Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Deterministic Packet Marking for Detecting Distributed Denial of Service Attacks in MANETS

Vijay Bharti, Prof. Nasib Singh Gill
Dept of Computer Science and Applications
Maharshi Dayanand University,
Rohtak, Haryana, India

Abstract— A mobile ad hoc network (MANET) is a multi-hop, wireless, self-configuring network that can be formed without the need of any pre-established infrastructure or centralized administration. All nodes in the network act at the same time as hosts and packet-forwarding routers. Wireless links, node mobility and lack of central administration make MANETs far more vulnerable to security attacks than conventional networks. In denial of service attack rightful users are prevented from access to services or network resources. DoS attacks can be launched at any layer of the protocol stack causing physical jamming, disconnection, and malfunction of routing, transport and application protocols. The attacks become extremely dangerous and hard to prevent if a group of attackers coordinate in DoS. This type of attack is called distributed DoS (DDoS) attack. When a DDoS attack occurs in MANET, the attacker actually compromises a number of mobile nodes, which can follow diverse patterns and can have different speeds. Distributed denial-of-service (DDoS) in MANETS is a rapidly growing problem. The massive amount and variety of both the attacks and the resistance approaches is overwhelming. Distributed denial-of-service (DDoS) attacks pose an immense threat to the ad hoc networks, and many defense mechanisms have been proposed to combat the problem. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks.

Keywords— Mobile Ad- hoc networks, Denial of Service attacks, DPM, IP trackback

I. INTRODUCTION MOBILE ADHOC-NETWORKS (MANETS)

A Mobile Ad-hoc network (MANET) is an autonomous collection of mobile routers or nodes communicating above radio links. MANET is a passing network with no communications. The wireless routers or nodes move arbitrarily and categorize themselves randomly. The nodes directly communicate via wireless links within each other's radio variety, while so as to be distant apart use additional nodes as relay in a multi-hop steering purpose. As the nodes are mobile, the arrangement of the network changes dynamically and unpredictably over time. Ad-hoc networks are self-congaing and self-organizing, so to preserve message amid nodes in the network, each node behaves as a spreader, a crowd and a router. It is a sovereign system of mobile hosts connected by wireless links. There is no stationary infrastructure such as stand station. If two hosts are not within radio variety, every communication messages between them must pass through one or more intermediate hosts that act as routers. These hosts move around randomly, thus change the network topology with dynamism. Such networks are very useful in military and other tactical applications such as emergency rescue or searching missions, where axed network infrastructure is not available.

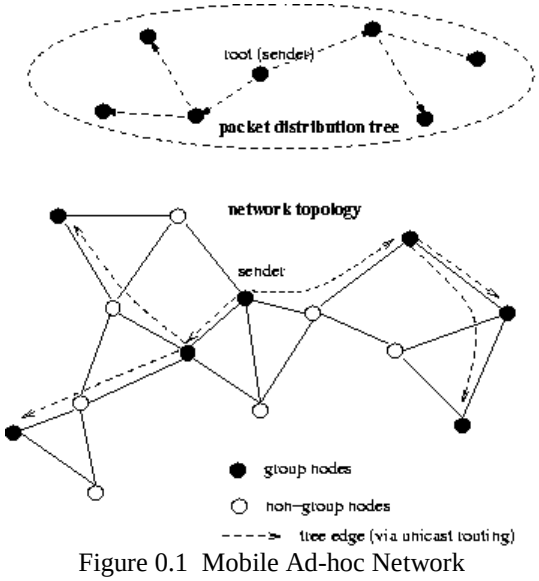


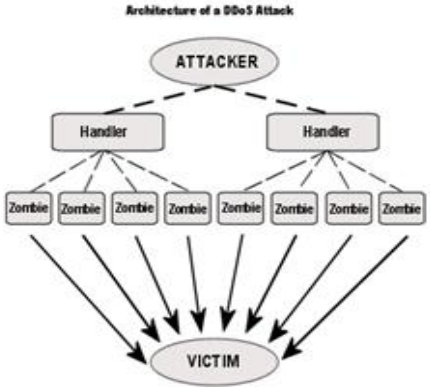
Figure 0.1 Mobile Ad-hoc Network

A MANET is required in situations where a fixed communication infrastructure, wireless or wired, does not exist or has been destroyed. A Mobile Ad hoc Network generally does not have any infrastructure and each mobile host also acts as a router. Communication between a variety of hosts takes place through wireless associations. Direct communication can take place between hosts that are within the communication range of the antennas of the respective hosts; if not, communication is achieved through multi-hop routing.

