International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.1, pp-316-319 ISSN: 2249-6645

AN EFFICIENT WAY OF RETRIEVAL DATA BY TRACKING ATTACKERS

G.Sindhu*, Mrs.R.Kalaiselvi**

*II M.E CSE, Sri Shakthi Institute Of Engineering and Technology, Anna University, Coimbatore

**Asst.prof CSE, Sri Shakthi Institute Of Engineering and Technology, Anna University, Coimbatore

ABSTRACT:

A major threat to the internet is that the Distributed Denial- of- Service (DDoS) attacks. There is no efficient way to traceback the attackers because of memoryless feature of routers. In this paper, trace back of the attackers in a wireless networks are efficiently identified and also to protect the data from the attackers using entropy variations. In the existing system, some approaches have been suggested to identify the attackers such as probabilistic Packet Marking (PPM), Deterministic Packet Marking (DPM). These two approaches are not efficient because it requires injecting marks into individual packets in order to trace back the attackers. In PPM, it can only operate in a local range of internet. In DPM, it requires all the internet routers to be updated for packet marking. Scalability is also a big problem in both PPM and DPM. In order to overcome the above drawbacks, a method based on Entropy Variation is proposed which is a measure changes of randomness of flows at a router for a given interval in a large scale attack network. This method is used to identify the attackers efficiently and supports a large scalability.

Index terms - DDOS, IPtraceback, Entropy Variation.

I.INTRODUCTION

A DoS(denial of service) attack is a malicious attempt by a single person or a group of people to cause the victim, site, or router to deny service to its customers. When this attempt derives from a single host of the network, it constitutes a DoS attack. On the other hand, it is also possible that a lot of malicious hosts coordinate to flood the victim with an abundance of attack packets, so that the attack takes place simultaneously from multiple points. This type of attack is called a Distributed *DDoS*, or DDoS attack. A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers. The main reason is that the network security community does not have efficient and effective trace back methods to locate the attackers in a wireless network as it is easy for attackers by taking the advantages of vulnerabilities of the world wide web [11]. In this Traceback of DDoS Attacks Using Entropy Variations is used to find out the Distributed Denial-of-Service (DDoS) attacks are a critical threat to the Internet and user's location with the help of Entropy Variation Mechanisms against DPM and PPM.

Traceback of DDoS Attacks is random. Therefore, a Entropy Variation Mechanisms against DPM and PPM should empower a router with the ability to determine whether it should move and where it should move to such that the movement can enhance Attacks quality without depleting scarce resources or significantly compromising coverage and network connectivity. It is the movement of the routers are purposeful. It is important to have an efficient Traceback of DDoS Attacks scheme to ensure that the sensor router mobility is exploited in the best possible way. At the same time the mobility management strategy should avoid inefficient usage of scarce resources, such as energy and network bandwidth. Vulnerable hosts are those that are either running no antivirus or out-of-date antivirus software. These are exploited by the attackers who use the vulnerability to gain access to these hosts. The next step for the attacker is to install new programs on the compromised hosts of the attack network. The hosts running these attack tools are known as zombies and they can be used to carry out any attack under the control of the attacker..IP trace back methods should be independent of packet pollution and various attack patterns. Because of the vulnerability, the original attackers cannot be found. An ad hoc network is a collection of mobile hosts forming a temporary network. The transmission of a mobile host is received by all hosts within its transmission range due to broadcast of wireless communication and Omni directional antennae.

In the existing system, there are two major methods for IP Trace back, Probabilistic Packet Marking (PPM) [1], [2], [3] and Deterministic Packet Marking (DPM) [4], [5]. The DPM strategy requires all the routers to be updated for packet marking. Hence, the scalability of DPM is a huge problem. Moreover, the DPM mechanism poses an extra ordinary challenge on storage for packet logging for routers. Both PPM and DPM are vulnerable to hacking, which is referred to as packet pollution. IP trace back methods should be independent of packet pollution and various attack patterns. Therefore, an entropy variation mechanism empowers a router with the ability to determine whether it should move and where it should move to such that the movement can enhance attack quality. It is important to have an efficient traceback scheme to ensure that the sensor router mobility is exploited. At the same time the mobility management

strategy should avoid inefficient usage of scarce resources such as energy and network bandwidth.

