

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

A Novel Solution to Nullify DDOS Attack in MANET

RANJU¹, NEERAJ MADAAN²

¹CSE Department, KUK University
Haryana, India
garg.ranju@gmail.com

²CSE Department, KUK University
Haryana, India
neeraj.k.madaan@gmail.com

Abstract: Distributed Denial of Service (DDoS) attacks in the networks needs to be prevented or handled if it occurs, as soon as possible and before reaching the victim. Trading with DDoS attacks is difficult due to their properties such as dynamic attack rates, big scale of botnet, various kinds of goals, etc. Distributed Denial of Service (DDoS) attack is hard to deal with because it is difficult to distinguish legitimate traffic from spiteful traffic, especially when the traffic is coming at a different rate from disseminated sources. DDoS attack becomes more difficult to handle if it occurs in wireless network because of the properties of ad hoc network such as low battery life, dynamic topologies, frequency of updates, multicast routing or mobile agent based routing, network overhead, scalability, and power aware routing, etc. Therefore, it is better to prevent the distributed denial of service attack rather than allowing it to occur and then taking the necessary steps to handle it. In this paper a novel solution is proposed to handle DDoS attacks in mobile ad hoc networks (MANETs).

Keywords: DDoS Attack, MANET, AODV, Flooding Attack.

1. INTRODUCTION

Mobile Ad hoc Network (MANET) comprises autonomous mobile nodes that dynamically and arbitrarily form multi-hop communication facilities to attack, Denial of Service (DoS) attack, selfish misbehaving, etc.. Among these security threats, MANET are particularly susceptible to DoS attacks due to the facts that resources on mobile nodes are limited and broadcast mechanism is resource consuming. make up for the absence of fixed infrastructure. Securing communication in MANET is a challenging issue. Firstly, traditional security mechanisms used in infrastructure networks may be inapplicable to MANET due to its unique characteristics: unreliability of wireless links, the absence of a certification authority, dynamically changing topology and the lack of a centralized observation or management point. Secondly, for the same reason, MANET suffers from a wide range of threats and attacks: impersonation attack, black-hole.

2. FLOODING ATTACK IN MANET

The flooding attack is the most common attack found in manet. The aim of the flooding attack is to fatigue the network resources such as bandwidth and to consume a node's resources or to disrupt the routing operation to degrade the network performance. This leads to a kind of Denial-of- Service (DoS) attack, wastage of bandwidth, wastage of node's processing power and exhaustion of node's battery power as well as a degraded performance. Most of the network resources are wasted in trying to generate the routes to the destination that do not exist. The Route Request Flooding Attack (RRFA) is a denial-of service attack which aims to flood the network with a large number of RREQs to non-existent destinations in the network. In this attack, the spiteful node will generate a

large number of RREQs, possibly in the territory of hundreds or thousands of RREQs, into the network until the network is saturated with RREQs and unable to transmit data packets. In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network.

2.1 EFFECTS OF FLOODING ATTACK

Flooding Attack can seriously reduce the performance of reactive routing protocols and affect a node in the following ways.

A. Degrade the performance in buffer:

The buffer used by the routing protocol may overflow since a reactive protocol has to buffer data packets during the route discovery process. Furthermore, if a large number of data packets originating from the application layer are actually beyond reach, authentic data packets in the buffer may be replaced by these unreachable data packets, depending on the buffer management scheme used.

B. Degrade the performance in wireless interface:

Depending on the design of the wireless interface, the buffer used by the wireless network interface card may overflow due to the large number of RREQs to be sent. Similarly, genuine data packets may be dropped if routing packets have priority over data packets.

C. Degrade the performance in RREQ packets:

Since RREQ packets are broadcast into the entire network, the growing number of RREQ packets in the network results in more MAC layer collisions and consequently, overcrowding in the network as well as delays for the data packets. Higher level protocols like TCP which is sensitive to round trip times and congestion in the network will be affected.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

D. Degrade the performance in lifetime of Manet:

Since MANET nodes are likely to be potential and bandwidth constrained, RRFA can reduce the lifetime of the network through useless RREQ transmissions as well as additional overheads of authenticating a large number of RREQs, if used.

