Journal of Advances in Science and Technology
Vol. 17, Issue No. 1, March-2020, ISSN 2230-9659

A Study of Mobile ADHOC network Routing Protocol

Nishi Pastor[1]*, Dr. Rajeev Yadav[2]

[1] Research Scholar, Sri Krishna University

[2] Professor, Sri Krishna University

Abstract - ***An Ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or infrastructure. Such networks have no fixed topology due to the high degree of node mobility. Hence, efficient and reliable routing is one of the key challenges in mobile ad hoc networks. Many routing algorithms have been proposed and developed for accomplishing this task. Therefore, it is difficult to determine which protocol performs best under a number of different scenarios. Hence, this paper presents review and a comparison of the typical representatives of routing protocols designed for MANETs and the study in which discussed about typesofMANET, CharacteristicofMANET, ApplicationsofMANET, MANETchallenges, Security issues inMANET, Routing.***

Keyword - MANET, NETWORK

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

INTRODUCTION

A network of wirelessly connected mobile devices that is self-configured and does not need any infrastructure is referred to as a "mobile ad hoc network." Ad-hoc is a Latin word that means "for this reason." Without the aid of pre-existing network infrastructure or centralized administration, this kind of network is made up of wireless mobile nodes that design their own architecture. Each node serves as both an end system and a router for all other nodes in the system in an autonomous system of mobile nodes connected by wireless networks. Users and devices may communicate with one another without previous communication planning thanks to self-organizing and cooperative nodes that can create unpredictable and transient network topologies. The Link Layer and the Routable Networking Environment are the two different categories of MANETs. Mobile ad hoc networks use point-to-point connections as opposed to mesh networks, which include a central controller. Mobile nodes are connected through wireless links inside the radio spectrum. Because nodes that are spread out throughout the network must rely on one another to relay messages, the topology of the network is continually changing. Mobile ad hoc networks are more practical in both military and civilian settings due to their self-organizing and self-configuring features. [1] Routing protocols are used to facilitate communication between nodes in these networks. There are two categories of MANET protocols. One form of protocol is the least power routing algorithm. It selects a path that uses the least amount of energy from the start to the finish. This category often selects the fastest-expiring, most energy-efficient routes. The network length is growing in the second group. The traffic load is distributed by using a multi-path forwarding method. The majority of nodes are kept awake; however others are let to sleep for extended periods of time. The MANET's traffic is balanced in this way, extending the network's overall useful life. Many reactive routing techniques have been created in order to enhance MANET performance. Since the middle of the 1990s, it has been a popular place to study due of the proliferation of laptops and 802.11/Wi-Fi wireless networking. Academic publications often assess how well processes can man oeuvre in a small space. Different protocols are graded according to these measures, which may include but are not limited to packet delivery ratio, overhead brought on by routing methods, network performance, and other metrics. [2]

Types of MANET

Vehicular Ad hoc Networks (VANETs): Through this, vehicles and roadside machinery interact. Intelligent vehicular ad hoc networks (InVANETs), a kind of artificial intelligence, let cars respond intelligently to collisions and accidents.

Smart Phone Adhoc Networks (SPANs): These networks employ the technology in currently available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure (mainly Bluetooth and Wi-Fi). In contrast to conventional hub-and-spoke networks like Wi-Fi Direct, SPANs do not need a group leader and let peers to join and leave the network without

disrupting it.[3]

Internet based mobile adhocnet works(iMANETs): Ad hoc networks are networks that link mobile nodes with internet gateways. A Hub-Spoke VPN, as an example, may be used to connect several sub-MANETs in a geographically scattered MANET. Typical ad hoc routing techniques do not immediately applicable in these networks.

Characteristic of MANET

The wireless transmitters and receivers used by mobile ad hoc network nodes might be very directional, omnidirectional, or steerable. Based on the nodes' positions, their transmitter and receiver coverage patterns, communication power levels, and co-channel interference levels, a "ad hoc" or random multihop graph network develops among them at any given time. This ad hoc topology could alter over time as the nodes move around or alter their transmission and reception capabilities. The following is a summary of these networks. [4]

Dynamic Network Topologies: The network's nodes move at different speeds, which lead to anomalies in the topology of the network. In a MANET, each node serves as both a host and a router. It therefore operates autonomously.

Energy-constrained Operation: All current electronic devices run solely on batteries. The design of the network may be improved to reduce the energy consumption of mobile devices.

