ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

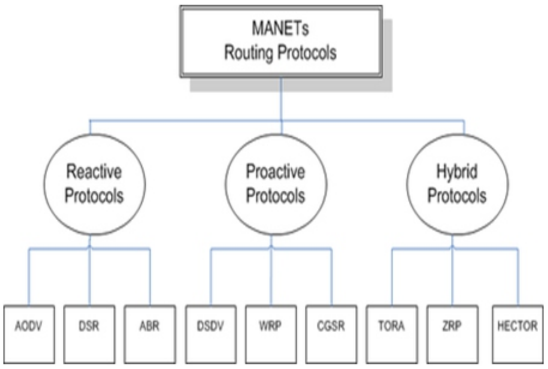
Implementation of Position Based Technique to Prevent Worm Hole Attack in AODV Routing Protocol for Manet

K.Madhuri
Assistant Professor,
Dept of CSE,
MVSR Engineering College,
Hyderabad, Telangana, India.

Dr.N.Kasi Viswanath
Professor and HOD,
Dept of CSE,
G.Pulla Reddy Engineering College,
Kurnool, India.

A mobile ad hoc network MANET is a collection of mobile nodes which communicate without the need of an access point or any infrastructure. MANET is a collection of two or more devices or nodes with wireless communications and networking capability that communicate with each other without any centralized administrator. The wireless nodes can dynamically form a network to exchange information without using any network infrastructure that already exists. It's an autonomous system in which mobile hosts connected by wireless links are free to move dynamically and some time act as routers at the same time. All nodes in a wireless ad hoc network act as a router and host i.e. each node acts as both sender and receiver. In MANETs intermediate nodes provide help in transmission of data. MANETS can be classified into two types single hop and multi hop. Nodes in a single hop network are in the transmission range and will communicate with each other directly. When the nodes are not within the range, then multi hop networks are used. Here, the intermediate nodes will help in transmission. The infrastructure of MANETs is decentralized and is not fixed, which means all the nodes are free to move. Routing protocols are used for the transmission of data packets between the nodes in MANET.

Routing protocols in MANET



Reactive Routing Protocols

Under a reactive (also called on-demand) protocol, topology information about the route is given only when needed. Whenever a node wants to know the route to a destination node, it sends a route request RREQ message to the network. A node obtains route by receiving route reply RREP packet. Advantages of this type of protocols are less routing overhead and high Scalability. Disadvantages are high latency and no predefined route is available. Some of the reactive routing protocols are Ad-hoc On Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR).We are concentrating on the reactive protocols as they overcome the limitation of proactive routing protocols that is maintenance of vectors to store route information.

AODV

AODV (Ad hoc On-demand Distance Vector routing) is a distance vector routing protocol, where routes are given as a vector of direction and distance. To find a route to a destination, a node broadcasts a RREQ (Route REQuest) message. This message is relayed by receiving nodes until it reaches the destination or an intermediate node with a fresh route to destination. If RREQ reaches the destination, then it generates RREP (Route REPly) message and unicasts to the originator of the RREQ. RERR (Route ERRor) messages are used to notify nodes about link breaks.

Different kinds of attacks in Network layer include
1.Black hole attack
2.Gray hole attack
3.Worm hole attack
4.Replay attack
5.Man in middle attack etc.

Numerous types of attacks occur in ad hoc network, mainly classified into two types, external attacks and internal attacks. In external attack, the attacker causes congestion, send fake routing information or disturb the nodes from providing services. In internal attack, the attacker tries to gain normal access to the network activities, using impersonation to get the access to network as the new node, or by directly compromising a current node and using it to conduct its malicious behaviour. Mobile ad hoc networks include different types of attacks.

Wormhole Attack in AODV

In this type of attacks, the attacker disturbs the routing process by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. Generally, two or more attackers connect using a link called “wormhole link”. They capture packets at one end and replay them at the other end using a private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network. Wormhole attack [10] is a kind of replay attack that is particularly challenging in MANET. Wormhole attack [8] commonly has two remote malicious nodes X and Y, both are attached via a wormhole link and they target to attack the source node S. These nodes are very well placed compared to other nodes in the network. Thus, a wormhole attack is not difficult to set up and can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks.

