International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

Analysis of On-Demand Routing Protocols under multiple Black hole Nodes

P. Naresh Kumar[1] , N.Venkatadri[2] , K. Ramesh Reddy[3], K. Srilatha Reddy[4]

[1]Research Scholar, Department of Computer Science, Rayala Seema Univesity, Kurnool, Andhra Pradesh, India

[2]Professor, Department of Computer Science and Engineering, TKREC, Meerpet, Hyderabad, Telangana, India

[3] Assistant Professor, Department of Computer Science, V.S.University, Nellore, Andhra Pradesh, India

[4]Assistant Professor, Department of Computer Science and Engineering, TKREC, Meerpet, Hyderabad, Telangana, India

ABSTRACT

Mobile Ad hoc Network (MANET) is an infrastructure less wireless network of one or more mobile nodes connected by wireless links. These networks do not rely on physical infrastructure so these are easy to deploy where establishment of infrastructure not possible. Rapid improvement in technology may affect the security concerns of the MANET. These networks are vulnerable to various attacks targeting all layers of the protocol stack. One of the major attacks targeting network layer is black hole attack. In this attack, the malicious nodes drop the data packets or forward the packets to the unknown addresses in the network. Many academicians and researchers analyzed the effect of this black hole attack and enhanced the existing protocols to avoid path through malicious nodes in the network. So it is a challenge for researchers in order to improve or enhance security mechanisms already developed or design new efficient security mechanism. In this work, we analysis the performance of on-demand routing protocols under the presence of multiple black hole nodes. We analyzed performance metrics Delay and Throughput. We used Network Simulator version 2(NS2) to carry out the implementations.

Keywords : Infrastructure less wireless network, DoS, Black hole attack, Routing Protocols, NS2, QoS metrics.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of dynamically connected and infrastructure less wireless mobile nodes. Because MANETS are mobile, they use wireless connections to connect to various nodes. This can be established using a cellular or Satellite transmission, Wi-Fi connection, or another medium. In these networks nodes are free to move arbitrarily. It takes part in discovery and maintain of routes to other nodes in the network. As it is highly dynamic environment it become critical task for stable routing, highly error prone and can go down frequently due to mobility of nodes.

Mobile Ad-hoc Network is highly dynamic in nature and no physical infrastructure available in this network. Due to this, many issues in designing Mobile Ad-hoc Networks are there such as [1]

i) Error-prone channel state, ii) Hidden terminal problem, iii) Exposed terminals, iv) Bandwidth – constrained, v) Energy-constrained operation and vi) Security Issues

MANETs are easily affected by various physical security attacks because of MANET features like open medium, no central monitoring, distributed nature, co-operative algorithms and so on.

II. ROUTING PROTOCOLS IN MANET

There are so many protocols have been developed so far to carry routing functionality in wireless networks. Providing routing in wireless networks is a critical task because these are much prone to security threats. So lot of research is going on to provide secure transmissions.

AODV Protocol

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is a modification of the DSDV algorithm. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes. AODV builds routes using a route request / route reply query cycle [2].

1) Route Discovery

When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

2) Route Reply

As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

3) Route Maintenance

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

TORA Protocol

The Temporally-Ordered Routing Algorithm (TORA) is an algorithm for routing data across Wireless Mesh Networks. Temporally-Ordered Routing Algorithm (TORA) is a distributed protocol designed to be highly adaptive so it can operate in a dynamic network. For a given destination, TORA uses parameter to determine the direction of a link

between any two nodes. As a consequence of this multiple routes are often present for a given destination, but none of them are necessarily the shortest route.

TORA does not use a shortest path solution, an approach which is unusual for routing algorithms of this type. TORA builds and maintains a Directed Acyclic Graph rooted at a destination. No two nodes may have the same height. Information may flow from nodes with higher heights to nodes with lower heights.

The key design concept of TORA is localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain the routing information about adjacent (one hop) nodes. The protocol performs three basic functions: Route creation, Route maintenance, Route erasure.

1) Route Creation

For a node to initiate a route, it broadcasts a Query to its neighbors. This is rebroadcast through the network until it reaches the destination, or a node that has a route to the destination.

2) Route Maintenance

This node replies with an Update that contains its height with respect to the destination, which is propagated back to the sender. Each node receiving the Update sets its own height to one greater than that of the neighbor that sent it. This forms a series of directed links from the sender to the destination in order of decreasing height. When a node discovers link failure, it sets its own height higher than that of its neighbors, and issues an Update to that effect reversing the direction of the link between them.

