A Study of Routing Protocols in Mobile Ad-HOC Network

Sanket Singh[1]*, Dr. Ashish Baiswar[2]

[1] Research Scholar, Shri Krishna University, Chhatarpur M.P.

[2] Associate Professor, Shri Krishna University, Chhatarpur M.P.

Abstract - A wireless ad hoc network made up of mobile devices is referred to as a "Mobile Ad Hoc Network." The phrase "for this reason" in Latin is ad hoc. Another way to put it is to state that an "ad-hoc" network is one that lacks a centralized management system or established architecture. A group of wireless mobile hosts that establish a temporary network without any centralized management or infrastructure is known as an ad hoc network. Various routing algorithms have been suggested and implemented to help with this job. As a result, it might be challenging to decide which protocol operates best in a variety of settings. This study reviews the usual representations of routing protocols created for mobile ad hoc networks.

Keyword - Routing protocols, MANET

----------------------------------X----------------------------------

INTRODUCTION

A mobile ad hoc network, or MANET, is an infrastructure consisting mostly of wireless mobile devices that is automatically optimized in real time. In Latin, ad hoc means "for this reason." Without the need for or ability to centrally operate preexisting 5 networks, remote ad hoc networking is made up of a dispersed set of mobile Wi-Fi nodes arranged in a complicated topology. Each node in a mobile ad-hoc network acts as both an end system and a router for other networks, making the network itself autonomous. By spontaneously forming and operating in ad hoc and fleeting topologies, nodes will let people and devices to communicate with one another without the need for prior communication planning. In an ad hoc network setting at the connection layer, MANETs are ad hoc Wi-Fi networks. In contrast to the centrally controlled mesh network, mobile ad hoc networks consist of the self-healing point-to-point network.

In most cases, the routing protocols used in such networks make it easier for nodes to communicate with one another. Different types of MANET protocols exist. Among protocols, the least power routing method is a special case. It picks a route that minimizes overall energy consumption between the source and the destination. The group's lack of patience is shown in its tendency to choose control strategies with the shortest time until expiration. The addition of a second group requires more network time. The transmission charge is spread in many different directions. To do this, we may put some of the nodes in charge of transmission to bed at odd hours. This helps maintain a steady flow of data across the MANET and extends the networks' useful lifespan. Several reactive protocols have been proposed to ensure the success of MANETs.[1]

Mobile Ad Hoc Networks

"Mobile Ad Hoc Network" is a self-configuring wireless ad hoc network made up of mobile devices (MANET). Latin "for this reason" is an ad-hoc expression. Another way to describe it is to say that a "ad-hoc" network refers to one that has no established infrastructure or central control. Ad-hoc mobile networks are self-contained networks in which each node may act as both an end system and a router for its neighboring nodes. Network topologies may be formed by self-organizing and co-operating nodes, allowing users and devices to communicate without the need for pre-planning. For the most part, MANETs are Wireless Ad Hoc Networks with Routable Networking Environments rather than Link Layer Ad Hoc Networks. There are no central controllers in mobile ad hoc networks, but a mesh network contains one in the form of a central controller. Wireless connections connect mobile nodes within the radio ranges. The topology of the network is constantly changing because nodes that are far away must depend on one another to send messages. The self-organizing and self-configuring characteristics of mobile ad-hoc networks make them more useful in both military and civilian contexts.[2]

Routing protocols are often used in these networks to ease communication between nodes. A MANET's protocols may be divided into two groups. The minimal power routing algorithm is one kind of protocol. From the beginning to the end, it chooses a route that consumes the least amount of energy. This category's drawback is that it always chooses the lowest-cost routes, which are those that "expire" quickly. In the second group, the network length is increasing. A multi-path forwarding strategy is used to distribute the traffic burden. By lowering the number of nodes required for forwarding and enabling a subset of those nodes to sleep for varying lengths of time, this may be accomplished. As a result, the MANET's traffic is more evenly distributed, resulting in longer network lifespan. MANET's speed may be improved by a variety of reactive routing techniques.

