvement. (II) - In** most traceback-based resource identification systems, additional hardware or software had to be installed on intermediate routers before connecting and tracking. Because ISPs are competitive and often reluctant to work together, the right approach may require very little involvement from them.
- **Security of Evidences (SE) -** A traceback-based source identification method should have the appropriate method for verifying appropriate signals. In order to avoid further ambiguity, evidence security information (SE) needs to be maintained.

From the table 1 it is noted that notation-based techniques and effective methods are used to identify the source of an attack only after it has occurred. In many cases, packet title fields are used to store proof information in these strategies. It is necessary to store a large amount of data on the victim in order to analyze and obtain accurate source information when using package marking methods. The flexibility and ease of use are the main points of these strategies. The ISP, on the other hand, has to be more involved in many ways.

Combining the appropriate techniques can reduce the memory and storage requirements. Reactive in nature, hybrid approaches rely on a single packet to locate the point of attack. The safety of evidence in transit has been a concern for many authors of hybrid approaches.

Table 1. Comparison of Existing Source Identification Techniques

Reference	PA				EC			PL		EA		PR		II		SE	
	Marking	Messaging	Overlay Network	Logging	Packet Header	Complete Packet	Network Node	Centralized	Distributed	Proactive	Reactive	Single	Multiple	High	Low	Yes	No
[19]			√			√		√			√	√			√		√
[20]	√			√	√		√			√		√		√			√
[21]			√			√			√	√			√		√	√	
[22]	√							√			√		√		√		√
[23]	√			√			√		√		√		√	√		√	
[24]	√			√	√		√		√			√			√		√
[25]		√							√	√		√			√		√
[26]	√				√			√			√		√		√		√
[27]	√			√	√		√		√		√	√			√		√
[28]	√				√			√			√		√	√		√	
[29]	√			√	√		√		√		√	√			√		√
[30]	√				√				√		√		√	√			√
[31]	√			√	√		√				√	√			√	√	
[32]			√		√			√			√		√	√			√
[33]	√				√			√		√		√			√		√
[34]	√					√		√			√		√		√		√
[35]	√				√			√			√		√		√		√
[36]	√					√			√		√	√			√		√
[37]		√							√	√		√		√			√

4. Proposed Hybrid Source Identification Scheme

The most critical stage in investigating the source of an attack is to include evidence of the attack packets, which provides information about the attack's origin [38]. The most important role is to gather such evidence and deliver it to the victim of the attack.

According to revisions made [39] of the package tagging fields and IP traceback information, when using a tracking method based on packet tagging, the evidence is embedded in the IP subject. When packets are sent, not all IP subject fields are used at once. These fields that are not used in the IP domain are used by most of the available tracking strategies.

During the transmission of the packet from one network to another, if the Maximum transfer unit (MTU) of a particular network is less than the size of the packet, the packet is fragmented. The identification field holds the ID of the fragment and the fragment offset field holds the information about the position of the fragment in the packet. It is used to arrange the fragments in sequence at the destination. Many authors have considered these fields for packet marking [40]. According to Savage et al. [12]. less than 0.25% of the separate packets on the actual network, so the overcrowded identification field and the fragment offset field will not have a significant impact on the IP network.

The Reserved Flag bit of IP header corresponds to an unused bit. The overlapping of this bit does not create any problem for IP protocol services. Many authors have considered these fields for packet marking [39].

In the proposed scheme the identification, flags and fragment offset fields are used for embedding the evidence information.

In the proposed system, the interface numbers of the routers are used as evidence and are embedded in the identification areas, flags and fragments of the IP header as shown in figure 7, to track the attack packet to identify the origin of the attack. Our evidence embedding process may need to include the evidence field in the hash table and save the table index in the pocket because each packet has a limited number of proof tag fields. Until the package reaches its final destination, we continue to mark the evidence and seal the packets. Then we can reverse the process of identifying the origin of the attack packets.

