International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Review for Detection of Distributed DOS Attack in MANET

Poorva Kakani[1], Sanjay Thakur[2]

[1]Department of Computer Science & Engineering, LKCT, Indore (M.P.), India
[2]Professor, Department of Computer Science & Engineering, LKCT, Indore (M.P.), India

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 it's simply liable to numerous attacks. The main security threat on MANET could be a DDoS attack. DDoS attack has the flexibility to make immense quantity of unwanted traffic as a result of this the licensed user cannot used the resources properly. It's terribly laborious to notice and management the DDoS attack as a result of massive scale and complicated network environments.***

Keywords: DDoS, AODV, MANET, Security, Detection

1. Introduction

Mobile Ad-hoc Network could be a self-configuring infrastructure less network of mobile device that is connected through wireless. In mobile ad-hoc network every node is liberated to move severally in any direction and can so modification in it's like with different node changes often. Security of Mobile ad hoc Networks (MANETs) has been lots of scope within the analysis community. Because of open nature of network, dynamic changing topology MANET is definitely at risk of numerous attacks. Additionally, different problems also contribute to its vulnerability, like the open design, shared radio channels, and restricted resources, etc. while not a transparent network boundary, it's extraordinarily tough to develop and perceive ad hoc security strategy for MANETs. Currently, 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 first 1980s. 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. it's an infrastructure less network.

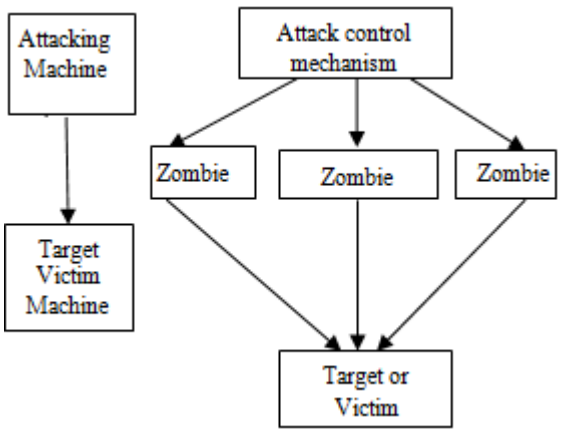

Figure 1.1: DoS and DDoS Attack Scenario

This paper focuses on mobile ad hoc networks -routing vulnerability and 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.

An Effective Intrusion Detection System for Routing Attacks in MANET using Machine Learning Technique, Author -Mr.Pratik Gite , Dr.Sanjay Thakur , March-2015-Wireless communication is widely adopted and application oriented technology There are a huge literature about Mobile Ad-hoc network is available. In these studies, the ad hoc network has two major issues security and performance. In this paper a feasible and adoptable solution is introduced for enhancing security in MANET. The presented work utilizes the network characteristics and their behavioral difference during attack. Using the attack and normal network behavior a machine learning algorithm is trained and the malicious patterns are distinguished according to the new network samples. The proposed machine learning based ad hoc network security is implemented using NS2 simulator and the performance of the system is evaluated in terms of metrics viz. throughput, packet delivery ratio, end to end delay and energy consumption. According to the obtained results the performance of the proposed secure network is optimum and adoptable.

An Attack investigation, Characterization and Simulation of Various attack in MANET, Author-Mr.Pratik Gite , Dr. Sanjay Thakur, 2015-A Mobile Ad Hoc Network (MANET) is a group of wireless mobile nodes forming a network without any infrastructure where all nodes are free to move randomly and where all the nodes in a defined range themselves . In MANET, each node proceeds both as a router and as a host. Additionally topology of network may also vary quickly. In such kind of network, topology creation is responsibility of routing protocol. Therefore, router may help in creating topology, finding path between source and destination and during path break condition route repairing. The above characteristics of MANET attract researchers in domain of MANET, but some

key issues and challenges are also available which limit the performance and security of MANET.

