Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Detection and Tracing source of Denial of Service attack using Hybrid Trace back Mechanism

Christopher Deepak G[1], Benedict J.N.[2]

[1,2]Department of computer science, Rajalakshmi Engineering College

Abstract:- Denial of service attack is one of the problems faced in networking which results in unavailability of resources to the network users.Tracing denial-of-service (DoS) attacks back to their source is a difficult task for network administrators. The source of attacks, sometimes, comes from a single source or multiple sources that makes harder to an investigator to trace attackers back to their original computer. This work provides a detection and IP trace route mechanism that can be able to identify a source of DoS attacks. The detection process is done by a NIDS called Snort and a hybrid trace back scheme is used to trace back the source of the IP. Altogether the system can monitor, detect and trace back the source of the DoS attack.

Index Terms—Denial-of-service attacks, IP trace back scheme, NIDS.

I. INTRODUCTION

Denial-of-Service (DoS) [4] is an attack attempting totemporarily disrupt computers to cause service unavailability.Typically, the source of attacks comes from a single source ormultiple sources that makes harder to an investigator to traceattackers back to their original computer. In order to make attacks more difficult to discover, sophisticated attackers couldhide their original IP address by using spoofing techniques, orthey can cover themselves by launching attacks behind the proxy. Even though many security devices, such as firewall and intrusion detection system (IDS), are used in the network forpreventing such attacks. They might be able to detect and prevent DoS attacks, however, they do not provide us a feature to identify the attack source. As a result, several detection andtrace back techniques are proposed in a research community. This works is focused mainly on performing a DoS attack, then detecting the DoS attack followed by tracing the route in which the attack is performed. The main advantage of this work is the use of a new trace route algorithm known as the exhaustive algorithm which can perform trace route even under heavy load. Load balancing is an important aspect that affects the performance of any trace route scheme by building a correct load balancing algorithm the trace back scheme works as directed. Many works that are proposed so far suffer from heavy load caused by the DoS attack so this problem is overcome by this algorithm. This work begins by performing an DoS attack using specified tools and then detecting the attack with the help of a Network intrusion detection system in this case snort then tracing the route of the source of the attack.

II. RELATED WORK

Since many attacks arise in the Internet nowadays, many security devices such as firewall and intrusion detection system(IDS) are commonly introduced in the network for preventingsuch attacks. As these preventive devices are considered as afirst security perimeter, they can only detect and prevent DoSattacks. However, they do not provide a feature to identify the source of attack. As a result, a research community has beendeveloping several traceback techniques in order to recover theattack path and identify a true IP address of an attack source. The main purpose of a traceback system is to reconstructattack paths, so the network administrators will be able toidentify an IP address of an attacker. In the real situation,attackers normally do not use the real IP address. From

Baba and Matsuda's [1]work, they roughly classify a traceback system into twocategories; proactive and reactive trace back. The proactive techniques prepare information for tracing when packets are incommunication, while the reactive techniques start tracing afterDoS attacks are detected.

2.1. Proactive tracing system.

In the proactive tracing, it records packet information during packet transmission. Once the attack occurs in thenetwork, investigators are able to use this information to trackrouting paths and identify a source of attack. Four proactivetracing schemes are discussed in this work.

2.1.1. Packet Marking Scheme

Savage and Wetherall[7] proposed a technique to record packet information in order to use for tracing back to asource of such packets if there are suspicious activitiesoccur in the network. This technique is also known aspacket marking. In this scheme, the information of the routers is stored in the packets that it passes. So, the recipient of the marked packet is able to use this router information to route the packet's path to its source.

2.1.2. ICMP Traceback Scheme

Bellovin [2] proposed ICMP traceback scheme in 2000.In this technique, each router that suspicious packets passthrough generates an ICMP trace back message or iTrace. Typically, the iTrace message consists of the hop information, and a timestamp. Theseinformation will be used as a path recovery to identify therouting path back to an originated source.Similarly to a packet marking scheme, thedisadvantages of this scheme are a requirement of a largenumber of packets to reconstruct attacking paths, as well asa modification of routers in which they can support afeature of routing information addition. Also, the ability to prevent major DoS and DDoS attacks is bad because thistechniques cannot deal with a large number of reflectors.

