A study of Mobile Ad-hoc Network-Challenges, Characteristics, Applications and Routing

Dr. V. Harsha Shastri[1], V.Sreeprada[2]

[1]*Department of Computer Science, Loyola Academy Degree and P.G College, Alwal, Telangana, India*

[2]*Department of Computer Science, St. Mary's Centenary Degree and P.G College, Secunderabad, Telangana, India*

Abstract- *In wired networks; we have firewalls and secured gateways as protection mechanism for secure communication. In case of wireless Mobile Ad-hoc networks (MANET), the nodes are self-organizing, infrastructure less, dynamic topology and no centralized authority. Each mobile node is free to move independently in any direction and changes its link to other devices frequently. In this paper, we discuss various vulnerabilities, applications, advantages, and routing protocols in MANET.*

Keywords: *Mobile Ad-hoc Networks, routing protocols, AODV, OLSR, ZRP,*

I. INTRODUCTION

With the emerging mobile technology, wireless communication is becoming popular these days. This is due to the laptops and wireless communication devices such as wireless modems and wireless LANs. There are two main approaches for enabling wireless communication between hosts. First is enabling cellular infrastructure to carry data and voice, but it pose a problem as it is limited to places where the cellular data network exists. Second approach is ad-hoc networking between users to communicate with each other. It is limited in range but has several advantages over cellular network.

A Mobile Ad-hoc Network is a self-organizing mobile network in which each device is free to move independently in any direction and change its links to other devices frequently. They can be deployed on places where there is no infrastructure. Fig 1 demonstrates working of MANET.

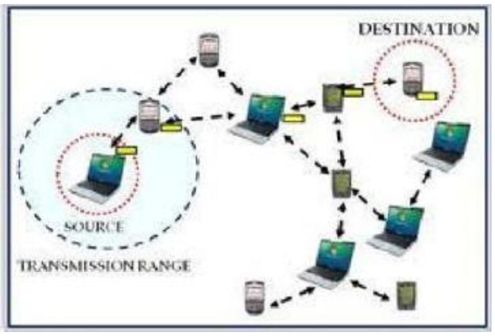

Fig 1 Working of MANET

Fig 2 shows a mobile ad-hoc network with three nodes. Node 1 and Node 3 are not within the range of each other; however, the node 2 can be used to forward packets between node 1 and node 3. Then node 2 acts as a router and these three nodes together form an ad-hoc network.

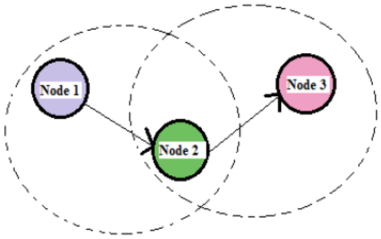

Fig 2 Example of mobile ad-hoc network

A. *MANET Characteristics*

1. Distributed Operations: There is no centralized authority and the control is distributed among the nodes. Each node must cooperate and communicate with each other. The node may implement functions such as routing and security.
2. Multi hop routing: When a node tries to send information to other nodes that is out of the communication range then the packet must be forwarded via intermediate nodes.
3. Autonomous terminal: In MANET, each node is independent and may function as a router and a host.
4. Dynamic topology: Nodes move freely in the network and may change the link to other devices. The nodes dynamically establish routing among themselves as they travel around establishing their own network.
5. Lightweight terminals: The nodes are mobile with less CPU capability, low power storage and less memory size.
6. Shared Physical medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. There is no restriction to access the channel.
7. Heterogeneity: MANET can be formed using variety of devices such as laptops, vehicles, ambulances, mobile phones etc.

B. *Advantages of MANET*

1. They provide access to information and services regardless of geographic position.
2. They do not have centralized control.
3. It is a self-configuring network, where nodes act as routers.
4. Less expensive compared to wired networks.
5. It is scalable as nodes can be added to or removed from the network.
6. The network can be setup at any place and time.
7. Robust due to decentralized administration.

C. *Challenges[1] of MANET*

1. *Limited bandwidth*: Wireless link significantly continues to have lower capacity. The throughput of wireless communication after accounting for the effect of multiple access, fading, noise etc is less than the radio’s maximum transmission rate.
2. *Routing overhead*: Nodes often change their location in the network. Some static routes generated in the routing table leads to unnecessary overhead.
3. *Hidden terminal problems*: It refers to collision of packets at a receiving node due to simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
4. *Battery constraints*: Devices in this network have restrictions on the power source in order to maintain portability, size and weight of the device.
5. *Security threats*: The wireless medium is vulnerable to eaves dropping and the nodes in the network cooperate with each other. MANET are exposed to numerous security attacks.
6. *Packet losses due to transmission errors*: MANET experiences high packet loss due to increased collisions, presence of interference, uni-directional links and frequent path break due to mobility of nodes.

D. *MANET Applications*

Some of the typical applications [1] include:

1. *Military battlefield*: MANET would allow the military to maintain an information network between soldiers, vehicles, and military information headquarters.
2. *Local level*: Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread information among participants at a conference or classrooms.
3. *Personal area network and Bluetooth*: A personal area network is a short range, localized network where nodes are usually associated with a given person. Bluetooth can simplify the inter communication between various nodes such as laptop and mobile phone.
4. *Commercial sector*: Ad-hoc network can be used in rescue/ relief operations such as fire, floods, and earthquake.

II. VULNERABILITIES IN MANET

Vulnerability [1] can be described as a weakness in the security system. A system may be vulnerable to unauthorized data manipulation because the system does not verify user’s identity. MANET is more vulnerable than wired network. The following are the vulnerabilities:

1. *Lack of centralized management*: MANET does not have centralized monitor server. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large-scale ad-hoc network.
2. *Cooperativeness*: Routing algorithm for MANET assumes that the nodes are cooperative and non-malicious. As a result, a malicious attacker can become a routing agent and disrupt the network operation.
3. *No predefined boundary*: We cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment as the nodes join and leave the network. As soon as the adversary comes in the radio range of a node it will be able to communicate with that node.
4. *Adversary inside the network*: The mobile nodes within the MANET can freely join and leave the network. The nodes may also behave maliciously. This is hard to detect that the behaviour of the node is malicious.
5. *Limited power supply*: The nodes in the MANET need to consider restricted power supply. The nodes may behave in a selfish manner where it is finding that there is only limited power supply.

III. ROUTING IN MANET

Ad-Hoc routing protocols are commonly divided into three main classes; Proactive, reactive and Hybrid protocols. The fig 3 shows the routing protocols [4].

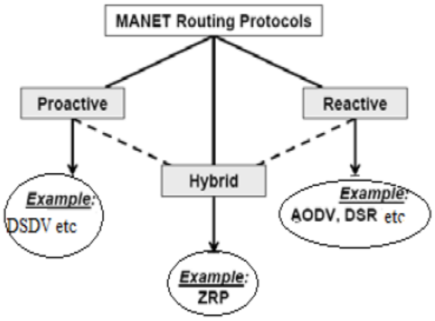

Fig 3 Routing protocols in MANET

1. **Proactive protocols**: It is also known as table driven protocols. They maintain the routing table of entire network constantly. Each node has to maintain one or more tables to store routing information and response to changes in network topology by broadcasting and propagating. The routing tables are updated constantly whenever the network topology changes in order to have a consistent view. Each node in the network sends a broadcast message to the entire network if there is any change in the network topology. This leads to maintenance of the routing table because the entries must be updated and must provide the actual information of the entire network. For a large network, proactive routing protocols are not recommended as it leads to overloading of the routing table and more bandwidth consumption. Examples are DV (distance vector) , DSDV(Destination sequenced distance vector), OLSR (optimal link state routing) and WRP (wireless routing protocol).

