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

Yog Kunwar

Punjabi University Regional Centre for I.T. and Mgmt.
Mohali, India
Email: *yogkunwar@yahoo.co.in*

Abstract
Mobile ad hoc network (MANET) is a Wireless, self-configuring network that consists of many movable mobile nodes. These mobile nodes contact with one another with none infrastructure. Because wireless Ad-hoc networks lack associate degree infrastructure, they're exposed to plenty of attacks. One in all these attacks is the Black Hole attack. In Black Hole attack, a malicious node incorrectly advertises shortest path to the destination node and absorbs all information packets in it instead of forwarding information packet.
Keywords: MANET, AODV, Black Hole attack, malicious node.

1. Introduction

A Mobile Ad-hoc Network is an aggregation of mobile nodes that are autonomous and each can communicate with other using radio waves without any centralized command. Each of the nodes has a wireless interface and using it nodes communicate with each other. The mobile nodes that are in communication range of each other can interact directly with each other, whereas other nodes which are not in the radio range take the help of intermediate nodes to route their information packets to the destination i.e. intermediate nodes act as routers [1]. There are different types of routing protocols used in MANETs. Proactive routing protocols also are called table driven routing protocols. In this, node maintains the routing table, consists of recent routes to the destination, at the regular interval of your time, by exchanging the table data between the nodes sporadically. Examples: Destination Sequenced Distance Vector Routing (DSDV) etc. Reactive routing protocols initiate the route discovery only if a node needs a route to the destination node, to that the node desires to send the information. That's why, they're additionally termed as on-demand routing protocols. Examples: Ad-hoc On-Demand Distance Vector Routing (AODV), Dynamic supply routing (DSR) etc. Hybrid routing protocols square measure the mixture of each the techniques utilized in proactive and reactive protocols. Examples: Zone Routing Protocol (ZRP) etc [9].

The network layer in MANET is prone to numerous attacks viz. eavesdropping with a malicious intent, spoofing the management and /or knowledge packets transacted, malicious modification of packet contents and therefore the Denial-of-service (DoS) attacks viz. Wormhole attacks, Sinkhole attacks, Blackhole attacks. Blackhole is one among several attacks that happens in MANET and is taken into account as foremost common attacks created against the AODV routing protocol. The Blackhole attack involves malicious node feigning to own the shortest and freshest route to the destination by constructing false sequence range up to the mark message. AODV routing protocol was created with none security issues. Thus, no protection mechanism was engineered to sight the existence of malicious attack. Within the AODV, maintaining a contemporary route to confirm safe path to destination is incredibly important as a result of the speedy amendment of the topology. The manipulation done by the malicious node can deny the real Route Reply (RREP) message from various nodes particularly the reply message returning from the particular destination node [4]. In this paper a node is shown as malicious node that acts as a Blackhole attack in AODV.

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

Ad hoc On-Demand Distance Vector (AODV) is a routing protocol for wireless Ad hoc networks. It's a reactive protocol that discovers a route to a destination only when needed [5]. AODV could be a variation of DSDV (Destination Sequenced Distance Vector). The essential feature of AODV is to attenuate the broadcasts. AODV solely establishes route on demand and create use of destination sequence numbers to stay track of current routing ways [6].

In AODV the node that wants an association broadcasts a route request message i.e. RREQ. Every neighboring node will perform one amongst the subsequent 2 actions [5]:Send the route reply message i.e. RREP message to the sender node if it already has the route to the destination or Make entry into its routing table regarding the sender node, increment hop count within the RREQ message and air the RREQ message to its neighbors.

The route request reaches the destination or some intermediate node that has recent route to destination and mechanically creates the reverse path. The RREP message follows the reverse path and sets up forward pointers for sending data packets to the destination. In no time the sender receives a RREP message and it will begin causation the information packets. If later sender receives a RREP message having the greater sequence number or same sequence number with less number of hops count, it updates its routing table and starts using the best route to the destination i.e. a route with less hop count higher sequence number. If a link break happens, the upstream node sends a route error message i.e. RERR message to the sender, and route discovery is reinitiated at the sender if the sender still needs a route to the destination [5].

