ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 2, February 2013

A Novel Approach to Reduce the Packet Pollution in Large Scale Network

S.Stewart Kirubakaran, D.Prabakar, Dr.S.Karthik

Abstract- **Distributed Denial of Service attacks (DDoS) is vulnerable to the internet. It is extremely hard to trace back the source of these attacks. Because of the vulnerability of the original design of the Internet, it's hard to find the actual hackers at present. In this paper, we propose a novel mechanism for IP Traceback using information theoretical parameters, and there is no packet marking in proposed strategy. Packet Pollutions are overcomed and it is also independent of attack traffic patterns. Our analysis, experiments, and simulations demonstrate that the proposed traceback mechanism is effective and efficient compared with the existing methods**

Index Terms: DDoS, IP Traceback, Local Flow Monitoring Algorithm

I. INTRODUCTION

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 these 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, we may not be able to find the actual hackers 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. Research on DDoS detection mitigation and filtering has been conducted pervasively [1][7]. However, the efforts on IP traceback are limited. 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.

S.Stewart Kirubakaran*, Assistant Professor, Dept of CSE, SNS College of Technology., Coimbatore , India.,.mobile.No : 9952556668*
D.Prabakar, *Assistant Professor, Dept of CSE, SNS College of Technology., Coimbatore, India.,mobile.No : 9942033952*
Dr.S.Karthik *Professor and Dean, Dept of CSE, SNS College of Technology., Coimbatore, India.,mobile.No : 9842720118*

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. IP traceback methods should be independent of packet pollution and various attack patterns. However, traffic patterns have no impact on the proposed scheme.

II BACKGROUND WORK

A. DDoS Attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. There are two categories of DDoS attacks, typical DDoS attacks and Distributed Reflection Denial-of-Service (DRDoS) attacks. In a typical DDoS attack, the master computer orders the zombies to run the attack tools to send huge volume of packets to the victim, to exhaust the victim's resources[9][6]. Unlike the typical DDoS attacks, the army of a DRDoS attack consists of master zombies, slave zombies, and reflectors. The difference in this type of attack is that slave zombies are led by master zombies to send a stream of packets with the victim's IP address as the source IP address to other uninfected machines (known as reflectors), exhorting these machines to connect with the victim. Then the reflectors send the victim a great volume of traffic, as a reply to its exhortation for the opening of a new connection, because they believe that the victim was the host that asked for it.

B. IP Traceback

IP traceback means the capability of identifying the actual source of any packet sent across the Internet[3]. IP traceback methods should be independent from packet pollution and various attack patterns. Entropy rate, the entropy growth rate as the length of a stochastic sequence

increases, was employed to find the similarity between two flows on the entropy growth pattern.

The next step for the attacker is to install new programs (known as attack tools) 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. Numerous zombies together form an army or botnet.

III SYSTEM MODELING

A. A Sample Network with DDoS Attacks

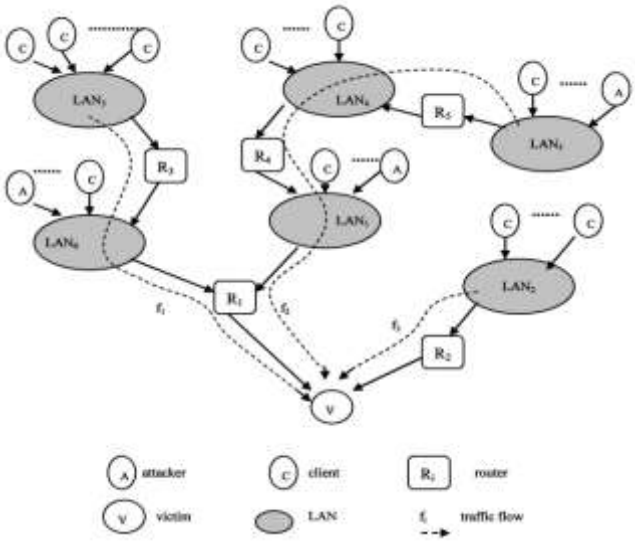

Fig 1.A Sample Network with DDoS Attack

In a DDoS attack scenario, as shown in Fig. 1, the flows with destination as the victim include legitimate flows, such as f3, and a combination of attack flows and legitimate flows, such as f1 and f2. Compared with nonattack cases, the volumes of some flows increase significantly in a very short time period in DDoS attack cases. Observers at routers R1, R4, R5, and V will notice the dramatic changes; however, the routers who are not in the attack paths, such as R2 and R3, will not be able to sense the variations. Therefore, once the victim realizes an ongoing attack, it can pushback to the LANs, which caused the changes based on the information of flow entropy variations, and therefore, we can identify the locations of attackers [8].

