Tracing DoS and DDoS Attack Origins: IP Traceback Methods Comparison and Evaluation for IoT Environments

Description:
A concise study comparing IP traceback methods to identify the origins of DoS and DDoS attacks, focusing on their efficacy and applicability within IoT ecosystems.

Author: Sunny Thakur

Abstract

As society transitions to new technological paradigms, such as the Internet of Things (IoT), vulnerabilities like hacking, DoS (Denial of Service), and DDoS (Distributed Denial of Service) attacks become increasingly prevalent. These attacks impose significant economic costs on businesses, public organizations, and compromise user privacy. IoT introduces new, accessible points of vulnerability as personal and private devices that previously lacked connectivity are now exposed. Identifying the origin of these attacks is a critical step in gathering evidence for potential prosecution. This theoretical study evaluates and compares IP traceback methods and consolidates them into a set of metrics that can be leveraged against attackers.

Keywords: Attack Origins, DoS, DDoS, TTL, Traceback, IoT Security

1. Introduction

Denial of Service (DoS) attacks are designed to prevent legitimate users from accessing specific network services, such as websites or computer systems. Distributed Denial of Service (DDoS) attacks, on the other hand, amplify this effect by coordinating multiple compromised systems to target a specific service or network, creating a more disruptive impact. These "secondary victims" play a role in completing the attack, making it challenging for digital forensic investigators (DFI) to track the original source.

Flooding attacks can generally be categorized as direct or reflector attacks. In a direct attack, the attacker sends numerous malicious packets directly to the target. These can include Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), or mixed protocol packets. Examples of direct attacks include IP and SYN flooding. Conversely, a reflector attack uses intermediary devices, or "reflectors," to indirectly target the victim. The attacker manipulates source addresses to trick reflectors into responding to the victim, thus overwhelming the target without the reflectors' knowledge.

A critical aspect of DDoS attacks is IP spoofing, which allows attackers to disguise their origin by altering the source IP address. Combined with the stateless nature of IP routing, where routers only know the immediate next hop in a packet’s path, tracing the origin of an attack becomes complex. The Internet’s original design prioritized fast data sharing in a trusted environment, rendering security a secondary consideration. Consequently, the unverified source addresses and trust-based routing are now exploited, particularly in IoT contexts where vulnerabilities are abundant.

DDoS defense mechanisms are typically categorized into three approaches based on their deployment locality:

1. **Source-end approach**: Detection is implemented in the attacker's network routers.
2. **Victim-end approach**: Detection is implemented in the routers within the victim's network.
3. **In-network approach**: Detection is implemented in intermediary routers.

Although victim-end detection is straightforward, it is only beneficial if it operates in real-time, providing immediate detection to combat attacks. Conversely, source-end detection is more challenging, given that attacks can originate from any global point. Consequently, a practical solution involves a real-time victim-end detection approach, balancing high accuracy with low computational complexity to maintain system performance.

2. Importance of IP Traceback

Tracing back to an attack origin is crucial for identifying and prosecuting malicious actors. IP traceback aims to pinpoint the origin of malicious packets, typically by leveraging routers, as they are integral to the Internet's data flow. Most IP traceback techniques require collecting substantial packet data from routers along the attack path. However, this process is resource-intensive and challenging without sufficient data, often necessitating full-stream packet data to accurately reconstruct the attack's trajectory.

3. Objectives and Structure

This paper aims to:

1. Compare and evaluate existing IP traceback methods.
2. Identify challenges in IP traceback.
3. Propose research directions for future work.

The paper is structured as follows:

- **Section 2** provides a literature review of traditional IP traceback methods for context.
- **Section 3** analyzes recent IP traceback techniques and their limitations.
- **Section 4** proposes evaluation metrics for assessing IP traceback methods.
- **Section 5** concludes with recommendations for future research directions.

2. Traditional IP Traceback Methods

IP traceback methods are essential for identifying the origin of a packet in cyber-attack scenarios. Each traceback approach explores the technical possibilities of network tracking but faces challenges due to the complex architecture and network dynamics. The diversity of network communication types, such as multicast routing and many-to-many communication, makes it challenging to develop a universal solution for all traceback needs. These methods are often limited by unknown host relationships—whether unicast (one-to-one), multicast (one-to-many), or broadcast (one-to-all)—and the specific interactions between network entities, like a web server and client, which restrict the effectiveness of any single approach.

