International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Performance Evaluation of Different Protocols under Blackhole and Wormhole Attacks

Gurmeet Singh[1], Deepinder Singh[2], Dr. Ravi Kant[3]

[1]Bhai Gudas Global Polytechnic College, Patiala, India

[2, 3]Bhai Gurdas Institute of Engineering and Technology, Sangrur, India

Abstract: ***Mobile Ad hoc Networks (MANETs) refer to mostly wireless - networks where all network components are mobile. In a MANET there is no distinction between a host and a router since all network hosts can be endpoints as well as forwarders of traffic.***

Keywords: MANET, AODV AOMDV, TORA, BLACK HOLE , WORMHOLE , NS-2

1. Introduction

Mobile Ad hoc Networks (MANETs) refer to mostly wireless - networks where all network components are mobile. In a MANET there is no distinction between a host and a router since all network hosts can be endpoints as well as forwarders of traffic. Mobile ad hoc networks are self-organizing network of mobile nodes that use wireless links to form a network. This network is a momentarily network that can be destroyed anytime. This network formed dynamically and share common wireless link. As in tradition networks there is not basic fixed structure. Nodes are free to move randomly and can leave or join the network on the fly. In MANET each node works as both host and route. A mobile ad hoc network (MANET) is a group of mobile devise connected by wireless link without the requirement of fixed common infrastructure in place like wireless access point or base station point.[1] A significant number of research efforts have been devoted to investigate Mobile Ad Hoc Networks (MANETs) over the past few years [1,3]. Interest in MANETs is due to their promising ubiquitous connectivity beyond that is currently being provided by the Internet. Firstly, MANETs are easily installed allowing a plug-and-communicate method of networking. Secondly, MANETs need no fixed type of network. A number of MANET routing protocols were proposed in the last years. These protocols can be organize according to the "routing strategy" that they follow to find a path "route" to the destination. [1] In general, mobile ad hoc network (MANET) is formed dynamically by autonomous systems of mobile nodes that are connected wirelessly without support of any existing network infrastructure or centralized administration. Without any wired infrastructure, it is envisaged that MANET could be install in applications such as search and rescue, automated battle fields, calamity recovery, intelligent transportation and sensor networks. The nodes that make up a network at any time communicate with and through each other. In this way every node can begin a connection to every other node that is included within MANET.[2] The nodes of such a network are allowed to move freely in random fashion due to which the network topology changes dynamically. The mobility (i.e. how nodes move) of mobile nodes plays an important role on the performance of routing protocols [7] MANETs exhibit some of the characteristics to accomplish consistent and secure wireless communication. They may include Confidentiality, Availability, Authentication, Integrity and Non-repudiation [8].

Confidentiality: Protection of data packets from malicious nodes. Normally intermediate nodes may eaves drop the information which is passing through those nodes. It‟s a searching job to prevent data packets being disclosed by compromised nodes.

Availability: The feature of present at any time. Denying a service when it is required is one kind attack happens in MANET environment. Security protocols should offer minimum survivability even though there is a Denial of Service (DOS) attack.

Authentication: A security measure intended to protect communication system from fraudulent transmission. An attacker may imitate a node and achieve unauthorized access to resource and sensitive information if there is no authentication.

Integrity: Giving assurance that information being whole and unchanged.

Non-repudiation: protect that source and destination nodes can never deny about their sending and receiving of information

This paper is structured as follows**. In Section 2, common network security attacks include advanced attacks in network layer. In Section 3, defense Metrics against Routing Attacks in ad hoc environment. In Section 4, a discussion on open challenges and future directions.**

2. Literature Review

The Author assess the performance of three well-known and widely investigated MANET routing protocols. They have analyzed the performance of DSR, AODV and OLSR routing protocols are used. The simulation is done by the NS-2, and nodes are moving at speeds ranging from 0 to 20 m/s. In order to mimic traffic models that are statistically self-similar, a number of Pareto traffic connections were aggregated yielding an ever bursty traffic model. Different

performance aspects are conduct are packet delivery ratio, routing overhead, throughput and end to- end delay. The results indicate that DSR routing protocol performs well with bursty traffic models compared to AODV and OLSR parameters are used delivery ratio, throughput and end-to-end delay. The OLSR performed poorly in the presence of self-similar traffic at high mobility especially in terms of data packet delivery ratio, routing overhead and delay. As for AODV routing protocol, the results show an average performance, yet a remarkably low and stable end-to-end delay. [1]

