Security in MANET Against DDoS Attack

V.Kaviyarasu[1], S.Baskaran[2]

[1](PG Scholar, ECE department, Sri Manakula Vinayagar Engineering College, Puducherry)

[2](Assistant Professor, ECE department, Sri Manakula Vinayagar Engineering College, Puducherry)

ABSTRACT: *Mobile ad-hoc network is a group of two or more devices or nodes with the capability of communication and networking. It is an infrastructure less network. Such network may operate by them or may be connected to a larger internet. Due to its mobility and self routing capability nature, there are many weaknesses in its security. The security of the network from various attacks is an important issue in MANET application now days. Due to the dynamically changing topology, open environment and lack of centralized security infrastructure, a mobile ad hoc network (MANET) is vulnerable to many attacks. This paper focuses on mobile ad hoc network's 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 validated using NS2 simulations.*

Keywords – *Security, Mobile ad-hoc network, Denial of service, Flooding attack, Black hole attack*

I. INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.In this paper DDoS attacks are analyzed in detail. The resisting mechanisms over these attacks are proposed and the effectiveness of the system is validated.

II.DISTRIBUTED DENIAL OF SERVICE

A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. DoS (Denial of Service) attacks are sent by one person or system. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests’. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

III. 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. 3.1. The anomaly intrusion detection system uses two intrusion detection parameters. They are,

1. Packet reception rate (PRR) and
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.

3.1 Anomaly based intrusion detection system

To overcome the drawbacks of existing system, the proposed system takes in to account few more parameters along with the existing ones.

The parameters includes

(i) Throughput

(ii) Packet Delivery Ratio (PDR)

(iii) End to end delay

Anomaly based IDS are based on tracking unknown unique behavior pattern of detrimental activity. The advantages includes,

1. Helps to reduce the “limitations problem”.
2. Conducts a thorough screening of what comes through.

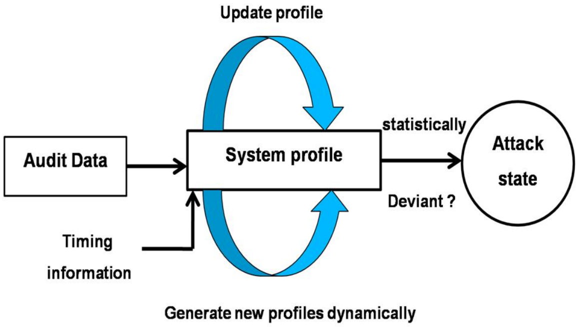

Fig 3.1 Anomaly based intrusion detection

Along with these, AODV routing protocol is used in normal module, attack module and IDS cases.

3.2 AODV Routing Protocol

The AODV Routing Protocol uses an on demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the Route Request packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single Route Request. The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the DestSeqNum of the current packet received is greater or equal than the last DestSeqNum stored at the node with smaller hop count.

A Route Request carries the source identifier, the destination identifier, the source sequence number (SrcSeqNum), the destination sequence number (DestSeqNum), the broadcast identifier (BcastID), and the time to live (TTL) field. DestSeqNum indicates the freshness of the route that is accepted by the source. When an intermediate node receives a Route Request, it either forwards it or prepares a Route Reply if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the Route Request packet. If a Route Request is received multiple times, which is indicated by the BcastID SrcID pair, the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send Route Reply packets to the source. Every intermediate node, while forwarding a Route Request, enters the previous node address and it's BcastID. A timer is used to delete this entry in case a Route Reply is not received before the timer expires. This helps in storing an active path at the intermediate node as AODV does not employ source routing of data packets. When a node receives a Route Reply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

3.3 Algorithm for IDS case

```
Create node =ids;
Set routing = AODV;
If ((node in radio range) && (next hop! =Null)
{
Capture load (all_node)
Create normal_profile (rreq, rrep, tsend, trecv,
tdrop)
{pkt_type; // AODV, TCP, CBR, UDP
Time;
Tsend, trecv, tdrop, rrep, rreq
}
Threshold_parameter ()
If ((load<=max_limit) &&
(new_profile<=max_threshold) &&
(new_profile>=min_threshold))
{
No any attack;
}
Else
 {
Attack in network;
Find_attack_info ();
}
Else
{
"Node out of range or destination unreachable"
}
Find_attack_info ()
{
Compare normal_profile into each trace value
If (normal_profile! = new trace_value)
{
Check pkt_type;
Count unknown pkt_type;
Arrival time;
Sender_node;
Receiver_node;
Block_Sender_node(); //sender node as attacker
}
```

3.4 Cases of Attack Detection

The three cases of attack detection are listed below:

3.4.1 Normal Case

The number of sender and receiver nodes and transport layer mechanism as TCP and UDP with routing protocol as AODV (ad-hoc on demand distance vector) routing.

