WON (Wireless Overlay Network) for Traceback of Distributed Denial of Service

Yan Sun, Anup Kumar, S. Srinivasam*
Mobile Information Network and Distributed Systems (MINDS) Lab
Computer Engineering and Computer Science Department
**Computer Information System Department*
University of Louisville
{y0sun005, ak}@louisville.edu

Abstract

This article presents an incremental and scalable solution for tracing Denial of Service (DoS) and Distributed DoS (DDoS) attacks. Our approach allows the victim to identify the network paths traversed by attack traffic without requiring the support from ISP or knowledge of the network topology. In contrast to previous probabilistic packet marking work, our approach has no false positive and fixed computation overhead for the victim to reconstruct the attack paths. Furthermore, the volume of attack packets required to reconstruct the attack path is dramatically less.

1. Introduction

The current Internet infrastructure provides connectivity to millions of computers worldwide. The core Internet was designed to operate under the spirit of trustworthiness among computers. However, it was not designed to withstand different kinds of cyber attacks that are prevalent today. The ubiquitous connectivity provided by the Internet has made it a primary mechanism to perpetuate various attacks on the critical host computers. Examples of significant attacks include Code Red [1] launching Distributed Denial of Service (DDoS) and Slammer attacking Bank of America's ATM network in January 2003. The goal of cyber forensic includes monitoring, and identification of cyber criminals.

There are many techniques proposed in the literature to address prevention and detection of different types of attacks in wired and wireless networks [2, 3]. Relatively little attention has been focused on the identification and prosecution of attacks. Locating a source of attack will not only help identify criminals but also could prevent information stolen including identity theft, intellectual property theft etc. A typical attack [4] model is shown in Figure 1. In this case an intruder initiates an attack by contacting next level of hosts termed as stepping stone 1 to 4. Stepping-stone illustrates the compromised nodes that are used as an attack channel while hiding the attacker. Stepping-stones could change the inter-packet delay to avoid detection through causality relation mapping between in and out packets. The actual attack packets may travel through several stepping-stones to hide the identity of attacker(s) before reaching the victim. The identity of an attacker could be further disguised by the use of one or more zombie nodes. A stepping-stone could install a Trojan-horse on zombie nodes that could initiate DDOS attack some time in future. In this manner the attacker may not be easily identified through simple causality relationship mapping between packets. In this case zombie of stepping stone could spoof the identity of the victim and send packets to a forwarding node (shown in Figure 1), while the uncompromised forwarding node which is not the actual attacker, sends the packet forward to the victim. In this case the forwarding node is not the actual attacker. The attacker could initiate an attack by selecting stepping-stones in different geographical locations on the Internet making the identification of the attacker(s) even more difficult.

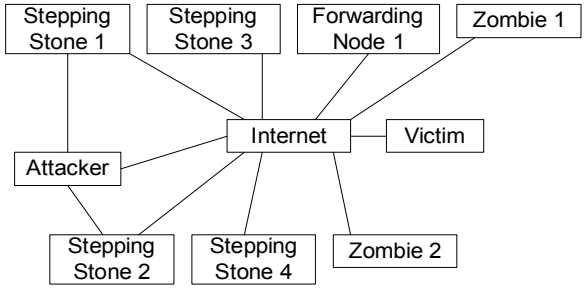

Figure 1. Generic attack configuration

Figure 2 depicts a simple network from attackers to victim, routers are presented by Ri, possible attackers are presented by Ai, and victim is presented by V. the dotted line represents a particular attack path between an attacker and the victim. The attack path from attacker Ai to victim V is a unique ordered list of routers between Ai and V. for instance, if attack originates from A1, then to reach V it must traverses the routers R1, R3, R5, R6 as shown by the dashed line. When victim V detects an intrusion, the trace back problem is to identify nodes R6, R5, R3, and R1 in order until it reaches the actual origin A1.

