Investigation of Application Attack on MANET

Amit M Holkar
ME Scholar
Department of ECE
IET-DAVV Indore

Neha Shinde Holkar
ME Scholar
Department of IT
MIST, Indore

Dhiiraj Nitnawwre
Assistant Professor
Department of ECE
IET-DAVV, Indore

ABSTRACT
Security in Mobile Ad-hoc Networks always draws attention of the researcher due to its unsecured boundaries, infrastructure less system and dynamic & random behavior. Most of the works in MANET have been focused on the Network Layer attacks because the attacks can be identified and its effects can be minimized on the Network layer itself. On the other hand, few attacks bypass the network layer security and reached the Application Layer. This paper investigate the effect of Application layer attack on Mobile Ad-hoc Network using OPNET simulator and compare the outcomes of investigation of with and without attacks using different routing protocols. In our simulation, we investigate the Malicious code attack using a jammer node and compare it with a scenario of nodes having no attack. Among the two routing protocols AODV & DSR, simulation we found that under the effect of Malicious code attack AODV protocol outperforms while we concern about the delay and DSR protocol gives best result while we concern about the load.

General Terms
Malicious code Attack, Repudiation Attack, Routing Protocols

Keywords
Application Layer attacks, Throughput, Delay, OPNET

1. INTRODUCTION
Recent advances in computer networking have introduced a new technology for future wireless communication, a mobile ad hoc network (MANET). This technology, which is the combination of peer-to-peer techniques, wireless communications, and mobile computing, provides convenient infrastructure-less communications and could be very useful to provide communications for many applications especially when the infrastructure networks is not feasible. MANET could be used to overcome geographical constraints in a military operation. As it is easy to deploy, it may also very useful to assist in the disaster relief operations where temporary network infrastructure is immediately needed to replace the damaged infrastructure networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network.

The mobile ad hoc network has the following typical features [1]:

1. Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

2. Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

3. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

1.1 Routing Protocol

We select the most popular routing protocols, which is On-Demand routing protocols according the these routing protocols they are used when they are need and also in this routing protocols a node simply maintains routes information to get destination that it needs to send required data packets. The routes to get their desire destinations will expire automatically after some time of idleness, while the network is not being used, which give less load on the network and that's why it's very hard to attack on such routing protocols.

1.1.1 AODV
AODV using a classical distance vector routing algorithm. It is also shares DSR's on-demand discovers routes. During repairing link breakages AODV use to provide loop free routes. It does not add any overhead to the packets, whenever a route is available from source to destination. Due to this way it reduces the effects of stale routes and also need for route maintenance for unused routes. One of the best features of AODV is to provide broadcast, unicast, and multicast communication. During route discovery algorithm AODV uses a broadcast and for reply it uses unicast.

1.1.2 DSR
The DSR is an on-demand routing protocol that is based on source routing. It uses no periodic routing messages like AODV, and due to this way it reduces network bandwidth overhead, and also avoids large routing updates as well as it also reduces conserves battery power. In order to identify link layer failure DSR needs support from the MAC layer. It is consist of the two network processes, Route Discovery and

Route Maintenance. Both of neither AODV nor DSR guarantees shortest path.

2 APPLICATION LAYER ATTACKS

Applications layer need to be designed to handle frequent disconnection and reconnection with peer applications as well as widely varying delay and packet loss characteristics [3]. Like other layers application layer also vulnerable and attractive layer for the attacker to attack. Because this layer contains user data that supports many protocols such as SMTP, HTTP, TELNET and FTP which have many vulnerabilities and access points for attackers. The main attacks in application layer are malicious code attacks and repudiation attacks.

2.1 Malicious Code Attack

Various malicious codes such as virus, worm, spy-wares and Trojan horse attack both operating systems and user applications that cause the computer system and network to slow down or even damaged. An attacker can produce this type of attacks in MANET and can seek their desire information [4].

2.2 Repudiation Attack

The solution that taken to solve authentication or non-repudiation attacks in network layer or in transport layer is not enough. Because, repudiation refers to a denial of participation in the communication. Example of repudiation attack on a commercial system: a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction [4].

Table1. Security attacks at each layer in MANET

Layer	Attack
Application Layer	Repudiation, Data Corruption, Malicious code attack
Transport Layer	Session Hijacking, SYN flooding
Network Layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data Link Layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP Weakness
Physical Layer	Jamming, interceptions, eavesdropping

3. SIMULATION ENVIRONEMNT

In this paper we have explained the investigative result obtained from the simulation of different scenarios using OPNET Modeller 14.5. There are four different network scenario which we implement in OPNET and they are given below:

1.MANET using DSR protocol without attack.
2.MANET using AODV protocol without attack.
3.MANET using DSR protocol with Malicious code attack.
4. MANET using AODV protocol with Malicious code attack.

We compare the above scenarios by taking Delay and Throughput as performance parameter.

