Open access Journal International Journal of Emerging Trends in Science and Technology

Performance Analysis and Comparison of MANET Routing Protocols under Black Hole Attack

Authors

Mrs. Amninder Kaur Gill[1] and Yog Kunwar[2]

[1]Punjabi University Regional Centre for Information Technology and Management, Mohali, India

Email: *amninder02@gmail.com*

[2]Punjabi University Regional Centre for Information Technology and Management, Mohali, India

Email: *yogkunwar@yahoo.co.in*

Abstract:

A Mobile Ad-Hoc Network (MANET) consists of portable wireless nodes. The communication between these mobile nodes is dispensed with non-centralized management. There are still many open problems concerning MANETs like security problem. Black Hole Attack is one amongst the security threats that is applicable in the network. The aim of this work is to analyze the effect of Black Hole Attack in MANET routing protocol i.e. Ad-Hoc On-Demand Distance Vector (AODV) and Temporarily Ordered Routing Algorithm (TORA). Comparative analysis of both protocols with Black Hole Attack is taken into account. The simulation is done using NS2 simulator.

Keywords: *AODV, MANET, NS2, TORA.*

1. Introduction

A group of independent mobile nodes each of which can communicate with each other using radio waves without any centralized management is called Mobile Ad-Hoc Network (MANET). Nodes communicate with each other using wireless interface. Mobile nodes falling within radio range of each other can communicate directly with each other without using intermediate nodes which act as routers. Whereas nodes which don't falls within the range of radio waves can use intermediate nodes to route their information packets to the destination [6]. Mobile Ad-Hoc Networks have a number of various applications. It can be established in areas where quick and temporary networks are required or it can also be established in some emergency scenarios such as in the battle field etc [8]. The classifications of Mobile Ad-Hoc routing protocols based on routing Messages information update mechanism employed are Proactive/Table driven Routing Protocol, Reactive/On-Demand Routing Protocol and Hybrid Routing Protocol [2]. MANETs have several silent characteristics such as Dynamic topology, Distributed operation, Multi hop routing, Light-weight terminals etc. which provides it flexibility that it can be setup and work at any place or point without the help of any fixed infrastructure and check point. But because of these characteristics it is also vulnerable to many types of attack [1]. Attacks can be performed at different layers of MANET. Black Hole Attack is one of the several attacks that are possible in MANETs. Black Hole Attack works at network layer as its main aim is to drop data rather than forwarding the data when it receives the data [4]. Black Hole Attack is among numerous attacks and is taken into account for AODV and TORA

routing protocols in MANET. A performance comparison of MANET routing protocols i.e. Ad-Hoc On-Demand Distance Vector (AODV) and Temporarily Ordered Routing Algorithm (TORA) under Black Hole Attack have been done finding out which protocol is more vulnerable to attack.

2. Ad-Hoc On-Demand Distance Vector Routing Protocol (AODV)

AODV is an Ad-Hoc reactive routing protocol which implies that it establishes a route to a destination only on demand. When the source node needs to send a packet to the destination node within the network only then the event of route discovery procedure in AODV takes place. As a result of its fine operation even in high load conditions, it consumes very low memory for its operation in comparison to other routing protocols. It's one of the most widely used protocols in Mobile Ad-Hoc Networks. Flooding method is being used by AODV in order to search a route to the destination and the number of route request packets rebroadcasted by the node is proportional to the total number of nodes [11]. In AODV, there is no requirement of maintaining the information about the routes by nodes which do not participate in the communication.

The AODV routing protocol consists of two steps: Route Discovery and Route Maintenance. In route discovery, if a route from the source to the destination does not exist, the route request (RREQ) messages are broadcasted by the source node to its neighbours. When RREQ message reaches to some intermediate node that has a fresh route to the destination or to the destination itself then reply is send back to the source regarding route to the destination in the form of route reply message (RREP) and forward path is setup to send data from source to destination. After receiving RREP message, source node can start sending the data through selected route. But it is also possible that nodes get out of range in the network. So selected route will be broken. In that case route maintenance is required. In maintaining routes, the node which identifies the route disconnection, sends route error message (RERR) to other node on the selected route and invalid entries are removed from their routing tables as each node maintain table for its neighboring nodes only and if route from source to destination is still required then route discovery process is initiated again [9].