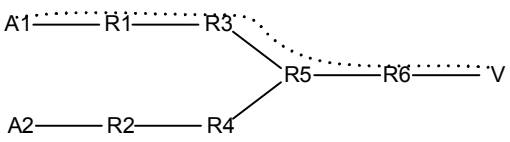

Figure 2. A network from attackers to victim

Analyzing the trace back of attack is a highly complex problem. Several approaches have been proposed to solve this problem of trace back in literature [5, 6, 7, 9, 10, 13, 16]:

- Packet filtering approach implemented via ingress and egress filtering by service providers can provide some degree of tracking of an attacker.
- Backscatter trace back tracks back a flood of packets targeting a DDOS victim.
- Probabilistic approaches for packet tracing such as iTrace include sending special packets on the network to identify the source of an attack.
- Hop by Hop tracing- A tracing program running near the victim identifies the attack packet by comparing the packet's source Internet packet (IP) address with the routing table information and sending a warning to its upstream router which upon encountering such a packet sends a notification to its upstream router and this goes on recursively until the source.
- Internet overlay network- An overlay network consisting of IP tunnels between edge routers and tracking routers is built and the tracking routers are vested with special diagnostic tools capable of performing the tracing.

A detailed survey of various trace back approaches can be found in [4,11,12]. A number of limitations exist in current approaches for identifying the origin of an attack and one of them is tracing the packet stream through a number of stepping stone hosts, which tend to keep the attacker sheltered from identification. The key limiting factors of existing approaches include:

- All the approaches attempt the trace back using step-by-step backward trace from victim to attacker.
- All the approaches use same IP network for trace back as the attackers use for attacking.
- Most of the approaches require changes or additions in the existing routing protocols.
- Most of them operate in active mode and could be evaded by the attackers easily.
- Most of the approaches have high memory requirement, high routing overhead and high detection latency.
- Most of the approaches cannot detect attacks across stepping stone or zombie nodes accurately.

In this paper, we present a new IP marking technique to solve the IP traceback problem. Our approach is using IP record route option to probabilistically mark packets with entire path information as they arrive at the routers and use a Wireless Overlay Network (WON) to store the router address list once the IP record route option is full. Because each marked packet represents the entire path it has traversed, with a single such packet a victim can reconstruct the entire path. Our approach may be incrementally deployed, and is backward compatible with the existing infrastructure. We describe a marking and reconstruction algorithm that has fixed computation overhead and no false positive. Furthermore, we demonstrate our approach can handle distributed Dos attacks very well and the volume of attack packets needed to reconstruct the attack path is controlled by victim, and all above functionalities don't need support from ISP or knowledge of network topology.

The rest of this paper is organized as follows. Section 2 provides related work and section 3 outlines our basic approach and characterizes marking and reconstruction algorithms for implementing it. In section 4, we detail evaluation of our approach and comparison to other probabilistic packet marking approaches. Finally; in section 5 we conclude and summarize our findings.

2. Related work

Recently Probabilistic Packet Marking (PPM) [8,14] and PPM based approaches have been proposed for tracing the source. While PPM has the advantages of efficiency and easy implementability over deterministic packet marking and router based logging and messaging, it has the potential drawback that an attacker may impede traceback by sending packets with spoofed marking field values as well as spoofed source IP addresses. The following sub section will review two well known PPM based approaches and their limitations.

2.1. Probabilistic Packet Marking

This scheme is based on the idea that routers mark packets that pass through them with their full addresses or a part of their addresses. Packets for marking are selected randomly with some predefined probability. As the victim receives the marked packets, it can reconstruct the full path.

Node sampling samples the path one node at a time. A single static "node" field is reserved in the packet header, upon receiving a packet, each router chooses to write its address in the node field with a certain predefined probability p. after enough such packets are sent, the victim would have received at least one sample for every router in the attack path and the victim can reconstruct the attack path using such samples. However,

this method has two serious limitations: first, routers are that far away from the victim contribute fewer samples and random variability can easily lead to disordering; secondly, if there are multiple attackers, then multiple routers may exist at the same distance making detection of attack more difficult. Therefore, this approach is not robust for DDoS. This approach has a number of limitations:

- Large volume of packets needed to reconstruct the attack path.
- Large computation overhead to path reconstruction.
- Large number of false positives.
- Can not handle major DDoS.

