Study of Protocols (AODV, DSR)Of MANET(Mobile ad-hoc network)& Black hole attack inAODV

Miss. Bhandare A. S[1], Dr.Mrs. Patil S.B[2]
[1]*Dept of E&Tc ,Dr. J.J.Magdum COE, Jaysingpur,Tal-Shirol,Dist-Sangli, India*
[2]*Head,Dept of electronics Engg, Dr. J.J.Magdum COE, Jaysingpur,Tal-Shirol,Dist-Sangli, India*

Abstract-*Mobilead-hocnetwork (MANET) is an autonomous system ofmobile nodes connected by wireless links. Due to Open medium, dynamic topology, Distributed Cooperation, ad-hoc networks are vulnerable to many types of security attacks. Black hole attack is one of the severe security threatswhich can be easily employed by exploitingvulnerability of on-demand routing protocols such as AODV.In this paper, we have discussed two routing protocols-AODV and DSR and Intrusion Detection using Anomaly Detection (IDAD) toprevent black hole attacks imposed by both single and multipleblack hole nodes in AODVwhich helps to maximize network .*

Keywords-*Ad-hoc, Anomaly detection AODV, Blackhole*

I. INTRODUCTION

A mobile ad-hoc network is a self organizing networkthat consists of mobile nodes that are capable ofcommunicating with each other without the help of fixed infrastructure orany centralized administration. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes.On the contrary to traditional wired networksthat use copper wire as a communication channel, ad-hocnetworks use radio waves to transmit signals.Mobility, an advantage of wireless communication, givesa freedom of moving around while being connected to anetwork environment. Ad-hoc networks are so flexible thatnodes can join and leave a network easily. But this flexibilityof mobile nodes results in a dynamic topology that makes itvery difficult in developing secure ad-hoc routing protocols.Security being a serious issue, the nature of ad-hoc networks makes them extremely vulnerable to adversary's malicious attacks. First of all, the use of wireless linksrenders a mobile ad-hoc network to be vulnerable to attacks of various types - black hole attack being one of them.The use of wireless links, lack of fixed infrastructure and the characteristic of dynamic topology associated with ad-hoc networks make it impossible to use wired network security mechanism as is.

II. Routing Protocol

An ad-hoc routing protocol is a convention, or standard, that controls how nodes decide which wayto route packets between computing devices in a mobile ad-hoc network.The primary goal of routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. The currently available routing protocols for MANETs are mainly categorized into proactive, reactive and hybrid routingprotocols [4]. In a proactive routing protocol, every node proactively searches for routes to other nodes, andperiodically exchanges routing messages, in order to ensure that the information in the routing table is up-to-date andcorrect, such as DSDV (Destination Sequence Distance Vector) and OLSR (Optimized Link State Routing Protocol. In a reactive routing protocol,aroute is searched and established only when two nodes intend to transfer data; and therefore, it is also called an on-demand routing protocol, such as AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing)[7][5].A source node generally broadcasts a route request message to the entire network by means of flooding, in order to search for and establish a route to the destination node.Wireless hybrid routing is based on the idea of organizing nodes in groups and then assigning nodes differentfunctionalities inside and outside a group.

2.1 Ad-hoc on Demand Distance Vector (AODV)

AODV is a purely reactive routing protocol.In an ad-hoc network that uses AODV [1] as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) Messageto find a fresh route to a desired destination node.This process is called route discovery. Every neighboring node that receives RREQ broadcast first saves the path theRREQ was transmitted along to its routing table.

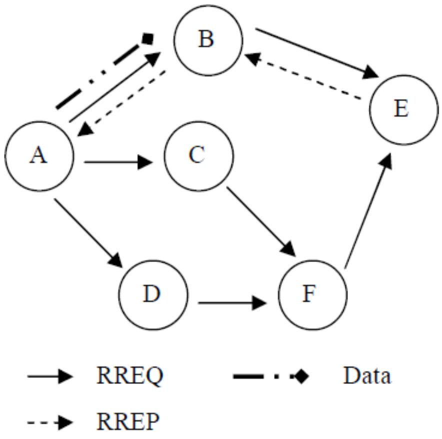

Fig 1. Propagation of RREQ and RREP from A to E

It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQMessage.The freshness of a route is indicated by adestination sequence number that is attached to it. If a node finds a fresh enough route, it unicasts an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise. The sameprocess continues until an RREP message from the destination node or an intermediate node that has fresh routeto the destination node is received by the source node

2.2 Dynamic Source Routing (DSR)

2.2.1 Basic Operation

Each node in the network maintains a *route cache* inwhich it caches the routes it has learned. To send data toanother node, if a route is found in its route cache, thesender puts this route (a list of all intermediate nodes) inthe packet header and transmits it to the next hop in thepath. Each intermediate node examines the header andretransmits it to the node indicated after its id in thepacket route. If no route is found, the sender buffers thepacket and obtains a route using the route discoveryprocess described below .