The traceback can be done in a parallel and distributed fashion in our proposed scheme. In Fig. 1, based on its knowledge of entropy variations, the victim knows that attackers are somewhere behind router R1, and no attackers are behind router R2. Then the traceback request is delivered to router R1. Similar to the victim, router R1 knows that there are two groups of attackers, one group is behind the link to LAN0 and another group is behind the link to LAN1. Then the traceback requests are further delivered to the edge routers of LAN0 and LAN1, respectively. Based on entropy variation information of router R3, the edge router of LAN0 can infer that the attackers are located in the local area network, LAN0. Similarly, the edge router of LAN1 finds that there are attackers in LAN1; furthermore, there are attackers behind router R4.

The traceback request is then further passed to the upstream routers, until we locate the attackers in LAN5.

B. Proposed Work

A flow is defined by a pair—the upstream router where the packet came from and the destination address of the packet. Entropy is an information theoretic concept, which is a measure of randomness. We employ entropy variation in this paper to measure changes of randomness of flows at a router for a given time interval. We notice that entropy variation is only one of the possible metrics. Chen and Hwang used a statistical feature, change point of flows, to identify the abnormality of DDoS attacks [6]; however, attackers could cheat this feature by increasing attack strength slowly. We can also employ other statistic metrics to measure the randomness, such as standard variation or high-order moments of flows. We choose entropy variation rather than others in this paper because of the low computing workload for entropy variations.

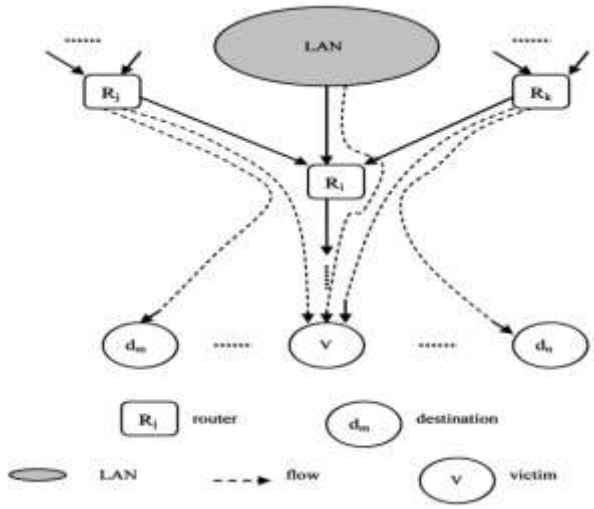

Fig. 2 Traffic flows at a router on an attack path

First, let us have a close investigation on the flows of a router, as shown in Fig. 2. Generally, a router knows its local topology, e.g., its upstream routers, the local area network attached to the router, and the downstream routers. We name the router that we are investigating now as a local router. In the rest of the paper, we use I as the set of positive integers, and R as the set of real numbers. We denote a flow on a local router by <ui; dj; t>; i; j 2 I; t 2 R, where ui is an upstream router of a local router Ri, dj is the destination address of a group of packets that are passing through the local router Ri, and t is the current time stamp.

For example, the local router Ri in Fig. 2 has two different incoming flows—the ones from the upstream routers Rj and Rk, respectively. We name this kind of flows as transit flows. Another type of incoming flows of the local router Ri is generated at the local area network; we call these local flows, and we use L to represent the local flows.

We name all the incoming flows as input flows, and all the flows leaving router Ri are named as output flows [10]. We denote ui; i 2 I as the immediate upstream routers of the local router Ri, and set U as the set of incoming flows of router Ri. We use a setD ¼ fdi; i 2 Ig to represent the destinations of the packets that are passing through the local router Ri. If v is the victim router, then v 2 D. Therefore, a flow at a local router can be defined as follows:

$$f_{ij}(u_i, {}_{dj}) = \{< u_i, d_j, t> | u_i \in U, d_j \in D, i, j \in I\}.$$

We denote $| f_{ij}(u_i,d_j,t)|$ as the count number of packets of the flow fij at time t. For a given time interval _T, we define the variation of the number of packets for a given flow as follows:

$$Nij(ui,dj,t+\Delta T)=|fij(ui,dj,t+\Delta T)|-|fij(ui,dj,t)$$

Based on the large number theorem, we have the probability of each flow at a local router as follows:

$$pij(ui,dj) = \frac{Nij(ui,dj)}{\sum_{i=1}^{\infty}\sum_{j=1}^{\infty} N_{ij(ui,dj)}}$$

Let F be the random variable of the number of flows during the time interval ΔT on a local router, therefore, we define the entropy of flows for the local router as follows:

$$H(F) = -\sum_{ij} pij(ui,dj)\log pij(ui,dj)$$

In order to differentiate from the original definition of entropy, we call H(F) as entropy variation in this paper, which measures the variations of randomness of flows on a given local router.

