A Review of Denial of Service Attack in MANET

*** Varsha Kushwah**
**** Prof. Shiva Bhatnagar**

ABSTRACT

Mobile ad-hoc network could be a collection of node that is self-configuring, decentralized, framework less mobile network .As a result of open nature of the network simply liable to numerous attacks. The main security threat on MANET could be a DDoS attack. Distributed Denial of Service (DDoS) attacks are a virulent, relatively new type of attack on the availability of Internet services and resources. DDoS attackers infiltrate large numbers of computers by exploiting software vulnerabilities, to set up DDoS attack networks. As specific countermeasures are developed, attackers enhance existing DDoS attack tools, developing new and derivative DDoS techniques and attack tools. It would be desirable to develop comprehensive DDoS solutions that defend against known and future DDoS attack variants.

Keywords:- DDoS, AODV, MANET, Security.

* Varsha Kushwah, Department of Electronics and Communication, PCST INDORE, varsha.kushwah.1994@gmail.com
** Prof. Shiva Bhatnagar, Department of Electronics and Communication, PCST INDORE

I. INTRODUCTION:

A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource. liberated to move severally in any direction it is like with different node changes often. This understanding can help to produce more effective and encompassing DDoS detection, prevention and mitigation mechanisms. A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms.

MANETs are infected with a numerous attacks together with impersonation, message distortion, eavesdropping, and Distributed DoS (DDoS) [1]. Denial of Service (DoS) attacks, that are meant at attempting to stop approved users from accessing or utilizing various network resources, are illustrious to the network analysis community since the first1980s. The primary Distributed DoS (DDoS) attack incident and most of the DoS attacks since then are distributed in nature [2]. Mobile ad-hoc network may be a group of two or additional devices or nodes with the capability of communication and networking.

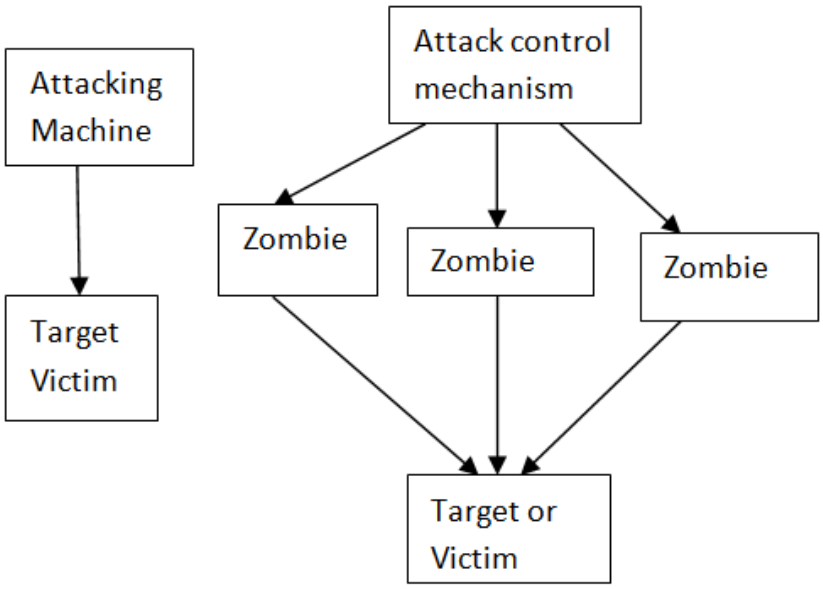

Figure 1.1: DoS and DDoS Attack Scenario

analyzes the network performance under Distributed Denial of Service MANETS. The resistive schemes against these attacks were proposed for ad hoc on demand Distance Vector (AODV) routing protocol and the effectiveness of the schemes is valid using NS2 simulations.

II. PROPOSED WORK

The existing intrusion detection system (IDS) was categorized in to two types: Signature based IDS and Anomaly based IDS. The benefit of IDS technique is that it can be able to detect the attack without prior knowledge of attack. In Signature based intrusion detection some of the previously detected patterns or signatures are stored into the data base of the IDS. If any disturbance is found in the network by IDS, it checks it with the previously saved signature. If it matches, then IDS has found the attack. The disadvantage of this system is that if there is an attack and its signature is not in IDS database then IDS cannot be able to detect that attack. To overcome the drawbacks of signature based system, anomaly based IDS were proposed. In this system, first the normal profile of the network is set by the IDS and is taken as a base profile and then is compared with the monitored network profile as shown in Fig. 1.1. The anomaly intrusion detection system uses two intrusion detection parameters. They are,

1. Packet reception rate (PRR).

2. Inter arrival time (IAT).

But only these two parameters are not completely sufficient for intrusion detection in wireless sensor network and as well as in MANET.