II. DDOS ATTACKS

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. DDoS attack are the greatest threat to network security in these days[1], in time detection of this attack is the main problem of DDoS attack, many other techniques and formulation has already been introduced to detect DDoS, but the problem still lies there. A smart attacker can penetrate the network by launching a DDoS attack as it doesn't have some common characteristics that can be classified as an attack. at present obtainable discovery systems like IDS can be beaten easily by such attackers.

Keeping this in mind, we have proposed a distributed approach to detect DDoS attack at intermediate network with some more deficient and accurate manner [2]. Many make use of Gossip[3] based scheme to multicast the information amongst the connected nodes within the network. If any of the connected node reports an abnormal behavior in the packet, this node will share this anomaly with all the nodes and in the end a decision is calculated to declare the packet as friendly or attack and secure the whole network from DDoS attack.



What is DoS Attack

A Denial of Service (DoS) is an attack with the purpose of thwart legitimate users from using a particular resource of network such as a website, web service, or computer system. If we look at the facts below, we can see just how much consumption of bandwidth can be in a simple enough attack [4].

A single attack consists of Magnitude of 25.000 bytes/sec or 24 KB/sec. or 192 Kbps. if we Assume N as number of attackers and N=100 attackers = 192×100 = 18.7 Mbps DoS attack

If we multiply these facts exponentially by the number of attackers, one can launch such an extensive attack with great impact**.** [5]

What is DDoS Attack

A Distributed Denial of Service (DDoS) is a co operational attack on the availability of services of a given target system or network that is indirectly launched through many compromised computing systems. The service or system which is directly under attack are called "primary victim" while the cooperated systems used to commence the attack are called the "secondary wounded or zombies". The employ of minor wounded in a DDoS assault - provides the attacker with the ability to launch a larger and more disruptive attack while remaining unidentified, since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker.

III. DDOS DETECTION WITH IP TRACEBACK

IP trackback is a term given to each method for reliably ascertaining the basis of a packet on the Internet. The datagram natural world of the Internet make it difficult to ascertain the initiating host of a packet, the basis id supplied in an IP packet can be falsified (IP spoofing) permitting for Denial of Service aggressions (DoS) or one-way aggressions whereas the reply from the victim host is so well recognized that revisit packets demand not be consented to tolerate the attack. The setback of ending the basis of a packet is shouted the IP trackback problem. IP Trackback is a critical skill for recognizing origins of aggressions and instituting protection measures for the Internet.

In DoS/DDoS attack, attacker uses fake source IP addresses to make tracing and stopping of DoS difficult. This technique is called IP spoofing. This technique involves the manipulation of the source IP address in the IP header of a transmitted packet. This gives the attacker a form of anonymity. It is difficult to solve problem of IP Spoofing because of lack of security features in TCP/IP specifications. Ingress altering,Use of cryptographic verification, IP trace back are of several different kind of the approach used to handle forged IP source addresses. The purpose of IP trackback is to identify the true IP address of a host originating assault packets. IP trace rear is crucial for rapidly restore normal network functionality and preventing reoccurrence.

We describe a more realistic topology for the Internet – that is composed of LANs with a connective boundary and attempt to put a single mark on inbound packets at the point of system way in. Their idea is to put, with chance likelihood of .5, the upper or lower half of the IP address of the ingress interface into the fragment id field of the package, advantage next set a reserve bit representative which portion of the address is contained in the piece field. By using this advance they maintain to be able to obtain 0 false positives with .99 probabilities after only 7 packets.

Another way is comparable in that they desire to use and encoded IP address of the input interface in the fragment id field of the packet. Whereas they differ from Blenny and A sari is that they desire to encode the IP address as a 16-bit hash of that IP address. Primarily they select a recognized hashing function. They state that there should be a little encounters if there were larger than 2^16 frontier routers acting the marking.

