Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network

Romina Sharma
SRIT Jabalpur
Jabalpur, India

Rajesh Shrivastava
SRIT Jabalpur
Jabalpur, India

Abstract
A Wireless ad-hoc network is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. In this research paper we modify the working of AODV routing protocol to prevent black hole attack. So we investigate the performance impact of a blackhole attack on a mobile ad hoc network and compare it with our modified AODV routing protocol. The simulation work is carried out by OPNET Modeler. To analyze performance of our proposed algorithm we use performance metrics ex. Network throughput, network load, packet send and received, packet dropped and end-to-end delay.

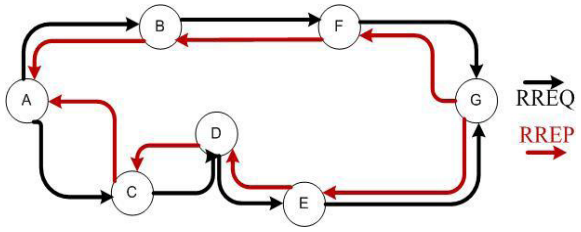
Keywords
Wireless Ad-hoc Network, Black Hole Attack, Simulation, Security, AODV, OPNET

I. Introduction

A Mobile Ad Hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure. Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. An ad hoc network uses no centralized administration. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to enter and leave the network as they wish. Because of the limited transmitter range of the nodes, multiple hops are generally needed to reach other nodes. Every node in an ad hoc network must be willing to forward packets for other nodes. Thus, every node acts both as a host and as a router. The topology of ad hoc networks varies with time as nodes move, join or leave the network. This topological instability requires a routing protocol to run on each node to create and maintain routes among the nodes.

II. AD-HOC ON DEMAND ROUTING (AODV) PROTOCOL AND BLACK HOLE ATTACK

1. The Ad hoc On-Demand Distance Vector (AODV) is a routing protocol. AODV is designed for ad hoc mobile networks and of both routing, that is unicast and multicast routing. AODV establish routes between different nodes as needed by source nodes. There are three messages which are defined by AODV. These messages are Route Errors (RERRs), Route Request (RREQs) and Route Replies (RREPs). For discovering and maintaining routes in the network these three messages are used, by using UDP packets from source to destination. A node uses its IP address as the source address in the IP header of a message when it request for a route, and for broadcast 255.255.255.255. Route Request Message RREQ Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted. Route Reply Message RREP A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node. Route Error Message RERR Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, Route error (RERR) message is generated by the node in order to notify other nodes that the link is down.



Manuscript received March 5, 2014
Manuscript revised March 20, 2014

Figure 1. AODV Route Discovery

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating destination node i.e. from node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error. The scheme is shown in the Fig.2.3 bellow.

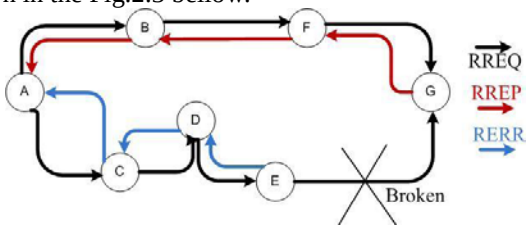


Figure 2. Route Error Message in AODV

2. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address. The method how malicious node fits in the data routes varies. Fig. 4.1 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

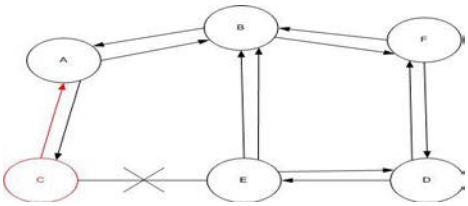


Figure 3. Black Hole Problem

III. RELATED WORK

H.Weerasinghe and H. Fu 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. It is evident that maintaining past routing experiences wastes memory space as well as consuming a significant amount of processing time which contributes to slow communication .The second drawback is over consumption of limited bandwidth.

P. Raj and P. Swadas , 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. Generate a token, which is appended to the data packets to identify the authenticity of the routing packets and to choose correct route for data packets. TRP provides significant reduction in energy consumption and routing packet delay by using hash algorithm.

