Simulation Modelling of Selfish Node Attack Using ICMP Protocol

Nitin Kumar Gohal
M.Tech Student
SUSCET Tangori

Ranbir Singh
Assistant Professor
SUSCET Tangori

Abstract-**The Mobile Ad Hoc networks (MANETs) connects number of temporary mobile nodes through wireless interface that form either fixed infrastructure or centralized administration. The MANET networks are open medium and therefore, wide ranges of attack happen on this network. We classified the number of attacks in the subsections and draw selfish node attack only. The selfish node interprets the packet data unit (PDU) and extracts the useful information, other unused information dropped in the wireless link. This kind of attack is considered even more destructive than black hole attack. The absence of central co-ordination node MANET network more vulnerable to selfish node attack on wireless medium. The OPNET network simulator has been used to analyze the selfishness attack on wireless networks. The traffic model is used to generate traffic on the MANET Scenario and set of applications that generates and forward the formatted packet both exponential and constant form.**

Keyword: MANET, Attacks, AODV, Selfish Node, ICMP.

1. INTRODUCTION

1.1 Mobile Ad-hoc Network

A Mobile Ad-hoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system but as arouter also to forward packets.The MANET does not require any fix infrastructure such as base station.Networks areopen systems that dynamically change their topology by means of node mobility.

1.2 Characteristicsof MANETs

- **Autonomous Terminal*:*** In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.
- **Distributed operation:** There is no background network for the central control of the network operations and so the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. Security and routing.
- **Dynamic network topology:** Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals varies with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish connectivity among themselves as they move about, forming their own network on the fly. Moreover, auser in the MANET may not only operate within the ad hoc network, but mat require access to a public fixed network.
- **Multihop routing*:*** Basic types of ad hoc routing algorithms can be single-hop and multi-hop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multi-hop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.
- **Light-weight terminals:** In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

1.3 Working of MANETs

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discovermultihop paths through the network to any other node. This idea of Mobile ad-hocnetwork is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly.

2. ADOV PROTOCOL

AODV is an on-demand dynamic routing protocol that uses routing tables. When a source node needs a route to a destination, it initiates a route discovery process to locate the destination node.

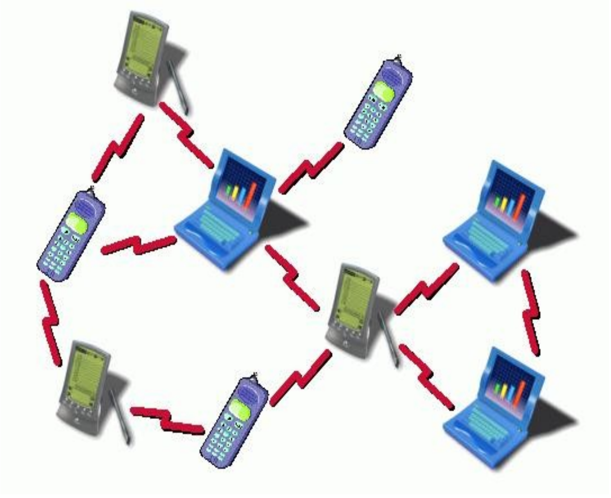

Figure 1: Mobile Ad-hoc Network

The source node floods a query packet, i.e., route request (RREQ), requesting a route to be set up to the destination. A reply, i.e. route reply (RREP), is sent back directly to the source node either by the destination itself or any other intermediate nodethat has a current route to the destination. On receiving a route request, intermediate nodes update their routing table for the reverse route to the source. Similarly, the forward route to the destination is updated on receiving a route reply packet.

AODV uses sequence numbers to determine the timeliness ofeach packet and to prevent loops. Expire timers are used to keep the route entries fresh. Link failures are propagated by a route error (RERR) message from the site of a link break to the source node for thatroute. Whenthe next hop link breaks, RERR packets aresent to a set of neighbouring nodes that communicate over the broken link with the destination.This recursive processerasesall broken entries in the routing table of the nodes. Sincenodes reply to the first arriving RREQ, AODV favours the leastcongested route instead of the shortest route. The AODV ondemandapproach minimizes routing table information. However, this potentially leads to a large number of route requests being generated.

