International Journal of Electrical and Electronics Engineers
Vol. No.7 Issue 02, July-December 2015
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

MANET TECHNOLOGY

Dharna[1], Varsha Saroha[2], R. B. Dubey[3]

[1,2,3]Department of Electronics and Communication Engineering,

Hindu College of Engineering, Sonepat, Haryana,(India)

ABSTRACT

Wireless technology has recently gained more attention in today's world. Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. A mobile ad hoc network is an autonomous collection of mobile devices like laptops, smart phones, sensors, etc. which communicate with each other over wireless links and cooperate in a distributed manner to provide the necessary network functionality in the absence of a fixed infrastructure. This paper provides insight into the potential applications of ad-hoc networks, various attacks and discusses the technological challenges that protocol designers and network developers are faced with.

Keywords: MANET, Wireless Nodes, Ad-Hoc Network, Mobile Nodes, Routes Protocols.

I. INTRODUCTION

As we know science and technology has taken over the world with a storm. We cannot imagine our lives without technologies around us. It has also become a very important part of our lives without which we cannot even think about our survival. Wireless network technology has recently gained more attention in research. MANET is a wireless technology in which it does not support any kind of infrastructure or MANET does not have any type of fixed infrastructure. As MANET does not have fixed infrastructure therefore it has dynamic topology. A MANET network is completely based on a mobile node which is moving continuously. These nodes may be computers or mobile phones. In MANET, computers do the dual role of being a host and a router. It acts as a router to the nodes which cannot transfer or receive direct packets to each other. MANET network uses limited bandwidth. Such networks may be easily deployed and are inexpensive. Due to the absence of any fixed infrastructure support in MANET the nodes in this network are continuously moving and supports dynamic topology.

Fig. 1: Wireless MANET Network

MANET offers many advantages such as ease of establishment, reduced cost for establishment or installation of network, tolerance to faults. MANET was required in the places where there is absence of fixed infrastructure as

infrastructure may not be present in disaster area or war zone, infrastructure may not always be present for short range radio and where the infrastructure is destroyed.

II. APPLICATIONS

MANET is useful in a place of war or battlefield where soldiers, army and tanks need to interact with each other but it can be done in a limited area of bandwidth. MANET can be used for the invigilation of environmental or surrounding conditions. MANET are widely used as a personal network known as Personal Area Network in which number of devices such as laptops and mobiles can be connected using wireless network. MANET are also useful in VANET(Vehicular Ad hoc Network) which is a term used for intelligent communication between the vehicles or intelligent communication for controlling and monitoring the vehicles and also to avoid accidents, traffic jamms. MANET can be used for civilians also such as in the case of cab network, sports stadium and meeting rooms. These networks are also helpful in crisis situation in the country such as an emergency, flooded area, earthquakes for rescuing the people, policing, and fire brigade to interact with the distant devices when the infrastructure is not present.

III. FEATURES

MANET nodes have peer to peer connectivity between themselves, it enables fast establishment of network, and the only requirements for the establishments of network is availability of some nodes. A MANET node can find its nearest node using a service discovery protocol and interact with that node. The range in MANET for connectivity of nodes is only its neighboring nodes. If one node fails it will affect the other node due to the latency in communicating with remote server. MANET nodes can be a laptop, a computer, mobile, handheld pc, smart phones and i-phones.

Routing Protocols in MANET Routing is an integral part in MANET as MANET has not fixed infrastructure since the nodes are continuously moving and the routing in MANET is similar to internet routing but instead of using routing protocols as in case of internet routing MANET uses route discovery & route maintenance protocols. The other difference between MANET and internet routing is network address i. e; in internet routing the network address consists of network ID and computer ID whereas in MANET it consists of only nodes id containing the address. Internet routing is hierarchical while MANET routing is not.

IV. TYPES OF MANET ROUTING ALGORITHMS

Based on applications different types of MANET routing algorithms are:

- Based on information used in building the routing table shortest distance algorithm: This algorithm uses the distance information to build the routing table.
- Link state algorithm: This algorithm first uses connectivity information to build the topology graph and then uses this graph to build the routing table.
- Based on when routing tables are build: In this category, three types are proactive algorithm, reactive algorithm and hybrid algorithm.

4.1 Proactive Algorithm

This algorithm maintains routes to the destination even when the routes are not required or we can say that proactive protocols depends upon maintaining routing tables of known destinations therefore it takes very little or no delay for the route determination but there is also one drawback that as it maintains route for no reason so there may be some route which may never be required or used in other words routing tables must be kept up to date which uses memory any nodes to send updated messages to the neighbors even when no traffic is present the other drawback of the proactive algorithm is that it also consumes bandwidth to maintain routes and also the route repair depends on the frequency of update[1]. Also the proactive algorithm is not suitable for very high dynamic network because the topology changes rapidly and therefore routing tables must be updated which causes increase in control message overhead and can degrade network performance at high loads [2]. On the other hand, the quality of service is guaranteed in relation to the connection set up, this algorithm also has low route latency. Examples of proactive algorithm are Destination Sequenced Distance Vector (DSDV), Wireless Routing Algorithm (WRP), Global State Routing (GSR), Source-tree Adaptive Routing (STAR), Cluster-Head Gateway Switch Routing (CGSR), Topology Broadcast Reverse Path Forwarding (TBRPF), Optimized Link State Routing (OLSR) etc.

4.2 Reactive Algorithm

Reactive protocols maintain routes to destination only when they are required. It uses a route discovery process and flood the network by route request message when a packet needs to be sending to the destination or needs to be routed. Reactive protocols uses packet header to route the destination therefore it does not require routing tables so the memory usage is also very low and very little control traffic. Main advantages are no overhead from periodic update as there is no updating of routing tables; other advantage is it provides scalability as long as there is low traffic and low mobility. The drawback of reactive protocol is high route latency. Examples of reactive protocols are: Dynamic Source Routing (DSR), Ad hoc-On demand distance Vector (AODV), temporally ordered Routing Algorithm (TORA), Associativity-Based Routing (ABR) etc.

4.3 Hybrid Algorithm

Hybrid protocol is a combination of Proactive and reactive algorithm as it combines the features of both the algorithm as it attempts to reduce the control traffic overhead in proactive protocols and also reduced the route discovery delays of reactive protocols as it maintains some of the routing tables. Example of hybrid protocol is Zone Routing Protocol (ZRP).

4.4 Destination Sequence Distance Vector (DSDV)

DSDV is an acronym for Destination sequence distance vector. It is a type of proactive algorithm and it is based upon the Bellman-ford algorithm to calculate the shortest no of hopes to the destination Wired network used routing information protocol (RIP) but it was not successful with the wireless network because of the rapidly changing topology in ad hoc network which can create loops in the network whereas in RIP the nodes exchange its neighbor tables in a regular interval with its neighbor therefore this change moves in the network slowly and slowly. DSDV was a kind of enhancement in this routing information protocol. DSDV uses the idea of sequence number to the distance vector protocols.

Each routing request comes with a sequence no. in the network, now this route request will propagate in the network in many paths so this sequence no assigned to each node will help it in moving towards the right path and destination which automatically avoids the formation of loops. Each node in the network has a routing table which has its next destination or next hop and a sequence no. which is assigned to it by the destination. When the node moves to the next destination it forwards its routing table to its neighbor and its sequence no is incremented. Each route has its sequence no and after increasing this sequence no this no is updated. The route with the largest sequence no is preferred. Then each node advertises for its sequence no and when a route is broken, the sequence no of the route is incremented and then with infinite metric that route is advertised.

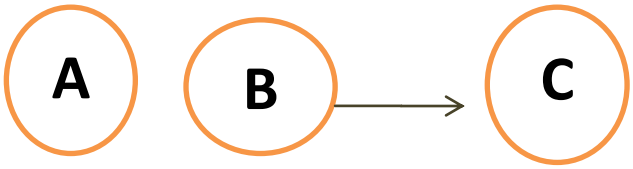


Fig. 2: Route communications

When C receives information about route to A from B:

Let destination sequence number for A at C be S (B) and S(C) sent from B.

If S(C) is greater than S (B) then C ignores the routing information from B.

If S(B) = S(C) and the cost of going through B is smaller than the route known to C then C sets the B as next hop to A.

If S(C) < S(B) , then C sets B as the next hop to A and S(C) is updated to S(B).

Advantages of DSDV are that It is loop free, low memory requirements, and a quick convergence. Its disadvantages are large routing overhead and use of only bidirectional links.

4.5 Dynamic Source Routing (DSR)

It is a type of reactive algorithm and a simple and self-organizing protocol. DSR addresses mobility issues through the use of packet acknowledgment; failure to receive an acknowledgment causes packet to be buffered and route error messages to be sent to all upstream nodes [2]. It is broken into two parts route discovery and route maintenance.

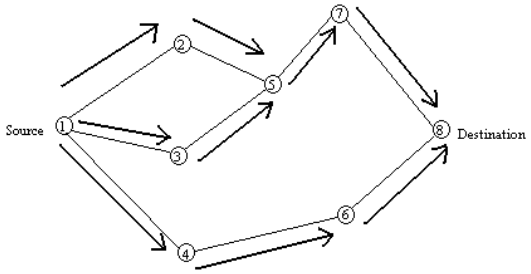
Route maintenance: When a mobile node has a packet to send to some destination, it checks its route cache that whether it has the route to the destination or not if the route cache has the route to destination it send that packet to the destination but on the other hand, if node does not have the route to destination it initiates a route discovery mechanism by broadcasting a route request packet which consists of the address of the destination along with the source node address and a unique identification number[4]. Each node that receives the packet checks that whether it has the route to destination and if it does not contain it adds its own address to the route record of the packet and forward the RREQ to the next hop.

Route Reply: When the destination receives the route RREQ, it sends back a route reply message to the source. If the destination has a route to the source in its route cache, then it can send a route response (RREP) message along this route. Otherwise, the RREP message can be sent along the reverse route back to the source. If an intermediate node has a route to the destination in its cache, then it can append the route to the route record in

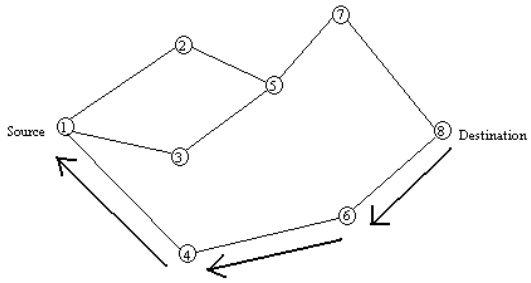
the RREQ, and send an RREP back to the source containing this route. This can help limit flooding of the RREQ.

Route maintenance: When a node detects a broken link while trying to forward a packet to the next hop, it sends a route error (RERR) message back to the source containing the link in error. When an RERR message is received, all routes containing the link in error are deleted at that node.

Advantages of DSR are that routes are being maintained only between those nodes which want to communicate therefore reducing the overhead of route maintenance. Their disadvantage is that packet header size grows with the route length due to source routing.



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

Fig. 3: Different route propagation.

4.6 Ad hoc on Demand Distance Vector Routing (AODV)

AODV is a reactive protocol. AODV utilizes sequence numbers and routing beacons from DSDV but performs route discovery using on-demand route requests (RREQ); the same process as the DSR protocol. AODV is different to DSR in that it uses distance vector routing distance vector means distant nodes; this requires every node in the route to maintain a temporary routing table for the duration of the communication. AODV has improved upon the DSR route request process using an expanding ring search mechanism based upon incrementing time-to-live (TTL) to prevent excessive RREQ flooding [2].

Route Discovery: Whenever a node wants to send a data packet to the destination, the routing table is checked that if it consists of that route or not. If it has the route then the packet is forwarded to the next hop towards the destination otherwise the route discovery mechanism is initiated. AODV uses route discovery and route reply for the route discovery process. The source node will create a RREQ packet containing its IP address, its current sequence number, the destination's IP address, the destination's last sequence number and broadcast ID. If the node has the destination address then that node send a RREP to the source via same path in reverse direction and

the each node sets a forward pointer to each node it receives in RREP form. On other hand, if the node does not have destination then it again rebroadcast the RREQ message to the nodes, and the intermediate nodes discards the duplicate RREQ packets. A larger destination sequence number indicates a more current (or more recent) route. Upon receiving an RREQ or RREP packet, a node updates its routing information to set up the reverse or forward path, respectively, only if the route contained in the RREQ or RREP packet is more current than its own route.

Route Maintenance: When a node detects a broken link while attempting to forward a packet to the next hop, it generates a RERR packet that is sent to all sources using the broken link. The RERR packet erases all routes using the link along the way. If a source receives a RERR packet and a route to the destination is still required, it initiates a new route discovery process. Routes are also deleted from the routing table if they are unused for a certain amount of time.

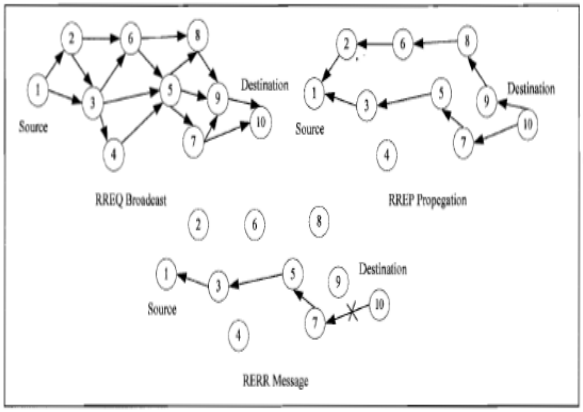


Fig. 4: Nodes propagation in route maintenance.

Advantages of AODV are that it supports the less or least congested route and ignore the shortest route, favors unicast and multicast packet transmission, and does not put overheads on data packet. Its disadvantages are the size of network grows various performance metrics starts decreasing and it is vulnerable to many kinds of attack.

4.7 Cluster-head gateway switch routing (CGSR)

It is a type of proactive protocol. It is a hierarchical routing protocol. When a source provides a route towards the destination the routing table is available at the nodes. A cluster higher in hierarchy sends the packets to the cluster lower in hierarchy. Each cluster can have several daughters. CGSR forms a cluster structure. The algorithm defines a cluster-head, the node used for connection to other clusters. It also defines a gateway node which provides switching (communication) between two or more cluster-heads. There will thus be three types of nodes—internal nodes in a cluster which transmit and receive the messages and packets through a cluster-head, Cluster-head in each cluster such that there is a cluster-head which dynamically schedules the route paths. It controls a group of ad-hoc hosts, monitors broadcasting within the cluster, and forwards the messages to another cluster-head, and Gateway node to carry out transmission and reception of messages and packets between cluster-heads of two clusters. The cluster structure leads to a higher performance of the routing protocol as compared to other protocols because it provides gateway switch-type traffic redirections and clusters provide an effective membership of nodes for connectivity. CGSR works as follow:

i) Periodically, every node sends a hello message containing its ID.

ii) Using these messages, every cluster-head maintains a table containing the IDs of nodes belonging to it and their most recent sequence numbers.

iii) Cluster-heads exchange these tables with each other through gateways; eventually, each node will have an entry in the affiliation table of each cluster-head. This entry shows the node's ID & cluster-head of that node.

iv) Each cluster-head and each gateway maintains a routing table with an entry for every cluster-head that shows the next gateway on the shortest path to that cluster head.

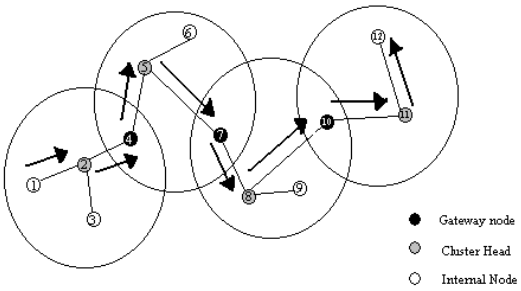


Fig. 5: Nodes Propagation in Cluster-Head Gateway Switches Routing.

Main security issues in MANET are internal attacks, external attacks, denial of service attack, impersonation, eaves dropping, routing attacks, black hole attack, wormhole attack, replay attack
jamming, man in the middle attack and gray hole attack.

V. CONCLUSIONS

Mobile Ad hoc networks are generally more vulnerable to physical security threats than fixed or hardwired networks. This paper throws a light on different concepts of MANETS that can help researchers to the maximum. Its intrinsic flexibility, lack of infrastructure, ease of deployment, auto-configuration, low cost and potential applications makes it an essential part of future pervasive computing environments. As the involvement goes on, especially the need of dense deployment such as battle field and sensor networks, the nodes in ad-hoc networks will be smaller, cheaper, more capable, and come in all forms.

REFERENCES

[1] Elizabeth M. Royer and Santa Barbara Chai-Keong Toh, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, IEEE Personal communications, 1999.

[2] Sunil Taneja and Ashwani Kush, A survey of routing protocols in mobile ad hoc networks, International Journal of Innovation, Management and Technology, vol. 1, no. 3, pp. 279-285, August 2010.

[3] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, A review of routing protocols for mobile ad-hoc networks (MANET), International Journal of Information and Education Technology, vol. 3, no. 1, pp. 1-5, February 2013.

[4] Vikas Kumar, Amit Tyagi and Amit Kumar, Mobile Ad-hoc Network: Characteristics, Applications, Security Issues, Challenges and Attacks, International Journal of Advanced Research in Computer Science and Software Engineering vol. 5, no. 1, pp. 258-262, January 2015.