International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 6, August - 2012

Enhanced AODV Protocol in Manet due to Black hole Attacks

M.Radha

Naga Sharief Shaik

***Abstract* : MANETs can operate without fixed infrastructure and can survive rapid changes in the network topology. 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 which incorrectly replies route requests that it has a fresh route to destination and then it drops all the receiving packets. This type of attack is called cooperative black hole attack. MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. So security in MANET is a complex issue This 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**

***Keywords*- MANET, Blackhole, AODV, REQ, RREP, RERR.**

1. INTRODUCTION

In areas in which there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use, wireless mobile users may still be able to communicate through the formation of an ad hoc network [1]. In such a network, 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 direct wireless transmission range of each other. Each node participates in an adhoc routing protocol that allows it to discover “multichip” paths through the network to any other node.The idea of adhoc networking is sometimes also called infrastructure less networking [1], since the mobile nodes in the network dynamically establish routing among themselves to form their own network “on the fly.”

Some examples of the possible uses of ad hoc networking include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information for situational awareness on the battlefield, and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake. Many different protocols have been proposed to solve the multi hop routing problem in Ad hoc networks ,each based on different assumptions and intuitions. The rest of this paper is organized as follows. In Section 2 we briefly describes the different types of routing protocols with its descriptions and detail note on AODV routing protocol. Section 3 discusses about black hole attack. Section 4 presents the related work in literature, Section 5 we discuss our solution to AODV algorithm. Finally, we conclude in Section 6 with future scope.

II.SECURITY ISSUES

Ad-hoc networks are more vulnerable than wired networks therefore security is much more difficult ad hoc networks. Following are the various vulnerabilities that exist in wireless ad-hoc networks: Open Medium - Eavesdropping is easier than in wired network’s there is no centralized medium. Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network. They dynamically change their topology. This allows any malicious node to join the network without being detected. Cooperative Algorithms The routing algorithm of MANETs requires mutual trust between the neighbor nodes which violates the principles of Network Security. Lack of Centralized Monitoring – There is absence of any centralized infrastructure that prohibits any monitoring agentin the system. Lack of Clear Line of Defense - The only use of I line of defense- attack prevention may not secure. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process. that is as secure as its weakest link. In addition to prevention, we need two line of defense detection and response.

III. ROUTING PROTOCOLS

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. A MANET protocol should function effectively over a wide range of networking context from small ad-hoc group to larger mobile Multihop networks. As fig 1 shows the categorization of these routing protocols. Routing protocols can be divided into **proactive, reactive and hybrid protocols**, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

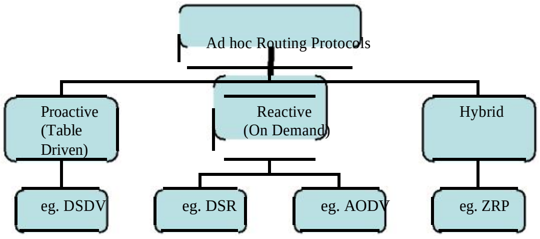

Fig 1. Hierarchy of Routing Protocols

A. Proactive Routing Protocol

In a network utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up -to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. On the other hand, routes will always be available on request. Many proactive protocols stem from conventional link state routing, including the Optimized Link State Routing protocol (OLSR).

B. ReactiveRrouting Protocol

Reactive routing protocols [1] are on-demand protocols. These protocols do not attempt to maintain correct routing information on all nodes at all times. Routing information is collected only when it is needed, and route determination depends on sending route queries throughout the network. The primary advantage of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be used. While reactive protocols do not have the fixed overhead required by maintaining continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network due to query flooding. Because of these weaknesses, reactive routing is less suitable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

C. Hybrid Routing Protocol

Wireless hybrid routing is based on the idea of organizing nodes in groups and then assigning nodes different functionalities inside and outside a group [1]. Both routing table size and update packet size are reduced by including in them only part of the network (instead of the whole); thus, control overhead is reduced. The most popular way of building hierarchy is to group nodes geographically close to each other into explicit clusters. Each cluster has a leading node (*cluster head*) to communicate to other nodes on behalf of the cluster. An alternate way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications

pass across overlapping scopes. More efficient overall routing performance can be achieved through this flexibility.

Since mobile nodes have only a single Omni-directional radio for wireless communications, this type of hierarchical organization will be referred to as logical hierarchy to distinguish it from the physically hierarchical network structure.

D. An Overview of AODV Routing Protocol

AODV routing protocol is based on DSDV and DSR algorithm and is a state-of-the-art routing protocol that adopts a purely reactive strategy: it sets up a route on-demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated [2]. This protocol is composed of two mechanism (1) Route Discovery and (2) Route Maintenance. AODV uses **R**oute **Req**uest (RREQ), **R**oute **Rep**ly (RREP) control messages in Route Discovery phase and **R**oute **Err**or (RERR) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in [3].