Worm hole attack is a attack that records the packets at one location in the network and tunnels them to another location (i.e., from one compromised node to other compromised node). The routing process can be disturbed whenever the control messages are tunneled.In our strategy we are trying to prevent worm hole attack by using Position Based Technique which is based on the positions of source and destination. Initially the source node will broadcast the route request message in case it doesn’t have a route towards the destination. The nodes that receive the request message will rebroadcast the request if they don’t have a route towards the destination node, if not, they are responsible for routing the messages. Once the destination node receives the route request message it checks the chance of attack in the route. It is done by calculating the distance between the source and destination nodes by using following formula.

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Once the distance is calculated, it is going check whether the hop count should be greater than (Distance/coverage area). If less number of nodes is present, then it assumes that there may be greater chance of attack, because the nodes that are compromised are said to have a greater range when compared to the normal node. If assumed number of nodes are present in that calculated area using hop count, data transfer can be done i.e., there is less chance for attacks.

•Calculate the distance between source and destination.

•Calculate the value of distance by coverage area.

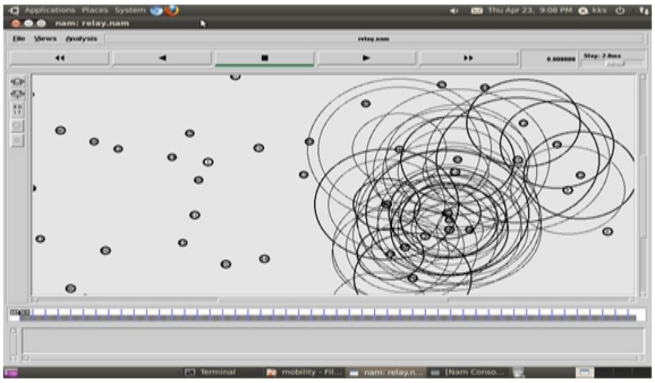
•Comparing distance/coverage area with hop count

•If calculated value is less than the hop count means that is not good path for transferring data from source to destination.

•Because in this path there may be chance for malicious nodes.

•In case of normal path the hop count should be little greater than calculated value (which is distance/coverage area).

•Still if we choose that path, there may be more chances of data being dropped or modified so better not to choose that path.



AODV Simulation

The above figure shows the simulation of 100 nodes in AODV routing protocol

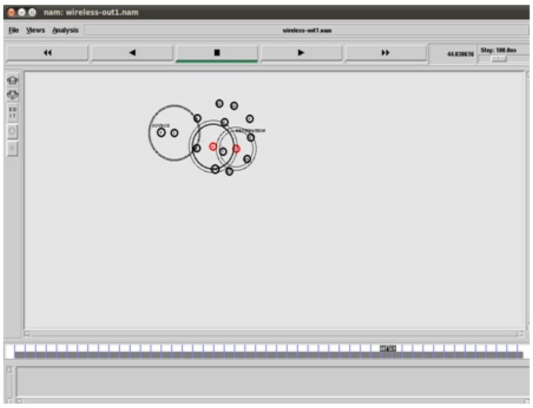
Simulation Environment for AODV Parameter	Value Taken
Number of Nodes	100
Maximum Speed	10,20,30,40 mps
Simulation Time	0-100sec
Traffic Type	Constant Bit Rate
Terrain	1600x1600
Mobility Model	Random Waypoint
Packet Size	1000

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Simulation Parameters

Analysis of AODV routing under wormhole attack

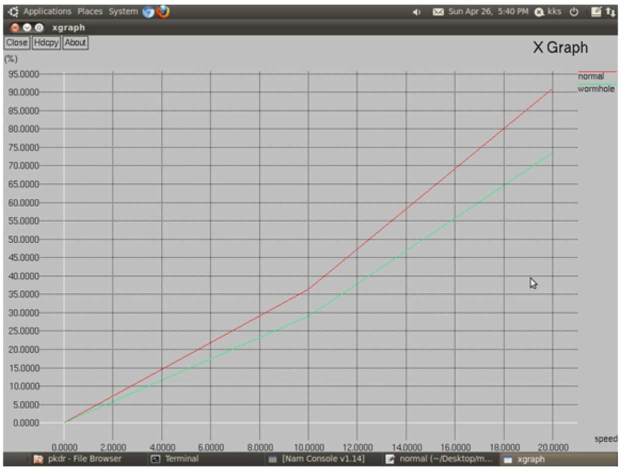
Parameter	Value Taken
Number of Nodes	100
Maximum Speed	10,20 mps
Simulation Time	0-100sec
Traffic Type	Constant Bit Rate
Terrain	1600x1600
Mobility Model	Random Waypoint
Packet Size	1000
Routing Protocol	AODV
Attack	Wormhole