5.1 Network Scenario Description

In the simulation of mobile ad-hoc networks through OPNET we use 6 MANET stations, Jammer node, Profile configuration, Application configuration & Mobility configuration. Attributes of MANET stations are used as below:

1.Adhoc routing protocol-AODV/DSR
2.Packet size (packets)-infinity
3.Addrssing mode –IPv4
4.Transmit power -0.0005 (W)
5.Buffer size (bits)-256000
6.Larg packet processing-Drop

Application configuration model is used in the network topology. The application config node can be used for the following specification.
1. ACE Tiers information
2. Application specification
3. Voice encoder schemes

Profile configuration model is used in the network topology. The profile config node can be used to create user profiles. These user profiles can then be specified on different nodes in the network to generate application layers traffic. Mobility configuration is used to define the mobility of wireless stations.

In our simulation we use a Jammer node to create a Malicious code attack. We use mobile jam pulsed node. A jam pulsed node represents a jammer which can be deployed as a fixed, mobile or satellite node. The jammer provides transmission on a fixed single fixed frequency band which is masked by periodic pulse train in time. We use low power jammer node (.0001W) to show the effect of Jammer even when it transmit low power.

A network scenario with 6 mobile nodes and a jammer node is shown below.

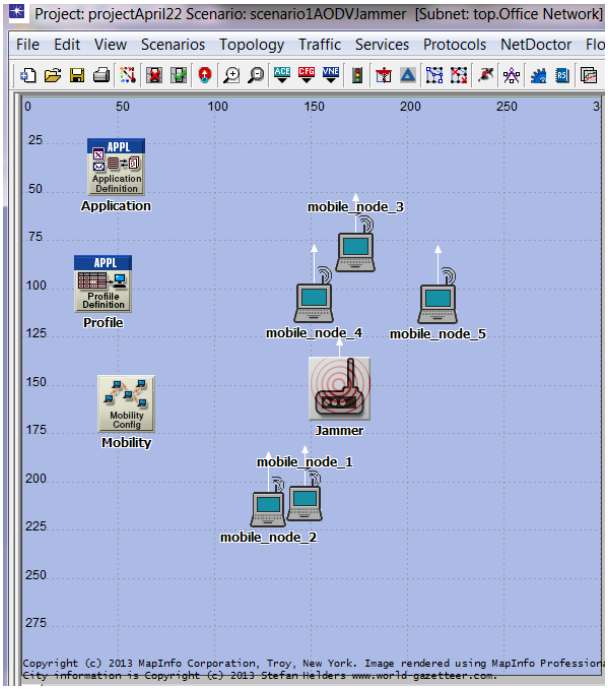

Fig 1 : Network Scenario with Jammer node

4 SIMULATION RESULT & ANALYSIS

We got four comparative results, two for each routing protocol (AODV & DSR), between scenarios with one attack and one without attack. We simulate the result keeping simulation time of 300 sec. All results are taken on the scale of time-average. Below we describe the analysis of our simulated result:

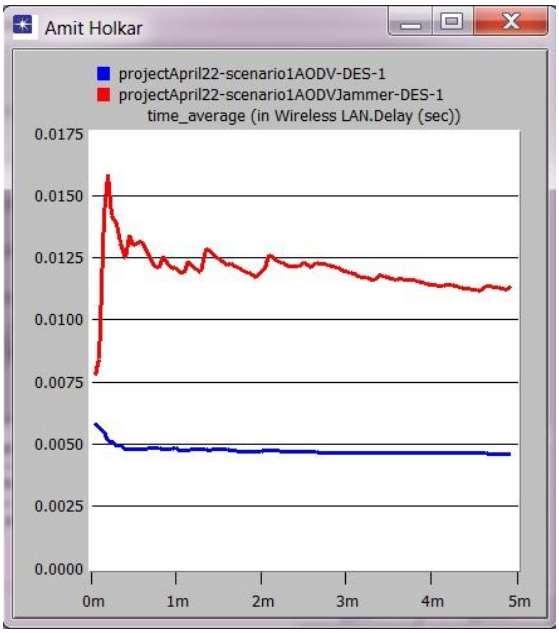

Fig 2: Comparison of Simulation result of Delay in MANET using AODV protocol with and without Malicious code attack

Above graph shows that using AODV protocol the maximum delay without attack is 0.005854355 at 3 sec and maximum delay with attack is 0.015838839 at 12 sec.

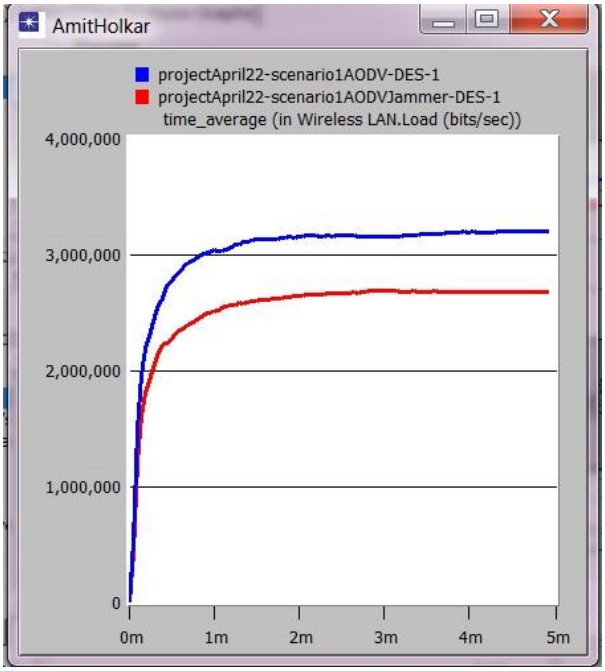

Fig 3: Comparison of Simulation result of Load (bits/sec) in MANET using AODV protocol with and without Malicious code attack

Above graph shows that using AODV protocol the maximum load with & without attack increases with time.