Balakrishnan *et al.* propose a mechanism to defend against flooding and packet drop attacks in MANETs. They present an obligation-based model called fellowship and describe how this model can be used to identify and penalize malicious and selfish nodes. Zhang and Lee propose a distributed and cooperative intrusion detection model based on statistical anomaly detection techniques. In the intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and confirmation message, the source determines the validity of path according to its policy.

Juwad and Al-Raweshidy presents an experimental performance comparison between Secure-AODV (SAODV) and AODV. They claim that there has been a lack of performance and security analysis in real network test-beds. A quantitative performance comparison between routing protocols AODV and SAODV is presented in an experimental test-bed and using the OPNET network simulator. These results show that SAODV is more effective in preventing two types of attacks (control message tampering and data dropping attacks) than AODV.

Chen *et al.* quantitatively evaluate an approach detailing network survivability in wireless ad-hoc networks. They define network survivability as a combination of network failure impacts and failure durations and use a performance metric called excess packet loss due to failures.

IV. MODIFIED AODV PROTOCOL TO PREVENT BLACK HOLE ATTACK

In our proposed work we modify the AODV protocol to prevent black hole attack. The solution that we propose here, basically, modifies the working of AODV protocol by adding next hop information in the RREP message and two other control messages including further route request (FRREQ) and Further route reply (FRREP).Once the source receives RREP with next hop information it broadcasts Further RREQ message to next hop nodes to the received RREPs and then next hop nodes reply back with Further RREP message to source node. After receiving FRREP source node routes data packets to the destination with the shortest path. If the node is black hole node the next hop of its does not exists so it never receives FRREQ and not reply FRREP to the source node so source node never send data to path suggest by black hole node.

Steps of the proposed algorithm

1: Source node broadcasts RREQ
2: Source node receives RREPs with next hop information from nodes
3: Source node fetch next hop information from RREPs received
4: Source node send further route request (FRREQ) to all next hop nodes
5: if (next hop node is of black hole) {
FRREQ will not reach to next hop node and no FRREP will send to source
} else {
FRREQ will reach to all reliable next hop nodes and FRREP is send to source by these reliable next hop nodes }
6: Source node now receives FRREPs from reliable nodes; it will update its routing table
7: Source node routes data packets to the destination

V. SIMULATION RESULTS

Our simulation model was carried out using the OPNET Modeler 14.0. It is a useful research tool for achieving good simulation results. Each cycle of the simulation runs for 20 minutes. The simulated network consists of 20 randomly allocated nodes in a space of 1000*1000 square-meters .In order to compare the performance of our proposed algorithm – three scenarios are created .In first scenario we have 20 reliable nodes without any blackhole node and prevented algorithm. .In second scenario again we have 20 nodes but with one black hole node and no prevention algorithm. In third scenario we have the same 20 nodes with one blackhole node and with our proposed algorithm. All scenarios are run under identical mobility and traffic conditions. The performance metrics chosen for the evaluation of our algorithm with black hole were total packet dropped, traffic sent and received, wireless end to end delay, network throughput and network load.

These performance metrics is defined below-

Total packet dropped: When no route is found to the destination, the node drops the packets queued to the destination. This statistic represents the total number of application packets discarded by this node. This statistic is collected in the bucket mode with the "Sum" of the values within the bucket by default.

Total traffic sent: Total number of MANET packets sent per second by this node to other MANET nodes in the network.

Total traffic received: Total number of MANET packets received per second by this node from all other MANET traffic sources in the network.

End to end delay: It represents the end-to-end delay of all the data packets that are successfully received by the WLAN MAC and forwarded to the higher layer.

Throughput: Throughput is the average rate of successful message delivery over a communication channel. Throughput is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is calculated according to this formula: Throughput = Packets Received / Packets Sent.

Network load: It is the total traffic received by the entire network from higher layer of MAC which is accepted and queued for transmission. It indicates the quantity of traffic in entire network. It represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission. It does not include any higher layer data traffic rejected without queuing due to large data packet size.

The network topology graph for 20 nodes is shown below follow with three scenarios simulation result.

