Modified AODV Routing Protocol for enhanced fault tolerance to Blackhole attack in IEEE 802.11 based Adhoc network

Sarabjeet Kaur
M.Tech(CSE)
BBSBEC Fatehgarh Sahib

Er.Birinder Singh
Assistant Professor
BBSBEC Fatehgarh Sahib

Abstract

An adhoc network is a collection of communication devices called nodes that communicate with each other without any infrastructure (such as routers in wired network or access points in infrastructure wireless network) and have no pre-defined link organization. Ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks. In adhoc networks all the devices have equal status that means each node can act as host as well as router. Three types of routing protocols are used to find path from source to destination. These are reactive routing protocols, proactive routing protocol and hybrid protocols. Security in adhoc network is the most crucial and challenging task. Due to the lack of security these protocols are prone to various types of attacks. In this paper we analyze the performance of AODV routing protocol.We consider three scenario:- performance analysis of AODV routing, performance analysis of AODV routing with blackhole attack, performance analysis of modified AODV routing. This has been done by establishing WMN testbed using Qualnet simulator 4.5

1. Introduction

In wireless adhoc networks[1] nodes communicate with each other without centralized administration. This feature makes adhoc network more vulnerable to attacks such as Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack. Security[2] in adhoc network is the most challenging task for the functionality of the network. The other features that make adhoc network to suffer from attacks are lack of centralized and management point, dynamic topology, open medium, cooperative algorithms etc..The attacks in adhoc networks are categorized into internal attack, external, attack, Passive attack, Active attack, and network layer attack. These attacks decreases throughput and increases packet loss, as a result the network performance degrades. In our work we use AODV routing protocol which is one of the reactive routing protocol[3] that suffers from blackhole attack and analyze its performance in different scenarios. In this work we modify AODV routing protocol to enhance fault tolerance to blackhole attack in IEEE 802.11 based adhoc network. In AODV routing protocol there is one feature that intermediate nodes and destination node can send reply messages to source node. As black hole attack is caused by fake reply messages by intermediate (malicious) nodes. We try to make AODV protocol more secure by modifying this feature of AODV protocol (disabling the functionality of intermediate nodes). Then we compare the results of AODV protocol without blackhole attack, AODV protocol with blackhole attack and AODV protocol with blackhole attack but by modifying its feature.

2. Classification of attacks [2]

The attacks are categorized on the basis of source of the attack(ie internal/external attacks)and on the basis of behavior of the attack(ie active/passive attacks).

1. Internal attack

2. External attack

3. Active attack

4. Passive attack

1. Internal attack

In an internal attack attacker participate in the normal activities of the network and wants to gain normal access to the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks than external attacks.

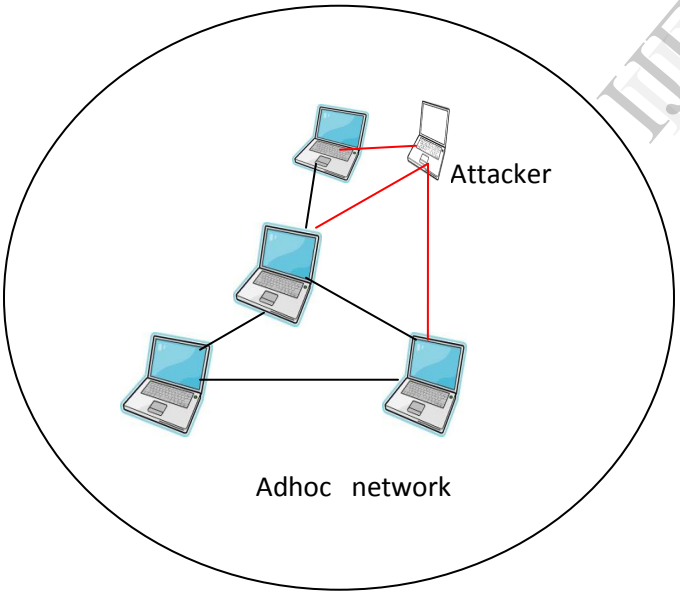


Figure 1: Internal attack in Adhoc network

2. External attack

External attacks are caused by attackers that are outside the network and want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated.