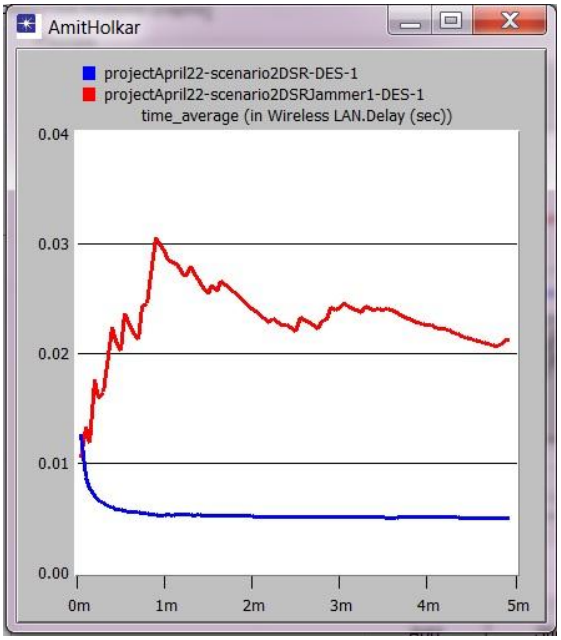

Fig 4: Comparison of Simulation result of Delay in MANET using DSR protocol with and without Malicious code attack

Above graph shows that using DSR protocol the maximum delay without attack is 0.01253664 at 3 sec and maximum delay with attack is 0.03046928
at 54 sec.

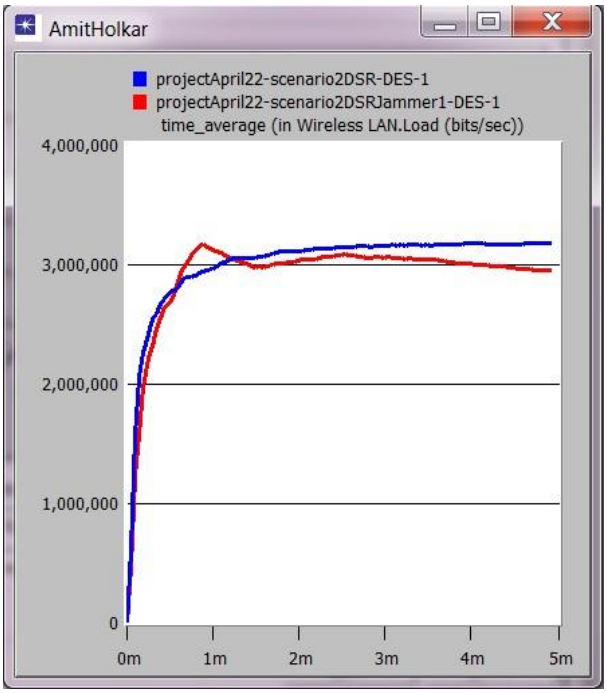

Fig 5: Comparison of Simulation result of Load in MANET using DSR protocol with and without Malicious code attack

Above graph shows that using DSR protocol the maximum load without attack increases with time and maximum load with attack is 3165760 at 54 sec.

5. CONCLUSION

After this simulation result we can conclude the following:

1. Under the Malicious code attack, AODV protocol outperforms when delay is the prime concern.

2. Under the Malicious code attack, DSR protocol gives best result when we concern about the Throughput.

6. REFERENCES

[1] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[2] Dr. Shahriar Mohammadi and Hossein Jadidoleslamy, "A COMPARISON OF LINK LAYER ATTACKS ON WIRELESS SENSOR NETWORKS", March 2011

[3] R. Ramanathan, J. Redi and BBN Technologies, "A brief overview of ad hoc networks: challenges and directions," IEEE Communication Magazine, May 2002, Volume: 40, page(s): 20-22, ISSN: 0163-6804

[4] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Department of Computer Science and Engineering, Florida Atlantic Universitymi

[5] Renu Mishr, Sanjeev Sharma, Rajeev Agrawal, IEEE 2010, Vulnerabilities and Security of Ad-hoc Networks.

[6] N. Meghanathan, "A Simulation-based Performance Analysis of Multicast Routing in Mobile Ad hoc Networks," International Journal of Information Processing and Management (IJIPM), Vol. 1, No. 1, pp. 4-14, July 2010.

[7] Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks.