Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced AODV Routing Protocol against Black hole Attack

Neeraj Saini[#1], Lalit Garg[*2]
[#]CSE Department, KUK University
Haryana, India
*CSE Department, KUK University
Haryana, India

Abstract- MANET is a self-configuration wireless ad-hoc network of mobile nodes. Each node has a router or a switch connected by the wireless connection. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Wireless MANET is specific vulnerable due to its fundamental characteristics such as open medium, dynamic topology, spread cooperation and constrained ability. So security in MANET is a difficult issue. In this Paper ,therefore, we have examined the effects of Black hole attack on mobile ad hoc routing protocols and improving the security of the Adhoc On Demand Distance Vector (AODV) routing protocol against the Blackhole Attack. The proposed solution is capable of detecting and removing black hole nodes in the MANET at the starting stage itself without any delay and packet loss in the network.

Keywords - MANET, Dynamic, Security, AODV, Blackhole.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. As mobile nodes are not controlled by any other controlling entity, they have free mobility and connectivity to others. Nodes in the Network also act as router. The routers move freely and organize themselves randomly. The network topology may change quickly and spontaneously. Such a network may run in an individual way or may be connected to the Internet. Routing protocol AODV with blackhole and modified AODV have been discussed in this paper.

1.1 MANET CHALLENGES

1) Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
2) Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.
3) Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.
4) Hidden terminal problem: The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

1.2 ROUTING PROTOCOLS

MANET routing protocols are categorized into three main categories depending upon the criteria when the source node possesses a route to the destination, as shown in figure 1.

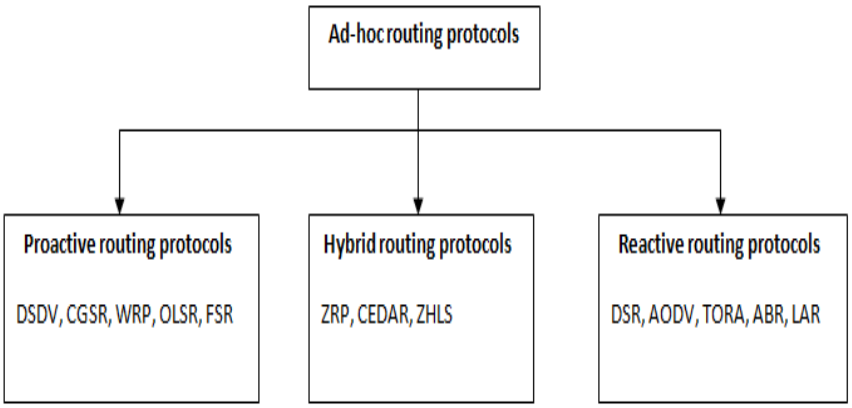


Figure 1 Classification of MANET Routing Protocols

- Table driven/ Proactive
- Source initiated (demand driven) / Reactive
- Hybrid

1.3 AODV ROUTING PROTOCOL

AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbours, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself. Each intermediate node receiving the RREQ, makes an entry in its routing table for the node that forwarded the RREQ message, and the source node

The destination node or the intermediate node with a fresh enough route to the destination node, unicast the Route Response (RREP) message to the neighbouring node from which it received the RREQ. An intermediate node makes an entry for the neighbouring node from which it received the RREP, then forwards the RREP in the reverse direction. On receiving the RREP, the source node updates its routing table with an entry for the destination node, and the node from which it received the RREP. The source node starts routing the data packet to the destination node through the neighbouring node that first responded with an RREP.

1.4 BLACKHOLE ATTACKS

A Blackhole attack is one of the active DoS attacks possible in MANETs. In this attack, a malicious node sends a *false* RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbor to the actual destination node. In such a case, the source node would forward all of its data packets to the malicious node, which originally were intended for the genuine destination.