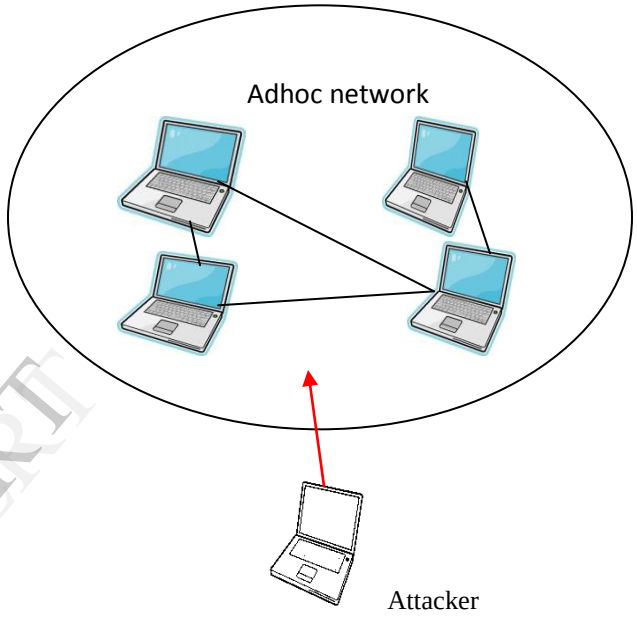


Figure 2: External attack in Adhoc network

3. Active attack

In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network [4]. Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network [4].

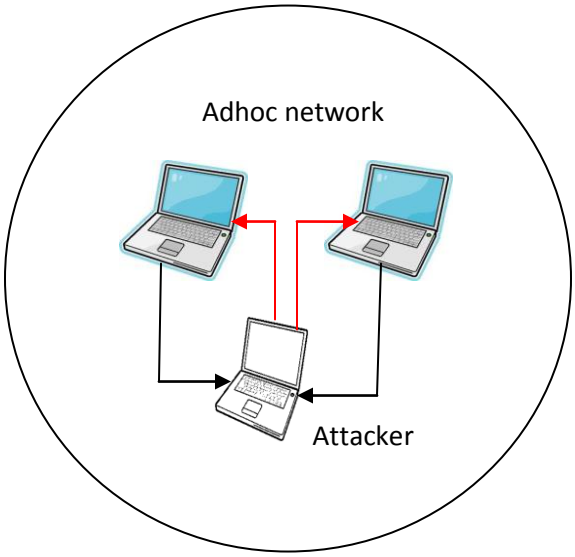


Figure 3: Active attack in adhoc network

4. Passive attack

In passive attacks the content and data stream is observed and then utilized in future for the malicious purpose. The attackers listen to network in order to get information, what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

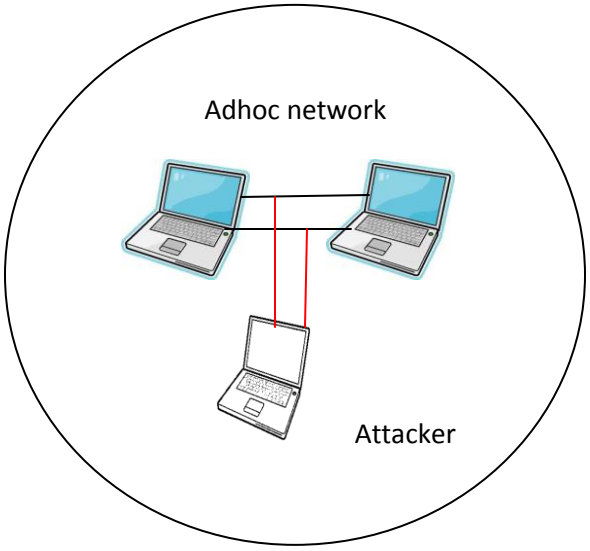


Figure 4: Passive attack in adhoc network

3. Problem formulation: Blackhole attack

Black hole attack is one of the network layer attacks. A black hole attack[5] is a type of denial of service attack in which malicious node intercept all data packets being sent to the destination node. In this attack the malicious node listen to a route request packet in the network, and advertise the source node with claim of having most reliable link and an extremely short route to the destination node, even if it does not have any such route. As a result, the malicious node easily misroute network traffic to it and then drop the packets. As a result packet loss increases and throughput decreases. AODV suffers black hole attack[6].

4. Solution

In this work we modify the feature of AODV routing protocol so that the packet loss can be decreased and throughput can be increased to some extent.

5. Experimental setup

Simulation work is performed using Qualnet simulator 4.5 and AODV routing protocol with varying number of nodes. Network traffic load is provided by constant bit rate (CBR) application.

Parameters	Values
Start time	1 second
End time	20 seconds
Items to send	20,000
Size in bytes	256 bytes
Interval	1 milliseconds

Following parameters were considered:

1.First packet received at(s)
2.Last packet received at(s)
3.Total bytes received
4.Total packet received
5.Throughput:
6.Avg. End to end delay(s)
7.Avg. Jitter(s)

1.First packet received at(s)

It is defined as time taken by first packet to reach destination.

