Examination of AODV Routing Protocol with Wormhole Attack

Gulzar Ahmad Wani
M.Phil Student
Department of Computer Science
BGSB University, Rajouri, J&K, India

Sanjay Jamwal,PhD
Assistant Professor
Department of Computer Science
BGSB University, Rajouri, J&K, India

ABSTRACT
In Adhoc Network, Mobile Adhoc Network (MANET) is vibrant Adhoc network. MANET is collection of mobile network devices that are connected through wireless medium i.e., radio signals. These mobile network devices form a dynamic topology i.e., mobile nodes move freely and quickly, in and out from network. These is no central control for co-coordinating these network device i.e. decentralized network .These devices control each other directly i.e, peer-to-peer connection. The dynamic nature of MANET makes it vulnerable to variety of security threats like wormhole attack, eavesdropping etc. The performance and reliability of the network is affected by making alteration in routing protocols by the attacker. Wormhole attack is a type of tunneling attack where an attacker at one end of tunnel attracts data packets from one hop neighbors and transmits these data packets to another attacker of the tunnel which delivers these data packets to destination node. Transmitting data packets through tunnel may result various security attacks like wormhole attack, black hole attack, eavesdropping attack. This proposed paper examines the consequences of wormhole attack in AODV routing protocol based MANET using OPNET Simulator.

General Terms
Adhoc Network, Mobile Adhoc network, Routing Protocols.

Keywords
MANET, Wormhole Attack, AODV Protocol, Route Request (RREQ),Route Reply(RREP),Broad-cast.

1. INTRODUCTION
Ad-hoc network is the modern image of wireless network especially for mobile node. A mobile ad hoc network (MANET) is a collection of two or more nodes, continuously self-configuring, self-organizing, dynamic topology, infrastructure-less network of mobile devices connected without wires. Ad hoc network supports more advanced applications, such as transportations, military, security, health, educations, disaster recuperation, search and rescue and battlefields are the true examples where Ad-hoc network are used [1]. In Ad-hoc network, a node behaves as both end system as well as router (i.e., it stores and forwards the routing packet to forwarding node in the network). The selection for shortest path for forwarding the data packet to other node is made by routing protocols [2]. DSR (Dynamic Source Routing) [4], DSDV (Destination Sequence Distance Vector) [3] and AODV (Ad-hoc On-Demand Vector) [5] are few routing protocols developed for MANET. Dynamic topology, limited battery power, limited memory storage, no central control, limited bandwidth constraint is the characteristics of MANET. Nodes can move freely out and join the network. In MANET node acts End node as well as router for forwarding data. Sometime mobile nodes are not able to communicate with destination node directly. Then they have to depend on the intermediate node along the route and packets are relayed in store and forward mechanism through intermediate node.

Security in mobile ad-hoc network is the current important issue of network. The Services of network like confidentiality and integrity of data is attained by facing and solving the security issue of MANET. The dynamic topology and open nature makes the wireless network (especially Mobile Ad-hoc network) more vulnerable to security threats. The various loopholes that threatens the security of wireless network that consists of sink/black hole, MAC spoofing, Denial-of-Service attack , Network injection, worm hole, Man-in-the-middle attacks, Sybil attack and etc

1.1.Classification
The routing protocols for Ad-hoc network is broadly categorized into three types:

- Proactive (table-driven) protocols.
- Reactive (on-demand) protocols.
- Hybrid Protocols

1.1.1. Proactive (Table driven) Routing Protocols
In this type of routing protocols nodes maintain routing information in the routing table and that routing information is obtained from its neighbor nodes. This type of routing protocols periodically exchange the routing information among nodes in the network or when there is a change in network topology caused by the moving mobile nodes out or join the network. The routing table contains routes to the destinations if there is a frequent change in network topology, the cost for maintaining the route information in such type is very high. Routing Information Protocol (RIP), Destination Sequenced Distance Vector (DSDV) Protocol [7], and Optimized Link state Routing (OLSR) protocol [8].

1.1.2. Reactive (On-Demand) Routing Protocol
In this category of routing protocol, routing table are not maintained or exchanged periodically. Here the route from source to destinations discovered "on-demand" When source node wants to send the data packet to destination .it initiates the process of finding the route to destination. Once the route is established. It is maintained till either the destination gets unreachable or it is not needed any more. Examples of Reactive routing protocols are Dynamic Source Routing (DSR) protocol [9], Ad-hoc on demand Distance Vector (AODV) Routing protocol [10], Temporary ordered Algorithm (TORA) protocol [11].

