© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

# An Analysis on Characteristics, Challenging Issues and Comparisons of Routing Protocols of MANET

**Gurucharan Banerjee*, Anjani Kumari, Arvind Thakur, Komal Kumari, Jitendra Parit**
Department of Computer Science and Engineering, BITM, Shantiniketan, West Bengal, India

## ABSTRACT

As the popularity of mobile device and wireless networks significantly increase over the past few years, wireless ad-hoc networks has now become one of the most vibrant and active field of communications of networks. Due to serve challenges the special features of MANET bring the technology great opportunities together. Our project describes fundamental problems of ad-hoc network by giving its related research background including the concept, features, status and vulnerabilities of MANET.

**Keywords:** Network, Ad-hoc, MANET, Protocol, DSR, AODV

## I. INTRODUCTION

MANET is new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network. Like in a cellular network, users are connected through base station and backbone networks. Users mobility is limited within a range of base station. In ad-hoc network communicating devices can form arbitrary networks "on the fly" to exchange information without the need of pre-existing network. A mobile ad-hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors etc) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide necessary functionality in absence of a fixed infrastructure. This type of network, operating as a standalone network or with one or multiple points of attachment to cellular networks or to the internet, paves the way to numerous way and exciting applications. Applications include: emergency and rescue operations, conference or campus settings, personal networking etc

## II. METHODS AND MATERIAL

### A. Characteristics

1) Dynamic Topology: Nodes are free to move arbitrarily with different speeds, thus the network topology may change randomly and at unpredictable time. The nodes in MANET dynamically establish routing among themselves as they travel around, establishing their own network.
2) Distributed Operation: There is no network for central support, the control of network is distributed among nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node act as a relay as needed, to implement specific functions such as routing and security.
3) Multi routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.
4) Autonomous Terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.
5) Light Weight Terminal: In maximum cases, nodes in a MANET are mobile with less CPU capability, low power storage and small memory size.

### B. Vulnerabilities

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify

a user's identity before allowing data access. MANET is more vulnerable than wired networks.

1) Lack of centralized management: MANET doesn't have a 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) Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such a changing environment as well as protection against specific threats and attacks, leads to the development of various security schemes and architectures.

3) Scalability: Due to mobility of nodes, scale of ad hoc network changing all the time.So, scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

4) Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are non-malicious and cooperative. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specification.

5) Dynamic topology: Nodes are free to move arbitrarily with different speeds, thus the network topology may change randomly and at unpredictable time. The nodes in MANET dynamically establish routing among themselves as they travel around, establishing their own network.

### C. Attacks in MANET

Absence of any central coordination mechanism and shared wireless medium makes MANET more vulnerable to digital /cyber-attacks than wired network. There are two types of attacks-

1) External attacks: External attacks are carried out by nodes that do not belong to the network. It causes congestion, sends false routing information are causes unavailability of services.

2) Internal attacks: Internal attacks are from compromise nodes that are part of the network .In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node.

### D. MANET Challenges

Regardless of the attractive application,the features of MANET introduce several challenges.Securing wireless ad hoc networks is a highly challenging issue.Understanding possible form of attacks is always the first step towards developing good security solutions. Regardless of attractive applications,the feature of MANET introduces several challenges.

1) Routing: Since the topology of the network is constantly changing,the issues of routing packets between any pair of nodes becomes a challenging issues.Most protocols should be based on reactive instead of proactive.Multicast routing is another challenge because the multicast tree is no longer static due to random movement of nodes within the network.

2) Dynamic challenges: Nodes are free to move arbitrarily thus,the network topology which is typically multi.hop may change randomly and rapidly at unpredictable times and may consist of both bidirectional and unidirectional links.

3) Power constrained and operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy.For these nodes,the most important system design criteria for optimization may be energy conservation.For most of the light weighted mobile-terminals,the communication related functions should be optimized for lean power consumption.Conservation of power and power aware routing must be taken into consideration.

4) Security and vulnerability: In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to nasty neighbour relaying packets. The feature of distributed operation requires different schemes of authentication and key management ,Further wireless link characteristics introduce also reliability problems because of the limited wireless transmission range, the broadcast nature of the wireless medium, mobility induced packet losses and data transmission errors. The increased possibility of spoofing and denial of service attack should be carefully considered.

5) Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. Network's ability to provide QoS depends on the intrinsic characteristics of all the network components, from transmission links to MAC and network layers. MANET characteristics generally lead to the conclusion that this type of network provides a

weak support to QoS. Wireless links have a low reliability and highly dynamic with frequent links breakages. Random-access based MAC protocols, which are commonly used in this environment, have no QoS support.

## III. RESULTS AND DISCUSSION

**Routing Protocols**

The classification of MANET routing protocols, depending on how the protocols are handle the packet to deliver from source to destination. Due to their functionality of routing protocols are broadly classified into three types such as Reactive, Proactive and Hybrid protocols.

1) Proactive protocol: These types of protocols are called the table driven routing protocols in which, all the route information is maintained in routing table. The packets are transferred over the network in manner of specified and predefined route in the routing table. In this method, the packet forwarding is done faster but the routing overhead is greater because all the routes have to be defined before transmitting the data and control packets. Table driven protocols lower intermission because all the routes are maintained at all the times. Example- DSDV, OLSR (optimized link state routing).

2) Reactive protocols: This network maintains only the routes that are currently in use, so reducing the burden on the network when only a few of all available routes is in use at any time .These type of protocols are called as On Demand Routing Protocols where the routes are not before discovery phase to determine a new route whenever a transmission is necessary. This routes discovery mechanism is based on flooding algorithm which employs on the technique that a node just broadcasts the packets to all of its neighbours and intermediate nodes just forward that pocket to nearly nodes. This is a respective technique until it reaches the destination.

Ex-Protocols: DSR, AODV.

3) Hybrid protocols: The hybrid protocols are the combine of reactive and proactive routing protocols and take the advantage of these protocols and as a result routes are found quickly in the routing zone. Ex-ZRP (Zone Routing Protocol).

Destination Sequenced Distance Vector (DSDV): DSDV table driven routing scheme for ad-hoc mobile networks based on the Bellman-ford algorithm. The improvement made to the Bellman-ford algorithm includes freedom from loops in routing table by using sequence numbers. Each node acts as a router where the routing table is maintained and periodic routing updates are transferred, even if the routes are not necessary. A sequence number is associated with each route or path to the destination to prevent the routing loops .The routing updates are exchanged even if network is idle which uses battery and network bandwidth. So, it is not preferable for highly dynamic networks.

Ad hoc On-Demand Distance Vector Routing (AODV): AODV is an On-Demand protocol which is confluence of DSDV and DSR. Route calculated on demand, just as it is in DSR via route discovery process. On the other hand, AODV maintains a routing table where it maintains one entry per destination unlike the DSR that maintain multiple route cache entries for each target. AODV provides loops free routes while repairing link breakages but, DSDV doesn't require global periodic routing advertisements.

Dynamic Source Routing (DSR): DSR is pure on-demand routing protocols, where the routes are calculated only when it is necessary. It is designated for use of multi-hop adhoc networks of mobile nodes. DSR allows the network to be self-organized and self-configured without any central administration and network setup .It uses no periodic message like ADOV, thus bandwidth overhead and conversed battery power and also huge routing updates. It need only the efforts from the MAC layer to identify the link failure's uses source routing where the whole routes is carried as an overhead . In DSR, the whole routes is carried with the message as an overhead where as in ADOV, the routing table is maintained thus it is not requires to send the whole routes with the message during the Routing discovery process.

## IV. CONCLUSION

The future of ad-hoc networks is really appealing, giving the vision of "anywhere, anytime" and cheap communication. Due to dynamic topology, distributed operation limited bandwidth MANET is more vulnerable to many attacks. At present, general trend in MANET is

towards mesh architecture .Improvement in bandwidth and capacity is required which implies need for a higher frequency. In our project we will discuss MANET and its characteristics, goals, application, various types of attacks in routing protocols and vulnerabilities.

## V. REFERENCES


[1] *"Study of MANET: Characteristics, Challenges, Application and Security Attacks"* by Aarti and Dr S.S Tyagi , International Journal of Advanced Research in Computer Science and Software Engineering, volume 3,May 2013.

[2] *"MANET:Vulnerabilities,challenges,attacks,application of MANET"* by Rahul Rishi,Vinti Parmar,Rahul Rishi from International Journal of Computational Engineering and Management, Volume 11, January 2011.

[3] *"An overview of MANET History, Challenges and Applications"*, by Mohit Kumar and Rashmi Mishra ,Indian journal of Computer Science and Engineering, volume 3,February 2012.

[4] 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, 279-285, August 2010.

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

[6] Gagandeep, Aashima and Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack". International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012.