3. Temporally Ordered Routing Algorithm (TORA)

Temporally Ordered Routing Algorithm (TORA) is a distributed, extremely adjustive routing protocol that is additionally called link reversal protocol. TORA uses a discretional height metric to ascertain an immediate direct acyclic graph and length of the route that physically (DAG) leads to the destination. As a result, multiple routes typically exist for a given destination however none of them are necessarily the shortest route. In order to find route to the destination, TORA does not exploit the shortest concept instead the direction of the next destination is maintained by TORA algorithm to forward the packets. Therefore one or more downstream links are maintained by the source node. TORA reduces the control messages within the network by allowing the nodes to request for a route only when it requires sending a packet to the destination [7].

TORA is a complicated routing algorithm as compared to other routing algorithms. Three basic functions performed by the protocol are: Route discovery, Route maintenance and Route erasure [5]:

3.1 Route Discovery

When a node has no route to the destination and needs a route only then route discovery process is initiated. The QRY and UPD packets are employed for creating routes. When query packet (QRY) is received by an intermediate node with fresh enough routes to the destination, an update packet (UPD) propagates back to the source node setting the heights of all upstream nodes and route is created from the source to the destination. The

source node then uses that route to send data to the destination [5].

3.2 Route Maintenance

Due to node mobility, the established routes can get broken and once it is discovered by a node that a route to the destination is not valid any more then route maintenance is important for reestablishing a DAG leading to the same destination [5].

3.3 Route Erasure

When a network partition takes place, the height of the node and also the heights of all its neighbors are set to NULL for the destination in its table and a CLR (Clear) packet is broadcasted [5].

4. Black Hole Attack

MANETs are at risk of numerous attacks carried out intentionally by attacker against MANETs to disrupt the normal network performance. Among numerous attacks, Black Hole is one kind of attack which happens in MANET. It is active attack within which a malicious node will lure all information packets by incorrectly claiming a contemporary route to the destination and once the malicious node is chosen as a route, the malicious node executes to forbid forwarding the information packets [10].

Black Hole Attack can be classified into two classes [3]:-

4.1 Single Black Hole Attack

In Single Black Hole Attack, single node acts as a malicious node inside a zone.

4.2 Cooperative Black Hole Attack

In Collaborative Black Hole Attack, more than one node in a group performs malicious activity.

Fig. 1 shows the Black Hole problem. The figure shows that node “F” is acting as the source node, node “E” is acting as the destination node and node “B” is acting as the Black Hole node. Node “F” wants to send data to node “E”. Route discovery process is initiated by node “F”. On receiving route request message, node “B” claims that it has a recent and short route to node “E” and sends a RREP to node “F” within no time. After receiving RREP, node “F” is convinced that node “B” has a recent and short route to node “E” then node “F” reject all other RREPs from other nodes in the network and starts sending data through node “B”, which in turn drops the data instead of forwarding it to the destination [12].

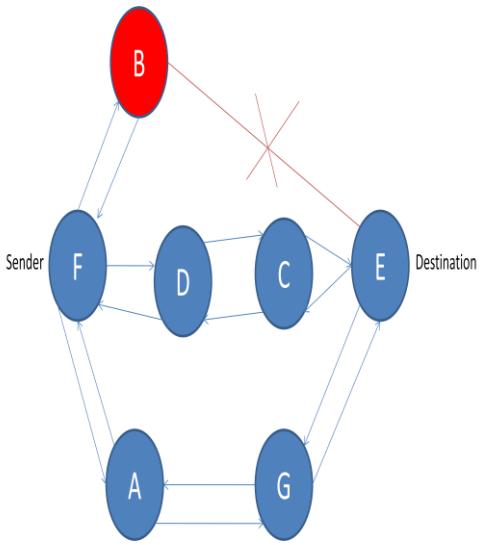

Figure 1: Black Hole Attack

5. Performance Metrics

The metrics used to compare the performance of AODV and TORA with Black Hole Attack are End-to-End Delay, Throughput, Network Load, Packets Received, Packets Dropped and Routing Overhead.

6. Simulation Results

For the simulation, NS2 (v-2.35) network simulator is used on Linux Platform. XGRAPH utility has been used to draw graphs and analyze the results. Radio propagation model is being used in this simulation with antenna type as Omni directional. At the physical and data link layer, IEEE 802.11 is used. The channel used is Wireless Channel. At the network layer, AODV and TORA are used as the routing protocol. Black Hole Attack works at network layer.

Node 7 and Node 8 are acting as the source nodes, Node 5 is acting as the destination node and Node

1 is acting as the Black Hole node in AODV and TORA with Black Hole Attack.

Fig. 2 shows the simulation of AODV routing protocol with Black Hole Attack.