FireCol: A collaborative Protection Network for the Detection of Flooding DDoS Attacks, Author- Jérôme François, Dec-2012-Distributed denial-of-service (DDoS) attacks remain a major security problem, the mitigation of that is very hard especially when it involves extremely distributed botnet-based attacks. the first discovery of those attacks, though difficult, is necessary to protectend-users as well as the costly network infrastructure ,resources. during this paper, we address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of FireCol. The core of FireCol consists of intrusion prevention systems (IPSs) settled at the internet service providers (ISPs) level. The IPSs kind virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The analysis of FireCol using extensive simulations and a real dataset is presented, showing FireCol effectiveness and low overhead, further because it support for incremental deployment in real networks.

Flooding Attack preclusion in MANET, Authors- Ms. Neetu Singh Chouhan, Ms. Shweta Yadav, 2006-This is work proposed a new DOS attack and it is defence in ad hoc network. The new DOS attack, is called Ad Hoc Flooding Attack, that can result in denial of service when use beside on-demand routing protocol used for mobile ad hoc network, such that as AODV, DSR. The impostor transmit mass Route Request packet to wear out the communication bandwidth and node resource so that the valid communication cannot be kept back. After analyze Ad Hoc Flooding Attack, we expand Flooding Attack Prevention, a resistance against the Ad Hoc Flooding Attack in mobile ad hoc network. When the impostor transmits exceeding packets of Route Request, the instant neighbours of the intruder record the behaviour of sender and check its trust by a trust function. Once the threshold is go beyond, node deny any future request packets from the impostor The result of this implementation illustrate FAP can avoid the Ad Hoc Flooding attack economically The RREQ flooding packet more than the threshold value then the sender is unspecified as a attacker and all the packet from attacker is unnecessary by the receiver node. This technique reduces the flooding packet but if the impostor has the thought about the threshold value then it can bypass the TP machine.

Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks, Authors- Jian-Hua Song1, 2, Fan Hong1, Yu Zhang1, 2006- This kind of attack is solid to sense since spiteful node mimic normal node in all portion except for that they do route detection much more commonly than the other node. A suspected filtering mechanism is proposed to moderate such conditions and condense the loss of throughput. The proposed device could prevent this specific kind of DoS attack and does not use any extra network transmit. In Mobile Ad hoc Networks (MANET), various kinds of Denial of Service Attacks (DoS) are possible because of the intrinsic restrictions of its routing protocol. The attack of initiating forwarding false Route Requests (RREQs) can direct to hogging of network resources and hence denial of service to authentic node.

Security in MANET against DDoS Attack, Authors- V.Kaviyarasu1, S.Baskaran2, Jan-2014- The security of the network from the variety of attack is an imperative issue in MANET purpose now day. Due to with passion changing topology, open environment and lack of centralized security communications, a mobile ad hoc network (MANET) is exposed to many attacks. This paper focuses on mobile ad hoc network routing exposure and analyzes the network performance under Distribute Denial of Service MANETs. The resistive systems beside these attacks were planned for a Ad hoc on demand Distance Vector (AODV) routing protocol and the efficiency of the schemes is validated using NS2 simulations. Mobile ad-hoc network is a group of two or more device or nodes with the potential of communication and networking. It is a infrastructure less network. Such that network may function by them or may be connected to a larger internet. Due to its mobility and self routing potential environment there are many weaknesses in its security.

Detection and prevention of Denial of Service Attacks using Distributed Denial-of-Service Detection Mechanism, Author- A.Prathap, Dec-2012-In the networking systems the flow of information is the most important service. it's clear that an easy self-propagating worm will quickly spread across the web and cause severe damage to our society. Facing this great security threats like Denial-of-Service (DoS), we want to make an early detection system which will detect the presence of a worm within the net as quickly as attainable so as to present people correct early warning information and possible reaction time for counteractions. To avoid these types of threats more effective approaches are needed to counter the threats. This requirement has motivated us to form novel mechanism for effective early detection and prevention of DoS attacks at the router level within an Internetworking infrastructure. Here our system presents a “trend detection” methodology to detect DoS at its early propagation stage by using Kalman filter. in addition, for uniform-scan worms like Code Red, we can effectively predict the vulnerable population size, and estimate accurately how many computers are very infected within the global net based on the biased monitored information. also during this system we propose a domain-based approach, the mechanism that combines each stateful and stateless signatures to provide early detection of DoS attacks, therefore, protect the network. During this project we are using the novel Distributed DoS Detection Mechanism (DiDDeM) using the Kalman filter mechanism to detect DoS attacks at the early stage.

