Survey of Security of AODV, OLSR AND TORA

[1]Ginni Bhasin, [2]Dr.Puneet Goswami
[1]GGITC, Ambala, India
[2]Professor, GGITC, Ambala, India

***Abstract* - Security in Wireless Ad hoc Network (WAN) is very important issue. Due to dynamic topology and mobility of nodes, node. Wireless Ad hoc Networks are more vulnerable to attacks than conventional wired and wireless networks. Nodes of node. Wireless Ad hoc Network communicates directly without any central base station . A wireless ad-hoc network is a temporary network set up by wireless mobile nodes moving random in places that have no infrastructure. For communication in mobiles nodes routing protocols are used like Reactive routing protocol i.e. Ad-Hoc on Demand Distance Vector (AODV), Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Hybrid routing protocol i.e. Temporary Ordered Routing Algorithm (TORA).**

***Index Terms* - Wirless, Tora, Aodv, Black Hole Attack**

I. INTRODUCTION

Wireless networking is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical.
- To remotely connect mobile users or networks.

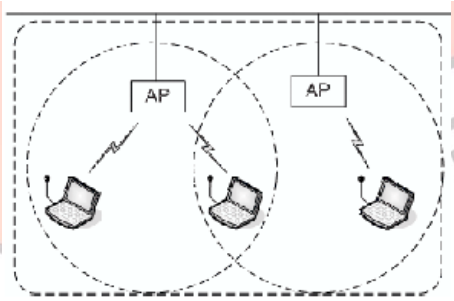


Fig. 1.1 Infrastructure wireless network

To reduce these anomalies IEEE discovered new network called infrastructure less wireless networks also called Ad-hoc network. In this network each node connected to the node or nearly base station. This network also called node to node network. This network establishes a peer to peer relationship. An example of the mobile adhoc network is that a group of soldiers move in outdoors while communicating with one another though the radios without a central controller to control the communication in the network.

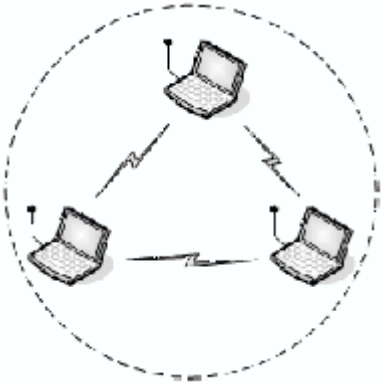


Fig 1.2 Infrastructure less wireless networks

II. ROUTING PROTOCOL

Routing Protocol

Routing protocols between any pair of nodes within an ad hoc network can be difficult because the nodes can move randomly and can also join or leave the network. This means that an optimal route at a certain time may not work seconds later. Discussed below are three categories that existing ad-hoc network routing protocols fall into:

1. Table Driven Protocols (Proactive)
2. on Demand Protocols (Reactive)
3. Hybrid Protocols

Ad-hoc Mobile Routing Protocols

Table Driven Protocols (Proactive):- Proactive protocols are table-driven and actively determine the layout of the network. Through a regular exchange of network topology packets between the nodes of the network, a complete picture of the network is maintained at every single node . Hence, there is minimal delay in determining route to the destination. This is especially important for time-critical traffic. Examples of proactive protocols include: OLSR, DSDV etc.

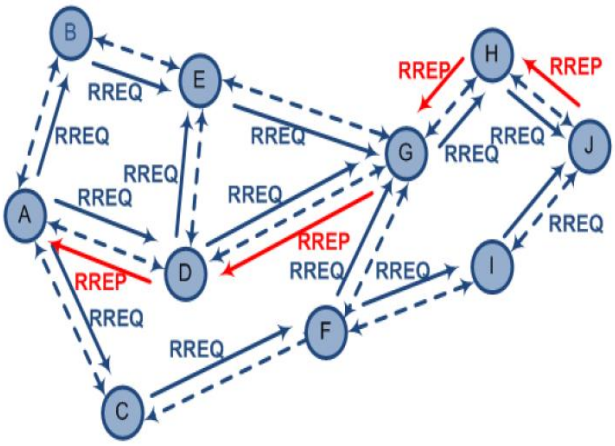
1. **OLSR (*Optimized Link State Routing Protocol (OLSR)*** – PMP OLSR is a table-driven routing protocol and naturally possesses specialties of proactive protocols. It uses an optimized link-state scheme, which is based on the technique *Multipoint Relaying (MRP)*, to diffuse topology information. The operation of OLSR consists of a necessary core function and a set of auxiliary functions, which could be optionally utilized according to specific scenarios.
2. **DSDV (Destination Sequenced Distance Vector) -** Destination-Sequenced Distance-Vector Routing protocol is a proactive table driven algorithm based on classic Bellman-Ford routing. In proactive protocols, all nodes learn th network topology before a forward request comes in. In DSDV protocol each node maintains routing information for all known destinations. The routing information is updated periodically. Each node maintains a table, which contains information for all available destinations, the next node to reach the destination, number of hops to reach the destination and sequence number. The nodes periodically send this table to all neighbors to maintain the topology, which adds to the network overhead. Each entry in the routing table is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops .

On Demand Protocols (Reactive):-Reactive protocols only find a route to the destination node when there is a need to send data [8]. The source node will start by transmitting route requests throughout the network. The sender will then wait for the destination node or an intermediate node (that has a route to the destination) to respond with a list of intermediate nodes between the source and destination. Examples of reactive protocols include:- AODV , DSR , TORA etc.

1. Dynamic Source Routing (DSR)

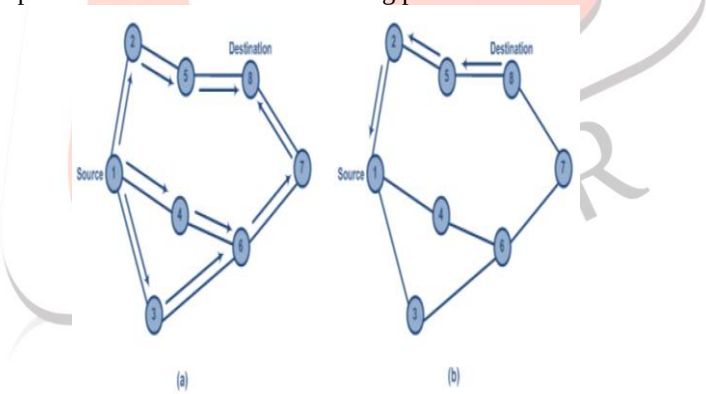
DSR is a reactive routing protocol in which the primary aspect is to store the whole path from source to destination in the routing table instead of having the next hop stored (AODV routing protocol). Therefore, the packet header must include all nodes through which the packet must travel to be delivered to the destination. Similar to AODV, the RREQ and RREP are used to perform the route discovery and delivering the reply message back to the source. In this protocol, the RREQ message rebroadcast method is used if the node receiving the RREQ message does not have the destination information in its routing table. However, in DSR routing protocol, cache route mechanism is used in case of link breakage. For instance, suppose the source node S has route <S, A, B, C,D> to destination node D, and the link <C, D> encountered a failure due to node`s movement. In such scenario, the source node S looks up in its cache route for another route to destination node D. It is noted that other routes to destination node were maintained in cache route due to overhearing the RREQ message by intermediate nodes via various routes. The cache route mechanism results in boosting up the data transmission. Upon receiving the RERR message by the source node, the new route discovery procedure will be initiated. The RERR message will be originated and sent to the source by the very first node which is closer to the source than others. Thereafter, the source applying piggyback strategy based on the RERR message received and the new RREQ message will be broadcasted to all the nodes used to deploy the failed link. Figure 2 illustrates the transmission of pair of <RREQ, RREP> while performing the route discovery procedure until receiving the reply message.

possible drawback when the number of nodes increases. Another issue that must be taken into account is being unaware of neighbor list or their link status. Since no periodic updating packet exchanged between nodes, applying cache route mechanism may cause failure due to deployment of invalid or expired links.



Route Discovery Procedure in DSR Routing Protocol

2. **Ad Hoc on Demand Distance Vector (AODV) -** AODV is the on-demand (reactive) topology-based routing protocol in which backward learning procedure is utilized in order to record the previous hop (previous sender) in the routing table. In the backward learning procedure, upon receipt of a broadcast query (RREQ)10 which contains source and destination address, sequence numbers of source and destination address, request ID and message lifespan, the address of the node sending the query will be recorded in the routing table. Recording the specifications of previous sender node into the table enables the destination to send the reply
packet (RREP) to the source through the path obtained from backward learning. A full duplex path is established by flooding query and sending of reply packets. As long as the source uses the path, it will be maintained. Source may trigger to establish another query-response procedure in order to find a new path upon receiving a link failure report (RERR) message which is forwarded recursively to the source. Being on-demand to establish a new route from source to destination enables AODV protocol to be utilized in both uni cast and multicast routing. Figure 1 illustrates the propagation of RREQ packet and path of RREP reply packet to the source .Multiple RREP messages may be delivered to the source via different routes but updating the routing entries will occur under one condition which is if the RREP has the greater sequence number. A message with higher sequence number represents the more accurate and fresh information. Several enhanced approaches were proposed to eliminate the large overhead and high latency (End-to-End Delay) which result in encountering high amount of packet loss occur in AODV routing protocol.



(a)Propagation of the RREQ, (b) RREP Path to the Source

3. **TORA (Temporally Ordered Routing Algorithm) -** TORA is an on-demand routing protocol. The main objective of TORA is to limit control message propagation in the highly dynamic mobile computing environment. Each node has to explicitly initiate a query when it needs to send data to a particular destination. The protocol has three basic functions: – Route creation, Route maintenance, Route erasure. The route creation process converts an undirected network into a DAG rooted at the destination by assigning directions to the links. The purpose of route maintenance Is to reverse some of the links so that network reorients itself in a state where each node has a path to the destination. If a network is partitioned the route erasure mechanism erases all paths in partitions which do not contain the destination.

III. Related Work

Dong-Won Kum et al [1]Wireless mesh networks (WMNs) are attractive as a new communication paradigm. Ad hoc routing protocols for WMNs are classified into: (a) proactive, (b) reactive and (c) hybrid approaches. In general, proactive routing is more suitable for a stationary network, while reactive routing is better for a mobile network with a high mobility. In many applications, a node in WMN is mobile but it can fluctuate between being mobile and being stationary. Therefore, a hybrid routing approach with the ability to adapt to node mobility could improve the performance of WMNs. In this paper, we propose a Mobility-aware Hybrid Routing (MHR) approach for WMNs, which varies its routing between reactive and proactive to adapt to node mobility.

The MHR basically uses a reactive approach for route discovery, and as a proactive approach it maintains the route entry in the routing table unless the route fails due to node movement, even if the route is not used. In this paper, the MHR approach was applied to AODV, and herein called AODV-MHR. Its performance was compared with that of AODV and OLSR by simulation.

Saad Khan et al[2]Wireless mesh networks have recently gained a lot of popularity due to their rapid deployment and instant communication capabilities. AODV is a well known routing protocol that can discover routes on-the-fly in a mobile environment. The protocol is highly scalable and can support thousands of nodes making it an ideal protocol for wireless mesh networks. WMN consists of two major components, the Mesh Router and the Mesh Client Mesh Routers are static, high powered devices that form the structure of the WMN, often consisting of multiple radios. Mesh Clients are generally single radio communication devices that can either be mobile or stationary. Wireless mesh networks are used to provide connectivity in a region, without necessitating a fixed infrastructure. The network is generally formed using an ad-hoc routing protocol, which enables communication in a dynamic topology. AODV is a well know routing protocol, which is currently being used in a number of mesh products. However, as AODV was actually developed for single-radio nodes, it shows degraded performance in densely populated mesh networks. In this paper, we have discussed and compared four variants of the AODV protocol, which can be used to establish a hybrid wireless mesh network.

Fahim Maan et al[3] The fundamental characteristic which differentiates MANETs from other wireless or wired networks is mobility. Therefore, MANET routing protocols are designed to adaptively cater for dynamic changes in topology while maximizing throughput and packet delivery ratio, and minimizing delay, routing load and energy consumption. Our simulative study on MANET routing protocols and mobility models aims to determine the performance of current MANET routing protocols with respect to various mobility models implemented in ns-2. We compare a number of reactive and proactive routing protocols including AODV, DSR, DSDV, OLSR. In this paper, we have analyzed the behavior of MANET. The results of our extensive ns-2 simulations clearly indicate the significant impact that node mobility pattern has on routing performance.

Rahaman, Z. et al [4] A mobile adhoc network (MANET) is formed by a group of wireless mobile hosts or nodes without any fixed infrastructure. As there is no central control in a MANET, a mobile node itself acts as a router. A MANET may function in a stand-alone fashion or may be connected to the Internet. Undoubtedly, MANETs play a critical role in situations where a wired infrastructure is neither available nor easy to install. MANETs are found in applications such as short-term events, battlefield communications and disaster relief activities etc. Therefore, while designing such a network we need to look out for a good Quality of Service (QoS) of it. Many approaches have been proposed for MANET QoS but very few have addressed it from the message transmission point of view. In this paper, we discuss different factors that affect QoS and also the challenges of QoS in MANET.

IV. SECURITY IN NETWORKS

Black Hole Attack

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the 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 [4, 8 and 9].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 [10]. 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 [11].

A Black hole Attack has two properties:

- The node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets.
- The node consumes the intercepted packets.

1.7.1 Black Hole attack on AODV protocol

Black hole attacks in AODV protocol routing level can be classified into two categories: RREQ Black hole attack and RREP Black hole attack.

Black Hole attack caused by RREQ

An attacker can send fake RREQ messages to form Black hole attack [2]. In RREQ Black hole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will be broken down. The attacker can generate Black hole attack by faked RREQ message as follows:

- Set the type field to RREQ (1);
- Set the originator IP address to the originating node's IP address;
- Set the destination IP address to the destination node's IP address;
- Set the source IP address (in the IP header) to a non-existent IP address (Black hole);
- Increase the source sequence number by at least one, or decrease the hop count to 1.

The method how malicious node fits in the data routes varies. Fig. 1.11 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.

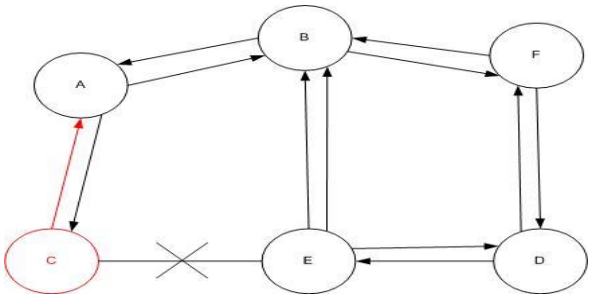


Fig. 1.11 Black Hole is formed by Faked RREQ.

Black Hole attack caused by RREP

The attacker may generate a RREP message to form Black hole as follows:

- Set the type field to RREP (2);
- Set the hop count field to 1;
- Set the originator IP address as the originating node of the route and the destination IP address as the destination node of the route;
- Increase the destination sequence number by at least one;
- Set the source IP address (in the IP header) to a non-existent IP address (Black hole).

The attacker uncast the faked RREP messages to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non-existent node. Then RREP Black hole is formed as it is shown in Fig. 1.12

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 send 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.

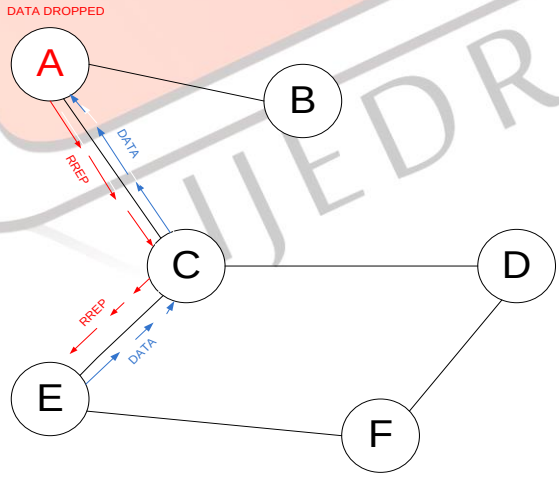


Figure: 1.12 Black Hole is formed by Faked RREP

1.7.2 Black Hole attack on OLSR protocol

A node acting as black hole sends fake HELLO messages. In these messages an attacking node claims to have links to more neighbors than it actually has. Thus, there is a high probability that this node is chosen as an MPR by its neighbor. The more neighbors the attacking node claims to have, the larger the potential impact of the attack. Due to the fake messages of the attacker, in its neighborhood falsified TC messages with too few entries or no TC messages due to an empty MPR selector set are propagated. Thus, the attacker is able to capture routes. Fig 1.14 shows the OLSR network presented in Fig1.13.This time node F has been taken over and acts as black hole. This leads to some changes in the network. In this figure, the lines just show Node A's view of the network is the fake Hello message of the black hole node. It contains nodes A, B, C, D and E. This leads to Node A selecting only the black hole node as MPR. Since Node A does not select nodes B,C as MPRs, these send TC messages not containing Node A . Additionally, instead of sending data packets to nodes D, E via nodes B respectively C, node A tries to send these data packets via the black hole node. Therefore, the black hole has gained control over the connections from A to D and E.

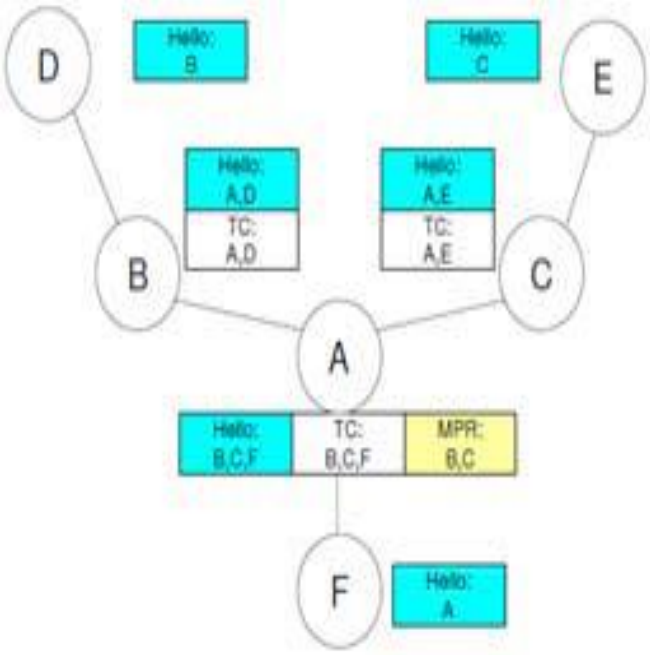


Fig. 1.13 OLSR without Black Hole attack

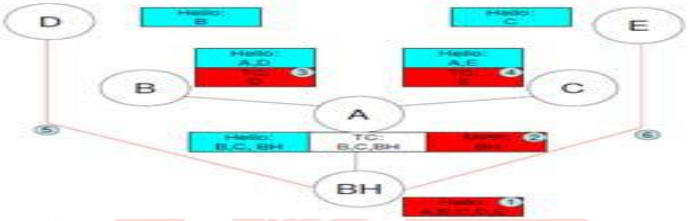


Fig. 1.14 OLSR with Black Hole attack

1.7.3 Black Hole attack on TORA protocol

TORA is hybrid protocol which has the advantages of both Proactive and Reactive protocols. As described in 1.7.2 and 1.7.3 the effect of Black hole on AODV and OLSR respectively. In the same way Black hole affects TORA severely.

In TORA routing protocol firstly it perform like proactive protocols and then reactive protocols. At the when Query packet is send to Neighbors Black hole node may interact in the same way as in the AODV protocol. Neighbors routing table may be updated by Black hole fake path to destination as in the OLSR protocol. Back hole node degrade the performance of routing protocol. It destroys the routing tables made by the nodes. Black hole nodes convince all the nodes which are in its range to update routing tables with its fake path to destination.

In this, way Black hole node attacks on the routing protocols AODV, OLSR and TORA

V. CONCLUSION

In this research paper we are describing To understand the functioning of the black hole node and black hole attack which is easy to launch in wireless ad hoc network. Black hole attack is referred to as a node, dropping all packets and sending bogus information

REFERENCES

[1] Dong-Won Kum, Jin-Su park, You-Ze Cho, Byoung-Yoon Cheon and Daejea Cho., "Proposed an Mobility –Aware Hybrid Routing Approach For Wireless Mesh Network"{ 978-0-7695-4092-4/10 © 2010 IEEE}

[2] Saad Khan, Asad Amir Pirzada And Marius Portmann, "Analysis of Comparison of Reactive Routing Protocols for Hybrid Wireless Mesh Networks"{ 0-7695-2842-2/07 © 2007 IEEE}

[3] Fahim Maan, Nauman Mazhar, "Analysis of Performance of widely used MANET routing protocols DSDV, AODV, OLSR , DYMO and DSR with mobility models"{978-1-4577-1177-0/11/©2011 IEEE}

[4] Rahaman, Z.-" An algorithm to enhance the quality of service in mobile adhoc network", Parallel Distributed and Grid Computing (PDGC), 978-1-4673-2922-4@2012 IEEE.

[5] Amitangshu Pal and Asis Nasipuri, "Analysis of Quality Aware Anycast Routing Protocol For Wireless Mesh Network"{978-1-4244-5638-3/10/©2010 IEEE}

[6] Chen Lijuan, "Research On Routing protocol Applied To Wireless Mesh Network"{ 978-0-7695-3989-8/10© 2010 IEEE}

[7] Mehdi Khabazian and Sonia Aissa, "A Load Distributive QoS Routing Protocol For Multi-Service Wireless Mesh Network"{ 978-1-4244-7742-5/10/©2010 IEEE}

[8] Divya Bansal,Sanjeev Sofat and Gurdit Singh, "An Secure Routing Protocols For Hybrid Wireless Mesh Networks(HWMN)"{ 978-1-4244-9034/10©2010 IEEE}