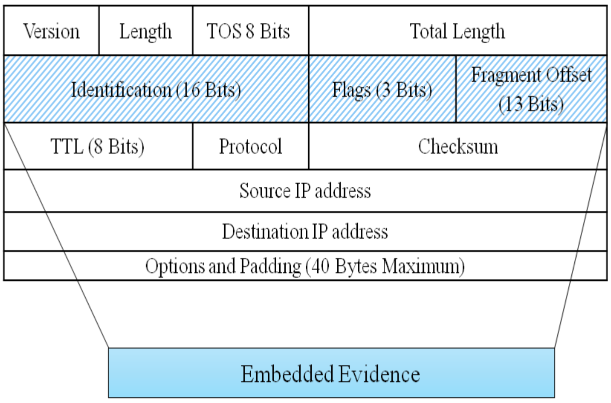

Fig. 7. Fields used in IP header

4.1 Evidence Embedding Module

When the packet arrives on the edge of the route from the local network, and proof field is set to zero and the packet is transferred to the next main route. As shown in Figure 4 when the package arrives at the main route, it includes Enew = P.evidence * (I (Ri) +1) + UIi + 1. Suppose if Enew <255, then the primary router strongly proposes P.evidence with the new and then further pack on the next main route. If Enew > 255, the main router is required to enter P.evidence and UIi. The core router needs to integrate H (P.evidence) and use a quadratic test method to search the UIi and Evidence in the hash table of the router. Suppose if P.evidence and UIi are not available then, the main route is inserting the P.evidence and UIi pairs into the hash table. Then, find their index in the table and computes Enew = Index * (I (Ri) +1). Finally, Enew and superimposes P.evidence transfers the package to the next router in the network. The detailed process of embedding the evidence is described in the form of flowchart in figure 8.

4.2 Source Identification Module

As soon as victim is under attack, the source identification request has been sent to upstream router, which contains the attack packets evidence marking filed, here we termed it as Evidence$_{req}$, As Evidence$_{req}$ is received by router, it attempts to search the attack packets upstream router as shown in fig 6. Initially it counts Ui$_i$ = Evidence$_{req}$% (I (Ri +1) -1. To determine whether the requested router is the router at the end of the attacker, the router computes index = Evidence$_{req}$ / (I (Ri) +1). hash and color UI$_i$ = Hash Table (Index) .UI and E$_{old}$ = Hash Table (Index).evidence.

Next the requests Evidance$_{req}$ is replaced with E$_{old}$ and the request is forwarded to the upstream router. but, if index=0 then the requested router becomes the source router and the process starts the path rebuilding up to the source of attack is completed.

Suppose if, UI$_i$≠ -1, means that the arrived packet from upstream near the UI$_i$ of the top visual interface, the requested router then reconstructed the marking field into its first marking state. The router calculates E$_{old}$ = Evidence$_{req}$ / (I (Ri) +1), so that we can find Evidence$_{req}$ for the ascending package route, i.e., E$_{old}$ here. Then replace the Evidence$_{req}$with E$_{old}$ move the request to a vertical route. The detailed process of source identification is described in the form of flowchart in figure 9.