In this paper the authors described the formal evaluation of performances of three types of MANET DSR ,AODV and TORA routing protocols when the node density or the number of nodes varies.. The analysis had been done using an Optimized Network Engineering Tools (OPNET) Modeler. The performances had been analyzed are packet delivery ratio, end-to-end delay, packet dropped, routing load and end-to-end throughput. DSR to have a longer delay than the rest of two. AODV shows the better delay characteristic. In all the scenarios, AODV displays the smallest delay and loss ratio and the adaptive ability is also of relative strength.[2]

The performance of three routing protocols AODV, DSR and used and WRP for FTP, TELNET and CBR traffic are analyzed. Performance parameters are packet delivery ratio, throughput, average end to end delay and routing message overhead. The AODV shows the best performance in terms of delivery ratio, throughput, routing message overhead, and end-to-end delay. WRP has the minimum end-to end delay while DSR requires minimum number of routing messages. The proactive protocol WRP shows better results than reactive protocol DSR but AODV outperforms the two. DSR tends to performs poorly in more stressful scenarios. [3]

3. Overview of Adhoc Routing Protocols

The primary goal of routing protocols in ad-hoc network is to establish minimum path (min hops) between source and destination with minimum overhead and minimum bandwidth use so that packets are transmitted in a timely manner. A MANET protocol should function adequately over a large range of networking context from small ad-hoc group to larger mobile multihop networks[4]In MANETS, the main purpose of the convention or standard protocols is to control the way in which the mobile nodes decide how to transfer the route packets to each other. These protocols are broadly classified into three main categories namely proactive, reactive and hybrid protocols. Proactive protocols maintain routes to all nodes, including nodes to which no packets are sent. Proactive protocols include DSDV, OLSR and WRP. In reactive protocols, routes between hosts are determined only when they are explicitly needed to forward packets. Reactive protocols include AOMDV, AODV, DSR, TORA and CBRP. Hybrid methods combine proactive and reactive methods to find efficient routes, without much control overhead

3.1 AODV

Ad Hoc On-Demand Distance Vector routing protocol uses broadcast discovery mechanism, similar to but modified of that of DSR[1], [3], [4] ,[6] . To ensure that routing information is up-to-date, a sequence number is used. The *path discovery* is established whenever a node wishes to communicate with another, provided that it has no routing information of the destination in its routing table. *Path discovery* is initiated by broadcasting a route request control message "*RREQ*" that propagates in the forward path. If a neighbor knows the route to the destination, it replies with a route reply control message "*RREP*" that propagates through the reverse path. Otherwise, the neighbor will re-broadcast the *RREQ*. The process will not continue indefinitely, however, authors of the protocol proposed a mechanism known as "*Expanding Ring Search*" used by Originating nodes to set limits on *RREQ* dissemination. Out of various reactive protocols proposed for MANET, AODV [7] is an on-demand routing protocol, in which the route between the source and destination node is discovered as and when needed

3.2 AOMDV

AOMDV has got similarity in features comparing to AODV. AOMDV is based on the distance vector concept and uses hopping routing approach. Apart from that, AOMDV also finds routes on demand using a route discovery procedure. The main difference is in the number of routes found in each route discovery.

In AOMDV, RREQ propagation would entitle the source towards the destination multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back to create multiple forward paths to the destination at the source and intermediate nodes. AOMDV provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency. AOMDV protocol should ensure that multiple paths discovered do not make any loop and disjoint, and in efficiently finds if such paths use a flood-based route discovery.

