RESEARCH ARTICLE OPEN ACCESS

Prevention of Black Hole Attack Using AOMDV

Naseera K. M*, Dr. C. Chandrasekar**
*(Department of Computer Science, SreeNarayanaGuruCollege, Coimbatore-105)
** (Department of Computer Applications, Sree Narayana Guru College, Coimbatore-105)

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. A variety of routing protocols have been proposed and most of them have been extensively simulated or implemented as well. 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.Due to security vulnerabilities of the AODV routing protocol, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack. In this study to analyze the comparison between with and without attacks.
Keywords– MANET, Black Hole Attack, AODV.

I. INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which is called as nodes). In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers [1].

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much exposed to attacks [2]. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [3]. Different kinds of attacks have been analyzed in MANET and their affect on the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. MANETs routing protocols are also being exploited by the attackers in the form of flooding attack, which is done by the attacker either by using RREQ or data flooding.

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure [4]. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure.

Ad hoc networks are characterized by open medium, dynamic topology, distributed cooperation and constrained capability. These characteristics set more challenges for security. Routing security is the most important factor in the security of the entire network. However, few of current routing protocols have the consideration about the security problems. [5]Analyzes the potential insecurity factors in the AODV protocol. A security routing protocol based on the credence model is proposed, which can react quickly when some malicious behaviors in the network are detected and effectively protects the network from kinds of attacks and guarantees the security of ad hoc networks

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [6].

Security is a main concern in the establishment of tactical MANETs. Literature is abundant in defining protocol extensions to provide more secure MANET communications. Also many techniques have been developed to identify different types of network attacks, such as the wormhole attack, for example. However, all these security solutions are designed for specific routing protocols. In the absence of generic security architecture, nodes from different MANET domains cannot cooperate and benefit from security advantages across the entire network, such as secured inter-domain routing, etc. [7] presented a general architecture for a security trust monitoring layer that runs on top of routing protocols.

II. RELEATED WORK

Mobile ad hoc networks (MANETs) are collections of wireless mobile devices with restricted broadcast range and resources, and no fixed infrastructure. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security points of view. Among the novel characteristics of this security model is that it promises security guarantee under concurrent executions, a feature of crucial practical implication for this type of distributed computation. A novel route discovery algorithm called endair. A was also proposed, together with a claimed security proof within the same model. [8]Revealed that the security proof for the route discovery algorithm endair. A is flawed, and moreover, this algorithm is vulnerable to a hidden channel attack. This approach also analyzes the security framework that was used for route discovery and argues that composability is an essential feature for ubiquitous applications.

AODV routing protocol is widely used in mobile ad hoc networks, but it does not have any security mechanism, so it is very vulnerable to security attacks. In [9] analyses the common threats of AODV and then a security improvement is carried out. By setting up black holes and rushing attack models, the performance of improved protocol is simulated using QualNet simulation tools. The results show that this security enhanced solution can not only protect against those attacks but also maintain the efficiency of AODV.

In [10] presents a trust based security framework to identify malicious nodes in ad hoc on-demand distance vector (AODV) protocol. In this framework each node calculates trust level of its neighboring nodes for route selection. Trust calculation process involves opinions of other nodes about the node whose trust level is to be determined. If a neighboring node has a trust level lower than a predefined threshold value, it is identified as malicious and it is not considered for route selection. The proposed security framework does not use any key distribution process and no changes are made in control packets of AODV. Simulation results show that the proposed framework improves performance of AODV by identifying and removing malicious nodes. Performance of the framework has been evaluated for three different types of malicious attacks (impersonation attack, colluding nodes attack and black hole attack).

Black hole attack is a serious threat in a mobile ad hoc network (MANET). In this attack, a malicious node injects a faked route reply message to deceive the source node so that the source node establishes a route to the malicious node and sends all the data packets to the malicious node. Every conventional method to detect such an attack has a defect of rather high rate of misjudgment in the detection. In order to overcome this defect, [11] proposed a new detection method based on checking the sequence number in the route reply message by making use of a new message originated by the destination node and also by monitoring the messages relayed by the intermediate nodes in the route. Computer simulation results demonstrate that this method has a feature of much lower false positive and negative rates in detecting any number of malicious nodes than the conventional methods.

III. METHODOLOGY

A. An Overview of AODV Routing Protocol

Ad Hoc On-Demand Vector Routing (AODV) protocol is a reactive routing protocol for ad hoc and mobile networks that maintain routes only between nodes which need to communicate. The AODV routing protocol builds on the DSDV algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information. That means, the routing messages do not contain information about the whole route path, but only about the source and the destination. Therefore, routing messages do not have an increasing size. It uses destination sequence numbers to specify how fresh a route is (in relation to another), which is used to grant loop freedom.