2.1.3Hash-based IP Traceback Scheme

The hash-based IP traceback technique or Source PathIsolation Engine (SPIE) was introduced by Snoeren et al.[8] in 2002. The router, called Data Generation Agents(DGAs), records packet information from packets passingthrough it. The other components in this technique consistof; 1)SPIE Collection and Reduction Agents (SCARs) which are used for query necessary information fromconnected DGAs, 2) SPIE traceback manager (STM) which is used to communicate to the victims IDS through a central managing unit . This scheme reduces the size of storage space to store pathinformation by using hash functions.The negative side of this scheme is investigated byBhaskaran et al. [3]. They found that when we use SPIE totrace attacks on high-rate interface, we must perform theaction within a very short period of time. This situation getsworse if the victim does not realize he/she is under attacks,or he/she is unable to contact STM.

2.1.4 Bhaskaran et al. Traceback Scheme

Bhaskaran et al. [3] proposed a technique based on apacket marking scheme. The system consists of two parts;1) Controller which is a trusted entity that manages the denial of service attacks, and 2) Agent which has information about the domain controller. During the operating process, controller maintains a database about all agent IDs. As agents areinstalled on all the edge routers, the victims incoming packets are marked with the controller ID and agent ID.After that the victim sends request, the packets are marked by the agents upon receiving command from the controller as suspicious traffic and then the controller identifies the nearest source of the packet by extracting IP address against the given agent ID. Therefore, a single packet is enough to identify theapproximate originated source of suspicious packet.However, their schemerequires more ISPassistance to recover the attack path thanother schemes. This technique can successfully trace back to the source within a ISP domain only.

2.2. Reactive tracing system

Different from proactive tracing, reactive tracing starts torecord packet information and traceback to an originated IPaddress after the attacks have been detected. The challenge ofthis technique is to develop methods that be able to detect andmatch the attack effectively. Two different reactive tracingschemes are discussed in this work.

2.2.1. Hop-by-Hop Tracing

Hop-by-hop traceback [5] is the basic method in usetoday for tracing attacks. This method is suitable for tracingdenial-of-service attacks because the nature of DoS trafficis large and continuous packet flows. Moreover, the source of attack is mostly spoofed IP addresses. In this technique,a tracing program which is installed into the router locatedclosest to the attacker, is used for monitoring incomingpackets. If attackers use spoofed IP address to launchattack, these packets will be stored into the routers formonitoring. This procedure is repeated to the adjacencyrouters until the program is able to identify the attacker'soriginated IP address.

On the other hand, the limitation of this scheme occurswhen it deals with DoS/DDoS attacks in which the packetscome from multiple sources and each source generates onlya small number of packets. So, the information recorded insome routers might not enough for a program to trackattackers back to their original source. Similarly, if theattacker stops their action before the trace is finished, theexamination will be failure.

2.2.2. Overlay Network

Generally, the standard function of routers onlyexamines a packet header and chooses the best path toforward packets to intended destination. Stone [9] has proposed a technique to add a traceability feature to routerin order to recover attacking path back to attackers. Thistechnique can be accomplished by adding a device calledtracking router (TR) to monitor all traffic passing through this network.In this scheme, even it does not require anymodification on the user's router to run a tracing process, the drawback is in a large number of requirement in ISPinvolving in order to identify the attack source IP address.Moreover, the high processing overhead over each packetis another drawback of this scheme.

2.2.3. Baba and Matsuda's Tracing scheme

Baba and Matsuda [1] proposed an IP tracing techniquebased on a hop-by-hop tracing scheme with an ability ofusing only single packet to accomplish a job. In addition toa simplified version of hop-by-hop tracing, this schemeuses more information such as MAC address, ATM's virtual path identifier/virtual channel identifier (VPI/VCI)to identify nodes in the attack path. Furthermore, anadditional device named tracer is used for storing incoming packet information and data link identifier that can be used to identify the adjacent node by searching the datalink identifier of the forwarded package that matches the attack packets. Similarly to other reactive IP traceback schemes, it requires some alteration to router functions and packetinformation. Also, the assistance from ISP to reveal true IPaddress of attackers is another concern.