2.Last packet received at(s)

It is defined as time taken by last packet to reach destination.

3.Total bytes received

It is defined as total number of bytes received by the destination.

4.Total packet received

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source).

5.Throughput

Throughput[7] is the measure of no. of packets successfully transmitted to their final destination per unit time.It is measured as bits per second

6.Avg. End to end delay(s)

Average End to End Delay **[8]** signifies the average time taken by packets to reach one end to another end (Source to Destination)**.**

7.Avg. Jitter(s)

Signifies the Packets from the source will reach the destination with different delays [9].

6. Simulation result and analysis

Three cases were considered:

1. Performance analysis of AODV routing: In this case **DESTINATION NODE ONLY** parameter is set to **NO** This is prone to black hole attack.

Table 1

No. of nodes	20	40	60	80	100
First packet received at(s)	1.9342	1.9341	1.9341	1.9340	1.9340
Last packet received at (s)	20.5991	20.5991	20.5990	20.5990	20.5989
Total bytes received	49.80736	44.50816	39.44704	37.00736	31.45728
Total packet received	19456	17386	15409	14456	12288
Throughput	24.9036	22.2540	19.7235	18.5036	15.7286
Avg. end to end delay	0.1300	0.1550	0.1600	0.1800	0.1830
Avg. Jitter	0.3540	0.5326	0.7930	0.9802	1.2150

2.Performance analysis of AODV routing with malicious nodes sending fake RREPs: - In this case **DESTINATION NODE ONLY** parameter is set to **NO** This is attacked with black hole attack as intermediate as well as destination node can send RREP message.

Table 2

No. of nodes	20	40	60	80	100
First packet received at(s)	1.9341	1.9340	1.9340	1.9339	1.9339
Last packet received at (s)	24.0289	24.0285	24.0285	25.0284	25.0285
Total bytes received	6.4	5.12	4.608	2.56	1.28
Total packet received	2500	2000	1800	1000	500

Throughput	3.2	2.56	2.304	1.28	0.0025
Avg. end to end delay	1.0514	1.1090	1.2360	1.3084	1.4140
Avg. Jitter	1.0200	1.4260	1.8100	4.3640	4.3819

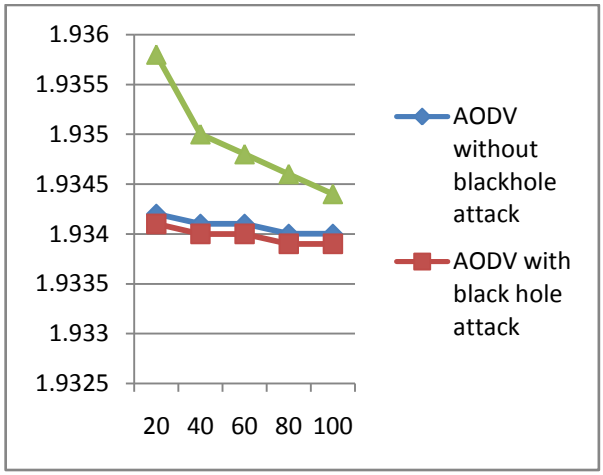
3. Performance analysis of modified AODV routing: - In this case **DESTINATION NODE ONLY** parameter is set to **YES**

Table 3

No. of nodes	**20**	**40**	**60**	**80**	**100**
First packet received at(s)	1.9460	1.9350	1.9348	1.9346	1.9344
Last packet received at (s)	21.5898	21.5897	21.5897	21.5896	21.5896
Total bytes received	30.72	20.48	12.80	7.68	3.84
Total packet received	12000	8000	5000	3000	1500
Throughput	15.36	10.24	6.4	3.84	1.92
Avg. end to end delay	0.0310	0.1000	0.1110	0.1150	0.1370
Avg. Jitter	0.3430	0.5180	0.7250	0.9236	1.1500