Freshness of the routing management messages i.e. RREQ, RREP and RERR etc. is decided by the sequence numbers utilized in the messages. Before forwarding any form of routing management message, the node increments the sequence number of the message. The greater sequence number indicates a lot of recent data. Whenever a node receives multiple management messages, the one with the very best sequence number is taken into account as newest and it's utilized in forming route to different nodes [5].

3. Blackhole Attack

MANETs are susceptible to varied sorts of attacks. Attackers carry out attacks against MANETs with the intention of disrupting the normal performance of the networks. Among various attacks, Black hole attack is a kind of attack which occurs in Mobile Ad-Hoc networks (MANET). It's similar to the Blackhole in the universe within which things disappear [8]. It is a basic attack in which a malicious node executes to stop forwarding the data packets. The malicious node convinces the other nodes by claiming that it has the 'fresh route' information to the destination. If the malicious nodes fit into this ambush i.e. if the malicious node is selected as a route, they will send their data packets through the malicious node [4]. As a result, it does not allow the communication to take place or the node consumes the packets instead of forwarding them [10]. But it also depends upon the configuration of the malicious node set by the attacker that whether it drops all the packets or forwards some of them [8].

Fig. 1 shows how Blackhole problem arises. The figure describes that node "A" is the sender node and need to send knowledge packets to the destination node "D". Node A initiates the route discovery method. Thus if node "E" is acting as the malicious node then it'll claim that it's active route to the destination node and in no time it receives RREQ packets from the sender node. It'll then send the RREP to sender node "A" before any other node. This means the malicious node wins the confidence of node "A" that it has an energetic route and there's no ought to notice the other route to the destination node "D". Node "A" can ignore all alternative replies and can begin sending knowledge packets to node "E". As node "E" is the malicious node, thus the entire information packet are consumed instead of forwarding them. But it also depends upon the configuration of the malicious node set by the attacker that whether it drops all the packets or forwards some of them [8].

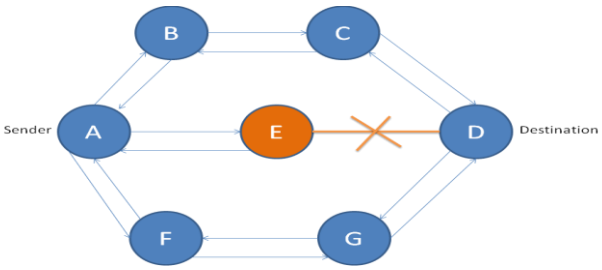

Figure 1: Black Hole attack.

4. Performance Metrics

The performance metrics chosen for the analysis of part attack are end-to-end delay, network output and network load.

4.1 End-to-End Delay: The packet end-to-end delay is that the time from the generation of a packet by the source up to the destination reception, thus this can be the time that a packet takes to travel across the network. This point is expressed in seconds (sec) [3].

4.2 Throughput: Throughput or Network output is the ratio of total quantity of information that reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It's represented in bits per second or packets per seconds [8].

4.3 Network Load: Network Load is that the quantity of information (traffic) being carried by the network at a selected time. The network load varies from time to time. It's represented in bits per second or packets per seconds [8].

5. Simulation Results

A piece of software or hardware that anticipate the actions or operations of the network, without a real network being present is called network simulator. Evaluating the network performance and other different network related tasks can be done simply by using varied network simulators. Varied network simulators are available in market. Examples of network simulation software are ns2/ns3, OPNET, NetSim etc [7].

NS-2 (version 2.35) is employed for simulation. Network Simulator-2 (NS-2) is an object-oriented, discrete event network simulator that plays a vital role in network analysis and development. It's one amongst the foremost wide used open source network simulators [2].

Single scenario has been considered to evaluate the parameters under consideration i.e. Network load, throughput and end-to-end delay. Implementation of AODV has been done using NS2 and XGRAPH utility has been used to draw graphs. In implementation scenario, 11 nodes are deployed in a 1363 × 651 area. Radio propagation model is being used in this simulation with antenna type as Omni directional and vbr traffic is used.

5.1 Comparative Analysis-End-to-End Delay

Fig. 2 shows the End-to-End Delay of AODV routing protocol with vs. without Blackhole attack. It describes that the End-to-End Delay of AODV routing protocol with

Blackhole attack is almost double than the End-to-End Delay of AODV routing protocol without Blackhole attack.

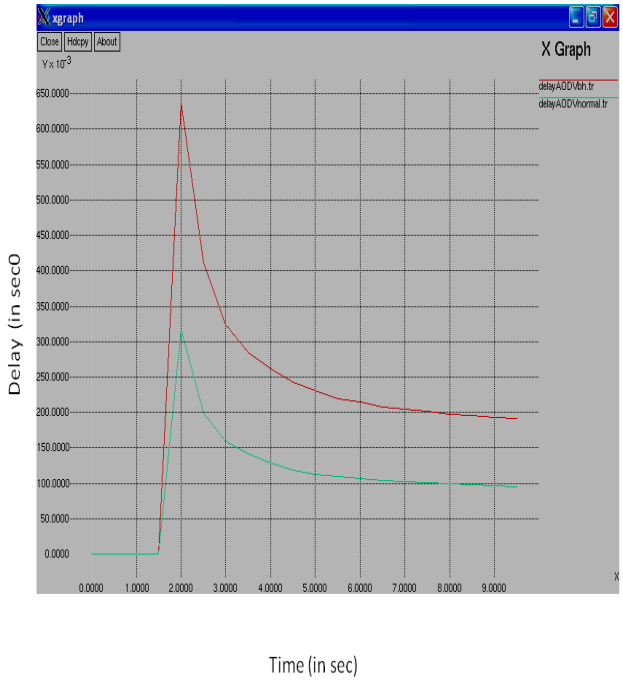

Figure 2: End-to-End Delay of AODV with vs. without attack

5.2 Comparative Analysis-Throughput

Fig. 3 shows the Throughput of AODV routing protocol with vs. without Blackhole attack. It describes that when simulation starts, the throughput of AODV routing protocol without Blackhole attack is higher than throughput of AODV routing protocol with Blackhole attack and remains higher. The throughput of AODV routing protocol with Blackhole attack is less because of malicious node or Blackhole node discard packets instead of forwarding them.

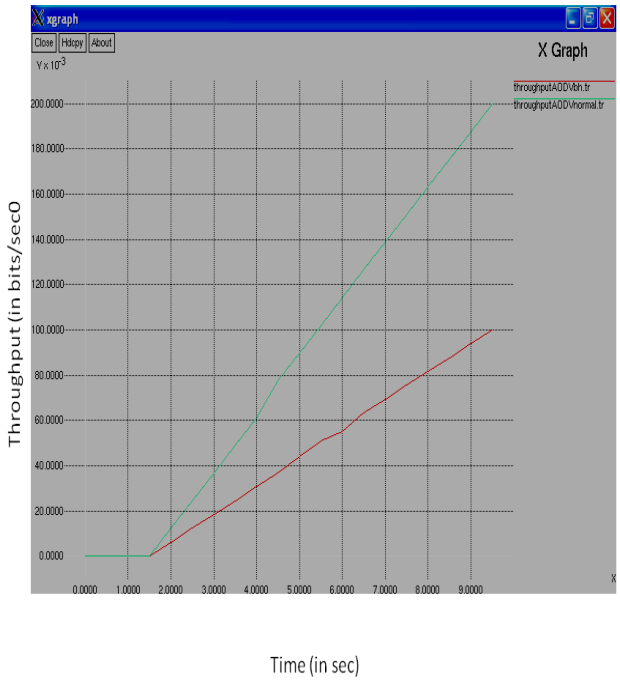

Figure 3: Throughput of AODV with vs. without attack

5.3 Comparative Analysis-Network Load

Fig. 4 shows the Network Load of AODV routing protocol with vs. without Blackhole attack. It describes that when simulation starts, the Network Load of AODV routing protocol without Blackhole attack is lower than Network Load of AODV routing protocol with Blackhole attack. Network Load of AODV routing protocol with Blackhole attack is almost double to that of Network Load of AODV routing protocol without Blackhole attack.