1.1.3. *Hybrid routing Protocols*

To overcome the drawbacks of above two types of routing protocols i.e., proactive routing protocols and reactive routing protocols. The concept of hybrid routing protocols came to get be most of their benefits .Examples of Hybrid routing protocols are Zone Routing Protocols (ZRP) [12], Wireless Adaptive Routing Protocols (WARP) [13].Diagrammatically classification of routing protocols are of MANET are shown Fig 1.

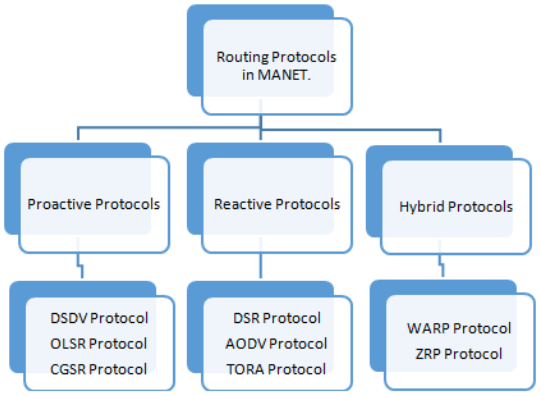

Fig 1: Classification of Routing Protocols in MANET

1.2.AODV Routing protocols

AODV is a reactive protocol that does not maintain any routing information in routing table or maintain any periodic update. A node does not keep any other nodes information until it needs to communicate. Nodes maintain connectivity with their neighbor by using a technique (sending hello messages to neighbors). The routing table contains information of next hop to destination and sequence numbers that provides freshness of route.

1.1.4. *Format of Packet in AODV*

In AODV uses following packet messages:

1. Route Request packet format

Source Add.	Source Seq. No	Broadcast-id	Dest. Add.	Dest. Seq. No	Hop count

2. Request Reply Packet Format[16]

Source Add.	Destination add.	Destination seq. no	Hop count	Life time

3. Route Error packet Format

Unreachable destination IP address	Unreachable Destination sequence No

4. Hello messages

To find active neighbors in the n/w Hello messages are used. AODV as a reactive protocol uses hello message periodically to make nodes active. When TTL=1 the hello messages are forwarded and on receiving the hello message the receiving node will update the routing table with new life time of the neighbor node information [14].

1.1.5. *Working*

The working of AODV protocol is divided into following phases

- Path Discovery phase
- Path reverse phase
- Path forward path
- Routing table management phase
- Routing Maintenance phase

Path Discovery

The discovery of path starts when a source node wants to communicate with a node whose entry is not available in its routing table. The source node broadcasts the Route Request (RREQ) packet to its neighbors [15]. The format of Route Request RREQ is given below

Source add.	Broadcast-id	Source Seq. No	Dest. Address	Destination Seq. No	Hop count

The broadcast_id an Source_id uniquely represents RREQ. On each new RREQ by the source node broadcasts_id is incremented. One-hop neighbor sends back Route Reply if it is a destination or rebroadcasts the RREQ to its neighbor before forwarding it to the next neighbor, hop counter is incremented and a reverse path pointer is set up with node from which it receives the RREQ. If Intermediate node can receive more than one same (duplicate) RREQ. Then the node checks RREQ with the broadcast_id if it has already received it simply rejects the RREQ otherwise processes the RREQAs the RREQ moves among intermediate nodes till destination. Each intermediate node setup a reverse path with its previous predecessor node as well as forward path setup

Reverse path Set Up

The two sequence numbers in the RREQ are source sequence number and destination sequence number. Source sequence number provides latest fresh reverse route to the source and destination sequence number provides fresh route information to the destination during route discovery phase, as the RREQ makes the route from source to destination while finding the route it passes through various intermediate nodes and each intermediate node make a reverse path with the previous node from which it got the RREQ the reverse path setup is retained for certain period of time so that for the same RREQ destination will send Route Reply RREP to the sender [15].The reverse path setup is shown below Figure 2:

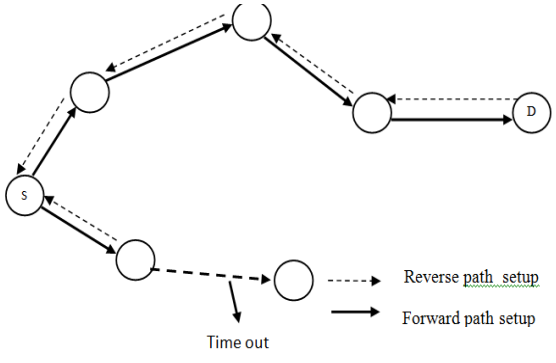

Fig 2. AODV Reverse/ Forward Path Setup

Forward Path setup

Whenever a sender sends a RREQ to destination. The sender node broadcasts the RREQ to its one-hop neighbor. The neighbor node that receives the RREQ will first see its routing table for the entry to the destination route. If it has route to the destination it will compare sequence number of RREQ with the sequence number of entry in the routing table. If the sequence number of the entry in routing table is greater than or equal to RREQ sequence number then it will send route reply RREP to the source node otherwise the node will rebroadcast the RREQ to its own neighbor. Simultaneously the node will increment the hop count value and sequence number and make a unicast reverse path with the previous node (source node) from which it receives the RREQ [15]. The format of unicast Route Reply is shown below

Source Address	Destination Address	Destination Sequence Number	Hop_count	Life time

Recursively using the same procedure the RREQ reaches to the destination by making reverse path setup.

The destination node send the RREP packet to the source node through reverse path setup. The intermediate node when receives a RREP from destination and passes it to source node. The intermediate node along path setup a forward pointer to the node from which it receives the RREP packet and the timeout in the entry is updated and records the latest sequence number for the path from Source to destination.

Route Table Management

In Route Table Management [15], In addition to the sequence number, a routing table contains other information also which is called soft-state associate with entry. The reverse path entry in the routing table also contains a timer which is known as route request expiration timer. The purpose of this timer is remove the route entries for those node who do not lie in the current topology. The expiration time relays on size of Ad-hoc network. The routing table contains also one more column which is called "Route cache timeout". The "route cache time-out" is used to find out valid or invalid routes in the routing table.

A node is active in the current network topology. if it sends at least one packet (hello message) to its neighbor's within "active_timeout_period" this information is also maintained in routing table for each entry. Every node contains destination node entry in the routing table which is shown below:

- Destination
- Next hop
- Number of hops(metrics)
- Sequence number for destination
- Active neighbor for this route entry time for the route table entry.

Route maintenance

Path maintenance in AODV is maintained using the hello message that are sent periodically. if the nodes move from this location and route failure occurs and Route error message is sent to the source node if the source node needs the connection, then again route discovery process starts. To determine whether the route is needed or not it will see the history whether this node route has been used recently or it inspect the protocol when connections are open [15].

1.3.Wormhole Attack

Wormhole is conjectural feature of topology that provides the short-cut through space. It is like a tunnel with two end points. The wormhole attack [6] is the most serve attack in the network security which involves two malicious nodes and high speed tunnel called wormhole link. In this attack, an attacker at one location receives the packet and transmit it to another attacker which is very far-way, by a high speed wormhole tunnel in the network.

Working

Working of wormhole attack can be well explained by the following Fig. 3.