3) Route Erasure

If it finds that it has no downstream neighbors, the destination is presumed lost, and it issues a Clear packet to remove the invalid links from the rest of the network. An advantage to TORA is that it supports multiple routes to any source/destination pair. Failure or removal of one node is quickly resolved without source intervention by switching to an alternate route.

Unfortunately, there are drawbacks to TORA as well. The most glaring being that it relies on synchronized clocks among nodes in the network. While external time sources are present (GPS for example), it makes the hardware to support it more costly, and introduces a single point of failure if the time source became unavailable. TORA also relies on intermediate lower layers for certain functionality. It assumes, for example, that link status sensing, neighbor discovery, in-order packet delivery, and address resolution are all readily available. The solution is to run the Internet MANET Encapsulation Protocol (IMEP) at the layer immediately below TORA.

III. REVIEW OF LITERATURE

In Black hole attack, an attacker node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol.

When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created.

Many authors published their research work on black hole attack and their counter measures such as[3].

Satoshi Kurosawa et. al. uses an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is defined to express

state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T anomaly detection is performed.

Payal N. Raj et. al. modifies the behavior of AODV to include a mechanism for checking the sequence number of the received RREP. As the source node receives the RREP it compares the sequence number of the received RREP to a threshold value. The replying node is suspected to be a black hole if its sequence number is greater than the threshold value. The source node adds the suspected node to its black list, and propagates a control message called an alarm to publicize the black list for its neighbors. The threshold is the computed average of the difference between the destination sequence number in the routing table and the destination sequence number in the RREP within certain periods of time. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated.

Latha Tamilselvan et. al. proposed a better solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 values is considered as malicious node and is eliminated from the network. The fidelity levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgement to the source; thereby the intermediate node's level will be increment is received, the intermediate node. The main drawback of this solution is processing delay in the network.

Hongmie Deng et.al. Proposed One possible solution to the black hole problem is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense they avoid the black hole problem and implement a secured AODV protocol. But there are two associated disadvantages. First, the routing delay is greatly increased, especially for a large network. Second, a malicious node can take further action such as fabricate a reply message on behalf of the destination node. The source node cannot identify if the reply message is really from the destination node or fabricated by the malicious node. In this case, the method may not be adequate.

IV. BLACK HOLE ATTACK

A packet drop attack or black hole attack is a type of denial-of-service attack accomplished by dropping packets. Black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipients .Black Hole attacks effects the packet delivery and to reduce the routing information available to the other nodes causes: (i) It down grade the communication, (ii) Effects of making the destination node reachable [4].

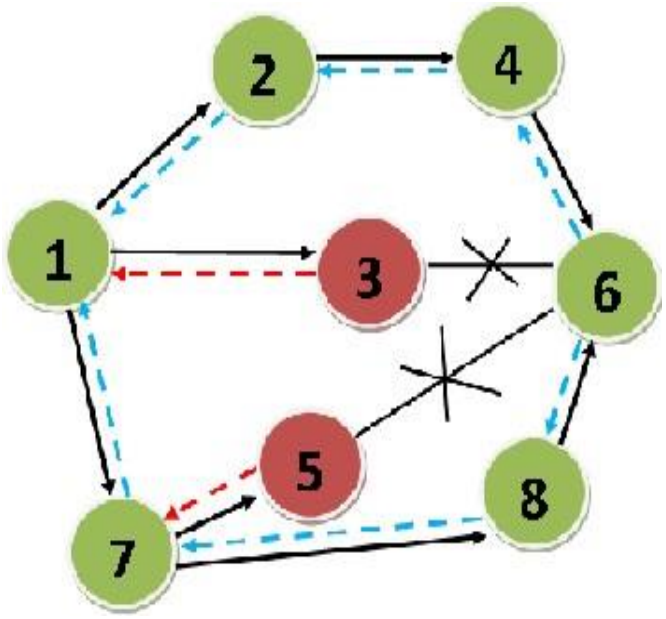

Figure 1. black hole attack involvement

As shown in the above figure nodes 3 and 5 are implemented as malicious nodes so packets transmission through these nodes will not reached their destination node 6. The nodes 1 and 7 can communicate with destination node either using the intermediate nodes 7,8 or 2,4.

In this work, we implemented multiple black hole nodes and we analyzed the performance of on-demand routing protocols TORA and AODV under the presence of multiple black hole nodes using NS2 simulator. Network Simulator Version 2(NS2) is a open source discrete event network simulator. In the presence of malicious nodes MANET shows poor performance because all packets are not reached their destination.