2. Distributed DoS Detection Scheme

Real-time Detection Scheme: A fingerprint based scheme is proposed by Xing et al. [12], where the fingerprint of a node is computed using the neighborhood information. In this scheme, each node is preloaded with a codeword generated from a superimposed s-disjunction code prior to their deployment. A node computes its unique fingerprint as well as the fingerprints of its neighboring nodes using their codeword. The fingerprint of a node is included in every message that is sent t o the BS. Neighboring nodes verify the genuineness of a node by comparing the fingerprint in the message with their own record. A conflict in the fingerprint

of any node is reported to the BS, and is detected as Dos. In this scheme, a Distributed DoS is detected either by the neighboring nodes or the BS. The generation of codeword from superimposed s-disjunct code is computationally expensive.

Neighbor-Based Detection Scheme (NBDS): A neighbor-based detection scheme was proposed by disjunction et al. [12]. According to their scheme, a node moving to a new location must broadcast a rejoining claim to its new neighbors. The rejoining claim consists of the list of its old neighbors. A new neighbor on receiving the rejoining claim forwards it to a randomly selected node from the list of old neighbors. An old neighbor on receiving the rejoining claim checks for the node ID in its neighbor table. If the node ID is present, then the old neighbor reports to the BS, otherwise it concludes that the node has moved to another location. The old neighbor then sends a challenge to the node to verify its existence in its neighborhood. If the node is present in the old position, then it is detected as a Distributed DoS. On the other hand, if the new neighbors do not receive any revocation message within a stipulated time period, then, they accept the newly joined node as their neighbor. This scheme allows occasional static of nodes in the network. However, an intelligent adversary may bypass the Distributed DoS detection process. The verification process of the scheme increases the communication overhead.

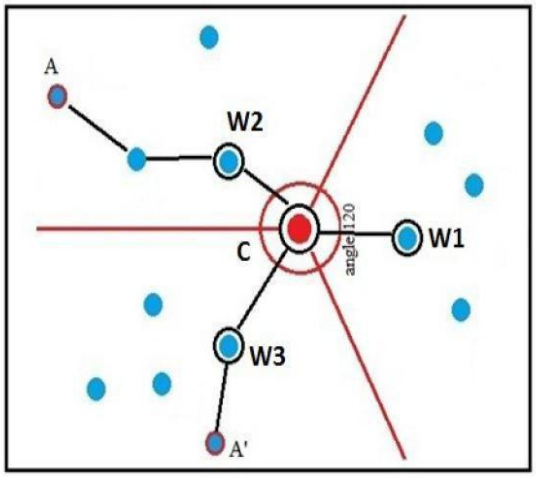

Figure: Area based approach for node Ddos detection

Hierarchical Node Distributed DoS Detection Scheme
Naidu et al proposed a mechanism for three-tier hierarchical network structure. Their mechanism is based on the use of Bloom filter [13, 14]. The Distributed DoS detection process is divided into the following three phases:

1) **Pre-distribution Phase**: In this phase, nodes are equipped with cryptographic keying materials and other parameters required for Bloom filter operation.
2) **Election Phase**: This phase is performed periodically to select cluster-head using Local Negotiated Clustering Algorithm (LNCA) protocol [13].
3) **Detection Phase**: Elected cluster-heads exchange their member IDs among themselves using Bloom filter. A node ID that is found to be a member of more than one cluster is detected as DoS.

The memory overhead of this scheme is significantly lower. However, it has an additional communication overhead in cluster formation. For a small number of hash functions the false detection probability is higher and requires relatively larger number of bits in Bloom filter.

