CONCEPT AND CHARACTERISTICS OF MOBILE AD-HOC NETWORK

Obidike, G. C., Nwabueze, C. A. and Onuzulike, V. C.
Department of Electrical/Electronic Engineering, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State.

ABSTRACT
Mobile Ad-Hoc Network (MANET) has gained popularity due to its flexibility and increased application in wireless communication. Its dynamic topology, decentralization and ease of administration have enhanced its preference for inclusion in infrastructure based network. In this paper, infrastructure-based and infrastructure-less based (ad-hoc) networks are critically analyzed and the characteristics of MANET, its application and challenges, routing protocol and challenges of routing protocol are presented.

Keywords: MANET, Characteristic, Ad-Hoc Network, Routing Protocol**.**

1.0 INTRODUCTION
The term "Ad-hoc" means "for this purpose only". Ad-hoc network therefore is a network created for a special purpose which consists of autonomous nodes, each acting as a host and as a router, connected to each other through a wireless link. The nodes here are mobile, hence the name Mobile Ad hoc Network (MANET). As a result, MANET is said to be time varying in nature as nodes leave and rejoin the network at will. MANET is a continuously, self-configuring, self-healing, infrastructure-less network of mobile devices which communicate wirelessly. This type of network has a dynamic topology [1]. Figure 1 shows a typical ad-hoc network.

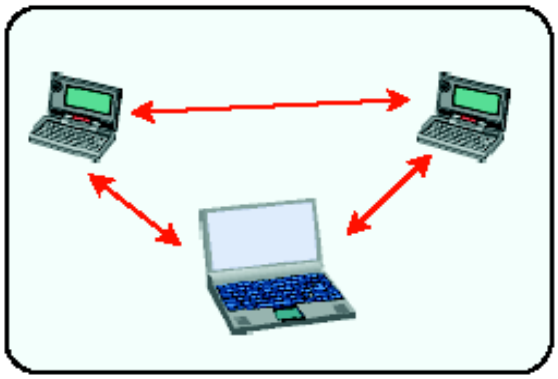

Figure 1: Typical Infrastructure-less (Ad hoc) Network [1].

A wireless network can be grouped into Infrastructure-based network and Infrastructure-less based network. In Infrastructure-based network, wireless nodes have a centralized administrator referred to as the Base Station (BS) or the Access Point (AP). The implication is that all messages to be communicated to a node in a region or from one region to another must be communicated through the BS as shown in Figure 2. Example of an infrastructure based network is seen in Cellular networks, UMTS, WLAN, etc. The base station serves as the router by mere finding the path of transmission, while nodes are the hosts. The BS is said to provide the needed

central control of the network which include smooth routing of packets, packet loss avoidance and traffic decongestion. In a case where a node move out–of-range of a given BS to another coverage area (i.e. in another region), it has to connect to another BS in that area. This process is termed "hands off". The major disadvantage of an infrastructure based network is that when one BS fails (faulty) the whole nodes attached to that BS will be cut off. This is a disadvantage as the network lacks robustness in failure.

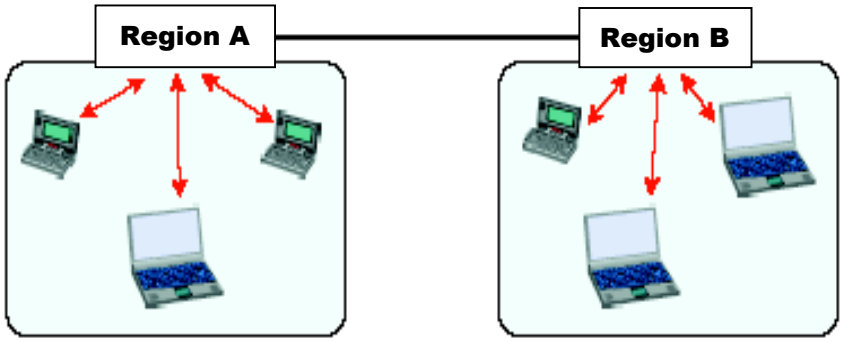

Fig. 2: Infrastructure-based Network [2].