3.4.2 Attack Case

In Attack module we create one node as attacker node whose set the some parameter like scan port , scan time , infection rate , and infection parameter , attacker node send probing packet to all other neighbour node whose belongs to in radio range, if any node as week node with nearby or in the radio range on attacker node agree with communication through attacker node, so that probing packet receive by the attack node and infect through infection, after infection this infected node launch the DDOS (distributed denial of service) attack and infect to next other node that case our overall network has been infected.

3.4.3 IDS Case

In IDS (Intrusion detection system) we set one node as IDS node, that node watch the all radio range mobile nodes if any abnormal behaviour comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDS block the attacker node and remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load, UDP analysis, TCP congestion window, Throughput Analysis and overall summary.

IV. SIMULATION RESULTS

The network simulator NS-2 is used to simulate the experiment. The parameter settings for the simulations are: the radio propagation mode is Two Ray Ground, antenna type is Omni antenna, interface queue length is 50 (packets), queue management scheme is Drop Tail, routing protocol is AODV, height of antenna is 1.5m, transmission distance is 250m, signal interference or sensing distance is 550m. The speed of the mobile node is 10m/s. The simulated traffic is Constant Bit Rate (CBR).

TABLE: Simulation Parameters for Case Study

Examined Protocol	AODV
Number of nodes	50
Dimension of simulated area	1200×1200

Simulation time (sec)	35
Radio range	250m
Traffic type	CBR, 100pkts/s
Packet size (bytes)	512
Number of traffic connections	TCP/UDP
Maximum Speed (m/s)	25
Node movement	Random
Types of attack	DDOS
speed of the mobile node	30m/s

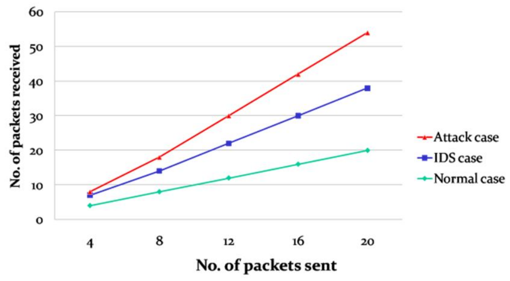

Fig 4.1 Impact of throughput

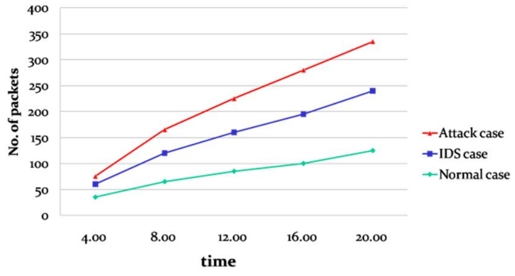

Fig.4.2 Impact of Packet Delivery Ratio with varying No. of Nodes

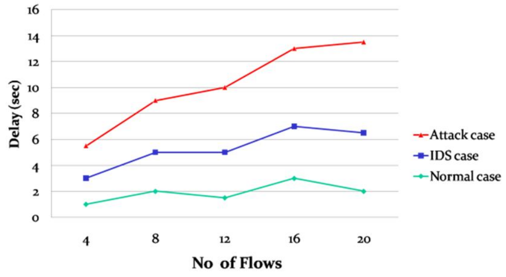

Fig.4.3 Impact of Average End to End Delay

V. CONCLUSION

Security is a very important in MANET. A variety of attacks have been discussed in this paper the proposed mechanism eliminates the need for a centralized trusted authority which is not practical in Ad-hoc network due to their self organizing nature. The results demonstrate that the presence of a DDoS increases the throughput of the network and also reduces the end to end delay.The proposed mechanism protects the network through a self organized, fully distributed and localized procedure. As a future work, we plan to experiment the proposed scheme for securing the network with other routing protocols and also to experiment the scheme for Blackhole and flooding attack

VI. ACKNOWLEDGEMENTS

It is my immense pleasure to express my deep sense of gratitude and indebtedness to my highly respected and esteemed Mr. S. Baskaran and Mrs. L. M. Varalakshmi (ECE) Department SMVEC puducherry. Her invaluable guidance, inspiration, constant encouragement sincere criticism and sympathetic attitude could make this paper possible.

REFERENCES:

[1] 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, pp.263- 272.

[2] 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, pp. 216-232.

[3] 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.*

[4] 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, pp. 579-582.

[5] N. Karthikeyan, V. Palanisamy and K.Duraiswamy, Optimum Density Based Model for Probabilistic Flooding Protocol in Mobile Ad Hoc Network, *European Journal of Scientific Research, Vol.39*, No.4, 2010, pp.577-588.