III. WORK DONE

According to proposes a way or place where security application can track more traffic instead of applying to all nodes that can save much more cost as compared to provide security for every node. Critical link are that place, from where maximum traffic can travel and monitoring of those nodes are easy. According to, DoS attack can be launched in two forms. The first form aims to break down the target by sending one or more carefully constructed control packets that make use of the protocol or operating system vulnerabilities. The second form is to overflow the target with a huge amount of rubbish data, which leads to exhaustion of network bandwidth or computer resources. In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes. As a consequence, routing loops may appear and introduce severe network congestion. Multiple attackers may completely isolate a victim, by preventing it from finding performed via network-layer packet blasting. The attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET. In a SYN flooding attack, the attacker creates a large number of half-opened Transmission Control Protocol (TCP) connections with a target node, but never completes the handshake to fully open the connection.

IV. EXPECTED OUTCOME

DDos attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, dos strategies include the continuous or random transmission of high power interference signals. Anti-Passive techniques rely extensively on spread-spectrum (SS) communications, or some form of Passive evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model .Ddos attack in parameter used are Packet delivery ratio, Throughput, End to End delay, Residual Energy. We are increasing the packet delivery ratio and throughput and increase result according previous paper.

V. CONCLUSION

As the use of MANETs increases, the protection becomes may be a critical issue. During this paper, Detecting, preventing, and mitigating DDoS attacks is important for national security. It is concluded that among all network attacks. This work carried out the detailed analysis of DDoS

attack detection through the trust mechanism with AODV routing protocol which is simulated by NS-2 for WSN on the basis of different performance metrics viz. packet delivery ratio, end to end delay, residual energy and average throughput. These performance metrics are analyzed for the AODV, DSDV and DSR routing protocols by varying the node density for fixed network. Simulation of routing protocol provides the facility to select a good environment for routing and gives the knowledge how to use routing schemes in attack network. Simulation results show that, as the density of nodes increases in the network, the performance of the routing protocols decreases. Attacker nodes affect the performance of routing protocols most as path break increases. According to simulation results as the prevent through the AODV, the packet delivery ratio, Throughput and End to End delay of routing protocol increases as compare to the detection of AAODV through the DSDV.

REFERENCES

1. George Theodorakopoulos and John S. Baras, On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. IEEE JSAC, Vol.24. No.2, February 2006.
2. Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, Elseiver publications 2003.
3. Jie Li and Jien Kato, Future Trust Management Framework for Mobile Ad hoc Networks. IEEE Communications Magazine, April 2008.
4. Panagiotis Papadimitratos and Zygmunt J.Haas, Secure Data Communication in Mobile Ad hoc Networks, IEEE JSAC, Vol.24, No.2, February 2006.
5. Zhi Ang EU and Winston Khoon Guan SEAH,"Mitigating Route Request Flooding Attacks inMobile Ad Hoc Networks", Proceedings ofInternational Conference on Informationnetworking (ICOIN-2006), Sendai, Japan, 2006.
6. S. Marti, T. J. Giuli, K. Lai, and M. Baker,"Mitigating routing misbehavior in mobile ad hocnetworks", Mobile Computing and Networking,2000.
7. Jonathan M. McCune, Elaine Shi, Adrian Perrig,Michael K. Reiter, "Detection ofdenial-of-message attacks on sensor networkbroadcasts", Proceedings of IEEE Symposium onSecurity and Privacy, May 2005.
8. S.A.Arunmozhi and Y.Venkataramani, A FlowMonitoring Scheme to Defend Reduction-of-Quality(RoQ) Attacks in Mobile Ad-hoc Networks, InformationSecurity Journal: A Global Perspective, Vol.19, No.5,2010
9. Jelena Mirkovic and Peter Reiher, D-WARD: A Source-End Defense against Flooding Denialof- Service Attacks,IEEE Transactions On Dependable And SecureComputing, Vol. 2, No. 3, 2005.
10. Ping Yi, Zhoulin Dai, YiPing Zhong and Shiyong Zhang,Resisting Flooding Attacks in Ad Hoc Networks,Proceedings of the International Conference onInformation Technology: Coding and Computing(ITCC'05), Vol. 2,2002.
11. Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeokSong, Novel Defense Mechanism against Data FloodingAttacks in Wireless Ad Hoc Networks, IEEE Transactions on Consumer Electronics, Vol. 56, No. 2,May 2010.

12. Rathna. R and Sivasubramanian, ― Improving energy efficiency in wireless sensor networks through scheduling and routing‖, International Journal Of Advanced SmartSensor Network Systems (IJASSN), Vol 2, No.1, January 2012
13. Razieh Sheikhpour, Sam Jabbehdari and Ahmad khademzadeh, ― A Cluster-Chain based Routing Protocol for Balancing Energy Consumption in Wireless Sensor**Networks ‖,** International Journal of Multimedia and Ubiquitous Engineering Vol. 7,No. 2, April, 2012
14. Se-Jung Lim and Myong-Soon Park, ― Research Article Energy-Efficient ChainFormation Algorithm for Data Gathering in Wireless Sensor Networks‖, InternationalJournal of Distributed Sensor Networks Volume 2012, Article ID 843413, 9 pages doi:10.1155/2012/843413 July 2012