In general, the nodes participating in the communication can be classified as source node, an intermediate node or a destination node. With each role, the behavior of a node actually varies. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors. This RREQ message will further be forwarded (again broadcasted) by the intermediate nodes to their neighbors. This process will continue until the destination node or an intermediate node having a fresh route to the destination. At this stage eventually, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be received. Fig. 2 depicts the traversal of control messages.

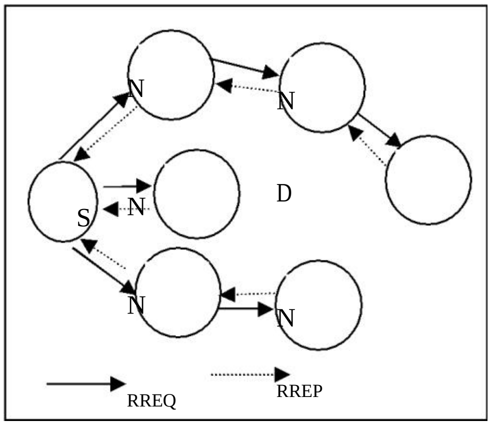

Fig 2. Traversal of Control Messages

gain the normal access to the network and it participates in Multiple Black Hole nodes in the ad hoc network the network activities, either by some malicious impersonation It simplifies that whether there is a single node that acts as to get the access to the network as a new node, or by directly Black Hole or multiple Black Hole nodes act as malicious nodes compromising a current node and using it as a basis to conduct in cooperative nature to grab the packets. its malicious behaviors. Internal attacks are more severe and Black hole attack detection proposals can be categorized a shard to detect. Below:

C. Examples of security attacks:

Single non malicious nodes identifying a black hole node Multiple non malicious nodes identifying a black hole node

1. *Denial of Service (DoS)***:** It aims to crab the availability of the node is Black hole or multiple non malicious nodes identify certain node or even the services of the entire ad hoc networks. a Black Hole node. It signifies whether a single non malicious node helps to identify the node is Black hole or multiple non malicious nodes identify certain node or even the services of the entire ad hoc networks' Black Hole node. In the traditional wired network, the DoS attacks a re carried services provided by the target become unavailable

2. *Impersonation:* Impersonation attack is a severe threat to the security of mobile ad hoc network. If there is not such a proper authentication mechanism among the nodes opponent can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information
3. *Eavesdropping:* Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access
4. *Sinkhole attack:* The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack
5. *Wormhole attack:* The attacker connects two distant parts of the ad hoc network using an extra communication channel (e.g. a fast LAN connection) as a tunnel. As a result two distant nodes assume they are neighbors and send data using the tunnel. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack.
6. *Sybil attack:* The Sybil attack especially aims at distributed system environments. The attacker plays multiple roles. It tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. For more information. The cloud appears to be many different nodes to the outside. Traffic Analysis: It is a passive attack used to gain information Multiple Black Hole nodes in the ad hoc network It simplifies that whether there is a single node that acts as Black Hole or multiple Black Hole nodes act as malicious nodes in cooperative nature to grab the packets. Black hole attack detection proposals can be categorized as in table:1.

IV. SUMMARY OF RELATED WORK

A number of protocols were proposed to solve the black hole problem. After studying the various proposed solutions an assumption have been made which is used in the table 1.

Few proposals assume Single Black Hole node in a network used to simulate the various scenarios. For analysis Perl, awk and shell programming has been used. Black hole behavior has been implemented by modifying the AODV routing protocol. Table 2 shows the simulation parameters when the number of Black Hole increases with the number of nodes.

Table 1: Summary of different proposed solutions

Proposal name	Approach	Assumption	Philosophy
Dynamic learning system using DPRAODV [5]	DPRAODV	Multiple black hole	Single non-black hole node detects
Cooperative black hole node detection using DRI and cross checking [6]	AODV	Cooperative black hole	Single non-black hole node detects
Black hole node detection using two different solutions [7]	AODV	Multiple black hole	Single as well as Multiple non black node detects
Distributed and cooperative mechanism [8]	AODV	Distributed and cooperative	Cooperative detection
Detecting Black hole Attack on AODV-based Mobile Ad Hoc using dynamic anomaly detection [9]	AODV	Multiple black hole	Single non black hole node detects
Single black hole node detection	AODV	Single black hole	Single non black hole node detects
Prevention of Black hole Attack using fidelity table [11]	Enhance ment on AODV	Multiple black hole	Multiple non- black hole node
Detection of black hole using DRI and Cross checking [12]	Modified version of AODV	Multiple black hole	Multiple non-black hole nodes detects

Table 2 : Simulation Parameters

Simulation Area	500 X 500
Number Of Nodes	10,20……90
Communication Traffic	CBR
Simulation Duration	200s
Maximum Number of Connections	8,16……..75
Pause Time	2s
Maximum Speed Of Node	20 m/s
Packet Rate	4 packets/s

In this study the three performance metrics packet loss, packet delivery ratio and average end to end delay has been used: Packet loss: Packet loss is the difference between the packets sent and the packets received. Packet loss for malicious node is counted by how many of the packets is there which could not reach to the destination node and are absorbed by the Black Hole node.

