A Study on detection of DDoS Attack in MANET

Priyanka[1], Professor Nasib Singh Gill[2]

[1]M.Tech (CSE), MDU Main Campus, Rohtak

[2]HOD, Dept. Of Computer Science and Application, MDU Main Campus, Rohtak

ABSTRACT: Mobile ad-hoc network is a assortment of autonomous node which is self-directed , decentralized, framework less mobile network. Because of their openness of the network it is easily exposed to various attacks. Today in MANET the main issue is of security from DDoS attack. DDoS attack make the congestion in the network traffic due to which the performance of network goes down. Because of this formal user cannot make the most use of the resources properly. MANET is use at a large scale due to their ease of use and complex environment, it is hard to detect and control the DDoS attack . The packet marking technique is not feasible because to it consume more memory and poor Measurability. In this paper, we use local flow tracking for detecting DDoS attack based on entropy variation

Keywords: MANET, DDoS, Flow Monitoring

I. INTRODUCTION

Mobile Ad-hoc Network is a self-shaped infrastructure less network of mobile device in which wire is not a medium for connection. 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. In research world security of manet has a large scope. Due to openness of network, vigorous changing topology MANET is easily susceptible to various attacks. In addition, other issues also contribute to its susceptibility, such as the open architecture, shared radio channels, and limited resources, etc. Without a sharp clearcut network boundary, it is much complicated to develop and understand ad hoc security strategy for MANETs. Currently, MANETs are contaminated with a various attacks including impersonation, message distortion, eavesdropping, Denial-of-Service (DoS), and Distributed DoS (DDoS) . Denial of Service (DoS) attacks, which are planned to prevent authorized users from admittance or employing various network resources, have been known to the network research community since the early 1980s. In mid 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. Now days, DDoS threats are often commence by a network of remotely controlled, well stabled , and widely distributed Zombies or concessional computers that are constantly sending a large amount of data or requests packets to the fatality system. Due to this, fatality system either grows slowly or ends up completely. Zombies or computers which are the parts of a bonnets 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]. Further the 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 scattered, large-scale challenged by malicious users to deluge the intentional network with a large number of packets. This consumes the suffered network resources such as bandwidth, battery power, computing power, etc., which results in suffered system is unable to access the provided services and network performance is greatly down. In DDoS attack, the attacker discovers unsafe machine connected in network. It discovered machine is impure with attack code then the impure machine can further be operate to discover and impure another machine in network and so on.

The attacker thus gradually 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 attack master, transmit attack packet to suffered system. DDoS attack basically target victim's 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:

When the number of IP attributes is changes then the remarkable changes in the mobile network can be found out e.g. source IP address, TTL, and the combination of multiple attributes. TTL is used by Jung et al. for the analysis of Internet Website load performance . A DDoS attack usually setup network and alter the value of the TTL attribute in traffic. On basis of this idea, Taped et al., designed 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 inconsistent 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 design could not increase overall network performance if the combined attributes are not related with the inconsistent changes created by the DDoS attacks.

B. IP traceback mechanism:

Ingress filtering, Packet logging, Packet marking these are the three basic method.

Ingress filtering: according to this each router must be familiar with the IP address space which is serve by the router's local interface. Then Whenever a packet comes to the router's ingress interface either it have a valid IP address or it is dropped [10]. Packet logging, the routers keep record related the packets that pass through them. With the help of those logs or records, recent packet can be trace back 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 consumption is also an issue in this method [11] [12].

C. Packet Marking

Savage et al suggest about packet marking, as they pass through routers through the internet. they suggest that the router mark the packet with either the router IP address or edge of the path that the packet follow to reach to the route. Packet marketing method can be define with two scheme probabilistic packet marking and deterministic packet marking. Procedure is done for all n packets in probabilistic packet marking. This condense the computational overhead of the marking but it will increase the number of packet which are require to reconstruct the path. In deterministic packet marking, procedure is execute for each packet at edge routers only. This moderate the number of packet needed for path creation.

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

comes from the destination address of the packet. Entropy is a measure of randomness or variations which is theoretic concept. We use entropy variation to measure of changes of randomness or variation of flows at a router for a given time period. Once the suffered 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 □) 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. CONCLUSIONS

As the use of MANETs increases, the security becomes critical issue. In this paper, we have discussed the DDoS attacks in MANET and related DDoS detection techniques.