AODV with wormhole attack

Packet Delivery Ratio VS Speed

Pkdr(%)	10ms	20ms
AODV	36.42	91.421
AODV(Attack)	29.0734	73.4824



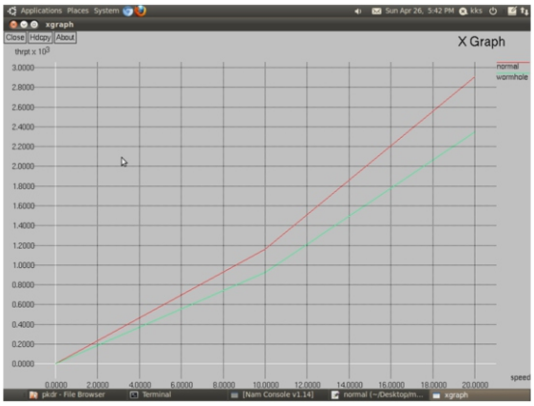
Packet delivery ratio in AODV with & without wormhole attack

The above graph shows the packet Delivery Ratio of AODV with and without wormhole attack. Here we are analyzing the performance by varying the speed of the nodes. In the presence of attack, the packet delivery of AODV is low.

X-axis-speed Y-axis – Packet Delivery Ratio

Throughput Vs Speed

Throughput(bps)	10ms	20ms
AODV	1162	2907
AODV(Attack)	928	2346



Throughput of AODV with and without wormhole attack

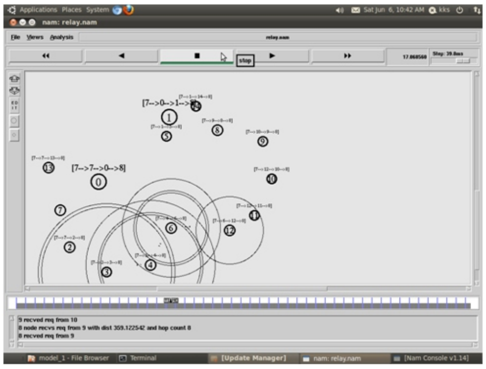
The above graph shows the throughput of AODV with and without wormhole attack.Here we are analyzing performance by varying the speed of the nodes. In the presence of attack, the Throughput of AODV is low.

X-axis-speed Y-axis –Throughput

After Applying Prevention technique in AODV

Parameter	Value Taken
Number of Nodes	30,100
Maximum Speed	20 mps
Simulation Time	0-20.5sec
Traffic Type	Constant Bit Rate
Terrain	1600x1600
Mobility Model	Random Waypoint
Packet Size	1000
Routing Protocol	AODV
Technique	Position based technique for preventing wormhole attack

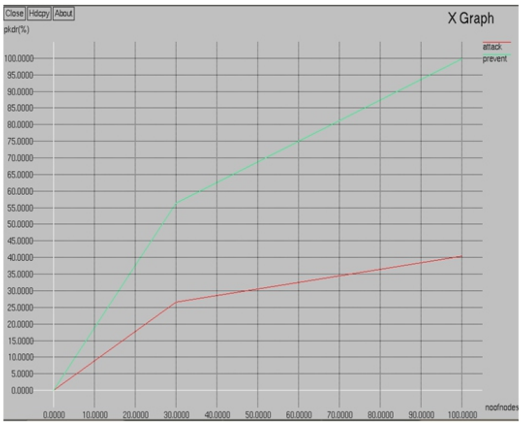
Simulation values



```
9 recved req from 10
8 node recvs req from 9 with dist 359.122542 and hop count 8
8 recved req from 9
```

Prevention of wormhole attack in AODV
Above Nam show the simulation of AODV after applying wormhole prevention technique.
Packet Delivery Ratio