Observe from Fig. 2 also that each node transmits directly to the Access point as indicated by the arrow. So, if a node wants to communicate to another, the node has to relay its message through the gateway and vice versa. There is no provision for a node communicating directly to another rather through AP. In contrast, ad hoc network has a distributed kind of network since there is no provision for direct communication to a BS (Access point). Instead, nodes communicate directly to each other (see Fig 1). Each node participates actively in the network since each of them serve as a router and as a host. When a node goes out of range of network, the network uses a routing protocol to find the shortest and safest path of locating the node, though at a cost of bandwidth (BW). Failure of one node does not disrupt the entire communication of the whole network. Example of ad hoc can be found in MANET. Wireless network can also be classified as a single hop and a multi hop [2].

2.0 History of Ad Hoc MANET

The existence of ad hoc network is categorized into first, second and third generation.

The first generation of ad hoc network called Packet Radio Network (PRNET) as far back as 1970's in conjunction with ALOHA (Ariel Location of Hazardous Atmosphere) and Carrier Sense Medium Access (CSMA) approaches for medium access control and a kind of distance-vector routing. PRNET were used in a trial basis then to provide different networking capacities in a combat environment.

The second generation of ad hoc network emerged in 1980's when the ad hoc network systems were enhanced and implemented as a part of the Survivable Adaptive Radio Program (SURAN). This provided a packet switched network to the mobile battle field in an environment without infrastructure.

For a long time the application of ad hoc network was found only in the military until the third generation of ad hoc, which is today's wireless ad hoc network deployed in mid1990's. The great potentials and advantages of ad hoc network outside the military witnessed the creation of mobile ad hoc networking group called IETF. Here nodes communicate within their radio range

and outside radio transmission range. Wireless ad hoc network do not have any gateway. Instead, every node is a gateway for another. The third generation of ad hoc network made ad hoc network popular due to rise in its commercial application.

2.1 Types of MANET

Types of MANET include VANET, iVANET, iMANET and FANET [3]

1. **Vehicular ad hoc Network (VANET):** In this type of MANET, cars are used as nodes in network to create a mobile network. It turns every participating car into a wireless router or a node at an approximate distance of 100m to 300m to order to communicate thereby creating a wide range of network. As mobile nodes fall out of range others join, creating a mobile internet. VANET is aimed at providing related information and traffic management.
2. **Intelligent Vehicle Ad hoc Mobile Network (INVANET):** This is an intelligent way of using vehicular network to integrate multiple ad hoc network technologies such as Wi-Fi IEEE 802.11, WAVE IEEE 1609, and Bluetooth. All these are deployed in the monitoring of vehicle collision and accidents. In other words INVANET helps in defining safety measures in vehicles. Vehicular ad hoc network can therefore be viewed as component of the intelligent transport system.
3. **Intelligent based Mobile Ad hoc Network (iMANET):** This is used in linking fixed nodes and mobile nodes via routing protocol which automatically establishes connection in decentralized manner.
4. **Flying Ad hoc Network (FANET):** FANET is a special case of MANET. The topology of this network can change frequently when compared to VANET. Here an Unmanned Aerial Vehicle (UAV) flies autonomously without carrying any human help. It does this by simply connecting directly to satellite or ground station to establish ad hoc network. This type of wireless networking architecture is called Flying Ad hoc Network (FANET).

2.2 Characteristics of MANET

1. Nodes are connected through a wireless link.
2. Each of the nodes act as a router and as a host.
3. The network lacks infrastructure leading to decentralized administration (control).
4. The network is less cost effective, due to lack of infrastructure.
5. MANET can easily be setup anywhere especially where there is no internet.
6. The network topology is dynamic in nature.
7. They are more vulnerable to attacks when compared to wired network.
8. They are capable of being multi-hopped when the intended node goes out of range of network.
9. Mobile nodes are characterized with less memory, power and light weight features.
10. The access to channel by any node is not restricted.