3. LITERATURE REVIEW

Rutvij H. Jhaveri [1] present survey of common Denial-of-Service (DoS) attacks on network layer namely Grayhole attack, Wormhole attack, Blackhole attack and which are serious threats for MANETs. We will also discuss some suggested solutions to detect and prevent these attacks. MANETs have unique characteristics like, limited resources, dynamic topology, lack of centralized administration and wireless radio medium; as a result, they are unprotected to different types of attacks in different layers of protocol stack. Each node in a MANET is proficient of acting as a router. Routing is one of the features having various security concerns.

Rajdeep Singh [2] discussed some attacks on MANET and DDOS also provide the security against the DDOS attack. Each device in a MANET is independently free to move in any route, and therefore change its connections to other devices frequently. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. There are many security attacks in MANET and DDOS (Distributed denial of service) is one of them.

Meghna Chhabra [3] discusses various the attack mechanisms and problems due to DDOS attack, also how MANET can be overblown by these attacks.

A mobile ad hoc network (MANET) is a spontaneous network that can be established without any fixed infrastructure or a topology. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes *i.e.* nodes within each other's radio range communicate directly via wireless connections, while those that are not in each other's radio range use other nodes as relays.

Yu Chen [4] proposes a strategy to mitigate DDOS attacks in MANETs. Mobile Ad Hoc Networks (MANETs) allow mobile hosts to form a communication network without a prefix framework. Although it provides high mobility, it also brings more challenges for MANETs to fight against malicious attacks. However, the property of moving and redundancy also inspires new ideas to design defence strategy. Assume that a malicious attacker normally targets specific sufferer. The attacker will give up if the attack failed to achieve the desired goals after a certain length of attacking time. In our protection scheme, we take advantage of high redundancy and select a protection node. Once a DDOS attack has been observed, the doubtful traffic will be redirected to the defence node. The sufferer will function

normally, and it is sensible to expect that the attacker will stop the meaningless efforts

B. B. Gupta [5] present a comprehensive study of a wide range of DDOS attacks and defense methods proposed to combat them. Propose an integrated solution for completely defending against flooding DDOS attacks at the Internet Service Provider (ISP) level. Distributed Denial of Service (DDoS) attacks on user machines, federation and framework of the Internet have become highly publicized incidents and call for instant solution. It is a complicated and difficult problem characterized by an explicit attempt of the attackers to prevent access to resources by legitimate users for which they have permission. Several schemes have been proposed on how to defend against these attacks, yet the problem still wants a complete solution.

Yinghua Guo [6] presents a detailed investigation of the flooding attack in MANET which is particularly vulnerable to flooding attacks. To avoid being recognized, attackers usually recruit multiple accomplices to dilute attack traffic density of each attack source, and use the address parody technique to challenge attack tracing. we design two flow based detection features, and apply the increasing sum algorithm on them to effectively and accurately detect such attack.

Hwee-Xian Tan [7] studies the vulnerability of MANETs to DDOS attacks and provide an overview of constant filtering, which is commonly used as a security mechanism against DDOS attacks in wired networks. Also propose a structure for statistical filtering in MANETs to combat DDOS attacks. Mukesh Kumar [8] a technique is proposed that can prevent a specific kind of DDOS attack named flood attack which Disable IP Broadcast. MANET has no clear line of defence so it is accessible to both malicious attackers and legitimate network users. In the presence of hostile nodes, one of the main Challenges in MANET is to design the robust security solution that can prevent MANET from various Ddos attacks. Individual mechanisms have been proposed using various cryptographic techniques to countermeasures these attacks against MANET.