[6] Xuan Yu, A Defense System On Ddos Attacks In Mobile Ad Hoc Networks, *Ph.D dissertation, Auburn University, Alabama*, May 2007.

[7] Ming-Yang Su, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems, *Computer Communications*, *Vol. 34, 2011*, pp. 107–117.

[8] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal, Antonio Nucci and Edward BKnightly, DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks, *IEEE/ACM Transactions On Networking, Vol. 17, No. 1*, February 2009, pp. 26-39.

[9] Amey Shevtekar and Nirwan Ansari, A routerbased technique to mitigate reduction of quality (RoQ) attacks, *Computer Networks*, *Vol. 52*, 2008, pp. 957–970.

[10] Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong, A New Routing Attack in Mobile Ad Hoc Networks, *International Journal of Information Technology, Vol. 11, No. 2*, 2005, pp.83 94.

[11] Michele Nogueira Lima, Aldri Luiz dos Santos and Guy Pujolle, A Survey of Survivability in Mobile Ad Hoc Networks,*IEEE Communications Surveys & Tutorials, Vol. 11, No. 1*, 2009, pp. 66-77.

[12] S.Sanyal, A.Abraham, D. Gada, R.Gogri, P.Rathod, Z.Dedhia and N.Mody, Security scheme for distributed DoS in mobile adhoc networks. *ACM, New York*, 2004.

[13] H. Deng, W. Li and D.P.Agrawal, Routing security in wireless ad hoc networks, *IEEE Communications Magazine, Vol. 40, No. 10*, 2002, pp. 70- 75

[14] P.Ebinger and M.Parsons, Measuring the Impact of Attacks on the Performance of Mobile BAd hoc Networks, ACM PE-WASUN: *Proceedings of the 6th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Network*, 2009.

[15] Zhiqiang Gao and Zhiqiang, Differentiating Malicious DDoS Attack Traffic from Normal TCP Flows by Proactive Tests, *IEEE Communications Letters, Vol. 10, No. 11*, 2006, pp. 793-795.

[16] Junhai Luo, Mingyu Fan and Danxia Ye, Black Hole Attack Prevention Based on Authentication Mechanism, *11th IEEE Singapore International Conference on Communication Systems*, 2008, pp.173-177.

[17] Elmar Gerhards Padilla, Nils Aschenbruck, Peter Martini, Marko Jahnke, and Jens T¨olle, Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, *Proceedings of 32nd IEEE Conference on Local Computer Networks*, 2007, pp. 1043-1052.

[18] M.Al-Shurman, S.Yoo and S.Park, Black hole Attack in Mobile Ad Hoc Networks. *ACM Southeast Regional Conference*, 2004, pp. 96- 97

[19] Jieying Zhou, Junwei Chen and Huiping Hu, SRSN: Secure Routing based on Sequence Number for MANETs, *International Conference on Wireless Communications, Networking and Mobile Computing*, 2007, pp.1569-1572

[20] Nital Mistry, Devesh C Jinwala and Mukesh Zaveri, Improving AODV Protocol against Blackhole Attacks, *Proceedings of the International Multiconference of Engineers and Computer Scientist*, Hong Kong, Vol. II, 2010.

[21 Z.Gao and N.Anzari, Differentiating malicious DDoS attack traffic from normal TCP flows by proactive tests, *IEEE Communications Letters, Vol. 10, No. 11*, 2006, pp. 793-795.

[22] X.Wu and D.K.Y Yau, Mitigating denialof- service attacks in MANET by distributed packet filtering: A game-theoretic approach, *Proceedings of the 2nd ACM Symposium on Information, Computer and Communication Security*, 2006, pp. 365–367.

[23] P.Ebinger and M.Parsons, Measuring the impact of attacks on the performance of mobile ad hoc networks. *ACM PE-WASUN: Proceedings of the 6th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, Canary Islands, Spain, 2009.

[24] J.Haggerty, Q.Shi and M.Merabti, Statistical signatures for early detection of flooding denial-of-service attacks, *Security and Privacy in the Age or ubiquitous Computing, IFIP Advances in Information and Communication Technology, Vol. 181*, 2005,
pp. 327-341.

[25] X.Luo, E.W.W.Chan and R.K.C.Chang, Detecting pulsing denial-of-service attacks with nondeterministic attack intervals, *EURASIP Journal on Advances in Signal Processing*, Vol.2009, pp.1-13.

[26] Buchegger and J. Boudec, Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks, *Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*, Canary Islands, Spain, 2002.

[27] S. Marti, T. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, *Proc. of the Sixth Annual International Conference on Mobile Computing and Networking* (MOBICOM), Boston, 2000.