We have also present proposed protection 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.

VI. REFERENCES

[1]. Lakshmi Santhanam, Anup Kumar, and Dharma P. Agrawal. "Taxonomy of IP traceback." Journal of Information Assurance and security 1, no. 2 (2006): 79-94.

[2]. Yanxin Wang, Smruti Ranjan Behera, Johnny Wong, Guy Helmer, Vasant Honavar, Les Miller, Robyn Lutz, and Mark Slagell. "Towards the automatic generation of mobile agents for distributed intrusion detection system." Journal of Systems and Software 79, no. 1 (2006): 1-14.

[3]. Paul Barford and Vinod Yegneswaran. "An inside look at botnets." In Malware Detection, pp. 171-191. Springer US, 2007.

[4]. Vrizlynn LL Thing, Morris Sloman, and Naranker Dulay. "Non-intrusive IP traceback for DDoS attacks." In Proceedings of the 2nd ACM symposium on Information, computer and communications security, pp. 371-373. ACM, 2007.

[5]. Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao. "Survey of network-based defense mechanisms countering the DoS and DDoS problems." ACM Computing Surveys (CSUR) 39, no. 1 (2007): 3.

[6]. Elias Athanasopoulos, Andreas Makridakis, Spyros Antonatos, Demetres Antoniades, Sotiris Ioannidis, Kostas G. Anagnostakis, and Evangelos P. Markatos. "Antisocial networks: Turning a social network into a botnet." In Information security, pp. 146-160. Springer Berlin Heidelberg, 2008.

[7]. Anjali Sardana and Ramesh C. Joshi. "Dual-Level Defense Framework for DDoS Attacked Network." International Journal of Computer Applications 1, no. 25 (2010).

[8]. Shelly Xiaonan,Wu and Wolfgang Banzhaf. "The use of computational intelligence in intrusion detection systems: A review." Applied Soft Computing 10, no. 1 (2010): 1-35.

[9]. Yang Xiang, Ke Li, and Wanlei Zhou. "Low-rate DDoS attacks detection and traceback by using new information metrics." Information Forensics and Security, IEEE Transactions on 6, no. 2 (2011): 426-437.

[10]. N. Jeyanthi and N. Ch Sriman Narayana Iyengar. "An Entropy Based Approach to Detect and Distinguish DDoS Attacks from flash Crowds in VoIP Networks." IJ Network Security 14, no. 5 (2012): 257-269.

[11]. Saman Taghavi Zargar, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." Communications Surveys & Tutorials, IEEE 15, no. 4 (2013): 2046-2069.

[12]. Shweta Tripathi, Brij Gupta, Ammar Almomani, Anupama Mishra, and Suresh Veluru. "Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks." (2013).

[13]. Huichen Dai, Yi Wang, Jindou Fan, and Bin Liu. "Mitigate ddos attacks in ndn by interest traceback." In Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on, pp. 381-386. IEEE, 2013.

[14]. Alberto Compagno, Mauro Conti, Paolo Gasti, and Gene Tsudik. "Poseidon: Mitigating interest flooding DDoS attacks in named data networking." In Local Computer Networks (LCN), 2013 IEEE 38th Conference on, pp. 630-638. IEEE, 2013.

[15]. Ho-Seok Kang, and Sung-Ryul Kim. "A new logging-based IP traceback approach using data mining techniques." Journal of Internet Services and Information Security 3, no. 3/4 (2013): 72-80.

[16]. Vahid Aghaei Foroushani and A. Nur Zincir-Heywood. "On evaluating IP traceback : a practical perspective." In Security and Privacy Workshops (SPW), 2013 IEEE, pp. 127-134. IEEE, 2013.

[17]. Yulong Wang and Rui Sun. "An IP-Traceback-based Packet filtering Scheme for Eliminating DDoS Attacks." Journal of Networks 9, no. 4 (2014): 874-881.

[18]. Madhav Kale and D. M. Choudhari. "DDOS Attack Detection Based on an Ensemble of Neural Classifier." IJCSNS 14, no. 7 (2014): 122.

[19]. Sonali Swetapadma Sahu and Manjusha Pandey. "Distributed Denial of Service Attacks: A Review." International Journal of Modern Education and Computer Science (IJMECS) 6, no. 1 (2014): 65