International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-116 PAGE NO: 672-678.

DDoS: Inspect the Different Trace back Techniques

[1#]M.Padmavathy, M.Sc (CS)., M.Phil.,
Research Scholar, Department of Computer Applications,
School of Information Technology, Madurai Kamaraj University,
Palkalainagar, Madurai – 625021.
E-Mail: padmaphd1@gmail.com

[2#]Dr.M.Ramakrishnan, M.E., Ph.D., Ph.D.
Professor and Head Department of Computer Application
Chairperson - School of Information Technology Madurai Kamaraj University
Madurai – 625 021.

Abstract—
Distributed Denial of Service (DDoS) is the significant hardest threats in internet security. These attacks are typically explicit attempts to disrupt legitimate user access services. So it is a necessary obsession to protect the resource and trace from the DDoS attack. But it was very tricky to discriminate normal traffic due to its identities and origins hiding. Developing a broad resistance mechanism against identified and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention. This paper discussed some of the mostly used predicting trace back techniques to solve the issues raised by DDoS attacks. In this paper it also asses the different trace back techniques which are provide effective, efficient detection of such attacks.

Key Words: Network Security, DDoS attacks, Trace back methods, Botnets, Flooding attack.

1. INTRODUCTION

Today's all works are depend on internet processing, so the attacks against network resources are common in the world. Basically attacks are commenced in variety of reasons like monetary gain, fraud, warfare and to gain an economic advantage (7). Attacks are directly compromise the networks and its resources confidentiality, integrity and availability. In networks and resources the attacks are fall into four general categories such as, Modification attack, Repudiation attack, Denial of service attack and access attacks. Denial-of-service (DoS) attacks are hardest problem in networks throughout its processing (12). The impact of DoS attacks is more serious due to their targeted action. In a distributed DoS (DDoS) attack, the attacker uses a number of compromised slaves to increase the transmission power coordinated flooding attack (1).

In DoS attacks, the packets are routed correctly but the destination is becomes the target of the attackers. It will be classified into two type's namely ordinary and distributed DoS attacks (12). In an ordinary network based denial of service attack, an attacker uses a tool to send packets to the target system. In the DDoS attacks, there might still be a single packets, but the effect of the attacks is multiple by use of attack servers. The attack not only disables that server but denies access to legitimate user (7). To find the DoS attacks

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-116 PAGE NO: 672-678.

activity in the internet is very difficult and complicated one. The major difficulty against DDoS is that attackers often use fake, or spoofed IP addresses as the IP source address. So the attackers can easily distinguish themselves as some other hosts on the internet. In the stateless nature of the internet, it is not an easy task to determine/trace the source of these attacker's packets and their location. This is actually known as IP Traceback problem (8).

The rest of the paper is structure as follows, section 1 provide today's internet attacks issues and its basic information's. Section 2 embraces the various existing papers which are based on DDoS IP Traceback methods. It is followed by section 3 includes the Traceback methods classification it include two types of classification and the Traceback method evaluation is also provided in this section. The next section 4 contains the detailed survey of various Traceback mechanisms and also this section asses the comparative analysis of this various mechanisms. Finally section 5 brings to a close with conclusion of the Distributed Denial of Service (DDoS) IP Traceback techniques and the future implementation idea.

2. RELATED WORK

In 2015, G.Florance (4) briefly describes various IP Traceback techniques of DDoS survey to provide the better solution of the attacks. The author also discusses possible attacks in a collaborative environment and their impacts are identified of which denial of service is a serious threat. There are many Traceback methods are available to identify the attacks. The real challenge in security provisioning is to identify the source of unknown attack at the earliest possible which motivated us to work on novel fast Traceback mechanism with less computation and storage costs, scalability to high attacker population, and providing best network performance.

In 2015, Amruta Kokate and Prof.Pramod Patil (2) have analyzed different techniques to get and identify the origin of DDoS attack with the help of IP Traceback. The most famous techniques in finding the attack source are the IP Traceback. In this paper it contains and evaluates some of the existing and recently evolving IP Traceback techniques with respect to their advantages and disadvantages. Through this paper they can analyze different techniques through which to detect man-in-the-middle attack and spoofing attack. The author's comparison of these paper methods is made based on complexity and efficiency.