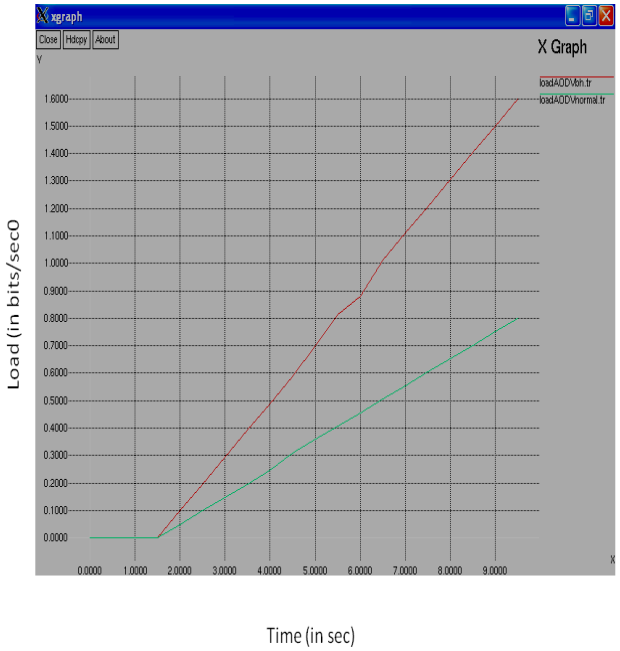

Figure 4: Network Load of AODV with vs. without attack

6. Conclusions

In this paper, the performance of AODV routing protocol with and without Blackhole attack has been analyzed for various performance metrics: end-to-end delay, throughput and network load. Simulation results show that once a node attains the behavior of a malicious node it will have an effect on the performance AODV, in turn affecting the performance of network. The route discovery procedure within the AODV is vulnerable to Blackhole attack and thus, it has become very important to have an efficient security mechanism so as to guard the protocol from such attacks.

7. Future Work

In future work, comparative analysis of various routing protocols like DSR, OLSR, DSDV etc using different parameters like traffic send, traffic received etc can be performed. As far as future security is concerned, new security mechanisms or solutions can be designed so as to supply security to different routing protocols against Balckhole attack. Plenty of analysis work needs to be done in this space.

S 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, May 2013, ISSN: 2277 128X.

[2] Agarwal T. & Jain N., *Simulate Your Network with NS2*, June 2013, Available: http://tejaswiagarwal.com/research.html.

[3] Al-ani R.,"Simulation and Performance Analysis Evaluation for Variant MANET Routing Protocols", *International Journal of Advancements in Computing Technology*, vol. 3, no. 1, pp. 1-12, February 2011.

[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] Ehsan H. & Khan F.A., "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs", *in proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012.

[6] Nayyer M. Z., "Analysis of AODV over increased density and mobility in Intelligent Transportation System", *IJCSI International Journal of Computer Science Issues*, vol. 9,issue 5, no. 1, 2012.

[7] Singh N., Rajeshwa P., Dua L. & Mathur V., " Network Simulator NS2-2 . 35", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 5, pp. 224–228, May 2012, ISSN: 2277 128X.

[8] 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/fou/cuppsats.nsf/all/448194ba63f382fdc1257751006226b8/$file/Final_Thesis_Report_irua08_resa08%20Analysis%20of%20Blackhole%20Attack.pdf.

[9] Vishesh K. & Verma A., " Formal Verification of Authenticated AODV Protocol using AVISPA", *International Journal of Computer Applications* , vol. 50, no. 19, pp. 38–43, July 2012.

[10] Yadav H. & Kuma R., "Identification and Removal of Black Hole Attack for Secure Communication in MANETS", *International Journal of Computer Science and T*elecommunications, vol. *3*, no. 9, pp. 60-67, September 2012.

Author Profile

Yog Kunwar has received the degree of B.Tech. in Computer Science and Engineering from Swami Devi Dyal Institute of Engineering and Technology, Barwala, Panchkula, India in 2011. She is currently pursuing M.Tech fromPunjabi University Regional Centre for I.T. and Mgmt., Mohali, India.