MANET: OVERVIEW, ISSUES, ROUTING ALORITHM AND STRATEGIES

Mr.N.B.Kadu[1]
[1] *Asst.Prof, Computer Engineering, P.R.E.C.Loni, Maharashtra, India*

ABSTRACT

Wireless network is type of network which uses the available radio frequencies to transmit data from one node to another. In wireless network the communication between the nodes does not relies on any physical cables to transfer data. A MANET (Mobile Ad-hoc Network) is an autonomous, self-governing decentralized dynamic network which composes of all the mobile nodes transmitting data on wireless transmission link. In MANET all nodes are moving in arbitrary directions and works as router to every other mobile node. As the MANET is dynamic in nature any node can be added or deleted automatically whenever needed. Nodes that lie within each other's range can discover each other and communicate by transmitting data packet. As the nodes in MANET are mobile and hence it is very much difficult and problematic to find out the direct path between two end nodes. This paper provides the final ultimate solution for finding transmission path between nodes. This paper present a various types of routing algorithms such as Proactive, Reactive, Hybrid routing Algorithms and also its sub types such as termite, AODV, DSDV, OLSR, DSR, LAR, ZRP.

Keyword : - *MANET (Mobile Ad-hoc Network), wireless network, Proactive, Reactive, Hybrid Routing algorithms, TAODV, DSDV, OLSR, AODV, DSR, LAR, ZRP.*

1. INTRODUCTION

Today's Wireless Network are most popular network. There are two types wireless network based on Infrastructure's Network:

1. Infrastructure Networks

2. Infrastructure-less Networks

1.1 Infrastructure Networks

An Infrastructure Networks contain special nodes called access points via existing networks. The other wireless nodes known as mobile stations communicate via AP's. The APs can also work as bridges with other networks. The node within the network find the nearer base station which is connected to it and try's to communicate with it.

1.2 Infrastructure-less Networks

Infrastructure-less Network have dynamic structure. They can be building up at any place. It is peer-to-peer network without any centralized server. It is group of various mobile stations within range of each other dynamically configuring into a temporary network.[1].Mobile Ad-Hoc Networks (MANETs) is one of the type of infrastructure less networks. Wireless MANETs are characterized as networks without physical network. In such type of network there is no fixed topology due to the mobility of nodes, interference, multipath propagation and loss of path. In ad hoc networks the mobile nodes create their routes between one node to another node in wireless network shown in Fig 1.2.[2].Thus a dynamic routing protocol is needed for these networks to function properly. Many Routing protocols have been developed for accomplishing this task. The purpose of this is to study, understand, analyses and discuss two mobile ad-hoc routing protocols are as follow:

2. PROTOCOLS

2.1Proactive Protocols

The first one is a proactive protocol depending on routing tables which are thus maintained at every mobile node. Exchange topology information with other nodes of the network regularly. The Advantage of proactive protocol algorithm is best suited for highly mobile ad-hoc network, low latency when establishing and easy to implement

QoS. Disadvantage of proactive protocol algorithm is not well suited for large network and overhead to maintain routes to all destinations.[3].Examples of Proactive Routing Protocols are:
1) Hierarchical State Routing (HSR)
2) Global State Routing (GSR)
3) Destination Sequenced Distance Vector Routing (DSDV).

2.2 Reactive Protocols

The other one is a reactive protocol, which finds a route to a destination on demand, whenever communication is needed. Reactive protocol is suited for general Ad-hoc networks. Advantage of reactive protocol algorithm is it requires less bandwidth, low storage and message overhead. Disadvantage of reactive protocol algorithm is application latency is increased, high latency when establishing new routes and difficult to implement QoS.[4].
Examples of reactive protocols are:
1) Dynamic Source Routing (DSR).
2) Ad hoc on-demand Distance Vector Routing (AODV).
3) Temporally Ordered Routing Algorithm (TORA).
4) Location Aided Routing (LAR).

3. RELATED WORK

A mobile ad hoc network (MANET) is a frequently recurring self-configuring, infrastructure-less network of mobile devices. It is connected without wires. Each device in a MANET is free to move self-governing in any direction, and will change its links to other devices self-governing. Each must forward traffic not connected to its own use, and therefore frequently recurring to be a router. The primary challenge in building a MANET understands each device to maintain the information required to conduct route traffic. Such networks connected to the larger Internet. They may contain one or more and different transceivers between nodes. This results is a highly dynamic, autonomous topology environment on top of a Link Layer ad hoc network.

MANET is a kind of Wireless ad hoc network that frequent has a routable networking. MANET consists of a peer-to-peer, self-forming, self-healing network. MANET is nearly 2000-2015 communicate at wireless radio frequencies (30 MHz -5 GHz). The growth of laptops and 802.11/Wi-Fi wireless networking have made of MANET is a connected with research topic since the mid-1990s. Many papers evaluated protocols and their abilities, assuming to be different in degrees of mobility within a bounded space, usually with all nodes with a few hops of each other. Different protocols are then evaluated based on amount of the packet drop rate, they introduced by the routing protocol, source-to-destination packet delays, network throughput, ability to scale, etc.

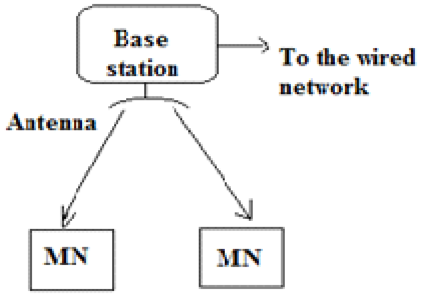

Fig1.1 Infrastructured Networks

Fig 1.1: Infrastructure Networks

4. ISSUES IN DESIGN OF MANET

Mobile Ad-hoc Network is autonomous and very dynamic in nature and there is no any fixed infrastructure in these type of network. Hence there are various issues in designing to this, so all issues in designing Mobile Ad-hoc Networks using a routing protocol are explain as below:

A. Error-prone channel state:

The Properties of the transmission links in a wireless network typically changes, and this gives rise for an interaction between the routing protocol, if needed, find alternate routes.[1].

B. Exposed Station Problem:

Consider previous figure, but along with an additional node A only in the range of node Z. Now, suppose node Y communicates with node X, and node Z wants to transmit a packet to node A. At the same instance when the node Y transmits data packet node X, node Z recognizes the channel busy. Node Z falsely concludes that it cannot send the data packet to node A, even though both the transmissions (i.e., between node Y and node X, and between node Z and node A) would be successful. Faulty reception would just occur in the region between node Y and node Z, where none of the receivers is situated. This problem is often referred to as “The exposed terminal problem”. This two problems Hidden station problem and exposed station problem leads to cause of significant reduction of network performance when the traffic load is high.[1]

C. Bandwidth-constrained

Wireless links will have ultimately lower capacity than their physical hardwired. Additionally, to realized performance of wireless communications after taking in accounts the effects of multiple access, fading of signals, noise, and interference conditions etc. is often much low in quantity than a radio's maximum transmission rate. One effect is congestion which is the special achievement rather than the exception, i.e. Aggregate application demand will likely to exceed network capacity on the frequent basis. As the MANET is often simply an extension of the field network infrastructure, mobile ad hoc users will demand same functionalities. These demands will further on continuously goes on increasing as multimedia computing and networking applications rise.[1]

D. Security Issues:

MANET is generally more prone to security threats than are in physical cable. The increased possibility of spoofing, denial-of-service attacks, eavesdropping, must be carefully taken into consideration. Already existing link security techniques are generally applied within wireless networks to reduce security threats. Snooping is activity where one person try to get unauthorized access to another person's data. It is likely to be similar to the activity of eavesdropping but not necessarily up to the limit for gaining access to data during its transmission. Snooping can include various activities such as normal glance at an e-mail that appears on any person's computer screen or watching what anyone is typing. Most sophisticated type snooping uses various types of software programs to monitor activity on a computer or network device remotely. In network layer wormhole attack, a malicious node receives packets at one location in the network and redirects them to different location in the network, where these packets are resent into the network.

This redirect between two colluding attackers is termed to as a wormhole. It could be established through the physical wired cable between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast behavior of the radio channel. In Black hole attack, an attacker uses the routing protocol to advertise itself of having the shortest path to the node whose packets it wants to intercept. An attacker recognizes the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an ultimately shortest route. If the malicious reply reaches the initiating.

E. Hidden Station Problem:

Node X and node Z are in range of node Y for communication, but not with each other. In the scenario the both try to communicate with node Y at the same time, X and Z might not recognize any interference on the wireless medium. Hence, the signals get collided at node Y, this cause of collision will be unable the node Y to receive the transmissions from node either node X or node Z. The typical solution for this well-known problem so-called “Hidden station” problem is that the nodes must 3 Synchronize transmissions between themselves by asking and permitting to send and receive data frames.. This scheme is called as RTS/CTS (Request To Send/Clear To Send).The basic notation behind this to detect the channel by informing other nodes about an next fore-coming transmission. This can be implemented by allowing the receiving node to broadcast a short frame so that other nearby nodes can recognize that a transmission is going to take place. The nearby nodes are then expected to take halt in transmitting data frames for the duration of the fore-coming data frame.[2] Fig.3.1.Hidden problem using three nodes.

5. PROACTIVE TYPES

5.1 OSPF (Open shortest path first)

In 2004 the Internet engineering task force(IETF) Hales two protocols as follow-
Overlapping Relay by Madhavi Chandra by point to point link neighbor's route LSA identify neighbor's adjacent neighbors.

5.2 DSDV (Destination sequence distance vector)

It is table driver protocol. In 1994 Perkins and P. Bhagwat were invented to solve routing loop problem i.e. nothing but control constant traffic and are available all time.

6. SECURITY

In MANET Security following factors may affects confidentiality, integrity, availability and often and authentication and non-repudiation.
1. Confidentiality-It is related to data privacy which is relevant to normally attained via cryptographic mechanism. Like, Symmetric key stream, block cipher.
2. Integrity-It is used for protect against the tampering of data .which is achieved by message authentication code (MACs) or by one-way hash function.
3. Authentication–It is nothing but origin integrity called as special integrity class.
4. Availability-When services are need then are ensured.
5. Non-repudiation-It is related to safeguard

7. STRATEGIES

It is nothing but stepwise execution.
A. Proactive routing algorithm-
Advantages:-
1. Connection time fast.
Disadvantages:-
2. Continuously uses source.
B. DSDV-Destination sequence distance vector-
With every entry maintain the node at destination node.
Advantages:-
1. Route is always available i.e. each node having path from other node.
Disadvantages:-
1. Larger routing overhead.
C. OLSR-optimized link state routing protocol-
Advantages:-
1. Minimize control information.
2. Broadcast traffic efficiently minimizes.
Disadvantages:-
1. Every route involves forwarding through a MPR node so, no necessary of shortest path.
D. Reactive Algorithm:
1. AODV-Ad-hoc demand distance vector.
Advantages:-
1. On demand it creates routes which reduce periodic control message.
Disadvantages:-
1. Loss in high mobility scenario.
2. DSR-(Dynamic source routing algorithm)
Advantages:-
1. Can't flood the network with table update message periodically.

2. Intermediate nodes are also used.
Disadvantages:-
1. Doesn’t repair locally broken links by using route maintenance mechanism.
2. Delay in connection setup.
E. Hybrid routing algorithm-
It is combines advantage of both reactive and proactive protocol.
Advantages:-
1. Minimize scope of route request flood.
2. Minimize overhead of route discovery.
F. LAR-Location aided routing.
Based on limited flooding used to reduce number of numbers.
Disadvantages:-
1. Physical location of nodes needs to know.
G. ZRP -Zone routing protocol.
It is used to minimize control of overhead of proactive routing protocol and also decrease latency.
Advantages:-
1. Less control overhead on demand protocol.
Disadvantages:-
1. Having shortest latency for finding new route.

8. CONCLUSIONS

This paper is about algorithm, routing, security, protocol of MANET. Due to have mobility in MANET network topology changes frequently and also in this paper various different viewpoints of protocols are discussed. And all survey concludes that MANET is most useful infrastructure for achieving future ubiquitous society’s well as creating and enlarging scope of emerging pervasive technologies.

9. REFERENCES

[1]Kenneth Holter, “Wireless Extensions to OSPF: Implementation of the Overlapping Relays Proposal", Master thesis, Department of Informatics, University of Oslo, Norway, 2nd May
[2]Vijay Kumar and Ashwani Kush. “A New Schemefor Secured on Demand Routing” IISTE Network
and Complex Systems ,Vol 2, No.2, 2012.ISSN2224-610X (Paper), 2225-0603 (Online).
[3]S. Corson& J. Macker “Mobile Ad hocNetworking: Routing Protocol Performance Issues
and Evaluation Considerations”, RFC 2501, Oct.1999.
[4]DonatasSumyla, Mobile Ad-hoc Networks,03/20/2006.
[5]Poongothai T. and Jayarajan K., “A non-cooperative game approach for intrusion detection in Mobile Adhoc networks”, International conference of computing, communication and networking (ICCC), 18-20 Dec 2008, St. Thomas, VI, pp 1-4.
[6]DjamelDjenouri and LyesKhelladi, “A survey of security issues in mobile ad hoc and sensor network”, IEEE communications Surveys and Tutorials journal,Volume 7, Number 4, 2005, pp 2-29.
[7]PadminiMisra, “Routing Protocols for ad hoc mobile wirelessNetworks”, Nov-1999
[8] Mario Joa-Ng, “A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks”, IEEE Journal on selected areas in communications, Vol. 17, No. 8, Aug-1999.
[9]Sunil Taneja&Ashwani Kush“PERFORMANCE EVALUATION OF DSR AND AODV OVER UDP AND TCP CONNECTIONS” International Journal of Computing and Business Research (IJCBR), Volume 1, No. 1 December . 2010
[10]DonatasSumyla, Mobile Ad-hoc Networks, 03/20/2006.http://ecom.umfk.maine.edu/MMobile%20Ad.pdf
[11] P. Jacquet,P. Muhlethaler,T. Clausen,A. Laouiti,A. Qayyum,L. Viennot“Optimized link state routing protocol for ad-hoc networks” in International Multi Topic Conference 2001(IEEE),Dec. 2001. Avaible: http://menetou.inria.fr/~muhletha/olsr.pdf