In 2013, Saman Taghavi Zargar and James Joshi et al. (11) have discovered the scope of the DDoS flooding attack problem and attempts to conflict it. The authors categorize the DDoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DDoS flooding attacks. In this paper, they have presented a comprehensive classification of various DDoS defense mechanisms along with their advantages and disadvantages based on where and when they detect and respond to DDoS flooding attacks. An ideal comprehensive DDoS defense mechanism must have specific features to combat DDoS flooding attacks both in real-time and as close as possible to the attack sources.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-116 PAGE NO: 672-678.

In 2009, A.John and T Sivakumar (6) discussed some of the mostly used predicting Traceback techniques which are used to solve the problem of DDoS attacks. The author says their main goal is to appraise the different Traceback techniques of the DDoS. This paper also evaluates various Traceback methods of the classification. The authors present a detailed survey of different Distributed Denial of Service Traceback mechanisms in this paper. It is also describes about two ways of classification such as preventive and reactive. The comparing Traceback mechanism by considering different categories such as compatibility, implementation, router overhead, Postmortem Capability, Classification, Network overhead, network Topology and Application.

3. TRACEBACK METHOD CLASSIFICATION

In IP Traceback methods it provides the victim's network administrators with the ability to identify the address of the true source of the packets causing DDoS. It is the vital for restoring normal network functionality as quickly as possible, preventing reoccurrences and holding the attackers (10). Basically a number of IP Traceback approaches are available to identify the attackers importantly preventive and reactive.

Reactive Method:

In reactive method (5) it initiates the Traceback process in response to an attack. They must be completed while the attack is active. If the attack is not active this mechanism cannot be worked.

This method is also referred as source based mechanism. Reactive methods are more effective for controlled networks then for the internet. The reactive methods solutions aim at identifying the source of the attacks. This is very important because attackers spoof their addresses, thus techniques are needed to trace back to the source to the source of the attack.

Preventive Method:

It takes precautionary steps in preventing DDoS attacks. This method (5) also referred as destination based mechanism. It record tracing information as packets are routed through the network. Simple examples of preventive methods are log based Traceback, FDPM Traceback, TBPM Traceback, traffic filtering, packet marking and filtering, distributed link list Traceback(DLLT), probabilistic pipelined packet marking(PPPM), Deterministic packet marking(DPM) and entropy variation.

3.1. Traceback Methods Evaluation

The evaluation is the main thing on analyzes a paper, because of the evaluation is the only thing to find out the appropriate solution on any methods. This section Traceback methods evaluation provides a current state of the art approaches to IP Traceback and evaluates them against the ideal system. The overview of ideal Traceback system is as follows,

1. Classification based Evaluation
2. High level protection
3. Network overhead based Evaluation
4. Router overhead based Evaluation

Classification based evaluation methods is depend upon the reactive and preventive Traceback methods. High level protection is the protective mechanism which is depends on the destination level. Network overhead based evaluation represents the level of protection on networks against spoof attacks.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-116 PAGE NO: 672-678.

4. DIFFERENT TRACEBACK METHODS

This section fully contributes various Traceback methods which are used to rectify the attacks in DDoS. A variety of Traceback methods are as follows (3),

1. Ingress Filtering:

When we want to find the anonymous attack, the better way is to eliminate the ability to fake source addresses. Ingress filtering is one of this approach is to configure routers block packets that arrive with illegal source addresses. This processing requires a router with sufficient power to examine the source addresses of every packet and sufficient knowledge to differentiate between the legal and illegal addresses.

2. Link Testing:

In link testing methods it contains two various types such as, Input Debugging and Controlled Flooding.

a. Input Debugging

It allows an operator to filter particular packets on some outlet port and determine which ingress port they arrived on. This capability is enough to implement a trace.

b. Controlled Flooding

Control flooding (9) it tests links by flooding them with large bursts of traffic and observing how this perturbs traffic from the attacker.

3. Logging:

Logging approach is to lag packets at key routers and then use data mining techniques to determine the path that the packets traversed.

4. ICMP Traceback:

Internet Control Message Protocol (ICMP) in need of trace out full path of the attacks. The principle idea in this schemes is for every router to sample with low probability (e.g.,1/20000) and generate an ICMP Traceback message or i-Trace directed to the same destination as the selected packet.

5. Packet Marking Algorithm:

In Packet Marking Algorithm (13) schemes, each router in addition to forwarding a packet also inserts a mark in the packet. This mark is a unique identifier corresponding to this particular router. As a result the victim can determine all the intermediate hops for each packet by observing the inserted marks.