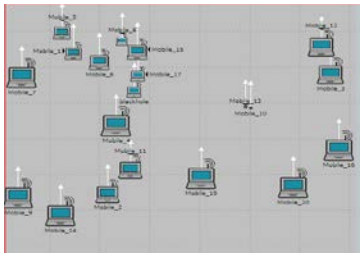


Figure 4. Network topology

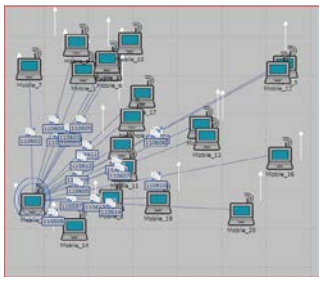


Figure 5. Simulation Animation Graph

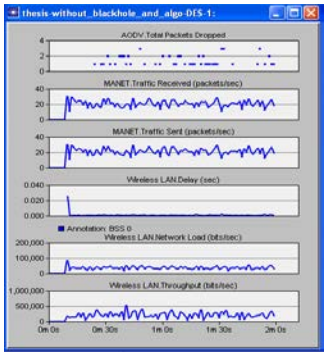


Figure 6. First Scenario results without black hole and proposed algorithm

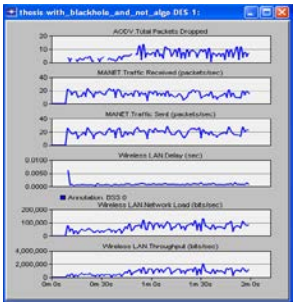


Figure 7. Second Scenario results with black hole but no prevention algorithm

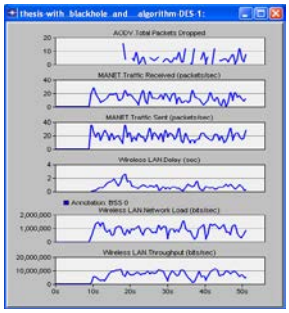


Figure 8. Third Scenario results with black hole and prevention algorithm

VI. CONCLUSION

Mobile Ad Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our research work we proposed a feasible solution for the AODV protocol. The proposed solution can be applied to prevent single black hole nodes in a MANET; also we showed the effect of delay, network load and Throughput of our proposed algorithm. There is reduction in Packet Delivery Ratio and Throughput .The consequences of this algorithm are that it only prevents single node black hole, co-operative black hole attack can not be prevented. The routing overhead also increases because of two extra control messages.

Acknowledgment

I express my heartfelt gratitude to all the staff members of computer science engineering department SRIT Jabalpur and my family and friends and also to each and every individual who was associated with my project work, including those whom I may have inadvertently failed to mention.

References

[1] Yibeltal Fantahun Alem , Zhao Cheng Xuan ,"Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" 2010 2nd International Conference on Future Computer and Communication.V3-672

[2] Rajib Das, Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach" International Journal of Engineering Science and Technology (IJEST). ISSN : 0975-5462 Vol. 3 No. 4 Apr 2011

[3] Razan Al-Ani ,"Simulation and Performance Analysis Evaluation for Variant MANET Routing Protocols" International Journal of Advancements in Computing Technology, Volume 3, Number 1, February 2011

[4] Shree Om, Mohammad Talib ,"Wireless Ad-hoc Network under Black-hole Attack" International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 628-633

[5] Abderrahmane Baadache, Ali Belmehdi, " Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks" International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010

[6] Shervin Ehrampoosh, Ali Khayatzadeh Mahani ,"Secure Routing Protocols: Affections on MANETs Performance" 1st International conference on communication engineering

[7] IRSHAD ULLAH, SHOAIB UR REHMAN ,"Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols" School of Computing Blekinge Institute of Technology, Sweden

[8] Thodeti Srikanth, Dr.V.B.Narsimha, "Simulation-based approach to performance study of routingprotocols in MANETs and ad-hoc Networks" International Journal of Computer Science and Network Security, VOL.11 No.9, September 2011

[9] Abdalla Ahmed Fekry Mahmoud ," Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN)" The American University in Cairo School of Sciences and Engineering

[10] OPNET Tutorial http://www.ensc.sfu.ca/research/cnl School of Engineering Science Simon Fraser University