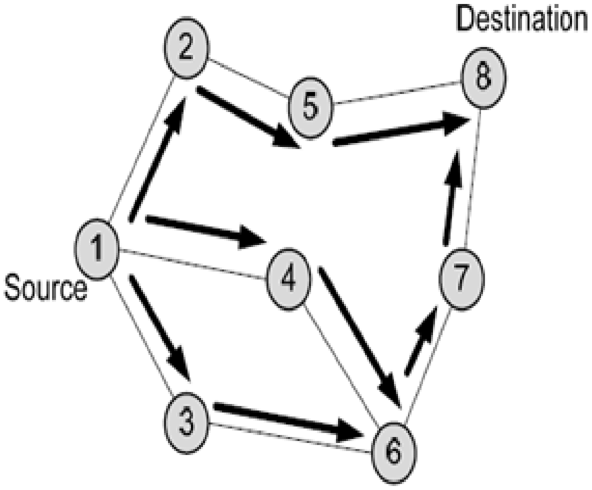

Figure 2: Propagation of the RREQ

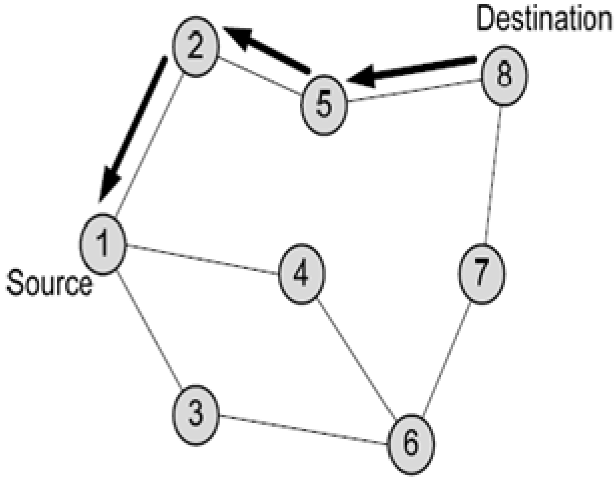

Figure 3: Propagation of the RREP

2.1 AODV Route Discovery

AODV uses route discovery by broadcasting RREQ to all its neighbouring nodes. The broadcasted RREQ contains addresses of source and destination, their sequence numbers, broadcast ID and a counter, which counts how many times RREQ has been generated from a specific node. When a source node broadcast a RREQ to its neighbours it acquires RREP either from its neighbours or that neighbour(s) rebroadcasts RREQ to their neighbours by increment in the hop counter. If node receives multiple route requests from same broadcast ID, it drops repeated route requests to make the communication loop free.

2.2 AODV Route Table Management

Routing table management in AODV is needed to avoid those entries of nodes that do not exist in the route from source to destination. In AODV Managing routing table information handled with the destination sequence numbers.

2.3 AODV Route Maintenance

When nodes in the network detects that a route is not valid anymore for communication it delete all the related entries from the routing table for those invalid routes. And sends the RREP to current active neighbouring nodes that route is not valid anymore for communication. AODV maintains only the loop free routes.

3. ICMP INTERNET CONTROL MESSAGE PROTOCOL

ICMP is a protocol within the TCP/IP stack that exists basically to provide control, troubleshooting, and error messages. It runs over IP. ICMP transmits error and control messages about the network situation between systems [4]. Two specific instances of the ICMP are the ICMP ECHO_REQUEST and ICMP ECHO_RESPONSE datagrams. These two instances can be used by a host to determine whether a remote system is reachable via the network.

4. LITERATURE SURVEY

In this chapter, a brief account has been put forth of the available literature that has been studied extensively. Considering the deterministic underlying AODV protocol parameters and MANETs, we collected additional knowledge of AODV for small MANETS and its applications through the literatures in order to make improved performance.

[EAACK- A Secure Intrusion-Detection system for MANETs] Elhadi M, 2013 thepaper propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgement (EAACK). It demonstrates higher malicious behaviour detection rates while does not greatly affect the network performances.