Authors have endeavored to mitigate the encounter setback by familiarizing a random distributed selection of a hash purpose from the universal set, and next requesting it to the IP address. In whichever hashing scenario, the basis address and the hash are mapped jointly in a table for afterward look-up alongside a bit indicating that serving of the address they have received. Across a complex procedure and a random hash selection, they are capable of cutting address crash. By employing a deterministic method they cut the period for their reconstruction procedure for their mark (the 16-bit hash). Though, by encoding that mark across hashing they familiarize the probability of encounters, and therefore false-positives.

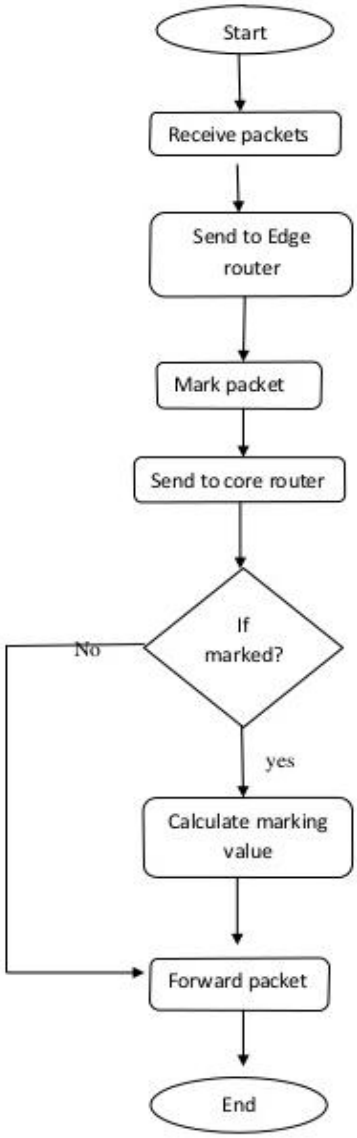


Figure 1.2 flow Chart for the proposed IP traceback technique

In vibrant marking it is probable to find the attack agents in a colossal scale DDoS network. In the box of a DDoS it enable the injured party to draw the attack one pace more back to the basis, to find a chief contraption or the real attacker alongside merely a insufficient numbers of packets. The counseled marking procedure increases the potential of DDoS attack detection at the victim across mark-based discovery. In the mark-based way, the discovery engine seizes into report the marks of the packets to recognize fluctuating origins of a solitary locale encompassed in a DDoS show aggression. This significantly increases the chance of detection. In order to gratify the end-to-end arguments way, fate-sharing and additionally respect to the demand for scalable and applicable schemes, merely frontier routers apply a easy marking procedure. The fairly negligible number of stay and bandwidth overhead added to the frontier routers make the DDPM implementable.

IV. RELATED WORK

The version of this What Every traceback approach try is to accurately identify the sources of attacking traffic but path re-construction algorithms in networks actually reveal identity of first router on the path. More suited approach would be to find an algorithm that can find the identity of first router without requiring the contribution of all the routers in the path. As the invader can forge any field in the IP header, he cannot forge.

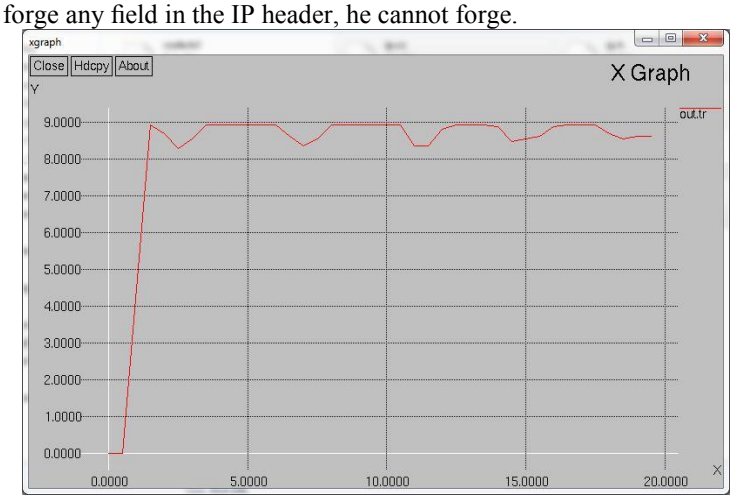


Figure 1.3 Overhead Caused by Zombies in the Network.