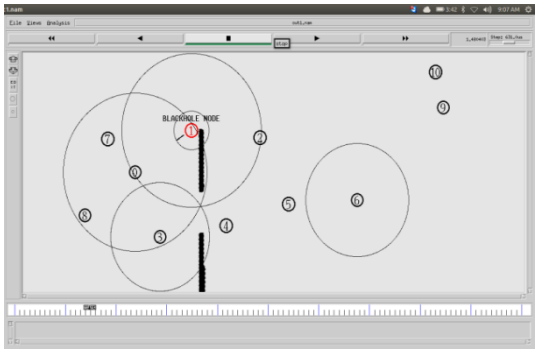

Figure 2: AODV Routing Protocol with Black Hole Attack

Fig. 3 shows the simulation of TORA routing protocol with Black Hole Attack.

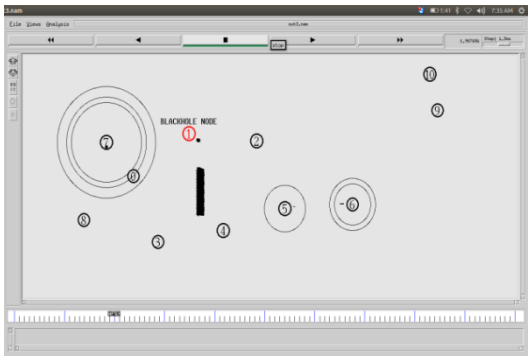

Figure 3: TORA Routing Protocol with Black Hole attack

For performing the work, simulation of AODV and TORA with Black Hole Attack has been done. After that, the results are averaged to evaluate and compare their performance of AODV and TORA with Black Hole Attack. The results obtained are illustrated in the form of graphs on the basis of each metric calculated.

6.1 Results of AODV vs. TORA routing protocols with Black Hole Attack

6.1.1 Comparative Analysis of End-to-End Delay

Fig. 4 shows the End-to-End Delay of AODV vs. TORA routing protocols with Black Hole Attack. It shows that the End-to-End Delay of AODV routing protocol with Black Hole Attack is higher than the End-to-End Delay of TORA routing protocol with Black Hole Attack.

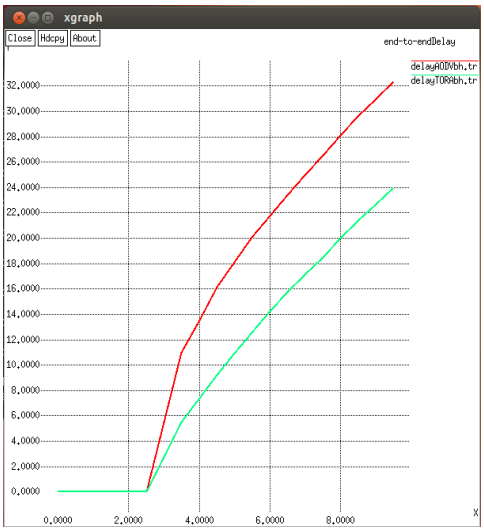

Figure 4: End-to-End Delay of AODV vs. TORA routing protocols with Attack

6.1.2 Comparative Analysis of Throughput

Fig. 5 shows the Throughput of AODV vs. TORA routing protocols with Black Hole Attack. It shows that the Throughput of AODV routing protocol with Black Hole Attack is less than Throughput of TORA routing protocol with Black Hole Attack and remains less.

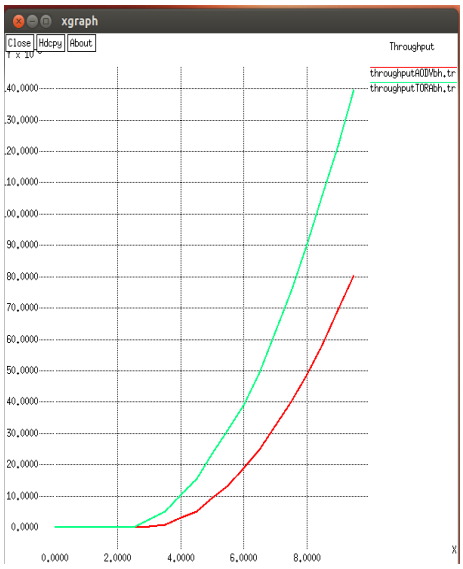

Figure 5: Throughput of AODV vs. TORA routing protocols with Attack

6.1.3 Comparative Analysis of Network Load

Fig. 6 shows the Network Load of AODV vs. TORA routing protocols with Black Hole Attack. It shows that the Network Load of TORA routing protocol with Black Hole Attack is higher than Network Load of AODV routing protocol with Black Hole Attack.