2.2. Adjusted PPM

In PPM and AAM, the routers far away from victim contribute fewer packets for path reconstruction. Adjusted PPM [15] uses an additional field in the IP header called IP Option field to record number of hops traversed by the packet. Packet is marked probabilistically proportional to the inverse of this distance. The farther the router is from victim, the higher probability it marks the packets. This significantly reduces the number of packets needed for path reconstruction. The approach has several limitations:

- It has low scalability.
- It is bad for DDoS handling.

3. WON for Probabilistic Packet Marking

Before we introduce our marking approach, we will give a brief introduction to the terminology used in the article.

IP Record Route Option*:* The record route option allows the source to create an empty list of IP addresses and arrange for each router that handles the packet to add its IP address to the list. Figure 3 shows the format of the record route option.

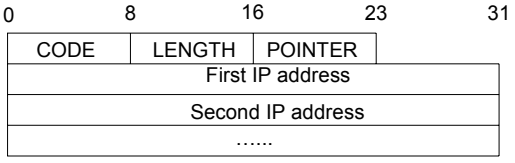

Figure 3. The format of the record route option

As described above, the CODE field contains the option number and option class (7 for record route). The LENGTH field specifies the total length of the option as it appears in the IP packet, including the first three octets. The fields starting with one labeled First IP address comprise the area reserved for recording router addresses. The POINTER field specifies the offset within the option of the next available slot.

DIR*:* DIR is a Double Interface Router equipped with both wired and wireless interfaces. Wireless routers with Internet connection sharing, networking and firewall features are an alternative to hard wired routers or networking software. Wireless routers are actually wired routers with wireless access points built in so it can have wired and/or wireless functionality at the same time [17].

WON*:* WON is Wireless Overlay Network built on top of existing network; a WON contains wireless nodes.

Partition*:* A network can be divided into partitions based on the coverage of the wireless node in WON. Each partition contains all the routers in the coverage area of one wireless node, and each wireless node can communicate with the DIRs in the partition.

Boundary Router*:* any router which has a link to a router or device outside its own partition.

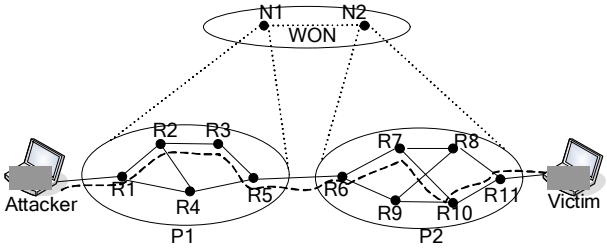

Figure 4. The architecture of WON

Our marking algorithm is similar to the IP Record Route Option [18] where each router's address is appended to the end of the packet as it travels through the network from attacker to victim. Consequently, the marked packet received by the victim has a unique complete ordered list of the routers it traversed.

The IP Record Route Option has two serious limitations: first, it has high router overhead by appending each router's address to the packet; secondly, the distance from attacker to the victim is unknown a priori, so it's impossible to reserve enough space in the packet for the complete list of the routers.

To solve above limitations, we introduce the following architecture first. Figure 4 depicts a simple wired network having two partitions p1 and p2, and a wireless overlay network containing two wireless nodes N1 and N2. Partition p1 has routers R1, R2, R3, R4, and R5 of which R1 and R5 are boundary routers, R1 has a link to attacker A and R5 has a link to partition p2; partition p2 has routers R6, R7, R8, R9, R10, and R11 of which R6 and R11 are boundary routers, R6 has a link to R5 in partition p1 and R11 has a link to victim V. Wireless node N1 monitors partition p1 and N2 monitors partition p2. The dashed line represents the attack path from the attacker to the victim, and the dotted line connecting each wireless node and wireless nodes to partitions

indicate the communication link is wireless link. Our approach has following assumptions:

- The network is already partitioned.
- The wireless link is stable.
- Each partition has a partition ID.
- Each router knows which partition it belongs to because each router need inscribe partition ID into packet for path reconstruction.

