International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

# Black Hole Attack Prevention and Detection Solutions on AODV Routing Protocol in MANET

**Pandi Selvam Raman**
Assistant Professor & Head, Department of CS & IT, Ananda College, Devakottai, Sivaganga, Tamil Nadu, India

## ABSTRACT

Mobile ad hoc network (MANET) is a self-configuring network that is formed via wireless links by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Securing wireless ad hoc networks is particularly difficult for many reasons including vulnerability of channels and nodes, absence of infrastructure, dynamically changing topology and etc. Black Hole attack is one of the major attack and this detection and prevention is still considered as a challenging task in ad hoc networks. Therefore this paper compares various Black Hole attack prevention and detection solutions that are explored recently.

**Keywords:** MANET, Routing, AODV routing protocol and Black hole attack

## I. INTRODUCTION

A MANET is a self-configuring (autonomous) system of mobile hosts connected by wireless links. The nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably [1]. An ad hoc network can be set up anywhere without any assistance of external infrastructure like wires or base stations. Networks are formed on-the-fly i.e. devices can leave and join the network during its lifetime. In general, MANET can operate in two modes namely peer-to-peer (communicate directly within their radio range) and multi-hop (communicate via intermediate nodes outside their radio range) [2]. MANETs are used at business meetings and conferences to confidentially exchange data, at the library to access the Internet with a laptop, and at hospitals to transfer confidential data from a medical device to a doctor's PDA etc.

Routing is the process of exchanging information from one station to the other stations of the network [3]. It may divide into different aspects. Route construction (topology) based it further divided into three types namely i. Tree based ii. Mesh based and iii. Hybrid. The tree based routing scheme has single path between the source and receiver. In mesh based approach multiple redundant paths connect the source and the destination. The hybrid approach attempt has been made to combine both the mesh-based and the tree-based approaches.

Based on routing update mechanism protocols are classified as table driven (proactive or pre-computed routing), on-demand (reactive routing) or hybrid. In proactive routing, nodes are continuously evaluate the routes to all reachable nodes and attempts to maintain up-to-date routing information. In reactive nodes do not maintain routing information if there is no communication. In hybrid, the nodes are balanced which delay and overhead of both proactive and reactive [4].

The structure based routing protocols are classified as flat and hierarchical. In a flat structure, all nodes in a network are at the same level and have the same routing functionality. In hierarchical, nodes are dynamically organized into partitions called clusters [5].

Security is an essential service for wired and wireless network communications. However, MANETs are much more vulnerable to attack because of its non-trivial challenges such as lack of fixed infrastructure, dynamic topology, link variation and energy constraints. So, each and every node in the network has to prepare for attacks at any point of time. And also as there is no central based controlling identity for the participating nodes; the attacks are much easier to launch in MANET.

Black Hole Attacks are a kind of serious security service where a malicious node advertise itself a shortest path during routing discovery and redirect the data towards malicious node. Malicious node dropped the data or its desired destination instead of original destination.

This paper organized as follows: Section II describes AODV routing protocol. Section III discusses how the Black Hole attacks have an effect on ad hoc network. Comparison of recent researches against black hole attacks on AODV are presented in Section IV followed by conclusions is Section V.

## II. AODV ROUTING PROTOCOL

Ad hoc On-demand Distance Vector (AODV) is one of the most effective routing protocol in MANET [6]. AODV is an On-Demand routing protocol that discovers route only when there is demand from mobile node. AODV uses three control messages. They are

*RREQ*: Initially when any node wants to communicate with other node but no any route is available already, the source node starts a route discovery process by flooding a Route REQuest (RREQ) message in the network. This message is broadcasted by each node to its neighbour.

*RREP:* When node in the network receive RREQ,if it is a destination node or an intermediate node has a valid route to the desired destination, it replies to a RREQ by unicasting a Route REPly (RREP) message back to the source node.

*RERR*: If a path breaks, the intermediate node generates a Route ERR or (RERR) message to inform its end nodes of the occurred link break.