1.1 OLSR (Optimized link state routing)

OLSR [12] protocol performs hop-by-hop routing; that is, each node in the network uses its most recent information to route a packet. Hence, even when a node is moving, its packets can be successfully delivered to it. The routing can be optimized in two ways: OLSR reduces the size of the control packets for a particular node by declaring only a subset of links with the node's neighbors who are its multipoint relay selectors, instead of all links in the network. Secondly, it minimizes flooding of the control traffic by using only the selected nodes, called multipoint relays to disseminate information in the network. As only multipoint relays of a node can retransmit its broadcast messages, this protocol significantly reduces the number of re-transmissions in a flooding or broadcast procedure.

1.2 DSDV (Dynamic Destination- Sequenced Distance Vector Routing)

DSDV [8] is developed on the basis of Bellman–Ford routing [9] algorithm with some modifications. Each mobile node in the network keeps a routing table that contains a list of all available destinations and the number of hops to each. Each table entry is tagged with a sequence number, which is originated by the destination node. Periodic transmissions of updates of the routing tables help maintaining the topology information of the network. If there is any new significant change for the routing information, the updates are transmitted immediately. So, the routing information updates might either be periodic or event-driven. DSDV protocol requires each mobile node in the network to advertise its own routing table to its current neighbors. The advertisement is done either by broadcasting or by multicasting. Through advertisements, the neighbouring nodes can know about any change that has occurred in the network due to the movements of nodes. The routing updates could be sent in two ways: one is called a ''full dump'' and another is ''incremental.'' In case of full dump, the entire routing table is sent to the neighbors, where as in case of incremental update, only the entries that require changes are sent.

2. **Reactive protocols**: It is also known as on-demand routing protocols. They maintain or discover routes only on demand. A control message is flooded to the routes to discover the appropriate route. A route is established only when a node in the network wants to send a message to another node in the network. It has an advantage because the routing table is not overloaded but there is long delay in establishing the route. Examples are DSR (Dynamic source routing), AODV (Ad-hoc on demand distance vector routing), LAR (location aided routing) and TORA (temporally ordered routing algorithm).

2.1 AODV (Ad-hoc On Demand Distance Vector) [6]

It establishes a route only on demand. It is capable of uncast, broadcast and multicast routing. It uses sequence numbers on route updates. It reacts quickly to the topological changes and updates only those hosts that may be affected by the change using RREQ message. The RREQ and RREP messages are responsible for route discovery. The fig 4 shows routing in AODV.

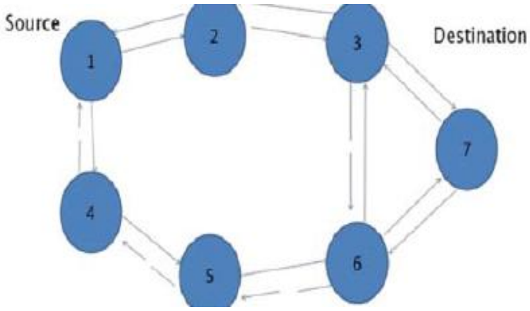

Fig 4 Routing in AODV

Advantages:

1. Does not require any inner organizational method to handle routing process.
2. Establishes route on demand and destination sequence numbers are applied to find the latest route to the destination.
3. Connection set up delay is lower.
4. Loop free and avoid counting to infinity problem.

5. At most one route per destination maintained at each node.

Disadvantages:

1. Leads to heavy control overhead.
2. Unnecessary bandwidth consumption.

2.2 TORA (Temporarily Ordered Routing Algorithm)

It is a reactive routing protocol where link between nodes is established creating using Directed Acyclic Graph (DAG) of the route from the source node to the destination. It uses link reversal model in route discovery. A route discovery query is broadcasted and propagated throughout the network until it reaches the destination or a node that has information about how to reach the destination. A parameter Height is defined as a measure of the distance of the responding node's distance up to the required destination node. In the route discovery phase, this parameter is returned to the querying node. As the query response propagates back, each intermediate node updates its TORA table with the route and height to the destination node. The source node then uses the height to select the best route toward the destination. This protocol has an interesting property that it frequently chooses the most convenient route, rather than the shortest route. For all these attempts, TORA tries to minimize the routing management traffic overhead.

