MITIGATION OF BLACK HOLE ATTACK IN AODV PROTOCOL

Ankita V Rachh[1], Khyati M Mewada[2], Tejas R Rohit[3]

[1]Asst.Professor, I.T. Department, Atmiya Institute of Technology & Science, Gujarat, India
[2]Asst.Professor, I.T. Department, Atmiya Institute of Technology & Science, Gujarat, India
[3]Asst. Professor, C.E. Department, Darshan Institute of Engineering & Technology, Gujarat, India

Abstract

Mobile Adhoc network (MANET) is a wireless network. It is collection of different mobile nodes. The basic characteristics of MANET are dynamic topology and lack of centralization. Due to these characteristics MANETs are vulnerable to many attacks. Black hole attack is one of the attacks, which is performed on network layer. In black hole attack, malicious nodes disrupt transmission of data by sending false routing information. There are two types of black hole 5attacks. Single and collaborative. Single black hole attack has one malicious node, which can act as node with highest sequence number. Source node will follow malicious node's path by assuming correct route. Collaborative black hole attack has more than one malicious node. In this attack, one malicious node receives packet and send to another malicious node. Detection and prevention of black hole attack is very challenging task.

In this paper, our propose solution EBAODV (Enhance Black hole AODV) is presented. Many researchers have invented detection and prevention schemes of black hole attack. The comparative study of many researchers is also presented in this paper. Our solution EBAODV, focus on leader nodes. Leader nodes are used to detect black hole attack and prevent it by sending block table of malicious nodes.

Keywords: *AODV, Blackhole, EBAODV, MANET*

---***---

1. INTRODUCTION

Mobile Adhoc network (MANET) consists of various mobile nodes which are connected without any infrastructure. They can communicate with each other directly within the wireless medium. MANET topology changes frequently because nodes are mobile. They can move at any point of time from one location to another. Due to this, they can enter or leave network and disturb whole network. MANET is infrastructure less network, so no access point is required for central administration.

The life of mobile nodes is less compared to wired nodes. Mobile nodes move rapidly so they required more energy compared to wired nodes [11]. MANET requires more battery power and memory for mobile nodes. In MANET, every node can act as router as well as host. The function of router is to find optimum route from source to destination and transmit data. Each node is also act as normal host [20].

Routing in MANET is very challenging because nodes can changing their position frequently and it can affect to route [18]. The main goal of routing protocol is to select the optimum route from source to destination. The basic types of routing protocols are:

i) Proactive
ii) Reactive
iii) Hybrid

Proactive routing protocols can compute route in advance. They are also known as table driven routing protocols. Routes are developed already so no delay in selection of routes. In this type, all nodes broadcast their routing information periodically to its neighbors [9].So each node has to maintain routing table which consist of all network information regarding routing. The big disadvantage of proactive routing protocol is it increases overhead when size of network increases. Types of proactive protocols are: DSDV (Destination sequence distance vector) and OLSR (Optimal link state routing).

Reactive routing protocols can compute route when demanded. They are also known as on demand routing protocols. There is no need of routing information distribution. When routing is demanded, route discovery occurs for routing. Reactive protocols consume less bandwidth compare to proactive protocols [18]. They can manage network by route maintenance. The big disadvantage of reactive routing protocol is it require more time in route discovery phase and also loss the packet. Types of reactive protocols are: AODV (Adhoc on demand distance vector) and DSR (Dynamic source Routing).

Hybrid routing protocols are combination of proactive and reactive routing protocol. It can merge the benefits of proactive and reactive protocols. They are consists of layered architecture. Types of hybrid protocols are: ZRP (Zone routing protocol) and TORA (Temporarily ordered routing algorithm).

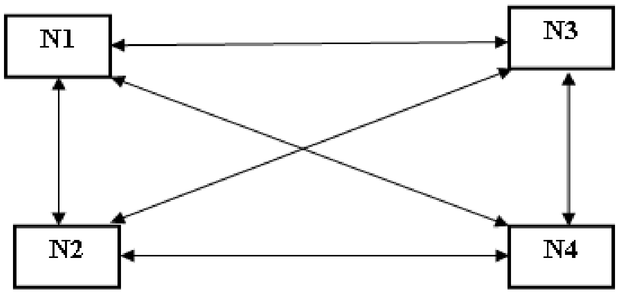


Fig -1: Mobile Adhoc Network

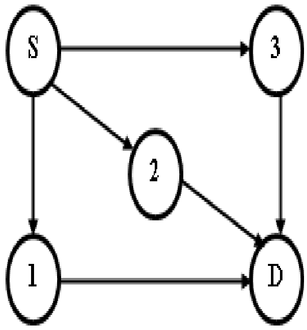
2. AODV PROTOCOL

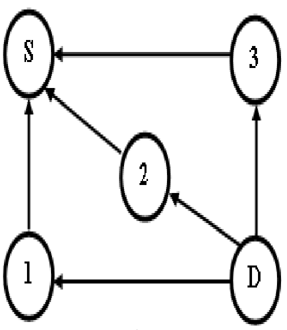
AODV (Adhoc on demand routing protocol) is reactive routing protocol, routes are establishes when it is demanded. AODV uses three control messages. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).These three control messages are used in two steps of AODV protocol, Route Discovery and Route Maintenance.