The malicious node, eventually may never forward any of the data packets to the genuine destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other [6].Since AODV treats RREP messages having higher value of destination sequence number to be fresher, the malicious node will always send the RREP having the highest possible value of destination sequence number. Such RREP message, when received by source node is treated afresh, too. The fallout is that there is a high probability of a malicious node attempting to orchestrate the Blackhole attacks in AODV.[1]

II. RELATED STUDY

[1] Nital Mistry et. al. has proposed an algorithm to counter Blackhole attack against the AODV routing protocol. observed that the proposed modification to secure AODV is indeed effective in preventing the Blackhole attacks with marginal performance penalty. A Blackhole attack is one of the active DoS attacks possible in MANETs. In this attack, a malicious node sends a *false* RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbour to the actual destination node

[2] Jaspal Kumar et. al. In this paper we have analyzed the effects of Black hole attack on mobile ad hoc routing protocols. Mainly two protocols AODV and Improved AODV have been considered. Simulation has been performed on the basis of performance parameters and effect has been analyzed after adding Black-hole nodes in the network. It is an enhanced version of AODV and is hybrid in nature

[3] Sarita Choudhary et.al. In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes by using OPNET network simulator 14.5; it is the latest version of simulation software. Basically, OPNET allows you to build a network with a range of simulated "real-life" equipment, so different configuration options can be tested. And considering two different networks with 15nodes and 35 nodes in network and evaluating a security attack against MANET as a network, different statistics or performance metrics Packet loss, Packet delivery ratio and Average end to end delay has been used.

[4] Vishnu k et. al. In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes. AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself.

[5] Akanksha Saini et. al Their paper includes the behavior of the Black Hole node studied by considering different scenarios. Performance of the Black Hole ADOV protocol has been analyzed by varying the number of mobile nodes and black hole nodes. The protocol is analyzed on various performance metrics like packet loss, packet delivery ratio and average end to end delay. It is observed that the effect on packet loss is much lower as compare to effect on delay. An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. A black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and then it drops all the receiving packets. The damage will be serious if malicious nodes work together as a group. This type of attack is called cooperative black hole attack.

[6] Yatin Chauhan, et. al. This paper illustrates how blackhole attack can affect the performance of routing protocol, AODV, in Mobile Ad hoc networks by using NS-2.34 simulator.Network Simulator (NS) is an object-oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP; routing and multicast protocols over wired and wireless networks. The simulator is a result of an ongoing effort of research and development. Even though there is a considerable confidence in NS, it is not a polished and finished product yet and bugs are being discovered and corrected continuously.

III. METHODOLOGY & ALGORITHM

The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table ie, whenever a new node joins the network, it sends a broadcast message as a request for IP address. The backbone node on receiving this message randomly selects one of the free IP addresses. The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes(BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.

3.1 ALGORITHM

Step1: Source node broadcasts RREQ to neighbours
Step2: Source node receives RREP from neighbours
Step3: Source node selects shortest and next shortest path based on the number of hops
Step4: Source node checks its routing table for single hop neighbouring nodes only
Step5: If the neighbour node is in its routing table then route data packet Else
The node is malicious and sends false packets to that node
Step 6: Invoke the route discovery
Inform all the neighbouring nodes about the stranger
Step 7: Add the status of stranger to the routing table of source node
Step 8: Again send packet to neighbouring node
Step 9: If step 5 repeats then broadcast the malicious node as black hole
Step 10: Update the routing table of source node after every broadcast
Step 11: Repeat step 4 to 10 until packet reaches the destination node correctly.

IV. SIMULATION ENVIRONMENT

We have implemented Black hole attack in an ns2 simulator [15]. CBR (Constant Bit Rate) application has been implemented. The problem is investigated by means of collecting data, experiments and simulation which gives some results, these results are analyzed and decisions are made on their basis. The simulator which is used for simulation is ns2. Using ns2, we can implement your new protocol and compare its performance to TCP.

To evaluate the performance of a protocol for an ad hoc network, it is necessary to analyze it under practical conditions, especially including the movement of mobile nodes. Simulation requires setting up traffic and mobility model for performance evaluation. Table 4 shows the parameters that have been used in performing simulation.

4.1 Performance Analysis

4.1.1 End-to-end delay: Packet end-to-end delay is the time delay it takes a network source to deliver a packet to its destination. Thus, the end-to-end delay of packets is the total amount of delays encountered in the whole network at every hop going to its destination. In MANETs, this kind of delay is usually caused by certain connection tearing or/and the signal strength among nodes been low. The reliability of a routing protocol can be determined by its end-to-end delay on a network, thus a steadfast MANET routing gives less packet end-to-end delay.

4.1.2 Packet delivery ratio : This refers to the ratio of the total number of data packets that reach the receiver (destination node) to the total number of data packets sent by the source node. This is another performance metric that is used to determine the efficiency and accuracy of MANET's routing protocol because it is used to calculate the rate of loosing packets. Similar to the network throughput, packet delivery ratio (PDR) is expected to be high.