2.3 Advantages of MANET

1. Because the network is easy to set up, it can be setup at any place.
2. It has a distributed administration
3. Lack of infrastructure makes the network robust in network failure.
4. It is scalable. This means that network accommodates addition of more nodes.

5. It is very cheap to set up since there is no wiring of nodes.
6. It has adaptive computing and self -configuring capability
7. It does not restrict access to channels.

2.4 Challenges of Mobile Ad hoc Network

1. **Limited bandwidth:** The limited radio band results in reduced data rate compared to wireless networks. Hence, optimal usage of bandwidth is necessary by keeping low overhead as possible.
2. **Energy constraints:** Most of the nodes rely on limited battery life. Some of the power of the batteries is used for data transmission, data processing and for routing packets to their destination. This is a critical issue in the design of an ad hoc network.
3. **Dynamic network topology:** The frequent movement of nodes compounds the challenges of designing an ad hoc network due to frequent path breaks**.**
4. **Routing overhead:** Due to the mobility of nodes within the ad hoc network, stale routes are generated in the routing table leading to routing overhead.
5. **Packet loss due to transmission error:** The vulnerable nature of wireless networks often lead to frequent packet loss due to traffic collision caused by hidden terminals, interference and frequent path breaks caused by mobility of nodes.
6. **Frequent network partitions:** The random movement of nodes often leads to network partition. This affects mostly the intermediate nodes.
7. **Limited physical security threats:** Mobile nodes are more vulnerable to attacks within and outside network.

2.5 APPLICATIONS OF MANET

(a)Tactical Networks

- Military communication and operations
- Coordination of military object moving at high speeds such as fleets of airplanes or ship.
- Automated battlefields such as in determining the position of troops during war fare.

(b) Sensor Networks

- Collection of embedded sensor devices used to collect real time data to automate everyday functions.
- Deployed in the monitoring and measurement of variables such as change in pressure, temperature etc especially in pipelining.
- In tracking of positions and movement of objects and animals.

(c) Emergency Services

- In Search, rescue, crowd control operations and in disaster control and recovery
- Replacement of a fixed infrastructure in case of earthquakes, hurricanes, fire etc.
- In policing and fire-fighting.
- Supports doctors and nurses in medical field

(d) Commercial and Civilian Environment

- E-commerce, e.g., electronic payments from anywhere (i.e., in taxi).
- Business: dynamic database access to customer files.

(e) Home and Enterprise networking

- Home/office wireless networking such as WLAN

- Conference meetings and lectures
- Personal area network (PAN)

(f) Educational Applications

- In universities and Campus setting
- Virtual classrooms or conference rooms
- Set up ad hoc communication during conferences, meetings, or lectures

(g) Entertainment

- Used in Multiuser games
- Robotic pets outdoor internet access

3.0 ROUTING PROTOCOL

Routing protocol has been defined in [4] as set of rules governing the routing of packets from source to destination. This standard controls how nodes decide the way to route packets between the computing devices. In ad hoc, nodes are not usually familiar with the topology of their network; instead they have to discover them. The Routing protocol therefore, is very crucial in establishing communication especially to nodes outside the communication radius. Routers are ever ready to find the shortest and safest route for packet delivery. Since the network has been characterized by a multi-hop network topology that can change frequently due to the mobility of nodes, efficient routing protocols are needed between nodes without causing unnecessary traffic overhead.

3.1Classification of Routing Protocol

Routing protocols used in MANET are classified into three, namely: Table driven, demand driven and Hybrid routing protocol.