2.1 Route Discovery

In this step, using RREQ message route is discovered from source to destination. Source node broadcasts RREQ message in the network. Intermediate nodes forward this RREQ message if they knows destination. Once RREQ is sent to destination, destination and intermediate node set reverse path to the source. By using this reverse path, data packets will be send. AODV uses destination sequence number for route discovery. Destination will send RREP (Route Reply) message when RREQ completes. Source node receives multiple RREP messages, source node selects short and fresh path to send data.

AODV is on demand routing protocol then also manage routing table. Unlike proactive protocols, AODV protocol does not carry full path of source to destination in header. AODV protocol maintain routing table fields like destination sequence number, next node, number of nodes, expiration time [24].





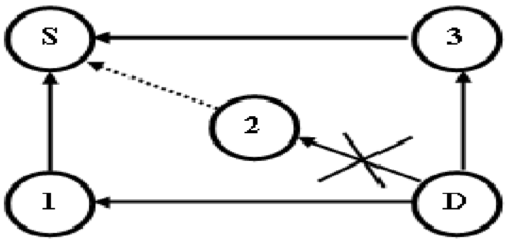
→ Represents RREQ ← Represents
RREP

Fig -2: Route Discovery **Fig -3**: Reverse Path Setup

When any path is selected from source to destination it means that destination has highest sequence number. AODV maintains routing table entries up to sometime duration. If route is not active then it is discarded from routing table [2].

2.2 Route Maintenance

In this step, route between source to destination is repaired locally. In route discovery step, RREQ is sent but RREP is not receiving then intermediate nodes broadcasts route error (RERR) message to inform other nodes that link is broken [4]. After sending RERR message again route discovery is initiated from source node.



←······Represents RERR

Fig -4: Route Maintenance

3. TYPES OF ATTACK

MANETs are vulnerable to many security attacks. There are two basic types attack: passive and active. Passive attack captures information from network without disturbing network [18]. Passive attack is very hard to detect. Traffic analysis and monitoring are example of passive attacks.

Active attack can disturb the whole network by modifying the network information by false message. Active attacks can be either internal or external. Internal attack means attacker is within the network and external attack means attacker is outside of network. Modification and fabrication are examples of active attack.

4. BLACK HOLE ATTACK

Black hole attack is an active attack, which is performed on network layer. This layer has malicious node which advertise itself as shortest route up to destination. Source node selects this route and malicious node will drop data packets.

There are basic two types of black hole attack. Single and collaborative. In single black hole attack, one malicious node consumes network traffic and then drops packets. In collaborative attack, more than one malicious nodes are there. Minimum two malicious nodes are work together [7]. One malicious node attracts traffic towards it and sends data packets to another malicious node. Second malicious node will drop data packets. Collaborative black hole attack is very hard to detect.

The primary role of black hole attacker is, send highest sequence number to the source node. Source node assume this route as fresh route and stop route discovery process, by sending data packets in black hole node’s route [11].

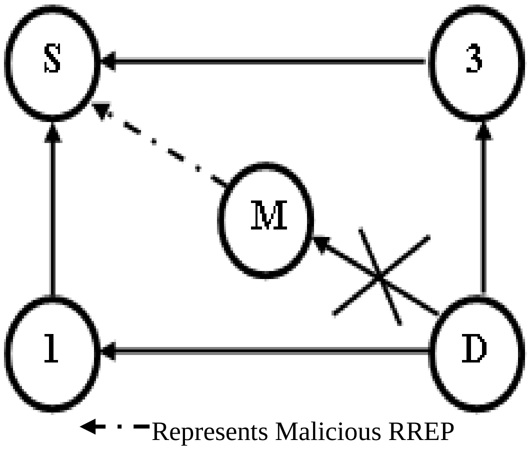


Fig -5: Single Black hole Attack

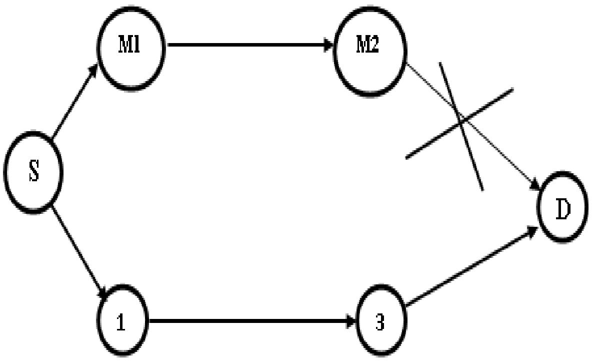


Fig -6: Collaborative Black hole Attack

Black hole attack can be performed either of three cases:

1. Black hole node drops RREQ initiated by source node.
2. Black hole node forwards RREQ but drops RREP received by intermediate or destination node.
3. Black hole node forwards RREQ and RREP but drops data packets.

In all above cases, black hole mitigation is challenging task. In first case, source node starts route discovery by sending RREQ message to all its neighbors. Malicious node drops this RREQ message and does not forward it to its neighbors. It immediately send RREP message with highest sequence number. In second case, black hole node forward RREQ message to its neighbors and get RREP also. After collecting RREP message, black hole node drops RREP message and send fake RREP message having highest sequence number. In third case, black hole node forwards RREQ and RREP message but when black hole node's path is selected for data transmission it will drop data packets.
Figure 5 represents single black hole attack. Source node S sends RREQ message to its neighbors. M represents the malicious node. M sends RREP message to source node having fresh and quick route. Source node sends data packets through M. M will drop data packets. Figure 6 represents collaborative black hole attack. M1 and M2 are malicious nodes. M1 node absorbs RREQ forwarded by source node and transfer data packet to node M2. M2 node will drop data packets. If TCP connection is used then source node will come to know that data packets are dropped because no acknowledgement is received. In UDP connection source node will never come to know about data loss [21]. Table I summarizes black hole detection methods from different researchers.

Table -1: Comparative analysis of black hole detection methods [1]

Research Paper	**Approach**	**Performance Matrices**	**Advantages**	**Disadvantages**
Malicious AODV-Implementations and analysis of routing attacks in MANET [31]	Malicious AODV	Packet efficiency, Throughput, Routing Overhead	Network is partitioned into two parts so attacker cannot degrade performance.	No proper IDS for free environment.
Black hole effect mitigation method in AODV routing protocol [15]	Enhance AODV	PDR using AODV,ERDA and EAODV	Extra route reply message is used from destination and gives better performance.	Throughput and delay's results are not specified.
Securing Routing table update in AODV routing protocol [27]	ERDA	PDR, NRL ratio and delay	Improves process of updating routing entry.	Does not work with outlier detection algorithm.
Secure routing protocol to prevent cooperative black hole attack in MANET.[9]	CBD-AODV	PDR and end to end delay	Up to 2.6 times more performance in PDR compare to AODV.	Always wait for second path.
Secure AODV protocol to mitigate black hole attack in MANET[11]	OAODV (weight updation and feedback method)	PDR with number of node varies and speed of nodes	Improves PDR	False positive

Prevention of selective black hole on MANET[20]	Anti black hole mechanism	Total packet loss	False positive rate is 0%.	For better performance more IDS required.
Improving AODV protocol against black hole attacks [39]	Nital Mistry et. Al's method	PDR and end to end delay	PDR is improved and RREP having high sequence no. is discarded.	More routing overhead.
Prevention of black hole attack in MANET[13]	SAODV	PDR, delay and overhead	No repeated nodes then random path selected and Less overhead.	Increases average end to end delay
A dynamic learning system against black hole attack in AODV [12]	DPRAODV	PDR	Very high PDR	More routing overhead and average end to end delay
Preventing cooperative black hole attack in MANET:Simulation, Implementation and evaluation [26]	DRI and cross check using FREQ and FREP	Throughput	Very high throughput	More routing overhead

5. PROPOSED WORK

In our proposed approach EBAODV (Enhance black hole AODV), leader nodes are used for detection of black hole attack. Leader nodes are created first. After generating route request, set expired time is 20ms. If RREP is arrived until this time interval then send fake packet. If RREP is not received then resend route request. After sending fake packet, if acknowledgement is received then and only then original data packet will be send otherwise set some threshold value(here 10) for comparison. If packet loss is greater than 10 (threshold) then leader nodes will send block message to all its neighbors, which contains id of malicious node.