Since the middle of the 1990s, as laptops and 802.11/Wi-Fi wireless networking have grown in popularity, MANETs have been a major study area. Protocols and their mobility within a contained environment are often evaluated in academic studies. As a result, several protocols are put through their paces using metrics like packet delivery ratio, routing overhead, end-to-end latency, and network performance, among others.[3]

Issues in Mobile Ad hoc Networks (MANETs)

Generally, MANETs were first proposed for military battlefield and disaster recovery communications. However, recent evolution in several application areas such as remote sensing, smart highways, remote environmental and animal movement outposts are based on ad hoc networks concepts. These applications require different QoS requirements. The bandwidth requirements vary from a few Kb/s to several Gb/s. Some are delay-sensitive, while others are loss-sensitive. Also, some are highly mobile and others may have limited mobility. There are several issues in MANETs that are very difficult to integrate with internet. We will address some of them below.

- **Security**

Security is an important issue in MANETs. In wireless networks, the link is more vulnerable to nose, error, and eavesdropping than a wired link. Providing security in the presence of mobility and wireless links is more challenging. Therefore, security is often performed through encryption and/or physical layer spread spectrum modulation (direct sequence or frequency hopping). It is a difficult problem to find a trust channel.[4]

- **Routing**

Routing is one of the most difficult problems to implement in MANETs. Routing is the process of finding the best path to send data packets from a source to a destination. Since every device acts as a router, the network becomes more complicated to manage. This is because each node can move randomly in any direction within the network. When a node moves, new paths need to be discovered and selected, as the optimal route in specific time might not work after a few seconds. Also, the environment can be changed from indoor to outdoor scenarios that cause a path to fail.

- **Scalability**

The operation of MANETs strongly depends on network size and packet size. Routing and finding feasible paths become more complicated with size. Similarly, packet size has major impact on forwarding. Scalability measures the ability of the network to provide an acceptable level of services as network grows in size and traffic. Routing protocols add more limitation for the scalability of MANETs. The dynamic topology of a MANET creates a big challenge to provide the huge amount of broadcast message in a dynamic environment.[5]

- **Quality of Services**

Quality of Services (QoS) is a very challenging issue for the developers. It is harder to achieve high performance in MANET due to highly dynamic topology. The network should be able to provide the required quality of service for user’s demand. The performance can be characterized by delay, jitter, and bandwidth. It is difficult to maintain the quality of these parameters under mobility. In a MANET, cross-layer optimization is needed to achieve quality of service.[6]

Types of MANETs

Vehicular Ad hoc Networks (VANETs): Using this, automobiles and roadside equipment may communicate. A kind of artificial intelligence known as intelligent vehicular ad hoc networks (InVANETs) is used to assist automobiles react intelligently to collisions and accidents.

Smart Phone Ad hoc Networks (SPANs): Instead than relying on cellular carrier networks, wireless access points, or traditional network infrastructure, peer-to-peer networks use the Bluetooth and Wi-Fi capabilities incorporated into widely available smart phones. While Wi-Fi Direct uses hubs and spokes, SPANs can manage multi-hop relays and have no designated group leader, enabling peers to join and leave the network without causing any damage to its infrastructure.[7]

Internet based mobile ad hoc networks (MANETs): Networks that connect mobile nodes and internet gateways are called ad hoc networks. In a conventional Hub-Spoke VPN, for example, numerous sub-MANETs may be joined to form a geographically spread MANET. Normal ad hoc routing methods don't function in these networks.

Characteristic of MANET

Mobile ad hoc network nodes may utilize wireless transmitters and receivers that are highly directional, omnidirectional, or steerable. An "ad hoc" or random multihop graph network emerges among the nodes based on their placements, the patterns of their transmitter and receiver coverage, the levels of transmission power and the degrees of co-channel interference. Over time, migration and other circumstances may affect how the nodes in an ad hoc architecture communicate. Networks like this may be described as follows:

Dynamic Network Topologies: The topology of the network changes as nodes move at different speeds. Nodes in a MANET are both hosts and routers since they all share the same network. Thus, it is entirely self-reliant.

Energy-constrained Operation: Batteries are the only source of power for contemporary electronic gadgets. In order to minimize the amount of power used by the mobile devices, the network's architecture must be improved.

Limited Bandwidth: Networks must be tuned to run at their optimum efficiency within the restricted bandwidth of the Wi-Fi network.