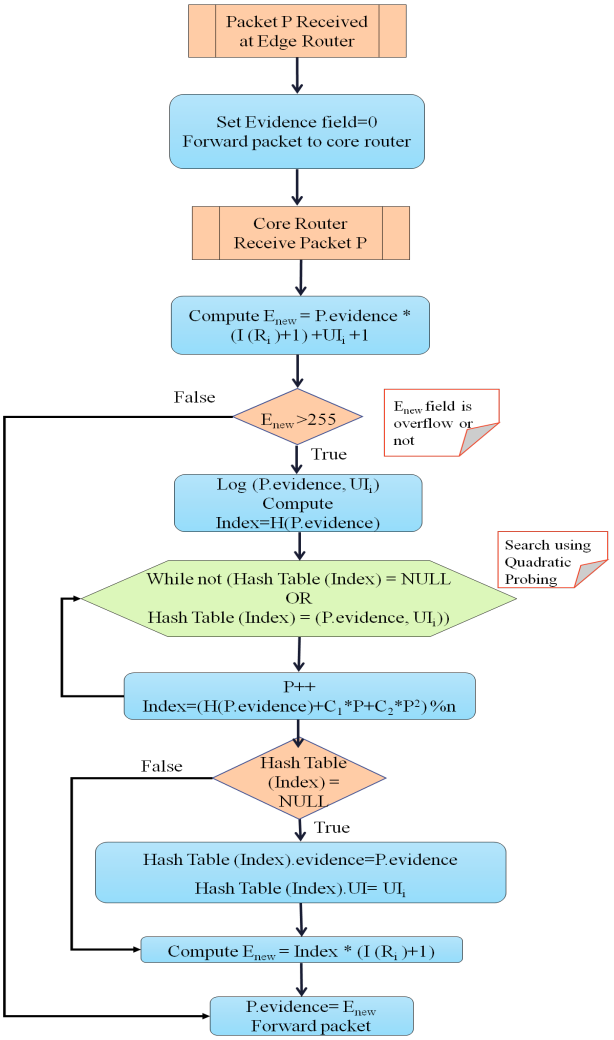
Packet P Received at Edge Router
Set Evidence field=0 Forward packet to core router
Core Router Receive Packet P
Compute E_{new} = P.evidence * (I (R_i)+1) +UI_i +1
False
E_{new} >255
E_{new} field is overflow or not
True
Log (P.evidence, UI_i) Compute Index=H(P.evidence)
Search using Quadratic Probing
While not (Hash Table (Index) = NULL OR Hash Table (Index) = (P.evidence, UI_i))
P++ Index=(H(P.evidence)+C_1*P+C_2*P^2) %n
False
Hash Table (Index) = NULL
True
Hash Table (Index).evidence=P.evidence
Hash Table (Index).UI= UI_i
Compute E_{new} = Index * (I (R_i)+1)
P.evidence= E_{new} Forward packet

Fig. 8. Evidence Embedding.

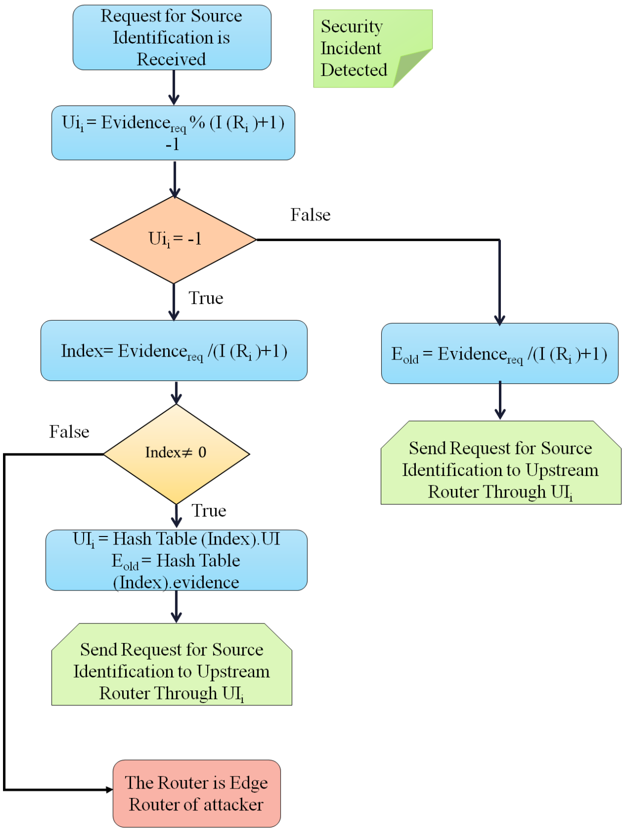
Request for Source Identification is Received
Security Incident Detected
Ui_i = $Evidence_{req}$ % (I (R_i)+1) -1
Ui_i = -1
False
True
Index= $Evidence_{req}$ /(I (R_i)+1)
E_{old} = $Evidence_{req}$ /(I (R_i)+1)
False
Index≠ 0
True
Send Request for Source Identification to Upstream Router Through UI_i
UI_i = Hash Table (Index).UI E_{old} = Hash Table (Index).evidence
Send Request for Source Identification to Upstream Router Through UI_i
The Router is Edge Router of attacker

Fig. 9. Source Identification.