Packet loss = (Packets sent – Packets received) X 100
Packets sent

Packet Delivery Ratio: It is the ratio between the number of CBR packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination.

PDR = Number of CBR packets received X 100
Number of packets sent

Delay: End to end delay is the average delay between the sending of the data packets by the CBR sources and its receipt at the corresponding CBI receiver. This consists of the delays caused by the buffering and processing at the intermediate nodes at the MAC layer

V. SIMULATION ENVIRONMENT

Two different scenarios have been created. In first scenario the total number of nodes forming the ad hoc network is kept constant. Black Hole nodes keep on increasing linearly where as in the second scenario number of Black Hole and other nodes are keep on changing in such a way that ratio of Black Hole nodes to total number of nodes remain constant. Open The percentage for livery of Packets has been calculated.

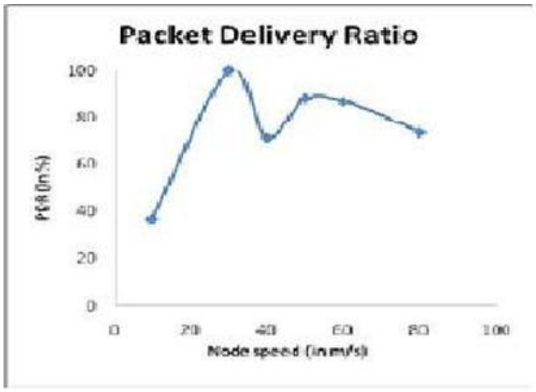

Fig:3

Fig. 3 shows the packet delivery ratio with respect to node mobility which gradually increases almost when the malicious node enters the route packet. The delivery ratio increases when the number of node are less but with the increase in number of nodes, the packet delivery ratio decrease gradually as when there are large number of nodes then alternative routes also increases almost exponentially. The packet can be send via other cooperative nodes

VII. CONCLUSION AND FUTURE WORK

In network topology in MANETs usually changes with time. Therefore, there are new challenges for routing protocols in MANETs since traditional routing protocols may not be suitable for MANETs. Researchers are designing new MANETs routing protocols, comparing and improving existing MANETs routing protocols before any routing protocols are standardized using simulations

REFERENCES

1.Poongothai T. and Jayarajan K., “A non-cooperative game approach for intrusion detection in Mobile Adhoc networks”, International Conference of Computing, Communication and Networking (ICCC), 18-20 Dec 2008, St. Thomas, VI, pp 1-4

2.Bo Sun,Yong Guan,Jian Chen,Udo , “Detecting Black-hole Attack in Mobile Ad Hoc Network” , The institute of Electrical Engineers, Printed and published by IEEE, 2003.

3.Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Vol.5, issue 3, Nov 2007, pp 338–346.

4.Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang,“A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network” , Springer-Verlag Berlin Heidelberg, 2007.

5.Payal N. Raj and Prashant B. Swadas, “DPRAODV: A dynamic learning system against black hole attack in AODV based MANET”, International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59

6.S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative black hole attack in wireless ad hoc networks,” International Conference (ICWN’03), Las Vegas, Nevada, USA, 2003, pp 570-575 Mohammad Al-Shurman, Seong-Moo Yoon Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACM Southeast Regional Conference , Proceedings of the 42nd annual Southeast regional conference, 2004, pp 96-97

7.Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng and Shun Chao Chang, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks”, PAKDD 2007 International Workshop, May 2007, Nanjing, China, pp 538–549

8.Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Volume 5, Number 3, 2007, pp 338–346

9.Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75

10.Latha Tamilselvan and V Sankaranarayanan, "Prevention of Black hole Attack in MANET", Journal of networks, Volume 3, Number 5, 2008, pp 13-20

11.Bo Sun Yong, Guan Jian Chen and Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", The Institution of Electrical Engineers (IEE) ,Volume 5, Number 6, 2003, pp 490-495

Marc Greis, "Tutorial for the Network Simulator", http:// www.isi.edu/nsnam/ns/tutorial/index.html

Author Profiles:

Marepalli Radha working as Associate professor in Adams Engineering college,palvoncha has interest to include Network Security information security and neural networks ,mobile computing.

Naga Sharief Shaik persuing Mtech in computer science engineering in Adams Engineering college,palvoncha has interest to include Network Security and mobile computing