3. **Hybrid protocols**: It is a combination of reactive and proactive routing protocols. It is basically used to overcome the disadvantages of both routing protocols. It uses the route discovery and on demand mechanism of reactive routing protocol and the routing table management mechanism of proactive routing protocol. A large network is divided into zones. The routing within zones is done by using proactive approach and the routing outside the zone done by using reactive approach.

3.1 ZRP

It was planned to decrease the control overhead of proactive routing protocols and discovery in reactive routing protocols and also decrease the latency by route. ZRP consists of several components, which work independently to give efficient result. Components of ZRP are:

a) IARP: Intra zone routing protocol- It is used to communicate with the interior node inside the zone. If the topology changes, the node rapidly changes. It is only for local route.

b) IERP: Inter zone routing protocol- it is a global reactive component. Uses reactive approach to communicate with nodes outside the zone. It changes the way the route discovery handles.

c) BRP: Broader cast routing protocol- it is used to direct route request initiated by global reactive IERP. It is used to maximize efficiency and increased disused queries.

Table 1: Comparison of routing protocols

Parameters	**Reactive Protocol**	**Proactive Protocol**	**Hybrid Protocol**
Routing Philosophy	Flat	Flat / Hierarchical	Hierarchical
Routing Scheme	On demand	Table Driven	Both
Routing Overhead	Low	High	Medium
Latency	High due to flooding	Low due to routing tables	Inside zone low outside similar to reactive protocols
Scalability level	Not suitable for large networks	Low	Designed for large networks

IV. CONCLUSION

In this paper, we discuss MANET and its characteristics, challenges, applications and vulnerabilities. We have also classified routing protocols into three classes as proactive, reactive and hybrid. We understood the comparison of the routing protocols.

V. FUTURE ENCHANCEMENT

Due to the dynamic topology, distributed operation and limited bandwidth, MANET is vulnerable to attacks. Different types of parameters and security mechanism need to be developed to prevent routing protocols from different types of attacks.

ACKNOWLEDGMENT

The authors would like to express their sincere thanks to the organization for their constant support and motivation. We would like to thank our colleagues for their support without which the article would be incomplete.

REFERENCES

[1] Priyanka Goyal, Vinti Parmar, Rahul Rishi " *MANET: Vulnerabilities, Challenges, Attacks, Application*" in proceedings of IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[2] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani "*A Survey of Secure Mobile Ad Hoc Routing Protocols*" in proceedings of IEEE communications surveys & tutorials, vol. 10, no. 4, fourth quarter 2008.

[3] Yau P.-W., Mitchell C.J., "*Security Vulnerabilities in Ad Hoc Networks*", In Proc. of the 7th Int. Symp. on Communications Theory and Applications, pp. 99-104, 2003.

[4] HumayunBakht, " *Survey of Routing Protocols for Mobile Ad-hoc Network*", International Journal of Information and Communication Technology Research, 258-270, October 2011.

[5] Mohit Kumar and Rashmi Mishra "*An Overview of MANET: History, Challenges and Applications*" , Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[6] C. Perkins, E. Belding-Royer and S. Das, "*Ad-Hoc On-Demand Distance Vector (AODV) Routing*", RFC3561, July 2003

[7] Naveen Bilandi and Harsh K Verma "*Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET*" International Journal of Electronics and Computer Science Engineering 1660 ISSN- 2277-1956.

[8] Perkins CE, Bhagwat P (1994) *Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers*. Proceedings of ACM SIGCOMM 1994:234–244.

[9] Cheng C, Riley R, Kumar SPR, Garcia-Luna-Aceves JJ (1989) *A Loop-Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect. ACM SIGCOMM Computer Communications Review*, Volume 19, Issue 4:224–236