S. A. Arunmozhi [9] discussed the DDOS attacks and proposed a defense scheme to improve the performance of the ad hoc networks. The wireless ad hoc networks are highly vulnerable to distributed denial of service (DDoS) attacks because of its unique characteristics such as open network architecture, shared wireless medium and strict resource constraints. These attacks block the tcp throughput heavily and reduce the quality of service (QoS) to end systems gradually rather than refusing the clients from the services completely.

K. Kuppusamy [10] discusses how best the degradation of the performance can be prevented using some algorithm proposed in the methodology. The choking is done using a different mechanism based on the category of the client. The possibility of distributing information through networking has been growing in geometric progression. In this connection it is to be noted network attacks, in other words,

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

DDoS attacks also are germinating in equal amount. Sharing of information is being carried out by means of server and client. The client appeal for the data from the server and the server provides the response for the client-request. Here the client can breach the server performance by sending continuous or irregular requests. The result is the server performance becomes degraded.

4. EXPERIMENTAL SETUP

In this section, we present the experimental setup which is used to measure the performance of the network when it is subject to DDoS attacks. We use GloMoSim, which provide a scalable simulation platform for wireless networks, to perform our simulations. The common parameters that we have used in our simulations are given in Table 1.

Performance Metrics: In our simulations we use several performance metrics to compare the proposed AODV protocol with the existing one. The following metrics used for the comparison were

- Throughput: Number of packets sends in per unit of time.
- Packet delivery fraction (*PDF*): The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.
- End to End delay: -The average end to end latency of data packets is measured.
- Normalized routing load: Measured the number of routing packets transmitted for each data packet delivered at the destination.

Table I: Summary of simulation parameters.

S. No	Parameter	Value
1	Terrain Size	1500 X 1200 meters
2	Mobility Model	Random Waypoint
3	[Min, Max] speeds	(0 ms-1 , 20 ms-1)
4	MAC Protocol	802.11
5	Routing Protocol	AODV
6	Nominal traffic type	Constant Bit Rate(CBR) 12 connections
7	Number of Nodes	100

5. ALGORITHM

```

Assign Ids to nodes;
Set routing protocol AODV;
Setmax_limit;
If node is in radio range and next hop is not Null
then
Capture load (all_node)
Create normal_profile (rreq, rrep, tsend, trecv, tdrop,
BCAST packets sent to channel, number of packets routed
to another node)
{
pkt_type;

```

// AODV, TCP, CBR, UDP

```

Time;
Tsend, trecv, tdrop, rrep, rreq
}
Set min_threshold
Set max_threshold
If load is less than equal to max_limit and new_profile is
less than equal to max_threshold and new_profile is greater
than equal to 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 is not equal to new_trace_value
then
{
Check pkt_type; Sender_node;
Receiver_node;
Black list_Sender_node();
}
Count unknown pkt_type;
Arrival time;

```

6. RESULTS AND DISCUSSION

Effect of Proposed Prevention Scheme with Different Number of Attackers on PDR: Table 2 and Figure 1 show the effect of existing & proposed prevention technique on PDR with different number of attackers per network.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Table 2: Effect on PDR of Existing & Proposed Prevention Technique with varying number of attackers.

NUMBER OF ATTACKERS PER NETWORK	PACKET DELIVERY RATIO (PDR)		
	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
3	.32	.83	1
6	.20	.69	1
9	.12	.56	1