6. FDPM Traceback:

Flexible Deterministic Packet Marking (FDPM) is falls into the packet marking categories. It is optimized version of DPM. In FDPM schemes, the Types of Services (ToS) fields will be used to store the mark under some circumferences. The two fields in the IP header are exploited, one is fragment ID and other is Reversed flag.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-116 PAGE NO: 672-678.

4.1 Comparison of the Different Traceback methods

Categories	Ingress Filtering	Link Testing	Logging	ICMP Traceback	Packet Matching Algorithm	FDPM Traceback
Compatibility	Moderate	High/Low	High	Low	Low	Moderate
Router Overhead	Moderate	Low/High	Low	High	Low	Low
Classification	Preventive	Reactive	Reactive	Reactive	Reactive	Reactive
Network Topology	No	No	No	Yes	Yes	No
Applications	DDoS	DDoS	DDoS others	DDoS others	DDoS	DDoS

The comparison of different Traceback methods is listed as the above table. It has various categories to evaluate the method like Compatibility, Router overhead, Classification, Network Topology and the used applications.

5. CONCLUSION

In internet security considerations Distributed Denial of Service (DDoS) is the main attack to destroy and terminate the processing. So the attack resolver is the main thing to overcome these issues. In this paper the detailed survey of Distributed Denial of Service (DDoS) Traceback mechanisms are discussed. The classification of the Traceback techniques is also refereed in this paper. This paper conferred some of mostly using Traceback methods to solve the attack issues raised by Distributed Denial of Service (DDoS). The comparative study in this paper is used to evaluate the various methods to select the good and better technique to rectify the problems. In future, the implementation of the entire processing is provided on further works and gives a better solution in later.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-116 PAGE NO: 672-678.

References

1. R. Alshammari, and A. N. Zincir-Heywood, "Can Encrypted Traffic be identified without Port Numbers, IP Addresses and Payload Inspection?" Journal of Computer Networks, Elsevier, 2011.
2. Amruta Kokate and Prof.Pramod Patil, A Survey on Different IP Traceback Techniques for finding The Location of Spoofers", International Journal Of Engineering And Computer Science ISSN: 2319-7242, Volume 4 Issue 12 Dec 2015, Page No. 15132-15135.
3. A-Duwairi and M. Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback," IEEE Trans. Parallel and Distributed Systems, vol. 17, no. 5, May 2006, pp. 403- 418.
4. G.Florance, "Survey of IP Traceback Methods in Distributed Denial of Service (DDoS) Attacks", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 7, July 2015.
5. Hakem Beitollahi, Geert Deconinck: Analyzing Well-known Countermeasures against Distributed Denial of Service Attacks, Computer Comm., Vol. 35, 2012, pp. 1312-1332.
6. A.John and T Sivakumar, "DDoS: Survey of Traceback Methods", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009, pp. 241-245.
7. H. I. Liu, and K. C. Chang, Defending systems Against Tilt DDoS attacks, Telecommunication Systems, Services, and Applications (TSSA), October 20-21, 2011, pp. 22-27.
8. X. Liu, X. Yang, and Y. Lu, "To filter or to authorize: network-layer DoS defense against multimillion-node botnets", in Proc. of the ACM SIGCOMM conference on Data communication (SIGCOMM '08), NY, USA, 2008, pp. 195-206.
9. R. M. Mutebi, and I. A. Rai, "An Integrated Victim-based Approach against IP Packet Flooding Denial of Service", International Journal of Computing and ICT Research, Special Issue Vol. 4, No. 1, October 2010, pp. 70-80.
10. M. Naveed, S. Un Nihar, and M. Inayatullah Babar, "Network Intrusion Prevention by Configuring ACLs on the Routers, based on Snort IDS Alerts," Proc. of 6th Intl' Conference.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
www.ijcsjournal.com Volume 4, Issue 2, No 1, 2016. ISSN: 2348-6600
Reference ID: IJCS-116 PAGE NO: 672-678.

11. Saman Taghavi Zargar and James Joshi et al., "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, published online Feb. 2013, pp. 1-24.
12. Thomas Dubendorfer, Matthias Bossardt, Bernhard Plattner, "Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation", Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 17 - Volume 18, 2005.
13. D. K. Yau, J. C. Lui, and F. Liang, "Defending against Distributed Denial-of-Service Attacks with Max-min Fair Server-centric Router Throttles", In *Proc. of IEEE IWQoS*, May 2002.