3.3 TORA

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal. TORA is proposed for highly dynamic, mobile, multi hop wireless networks. It is a source initiated routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes. The protocol has three basic functions: Route creation, Route maintenance and Route erasure. TORA can suffer from unbounded worst-case convergence time for very stressful scenarios. TORA has a unique feature of maintaining multiple routes to the destination so that topological changes do not require any reaction at all. [11]

4. Attacks in MANET

Wireless networks are more vulnerable than a wired network. There is a range of attacks aim at the weakness of MANETs. All data packets should pass through many intermediate nodes before reaching destination. Each node maintains route entry to other nodes in two ways either node itself initiates the route discovery or other nodes push to discover routes.

A. Wormhole Attack in MANET

In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called "wormhole link". They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network. Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets. [5].[8]

B. Black Hole Attack in MANET

The black hole attack[5] is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to announce itself as having a accurate route to a destination node, even though the route is counterfeit, with the intention of intercepting packets. In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have a fresh enough routes to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node instatly responds with an RREP message that contains the highest sequence number and this message is received as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source considers that the destination is behind the black hole and rejects the other RREP packets coming from other nodes. The source then starts to transmit out its data packets to the black hole believing that these packets will reach the destination. Vulnerabilities of ad-hoc networks against black hole attacks have solution based on modification of the AODV protocol

4.1 Simulation Model and Simulation Parameters

A. Performance Metrics

In order to evaluate the performances of three MANET protocols, several metrics need to consider. These metrics reflect how efficiently the data is delivered. In epidemic routing, multiple copies may be delivered to the destination. According to the literatures [1], [2], some of these metrics are suggested by the MANET working group for routing protocol evaluation.

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

ii. Average End-to-end Delay
This includes all the possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

iii. Throughput
The total successfully received packet to the destination. In the other words, the aggregate throughput is the sum of the data rates that are delivered to all nodes in a network.

4.2 Simulation Results

In this section we present the simulation results for AODV , AOMDV anf TORA routing protocol along with a detailed analysis of the performance. The analysis is based on the comparison of different metrics stated in the last section for the routing protocol. For the analysis we have also considered the metrics for the same network with different number of sources
The Simulation is carried out in NS2 under LINUX platform. The following table shows that the important parameters chosen for the NS2 simulation

Topology Size	710m x 550m
Number Of Nodes	19
MAC Type	MAC 802.11
Radio Propagation Model	Propagation/TwoRayGround
Radio Propagation Range	250m
Pause Time	0s
Max Speed	4m/sec-24m/sec
Initial Energy	7J
Transmit Power	0.4W
Receive Power	0.3W
Traffic Type	CBR
CBR Rate	512 bytes x 6 per second
Source id	5 for Blackhole
destination Id	6 for blackhole
attacker node Id	10 blackhole
Routing Protocols	AODV, TORA, AOMDV
Observation Parameters	PDF , end to end delay , Through put, energy
attacker node Id	8 and 9 for wormhole

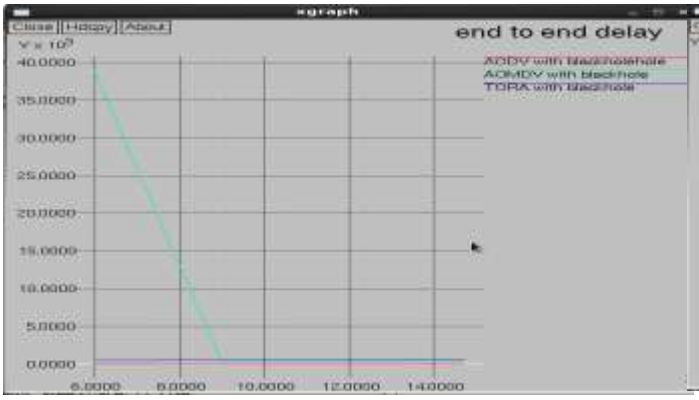

Figure 1.1: end to end delay with Blackhole

Figure 1. 1. Shows the comparison of end to end delay versus time TORA, AODV and AOMDV. It shows that the end to end delay is minimum using AOMDV compared to AODV, TORA, DSR and DSDV.TORA is having the highest end to end delay compared to all the other protocols. This comparison is analyzed with the Blackhole