5. Performance Analysis

Here, we will explore the basics of our simulation setup and show you how to get to our entry table size and limit values. In this section, we will focus on the role model. CAIDA's [29] project skitter topology is used as an online topology model in this study.

Paths to a particular host in topology are included in the database. Only 197,003 of the 197,003 paths in the CAIDA skitter data were used in our network topology. Figure 3 shows the analysis results. There are 130,267 rugs in total, with an average hop count of 14.42 and an upstream of 2.63 rivers per path. Figure 10 shows the path length distribution

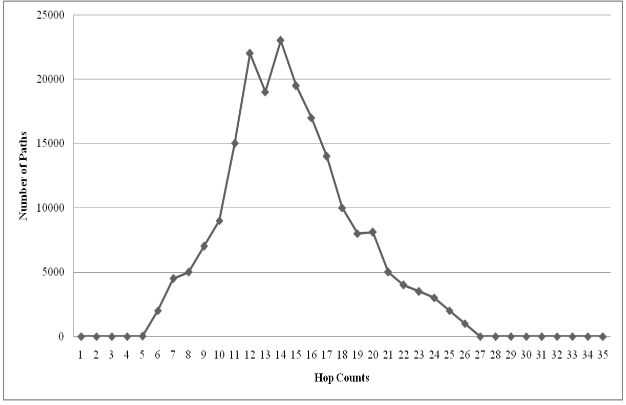

Fig. 10. Path length distribution.

.

5.1 Relation between the Router Degree and the Table Size

The size of the table size decreases rapidly as the number of rotor degrees increases, as shown in figure 11. When the rotor degrees fall below a certain limit, our method marks the number of the visible UIi connector at the head of the fixed size package. The index value should decrease as the maximum number of UIi increases in a degree-dependent manner. It also means that the maximum size of the table will be reduced. The proof field is able to accept the highest index value if the degree is more than 90 degrees. That is why the size of the log table increases significantly as the degree of the router exceeds 90. The maximum size of the entry table on the 66-degree route is 7. Only 4- to 7-inch log tables can be used with the router. The router supports log tables with a maximum size of 712 when the degree is 91. As a result, the size of the table decreases with increasing degrees.

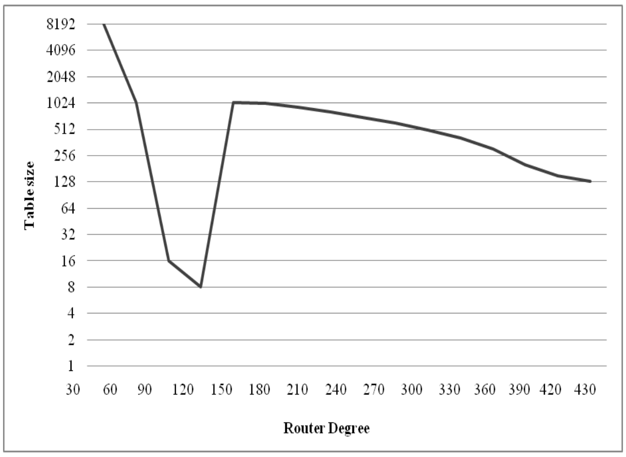

Fig. 11. Relation between the table size and the router degree.

5.2 Requirements for logging time

Cutting time and final requirements for our source identification method are comparable to those for the previous HAHIT resource identification strategy [43]. We send around 10 to 40 million packets to the network and record intermediate entry times for our route, as well as HAHIT Figure 12. HAHIT logging times increase as the number of packets increases, while our logging times remain unchanged regardless of the number of packets. Having a large index causes less space for the proof of the packet because the size of the proof field is adjusted. And this can lead to frequent logging. The limit value must be met before a virtual connector number can be entered into our system. As a result, we can reduce the frequency of logging.

In addition, our cutting frequency does not increase according to the number of packets, because our system is limited in terms of index value.