[A Co-Operative Intrusion Detection System inMobile Ad-Hoc Network]S.S.Chopade (2011) the author has proposed an IDS that should run continuously and not only detect but also respond to detected intrusions without human intervention. They havesimulated the various possible attacks on the wireless network system like the RESOURCE CONSUMPTION, NODE ISOLATION ROUTE DISRUPTION etc. then they have checked the performance of the network before and after the attack using various parameters like Simulation duration, Topology Number of mobile Nodes, Transmission range, Node movement model, Traffic type Data payload.

[MANET: Selfish Behavior on Packet Forwarding]byDjamelDjenouri, (2008) Thepaper deals with the problem of selfishness on packet forwarding in MANET and sketch the solutions currently proposed to mitigate this problem. It describes the limitation in energy resources along with the multi-hop nature of mobile ad hoc networks (MANETs)causes a new vulnerability that does not exist in traditional networks. To preserve its own battery, a nodemay behave selfishly and would not forward packets originated from other nodes, while using their servicesand consuming their resources.

[Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS)]Naveen Kumar Gupta, (2012) the paper provides the comparison study of different types of methods to increase the Selfish node detection rate and decrease the false detection rate. Finally, it proposesa model that was developed due to simulation of all these methods to increase the Selfish node detection rate and decrease the false detection rate and thus increase the efficiency of the system.

[Impact of Selfish Node Concentration in MANETs] Shailender Gupta, (2011) this paper studies the impact of selfish nodes concentration onthe quality of service in MANETs.A selfish node is one that tries to utilize the network resources for its own profit but is reluctant to spend its own for others. If such behaviour prevails among large number of the nodes in the network, it mayeventually lead to disruption of network**.**

[Performance analysis of Leader Election Algorithms in Mobile Ad hoc Networks] Muhammad Mizanur, (2008) The Author has explained the process of electing the Leader Node. It has described the leader election algorithm LEAA. The elected leader should be the most valued node among all the nodes of the network. The Value for the leader node selection is a performance related characteristics such as remaining battery life or computational capabilities.

[Intrusion Detection in MANETs] Prof. Mrs. Poonam Gupta, 2013 The paper first survey various attacks, problems and solutions in MANET, then proposes the intrusiondetection system which can find out misbehaving link in reliable manner and in short time also IDS implemented onthat node is also reliable. Here they remove the misbehaving node to avoid the future damage in the network.

[**Detection of false alarm in handling of selfish nodes in MANET with congestion control] I.Shanthi, (2013)**The author explores theimpression of selfish nodes in a MANET from theperspective of replica allocation and developed selfish node detection algorithm that considers the partial selfish node and fully selfish node as selfish replica allocation.The replica will be allocated using specific SCF treeconcept. An alarm will be raised based on the selfishbehaviour of overall nodes called overall selfishnessalarm.

[Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes]MarjanKuchaki Rafsanjani (2008) The author classify the architecture for Intrusion detection systems that have sofar been introduced for MANETs, and then existing intrusiondetection techniques like watchdog, Pathrater, Confident etcin MANET are presented and compared.

5. ATTACK CLASSIFICATIONS

Intrusion detection is a new and rapidly developing area and it has become an important issue in network security. Intrusion detection systems are hardware or software mechanisms that detect and logs inappropriate, incorrect, or anomalous activity for further investigation. Attacks by intruders cause unauthorized use of wireless network so that the whole network will be suffered from packet losses.

Attacks in MANET can be categorized according to their consequences as the following:

1. **Black hole:** All trace is redirected to a specific node, which may not forward any trace at all.

2**. Routing Loop:** A loop is introduced in a route path.

3. **Selfishness:** A node is not serving as a relay to other nodes.

4. **Denial-of-Service:** A node is prevented from receiving and sending data packets to its destinations.

These are prone to phenomenal attacks like development of selfish nodes due to resource constraints or other malicious contents.

6. MODELLING AND SIMULATION

The OPNET [14] provide better modelling and simulate the network in the area of networks specially wired and wireless. OPNET has been used to model the wireless networks (MANETS) and implement the selfish node attack through ICMP protocol by importingAODV Protocol. TheICMP Attack model ofAODV protocol shown in figure 4 can also be used to evaluate adhoc routing in environments that support the constant bit rate (CBR) traffic.