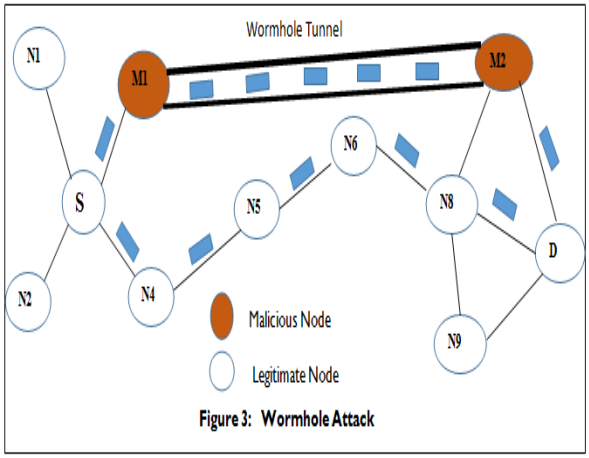

Fig. 3. Wormhole Attack in MANET

In this Fig 3, Nodes S is Source node and Node D is destination Node when Node Source node S wants to communicate with the Destination Node D with the help of using routing protocols using MANET. Source Node S broadcasts the Route Request RREQ to its neighbor nodes .Here nodes M1 and M2 are two malicious nodes that are connected with each other by a high speed communication channel which is known as wormhole tunnel. Malicious node M1 is also a member of Source node S , as soon as M1 receives the RREQ from Node S it instantly sends RREP back to node S having route to destination node D with less number of hops. The source node S sends the packet through node M1 as it offers the shortest path. Then M1 node receives the packet from source node S and sends it to other malicious node M2 through wormhole tunnel. The malicious node can drop the packet or selectively forward the packet to destination.

When the same Route Request RREQ that flows through legitimate nodes will arrive at destination. The destination node rejects these RREQ because it has already received the same Route request(RREQ) through the malicious node M2 .Hence it results in the disruption of routing protocols when the routing protocol are disrupted means whole network will be disturbed.

2. SIMULATION SETUP

Opnet 14.0 Simulators is used for performing simulation of proposed mechanism. For performing Simulation following parameters are used.

Total no of nodes =16

Infected nodes = 02

Packet size =512 bytes

Protocol= AODV

Area= 100 * 100 m

Network Traffic= CBR.

Fig. 4. Allocation of nodes with 2 wormhole attacker node.

Fig 4. Shows the scenario of node distribution with two nodes as wormhole nodes i.e., node 0 and node 5. These wormhole nodes are connected with tunnel and attract packets from these neighbor nodes.

3. EXPERIMENTAL ANALYSIS

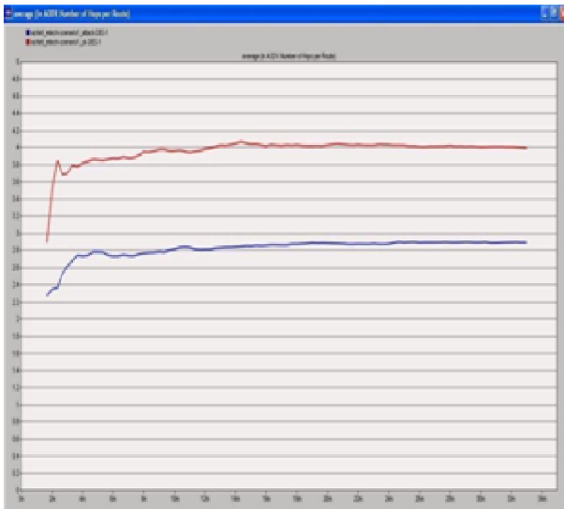

Fig 5. Average Hop-Count of each Path

Fig 5. Presents the average route length using number of hops for the condition when there is attack in network and no attack in the network. The X-axis represents the simulation time and Y-axis represents the number of hops. Here no attack condition is represented by red color line and attack condition is represented by blue color line. It occurs when attacker node starts sending packets via tunnel between them and thus reduces the no of hops as represented by blue color line.

Fig 6. Average Delay of each Path.

Fig 6. Presents the average route discovery time for wormhole attack in the network and no wormhole attack in the network. The X-axis represents the simulation time and Y-axis represents the average delay. Here no attack condition is represented by red color line and attack condition is represented by blue color line. Delayed is decreased by wormhole attack because packets are not transmitted through intermediate nodes as repressed by blue color line.

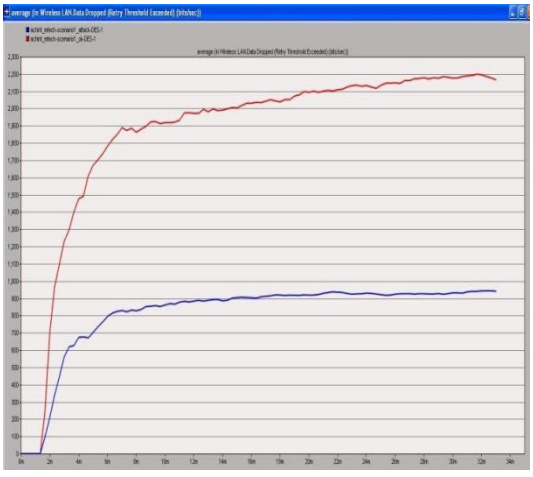

Fig 7. Average data dropped

Fig.7. Presents the average data dropped during transmission. The X-axis represents the simulation time and Y-axis represents the packet loss. Here no attack condition is represented by red color line. Packets have to travel through no of hops and data packets gets dropped who doesn't find their destination and attack condition is represented by blue color line. here packets are dropped because it travelled through tunnel.