Most traditional IP traceback methods struggle with issues like IP address spoofing, which complicates tracing attack origins. These methods typically require a substantial volume of packets to reconstruct malicious paths and are resource-intensive in terms of computational

power, storage, deployment, network throughput, and response time. Thus, the drawbacks of traditional methods often outweigh their benefits, and their performance may not meet the demands of efficient traceback.

Traditional IP traceback methods generally fall into five main categories: link testing (hop-by-hop tracing), ICMP messaging, logging, packet marking, and hop count filtering. Each approach is tailored to different conditions and offers unique features for tracing attack origins. However, most methods rely on collecting a considerable number of packets from routers along the attack route. In fact, a full packet stream from routers is often necessary to reconstruct the attack path, making these approaches resource-intensive.

Analysis of Traditional IP Traceback Methods

The following table highlights key advantages and disadvantages of widely used IP traceback schemes.

Traceback Scheme	Advantages	Disadvantages
Input Debugging	- Single packet analysis possible - Allows post-packet analysis - Effective for both DoS and DDoS - Low bandwidth and storage requirements	- High ISP cooperation required - Time-consuming and not scalable for simultaneous DoS/DDoS attacks - May require legal authorization
Controlled Flooding	- Does not need ISP cooperation - Easy to implement - Effective for DoS attack	- High time consumption - Requires substantial packets, causing network congestion - Potentially classified as a small DoS attack itself - Limited to use during attack and lacks distinction between DDoS and genuine network spikes
ICMP Messaging	- Compatible with existing protocols - Supports incremental deployment - Allows post-attack packet analysis - No need for ISP cooperation	- Adds extra network traffic - Lacks encryption for enhanced protection

Logging	- Compatible with current protocols - Moderate ISP cooperation required - Post-attack path reconstruction from single packets - Implementation is straightforward	- Demands substantial storage - Potential for hash collisions - Time delays due to data storage and retrieval - Increases computational demands on intermediary routers - May reduce network throughput
Packet Marking	- Minimal processing required - Suitable for multiple types of attacks - Lacks inherent security weaknesses	- Some packets leave routers unmarked - High memory requirements make implementation expensive

3. Recent IP Traceback Methods

While traditional IP traceback methods each offer specific benefits, they often prove challenging to implement due to high computational demands, large storage requirements, or added network traffic that can reduce overall performance. These methods struggle to deliver accurate and efficient traceback capabilities. Consequently, researchers have recently developed new traceback methods by merging various traditional techniques. This section will explore and evaluate these advanced IP traceback methods, examining how they attempt to achieve fast, single-packet traceback with improved accuracy and cost efficiency.

Table 2. Recent IP Traceback Methods Analysis

Traceback Scheme	Advantages	Disadvantages

TTL & DPM	- Suitable for a variety of attacks - Does not reveal internal ISP topologies - Scalable - Allows post-packet analysis - Does not require ISP cooperation - Can trace the attack even after it has ended	- High resource demands for processing and storage - Not effective for tracing DDoS attacks due to insufficient packet generation - Limited feasibility for wide deployment as routers must probabilistically mark packets - Some packets may not be marked due to probabilistic marking - Expensive memory overhead - Time-consuming due to additional encryption and decryption steps
Marking & Logging	- Compatible with existing protocols - Supports incremental implementation - Allows post-packet analysis - Compatible with existing routers and network infrastructure - Scalable - Provides single-packet traceback capability	- High resource demands for processing and storage - Sharing logging information among ISPs introduces logistical and legal challenges - Less suitable for DDoS - Some packets may not be logged due to probabilistic logging - Expensive memory overhead - Requires large packet size for reconstructing the attack path
Hop Count & Marking	- Suitable for a variety of attacks - Does not reveal internal ISP topologies - Scalable - Allows post-packet analysis - Does not require ISP cooperation - Effective against both DoS and DDoS - Feasible for wide deployment - Requires a small number of packets to reconstruct the attacking path	- High resource demands for processing and storage - Requires medium processing overhead - Some packets may not be marked due to probabilistic marking - Expensive memory overhead