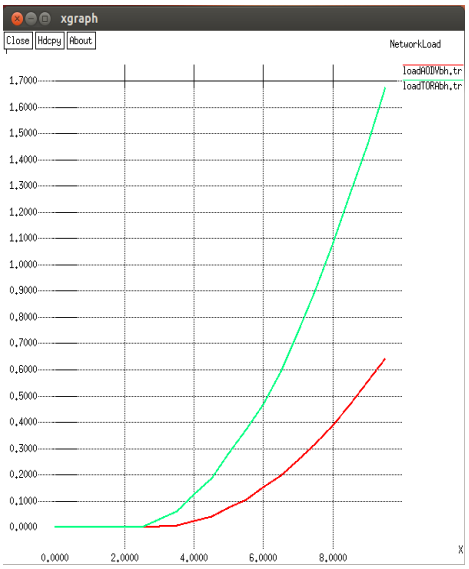

Figure 6: Network Load of AODV vs. TORA routing protocols with Attack

6.1.4 Comparative Analysis of Packets Received

Fig. 7 shows the Packets Received by AODV vs. TORA routing protocols with Black Hole Attack. It describes that Packets Received by AODV routing protocol with Black Hole Attack is less than the Packets Received by TORA routing protocol without Black Hole Attack.

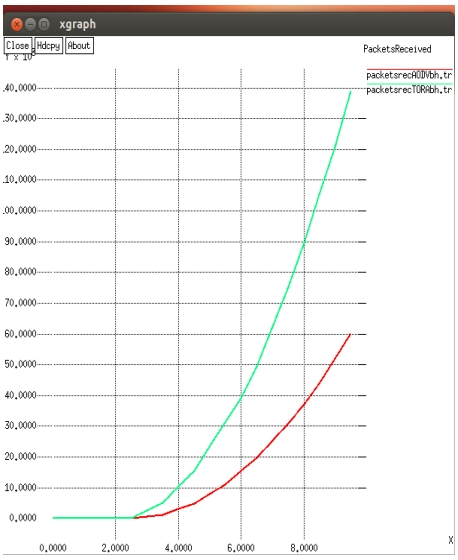

Figure 7: Packets Received by AODV vs. TORA routing protocols with Attack

6.1.5 Comparative Analysis of Packets Dropped

Fig. 8 shows the Packets Dropped by AODV vs. TORA routing protocols with Black Hole Attack. It shows that the Packets Dropped by AODV routing protocol with Black Hole Attack is greater than Packets Dropped by TORA routing protocol with Black Hole Attack.

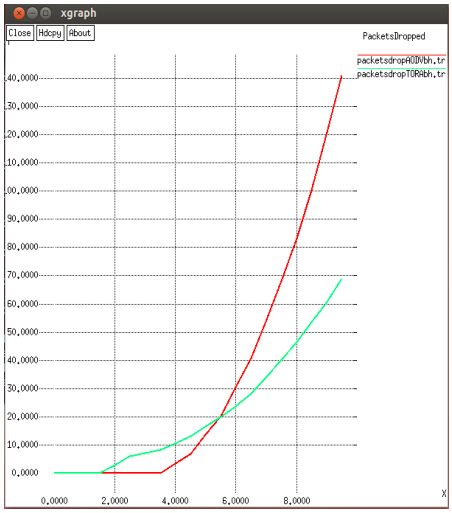

Figure 8: Packets Dropped by AODV vs. TORA routing protocols with Attack

6.1.6 Comparative Analysis of Routing Overhead

Fig. 9 shows the Routing Overhead of AODV vs. TORA routing protocols with Black Hole Attack. It shows that Routing Overhead of TORA routing protocol with Black Hole Attack is higher than the Routing Overhead of AODV routing protocol with Black Hole Attack. This is because data is dropped by the Black Hole node