To reduce router overhead, we probabilistically mark packet: in an attack path from the attacker to the victim, if router R is the first router following the attack source, upon receiving a packet w, R will generate a random number in (0, 1), if this random number is greater than predefined probability p, then R will open IP record route option and append its IP address to the end of the packet, and each following router along the attach path will append its IP address to the end of the packet after the first router R opens the IP record route option. When a packet w arrives at the victim, packet w is either unmarked or marked with a complete ordered list of routers along the path. In Figure 4, attack packets are originated from A, to reach victim V, each packet will traverse along the path R1-R2-R3-R5-R6-R7-R10-R11, in the attack path, R1 is the first router after attacker, once R1 decides to mark a packet, all other routers R2, R3, R5, R6, R7, R10, R11 should mark the packet also.

The distance between attacker and victim is unknown a priori, it's unsure that how much space in the packet should be reserved for the complete list of routers. The maximal internet header is 60 octets, the record route IP option header is 3 octets, a typical internet header is 20 octets [18], in our approach we reserve one octet for inscribing partition ID (one octet can represent $2^8 = 256$ partitions, this number is enough), now the format of record route option is depicted in Figure 5, one octet field PART_ID is used to store the ID of the partition where packet resides currently, when each router appends its IP address to the end of the packet it will also inscribe current partition ID into PART_ID field. If there are no other IP options in use, the maximum number of IP addresses that the IP record route option can contain is (60-20-3-1)/4 = 9.

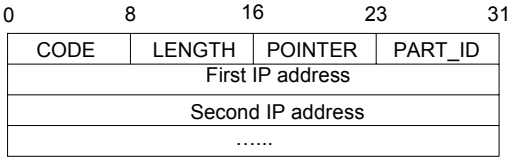

Figure 5. The format of the record route option

Our approach introduces WON to store the marking information: each wireless node of WON maintains a table stored in its memory, the record tuple has elements <packet_ID, previous_part_ID, partial_attack_path>, packet_ID is the ID of the packet, previous_part_ID is the partition ID that this packet came from, and partial_attack_path is attack path of the entire attack path that this packet has traversed.

The architecture in Figure 4 has two parts: one part is partition which consists of boundary routers and center routers; the other part is WON. The basic approach is when a packet w reaches an ingress boundary router R and R decides to mark w, before marking R it should notify WON from which partition packet w is coming and the packet ID of w, WON will store the information into previous_part_ID and packet_ID. When packet w reaches a egress boundary router R', after marking R' should notify WON to store the partial path of packet w traversed into partial_attack_path, and then router R' should clear the list of IP addresses stored in IP record route option. If IP record route option is full when packet w reaches a center DIR router R'', R'' should notify WON to store partial attack path before it marks the packet. Each time when a router clears the IP addresses list of record route option, the router should write the latest IP address of IP addresses list into the First IP address field of record route option, and then append its address to the Second IP address field; this makes it easy to append two adjacent partial paths together. The communication between WON and partitions requires boundary routers and certain center routers are DIRs.

Table 1. Marking steps using Figure 4.

Marking steps	Record route option	Packet _ ID	Previous _part_ID	Partial_ Attack_ path
Packet w reaches R1	null	w	null	null
R1 marks w	R1	w	null	null
R2, R3 mark w	R1R2 R3	w	null	null
W reaches R5	R3	w	null	N1(R1R2R3)
R5 marks w	R3R5	w	null	N1(R1R2R3)
Before w enters P2	R5	w	null	N1(R1R2R3) N1(R3R5)
……	……	……	……	……
W reaches Victim	R11	w	P1	N2(R5R6R7) N2(R7R10 R11)