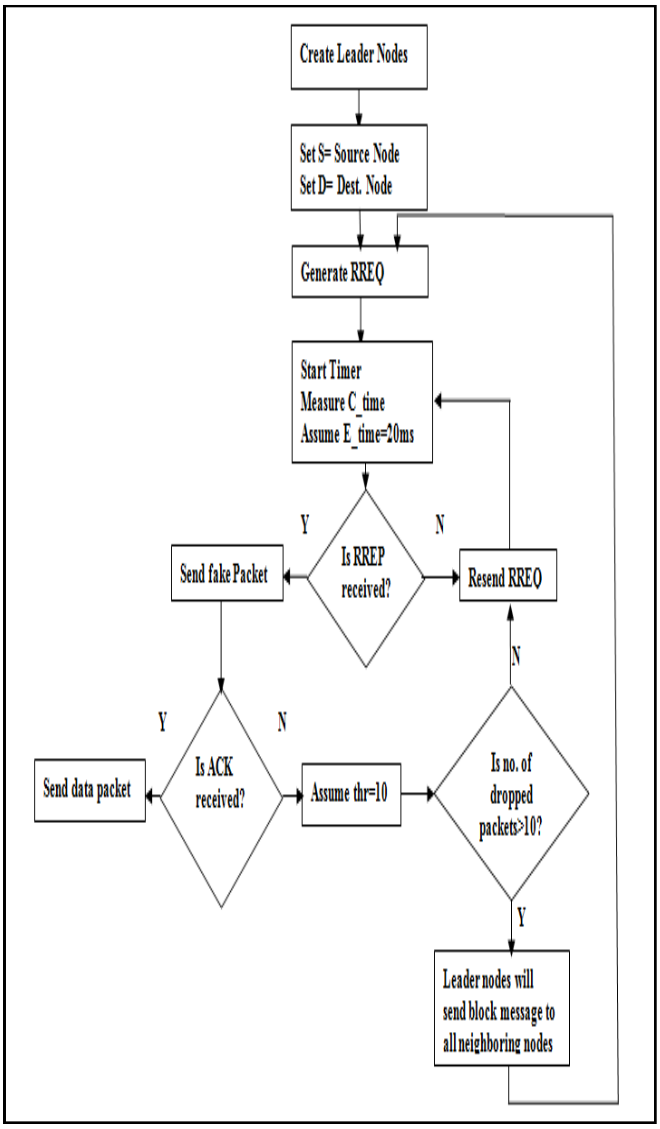


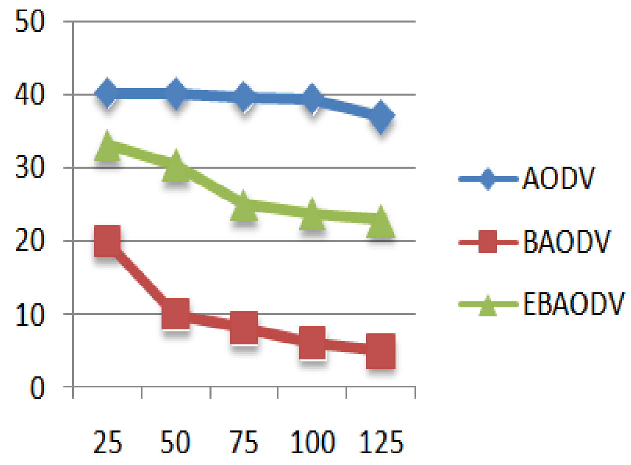
Fig -7: Flowchart of EBAODV [1]

6. IMPLEMENTATIONS AND RESULTS

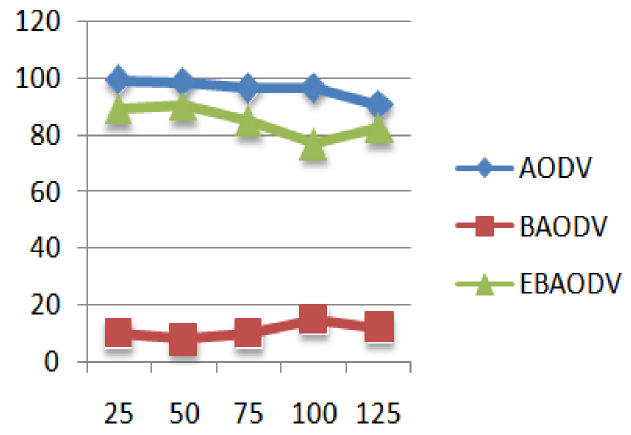
Table -2: Simulation Parameters

Parameter	**Value**
Simulator	Ns-2(ver.2.35)
Simulation Time	500 s
Number of nodes	25 to 125
Routing Protocol	AODV
Traffic Model	TCP
Pause time	10 s
Mobility	10 - 50 m/s
Terrain area	800m x 800m
Transmission Range	250m
No. of malicious node	1

1. Throughput vs No. of Node Varies



2. Packet Delivery Ratio vs no. of Nodes Varies



7. CONCLUSION

Security is big issue in MANET. Attacks can destroy whole network. Black hole attack is one of them. Due to network's dynamic topology it is very difficult to find position of malicious node. In case of collaborative black hole attack, it is very difficult to find more than one malicious nodes in network. In this paper, our proposed solution EBAODV is presented. In this approach, leader nodes are used for detection and prevention technique. Results of all protocol are implemented in NS 2 and measured throughput and packet delivery ratio.