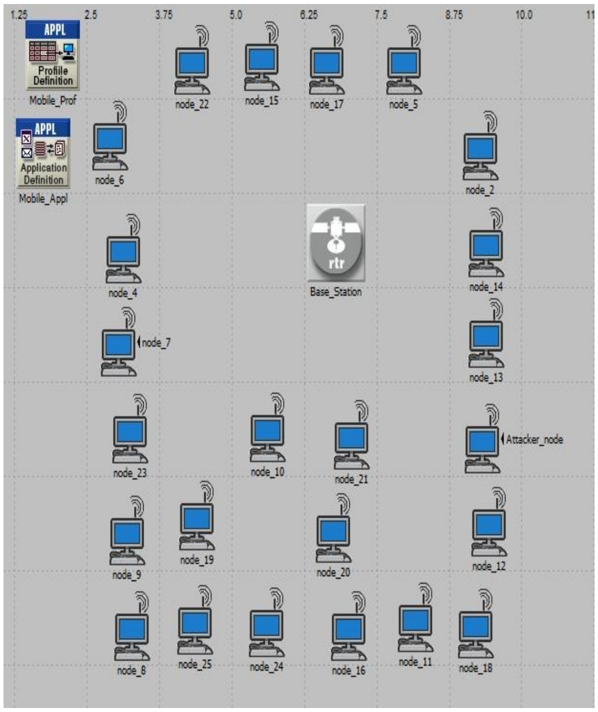

Figure 4: ICMP Attack Model

The simulation models allow ICMP Attack evaluation of important performance measures such as delay and network load.The 24 nodes are placed randomly ina rectangular simulation area. The attacker also interprets in this simulation area to access the important information. Thus, the packets drop on the wireless link and it directly affects the overall network scenario.

7. RESULTS AND DISCUSSIONS

6.1 Load and Network delay

We analysed the load distribution in thenetwork in order to get more information about theworking behaviour of ICMP Attack and to identify Network delay shown in figure 5 and 6. In figure 5 depicted that 12 s simulation pattern increases the network load utilization up to 100 percent. This means it directly affects the resources, memory and power levels of the wireless networks. As depicted in figure 6 network delay inversely proportional to the network load. As the load increases in the network scenario the delay increases per routing payload. The number of unnecessary routing requests increases towards base station and overall performance of the network exponentially down.