II.AN OVERVIEW OF RELATED WORK

It is obvious that to trace back the attackers is essential in solving the DDOS attacks. In general, the trace back strategies are based on packet marking which include PPM and DPM. It is an extra ordinary challenge to traceback the source of Distributed Denial-of-Service (DDoS) attacks in the Internet. In DDoS attacks, attackers generate a huge amount of requests to victims through compromised computers (zombies), with the aim of denying normal service or degrading of the quality of services. The key reason behind this phenomena is that the network security community does not have effective and efficient traceback methods to locate attackers as it is easy for attackers to disguise themselves by taking advantages of the vulnerabilities of the World Wide Web, such as the dynamic, stateless, and anonymous nature of the Internet. IP traceback means the capability of identifying the actual source of any packet sent across the Internet. Because of the vulnerability of the original design of the Internet, the actual hackers may not be able to find at present. In fact, IP traceback schemes are considered successful if they can identify the zombies from which the DDoS attack packets entered the Internet.

A number of IP traceback approaches have been suggested to identify attackers and there are two major methods for IP traceback, the probabilistic packet marking (PPM) and the deterministic packet marking (DPM). Both of these strategies require routers to inject marks into individual packets. Moreover, the PPM strategy can only operate in a local range of the Internet (ISP network), where the defender has the authority to manage. However, this kind of ISP networks is generally quite small, and we cannot traceback to the attack sources located out of the ISP network. The DPM strategy requires all the Internet routers to be updated for packet marking. However, with only 25 spare bits available in as IP packet, the scalability of DPM is a huge problem. Moreover, the DPM mechanism poses an extraordinary challenge on storage for packet logging for routers . Therefore, it is infeasible in practice at present. Further, both PPM and DPM are vulnerable to hacking, which is referred to as packet pollution.

The PPM mechanism tries to mark packets with the router's IP address information by probability on the local router, and the victim can reconstruct the paths that the attack packets went through. The PPM method is vulnerable to attackers, as stated in [7], as attackers can send spoofed marking information to the victim to mislead the victim. The accuracy of PPM is another problem because the marked messages by the routers who are closer to the leaves could be overwritten by the downstream routers on the attack tree .At the same time, most of the PPM algorithms suffer from the storage space problem to store large amount of marked packets for reconstructing the attack tree [1], [3].

Based on the PPM mechanism, Law et al. tried to trace back the attackers using traffic rates of packets, which were targeted on the victim [2]. Both of these strategies require routers to inject marks into individual packets.PPM strategy can only operate in a local range of the Internet, where the defender has the authority to manage. However, this kind of ISP Networks is generally small and we cannot trace back to the attack sources located of the ISP Network. The model bears a very strong assumption: the traffic pattern has to obey the Poisson distribution, which is not always true in the Internet. Moreover, it inherits the disadvantages of the PPM mechanism: large amount of marked packets are expected to reconstruct the attack diagram, centralized processing on the victim, and it is easy be fooled by attackers using packet pollution.

The deterministic packet marking mechanism tries to mark the spare space of a packet with the packet's initial router's information, e.g., IP address. Therefore, the receiver can identify the source location of the packets once it has sufficient information of the marks. The major problem of DPM is that it involves modifications of the current routing software, and it may require very large amount of marks for packet reconstruction. Moreover, similar to PPM, the DPM mechanism cannot avoid pollution from attackers.

Savage et al. [3] first introduced the probability-based packet marking method, router appending, which appends each router's address to the end of the packet as it travels from the attack source to the victim. Obviously, it is infeasible when the path is long or there is insufficient unused space in the original packet.

Snoeren et al. proposed a method by logging packets or digests of packets at routers [9]. The packets are digested using bloom filter at all the routers. Based on these logged information, the victim can trace back the leaves on an attack tree. The methods can even trace back a single packet. However, it also places a significant strain on the storage capability of intermediate routers.

III. ENTROPY VARIATION BASED TRACEBACK MECHANISM

Entropy variation is a measure of randomness flow of the routers at a given interval of time. The parameters to identify the attackers are time between the two routers in which the data was sent and delay for the overall routers. This mechanism comprises of two algorithms to traceback the attackers and to retrieve the original data.

The flow monitoring algorithm monitors the flow of each and every router. The packets that are passing through the routers are categorized into flows. A flow is defined by a pair-the upstream router where the packets came from and the destination address of the packet. A

router knows its local topologies such as its upstream router attached to another router in a local area network. In this paper, I is denoted as the set of positive integers, and R as the set of real numbers. A flow on a local router is denoted by $<u_i, d_j, t>$; I, j € I, t €R, where u_i is an upstream router of a local router R_i, d_j is the destination generated at the local area network which is the local flows, and L is used to represent the local flows. All the incoming flows are represented as input flows, and all the flows leaving router R_i are named as output flows. We denote u_i; i 2 I as the immediate upstream routers of the local router R_i, and set U as the set of incoming flows of router R_i. Therefore, $U=\{u_i, i \in I\} +\{L\}$. We use a set $D =\{d_i, i \in I\}$ to represent the destinations of the packets that are passing through the local router R_i. If v is the victim router, then v € D. Therefore, a flow at a local router can be defined as follows:

$$F_{ij} (u_i, d_j)=\{<u_i, d_j, t>/u_i \in U; d_j \in D, I, j \in I\}$$

The trace back mechanism performs in terms of scalability which is the size of the networks that can be handled, the storage space that need on routers, trace back time and the operation workload. During non attack period, local flow monitoring is done by gathering information from normal network flows progressing the mean and standard variation of flows. Once a DDOS attacks has been confirmed, the victim starts the IP trace back algorithm. In order to make analysis simple and clear some assumptions are made:

1. The changes may occur through network traffic in a very long time interval for non-DDoS attack cases. By breaking the long time interval into seconds, the change of traffic is recognized.

2. The number of attack packets is much higher than that of legitimate flows. For a local router, the number of flows is N and the probability is P(p1,p2,p3,…..pn) is considered. By considering the flows the attackers are identified and the original data is obtained.

IV. PERFORMANCE EVALUATION

A. Simulation model

Consider an ad hoc network in which routers are uniformly distributed in a square area. In the network, sessions are generated between randomly chosen source-destination routers with exponentially distributed inter-arrival time. The source router of the session transmits data packets with the constant rate 1 packet/sec. We developed our simulation model using ns 2.34 simulator. NS-2 simulator allows extracting from a simulation many interesting parameters, like throughput, packet delivery ratio, end-to-end delay.

B. Simulation Results

The following results show the Some parameters like, end to end delay, throughput and packet delivery ratio are analyzed.

Packet delivery ratio:

Data packet delivery ratio can be calculated as the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the sink. This is the amount of successful received bits at the destination routers for the entire simulation period. Packet delivery ratio should be always high for the efficient algorithm or a protocol. The below figure shows the packet delivery ratio was high when compared with the previous methodology.

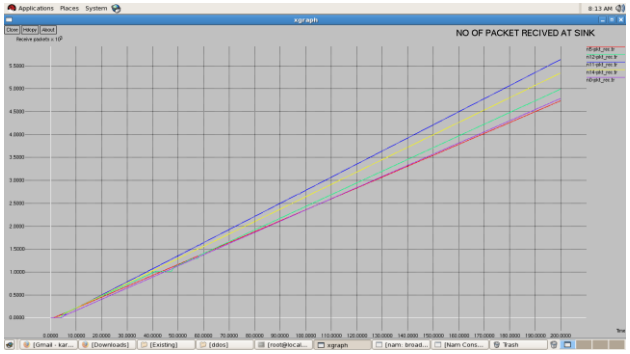

Fig 1: Packet Delivery Ratio

End To End Delay:

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination. End to end delay which includes all possible delays caused by buffering during route discovery time, queuing at the interface queue, retransmission, and processing time. It defines the ratio of interval between the first and the second packets to a total packets delivery.

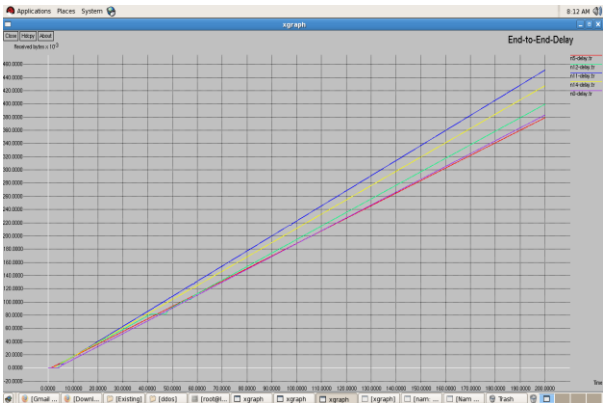

Fig 2: End to End delay

Throughput:

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network router. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

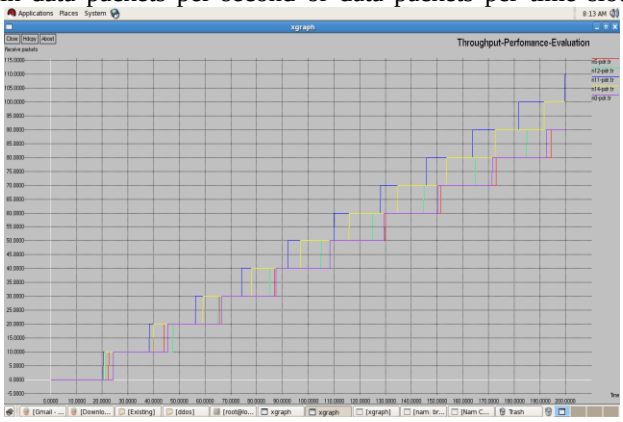

Fig 3: Throughput

Entropy Variation:

By the comparison of the parameters such as the packets received at the sink, End to End delay, Throughput, the actual position of the attackers are identified. The comparison of such parameters are shown in the graph as shown below.

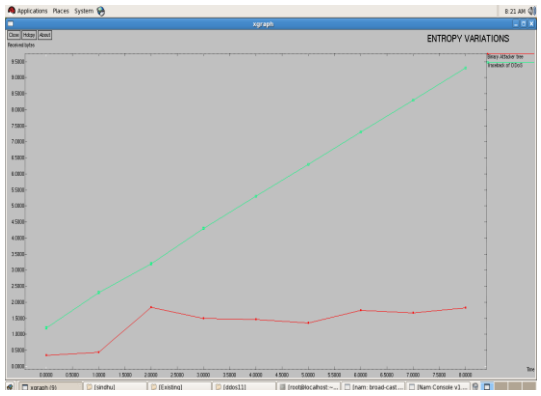

Fig 4:Entropy Variation

In this graph the comparison between the attack and the non attack path is shown. The variation in the attack path is accurately identified and the original data is retrieved.

VI.CONCLUSION

In this paper, the traceback mechanism based on entropy variation is much efficient when compared to the probabilistic packet marking or deterministic packet marking. Because of the vulnerability of the Internet, the packet marking mechanism suffers a number of serious drawbacks: lack of scalability; vulnerability to packet pollution from hacker.

REFERENCES

[1] M. T. Goodrich, "Probabilistic Packet Marking for Large- Scale IP Traceback," IEEE/ACM Trans. Networking, vol. 16, no. 1, pp. 15-24, Feb. 2008.

[2] T. K. T. Law, J. C. S. Lui, and D. K. Y. Yau, "You Can Run, But You Can't Hide: An Effective Statistical Methodology to Traceback DDoS Attackers," IEEE Trans. Parallel and Distributed Systems, vol. 16, no. 9, pp. 799-813, Sept. 2005.

[3] S. Savage, "Network Support for IP Traceback," IEEE/ACM Trans. Networking, vol. 9, no. 3, pp. 226-237, June 2001.

[4] Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking," IEEE Comm. Letters, vol. 7, no. 4, pp. 162-164, Apr. 2003.

[5] D. Dean, M. Franlin, and A. Stubblefield, "An Algebraic Approach to IP Traceback," ACM Trans. Information and System Security, vol. 5, no. 2, pp. 119-137, May 2006.

[6] G. Jin and J. Yang, "Deterministic Packet Marking Based on Redundant Decomposition for IP Traceback," IEEE Comm. Letters, vol. 10, no. 3, pp. 204-206, Mar. 2006.

[7] K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack," Proc. IEEE INFOCOM, 2001.

[8] Gong and K. Sarac, "A More Practical Approach for Single- Packet IP Traceback Using Packet Logging and Marking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1310- 1324, Oct. 2008.

[9] C. Snoeren et al., "Single-Packet IP Traceback," IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721-734,Dec.2002.

[10] D. Moore et al., "Inferring Internet Denial-of-Service Activity," ACM Trans. Computer Systems, vol. 24, no. 2, pp.115-139, May 2006.

[11] Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denial of Service Attacks," The Internet Protocol J., vol. 7, no. 4, pp. 13-35, 2004.