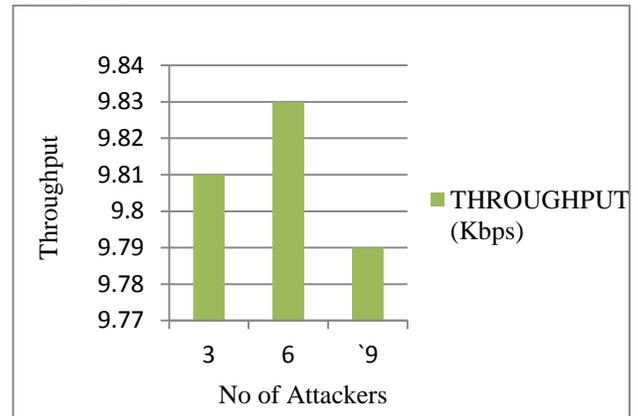


Figure2: Throughput with varying number of attackers

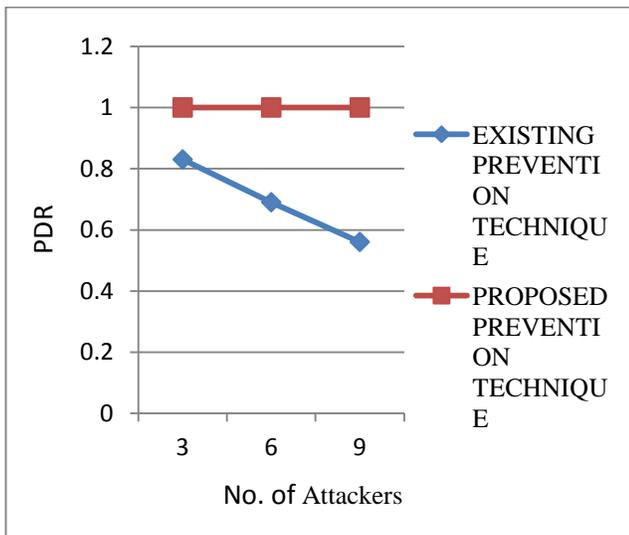


Figure1: PDR with varying number of attackers

Effect of Throughput with Different Number of Attackers on PDR: Table 3 and figure 2 shows the effect of throughput with different number of attackers per network.

Table 3: Effect of throughput with different number of attackers

NUMBER OF ATTACKERS PER NETWORK	THROUGHPUT (Kbps)
3	9.81
6	9.83
9	9.79

7. CONCLUSION

Security is the most important feature for deployment in mobile Ad-hoc network. Distributed Denial of Service attacks are more complex and major problem, and as a result, various approaches have been proposed to counter them. The proposed mechanism nullifies the DDOS attack in MNAET. The results demonstrate that the presence of a DDOS doesn't affect the delivery of the packets in the network considerably. The suggested mechanism protects the network. We believe that this is an adequate performance, given that the attack prevented has a much larger impact on the performance of the protocol. The proposed structure can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

REFERENCES

- [1] Rutvij H. Jhaveri, in *Second International Conference on "Advanced Computing & Communication Technologies"*, 2012.
- [2] Prajeet Sharma, Niresh Sharma, Rajdeep Singh *International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012.*
- [3] Meghna Chhabra, Brij Gupta, Ammar Almomani in *"Journal of Information Security"*, 2013, 4, 165-179 Published Online July 2013.
- [4] "Minda Xiang, Yu Chen, Wei-Shinn Ku, Zhou Su" This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.
- [5] "B. B. Gupta, R. C. Joshi and Manoj Mishra" in *Information Security Journal: A Global Perspective*, 18:224–247, 2009.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

- [6] “Yinghua Guo, Steven Gordon, Sylvie Perreau”
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.
- [7] “Hwee-Xian Tan, Winston K. G. Seah” in “Second International Conference on Embedded Software and Systems” (ICCESS’05).
- [8] “Mukesh Kumar & Naresh Kumar” in “International Journal of Application or Innovation in Engineering & Management (IJAIEEM) Volume 2, Issue 7, July 2013 ISSN 2319 – 4847.
- [9] S. A. Arunmozhi and Y. Venkataramani” in “International Journal of Network Security & Its Applications (IJNSA)” Vol.3, No.3, May 2011.
- [10] Dr. K. Kuppusamy, S. Malathi, in International Journal of Network Security & Its Applications (IJNSA), titled as “An effective prevention of attacks using giTime frequency algorithm under DDos” Vol.3, No.6, November 2011.