Limited Band width: Security Threats: Wireless forms of communication are more vulnerable to security threats than conventional forms of communication. The MANET's security has to be improved to ensure the security of the sent data. Operations including security, routing, and host setup are dispersed in nature. There is no central firewall present. It is important to take into account the increased risk of eavesdropping, spoofing, and denial-of-service assaults. These traits lead to a set of underlying assumptions and performance considerations for protocol design that go beyond those governing routing inside the fixed Internet's higher-speed, semi-static architecture. [5]

Multi-hop Radio Relaying: The MANETs are capable of multi-hop routing when a message's source node and destination node are outside of radio range. Mobile nodes are distinguished by having limited memory, power, and weight.

Bandwidth-Constrained, Variable Capacity Links: When compared to wired lines, the capacity, efficiency, dependability, and stability of wireless communications are often worse. This demonstrates how wireless communications' link bandwidth varies.

Other Features:

- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment. High user density and large level ofuser mobility.
- Nodal connectivity is intermittent.
- Frequent routing updates.

Applications of MANET

Since MANETs allow for temporary connectivity without a specific infrastructure, many applications are possible. Here are few instances.

Military Battlefield: Modern digital warfare requires a variety of reliable and effective communication channels. The most typical places for communication equipment are in vehicles, tanks, and trucks. The ability to communicate with wireless base stations or other telecom devices directly is another capability that soldiers may carry, if the radio range permits. On the other side, these forms of communication are said to be primitive. If the called party is not within radio range of their position, wireless base stations may be destroyed by the enemy, preventing soldiers from communicating with one another. This is the circumstance when it comes to mobile ad hoc networks. Ad hoc networks are sometimes referred to as self-organizing networks due to their resilience in the face of node destruction or mobility, Multi-hop C communication, which enables military personnel to send data from one radio device to another, enabling them to communicate information with other units. [6]

Sensor Networks: A different use for the technology is the construction of sensor networks using MANETs. This technology uses a network made up of a huge amount of small sensors. These may be used to reveal a variety of attributes about a place. This includes a broad variety of environmental elements, including toxins, pollutions, and other elements. Examples of usage include predicting earthquakes and agriculture. Since each sensor only has a little processing capacity, it must rely on others to convey data to a central computer. The processing capability of a single sensor is limited by the physical constraints of the sensor, rendering them prone to failure. Mobile ad hoc sensor networks may be the foundation of homeland security in the future.

Automotive Applications: Automotive networks are a topic of much debate right now. To allow automobiles to interact with the road, traffic lights, and other vehicles, several ad hoc networks of

various sizes need be developed. The network's data on traffic conditions, congestion, and accident notifications will be useful to drivers since it helps to optimize traffic flow.

Commercial Sector: Ad-hoc may be used in disaster relief activities like firefighting, flood control, or seismic relief efforts. When a communications infrastructure is either nonexistent or deteriorated during an emergency rescue effort, rapid network development is necessary. Data is sent between members of the rescue team via a portable device. Other commercial applications include police enforcement, ad hoc ship-to-ship communication, etc.

Personal Area Network: The most popular technique to set up PANs, or personal area networks, is via ad hoc connections between various mobile (and stationary) devices. PANS may be used as a stand-alone network to network various home appliances, but joining a larger network expands its functionality. PANs might be seen as an expansion of the internet or the telecommunications network when viewed in this context. People will interact with technology in their surroundings in a dynamic and close way, whether or not it is visible to them, according to the concept of ubiquitous or pervasive computing. [7]

MANET Challenges

A MANET setup has to get over several efficiency and restriction problems. It contains:

Spectrum Allocation: We must address problems such radio frequency (RF) interference, confined range, constrained data flow, mobile device, and spectrum sharing among devices. Today, the Federal Communications Commission (FCC) controls how radio spectrum is used. The majority of experimental ad hoc networks operate in the ISM band. Ad hoc networks must operate within a certain spectral range to prevent interference with one another. Most microwave ovens run in the 2.4GHz frequency band to prevent interference with wireless LAN networks.

Energy Efficiency: Conservation of energy is a problem. Since most existing protocols assume that all hosts and routes are powered by main power, power consumption is often not an issue. However, most modern mobile devices are powered by batteries. Microprocessors are more sophisticated than batteries. A lithium-ion battery can currently only be used for brief periods of time. A device's operational time must be limited via power conversion. Particularly mobile ad hoc networks will need the usage of router-like devices. Because of this, nodes in mobile ad hoc networks use a lot of power while forwarding packets for other nodes.[8]

The Wireless Link Characteristics are Time-Varying in Nature: Wireless channels are prone to transmission obstructions such as fading, route loss, blockage, and interference. Various variables undermine the wireless transmission's dependability.

Limited Range of Wireless Transmission: As a consequence of the constrained radio spectrum, data transmission speeds are lower than on wireless networks. By reducing overhead as minimal as feasible, bandwidth utilization may be maximized.[9]

Packet Losses Due to Errors in Transmission: As a consequence of these and other reasons, MANETs incur greater packet loss owing to factors such as concealed terminals that result in collisions, wireless channel difficulties (high BER), interference, and frequent breaks in routes caused by mobility of nodes.

