AOMDV Routing based Enhanced Security for Black Hole Attack in MANETs

D.Geetha*
*Assistant Professor of computer science,
SreeSaraswathiThayagaraja College of arts and Science
Pollachi-642 107, Tamil Nadu, India

B. Revathi**
**Research scholar of computer science,
SreeSaraswathiThayagaraja College of arts and Science
Pollachi-642 107, Tamil Nadu, India

ABSTRACT
A Mobile Ad-hoc Network (MANET) is a dynamic wireless network that can be formulated without the need for any pre-existing infrastructure in which each node can act as a router. One of the main challenges of MANET is the design of robust routing protocol that adapt to the frequent and randomly changing network topology. Several attacks are possible in the available routing protocols such as Wormhole attack, black hole attack, byzantine attack, etc. Among these attacks black hole attack is of major concern in AODV, is one of the popular routing protocols for MANET. In this study, analyzed the use of AOMDV (Ad-hoc On-demand Multipath Distance Vector) and improved the security of MANET against the black hole attack. The main objective is to provide security against the Black hole attack. Finally compared and evaluated the performance of On-demand routing protocols Ad-hoc On-demand Distance Vector (AODV) routing protocol, which is unipath and Ad-hoc On-demand Multipath Distance Vector (AOMDV) routing protocol. When compared to the existing AODV protocol, AOMDV has better packet delivery ratio and comparatively low average end-to-end delay. The number of packets dropped in the AOMDV against the black hole attack is very low. Thus the proposed technique which uses AOMDV is proved to be better against black hole attacks.

Keyword

Black hole, gray hole, warm hole attack, MANET, active attack, passive attack.

1. INTRODUCTION
In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. Black hole attack can be easily executed in the MANETs and it leads to various effects like packet delivery/receiving delay, packet loss, etc. To handle this problem, various routing protocols are developed. One among that protocol is Ad-hoc On-Demand Distance Vector which is proved to be effective. Sometimes, packet delay and packet loss can not be solved effectively using AODV protocol. This motivated to develop a better routing protocol which overcomes blackhole attack.

Black hole problem in MANETS is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [1]. The main objective of this research work is to develop an efficient routing technique which can overcome the black hole attack in the MANETs [3, 4]. The main focus is on improving the Ad-hoc On-Demand Distance Vector (AODV) protocol to result in eliminating the black hole attack which will result in lesser packet loss and reduces the data delivery time [10].

2. SECURITY MEASURES IN manet
Security in Mobile Ad Hoc Network is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

2.1Attacks on Mobile Ad hoc Network

Attacks on mobile ad hoc networks can be classified into following two categories:

2.1.1 Passive Attacks
A passive attack does not disrupt proper operation of the network. The attacker snoop the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard.

2.1.2 Active Attacks
An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and

firewalls [6]. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks [16].

2.1.3 Network Layer Attack

The list of different types of attacks on network layer and their brief descriptions are given below:

a) Wormhole Attack

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

For example in Figure 1.1, X and Y are two malicious nodes that encapsulate data packets and falsified the route lengths.

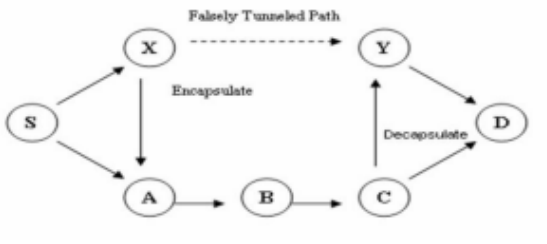

Fig 1.1: Wormhole attack

Suppose node S wishes to form a route to D and initiates route discovery. When X receives a route request from S, X encapsulates the route request and tunnels it to Y through an existing data route, in this case {X --> A --> B --> C --> Y}. When Y receives the encapsulated route request for D then it will show that it had only traveled {S --> X --> Y --> D}. Neither X nor Y update the packet header. After route discovery, the destination finds two routes from S of unequal length: one is of 4 and another is of 3. If Y tunnels the route reply back to X, S would falsely consider the path to D via X is better than the path to D via A. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network.

b) Black hole attack

In this attack, an attacker uses the routing protocol [15] to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them [15]. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

For example, in Figure 1.2, source node S wants to send data packets to destination node D and initiates the route discovery process. It is assumed that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately sends the response to node S. If the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 2. As a result, all packets through the malicious node is consumed or lost.