Putting aside for the moment the difficulty in deciding which certain center routers should be DIRs, this algorithm is efficient to implement. Use Figure 4 as an

example to understand thoroughly the entire algorithm it's better for us to assume the IP record route option reserves space for only three IP addresses (in real implementation, the reserved space should be enough for nine IP addresses), the Table 1 provides the packet marking work flow. The complete algorithm is shown in Figure 6.

```
Marking procedure at router R:
    For each packet w
      If record route option of w is close
        Let x be a random number from (0, 1);
        If x<p then,
          Open record route option of w;
          packet_ID ←- 16-bit ID of IP header;
          previous_part_ID ←- null;
          PART_ID ←- current partition ID;
          Mark R to IP record route option;
      Else
        If R is ingress boundary router
          packet_ID ←- 16-bit ID of IP header;
          previous_part_ID ←- PART_ID;
          PART_ID ←- current partition ID;
          Mark R to IP record route option;
        If R is egress boundary router
          Mark R to IP record route option;
          partial_attack_path ←- option list;
          Clear option list;
        If option list is full
          partial_attack_path ←- option list;
          Clear option list;
          Mark R to IP record route option;

Path reconstruction procedure at victim V:
    For each marked packet w received at V
    Request WON to report information for w
    Sort routers according to previous_part_ID
```

Figure 6. Packet marking algorithm

4. Evaluation and Comparison of PPM Based Approaches

We will evaluate our approach using the following metrics:

Number of attacking packets needed for traceback: the number of attacking packets needed for traceback in our scheme is $\frac{1}{p}$ where p is probability of a router marks a packet. In [8] the suggested number of p is 0.04, PPM and advanced and authenticated packet marking [13] need thousands of packets; other PPM based approaches such as adjusted PPM, DDoS Scounter [15][16] need hundreds of packets; but our scheme only need very few packets for traceback. Compared to PPM and PPM based approaches, our approach has another advantage: the number of packets needed for traceback is only related to probability which is decided by victim in our approach; in PPM and other PPM based approaches, the number of packets needed for traceback is $\frac{\ln d}{p \times (1-p)^{d-1}}$ where d is the distance between attacker and victim, this formula is related to both probability and distance, even if probability is decided by victim, but the distance is under control of attacker.

Path reconstruction overhead: in our approach we use IP record route option to mark the packets, one such marked packet can reconstruct the entire path, and the list of IP addresses is ordered. Once a detection system indentifies attacks, the system needs one step communication with WON to get the ordered list of IP addresses and append each partial attack path together in order of pervious_part_ID, there is no additional computation overhead incurred. PPM and other PPM based approaches inscribe a single node IP address or partial attack path into the packets; they require a large volume of combinations to reconstruct the attack path.

Ability to handle major DDoS attacks: the table stored in WON has tuple <packet_ID, previous_part_ID, partial_attack_path>; such tuple uniquely defines a record. Even distributed attackers reside in the network and all attackers are treated in the same manner even if they are far away from the victim. The combined information of packet_ID, previous_part_ID, and partial_attack_path can identify them.

Number of false positive: the attack path is reconstructed by detection system requesting WON for marking information, each marking record stored in WON is uniquely defined by tuple <packet_ID, previous_part_ID, partial_attack_path>, it's impossible for two attack packets to have the same tuple, so our approach has zero false positives.

Fragmentation handling: our approach uses IP record route option to mark the packets, the field used for fragmentation in IP header is 16-bits IDENTIFICATION field which is not changed in our approach, so this approach can handle packet fragmentation.

Scalability: our approach is highly scalable; it does not need additional configuration on other devices to add a single device to the scheme. If the router added is a double interface router, then it requires a radio link assignment to communicate with WON, and such requirement does not change the network.

Incremental deployment: To deploy the scheme, vendors need to implement two functions: marking and reconstruction functions. Once the marking function is available, it can perform traceback within the ISPs that deploy it.

ISP involvement: each router needs marking function, upgrade of such software on routers is straightforward: once routers are upgraded, the marking

function on each router is enabled, this requires very few ISP involvement.

Knowledge of topology: the path reconstruction procedure happens between detection system and WON, there is no need for detection system to know the network topology.

The following table gives a detailed comparison of various PPM approaches.