REFERENCES

[1] Ankita V Rachh, Yatin Y. Shukla, Tejas R. Rohit, "A Novel Approach for Detection of Blackhole Attacks ", IOSR-JCE, vol.16,issue. 2, pp. 69-74, March 2014.

[2] Sunil J. Soni , Suketu D. Nayak, "Enhancing Security Features & Performance of AODV Protocol under Attack for MANET", IEEE International Conference on Intelligent Systems and Signal Processing (ISSP), pp-325-328, 2013

[3] Sisily Sibichen, Sreela Sreedhar, "An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks ", IEEE-ICMICR-2013

[4] Ali M. Sagheer, IEEE Member, and Hadeel M. Taher, "Identity Based Cryptography for Secure AODV Routing Protocol", IEEE- TELFOR, pp-198-201, 2012

[5] Rajesh Yerneni, Anil K. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks", IEEE-ICCCNT-2012

[6] Christian Gottron, Pedro Larbig, Andr´e K¨onig, Matthias Hollick and Ralf Steinmetz, "The Rise and Fall of the AODV Protocol:A TestBed Study on Practical Routing Attacks", IEEE-LCN-2010

[7] F. Maan, Y. Abbas, N. Mazharg, "Vulnerability Assessment of AODV and SAODV Routing Protocols Against Network Routing Attacks and Performance Comparisons ", IEEE, pp-36-41, 2011

[8] Zaid Ahmad, Kamarularifin Abd. Jalil, Jamalul-lail Ab Manan, "Black hole Effect Mitigation Method in AODV Routing Protocol", IEEE, pp-151-155, 2011

[9] Fidel Thachil, K C Shet, "A trust based approach for AODV protocol to mitigate black hole attack in MANET", IEEE-CPS, pp-281-285, 2012

[10] Nai-Wei Lo and Fang-Ling Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET", Springer, pp-59-65, 2013

[11] Junguo Liao and Junwen Li, "ISPM: An Improved Secure Payment Mechanism to Prevent the Black Hole Attack and Selfish Node inWMN", Springer, pp-169-178, 2013

[12] Jayashree Padmanabhan, Tamil Selvan Raman Subramaniam, Kumaresh Prakasam and Vigneswaran Ponpandiyan, "A Secure Routing Protocol to Combat Byzantine and Black Hole Attacks for MANETs", Springer, pp-541-548, 2011

[13] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Springer, pp-1-16, 2011

[14] Davide Cerri and Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE, pp-120-125, 2008

[15] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, IEEE, "A Dynamic Anomaly Detection

Scheme for AODV-Based Mobile Ad Hoc Networks”, IEEE, pp-2471-2481,May 2009

[16] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan “Mitigation of Black Hole Attacks for AODV Routing Protocol ”, IEEE, pp-336-343, 2011

[17] Chanchal Aghi1, Chander Diwaker ,“ Black hole attack in AODV routing protocol: A Review”, IJARCSSE.pp-820-823,April 2013

[18] Alok Rao, Narendra Upadhyay, Vivek Kumar Rai, “ A Survey on AODV Protocol Performance with Black Hole Node in MANET” ,IJEAT, pp-574-577, April 2013

[19] Anu Bala, Munish Bansal, Jagpreet Singh, “Performance Analysis of MANET under Blackhole Attack” ,IEEE, pp-141-145, 2009

[20] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, “A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks ” ,IEEE, pp-556-560, 2012

[21] Ming-Yang Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems”,Elsevier, pp-107-117, 2010

[22] N. Bhalaji, Alok V. Kanakeri, Krishna P. Chaitanya and A. Shanmugam, “Trust Based Strategy to Resist Collaborative Blackhole Attack in Manet” , Springer, pp-468-474,2010

[23] Nai-Wei Lo and Fang-Ling Liu, “A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET”, Springer.pp-59-64, 2013

[24] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, “DoS Attacks in Mobile Ad-hoc Networks: A Survey” ,IEEE, pp-535-541,2012