III. PROPOSED WORK

The main goal of the proposed system is to monitor and detect DoS and to trace the route back to the source. So the first step is to perform an DoS attack using specified tools which can demonstrate a DoS attack. The attack is performed from another system to the host system. The host system is installed with a Network intrusion detection system which can monitor network traffic and detect the occurrence of a DoS attack. When a attack is detected by the NIDS in the host system. Then using the traceroute scheme the source of the attack can be identified. The traceroute scheme is based on an algorithm that can operate well even during high network load this algorithm is called Exhaustive algorithm. Using this algorithm the source of the attack can be traced back.

3.1. Performing DoS Attack

In order to understand the experimenting environment the first step is to perform a DoS attack on the host system. To perform a DoS attack port scanning process has to be done, this is done in order to find the specific port on which the attack is to be performed using a port scanner tool the victims system is identified along with its Ip address. This Ip address is then used to perform the attack. Once the victims Ip address is acquireda DoS attack tool is used to perform the DoS attack on the victim machine.

3.2. Monitoring and Detecting DoS Attacks

Recently, network intrusion detection system (NIDS) is animportant security architecture in computer network. This is because NIDS is able monitor suspicious traffic, such as denialof service attacks, and alert system administrators when attacks are detected. Network Intrusion Detection Systems (NIDS) are placed at a important points or critical points within the network to monitor traffic to and from the network. It analysis traffic on the entire subnet, works in a promiscuous mode, and matches the traffic on the subnets to the database of known attacks. Once an attack is detected, or an intrusion is sensed, an alert is sent to the administrator. To detect suspicious traffic, NIDS examinesevery incoming packets and compares them with rules orsometimes known as attack signatures. If any packets have asimilar pattern as defined in NIDS rules, they will be markedas suspicious packets and sent to system administrators formore investigation.In this work, we use snort as a denial-of-service detectingtool. Snort [6] is one of the most powerful open-source network intrusion detection tool that allows users to usestandard rules or implement their own rules to detect intrusion.Snort performs content pattern matching and detects a varietyof attacks, including many kinds of denial-of-service attacks.Snort uses a detection engine, which uses a simple language to program for describing per packet tests and actions. Ease of usein snort leads to the development from the research communityto implement new exploit detection rules. As a result, wedevelop snort rules to help our traceback system to inspectsuspicious packets and detect DoS attacks. Once the attack has been performed on the victim system, the NIDS present in the system monitors the network traffic and detects the DoS attack that has been performed on the system. Once detected it alerts the system that an attack has been performed. The details given by snort can be used to identify the source of the attack. Since Snort is open source it can be used to detect any type of intrusions. So using the Snort NIDS the system can be monitored for attacks and detected once an attack occurs.

3.3. Tracing Source of DoS

Once the DoS attack has been detected by the NIDS on the victim system, the details given by the NIDS can be used to trace the source of the DoS attack. This is done with the help of the trace back scheme. A traceback system is one which can trace back the source of an attack that has been happened on a system, but tracing a ip back to the source is a difficult task which comprises of many aspects such as ISP involvement, memory requirement, network overhead, victim overhead, network load and so on. So an effective trace back scheme should look into these key aspects. [10]This work uses an effective traceback scheme that works well with all the above aspects, many trace back schemes suffer with the presence of routers that implements load balancing based on packet header fields. This leads to the discovery of misleaded and **incomplete** paths, but the proposed scheme controls packet header contents, and obtains a more precise picture of the actual routes that packets follow.

In traditional trace route schemes routers uses per-packet, per-flow, or per-destination policy to spread traffic in multiple paths. In *per-flow load balancing*, packet header information describes the flow of each packets, and all the packets are forwarded by the router to a same flow and to the same interface. A natural flow identifier is the classic *five-tuple* of fields from the IP header and either the TCP or UDP headers: *Source IP address*, *Destination IP address*, *Protocol*, *Sourceport* and Destination *port*.

Per-flow load balancing ensures that packets from the same flow are delivered in order. *Per-packet load balancing* makes no attempt to keep packets from the same flow together, and focuses purely on maintaining an even load. *Per-destination load balancing* could be seen as a coarse form of per-flow load balancing, as it directs packets based upon the destination IP address. But, as it disregards source information, there is no notion of a flow per se. As seen from the measurement point of view, per-destination load balancing is equivalent to classic routing which is also per destination, and so we will not explore it here. Where there is load balancing, there is no longer a single path from a source to a destination. In the case of per-packet load balancing, a given packet might take more than one possible routes. With per-flow load balancing, the notion of a single route persists for packets belonging to a given flow, but different flows for the same source-destination pair can follow different routes. In this case the proposed scheme can be able to uncover all the routes from the source to the given destination. Thus enabling us to trace the source of the DoS attack.

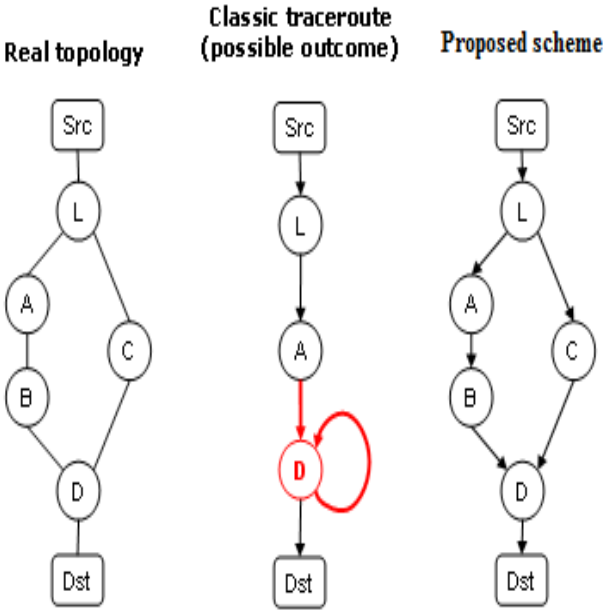

Figure 1. Brief Demonstration of proposed Scheme.

In the above fig, if the route between *Src* and *Dst* is to be measured, L is a router that balances load between two paths, via routers A or C. The middle part of the figure shows the result of the classic trace route. On the right is the result with the proposed scheme.

3.4. Exhaustive Algorithm

With the deployment of load balancing, there is no longer only one path between two Internet hosts. This algorithm sends enough probes at eachhop to find all the possible interfaces. Unlike the other algorithms,it varies the flow identifier of the probes in a controlled manner, toensure the discovery of all the interfaces with a high confidencedegree. It also categorizes load balancers as "per-packet" (pseudo-random, round-robin packet balancing) or "per-flow" (packets belonging to the same flow follow the same path).
Using this exhaustive algorithm the trace route scheme is able to trace back the source successfully.

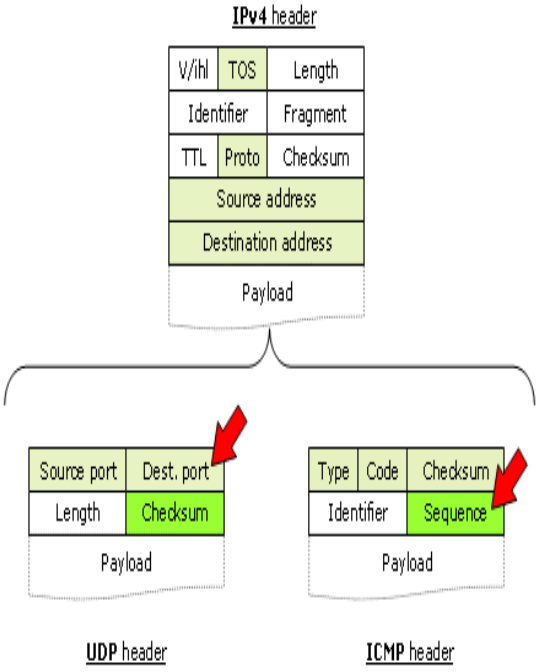

Figure2. The IP, UDP and ICMP headers. Per-flow load balancers use the grey fields to identify a flow. Red arrows show the fields incremented by classic traceroute, the proposed scheme uses green fields.