FDDA	- Uses features out of hackers' control for IP traceback - Not affected by packet pollution - Functions as an independent software module compatible with current routing software, facilitating implementation	- Cannot differentiate between DDoS attacks and flash crowds, leading to possible false positives - Unable to determine the specific router location - Exhibits poor performance

4.Proposed Evaluation Metrics for IP Traceback Methods

1. **ISP Involvement**: An effective traceback scheme should require minimal involvement from Internet Service Providers (ISPs) and enterprise networks. Minimal ISP involvement helps to avoid delays and reduces the need for extensive resources, making the investigation process more efficient.
2. **Number of Attacking Packets Needed**: An ideal traceback scheme should be capable of tracing the source of an attack with a minimal number of packets, ideally with just one. This allows for faster and more efficient identification once an attack is detected.
3. **Processing Overhead**: A desirable traceback method should impose minimal processing demands on network devices, such as routers. This reduces the computational load and avoids potential performance degradation on the network.
4. **Storage Requirement**: An efficient traceback method should require only minimal storage on network devices. Low storage requirements make the method more feasible for implementation across various network setups.
5. **Ease of Implementation**: The design of an IP traceback method should be straightforward and compatible with network or application layer standards, enabling easier adoption and deployment.
6. **Scalability**: An ideal traceback method should be scalable, meaning it can be implemented without extensive additional configuration or dependency on specific device manufacturers or vendors.
7. **Bandwidth Overhead**: To avoid strain on network capacity, the traceback method should introduce minimal additional traffic. This ensures that bandwidth overhead does not exhaust network resources or necessitate upgrades or new equipment.
8. **Number of Functions Needed**: The complexity of implementation should be minimized. Ideally, the traceback method should require only a single function for network equipment vendors, simplifying the deployment process.
9. **Ability to Handle Major DoS or DDoS Attacks**: A robust traceback method should effectively trace the origins of DoS or DDoS attacks, even under challenging conditions like multiple attackers or spoofed addresses. An ideal method can manage various types of attack vectors, providing comprehensive traceability.

Table 3. Proposed Evaluation Metrics for IP Traceback Methods

Metric	Description	Ideal Characteristics

ISP Involvement	Involvement of ISPs in monitoring and traceback of attack packets.	Minimal ISP involvement to reduce investigation time and resource usage.
Number of Packets Required	The number of packets needed to identify the source of an attack.	The traceback method should ideally require only a single packet to trace the attack source.
Processing Overhead	Additional processing burden on network devices for tracking packet flow and calculating statistics.	Minimal processing overhead for efficient traceback.
Storage Requirement	Memory needed in network devices to store information for traceback.	Requires minimal memory for efficient deployment on network equipment.
Ease of Implementation	Complexity of implementing the traceback algorithm in the network.	Easy to implement at the network or application layer, allowing broad deployment.
Scalability	Additional configuration and adaptability required when implementing the method.	Scalable and independent of device manufacturers or vendors.
Bandwidth Overhead	Extra traffic generated due to traceback that can affect network performance.	Minimal bandwidth overhead, ensuring network efficiency without needing upgrades.
Function Count for Implementation	Number of different functions required by equipment vendors to implement traceback.	Ideally, only one function needed for easier implementation.
Ability to Handle DoS/DDoS Attacks	Effectiveness in tracing large-scale DoS/DDoS attacks, especially under severe scenarios like address spoofing.	Capable of handling all major types of DoS and DDoS attacks effectively.

Conclusion

This review identifies and consolidates metrics for enhancing IP traceback methods, revealing limitations within traditional methods, which often lack scalability and are hindered by excessive data requirements. While advancements in hybrid traceback techniques have reduced overhead and improved efficiency, an optimal solution remains elusive, particularly regarding challenges like poor ISP cooperation and substantial storage demands. The growth of IoT underscores the urgency for effective traceback in IPv6 environments, as IPv4 becomes less feasible. This paper

provides a foundation for future research to develop advanced, scalable traceback algorithms that can effectively address modern network security demands.