Security Threats: The security of wireless communication is more compromised than that of cable communication. It is necessary to improve the MANET's security in order to protect the data being exchanged. There is a distributed aspect to security, routing, and host configuration. There is no central firewall in this environment. It's important to keep in mind the heightened risk of eavesdropping, spoofing, and denial-of-service assaults. For protocol design, there are underlying assumptions and performance issues that go beyond those in the higher-speed, semi-static architecture of fixed Internet routing.[8]

Multi-hop Radio Relaying: When a message's source and destination nodes aren't within radio range, MANETs may use multi-hop routing to get the message to its final destination. Mobile nodes are distinguished by their lack of memory, power, and weight.

Bandwidth-Constrained, Variable Capacity Links: Wireless connections are frequently less reliable, efficient, stable, and capable than conventional communications. This graph depicts the erratic behavior of wireless networks in terms of link bandwidth.[9]

Other Features:

- Configuration of the network is simplified thanks to mobile and spontaneous nature..
- The environment is entirely symmetric since all nodes have the same characteristics and capabilities. High number of users and high mobility of users.
- Nodal connectivity is intermittent.
- Frequent routing updates.

ROUTING

Routing is the process through which data packets are moved from one node to the next. Choosing the most efficient path is what we mean by the term "routing." To go from one place to another in MANET, the procedure of routing is used. The term "routing" is used by a wide range of networks to describe the process of bringing devices together. Mobile ad hoc networks that use packet switching are of special importance here.

As a result of this, packets are routed via a series of intermediary nodes in a packet switching network in order to reach their final destination. Routers, bridges, gateways, firewalls, and switches are common examples of intermediate nodes. Although not specialist hardware, general-purpose computers may also forward packets and conduct routing, although their performance may be restricted. Routes to multiple network destinations are recorded in routing tables, which are used to guide forwarding throughout the routing process. This is why building routing tables, which are saved to memory, is so critical to effective routing. In most cases, a single network route is all that is used by the routing algorithm. A multipath routing strategy allows for the use of numerous alternate pathways.[10]

To determine which routes are put in the routing table, the following factors must be taken into account: (sorted by priority):

4. **Prefix-Length:** longer subnet masks are preferable in these situations (independent of whether it is within a routing protocol or over different routing protocol)
5. **Metric:** In those cases when the lower cost/metric is desired (only valid within one and the same routing protocol)
6. **Administrative Distance:** if a route acquired from a more trustworthy routing protocol is preferable (only valid between different routing protocols)

As a general rule, network addresses are ordered and similar addresses indicate proximity to one other in the narrowest meaning of the term. By using structured addresses, a single routing table entry may represent the route to a group of linked devices. In large networks, organized addressing (routing) is preferable than unstructured addressing (bridging). Routing is currently the primary method for addressing the Internet. Despite their demise, bridges are still in use in a variety of locations. A routing protocol is needed to construct paths between MANET nodes in order for communication to take place inside the network. Some data may need to go over more than one network hop because of the restricted transmission range. To make the network more efficient, each mobile node serves as both a host and a router, passing data to other mobile nodes in the network. All of the nodes on an MAIN network will look for ways to connect to each other and exchange data packets via routing protocols.[11]

ROUTING PROTOCOLS

In a LAN, router communication protocols specify the ways routers utilize to transmit data and determine routes between any two nodes. Routing algorithms are methods for finding the optimum route. There are just a few networks recognized in advance by each router, and these are those that are physically linked. Initially, routing methods send this information to their local neighbors, and eventually to the whole network. Consequently, routers may learn about the network's structure. Routing protocols were created with routers in mind. Using these protocols, routers may more easily share their routing tables, or a list of recognized networks. Routing protocols are available for a variety of network sizes. Using routing strategies in an ad-hoc network, it is necessary for packets to be delivered on time while using as little overhead and bandwidth as feasible.

There are fewer mobile nodes in MANETs since they all use the same frequency channel. One of the most sought aspects is bandwidth efficiency since MANET routing methods must be such. A primary objective of the protocol is to reduce network costs while simultaneously improving network performance from an application viewpoint, or the requirements of the application. If you want a network to be able to support your application, you need a large number of nodes, a high density, frequent connections between nodes, and frequent topological changes.