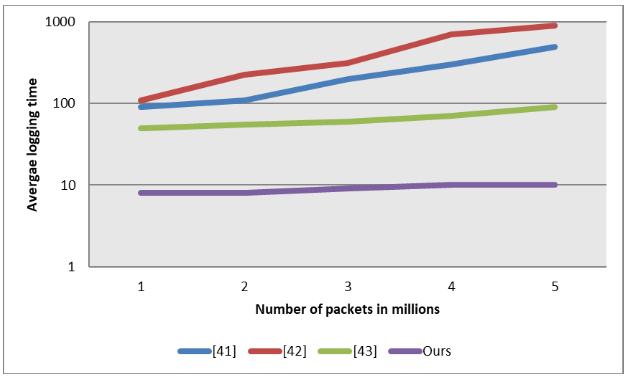

Fig. 12. Comparison of logging time.

The rate of false positives and false positives is high [41 - 43]. The required storages for each route are shown in Figure 13. We only need 16 bytes of logging space compared to [43] of 1500 and 320 bytes of logging space, respectively. When it comes to data storage, our method is 95 percent more efficient than that of [43]. Because we don’t employ fixed-size log tables, we have more records for routers with degrees below the threshold of 10. Consequently, we can avoid the pathways that have been logged twice.

As shown in figure 13 a comparison of the maximal storage requirements of our method with [41-43] for various packet counts. In these systems, the router with the most degrees has the most storage capacity because it logs the most frequently. Due to their continuous logging frequency, our storage requirements do not rise linearly with the number of packets they receive.

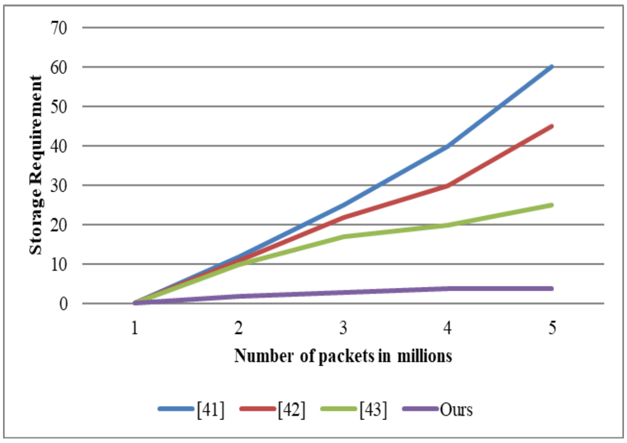

Fig. 13. A comparison of storage requirements of our method with [41-43].

6. Conclusion

Identifying true source of cybercrime is difficult when an attacker's identity can be masked in cyberspace, Many studies have been done, but the present IP traceback solutions still necessitate a large number of packets or place a great burden on router computation and storage. By introducing an innovative IP traceback based network forensic investigation scheme that identifies an attack's origin with only one attack packet and minimum compute and storage overhead, the goal of this work is to make security incident investigations easier. Compared to the existing traceback systems, the proposed method incurs substantially less computing overhead and significantly lowers the router's involvement in the traceback process. CAIDA Skitter data shows that it takes only 320kB of storage, which is much less than the current systems.