Pdr(%)	30nodes	100nodes
AODV(attack)	26	56
AODV(prevention)	40.33	90

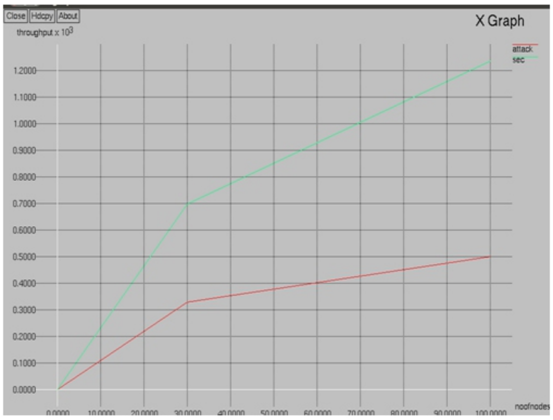


Packet Delivery Ratio

The above graph shows the Packet Delivery Ratio in AODV with wormhole attack and after applying the prevention technique. Here we consider number of nodes on X-axis and Packet Delivery ratio on Y-axis, For both 30 and 100 nodes AODV with prevention gives better performance.

Throughput

Throughput(bps)	30nodes	100nodes
AODV(attack)	328.9	499.10
AODV(prevention)	696.60	1235.100



Throughput
The above graph shows throughput of AODV with wormhole attack and after applying the prevention technique. Here we are analyzing the performance by varying the number of nodes from 30 and 100.AODV with wormhole attack gives fewer Throughputs than after applying prevention technique.On X-axis-number of nodes Y-axis- Throughput(bps) We have analyzed the performance of AODV under worm hole attack for various network parameters like packet drop ratio and Throughput and implemented Position based technique for preventing Worm hole attack.

REFERENCES:

[1]. survey of manet misbehavior detection approaches survey of manet misbehavior detection approaches survey of manet misbehaviour detection approaches Punya Peethambaran and Dr. Jayasudha J. S.1Department of Computer Science and Engineering, SCT College of Engineering, Trivandrum, Kerala2 Head of the Department, Department of Computer Science and Engineering,SCT College of Engineering, Trivandrum, Kerala.

[2]. Performance analysis of AODV & DSR Routing protocols for MANET Uma Rathore Bhatt, Abhishek Dangarh, Akanksha Kashyap, Aishwarya Vyas Department of Electronics&Telecommunication Engineering, Institute of Engineering & Technology Devi Ahilya University, Indore -452017, India

[3]. Study of MANET: Characteristics, Challenges, Application and Security Attacks Aarti Department of Computer Science & Engineering , MRIU Faridabad, Haryana, India Dr. S. S. Tyagi Professor and Head, Department of computer science & Engineering, MRIU, Faridabad, India

[4]. International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 3 Issue 2, May 2014A Study on Wormhole Attack in MANETAnshika Garg1, Shweta Sharma2 1School of Computing Science and Engineering, Galgotias University, Greater Noida 2 School of Computing Science and Engineering, Galgotias University, Greater Noida

[5]. A Survey of Routing Protocols in Mobile Ad Hoc Networks Sunil Taneja*and Ashwani Kush†

[6]. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012 269 Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review Gagandeep, Aashima, Pawan Kumar

[7]. Performance Analysis of Dynamic Source Routing Protocol 1 Amer O. Abu Salem, 2 Ghassan Samara, 3 Tareq Alhmiedat 1 College of Science & Technology Zarqa University, Zarqa-Jordan 2 College of Science & Technology Zarqa University, Zarqa-Jordan 3 College of IT Tabuk University, Tabuk, KSA.

[8]. Black-Hole and Wormhole Attack in RoutingProtocol AODV in MANETAmol A. Bhosle, Tushar P. Thosar and Snehal Mehatre Department of Computer Science and Engineering, SGB Amravati University,JDIET, Yavatmal, IndiaDepartment of Computer Science and Engineering, SGB Amravati University,JDIET, Yavatmal, India Department of Computer Science and Engineering, SGB Amravati University,JDIET, Yavatmal, India

[9]. Performance Metrics in Ad-hoc Network Joni Birla1, Basant Sah2 1 M. Tech Student,, BRCM, Bahal 2 Assistant Professor , BRCM, Bahal jonibirla@yahoo.com basantbitmtech2008@gmail.com

[10]. Security Threats in Mobile Ad Hoc Networks Sevil Şen, John A. Clark, Juan E. Tapiador Department of Computer Science, University of York, YO10 5DD, UK

[11]. Effects of Wormhole Attack on AODV and DSR Routing Protocol through the Using NS2 Simulator Mohamed Otmani, Dr. Abdullah Ezzati University Hassan Settat, Morocco.