Figure 1.2: end to end delay with wormhole

Figure 1.2. shows the comparison of end to end delay versus time for TORA, AODV and AOMDV. It shows that the end to end delay is minimum using AODV compared to AOMDV, TORA. TORA is having the highest end to end delay compared to all the other protocols. This comparison is analyzed with the wormhole attack

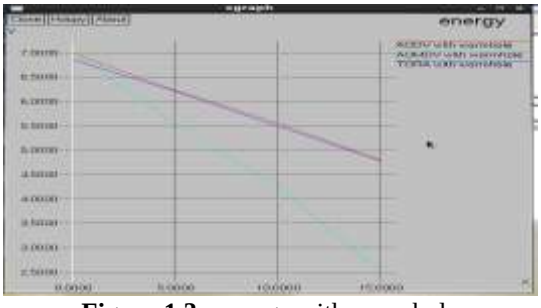

Figure 1.3: energy with wormhole

Figure 1.3. shows the Comparison of Energy consumption versus time for TORA, AODV and AOMDV .It shows that the energy consumption of networks using TORA is minimum compared to AOMDV and AODV. AODV is consuming maximum energy. AOMDV is consuming lesser energy than AODV and more than TORA. This comparison is analyzed with the Wormhole attack

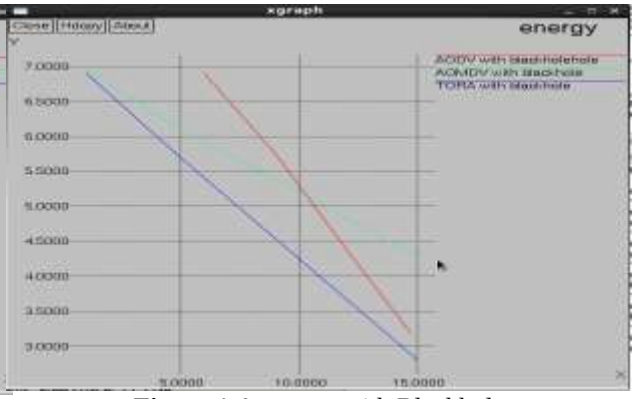

Figure 1.4: energy with Blackhole

Figure 1.4. Shows the Comparison of Energy consumption versus time for TORA, AODV and AOMDV. It shows that the energy consumption of networks using AOMDV is minimum compared to TORA and AODV.AODV is consuming maximum energy. This comparison is analyzed with the blackhole attack

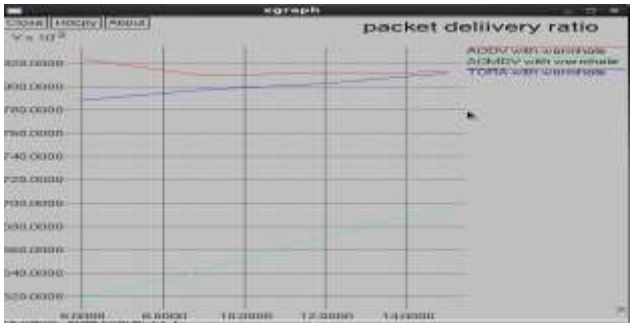

Figure 1.5: Packet delivery ratio with wormhole

Figure 1.5. shows the comparison of Packet delivery ratio versus time for TORA, AODV and AOMDV. It shows that the packet delivery ratio of networks using AOMDV is better compared to AODV and TORA .TORA has poor packet delivery ratio than all the other protocols. This comparison is analyzed with the wormhole attack

Figure 1.6: Packet delivery ratio with wormhole

Figure 1.6 shows the comparison of Packet delivery ratio versus time for TORA, AODV and AOMDV. It shows that the packet delivery ratio of networks using AOMDV is minimum than AODV and TORA. AODV has poor packet delivery ratio than all the other protocols. This comparison is analyzed with the wormhole attack

5. Conclusion & Future Work

We have simulated and compared the two reactive protocols AOMDV and AODV and TORA in different simulation scenarios and observing their behaviour in terms of three significant parameters i.e. Packet delivery fraction, energy and PDR The simulation scenario consisting of minimum 2 and maximum of 100 nodes is created by writing the OTCL script in NS-2 (version 2.34) and analyzing the parameters through with the help of generated X Graph. By studying and analyzing the outputs appeared in X Graph