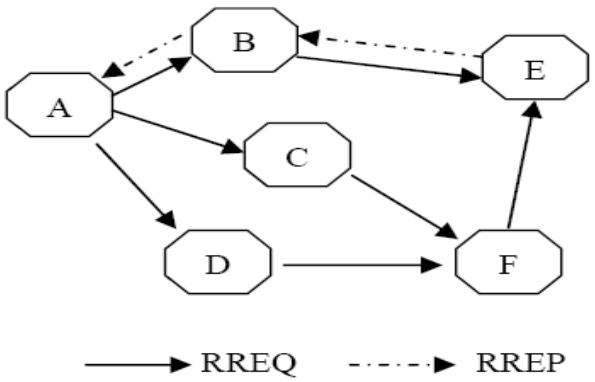

Figure 1: RREQ & RREP message exchange between A & E

Whenever a node needs to send a packet to a destination for which it has no ‘fresh enough’ route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ (unless it has a ‘fresher’ one).When the intended destination (or an intermediate node that has a ‘fresh enough’ route to the destination) receives the RREQ, it replies by

sending a Route Reply (RREP). It is important to note that the only mutable information in a RREQ and in a RREP is the hop count (which is being monotonically increased at each hop). The RREP travels back to the originator of the RREQ (this time as a unicast). At each intermediate node, a route to the destination is set (again, unless the node has a 'fresher' route than the one specified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ had set this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bi-directionally. In the case that a node receives a new route (by a RREQ or by a RREP) and the node already has a route 'as fresh' as the received one, the shortest one will be up dated. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP. The AODV protocol is vulnerable to the well-known black hole attack. This is illustrated in figure 1

B. Black Hole Problem in AODV

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [6]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [12].

The method how malicious node fits in the data routes varies. Fig. 2 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

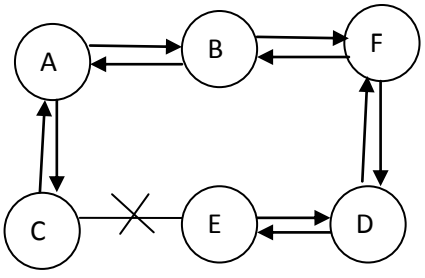

Figure 2: Black hole Attack in AODV

1) Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

i. Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself 20an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

ii. External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points

- Malicious node detects the active route and notes the destination address.
- Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
- Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
- The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
- The new information received in the route reply will allow the source node to update its routing table.
- New route selected by source node for selecting data

.

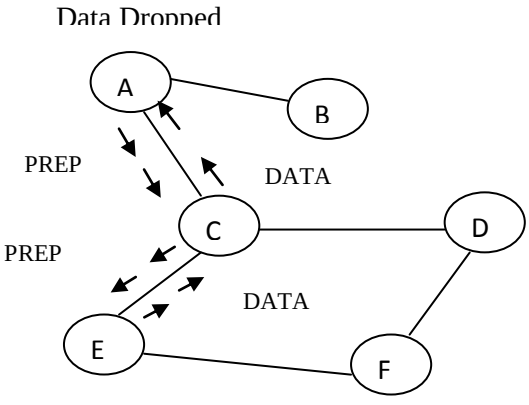

Figure 3 Black hole attack specification

In AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then sends the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack

IV. 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 with attack and AODV against the black hole attack is compared according to the following performance metrics [13]:

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.

1) Packet Delivery Ratio (PDR)

Packet delivery ratio is calculated for AODV with attack and AODV without attack. The results are summarized below with their corresponding graph.

TABLE I: COMPARISON OF PACKET DELIVERY RATIO (%)

Pause Time (sec)	Packet Delivery Ratio (%)	
	AODV with attack	AODV without attack
0	60	65
100	65	69
200	58	62
300	50	55
400	62	66
500	56	67

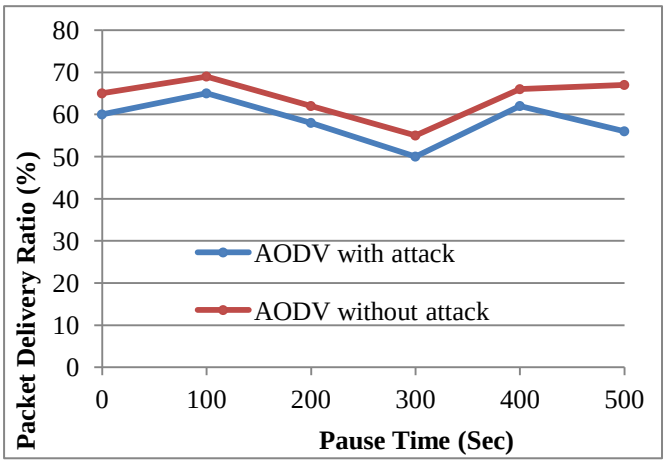

Figure 5: Comparison of AODV with attack and AODV without attack on basis of PDR

From the figure 5 and table 1, it is confirmed that AODV without attack has a better PDR value when compared to AODV for each set of connections. This is because, AODV with attack means it is attacked by a black hole whereas AODV is rendered useless at that point.

