ISSN : 2231-0711

Review on DDoS Attack Traceback Mechanism in MANET

Shinde Sandeep A.[#1], Dr. Bakal J. W.*[2]

[#]Dept. of Information Technology,
Pillais Institute of Information Technology, Mumbai University, India
[1]shinde.sa@gmail.com

*Principal, S.S. Jondhale College of Engineering,
Dombivali-west, Mumbai University, India
[2]bakaljw@gmail.com

***Abstract*— Mobile ad-hoc network is a collection of node which is self-configuring, decentralized, frameworkless mobile network. Due to open nature of the network it is easily vulnerable to various attacks. The major security threat on MANET is a DDoS attack. DDoS attack has the ability to create huge amount of unwanted traffic. Due to this the authorized user cannot utilized the resources properly. It is very hard to detect and control the DDoS attack due to large scale and complex network environments. The packet marking technique is not feasible because to it consume more memory and poor measurability. In this paper, we use local flow monitoring for detecting DDoS attack based on entropy variation.**

Index Term- MANET, DDoS, Flow Monitoring

I. Introduction

Mobile Ad-hoc Network is a self-configuring infrastructureless network of mobile device which is connected through wireless. In mobile ad-hoc network each node is free to move independently in any direction and will therefore change in it's like with other node changes frequently. Security of Mobile Ad hoc Networks (MANETs) has been a lot of scope in the research community. Due to open nature of network, dynamic changing topology MANET is easily vulnerable to various attacks. In addition, other issues also contribute to its vulnerability, such as the open architecture, shared radio channels, and limited resources, etc. Without a clear network boundary, it is extremely difficult to develop and

understand ad hoc security strategy for MANETs. Currently, MANETs are infected with a various attacks including impersonation, message distortion, eavesdropping, Denial-of-Service (DoS), and Distributed DoS (DDoS) [1].

Denial of Service (DoS) attacks, which are intended at trying to prevent authorized users from accessing or utilizing various network resources, have been known to the network research community since the early 1980s. In the summer of 1999, the Computer Incident Advisory Capability (CIAC) reported the first Distributed DoS (DDoS) attack incident and most of the DoS attacks since then have been distributed in nature [2].

Now days, DDoS threats are often launched by a network of remotely controlled, well organized, and widely distributed Zombies or compromised computers that are continuously sending a huge amount of data or requests packets to the victim system. Due to this victim system either grows slowly or crashes completely [3]. Zombies or compromised computers that are a part of a botnet network are usually assigned through the use of worms, Trojan horses or backdoors. Using the resources of compromised computers to perform DDoS attacks allows attackers to launch a huge amount of attack. It is very hard to detect and control the DDoS attack due to large scale and complex network environments [4].

The rest of paper is organized as follows, Section II, provides overview of DDoS attack in MANET. In section III, we discuss related DDoS detection techniques. In Section IV, we present proposed defense framework against DDoS attack in MANET. Finally Section V provides summery of the paper.

II. Overview Of Ddos Attack In Manet

A DDoS attack is a distributed, large-scale attempt by malicious users to flood the targeted network with a large number of packets. This consumes the victim network resources such as bandwidth, battery power, computing power, etc., which results in victim is unable to access services and network performance is greatly degraded [4],[5]

In DDoS attack, the attacker discovers insecure machine connected in network. It discovered machine is infected with attack code then the infected machine can further be utilized to discover and infect another machine in network and so on. The attacker thus slowly prepares an attack network called botnet depending on attacking code compromised machine called zombies. Attacker sends control instructions to master, which in turn controls the zombies. The zombies under the control of master/handler , transmit attack packet to victim. DDoS attack basically target victims computational or communication resources such as bandwidth, battery power, memory, CPU cycle, buffer, computational power etc.

III. Related Work

A. IP Attributes-based DDoS Detection:

Abnormal changes in the mobile network can be found out by considering variations in a number of IP attributes, e.g. source IP address [6], TTL [7], and the combination of multiple attributes [8]. TTL is used by Jung et al. for the analysis of Internet Website load performance [9]. A DDoS attack usually saturate network and changes value of the TTL attribute in traffic. Based on this idea, Taped et al. [7]. In these scheme a TTL-based statistical model to detect attack traffic generated by DDoS attacks. The performance is not normal level it affect the changes in final TTL value cannot reflect the anomalous changes in the traffic topology directly.

In our distance-based techniques, they use TTL to compute distance value. In [8], Kim et al. make a baseline profile on a number of attribute combinations, such as IP protocol-type and packet-size, source IP prefix and TTL values, as well as server port number and protocol-type, etc However, these scheme cannot improve overall network performance if the combined attributes are not related with the anomalous changes created by the DDoS attacks.

B. IP traceback mechanism:

There are three basic methods Ingress filtering, Packet logging, Packet marking.