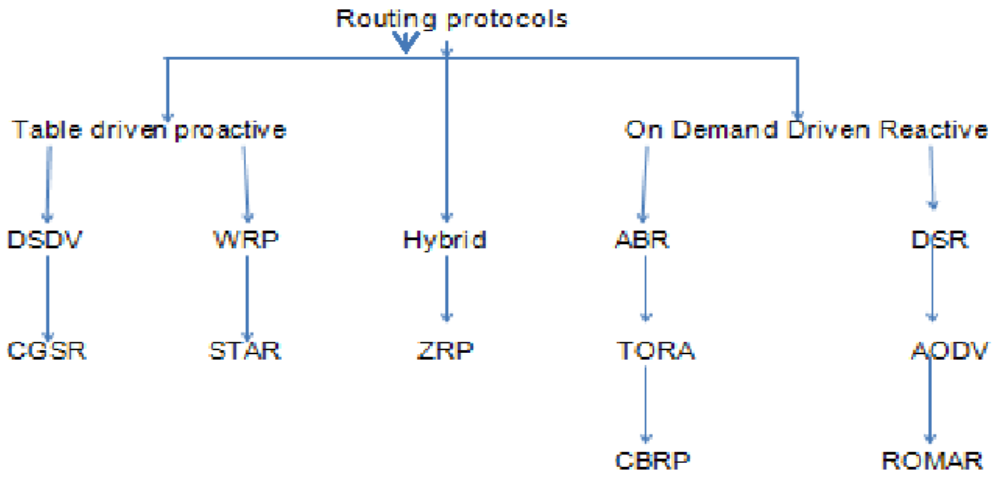

Figure 3: Classification of Routing Protocol [4].

I. Table Driven (Proactive) Protocol

Here each node has a routing table which contains information about the network topology. The routing table is periodically updated since routers frequently calculate routes to various nodes.

This protocol is therefore said to be proactive since the routers are readily available in the network. They attempt to maintain consistent and up-to-date routing information of the whole network, thereby minimizing delay in communication by allowing nodes to quickly determine the node to reach out to [5]. It does this by invoking a route discovery mechanism to find the path to the destination, which remains valid until the destination is reachable or is no longer needed [4]. The disadvantage of this protocol is that it generates control traffic that is needed to continually update stale route entries; especially in highly mobile environment. The communication overhead incurred in implementing this algorithm is exorbitant. Some of the existing proactive protocols include: Destination sequence distance vector (DSDV), Wireless Routing Protocol (WRP), Cluster head Gateway Switch Routing (CGSR) Source Tree Adaptive Routing (STAR) etc.

i) Destination sequence distance vector (DSDV)

Here each node in the network must be stored in the routing table. The routing table records the nodes, the distance of nodes from other nodes (number of hops). The protocol adds a sequence of number to the routing information protocol (RIP) routing table. This sequence number field is used to differentiate old route from new routes. Each node maintains a routing table which contains the next hop information for all reachable destinations. Each routing table consists of: the sequence number (received from the destination), destination address, number of hops required to reach the destination. The sequence number finds the new route. This happens whenever a node receives new information about a particular route it then compares the sequence number of the route. The one with greatest sequence number is kept while the other one is discarded. If it receives two updates with the same sequence number, the one with lower number of hops is used. The routing table is updated periodically or whenever information is available. When the routing table is updated periodically it is called full dump update but when update is sent when there is new information it is called incremental driven update. This protocol is highly unfavourable for networks which have high mobility and large number of nodes.

ii) Clustered Head Gateway Switching Routing protocol (CGSR)

CGSR routing involves cluster routing where a node finds the best route over cluster heads from the cluster member table. Nodes are divided into group of nodes with a head elected in each group called the clustered head. The clustered head is the gateway to nodes in a group which connects other nodes into a hierarchical structure. This implies that packets are not sent directly to destination rather to clustered head which routs the packet to the intended destination. All mobile devices maintain two tables: the clustered member table and the routing table. The clustered member table gives information about the Clustered head in each destination while the routing table gives routing information.

iii) Wireless Routing Protocol (WRP)

WRP makes use of routing table at each node. Each of the nodes operates four tables namely: i. Distance table – contains information about destination, next hop distance. ii. Routing table – contains information about routing. iii. Link cost table – cost information about each neighbour and iv. Message retransmission list table which provides sequence number of the message, a retransmission counter, acknowledgement and list of update sent in update message. Whenever

there is a change in network topology, an update will be made which will be broadcasted to other nodes [6].