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

From figure 6 and table 2, it is confirmed that AODV without attack has very low average delay than AODV with attack. 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 II: COMPARISON OF AVERAGE END-TO-END DELAY

Pause Time (sec)	Number of Packets Dropped	
	AODV with attack	AODV without attack
0	82	35
100	65	30
200	56	22
300	77	30
400	89	32
500	102	43

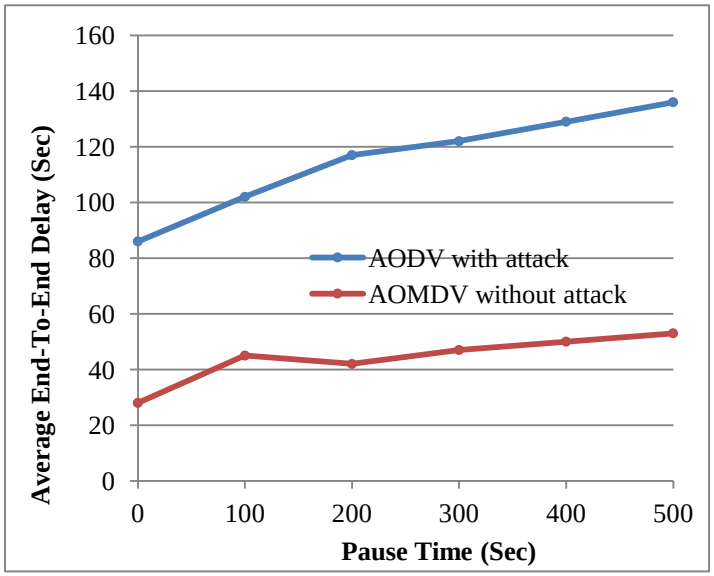

Figure 6 : Comparison of AODV with attack and AODV without attack on basis of average End-to-End delay

3) Number of Packets Dropped

The number of packets dropped in AODV with attack is more than the number of packets dropped in AODV without attack as presented in figure 7 and table 3.

TABLE III: COMPARISON OF NUMBER OF PACKETS DROPPED

Pause Time (sec)	Average End-to-End Delay (Sec)	
	AODV with attack	AODV without attack
0	86	28
100	102	45
200	117	42
300	122	47
400	129	50
500	136	53

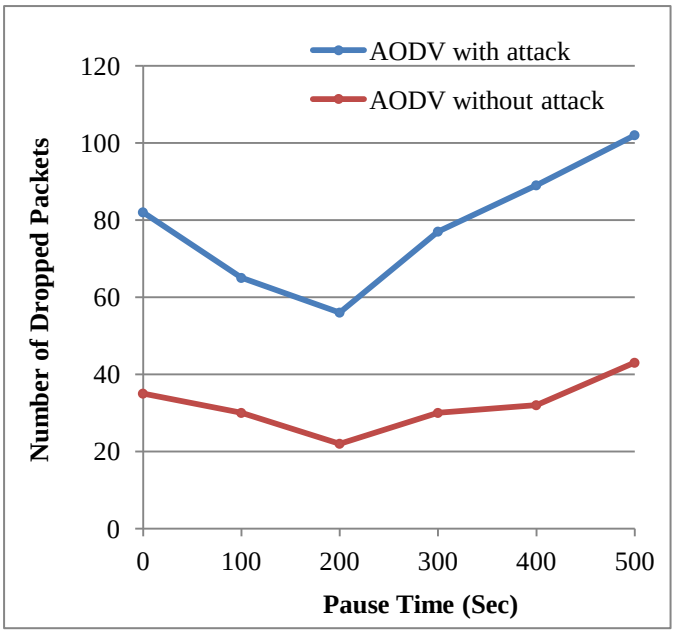

Figure 4.3: Comparison of AODV with attack and AODV without attack on basis of number of dropped packets

V. 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 paper presents a presents an analysis of AODV routing with and without black hole attack in different scenario in ad hoc network. By the Experimental results it can be observed that the AODV without black hole attack can provide better results than AODV with attacks.

The experimental observations evaluated that theAODV with attack and AODV without attack with the help of evaluation metrics such as packet delivery ratio, average end-to-end delay and the number of packets dropped. When compared to the existing AODV with protocol, AODV without protocol has better packet delivery ratio and comparatively low average end-to-end delay. The number of packets dropped in the AODV without protocol against the black hole attack is very low.

REFERENCES

[1] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks", published in IEEE network, special issue on network security, November/December, 1999

[2] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 2002.

[3] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[4] S. Ci, M. Guizani, H. H. Chen, and H. Sharif, "Self-regulating network utilization in mobile

ad-hoc wireless networks," IEEE Transaction on Vehicular Technology, vol. 55, no. 4, pp. 1302--1310, 2006.

[5] Liu Jun, Li Zhe, Lin Dan; Liu Ye, "A security enhanced AODV routing protocol based on the credence mechanism", Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing, Vol. 2, Pp. 719 – 722, 2005.

[6] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[7] 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.

[8] Burmester M, de Medeiros B. "On the Security of Route Discovery in MANETs", IEEE Transactions on Mobile Computing, Vol. 8, No. 9, Pp. 1180 – 1188, 2009.

[9] Zhang Guoqing, Mu Dejun, XuZhong, Yang Weili, "An Efficient Security Enhancement of AODV Protocol", Chinese Control Conference (CCC), Pp. 644 – 647,2007.

[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] 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.

[12] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.

[13] 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