2.2.2 Route Discovery and Maintenance

To find a route to its destination, a source broadcasts a*route request* packet to all nodes within its radiotransmission range. In addition to the addresses of thesource and the destination nodes, a route request packetcontains a *route record,* which is an accumulated recordof nodes visited by the route request packet. When anode receives a route request, it does the following.

If the destination address of the request matches itsown address, then it is the*destination.* The route record in the packet contains the route by which therequest reached this node from the source. This route is sent back to the source in a *route reply* packet by following the same route in reverse order. (We assume bidirectional links. The alternative reply mechanism for unidirectional links is not considered here.)

Otherwise, it is an *intermediate* node. If the node has not seen this request before and has a route to the destination in its cache table, it creates a route reply packet with the route from its cache, and sends it back to the source. Such replies are called Intermediate-Node replies; if it does not have a route, it appends its own address to the route record, and increments hop count by one, and rebroadcast the request. When the source receives a route reply, it adds this route to its cache and sends any pending data packets. If any link on a source route is broken (detected by the MAC layer of the transmitting node), a *route error* packet is generated. The route error is unicasted back to the source using the part of the route traversed so far, erasing all entries that containthe broken link in the route caches along the way.

III. Black hole attack in AODV

A Black Hole attack [1], is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorbs them without forwardingthem to the destination.In the following illustrated fig.1, imagine amalicious node ‘M’. When node ‘A’broadcasts aRREQ packet, nodes‘B’ ‘D’and ‘M’ receive it. Node ‘M’, being a malicious node, does not check up with its routing table for the requested route to node ‘E’. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node ‘A’ receives the RREP from ‘M’ ahead of the RREP from ‘B’ and ‘D’.

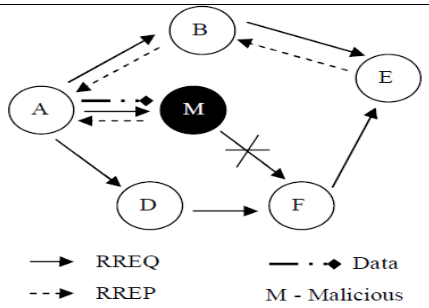

Fig.1. Black hole Attack in AODV

Node 'A' assumes that the route through 'M' is theshortest route and sends any packet to the destinationthrough it. When the node 'A' sends data to 'M', itabsorbs all the data and thus behaves like a 'Blackhole'**.**

IV.Existing Techniques of Preventing Black Hole Attack in Mobile Ad-Hoc Networks

- Researchers have proposed various techniques to prevent black hole attack in mobilead-hoc networks..LathaTamilsel van and Dr.VSankaranarayanann[1] have purposed a solution to prevent block hole attack**.**Through simulation study they showed that the protocol provides better performance than the conventional AODV in the presence of Black holes. It have disadvantage of time delay, since source node has to wait for other route replies and it cannot detect cooperative black hole attack. Medadian, M.; Mebadi, A.; Shahri, E.[2], have proposed solution through the judgment process by using honesty of a nodes, which is derived from the opinions of a neighbor nodes of a node in a network. When a node collects all opinions of neighbors, it decides if the replier is a malicious node or not. But it takes the help of opinions for neighboring nodes but it may not be always correct and also not works on Co-operative node.H.Weerasinghe and H.Fu [3], introduces the use of DRI (Data Routing Information) to keep track of past routing experience among mobile nodes in the network and crosschecking of RREP messages from intermediate nodes by source nodes. The main drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table which wastes memory space and consuming a significant amount of processing time which contributes to slow communication. P. Raj and P. Swadas [5], proposed an adequate solution by checking RREP messages from intermediate nodes for possible intrusion activities. This technique is successful based on the assumption of cooperation between nodes. If a mobile node discovers a possible attack by an intruder, the discovering node notifies all other nodes the presence of an attack by broadcasting an ALARM message. This process takes a considerable amount of time to notify all nodes for a large network in addition to the network overhead that can be caused by ALARM broadcast**.N.Mistry, D. Jinwala, M.Zaveri**,[6] have proposed a solution, where source node stores all the RREPs in the table, analyses them and discard the RREPs having a very high destination sequence number. To maintain freshness, it is flushed once as RREP is chosen from it. Every node stores the malicious node details to isolate the malicious node in the network. This solution has high processing delay.