II. On Demand Driven Routing (Reactive) Protocol

In Reactive protocol, each router calculates route for communication only when other nodes are ready to communicate. The node initiates the process of route discovery when it is ready to send packet. When it establishes connection, it maintains the route until the node is either unreachable or is no longer needed. The route discovery occurs by mere flooding of request packets throughout network. This protocol significantly reduces routing overhead as seen in proactive protocol. Some of these protocols are Dynamic source routing (DSR), Ad hoc –On demand distance vector routing (AODV), Temporary-Ordered Routing Algorithm (TORA) and Associativity based routing (ABR) etc.

i) Ad Hoc On-Demand Distance Vector Routing (AODV)

Ad Hoc On-Demand Distance Vector Routing uses distance-vector concept. It does not maintain a routing table, but only build a routing table when a node wants to communicate with another node on demand. AODV uses three messages in its routing procedure: Route request (RREQ), Route reply (RREP) and route error (RERR). When a node wants to send data to another node in the network, the node will first of all broadcast a Route Request (RREQ) packet. When a node receives the RREQ it will in return unicast a Route Reply (RREP) to the originator of the route request (host). When there is a link breakage during communication time, a Route Error (RERR) message is used to notify other neighboring nodes of the link loss. In order to enable this reporting mechanism, each node keeps a ``precursor list", containing the IP address for each of its neighbors that are likely to use it as a next hop towards each destination.

ii) Dynamic Source Routing Protocol (DSR)

This is an on demand protocol in which source finds unexpired route to the destination in order to send packets. This type of protocol is used in the network where mobile nodes move with moderate speed thereby reducing overhead significantly. It uses three steps in routing packets (i) Routing (ii) Route discovery and (iii) Route maintenance

Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which to forward the packet. The sender explicitly lists this path in the packet's header, identifying each forwarding hop by the address of the next node to which to transmit the packet on its way to the destination host [7].

Route Discovery

Route discovery is the mechanism by which a node wishing to send a packet to a destination obtains a path to the destination. To perform this, action, node broadcasts a ***route request*** packet with a recorded source route listing only itself. Each node that hears the route request forwards the request (if appropriate), adding its own address to the recorded source route in the packet. The route request packet propagates hop-by-hop outward from the source node until either the destination node is found or until another node is found that can supply a route to the target. Each node maintains a cache of recently received route requests and does not propagate any copies of a route request packet after the first. All source routes learned by a node are kept (memory permitting) in a route cache, which is used to further reduce the cost of route discovery.

When a node wishes to send a packet, it examines its own route cache and performs route discovery only if no suitable source route is found. Naturally, if a route request packet reaches the destination node, the destination node returns a route reply packet to the source node with the full source to destination path listed.

Route Maintenance

Route maintenance is a mechanism by which a node detects a break in its source route and obtains a corrected route. Conventional routing protocols integrate route discovery with route maintenance by continuously sending periodic routing updates. If the status of a link or node changes, the periodic updates will eventually reflect the change to all other nodes, presumably resulting in the computation of new routes.

However, using route discovery, there are no periodic messages of any kind from any of the mobile nodes. Instead, while a route is in use, the route maintenance procedure monitors the operation of the route and informs the sender of any routing errors.