References

1. Specht, S., & Lee, R. (2004). Distributed denial of service: taxonomies of attacks, tools, and countermeasures. *International Conference on Parallel and Distributed Computing Systems*, 543–550.
2. Kumar, K., Singal, A., & Bhandari, A. (2011). Traceback techniques against DDoS attacks: a comprehensive review. *2nd International Conference on Computer and Communication Technology (ICCCT)*, 491–498. IEEE.
3. CERT Coordination Center. (2015). Cert Advisories: CA-2000-01 denial of service developments. CERT Software Engineering Institute. Retrieved from http://www.cert.org/historical/advisories/ca-2000-01.cfm
4. Chen, T., Tsai, J., & Gerla, M. (1997). QoS routing performance in multihop, multimedia, wireless networks. *IEEE 96th International Conference on Universal Personal Communications Record*, 2, 557–561.
5. Eddy, W. (2007). TCP SYN flooding attacks and common mitigations. *RFC4987*. IETF. Retrieved from https://tools.ietf.org/html/rfc4987
6. Lemon, J. (2002). Resisting SYN flood DoS attacks with a SYN cache. *2nd European BSD Conference*, 89–98. USENIX.
7. Paxson, V. (2001). An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communication Review*, 31(3), 38–47.
8. Gilad, Y., & Herzberg, A. (2012). LOT: a defense against IP spoofing and flooding attacks. *ACM Transactions on Information and System Security*, 15(2), 6.
9. Kashyap, H., & Bhattacharyya, D. (2012). A DDoS attack detection mechanism based on protocol-specific traffic features. *Second International Conference on Computational Science, Engineering and Information Technology (CCSEIT)*, 194–200. ACM.
10. Yao, G., Bi, J., & Vasilakos, A. (2015). Passive IP traceback: disclosing the locations of IP spoofers from path backscatter. *IEEE Transactions on Information Forensics and Security*, 10(3), 471–484.
11. Ho, C. (2010). Email forensics: tracing and mapping digital evidence from my address. Unpublished Master's Thesis.
12. Savage, S., Wetherall, D., Karlin, A., & Anderson, T. (2001). Network support for IP traceback. *IEEE/ACM Transactions on Networking*, 9(3), 226–237.
13. Burch, H., & Cheswick, B. (2002). Tracing anonymous packets to their approximate source. *14th USENIX Conference on System Administration (LISA)*, 319–328. USENIX.
14. Bellovin, S. (2002). ICMP Traceback Messages. *Internet Draft: draft-bellovin-itrace-00.txt*.
15. Lee, H.C.J., Thing, V.L.L., Xu, Y., & Ma, M. (2003). ICMP traceback with cumulative path, an efficient solution for IP traceback. *International Conference on Information and Communications Security (ICICS)*, 124–135. Springer.
16. Izaddoost, A., Othman, M., & Rasid, M. (2007). Accurate ICMP traceback model under DoS/DDoS attack. *15th International Conference on Advanced Computing and Communications (ADCOM)*, 441–446. IEEE.

17. Sager, G. (1998). Security fun with OCxmon and cflowd. Presentation at the Internet 2 Working Group.
18. Song, D., & Perrig, A. (2001). Advanced and authenticated marking schemes for IP traceback. *INFOCOM 2001*, 878–886. IEEE.
19. Snoeren, A., Partridge, C., Sanchez, L., Jones, S., Tchakountio, F., Schwartz, B., Kent, S., & Strayer, W. (2002). Single-packet IP traceback. *IEEE/ACM Transactions on Networking*, 10(6), 721–734.
20. Ponec, M., Giura, P., Brönnimann, H., & Wein, J. (2007). Highly efficient techniques for network forensics. *14th ACM Conference on Computer and Communication Security (CCS)*, 150–160. ACM.
21. Sung, M., Xu, J.J., Li, J., & Li, L.E. (2008). Large-scale IP traceback in high-speed internet: practical techniques and information-theoretic foundation. Retrieved from http://www.cc.gatech.edu/*mhsung/pub/ddos_sp.pdf
22. Devasundaram, S. (2006). Performance evaluation of a TTL-based dynamic marking scheme in IP traceback. University of Akron.
23. Wang, H., Jin, C., & Shin, K. (2007). Defense against spoofed IP traffic using hop-count filtering. *IEEE/ACM Transactions on Networking*, 15(1), 40–53.