Routing Protocol Characteristics

The following features may be used to compare routing protocols:

Speed of Convergence: An architectural phrase describing how quickly routers learn one other's routes is known as "speed of convergence" in network design. Consistent routing tables may lead to routing loops in a rapidly changing network, hence a faster convergence mechanism is preferable over a slow one.

Scalability: A network's scalability is determined by the routing protocol used to implement the network. Router protocols must be more scalable as networks get bigger.

Class full or Classless (use of VLSM): A variable-length subnet mask cannot be supported by class complete routing protocols, which exclude the subnet mask from their routing headers (VLSM). The subnet mask is included in the updates in classless routing protocols. In addition to supporting VLSM and a more accurate summary of routes, classless routing protocols.

Resource Usage: Memory space (RAM), CPU utilization, and connection bandwidth consumption are all examples of resource utilization. Additional hardware is required to handle routing protocols and packet forwarding procedures because of the increased resource demands.

Implementation and Maintenance: Knowledge of implementation and maintenance means that network administrators need to be familiar with the routing protocol in order to install and manage their network.

Nodes must follow an ad hoc routing protocol in order to decide which path to travel from one point to another. Nodes join a network by broadcasting their existence and listening to broadcasts from other nodes in the network when they are interested in joining. According to the routing protocol algorithm applied in the network, this routing discovery is carried out in a different manner.

Security Issues in Routing Protocol

Several research initiatives are now ongoing to discover security dangers and solutions for mobile ad hoc networks, which have lately experienced an increase in security measures. Attacks such as listening in, impersonating another person, and denying services are all made a lot easier when using a wireless network. Nodes in ad hoc networks are free to come and go as they like. A rogue node might quickly penetrate the network this way, devouring bandwidth or depleting the batteries of other nodes to attach themselves to limited resources. Routing inefficiency or redirecting flows and intercepting packets that may be delayed, discarded, or manipulated is relatively simple to do. In many investigations, routing methods that solve these concerns may be identified. Nodes intrusion detection and denial of service resilience are two more options.[12]

The Packet Conservation Monitoring Algorithm (PCMA) was used to identify selfish nodes in MANETs (PCMA). Protocols such as the Secure Message Transmission, Secure Single Path, or SMT continually reorganize themselves in order to avoid and accept data loss. MIDS (Mobile Intrusion Detection System) and a threshold-based intrusion detection system were used to protect a multi-hop ad-hoc wireless network, detecting irregularities in packet forwarding, such as intermediary nodes discarding or delaying messages.

Link level security protocols (LLSP) may be implemented in Suburban Ad-hoc Network (SAN) architecture (SAHN). In order to verify LLSP's efficacy, they examined a number of its security features. LLSP's practicability has been determined by estimating the time required for each authentication procedure. ' For an ad hoc network like a SAHN, their early research shows that the LLSP link-level security service works well.

As a consequence of the security concerns raised by wireless sensor networks, a practical strategy for link layer security has been proposed. They came up with a lightweight CBC-X mode Encryption/Decryption method that achieved encryption/decryption and authentication at the same time. They've also come up with a unique padding method that allows the system to deliver encrypted/authenticated packets with zero redundancy. There were no additional bytes spent by the security activities.

Many assaults were averted by the security architecture for self-organizing mobile wireless sensor networks. The security effect of certain assaults that cannot be stopped was also minimized as a result of this. They examined its security architecture and found that it met all of the requirements for self-organizing mobile wireless sensor networks while still being a lightweight solution.

Protocol for MANETs that achieves packet secrecy and authentication via the use of trust-based security, using routing layer information, a strategy for identifying and isolating rogue nodes was developed in the protocol's initial phase. By keeping a trust counter for each node, it favored packet forwarding. By diminishing or raising the trust number, a node was penalized or rewarded. The intermediary node was tagged as malicious if its trust counter value went below a certain threshold. The CBC-X form of authentication and encryption has been added to the protocol's link-layer security in the next iteration.