If a node along the path of a packet detects an error, the node returns a ***route error*** packet to the sender. The route error packet contains the addresses of the nodes at both ends of the hop in error. When a route error packet is received or overheard, the hop in error is removed from any route caches and all routes which contain this hop must be truncated at that point.

There are many methods of returning a route error packet to the sender. The easiest of these, which is only applicable in networks which only use bidirectional links, is to simply reverse the route contained in the packet from the original host. Route maintenance can also be performed using end-to-end acknowledgments rather than the hop-by-hop acknowledgments described above. As long as some route exists by which the two end hosts can communicate, route maintenance is possible. In this case, existing transport or application level replies or acknowledgments from the original destination, or explicitly requested network level acknowledgments, may be used to indicate the status of the node's route to the other node [8]..

III. Hybrid Routing Protocol

Hybrid routing protocol combines the advantages of both proactive and Reactive protocol. It uses on demand mechanism of reactive protocol and table maintenance mechanism of proactive protocol so as to avoid latency and overhead problem in the network. This protocol is most appropriate for large networks where large numbers of nodes are present. Networks are divided into zones where routing inside the zone is done by using Proactive approach and routing outside the zone uses Reactive approach. Examples of Hybrid protocol are Zone routing protocol (ZRP) and Zone-based hierarchical link state routing protocol (ZHLS).

Zone Routing Protocol (ZRP)

ZRP divides the topology into zones and seek to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols. ZRP is totally modular, meaning that any routing protocol can be used within and between zones. The size of the zones is defined by a parameter *r* describing the radius in hops. Intra-zone routing is done by

a proactive protocol since protocols keep an up to date view of the zone topology which result in no initial delay when communicating with nodes within the zone. Inter-zone routing is done by a reactive protocol. This eliminates the need for nodes to keep a proactive fresh state of the entire network.

CONCLUSION

Ad-hoc networks are special purpose autonomous nodes that can act as hosts and routers. The nodes are mobile, hence the name Mobile Ad hoc Network (MANET). As a result, MANET is said to be time varying in nature as nodes leave and rejoin the network at will. MANET is a continuously, self-configuring, self-healing, infrastructure-less network of mobile devices which communicate wirelessly. Challenges Facing Routing in Ad Hoc networks include, but not limited to: Movement of routers, Frequent link changes, Packet losses due to transmission error, Frequent update of the routing table due to mobility of nodes, Inability of the routing table to converge, Existence of routing loop. These are surmountable and make Ad-Hoc Networks very vital in mobile communication.

REFERENCES

1. Dipobagio, M. (2013), "An Overview on Ad-hoc Network", Institute of Computer Science (ICS), Freie Universität, Berlin.
2. Raza et al (2016), "Mobile Ad-hoc Networks Applications and Its Challenges", Scientific Research Publication, www.scrip.org/journal/cn.
3. Amita Pandey, A. (2015), "Introduction to Mobile Ad-hoc Network", International Journal of Scientific and Research Publication, Vol. 5, Issue 5, pp. 234 – 245.
4. Sukhpreet Kaur et al (2013), "An Overview of Mobile Ad-hoc Network Application, Challenges and Comparison of Routing Protocols", IOSR Journal of Computer Engineering, Vol. 11, Issue 5, pp. 56 – 63.
5. Aarti, D. and Tyagi, S. S. (2013), "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advance Research in Computer Science and Software Engineering, Vol. 3, Issue 5, pp. 78- 89.
6. Vijayalaskshmi, S. and Sweatha, M. (2016), "A Survey of History and Types of Manet", International Journal of Emerging Trends in Science and Technology (IJESTST), Vol. 03, Issue07, pp. 4310-4315.
7. Chitkara, M. and Waseem, A. (2014), "Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 2, pp. 432 – 437.
8. Hoebeke, J., Moerman, I., Dhoedt, B. and Demeester, P. (2014), "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", International Journal of Scientific and Research Publication, Vol. 6, Issue 6, pp. 132 – 143.