The process of route discovery is started with checking route availability. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available or not. If required path is already available, it uses that route to send the packets to the destination. But if a route is not available or the previously entered route is inactivated, then the node initiates a new route discovery process by flooding RREQ (Route REQuest) packet in network.

Every node (neighbour) that receives the RREQ packet first checks if it is the destination for that packet and if so, it unicast back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination previously. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet.

RREQ packet contains the hop count, Source IP and Sequence number, Destination IP and sequence number in its packet format. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route otherwise it is outdated route.

The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. For such a reporting RERR contains a list of possible neighbors.

Figure1. Illustrates the AODV protocol where *S* is source node and *D* is destination node. First, the source node *S* refers to the route map at the start of communication to check previous available routes. In case when there is no route to destination node *D*, it broadcasts RREQ message. RREQ ID increases one every time node *S* sends a RREQ.

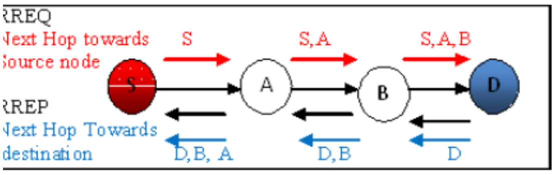

**Figure 1.** Working of AODV Routing Protocol

Node *A* and *B* which have received RREQ generate and renew the route to its previous hop. They also judge if this is a repeated RREQ. If such RREQ is received, it will be discarded. If *A* or *B* has a valid route to the destination *D*, they send a RREP message to node *S*. This process goes on until the packet is received by destination node. When node *D* receives the RREQ, it sends RREP to node *S* through reverse path. When node *S* receives the RREP, then a route is established. In case a node receives multiple RREPs, it will select a RREP whose destination sequence number (Dst_Seq) is largest among all previously received RREPs. But if Dst_Seq were same, it will select the RREP whose hop count is the smallest because it indicates that particular route have shortest distance towards destination.

## III. BLACK HOLE ATTACK

Black hole Attack is a type of Denial of Service Attack. Black hole Attack is a malicious node uses its routing protocol to advertise itself having the shortest path towards destination node. When route is established, then malicious node drops the packets or forwards it to the attacker desired address [7].

In the Black Hole Attack the attacker must create a RREP with Dst_Seq greater than the destination sequence of the receiver node. The sender node believes that black hole node and further communicates with this black hole node instead of original destination node. This misbehaving mostly damage nodes interface and hence wasting all resource utilization in addition to losing packets. Black hole Attacks are classified into two categories [8].

***Single Black Hole Attack:*** Single Black Hole attack uses only single node acts as malicious node within a zone.

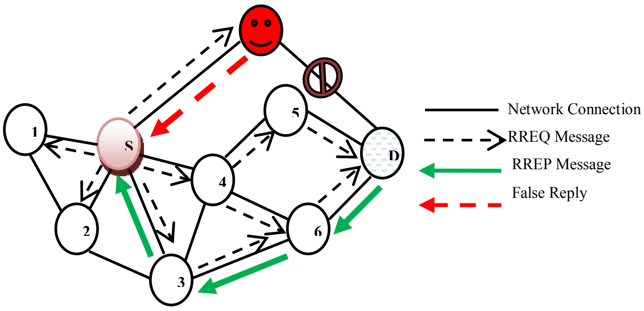

**Figure 2.** Single Black hole attack

***Cooperative Black Hole Attack:*** Collaborative Black Hole Attack uses multiple nodes in a group act as malicious node to drop all the data packets.