V. RESULTS

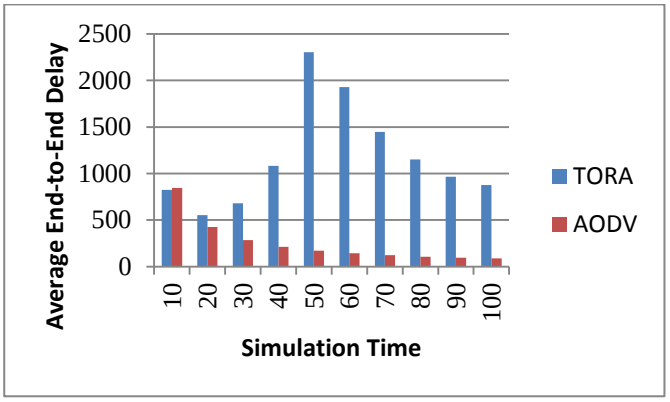

Figure 2. Analysis of Average Delay for AODV and TORA for network size 25nodes using ftp

As shown in the above figure, initially both the protocols took almost same average end to end delay but throughout the simulation TORA take more delay than AODV.

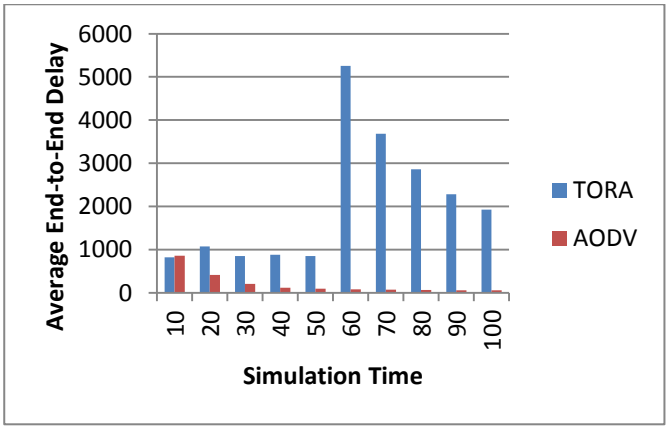

Figure 3. Analysis of Average Delay for AODV and TORA for network size 50 nodes using ftp

As shown in the above figure, initially both the protocols took almost same average end to end delay but throughout the simulation TORA take more delay than AODV and Delay of TORA also gradually decrease for the increase of the simulation time.

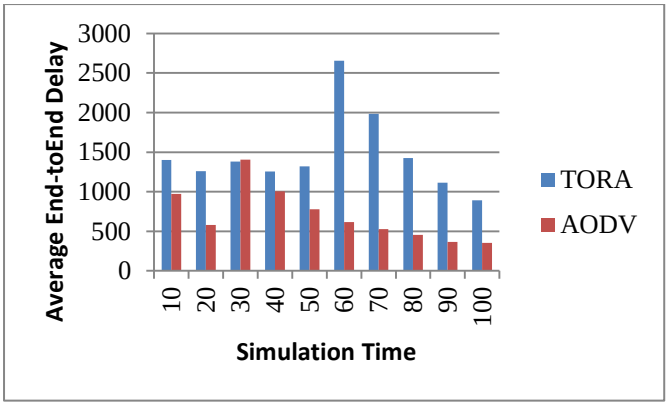

Figure 4. Analysis of Average Delay for AODV and TORA for network size 75 nodes using ftp

As shown in the above figure, initially AODV take more delay than TORA. After some time TORA take more delay than AODV.

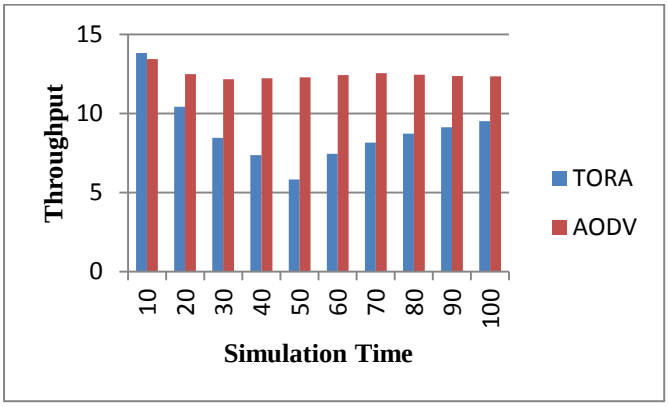

Figure 4. Analysis of Throughput for AODV and TORA for network size 25nodes using ftp.

As shown in the above figure, until first half of the simulation time throughput of the TORA decreases gradually. In the second half the simulation period throughput of the TORA increases gradually. During the entire simulation AODV produces more throughput than TORA.