Route Changes Due to Mobility: The dynamic nature of network topology results in frequent path breaks.

Frequent Network Partitions: The random movement of nodes of tenleads to partition of the network. This mostlyaffects the intermediate nodes.

Secure Network: Ad hoc wireless networks are exceedingly challenging to protect. Understanding the various attack vectors is the first step in developing a solid security plan. In addition to the vulnerabilities that are present in both wired and ad hoc networks, ad hoc networks also have vulnerabilities that are exclusive to the ad hoc environment. The complexity and diversity of the discipline have produced a vast range of concepts that this page is unable to explore. By reading this article, you may discover more about the security dangers of ad-hoc networking. The following paragraphs provide a summary of ad hoc network security. Active attacks include, among other things, the replication, modification, and deletion of data. Ad hoc networks are susceptible to certain active attacks. Attacks including impersonation, denial of service, and disclosure may all be combined. [10]

Secure Routing: Secure routing protocols deal with malicious nodes that might change routing information, make up false routing information, or pose as other nodes to interfere with a routing protocol's regular functioning.

Cooperation Enforcing: Ad hoc networks need contributions from ad hoc nodes to provide basic network functions like packet forwarding and routing. Ad hoc networks lack the support of specialized nodes for fundamental network functions including packet forwarding, routing, and network management. Instead, all reachable nodes provide these functions. Certain ad hoc network security problems are brought on by this discrepancy. In contrast to nodes in a traditional network, nodes in an ad hoc network cannot be trusted to perform crucial network activities successfully. For instance, because every device acts as a router, protecting routing in ad hoc networks may be challenging. The forwarding method is also cooperative. [11]

Communication between nodes that are separated by more than one hop is facilitated by intermediary relaying nodes. A node that does not cooperate with other nodes is said to be misbehaving. Selfish or malicious nodes may cause undesirable routing-forwarding behaviors. An evil node would purposefully interrupt the flow of packets through the network by ignoring them as opposed to collaborating. A selfish node declines even though it expects other nodes to forward packets on its behalf, even when it lacks the capacity to do so, even while it is not trying to purposefully hurt other nodes. This is a network node that is connected but does not use the network.

Securityand Privacy: The following are the difficulties with security and privacy in the context of ad hoc networks:

Ad hoc networks are particularly susceptible to link attacks, such as passive eavesdropping and aggressive impersonation, since they utilize wireless connections. Active assaults may provide the enemy the ability to compromise availability, integrity, authentication, and non-repudiation by removing communications, inserting false messages, changing messages, and impersonating a node.

Second, there is a non-negligible risk of hacking for nodes travelling in dangerous environments (like a battlefield) with relatively weak physical protection. Instead of merely considering hostile assaults coming from the outside of a network, one should also include attacks launched from inside it by compromised nodes.

It is also dynamic due to the network's membership and architecture continually changing (i.e. nodes frequently join and leave the network). The trust relationship between nodes also changes when it is discovered that certain nodes have been compromised.And last, an ad hoc network may have thousands of nodes. Scalable security solutions are required to handle such a large network.

Security Issues in MANET

The Mobile Ad-Hoc Network's (MANET) security is essential to the network's general functionality. Network availability, confidentiality, and data integrity may all be guaranteed by making sure security issues have been handled. Due to its open medium, variable topology, lack of centralized administration and monitoring, cooperative algorithms, and lack of a clear defensive mechanism, MANET is susceptible to attacks. These events have modified the MANET's defence against security threats.

In recent years, discussions and policy-making have focused heavily on computer network security. In these sessions, static and networking designs for wired systems were mostly explored. On the other hand, further investigation and development are needed for mobile Ad-Hoc networking security. The advent of cutting-edge networking technology has presented new difficulties for routing's basics. Ad-hoc wireless networks are distinct from traditional networks in a number of respects. Ad-hoc mobile networks use unique routing techniques from those designed mainly for the internet (MANET). A conventional routing table has historically been used by hosts connected by a non-dynamic backbone. Supporting Ad-Hoc networks is not practical due to network mobility and shifting topology.

Lack of infrastructure, a lack of trust between nodes, and a topology that is continuously changing make routing systems vulnerable to a number of assaults, Selfishness, dynamic nature, resource constraints, and open network medium are now the most prevalent types of vulnerabilities that have been examined. Despite the aforementioned protocols, there are several sorts of attacks that may be conducted on MANET. In addition to network-layer, routing, and packet forwarding assaults, these attacks also comprise passive, active, internal, and external attacks. [12]

Nodes in a MANET communicate with one another based on mutual trust; there is no central administration. As a consequence, attacks from inside the MANET network are more likely. With wireless connection, it is considerably easier for a hacker to infiltrate the MANET and get access to the ongoing conversation. Within the wireless link's coverage area, mobile devices may hear and potentially participate in network activity.