V. RESULTS & DISCUSSIONS

5.1 Packet Delivery Ratio

Simulation results of figure 9(a) show that Packet delivery ratio in AODV with blackhole attack is less than the Modified AODV.

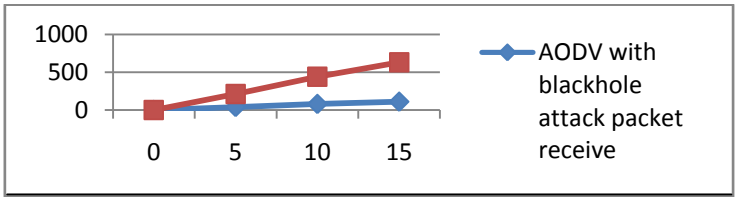
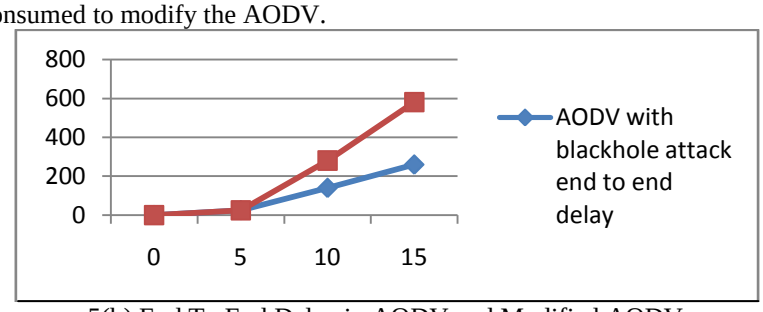


Figure5(a) Packet Receive in AODV and Modified AODV

5.2 End To End Delay

Simulation results in figure 9(b) show that End To End delay in AODV with blackhole attack is less than the Modified AODV. More Time is consumed to modify the AODV.



5(b) End To End Delay in AODV and Modified AODV

VI. CONCLUSION

In this paper, we have analyzed the Black hole attack with respect to different performance parameters such as end-to-end delay and packet delivery ratio. We have analyzed two protocols AODV with blackhole and modified AODV. This study was conducted to evaluate the effect of Black hole attacks on the performance of these protocols. The Simulation results show that modified AODV performs better than AODV with blackhole . Packet Delivery ratio is more in the modified AODV than the AODV with Blackhole .End to End delay is more in the modified AODV than the AODV with blackhole. Also the effect on modified AODV by the malicious node is less as compare to AODV. But still the detection of Black hole attacks in ad hoc networks is considered as a challenging task.

REFERENCES

[1] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) Improving AODV Protocol Against Blackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010

[2] Jaspal Kumar, M. Kulkarni, Daya Gupta," Effect of Black Hole Attack on MANET Routing Protocols", Published Online April 2013 in MECS (http://www.mecs-press.org/), *I. J. Computer Network and Information Security*, 2013, 5, 64-72

[3] Sarita Choudhary, Kriti Sachdeva," Discovering a Secure Path in MANET by Avoiding Black/Gray Holes",published in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-3, August 2012.

[4] Vipan Chand Sharma, Atul Gupta, Vivek Dimri," Detection of Black Hole Attack in MANET under AODV Routing Protocol", Volume 3, Issue 6, June 2013 International Journal of Advanced Research in Computer Science and Software Engineering.

[5] Akanksha Saini, Harish Kumar," Effect Of Black Hole Attack On AODV Routing Protocol In MANET", International Journal of Computer Science and Technology.

[6] Yatin Chauhan, Prof Jaikaran Singh, Prof Mukesh Tiwari, Dr Anubhuti Khare," Performance Evaluation of AODV based on black hole attack in ad hoc network", Global Journal of researches in engineering Electrical and electronics engineering Volume 12 Issue 2 Version 1.0 February 2012.

[7] Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." In: *International Journal of Network Security*, Vol. 5, No.3, pp.338–346, aNov. 2007.

[8] Isaac Woungang, Sanjay Kumar Dhurandher, RajenderDheerajPeddi, and Mohammad S. Obaidat, Fellow of IEEE and Fellow of SCS."Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks"

[9] R. Sudha, Dr. D. Sivakumar,"A Temporal table Authenticated Routing Protocol for AdhocNetworks", 978-1-4577-1894-6/11/$26.00©2011 IEEE.

[10] Mehdi Keshavarz, Mehdi Dehghan"MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks",WCNC 2012 Workshop on 4G Mobile Radio Access Networks.