IV. EXPERIMENTS & RESULTS

In the experiment, the traceback system is installed withUbuntu Desktop version 12.04.5 LTS amd64. The attacker runs DoSattacks by using a low frequency attack tool called LOIC. The attacker performs DoS attack on the victim, the victim systems that runs the NIDS in it monitors for incoming network traffics and detects the DoS attacks caused by the attacker. Once detected the NIDS alerts the system that an attack has been encountered. With the details given by the NIDS the trace route scheme is able to successfully track the source of the attack.

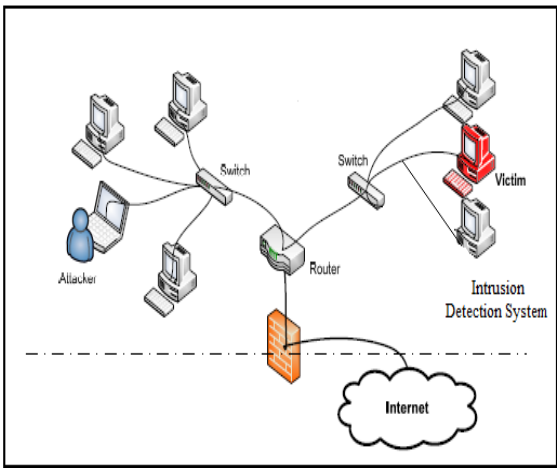

Figure 3. The attack scenario with NIDS.

Figure 4. Visualization of trace route

V. CONCLUSION

The hybrid trace back scheme is able not only to detect DoS attacks by using snort rules, but also reconstruct attacking paths back to the source IP address without any significant computation overhead on the victim machine. It is observed that our trace back scheme works even under high network load.

REFERENCES

[1] T. Baba, and S. Matsuda, "Tracing network attacks to their sources",*IEEE Internet Computing*, vol. 6, no. 3, pp. 20-26, Mar-Apr 2002

[2] S. M. Bellovin, "ICMP TracebackMessage"*IETF draft*, http://www.research.att.com/smb/papers/draftbellovin-itrace-00.txt

[3] V. M. Bhaskaran, A. M. Natarajan, and S. N. Sivanandam, "Analysis of IP Traceback Systems", *International Symposium on Ad Hoc and Ubiquitous Computing (ISAUHC '06)*, pp. 125-130, Dec 2006

[4] CERT/CC, (Computer Emergency Response Team), "Denial of Service Attacks", http://www.cert.org/tech_tips/denialofservice.html

[5] H. F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", Special Report, CMU/SEI-2002-SR-009, Nov 2002

[6] M. Roesch, "Snort - lightweight intrusion detection for networks", *"Proceedings of LISA '99: 13th Systems Administration Conference"*, USA, November 7–12, 1999

[7] S. Savage, and D. Wetherall, "Network Support for IP Traceback", *IEEE/ACM Transactions on Networking*, vol. 9, no. 3, pp. 226-237

[8] 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*, vol. 10, no. 6, pp. 721-734

[9] R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods", *Proceedings of 9th Usenix Security Symposium"*, UsenixAssoc., pp. 199-212, 2000

[10] Paris-traceroute http://www.paris-traceroute.net/.

[11] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger,T. Friedman, M. Latapy, C. Magnien, and R. Teixeira. "Avoiding traceroute anomalies with paris traceroute". In Proc. ACM SIGCOMM Internet Measurement Conference , Oct. 2006

[12] Brice Augustin, Timur Friedman, and Renata Teixeira, "Exhaustive path tracing with paris traceroute", Proceedings of the 2006 ACM conference article No. 49