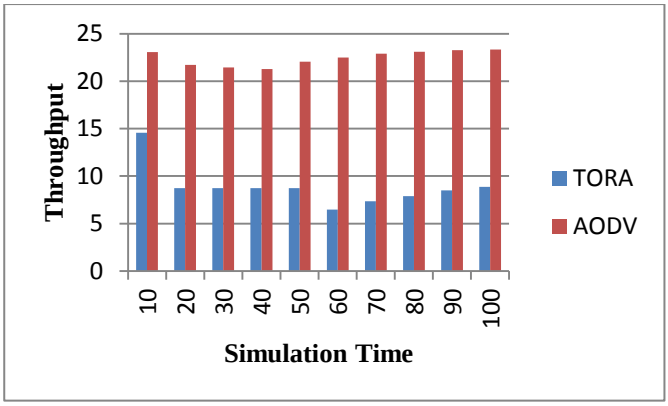

Figure 5. Analysis of Throughput for AODV and TORA for network size 50 nodes using ftp

As shown in the above graph, any instance of simulation time AODV produce double of the throughput produced by another on-demand routing protocol TORA.

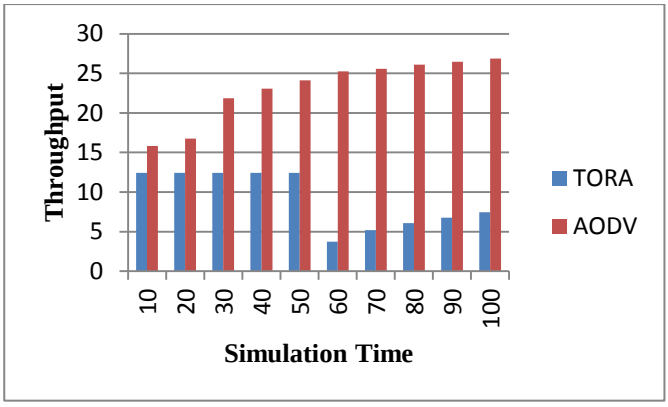

Figure 6. Analysis of Throughput for AODV and TORA for network size 75 nodes using ftp

As shown in the above figure, during the first half of the simulation duration AODV has little bit more throughput than TORA. During the second half of the simulation duration throughput of the AODV increases abnormally.

VI. CONCLUSIONS

In this work, we analyzed the performance of on-demand routing protocols AODV and TORA for performance metrics like DELAY and THROUGHPUT for the network size 25-Nodes, 50-Nodes, and 75-Nodes. In the literature, many of the

authors studied the performance of on-demand routing protocols AODV and DSR only.

In future, this work is extended to implement other types of DoS attacks using TORA. The counter measure for the multiple black hole nodes may also implement.

VII. REFERENCES

[1]. Gurpinder Singh, Jaswinder Singh," MANET: Issues and Behavior Analysis of Routing Protocols, ijarcsse, Volume 2, Issue 4, April 2012.

[2]. Aarti Bairagi, Prashant Panse," On Demand Routing Protocols in MANET",icac.

[3]. Sunil Gupta, Harsh Khatter , Ravi Kant"A Literature Survey on Black Hole Attacks on AODV Protocol in MANET",IJCA,Volume 80 – No 16, October 2013.

[4]. Puneet Kansal,Ishant Prabhat,Amit Rathee, "Black hole attack in Manet" ,ijarcsse, Volume 3, Issue 3, March 2013

[5]. N.Venkatadri and K.Ramesh Reddy,"Performance Metrics Comparison for Of On-Demand Routing Protocols Using NS2 ", International Journal Of Advanced Research in Computer Science and Software Engineering Volume 5,Issue 3, March 2015,ISSN 2277 128X.

[6]. G.Pragadeeswaram, D.Ezhilarasi and P.Selvakumar ,"A Performance Analysis of TORA, AODV and DSR Routing Protocols in MANET using NS2", International Journal Of Scientific & Engineering Research, Volume 3,Issue 6,June-2012, ISSN 2229-5518.

[7]. Anuj K.Gupta, Dr.Harsh Sadawarti, Dr. Anil and K.Verma, "A Performance Analysis of AODV,DSR andTORA Routing Protocols", IACSIT International Journal Of Engineering and Technology, Vol 2,No.2, April 2010, ISSN: 1793-8236.

[8]. Anand Pandey, Dinesh Kumar and Shailendra Kumar Singh, "Performance Evolution of TORA Protocol with Reference to Varying Number of Mobile Node", International Journal Of Application or Innovation Engineering & Management, Volume 2, Issue 12, December 2013, ISSN 2319-4847.

[9]. N Vetrivelan, Dr. A.V Reddy, "A Performance Analysis of Three Routing Protocols for Varying MANET Size", Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol II, IMECS 2008, 19-21 March, 2008,Hong Kong.