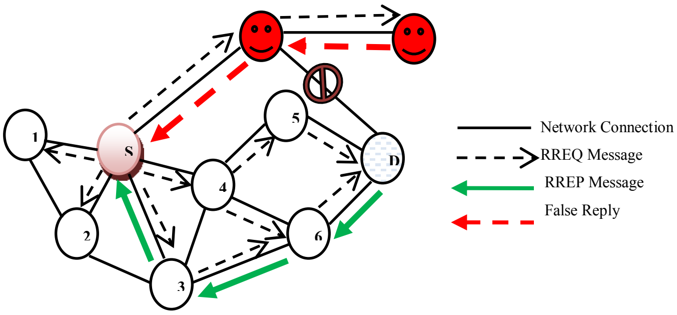

**Figure 3.** Cooperative Black hole attack

## IV. RECENT PREVENTION AND DETECTION AGAINST AODV ROUTING PROTOCOL

| SL. NO | AUTHOR | PAPER TITLE | METHOD NAME | DETECTION TYPE | TOOL USED | REMARKS | PUBLICATION YEAR |
|---|---|---|---|---|---|---|---|
| 1 | Ayesha Siddiqua et. al.[9] | Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm | Secure Knowledge Algorithm | Single Detection | NS-2.35 | Ensure data delivery to receiver node and finds packet drop reasons before declaring node as a black hole node. | **2015** |
| 2 | Miss Bhandare A.S. et. al.[10] | Securing MANET against Co-operative Black Hole attack and its performance analysis-A case study | Malicious Node Detection System | Cooperative Detection | NS-2.35 | Malicious Node Detection for AODV (MDSAODV) checks route reply against fake reply | **2015** |
| 3 | Nidhi Choudhary et. al.[11] | Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism | Timer-Based Detection Mechanism | Single Detection | EXata-cyber | Node defines a trust value for its neighbor node and inserts a timer with each data packet. | **2015** |
| 4 | Ali Dorri et. al.[12] | A New Approach for Detecting and Eliminating Cooperative Black hole Nodes in MANET | Data Routing Information | Cooperative Detection | Opnet 14.5 | Source node checks the Next_Hop_Node and Previous_Hop_Node of the RREP in order to check the malicious nodes in the path. | **2015** |
| 6 | Ashish Kumar Jain et. al.[13] | Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks | RREP caching mechanism | Single Detection | NS-2 | Modified the AODV routing protocol by ignoring the first RREP packet reaching the source node | **2015** |
| 7 | Anand A. Aware et. al.[14] | Prevention of Black hole Attack on AODV in MANET using hash function | Using Hash Function | Cooperative Detection | NS-2 | First RREP reject from its neighbor and will select the second optimal path | **2014** |
| 8 | Kriti Patidar et. al.[15] | Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks | Specification-Based Detection System | Single Detection | NS-2.35 | Individual nodes monitor the routing behavior of their neighbors for detecting run-time violation of the specifications | **2014** |
| 9 | Vishvas Kshirsagar et. al.[16] | Analytical Approach towards Packet Drop Attacks in Mobile Ad-hoc Networks | Bayes' Theorem and Prior probability | Single Detection | - | Finds packet dropper node from the network | **2014** |
| 10 | Gayatri Wahane et. al.[17] | Detection of Cooperative Black Hole Attack using Crosschecking with TrueLink in MANET | Crosschecking with True-Link (timing based countermeasure) concept | Cooperative Detection | NS-2 | True-Link-crosschecking method is designed to isolate and mitigate the effect of black hole<br>attack. | **2014** |

| SL. NO | AUTHOR | PAPER TITLE | METHOD NAME | DETECTION TYPE | TOOL USED | REMARKS | PUBLICATION YEAR |
|---|---|---|---|---|---|---|---|
| 11 | Harsh Pratap Singh et. al.[18] | A Mechanism for Discovery and Prevention of Cooperative Black hole attack in Mobile Ad hoc Network Using AODV Protocol | Broadcast Synchronization and Relative Distance method of clock synchronization | Cooperative Detection | NS-2.34 | The time sequence of internal and external clock compared with standard threshold time clock. | **2014** |
| 12 | Seryvuth Tan et. al.[19] | Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs | Secure Route Discovery | Single Detection | NS-2 | Verify the sequence numbers in the RREQ and RREP messages based on defined thresholds before establishing a connection. | **2013** |
| 13 | Durgesh Kshirsagar et. al.[20] | Blackhole Attack Detection and Prevention by Real Time Monitoring | Real Time Monitoring | Single Detection | NS-2.34 | Neighbors node maintains two counters Forward count-fcount and Receive Count-rcount for forwarded packets and number of received packets respectively | **2013** |

## IV. CONCLUSION

Mobile Ad-hoc network (MANET) is one form of temporary network which may get unprotected under different types of attacks. Black hole attack is a type of attack still which is an active research field. Therefore, this paper compared a few existing solutions of Black Hole Attack in AODV protocol. The researchers have considered many detection and prevention techniques for black hole attack whether single or cooperative. These solutions are discussed and compared with each other based on various metrics.