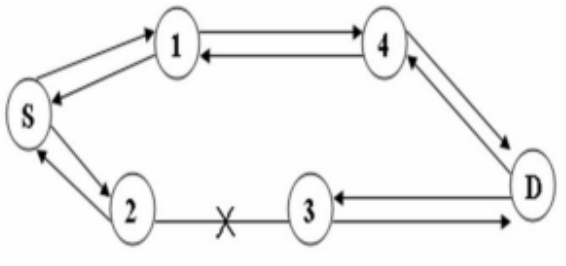

Fig 1.2: Black hole attack

3. EXPERIMENTAL RESULTS

Implementation of wireless ad-hoc networks in the real world is quite hard. Hence, the preferred alternative is to use some simulation software which can mimic real-life scenarios. Though it is difficult to reproduce all the real life factors such as humidity, wind and human behavior in the scenarios generated, most of the characteristics can be programmed into the scenario.

To compare two on-demand ad-hoc routing protocol against the black hole attack, it is best to use identical simulation environments for their performance evaluation.

a) Simulation Environment

NS-2 simulator is used which has support for simulating a multi-hop wireless ad-hoc environment completed with physical, data link, and medium access control (MAC) layer models on NS-2.The protocols maintain a send buffer of 500 packets. It contains all data packets waiting for a route, such as packets for which route discovery has started, but no reply has arrived yet. All packets sent by the routing layer are queued at the interface queue till the MAC layer transmits them. The maximum size for interface priority queue is 50 packets and it maintains it with two priorities, each served in FIFO order. Routing packets get higher priority than data packets.

b) Performance Evaluation Metrics

The performance of AODV and AOMDV against the black hole attack is compared according to the following performance metrics [19]:

Packet delivery ratio: The ratio of data packets delivered to the destinations to those generated by the constant bit rate.

Average End-to-End delay of data packets: This includes all possible delays caused by buffering during route discovery, queuing at the interface queue, retransmission delays, propagation and transfer times.

Number of packets dropped: The total number of routing packets dropped during the simulation.

c) Packet Delivery Ratio (PDR)

The simulation is done for 500sec for seven scenarios with pause times varying from 0 to 500 s. Packet delivery ratio is calculated for AODV and AOMDV. The results are summarized below with their corresponding graph.

Table 4.1: Comparison of Packet Delivery Ratio (%)

PauseTime (sec)	Packet Delivery Ratio (%)	
	AODV	AOMDV
0	60	72
100	65	69
200	58	67
300	50	68
400	62	66
500	56	67

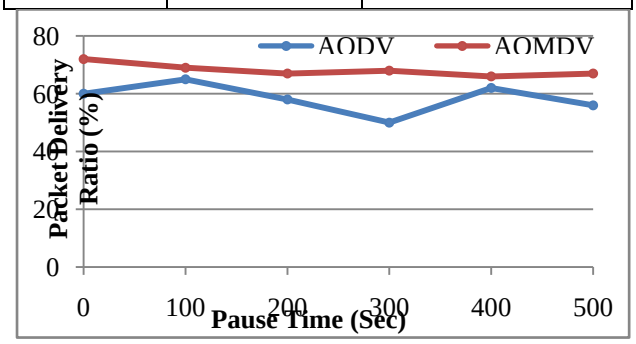

Fig 4.1: Comparison of AODV and AOMDV on basis of PDR

From the figure 4.1 and table 4.1, it is confirmed that AOMDV has a better PDR value when compared to AODV for each set of connections. This is because, AOMDV can find an alternate route if the current link attacked by a black hole whereas AODV is rendered useless at that point.

d) Average End-to-End delay of data packets

From the figure 4.2 and table 4.2, it is confirmed that AOMDV has very low average delay than AODV due to the fact if a link break occurs in the current topology, AOMDV would try to find an alternate path from among the backup routes between the source and the destination node pairs resulting in additional delay to the packet delivery time. In comparison, if a black hole attack occurs in AODV, the packet would not reach the destination another path from source to destination, since only singular paths exist in AODV between a source and destination node.