ROUTING

Data packets are sent from one node to another using the routing mechanism. To "route" anything is to "choose the best path." "Routing" in the context of MANET simply refers to choosing the fastest path between two points. Routing terminology is used in a variety of networks, including telephone, electronic data, and internet networks. In mobile ad hoc networks, routing is accomplished using packet-switching technology.

As a consequence, packets are routed through a packet switching network via a number of intermediate nodes before arriving at their destination. Switches, routers, bridges, and gateways are frequent examples of intermediate nodes in networks. However, even if their performance could be limited, general-purpose computers are still able to forward and route packets. Routing tables, which are used to direct forwarding throughout the routing process, include routes to several network destinations. The creation of routing tables, which are kept in the router's memory, involves a variety of aspects. The majority of routing techniques use only one network path. Multiple alternative routes may be used using a multipath routing method. [7-8]

The following factors are taken into account when

there are overlapping or equal routes to determine which routes are added to the routing table (sorted by priority):

1. **Prefix-Length:** where longer subnet masks are preferred (independent of whetheri t is within a routing protocol orover different routing protocol)

2. **Metric:** where a lower metric/costis preferred(only valid within one and the same routing protocol)

3. **Administrative Distance:** where a route learned from a more reliable routing protocol is preferred (only valid between different routing protocols)

When comparing routing to bridging, network addresses are considered to be ordered and similar to represent proximity throughout the network. A single entry in the routing table may be used to indicate the route to a group of devices when the address is structured. Unstructured addressing is inferior to structural addressing (routing) in large networks (bridging). Nowadays, the most used method of identifying an Internet address is router-based addressing.

CONCLUSION

Ad-hoc networks are practical and very dynamic, and this study may build and offer tools that make ad-hoc network research more approachable to other people. The three main contributions the thesis provides to the realm of research tools and methodology. I investigated the behavior of three alternative ad-hoc reactive routing algorithms for each protocol before coming to my conclusions. Determining the properties of protocol routing and techniques on demand might help future designers create new protocols.

REFERENCE

1. SachinDnyandeoUbarhande(2012)“PerformanceEvolutionofAODV and DSR Routing Protocols in MANET Using NS2”, International Journal of Scientific & Engineering Research Volume 3, Issue 5.

2. Udit Agarwal and Monika Saxena (2013) “Comparative and Behavioral Study of Various Routing Protocols inVANET”, International Journal of AdvancedResearchin ComputerScienceandSoftwareEngineering Volume 3, Issue 10.

3. ShivlalMewada et. al, “Simulation Based Performance Evaluation of Routing Protocols for Mobile Ad-hocNetworks (MANET)”, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.4, August 2012

4. Singh, T.P., S. Dua and V. Das, 2012. Energy-efficient routing protocols in mobile ad-hoc networks. Int. J. Adv. Res. Comput. Sci. Software Eng., 2: 1-7.

5. Anurag Porwal, B.L.Pal, Rohit Maheshwari, Gaurav Kakhani. (2012) “StudyandDesignofNewReactiveRoutingProtocolAdvanceAODV for Mobile Ad hocNetworks”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3.

6. AbolfazlAkbari,MehdisoruriandAliKhosrozadeh.(2012)"ANew AODV Routing Protocol in MobileAdhocNetworks".

7. Ammar Odeh, Eman Abdel Fattah and Muneer Alshowkan. (2012)“Performance Evaluation of AODV and DSR Routing Protocols in Manet Networks”, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4.

8. Petteri Kuosmanen. (2002) “Classification of Ad Hoc Routing Protocols”,FinnishDefenceForces,NavalAcademy,P.O.Box5,FIN- 00191 Helsinki, Finland.

9. C.E.Perkins,E.M.Royer,andS.R.Das,(2002)“AdHocOn-Demand DistanceVector(AODV)Routing”,InternetDraft,draft-ietf-manet- aodv-10.txt, work in progress.

10. T. S. Rappaport, (2002) “Wireless Communications: Principles and Practice”, 2/E”, Prentice Hall PTR.

11. R.Ramanathan and J. Redi, (2002) “A Brief Overview of ad hoc networks: challenges and Directions”, IEEE Commun. Mag., Vol.40, No.5.

12. Buttyan,L.,andHubaux,J.P.(2003)“Simulating cooperationinself-organizingmobileadhocnetworks.MobileNetworksandApplications: Special Issue on MobileAd Hoc Networks, 8(5).

Corresponding Author

Nishi Pastor*

Research Scholar, Sri Krishna University