Graphs

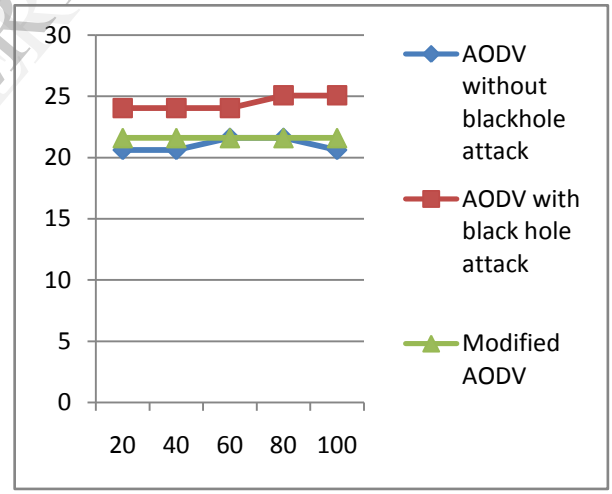
1) First packet received at(s)



Time(s)

No. of nodes

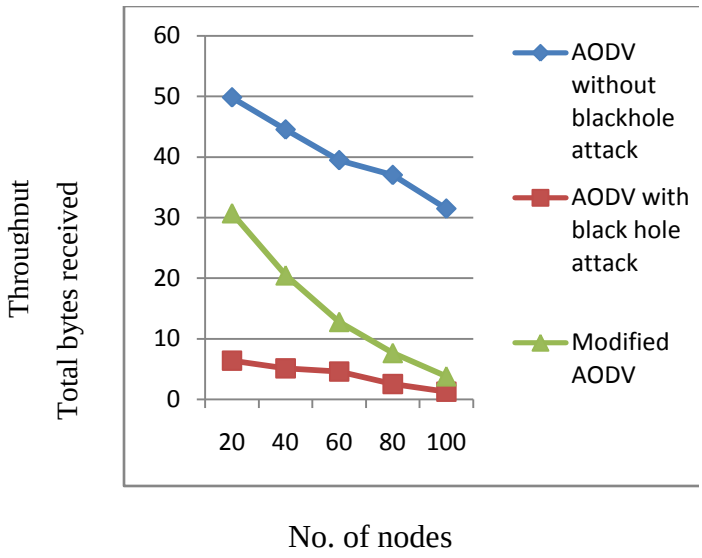
2) Last packet received at(s)



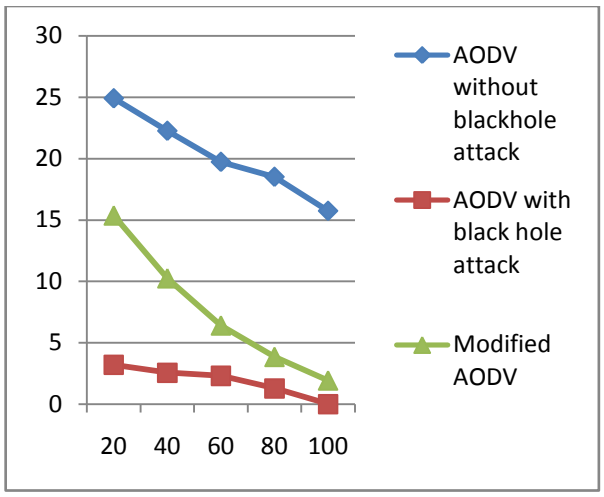
Time(s)