V .Intrusion Detection Using Anomaly Detection (IDAD)

Intrusion Detection Systems (IDS) [9] are one of the main techniques utilized to prevent attacks against security threats. Intrusion detection is a process of detecting an adversary and preventing its subsequent actions. IDS can be classified as Network-based and Host-based. Network-based IDS can be installed on data concentration points of a network such as switches and routers. Where as Host-based IDS are installed on hosts so that they can supervise the activities of a host and users on the host. As mobile ad-hoc networks where there is no central device that monitors traffic flow, it followsHost based IDS schema.IDAD assumes every activities of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomaly activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. To do so an IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. In a black hole attack, a malicious node sending a fake RREP message [10]. Fake RREP messages from a malicious node contain the following parameters:

- **maximum destination sequence number** - to make the route up to date
- **single hop-count** - to make a route with the shortest path
- **life-long route** - informs a route will exist as long as the network
- **destination IP address** - address of the destination node copied from RREQ

- **time-stamp** - the time the RREP was generated

These entries of an RREP message from a malicious node can be collected as audit data to differentiate anomaly activities from normal activities.Once audit data is collected and is given to the IDAD system, the IDAD system is able to compare every activity of a host with the audit data on a fly. If any activity of a host (node) resembles the activities listed in the audit data, the IDAD system isolates the particular node by forbidding further interaction. Furthermore, IDAD works in a principle that trusts no peer. This means mobile nodes do not rely on other nodes to prevent intrusions.

VI. Simulation

The current simulation research of implementing IDAD toenable AODV with a security mechanism will be carried out using NS2[10].The network simulator ns-2 is discrete event simulation software for network simulations which means it simulates events such as sending, receiving, forwarding and dropping packets. Ns-2 is written in C++ programming language and Object Tool Common Language (OTCL). To run a simulation with ns-2.34, the user must write the simulation script in OTCL, get the simulation results in an output trace file. Ns-2 also offers a visual representation of the simulated network by tracing nodes movements and events and writing them in a network animator (NAM) file.

6.1Metrics

The following metrics can beused to evaluate the performance.

- ***Number of data packets sent***-Itis the number of data packets that are sent by a source node
- ***Number of data packets received-*** It is the number of data packets received by a destination node
- ***Number of routing packets***-Itis the number of routing packets (AODV packets in this case) that are generated during simulation time.
- ***Packet Delivery Ratio***: The ratio between the numbers of packets originated CBR sources and the number of packets received by the CBR sink at the final destination
- ***Normalized routing load:*** It***is*** the ratio of routing packets over received data packets
- ***Average End-to-End Delay***:This is the average delay between the sending of the data packet by theCBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused duringroute acquisition, buffering and processing at intermediate nodes, retransmission delays etc. It is measured in milliseconds.

VII. Conclusion

With development incomputing environments, the servicesbased on Ad Hoc Networks have beenincreased. In this paper we have studied the two main routing protocols –AODV and DSR .Wireless Ad Hoc Networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. One type of attack, the black hole, which can easily be deployed against the MANET, is described and the self protection (no peer trust) principle of IDAD which effectively prevents a black hole attack regardless of thenumber of black hole nodes is explained. As future work, we intend to develop simulations to analyze the performance of the routing protocols and proposed solution based on various parameters like packet delivery ratio (PDR), average End-to-End delay, routing load, and throughput.

References

[1**Tamilselvan,L.;Sankaranarayanan V.**, "*Prevention of Blackhole Attack in MANET" Wireless Broadband and Ultra Wideband Communications, 2007.* Aus Wireless 2007. The 2nd International Conference on, pp.21, 27-30 Aug. 2007

[2] Medadian M.;Mebadi,A.; Shahri, E.,"*Combat with Black Hole attack in AODV routing protoco", Communications (MICC),2009* IEEE 9th Malaysia International Conference on, pp.530-535, 15-17, Dec.2009**.**

[3] **H. Weerasinghe and H. Fu**, "*Preventing cooperative black hole attacks in mobile ad-hoc networks: simulation, implementationandevaluation*," International Journal of Software Engineering and Its Applications, *Vol. 2, No. 3* (2008) pp. 39-54.

[4] **K. Lakshmi et al**, "*Modified AODV Protocol against BlackholeAttacks in MANET"*International Journal of Engineering and Technology *Vol.2 (6), 2010, 444-449*

[5]**Payal N Raj1 and Prashant B. Swadas2**, *"DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET"*, IJCSI International Journal of Computer Science Issues, *Vol. 2, 2009*

[6] NitalMistry, Devesh C Jinwala, MukeshZaveri,, "*Improving AODV Protocol against Blackhole Attacks",* proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 *Vol II,* IMECS 2010

[7]**V.Taksande, Dr.K..Kulat,***"Performance Comparison of DSDV, DSR, AODV Protocol with IEEE 802.11 MAC for Chain Topology for Mobile Ad-hoc Network using NS-2" IJCA Special Issue on "2nd National Conference- Computing, Communication and Sensor Network" CCSN, 2011*

*[8]***R. Boppana, A.Mathur***"Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks"* Workshop on Next Generation Wireless Networks, *December 2005*

[9] **Alem, Y.F.; Zhao Cheng Xuan**; , *"Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection,"* Future Computer and Communication (ICFCC), 2010 *2nd International Conference on , vol.3, no., pp.*V3-672-V3-676, 21-24 May 2010.

Theses

[10] S. Dokurer "*Simulation of black hole attack in wireless ad-hoc networks*," Master thesis, September 2006, Atilim University, Turkey**.**