References

1. Sikos, L.F.,. “Packet analysis for network forensics: A comprehensive survey.: *Forensic Science International: Digital Investigation*, 32 (1), 2020, pp.1-12.
2. Yogesh, P.R.,. “Backtracking tool root-tracker to identify true source of cyber crime.”, *Procedia Computer Science*, 171 (1), 2020 pp.1120-1128.
3. H. Kim, E. Kim, S. Kang and H.K. Kim., “Network Forensic Evidence Generation and Verification Scheme (NFEGVS).” *Telecommunication Systems.* Springer, 60(1), 2015, pp.261-273.
4. Patil, R.Y. and Devane, S.R., “Network forensic investigation protocol to identify true origin of cyber crime.”, *Journal of King Saud University-Computer and Information Sciences.* 34 (5), 2019, pp. 2031-2044.
5. Moustafa, N. and Slay, J., “A network forensic scheme using correntropy-variation for attack detection.”, In *IFIP International Conference on Digital Forensics,* 2018, pp. 225-239.
6. M Vijayalakshmi, N Nithya and S.M. Shalinie, “A novel algorithm on IP traceback to find the real source of spoofed IP packets.”, *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*. 325 (1), 2015, pp. 79-87.
7. V. Aghaei-Foroushani and A.N. Zincir-Heywood. “Investigating unique flow marking for tracing back DDoS attacks”. *In Proceedings of International Symposium on Integrated Network Management (IM).* IEEE, 2015, pp. 762-765.
8. M. Hamedi-Hamzehkolaie, M. J. Shamani and M. B. Ghaznavi-Ghoushchi, “Low rate DOS traceback based on sum of flows,” In *6th International Symposium on Telecommunications*, 2012, pp. 1142-1146.
9. R. Yogesh Patil and L. Ragha, "A rate limiting mechanism for defending against flooding based distributed denial of service attack," In: *2011 World Congress on Information and Communication Technologies*, 2011, pp. 182-186.
10. Patil, R.Y. and Ragha, L.,. “A dynamic rate limiting mechanism for flooding based distributed denial of service attack”. In: *Fourth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom2012),* , Bangalore India, 2012, pp.1-12.