No. of nodes

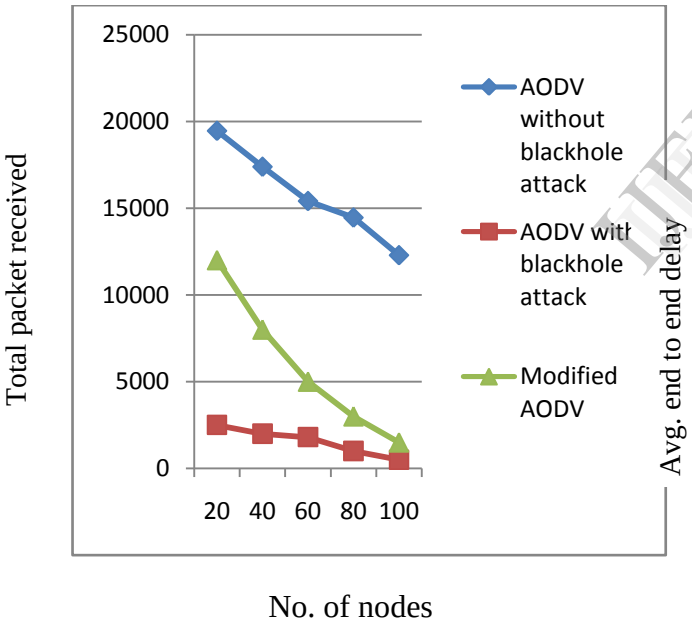
3) Total Bytes received



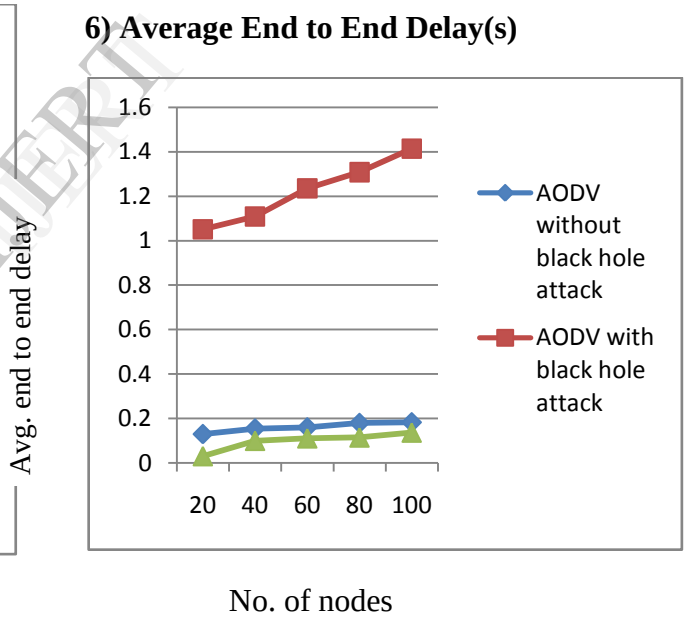
5) Throughput (bits/second)



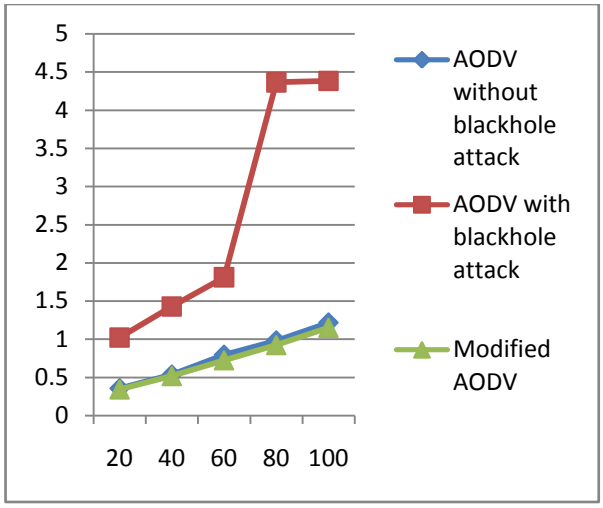
4) Total Packet received



6) Average End to End Delay(s)



7) Average Jitter(s)



Avg. jitter

No. of nodes

7. Conclusion

Security in adhoc network is a challenging task due to its features. Due to lack of security routing protocols suffer from vulnerable attacks. As a result network performance decreases.AODV is also one such protocol that is more vulnerable to blackhole attack due to lack of security. In this work we modify AODV routing protocol to enhance fault tolerance to blackhole attack in IEEE 802.11 based adhoc network. We have seen that by modifying its feature the throughput increases and packet loss decreases.

8.References

[1] Suryawanshi, Ranjeet and Tamhankar,Sunil (2012) "Performance Analysis And Minimization Of Black Hole Attack In MANET"International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue4,pp.1430-1437

[2] Ullah,Irshad and Rehman ,Shoaib ur(2010) "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols "

[3] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao(2011) "A survey of black hole attacks in wireless mobile ad hoc networks"Human-centric Computing and Information Sciences Vol.1,Issue 4

[4]C.Wei, L.Xiang, B.yuebin andG.Xiaopeng(2007), "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370

[5]Sharma, Govind , and Gupta, Manish (2012) "Black Hole Detection in MANET Using AODV Routing Protocol "International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6

[6]K,Sarabjeet and S,Birinder(2013)"A Survey on Blackhole attack on AODV routing protocol in Wireless Adhoc networks" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 8,pp-2523-2528

[7]D. Djenouri, A. Derhab, and N. Badache(2006). " Ad hoc networks routing protocols and mobility". Int. Arab J. Inf. Technol.3 (2):126–133

[8]Layuan, Li Chunlin, Yaun Peiyan(2007) "Performance evaluation and simulation of routing protocols in ad hoc networks", , Computer Communication

[9] Yi-Chun Hu, Adrian Perrig(2004), "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy

[10] Sharma, Arti and Jain, Satendra "A Behavioral Study of AODV with and without Blackhole Attack in MANET" International Journal of Modern Engineering Research (IJMER) Vol.1, Issue.2, pp-391-395