It can be further extended by implementing the scenario with the different mobility models, different network and traffic scenarios and observing the behaviour of protocols by varying the simulated time. Also the behaviour of the protocols can be studied further by carrying the simulations on different parameters like varying the number of mobile nodes, the topology area choice of the traffic type between the mobile nodes other than the simulation time. It could be analyzed the impact caused in value of QoS metrics when using different mobility patterns, because due to the increasingly mobility, the tendency is a degradation in values of QoS metrics. Wireless Ad-Hoc networks are widely used networks due to their flexible These networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is l need in this area. We tried to discover and analyze the impact of Black Hole attack in MANETs using AODV, TORA and AOMDV protocols.

References

[1] Ahmed Al-Maashri Mohamed Ould-Khaoua "Performance Analysis of MANET Routing Protocols in the Presence of Self-Similar Traffic ." pp. 801-807
[2] Adam, N., Ismail, M. Y. and Abdullah, J., 2010. "Effect of node density on performances of three MANET routing protocols", International Conference on Electronic Devices, Systems and Applications, pp. 321-325
[3] Arora,V. and Krishna, C.R., 2010 "Performance Evaluation of Routing Protocols for MANETs under Different Traffic Conditions." 2nd International Conference on Computer Engineering and Technology, vol. 6 pp. 79-84.
[4] Bhosle, A. A., Thosar , T.P. , and Mehatre. S. 2012. "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET."*International* Journal of Computer Science, Engineering and Applications, vol. 2, No. 1, pp 45-54
[5] Balachandran, N., 2012. "Surveying Solutions to Securing On-Demand Routing Protocols in MANETs" Int. J. Advanced Networking and Applications vol. 4 , pp. 1486-1491.
[6] Chaba , Y., Singh ,Y. and Joon .M., 2010. "Simulation based Performance Analysis of On-Demand Routing Protocols." Second International Conference on Computer Modelling andSimulation pp. 80 – 83.
[7] Das , M., Panda, B.K., and Sahu, B., 2012. " Analysis of Effect of Mobility on Performance of AODV in Mobile Ad hoc Network." International Conference on Computer Communication and Informatics,
[8] Devi, P., and Kannammal, A., 2012. "Security attacks and Defensive Measures for Routing Mechanisms in MANETs – A Survey." International Journal of Computer Applications,vol, 42, No.4, pp. 27-32.
[9] Ghahremanloo, P. 2011. "Multi-Path Routing Challenging Single-Path Routing in Wireless Mesh Networks.: Network modeling of AODV and AOMDV" International siberian Conferenceon Control and Communication , pp. 12-15. (Ghahremanloo,P. 2011)
[10] Goyal, P., Batra, S., and Singh, A., 2010 "A Literature Review of Security Attack in Mobile Ad-hoc Networks." International Journal of Computer Applications,vol, 9. No.12, pp. 11-15
[11] Jacob,J., and Seethalakshmi,V., 2012 , " Performance Analysis and Enhancement of Routing Protocol in MANET ." International Journal of Modern Engineering Research, vol. 2, pp. 323-328.
[12] Moses, G.J., Kumar, D.S., Varma, P.S., Supriya, N., 2012" A Simulation Based Study of AODV, DSR, DSDV Routing Protocols in MANET Using NS-2" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, March 2012 pp. 42- 51
[13] Nishat, H., Pothalaiah ,S. and Rao, D.S., "Performance Evaluation of Routing Protocols in MANETS." International Journal of Wireless & Mobile Networks .v ol. 3, No. 2, pp. 67-75.
[14] Shrestha, A., and Tekiner, F., 2009. "On MANET Routing Protocols for Mobility and Scalability." International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 451-456.

Author Profile

Gurmeet Singh received the B.Tech and Pursuing M.Tech. degrees in Electronics and communication Engineering from PTU in 2009 and 2012, respectively.