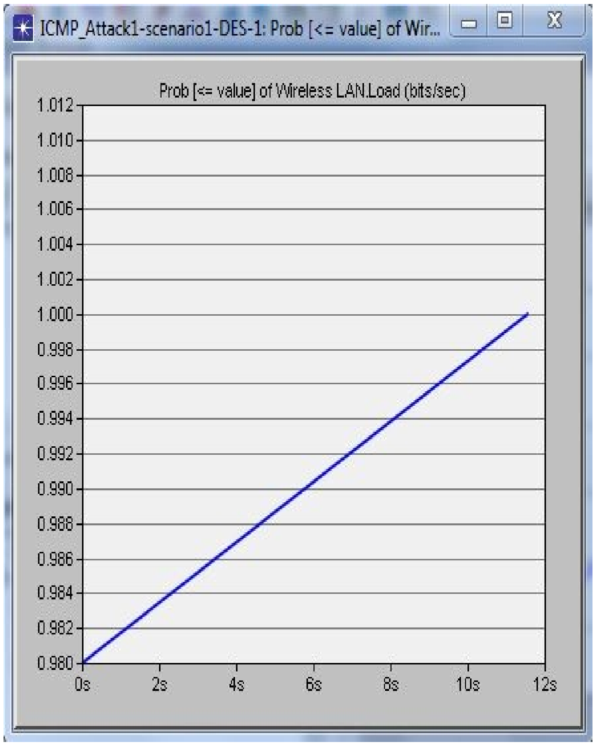

Figure 5: Network Load

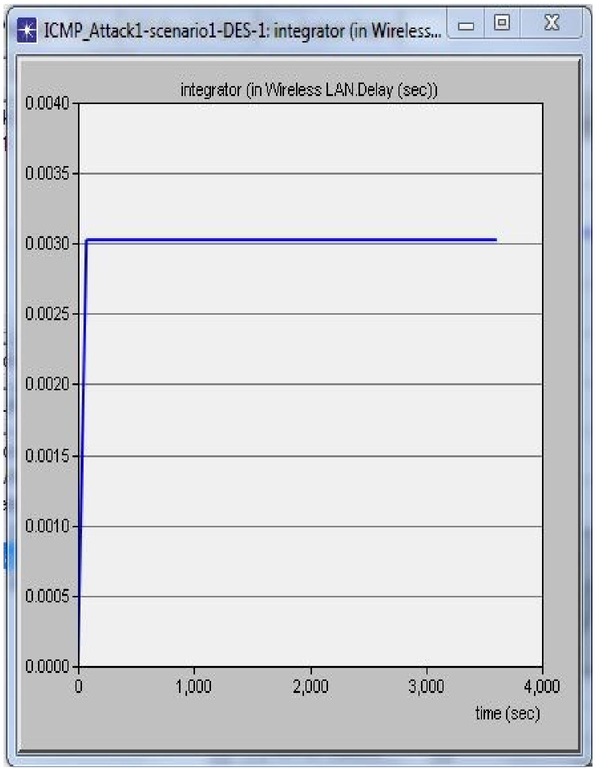

Figure 5: Network Delay

8. CONCLUSION

We classified the number of attacks in the mobile ad hoc networks that degrade the performances. The selfishness attack access the useful information from the network. The paper explores the ICMP (Internet control message protocol) attack from the selfish node accesses important information from the neighbouring machine, or it creates virtual path to the victim node. This attack degrades the performances of the network with increase of network load and delay.

REFERENCES

[1]Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-DetectionSystem for MANETs" IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, 2013,pp 1089-1098.

[2] S.S.Chopade, Prof.N.N.Mhala, "A Co-Operative Intrusion Detection System in Mobile Ad-Hoc Network",IJCA, 2011,pp.34-39.

[3]Naveen Kumar Gupta, Ashish Kumar Sharma, Abhishek Gupta,"Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS) IJRREST, 2012,pp 31-34.

[4]Shailender Gupta, C. K. Nagpal, CharuSingla," Impact Of Selfish Node Concentration In Manets",IJWMN,2011,pp.29-37.

[5] Shruti, Umang, Prof.B.V. R. Reddy, Prof. M.N. Hoda, "Analytical Study of Existing Methodologies of IDS for False Alarm Rate - A Survey and Taxonomy",IJEATE,2012,pp.393-399.

[6]MeeraGandhi,S.K.Srivatsa, "Detecting and preventing attacks using network intrusion detection systems",IJCSS,pp.49-60.

[7] Chun-Ta Li,Chou-Chen Yang,"A secure routing protocol with node selfishnessresistance in MANETs",International journal of Mobile Communications,2012,pp.103-118.

[8] DjamelDjenouri, Nadjib Badache, “MANET: Selfish Behavior on Packet Forwarding” Encyclopaedia of Wireless and Mobile Communications,2008,pp.576-587.

[9] Prof. Mrs. Poonam Gupta1, Mrs. Mugdha Kirkire, “Intrusion Detection in MANET” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 4, April 2013 pp 1532-1540.

[10] I.Shanthi, D. SornaShanthi, "Detection of false alarm in handling of selfish nodes in MANET with congestion control",IJCSI,2013,pp.449-457 .

[11] Marko Jahnke, Jens Toelle, Elmar Gerhards-Padilla,et.al.,"Methodologies and Frameworks for Testing IDS in AdhocNetworks",ACM,2007

[12] Muhammad Mizanur Rahman,” Performance analysis of Leader Election Algorithms in Mobile Ad hoc Networks”,IJCSNS,2008, pp 257-263.

[13] http://tools.ietf.org/html/rfc5927.

[14]www.opnet.com