CONCLUSION

There is large number of different kinds of routing protocols in mobile ad-hoc networks, the use of a particular routing protocol in mobile ad-hoc network depends upon the factors like size of the network, load, mobility requirements etc. A mobile ad hoc network is wireless ad hoc networks with routable networking environments rather than link layer ad hoc networks. There are no central controllers in mobile ad hoc networks, but a mesh network contains one in the form of a central controller. Wireless connections connect mobile nodes within the radio ranges. The topology of the network is constantly changing because nodes that are far away must depend on one another to send messages. The self-organizing and self-configuring characteristics of mobile ad-hoc networks make them more useful in both military and civilian contexts, routing protocols are mechanisms by which routing information is exchanged between routers so that routing decisions can be made. In the internet, there are three types of routing protocols commonly used them are: distance vector, link state, and path vector. Routing protocols are available for a variety of network sizes. Using routing strategies in an ad-hoc network, it is necessary for packets to be delivered on time while using as little overhead and bandwidth as feasible.

REFERENCE

1. Humayun Bakht, 2011. Survey Of Routing Protocols For Mobile Ad-Hoc Network.International Journal Of Information And Communication Technology Research, Pp.258-270.

2. Jabbar, W.A., Ismail, M. And Nordin, R., 2014. Performance Evaluation Of MBA- OLSR Routing Protocol For Manets. Journal Of Computer Networks And Communications, 2014.

3. Jacquet, P., Laouiti, A., Minet, P. And Viennot, L., 2002, May. Performance Of Multipoint Relaying In Ad Hoc Mobile Routing Protocols. In International Conference On Research In Networking (Pp. 387-398). Springer, Berlin, Heidelberg.

4. Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A. And Viennot, L.,2001. Optimized Link State Routing Protocol For Ad Hoc Networks. In Multi Topic Conference, 2001. IEEE INMIC 2001. Technology For The 21st Century. Proceedings. IEEE International (Pp. 62-68). IEEE.

5. Jane, Y.Y., Xie, L.F., Zhang, M. And Chong, P.H., 2012. A Performance Comparison Of Flat And Cluster Based Routings In Mobile Ad Hoc Networks. International Journal Of Wireless Information Networks, 19(2), Pp.122-137.

6. Khan, K.U.R., Reddy, A.V., Zaman, R.U., Reddy, K.A. And Harsha, T.S., 2008, November. An Efficient DSDV Routing Protocol For MANET And Its Usefulness For Providing Internet Access To Ad Hoc Hosts. In TENCON 2008-2008 IEEE Region 10Conference (Pp. 1-6). IEEE.

7. Kitasuka, T. And Tagashira, S., 2011, November. Density Of Multipoint Relays In Dense Wireless Multi-Hop Networks. In Networking And Computing (ICNC), 2011 Second International Conference On (Pp. 134-140). IEEE.

8. Kitasuka, T. And Tagashira, S., 2013, June. Finding More Efficient Multipoint Relay Set To Reduce Topology Control Traffic Of OLSR. In World Of Wireless, Mobile And Multimedia Networks (Wowmom), 2013 IEEE 14th International Symposium And Workshops On A (Pp. 1-9). IEEE.

9. Morshed, M.M., Rahman, M.U., Rahman, M.H. And Islaml, M.R., 2012, May. Performance Comparison Of TCP Variants Over AODV, DSDV, DSR, OLSR In NS-2. In Informatics, Electronics & Vision (ICIEV), 2012 International Conference On (Pp. 1069-1074). IEEE.

10. Murthy C. S. R. And Manoj B. S., 2005. Ad Hoc Wireless Networks, Pearson Education, Pp. 330-334.

11. Oo, M.Z. And Othman, M., 2010, March. Performance Comparisons Of AOMDV And OLSR Routing Protocols For Mobile Ad Hoc Network. In 2010 Second International Conference On Computer Engineering And Applications (Vol. 1, Pp. 129-133). IEEE.

12. Rousseau, S., Benbadis, F., Lavaux, D. And San, L., 2011, June. Overview And Optimization Of Flooding Techniques In OLSR. In 2011 IEEE International Symposium On A World Of Wireless, Mobile And Multimedia Networks (Pp. 1-7). IEEE.

Corresponding Author

Sanket Singh*

Research Scholar, Shri Krishna University, Chhatarpur M.P.