C. Analysis of Entropy-Variation Based Traceback Model

We assume the following:

1. There is no extraordinary change of network traffic in a very short time interval.
2. The number of packets is at least an order of magnitude higher than that of normal flows.
3. Only one DDoS attack is ongoing at a given time.
4. The number of flows for a given router is stable at both the attack cases and nonattack cases.

IV CONCLUSION

It is a fundamentally different traceback mechanism from the currently adopted packet marking strategies. Many of the available work on IP traceback depend on packet marking, either 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 hackers and extraordinary challenge on storage space at victims or intermediate routers. On the other hand, the proposed method needs no marking on packets, and therefore, avoids the inherent shortcomings of packet marking mechanisms. It employs the features that are out of the control of hackers to conduct IP traceback. We observe and store short-term information of flow entropy variations at routers. Moreover, the proposed model can work as an independent software module with current routing software.

ACKNOWLEDGMENT

Our Sincere thanks to the Dean Professor.Dr.S.Karthik, his valuable suggestion and thoughts is motivated to publish this paper and our beloved HOD Dr.T.Kalaikumaran, of our department of computer science and engineering, his excellence and suggestion is very useful towards this paper.

REFERENCES

[1] "IP Flow-Based Technology," ArborNetworks, http://www.arbornetworks.com, 2010.

[2] C. Patrikakis, M. Masikos, and O. Zouraraki, "Distributed denial of Service Attacks," The Internet Protocol J., vol. 7, no. 4, pp. 13-35, 2011.

[3] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network- Based Defense Mechanisms Countering the DoS and DDoS Problems," ACM computing Surveys, vol. 39,no.1, p. 3, 2012.

[4] R.R. Kompella, S. Singh, and G. Varghese, "On Scalable Attack Detection in the Network," IEEE/ACM Trans. Networking, vol. 15, no. 1, pp. 14-25, Feb. 2010.

[5] Z. Duan, X. Yuan, and J. Chandrashekar, "Controlling IP Spoofing through Interdomain Packet Filters," IEEE Trans.Dependable and Secure Computing, vol. 5, no. 1, pp. 22-36,Jan.-Mar. 2009.

[6] M.T. Goodrich, "Probabilistic Packet Marking for Large Scale IP Traceback," IEEE/ACM Trans. Networking, vol.16, no. 1, pp. 15-24, Feb. 2012.

[7] 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. 2011.

[8] H. Aljifri, "IP Traceback: A New Denial-of-Service Deterrent?" IEEE Security & Privacy, vol. 1, no. 3, pp. 24-31, May/June 2011.

[9] P.E. Ayres et al., "ALPi: A DDoS Defense System for High-Speed Networks," IEEE J. Selected Areas Comm., vol. 24, no. 10, pp. 1864- 1876, Oct. 2010.

[10] R. Chen, J. Park, and R. Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks," IEEE Trans. Paralle and Distributed Systems, vol. 18, no. 5, pp. 577- 588, May 2009.

S.Stewart Kirubakaran, received B.Tech Degree in Information Technology from the Anna University, Chennai, and Master's Degree in Information Technology in kalasalingam University,India. At present, He is an Assistant Professor of Computer Science and Engineering in SNS College of Technology, Coimbatore. His research interest focuses on Wireless Networks and Network Security.

PRABAKAR.D, received B.E Degree in Computer Science and Engineering from the Anna University, Chennai, in 2004 and Master's Degree in Computer Science and Engineering in Anna University of Technology, Coimbatore, in 2008. At present, He is an Assistant Professor of Computer Science and Engineering in SNS College of Technology, Coimbatore. His research interest focuses on Wireless Communication, Mobile Computing and Wireless Sensor Networks.

Dr.S.Karthik, is presently professor & Dean in the department of computer science and engineering, SNS College of Technology, affiliated to Anna University- Coimbatore, Tamilnadu, India. He received the M.E. degree from Anna University-Chennai and Ph.D. degree from Anna University of Technology, Coimbatore. His research interests include Network security, web services and wireless systems. In particular, he is currently working in a research group developing new Internet Security architectures and active defense systems against DDoS attacks. Dr.S.Karthik published more than 35 papers in refereed international journals and 25 papers in Conferences and has been involved many international conferences as Technical chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.