Table 2. Comparison of PPM based approaches

Evaluation metrics	PPM	AAM	Adj. PPM	DDoS Scounter	**WON**
incremental deployment	yes	yes	yes	yes	**yes**
Number of packets for tracing	1000	1000	Less	Less	**10s**
ISP involvement	low	low	low	fair	**low**
Fragmenta-tion handling	no	no	no	yes	**yes**
Scalability	high	high	low	Very high	**Very high**
Reconstruc-tion overhead	Very high	less	less	less	**Very less**
Knowledge of topology	no	yes	no	no	**no**
DDoS handling	fair	fair	bad	Very good	**Excell-ent**
Number of false positives	large	Very low	fair	less	**Zero**

5. Conclusion

In this article we present an IP trace back scheme which is more efficient than the schemes available up to now. In contrast to previous work, our techniques have significantly higher precision (no false positive) and very lower path reconstruction overhead for the victim to reconstruct the attack paths under large scale DDoS.

6. References

[1] Cyber Security: A Crisis of Prioritization, Report to the President, President's Information Technology Advisory Committee, February 2005.

[2] Tracking and Tracing Cyber Attacks: Technical challenges and Global Policy Issues, CMU, SEI-2002-SR-009, November 2002.

[3] Sathish Alampalyam, Anup Kumar, S. Srinivasan, "Mobile Ad hoc Network Security - a Taxonomy", Accepted for Proceedings of 7th International Conference on advanced communication Technology, 21-23 February 2005 at Phoenix Park, Korea.

[4] S. C. Lee and C. Shields, "Tracing the Source of Network Attacks: A Technical, Legal and Societal Problem," Proceedings of the 2001 IEEE, pp. 239-246, 2001.

[5] T. Baba and S. Matsuda, "Tracing Network Attacks to Their Sources," Internet Computing, vol. 6, pp. 20-26, 2002. Mar/Apr 2002.

[6] Jelena Mirkovic, Gregory Prier and Peter L. Reiher, "Attacking DDoS at the Source," Proceedings of the 10th IEEE International Conference on Network Protocols, pp. 312 - 321, 2002.

[7] J. Rowe, "Intrusion Detection and Protocol Isolation: Automated Response to Attacks," in Recent Advances in Intrusion Detection, 1999.

[8] S. Savage, D. Wetherall, A. R. Karlin and T. Anderson, "Practical Network Support for IP Trace back," in SIGCOMM, 2000, pp. 295-306.

[9] R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods," in Proceedings of the 2000 USENIX Security Symposium, Jul 2000, pp. 199- 212.

[10] S. Dan, H. Harley, "Cooperative Intrusion Trace back and Response Architecture (CITRA)", in DARPA DISCEX2001, June 12-14, 2001, California.

[11] A. Belenky and N. Ansari, "On IP Traceback," IEEE Communications Magazine, Vol. 41, No.7, pp. 142-153, July 2003.

[12] Z. Gao and N. Ansari, "IP Traceback from the Practical Perspective," IEEE Communications Magazine, Vol.43, No. 5, May 2005.

[13] Dawn Xiaodong Song and Adrian Perrig, "Advanced and authenticated marking schemes for IP traceback," *Proc. IEEE INFOCOM,* IEEE CS Press, 2001, pp. 878-886.

[14] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack", In *Proc. IEEE INFOCOM,* IEEE CS Press, 2001, pp. 338-347.

[15] Teo Peng, Christopher Lecki amd Kotairi Ramamohanroa, "Adjusted Probabilistic Packet Marking", *In Proceedings of IFIP-TC6 Networking Conference 2002,* Pisa, Italy , May 2002.

[16] Chen Kai, Hu Xiaoxin, Hao Ruibing, **"**DDoS Scounter: A Simple IP Traceback Scheme**",** in *Progress on Cryptography*: 25 years of Cryptography in China, Kluwer Academic Publishers, 2004.

[17] Wireless Router Reviews, http://www.firewallguide.com/wireless.htm

[18] J. Postel, "Internet Protocol", RFC791, Sep. 1981.