## V. REFERENCES

[1] Ram Ramanathan and Jason Redi, "A Brief Overview of Ad hoc Networks: Challenges and Directions," *IEEE Computer Magazine,* pp.20-22, 2002.

[2] Sheltami, Tarek, "Ad hoc Network Overview," http://www.ccse.kfupm.edu.sa/~tarek, Ad hoc network Technology, 2003.

[3] Changling Liu and Jorg Kaiser, "A Survey of Mobile Ad hoc Network Routing Protocols," Univ. of Ulm, *Tech. Rep.Series*, 2005.

[4] Krishna Gorantala, "Routing Protocols in Mobile Ad hoc Networks," *Master Thesis in Computing Science*, Umea University, Sweden, 2006.

[5] Geetha Jayakumar, and G. Gopinath, "Ad Hoc Mobile Wireless Networks Routing Protocols – A Review," *Journal of Computer Science* 3 (8), pp.574-582, 2007.

[6] S. Kalwar, "Introduction to reactive protocol," Potentials, IEEE, vol. 29, pp. 34-35, 2010.

[7] Ranjan, Rakesh, Nirnemesh Kumar Singh, and Ajay Singh. "Security issues of black hole attacks in MANET." *Computing, Communication & Automation (ICCCA), International Conference on*. IEEE, 2015.

[8] Kishor Jyoti Sarma, Rupam Sharma, Rajdeep Das, "A Survey of Black Hole Attack Detection in Manet." IEEE, 2014

[9] Ayesha Siddiqua, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." *Signal Processing and Communication Engineering Systems (SPACES), 2015 International Conference on*. IEEE, 2015.

[10] Miss Bhandare A. S., and S. B. Patil. "Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis-A Case Study." *Computing Communication Control and Automation (ICCUBEA), International Conference on*. IEEE, 2015.

[11] Nidhi Choudhary, and Lokesh Tharani. "Preventing black hole attack in AODV using timer-based detection mechanism." *Signal*

*processing and communication engineering systems (SPACES), International conference on*. IEEE, 2015.

[12] Ali Dorri and Hamed Nikdel. "A new approach for detecting and eliminating cooperative black hole nodes in MANET." *Information and Knowledge Technology (IKT), 2015 7th Conference on*. IEEE, 2015.

[13] Ashish Kumar Jain and Vrinda Tokekar. "Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile Ad hoc Networks." *Pervasive computing (ICPC), 2015 international conference on*. IEEE, 2015.

[14] Anand A.Aware and Kiran Bhandari. "Prevention of Black hole Attack on AODV in MANET using hash function." *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on*. IEEE, 2014.

[15] Kriti Patidar and Vandana Dubey. "Modification in routing mechanism of AODV for defending blackhole and wormhole attacks." *IT in Business, Industry and Government (CSIBIG), 2014 Conference on*. IEEE, 2014.

[16] Vishvas Kshirsagar, Ashok M. Kanthe, and Dina Simunic. "Analytical approach towards packet drop attacks in mobile ad-hoc networks." *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*. IEEE, 2014.

[17] Gayatri Wahane, Ashok M. Kanthe, and Dina Simunic. "Detection of cooperative black hole attack using crosschecking with truelink in MANET." *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*. IEEE, 2014.

[18] Harsh Pratap Singh and Rashmi Singh. "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol." *Electronics and Communication Systems (ICECS), 2014 International Conference on*. IEEE, 2014.

[19] Seryvuth Tan and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." *High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on*. IEEE, 2013.

[20] Durgesh Kshirsagar and Abhijit Patil. "Blackhole attack detection and prevention by real time monitoring." *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on*. IEEE, 2013.