Table 5.4 and figure 5.2 show the effect of proposed prevention technique on Number of Collisions with different number of attackers and it also shows comparison with the existing prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. By using this technique number of collisions decreases as compared to the collisions of existing prevention scheme

Table 1.4: Effect of Proposed Prevention Technique on Throughput with varying number of attackers.

NUMBER OF ATTACKERS PER NETWORK	THROUGHPUT
3	1714653
4	1617242
5	1530967

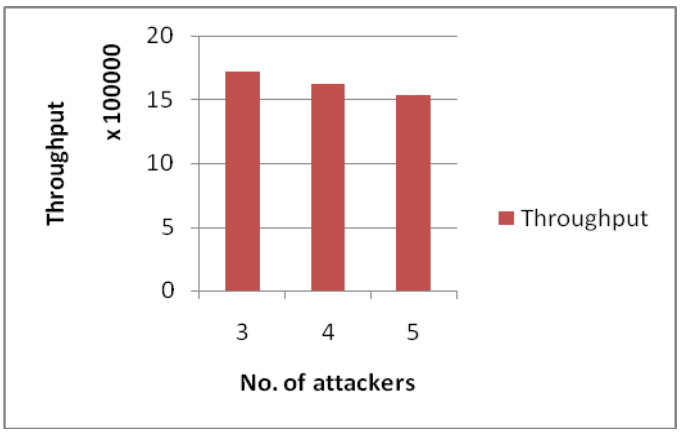


Figure 1.5: Effect of Proposed Prevention Technique on Throughput with varying number of attackers

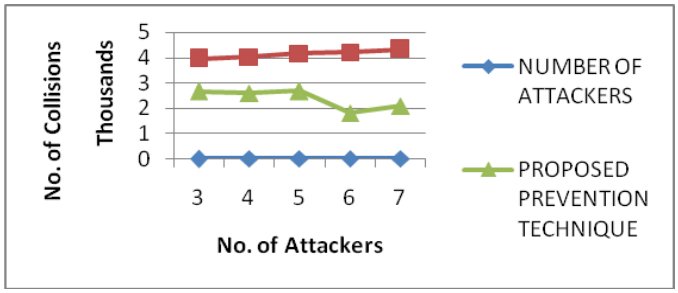


Figure 1.6: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers

V. CONCLUSION AND FUTURE SCOPE

In MANETs dandling DDoS attacks is quickly becoming more and more complex, and has reached the point where it is difficult to see zombies spread throughout network. On one hand, this hinders an understanding of the DDoS phenomenon. The variety of known attacks creates the impression that the problem space is vast, and hard to explore and address. For classifying attacks and defenses researchers needs a better understanding of the problem and the current solution space. The attack classification criteria in MANETS is even more difficult. After analyzing existing frameworks, we have found three types of DDOS frameworks: victim-end defense frameworks, source-end defense frameworks, and distributed defense frameworks. It is too late for victim-end defense frameworks to respond to DDOS attacks. A source-end defense framework cannot achieve good performance due to lack of attack information. In contrast, a distributed framework can achieve better performance by cooperating among distributed multiple defense subsystems. In this work we proposes trackback methodologies to control unwanted tragic by mitigating flooding based DDOS attacks. The work concentrates mainly on the detection algorithm should detect a DDOS attack at the originating source with high reliability. In future we would like work on implementing the Trace back techniques in IPv6 environments Other direction of future work would be to improve the detection efficenacy related to DNS and related spoof threats. Improvement of detection delicacy is in terms of scrutinizing the proposed scheme with several other Trackback techniques. More work is needed for strictly restricting the bandwidth attack threats then it is almost impossible to launch memory resource attack towards DCs of cloud computing environment.

ACKNOWLEDGEMENT

I am profoundly thankful to Lecturer Nasib Singh Gill, department of computer science and applications, MD University for accepting me as a M.Tech Dissertation student.

Professor Nasib's depth of vision, thoughts and work control has been extremely inspirational. I should like to express my genuine cheers to Lecturer Nasib for his support,wise suggestions, motivation and priceless freedom in leading the research throughout the dissertation period.

I am indebted to my family for their support, understanding and aid, lacking them this work should not have been possible.

I would like to thank all the friends and teachers who helped me directly or indirectly to accept this research work.

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.