Ingress filtering: It is dictates that each router should know the IP address space that each router's local interface is serving. When a packet arrives to the router's ingress interface it should have a valid IP address or it is dropped [10]. Packet logging, the routers keep logs regarding the packets that pass through them. With the help of those logs, recent packet can be traceback can be to its original source. Router is required to keep considerable amount of information especially in high bandwidth network. The memory overhead can be reduced by storing only a digest of packet's header, Global deployment is also an issue in this method [11] [12].

C. Packet Marking

In packet marking, the routers overload parts of the IP header of the traversing packet in order to put a marking that notified the recipient of the packet of their presence on the route [11]. The recipient gathers those marking and rebuilds the complete path that this packet traversed. Packet marking method has two types probabilistic packet marking and deterministic packet marking. In probabilistic packet marking perform once every n packet. This reduces the computational overhead of the marking but increase the number of packet needed to reconstruct the path. In deterministic procedure is performed for each packet at edge routers only. This reduces the number of packet needed for path construction [12].

IV. Proposed Work

DDoS Detection Scheme using Local Flow Monitoring based on Entropy Variation

A simple mobile ad-hoc network with DDoS attack to demonstrate our proposed detection scheme. We here consider the packets that are passing through a router as a flow. Flow is a pair the upstream router where the packet comes from the destination address of the packet. Entropy is an information theoretic concept, which is a measure of randomness or variations. We use entropy variation to measure of changes of randomness or variation of flows at a router for a given time period. Once the victim realizes an ongoing attack, it can push back to the networks, which caused the abnormal changes based on the information of flow entropy variations, and therefore, we can trace the locations of attackers [13].

In this scheme we calculate threshold (local threshold parameter δ) by differentiating current flow probability distribution, entropy distribution and according calculate the mean and the changes threshold value for next flow many times it wastes resources or over exceeds by threshold value considering only current flow.

To overcome this drawback it is important to consider current differences i.e. current probability distribution, cumulative distribution of all the flow and best probability distribution between the flows i.e. called as recommended probability distribution. Compare all these three probability distributions and according decide threshold for the next flow.

V. Conclusion

As the use of MANETs increases, the security becomes is a critical issue. In this paper, we have discussed the DDoS attacks in MANET and related DDoS detection techniques. We have also present proposed defense framework against DDoS attack in MANET. We use local flow monitoring for detecting DDoS attack based on entropy variation. We expect to improve the false positive rate. It's concluded that among all network attacks, DDoS and flooding attacks are the most harmful threats to network functionality and MANETs are even more vulnerable to those attacks.

References

[1] Minda Xiang, Yu Chen, Wei-Shinn Ku, Zhou Su, "Mitigating DDoS Attacks using Protection Nodes in Mobile Ad Hoc networks" Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , DEC. 5 - 9, 2011.

[2] P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

[3] R. K. C. Chang, Defending against flooding-based distributed denial of service attacks: A tutorial, Computer J. IEEE Commun. Magazine,Vol. 40, no. 10, pp. 42-51, 2002.

[4] CERT, Denial of Service Attacks, June 4, 2001[online], http://www.cert.org/tech tips/denial of service.html

[5] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state of the art,"Computer Journal of Networks, vol. 44, no. 5,pp. 643-666,Apr.2004.

[6] T. Peng, C. Leckie, and R. Kotagiri, “Proactively detecting DDoS attack using source ip address monitoring,” in Proceedings of the Third International IFIP-TC6 Networking Conference, 2004, pp.771–782.

[7] R. R. Talpade,G. Kim, and S. Khurana, “Nomad: traffic based network monitoring framework for anomaly detection,” in the Fourth IEEE Symposium on Computers and Communications, 1999, pp. 442–451

[8] Y Kim,J.-Y. Jo, and K. K. Suh, “Baseline profile stability for network anomaly detection,” in Proceedings of the 3rd International Conference on Information Technology: New Generations, 2006, pp. 720–725.

[9] J. Jung, A.Berger,and H Balakrishnan, “Modeling TTL-based internet caches,” in Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, 2003, pp. 417–426.

[10] Ping Du Nict,Tokyo, Japan Nakao A. “DDoS Defense Deployment with Network Egress and Ingress Filtering” in Communication (ICC), 2010 IEEE International Conference, 23-27 May 2010.

[11] Chao Gong, Sarac,K. "IP traceback based on packet marking and logging" Communications 2005. IEEE International Conference 2005 page 1042-1047.

[12] Chao Gong, Sarac, K.“A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking” Parallel and Distributed Systems, IEEE Transactions, Page 1310-1324.

[13] Shui Yu and Wanlei Zhou, “Traceback of DDoS Attacks Using Entropy Variations”, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 3, March 2011.