11. H. Burch and B. Cheswick, "Tracing Anonymous Packets to Their Approximate Source", In: *14th USENIX conference on System administration,* , USA, 2000,pp. 319-327.
12. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback" In: *Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, 30(4), 2020, pp. 295-306.
13. A. Belenky and N. Ansari, "On IP traceback," *IEEE Communications magazine,* 41(7), 2020, pp.142-153.
14. A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S.T. Kent and W. T. Strayer, "Single-packet IP traceback," *IEEE/ACM Transactions on Networking* (ToN), 10(6), 2002, pp.721-734.
15. S. M. Bellovin, M. Leech and T. Taylor, "ICMP traceback messages,". Retrieved from https://tools.ietf.org/html/draft-ietf-itrace-04.2003, 2022-6-10.
16. R. Stone, "CenterTrack: An IP overlay network for tracking DoS floods," In*: Proc. Of USENIX Security Symposium*,. 21, 2000, pp. 114-120.
17. V. L. Thing, M.Sloman, and N. Dulay, "Non-intrusive IP traceback for DDoS attacks," In: Proc. of the *2nd ACM symposium on Information, computer and communications security*, 2007, pp. 371-373.
18. B.Al-Duwairi and G. Manimaran, "A novel packet marking scheme for IP traceback," In: *Proc. Tenth International Conference on Parallel and Distributed Systems*, 2004, pp. 195-202.
19. M Fadel, M.,. "HDSL: A Hybrid Distributed Single-packet Low-storage IP Traceback Framework. (Dept. E)", *Mansoura Engineering Journal*, 46(4), 2021, pp.75-89.
20. Mohamed, H., Ouldmohamed, Y. and Nacera, B.. "A Single-Packet IP Traceback: Combating DOS-DDOS Attacks. *EDPACS*, 66(1) 2021, pp.1-12.
21. Arjmandpanah-Kalat, M., Abbasinezhad-Mood, D., Mahrooghi, H.R. and Aliabadi, S., "Design and performance analysis of an efficient single flow IP traceback technique in the AS level", *International Journal of Communication Systems*, 33(9), 2020, pp. 1-17.
22. Fazio, P., Tropea, M., Voznak, M. and De Rango, F., "On packet marking and Markov modeling for IP Traceback: A deep probabilistic and stochastic analysis.", *Computer Networks*, 182(1), 2020, pp. 1-14.
23. Li, C., Hu, F. and Xu, D., "RPDT: An architecture for IP traceback in partial deployment scenario.", In: *IEEE 5th International Conference on Computer and Communications* (ICCC), IEEE, 2019, pp. 1602-1608.
24. Mythili, T., Kiran, M.K., Noorjahan, S. and Malliga, D.,. "An enhanced packet marking and traceback algorithm for ip traceback.", *Iconic Research and Engineering Journals,* 2(10), 2019, pp.300-305.
25. Malliga, S., Kogilavani, S.V. and Nandhini, P.S., "A low traceback and zero logging overhead IP traceback approach for communication networks.", In*: 2018 International Conference on Intelligent Computing and Communication for Smart World* (I2C2SW), IEEE, 2018, pp. 100-105.
26. Nur, A.Y. and Tozal, M.E., "Record route IP traceback: Combating DoS attacks and the variants.", *Computers & Security*, 72(1), 2018 pp.13-25.
27. Murugesan, V., Selvaraj, M.S. and Yang, M.H., "HPSIPT: A high-precision single-packet IP traceback scheme.", *Computer Network*s, 143(1), 2018, pp.275-288.
28. Patel, H. and Jinwala, D.C., "LPM: A lightweight authenticated packet marking approach for IP traceback.", *Computer Networks*, 140(1), 2018, pp.41-50.
29. Malik, M. and Dutta, M., "Implementation of single-packet hybrid IP traceback for IPv4 and IPv6 networks.", *IET Information Security*, 12(1), 2018, pp.1-6.
30. L. Cheng, D.M. Divakaran, A.W.K. Ang, W.Y. Lim and V.L. Thing., "FACT: A Framework for Authentication in Cloud-Based IP Traceback.", *Transactions on Information Forensics and Security*. IEEE, 12(3), 2017, pp.604-616.
31. M.M. Fadel, A.I. El-Desoky, A.Y. Haikel and L.M. Labib., "A Low-Storage Precise IP Traceback Technique Based on Packet Marking and Logging", *Computer Journal*, 53(11), 2016, pp.1581-1592.
32. V. Aghaei-Foroushani, A.N Zincir-Heywood, "Autonomous system-based flow marking scheme for IP-Traceback.", In: *Network Operations and Management Symposium (NOMS).* IEEE, 2016, pp. 121-128.
33. S. Yu, W. Zhou, S. Guo and M. Guo., "A feasible IP traceback framework through dynamic deterministic packet marking.", *Transactions on Computers. IEEE*, 65(5), 2016, pp. 1418-1427.
34. X. Liu, M.Dong, K. Ota L.T. Yang and A. Liu., "Trace malicious source to guarantee cyber security for mass monitor critical infrastructure", *Journal of Computer and System Sciences,* 98(1) 2016, pp.1-26.
35. P. Fazio, M. Tropea, S. Marano and M. Voznak., "Meaningful attack graph reconstruction through stochastic marking analysis.", In: *International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS). IEEE*, 2016, pp. 1-6.
36. X.Wang., "On the feasibility of real-time cyberattack attribution on the Internet.", In: *Proceedings of Military Communications Conference, MILCOM* 2016, IEEE, 2016, pp.289-294.
37. G. Yao, J. Bi and A.V. Vasilakos., "Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter.", In: *Transactions on Information Forensics and Security*. IEEE, 2015, pp. 471-484.
38. Patil, R.Y. and Devane, S.R., "Hash tree-based device fingerprinting technique for network forensic investigation.", In *Advances in Electrical and Computer Technologies,* Singapore 2020, pp. 201-209.
39. Patil, R.Y. and Devane, S.R., "Unmasking of source identity, a step beyond in cyber forensic.", In: *Proceedings of the 10th international conference on security of information and networks* 2017, pp. 157-164.
40. X.Wang, "On the feasibility of real-time cyber-attack attribution on the Internet," In: *Proc. of IEEE Military Communications Conferenc*e, 2016, pp. 289-294.
41. Malliga, S. and Tamilarasi, A., "A hybrid scheme using packet marking and logging for IP traceback.", *International Journal of Internet Protocol Technology*, 5(1-2), 2010, pp.81-91.
42. Malliga, S. and Tamilarasi, A., "A proposal for new marking scheme with its performance evaluation for IP traceback.", *WSEAS Transactions on Computer Research*, 3(4), 2008, pp.259-272.
43. Yang, M.H., "Storage-efficient 16-bit hybrid IP traceback with single packet.", *The Scientific World Journal*, 2014 (1), 2014, pp. 1-11.