3. Proposed Algorithm

The proposed algorithm Modified Low Energy Adaptive Clustering Hierarchy (M-AODV) is based on the trust values of individual nodes. All the nodes of wireless ad-hoc network have a specific trust value. The algorithm encompasses the following steps:

3.1 Initialization

- Trust values of all the participating nodes are set to be initialized by specific previously assigned trust value.
- Initialize the trust value of every node with 100.
- Assumption: 1 trust value = 10 packets dropped.

Updating of trust values:
If the packets are correctly transmitted from one node to another node:

(a) If the correctly transmitted no of packets is between 1 and 10, then trust values of the respective nodes will be incremented by one time.
Updated trust value = old trust value + 1;

(b) If the correctly transmitted number of packets is greater than 10, then the updated trust value will be:
Updated trust value = old trust value + (correctly transmitted packets / 10);

- If the packets are dropped/delayed:

i) The number of dropped or delayed packets is between 1 and 10 and then trust value of that particular node is decremented by one.
Updated trust value = old trust value – 1;

ii) The number of dropped or delayed packets are greater than 10, then trust value of that particular node will be,
Updated trust value = old trust value – (Packet dropped or delayed / 10);

- If the trust value of particular node is negative, then print -Invalid node‖.

Isolating the Packet drop node from the network:
- If (Updated trust value < Threshold trust value)

Then, the particular node is treated as malicious node (Ddos node attack)

- If (Updated trust value > Threshold trust value)

Then, the particular node is treated as legitimate node.

4. Conclusion

As the use of MANETs increases, the protection becomes may be a critical issue. During this paper, I've got mentioned the DDoS attacks in MANET and related DDoS detection

techniques. I have got also present projected defense framework against DDoS attack in MANET. It's concluded that among all network attacks, DDoS attacks are the most harmful threats to network functionality and MANETs are even a lot of vulnerable to those 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 of International Conference on Information* networking (ICOIN-2006), Sendai, Japan, 2006.
[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker,"Mitigating routing misbehavior in mobile ad hoc networks", Mobile Computing and Networking, 2000.
[7] Jonathan M. McCune, Elaine Shi, Adrian Perrig, Michael K. Reiter, "Detection of denial-of-message attacks on sensor network broadcasts", *Proceedings of IEEE Symposium on Security and Privacy*, May 2005.
[8] S.A.Arunmozhi and Y.Venkataramani, A Flow Monitoring Scheme to Defend Reduction-of- Quality (RoQ) Attacks in Mobile Ad-hoc Networks, *Information Security 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 Secure Computing, 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 on Information Technology: Coding and Computing (ITCC'05), Vol. 2,2002.*
[11] Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song, Novel Defense Mechanism against Data Flooding Attacks 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 Smart Sensor 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‖, *International Journal of Distributed Sensor Networks Volume 2012, Article ID 843413, 9 pages doi:10.1155/2012/843413 July 2012.*
[15] Mr. Pratik Gite, Dr. Sanjay Thakur- An Effective Intrusion Detection System for Routing Attacks in MANET using Machine Learning Technique ||, *International Journal of Computer Applications (0975 – 8887) Volume 113 – No. 9, March 2015.*
[16] Mr. Pratik Gite, Dr. Sanjay Thakur- An Attack Investigation, Characterization and Simulation of Various Attacks in MANET ||, *International Journal of Electronics Communication and Computer Engineering Volume 6, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209, 2015.*
[17] Jérôme François, Issam Aib - FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks ||, *IEE/ACM transactions on networking, Vol. 20, no. 6, December 2012.*
[18] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav - Flooding Attacks Prevention in MANET ||, *International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3.*
[19] Jian-Hua Song, Fan Hong - Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks ||, *IEEE 2006.*
[20] V.Kaviyarasu1, S.Baskaran - Security in MANET against DDoS Attack ||, *International Journal of Computer Trends and Technology (IJCTT) – volume 7 number 1– Jan 2014.*
[21] A.Prathap , R.Sailaja - Detection and Prevention of Denial of Service Attacks Using Distributed Denial-of-Service Detection Mechanism ||, *(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012,5434-5438.*