4. CONCLUSION

The Characteristics of MANET depicts that MANET is vulnerable to various security threats, it needs to have an efficient, reliable and secured routing protocol so that it can be deployed rapidly and use dynamic routing. An AODV is less secure and is susceptible to various security threats like change in sequence number and hop counts, spoofing and fabrication. Wormhole attack is a real threat against AODV protocol in MANET. Various trustworthy techniques for detection and prevention of wormhole attack should be used. Some existing solutions cannot work well in the presence of more than one malicious node, node while some other requires special hardware. Proposed paper works well with limited no of nodes and is not suitable where density of nodes is large. So, there is need to develop such a technique that can be best suited in any environment to make the MANET more secure.

5. REFERENCES

[1] L.Sudha Rani, R.Raja Sekhar, " Detection and prevention of wormhole attack in stateless multicasting ", International journal of Science & Engineering Research Volume 3, issue 3, March – 2012. Page 1-5.

[2] Jian Yin, Sanjay Madria, "A hierarchical secure routing protocol against black hole attack in sensor network", IEEE SUTC, 2006.

[3] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. 6th Ann. ACM Int'l Conf. Mobile Computing and Networking, ACM Press, 2000, pp. 255– 265.

[4] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol ", in Proc. 3rd ACM Intl. Symp., on Mobile Ad Hoc Networking and Computing, Jun 2002.

[5] P.G. Argyroudis and D. O'Mahony, "Secure Routing for mobile ad hoc networks", IEEE Communications Surveys & Tutorials, third quarter 2005, Vol. 7, no3, 2005 258 Authorized licensed use limited to: University of Allahabad. Downloaded on July 30, 2010 at 16:19:57 UTC from IEEE Xplore. Restrictions apply.

[6] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Tohoku University and Abbas Jamalipour, University of Sydney, "A Survey of Routing Attacks in Mobile Ad Hc Networks", Security in Wireless Mobile Ad Hoc Networks and Wireless Sensors, IEEE Wireless Communications, October 2007.

[7] C. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In Proceedings of SIGCOMM '94 Conference on Communications, Architectures, Protocols, and Applications, (London, UK, Sept. 1994), p. 234-244.

[8] C. Adjih, A. Laouiti, P. Minet, et. al., Optimized link state routing protocol. Work in Progress, IETF draft, MANET Working Group, INRIA Rocquencourt, France, 2003.

[9] D. Johnson and D. Maltz,"Dynamic source routing in ad hoc wireless networks", In Mobile computing, T. Imielinski and H. Korth, Eds. Kluwer Academic Publishers, 1996: Ch. 5, p. 153-181.

[10] C. Perkins and E. Royer. Ad-hoc on-demand distance vector routing. In Workshop on Mobile Computing and Systems Applications, 1999.

[11] Park and M. Corson, Temporally-ordered routing algorithm (TORA) version: 1 functional specification. Internet-Draft, draft-ietfmanet-tora-spec-00. Txt, November 1997.

[12] Haas and M. Pearlman, The zone routing protocol (ZRP) for ad hoc networks. Internet draft, Mobile Ad-Hoc Network (MANET) Working Group, IETF, 1998.

[13] P. Khengar and A. Aghvami, Warp-the wireless adaptive routing protocol. In Proceedings of IST Mobile Communications Summit 2001, 2001, p. 480–485.

[14] Preeti Bhati, Rinki Chauhan, and R.K. Rathy, "An Efficient Agent Based Routing Protocol in MANET", International Journal of Computer and Engineering, Vol No. 7, July 2011.

[15] Charles E. Perkins and Elizabeth M. Royer," Ad-hoc On-Demand Distance Vector Routing", 2nd IEEE WorkShop on Mobile Computing System and Application (WMCSA'99).

[16] Laxmi Shrivasta, Sarita S. Bhadauria, G.S. Tomar, "Performance Evaluation of Routing Protocols in MANET with Different Traffic Loads", International Conference on Communication System and Network Techonologies IEEE 2011.