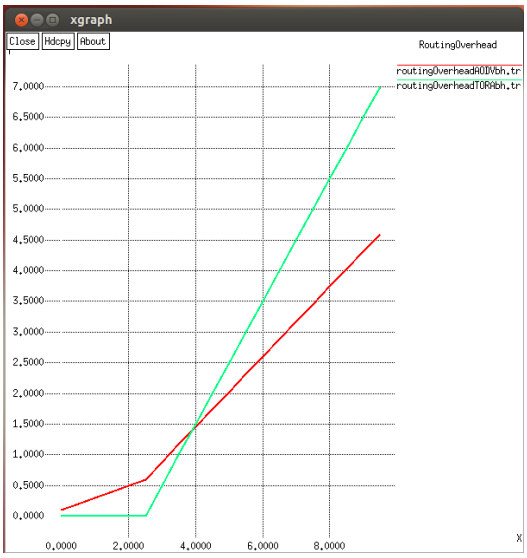

Figure 9: Routing Overhead of AODV vs. TORA routing protocols with Attack

Table 1: Result of AODV vs. TORA (with Black Hole Attack)

Protocols & Parameters	*AODV with Attack*	*TORA with Attack*
End-to-End Delay	High	Low
Throughput	Low	High
Network Load	Low	High
Packet Received	Low	High
Packets Dropped	High	Low
Routing Overhead	Low	High

7. Conclusion

The results shows that Black Hole Attack has severe effect on the performance of both the routing protocols and when comparing the performance of both the routing protocols (AODV and TORA) with Black Hole Attack, the overall performance of TORA with Black Hole attack is marginally better than AODV i.e. AODV is more vulnerable to attack than TORA. TORA with Black Hole attack, under the in terms of all six network performance parameters i.e. throughput, network load, end-to-end delay, packets received, packets dropped and routing overhead performs better than AODV with Black Hole attack.

8. Future Scope

In future work, a number of other routing protocols like DSR, OLSR, DSDV etc can be compared against TORA with Black Hole Attack for other parameters like bit rate, packet delivery ratio etc so as to work out the impact of Black Hole Attack on other routing protocols. As far as future security is concerned, new security mechanisms or solutions will be designed so as to provide security to different routing protocols against Black Hole Attack. Lots of analysis work requires to be done in this area.

References

1. Aarti & Tyagi S. S., "Study of MANET: Characteristics, Challenges, Application and Security Attacks", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 5, pp. 252-257, May 2013.
2. Abusalah L., Khokhar A. & Guizani M., "A Survey of Secure Mobile Ad-Hoc Routing Protocols", *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.
3. Badiwal S. & Verma V., "Survey of IDS in MANET against Black Hole Attack", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, vol. 2, no. 5, pp. 401–406, May 2013.
4. Chamoli S., Kumar S. & Rana D., " Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks", *Int.J.Computer Technology & Applications*,vol. 3, no. 4, pp. 1395–1399, August 2012.
5. Hilal A. R., Nahas A.E. & Bashandy A., "RT-TORA: A TORA Modification for Real-Time Interactive Applications", *IEEE/Canadian Conference on Electrical and Computer Engineering*, pp. 1403-1406, May 2008.
6. Ivan S., *Handbook of Wireless Networks and Mobile Computing*, Wiley Publications, India, 2002.
7. Kuppusamy P. & Thirunavukkarasu K., "A Study and Comparison of OLSR, AODV and TORA Routing Protocols in Ad Hoc Networks", *in proceedings of IEEE 3rd International Conference on Electronics Computer Technology (ICECT)*, 2011.
8. Ramanathan R. & Redi J., "A Brief Overview of Ad Hoc Networks: Challenges and Directions", *IEEE Communcation Magazine*, vol. 40, no.5, pp. 20-22, August 2002.

9. Royer E. M. & Toh C. K., " A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", *IEEE Personal Communications*, vol. 6, no. 2, pp. 46-55, April 1999.
10. Selvavinayaki K., Shankar K. K. S. & Karthikeyan E., "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs", *International Journal of Computer Applications*, vol. 7, no. 11, pp. 15–19, October 2010.
11. Song J., Wong V. W. S. & Leung V. C. M., "Efficient On-Demand Routing for Mobile Ad Hoc Wireless Access Networks", *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 7, pp. 1374–1383, September 2004.
12. Ullah I. & Rehman S. U. R., *Analysis of Black Hole Attack on* MANETs *Using Different MANET Routing Protocols*, School of Computing/ Blekinge Institute of Technology, June 2010, available: http://www.bth.se/[accessed on18/1/2014,1:30 p.m].

Authors Profile

Mrs. Amninder Kaur Gill is Teaching as Assistant Professor (CS) in Punjabi University Regional Centre for Information Technology and Management, Mohali, India.

Yog Kunwar is a Student and Doing M. Tech From Punjabi University Regional Centre For Information Technology and Management, Mohali, India.