Table 4.2: Comparison of Average End-to-End Delay

Pause Time (sec)	Average End-to-End Delay (Sec)	
	AODV	AOMDV
0	86	22
100	102	36
200	117	38
300	122	39
400	129	41
500	136	43

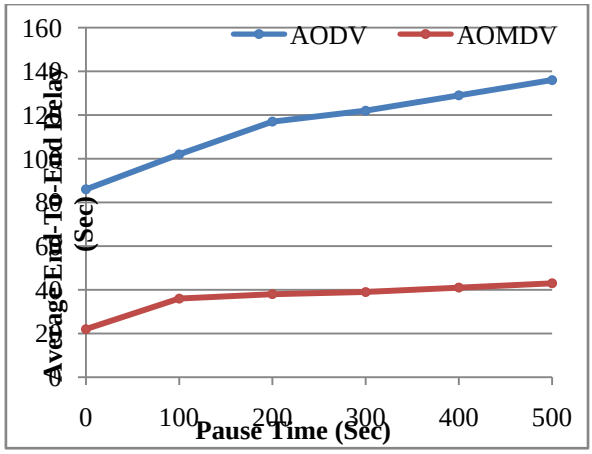

Fig 4.2: Comparison of AODV and AOMDV on basis of average End-to-End delay

e) Number of packets dropped

The number of packets dropped in AODV is more than the number of packets dropped in AOMDV as presented in figure 4.3 and table 4.3. This is because of the fact that due to AODV being a unipath routing protocol and it is more vulnerable to black hole attack and also if a black hole attack occurs on a link, the packet will not be delivered to the destination node. Thus that packet will get dropped. But due to AOMDV being a multipath routing protocol, even if the current link breaks due to black hole attack, the network will find an alternate path from the source to the destination node and have a better chance of packet delivery without any block hole attack; hence less number of packets will be dropped for AOMDV.

Table 4.3: Comparison of Number of Packets Dropped

Pause Time (sec)	Number of Packets Dropped	
	AODV	AOMDV
0	82	26
100	65	s29
200	56	19
300	77	25
400	89	27
500	102	31

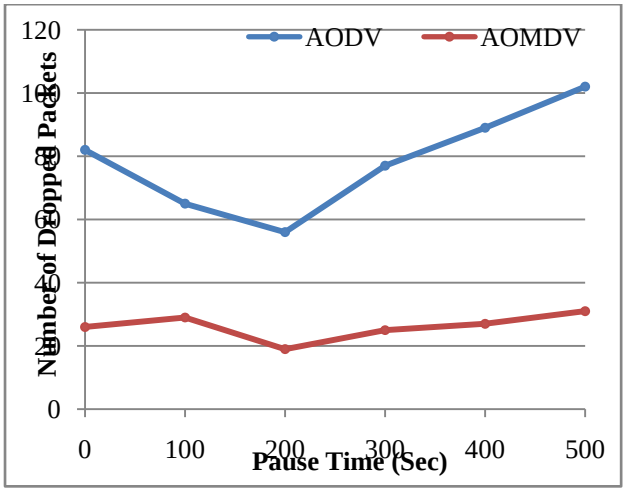

Fig 4.3: Comparison of AODV and AOMDV on basis of number of dropped packets

In this experimental result the performances of AODV and AOMDV against black hole attack using NS-2. The comparison was based on of packet delivery ratio, average end-to-end delay and the number of packets dropped. It is found from the results, that AOMDV is better than AODV. AODV can be easily attacked by black holes due its inability to search for alternate routes when a current link breaks down but AOMDV uses multipath routing which avoids black hole attack.

4. CONCLUSION

This work analyzed the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. This work used a protocol called Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) to avoid the black hole attack in the AODV.

The idea behind multipath routing is to look for a multiple routes to a host with the intention of avoiding black hole attack. There could be a lot of reasons to do this, if the black hole attack occurs in a single path, the AOMDV will send the data packets in some other route which is available in the multipath routing. The main objective of this research is to avoid the black hole attack in the MANET. The existing AODV protocol routes their data packets in a single route i.e., unicast. But the proposed technique which uses AOMDV protocol utilizes multipath routing. Hence, if a black hole attack occurs in a path, the AOMDV will route the data packets in some other route.

The experimental observations evaluated the proposed AOMDV with the existing AODV with the help of evaluation metrics such as packet delivery ratio, average end-to-end delay and the number of packets dropped against the black hole attack. When compared to the existing AODV protocol, AOMDV has better packet delivery ratio and comparatively low average end-to-end delay. The number of packets dropped in the AOMDV against the black hole attack is very low. Thus the proposed technique which uses AOMDV is proved to be better against black hole attacks.

5. SCOPE FOR FUTURE WORK

This study simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In this technique used the AOMDV routing protocol. From the simulated results it is found that the AOMDV protocol is less prone black hole attack than the AODV routing protocol.

- This study considered the AODV and AOMDV protocol, but the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be determined.
- In future, a robust framework that uses minimal public key cryptography to avoid overload on the network and uses shared key cryptography extensively to provide security against the black hole attack.
- The detection of Black holes in ad hoc networks is still considered to be a challenging task. Some techniques should be developed to detect the black hole nodes in MANETs.

6. REFERENCES

[1] S. Ci et al., “Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks,” IEEE Trans. Vehic. Tech., Vol. 55, No. 4, Pp. 1302–1310, 2006.

[2] K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology”, Sweden, 2007.

[3] B. Awerbuch, D. Holmer, C. Nita Rotaru and Herbert Rubens. “An On-Demand Secure Routing Protocol Resilient to Byzantine Failures”, Proceedings of the ACM Workshop on Wireless Security, Pp. 21-30, 2002.

[4] C. E. Perkins and E. M. Royer. "Ad Hoc On-Demand Distance Vector Routing". Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, Pp. 90-100, 1999.

[5] Elizabeth M. Royer “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal Communication, 1999.

[6] B. Wu et al., “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,” Wireless/Mobile Network Security, Springer, Vol. 17, 2006.

[7] Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and Kendall Nygard. “Prevention of Cooperative Black Hole Attack

in Wireless Ad Hoc Networks". Department of Computer Science, IACC 258 North Dakota State Universities, Fargo, ND 58105.

[8] Dhurandher, S.K.; Obaidat, M.S.; Verma, K.; Gupta, P.; Dhurandher, P.; "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", IEEE Systems Journal, Vol. 5, No. 2, Pp. 176 – 188, 2011.

[9] Lacharite, Y.; Dang Quan Nguyen; Maoyu Wang; Lamont, L.; "A trust-based security architecture for tactical MANETS", IEEE Military Communications Conference (MILCOM), Pp. 1 – 7, 2008.

[10] Raza, I.; Hussain, S.A.; "A Trust based Security Framework for Pure AODV Network", International Conference on Information and Emerging Technologies (ICIET), Pp. 1 – 6, 2007.

[11] Bhargava, S.; Agrawal, D.P.; "Security enhancements in AODV protocol for wireless ad hoc networks", IEEE VTS 54th Vehicular Technology Conference (VTC), Vol. 4, Pp. 2143 – 2147, 2001.

[12] Songbai Lu; Longxuan Li; Kwok-Yan Lam; LingyanJia; "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security (CIS '09), Vol. 2, Pp. 421 – 425, 2009.

[13] Mahajan, V.; Natu, M.; Sethi, A.; "Analysis of wormhole intrusion attacks in MANETS", IEEE Military Communications Conference (MILCOM), Pp. 1 – 7, 2008.

[14] Bala, A.; Bansal, M.; Singh, J.; "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks and Communications (NETCOM '09), Pp. 141 – 145, 2009.

[15] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y.; "Proposal of a method to detect black hole attack in MANET", International Symposium on Autonomous Decentralized Systems (ISADS '09), 1 – 6, 2009.

[16] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., Vol. 9, No. 4, Pp. 363–65, 2005.

[17] Y-C Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Sec. and Privacy, 2004.

[18] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 2002 IEEE Int'l. Conf. Network Protocols, 2002.

[19] H.D.Trung, W.Benjapolakul, P.M.Duc, "Performance evaluation and comparison of different ad hoc routing protocols", Department of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand, 2007