Volume 6, Issue 1, January 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Overview of Manet and Unicast Routing Protocols

Dr. S. Mythili
MCA, M.Phil., Ph.D., Associate Professor and Head
Department of Information Technology
Kongunadu Arts and Science College
Coimbatore, Tamilnadu, India

A. Anitha
M.sc (CT)., Research Scholar
Department of Computer Science
Kongunadu Arts and Science College
Coimbatore, Tamilnadu, India

Abstract— Mobile ad-hoc network (MANET) does not have any fixed infrastructure network. It is an autonomous collection of mobile nodes that communicates over the radio links. The MANET is used mostly in the rapid deployment and dynamic reconfiguration are necessary and it includes the areas such as military battlefields, emergency search, rescue operations, classrooms and conferences where the participants are allowed to share the information using their mobile devices dynamically. The devices can communicate using the wireless spectrum in a peer-to-peer fashion, and route messages with the help of the intermediate nodes or with the node itself. MANET does not a centralized administration or control over the network so before deploying, it needs to be addressed with the challenges related to security and routing. This paper provides the characteristics, advantages, challenges, applications, vulnerabilities, security goals and attacks, how the protocols are basically classified and about unicast routing protocols.

Keywords— ad-hoc network, routing protocols, proactive, reactive and hybrid

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) does not have a fixed infrastructure environment because it is a dynamic network. It has a collection of independent mobile nodes. The mobile nodes communicate through the radio range. The radio range is otherwise called as a transmission range. The mobile nodes can communicate with the other nodes. The communications between nodes are based on two categories that is direct communication and with the help of intermediate routers. The direct communication occurs between the mobile nodes if and only if the mobile nodes are within the radio range or transmission range. When the radio range or transmission range of the mobile nodes are beyond each other the communication between those nodes occurs with the help of the intermediate node which is in range. The intermediate node also acts as a router.

The mobile nodes communicate with each with the help wireless interface. MANET (Mobile Ad-Hoc Network) is a fully distributed system and it does not have a centralized control for the network administration. It works without seeking the aid from fixed infrastructure necessities like access points or base stations. The figure shows an example of Simple Ad-hoc Network [1]

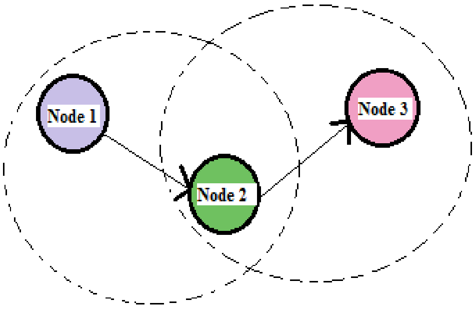

Fig. 1 Example of Simple Mobile Ad-Hoc Network

The Fig. 1 represents the mobile nodes such as Node1 and Node3 want to communicate with each other but both the nodes are not within the radio range to establish a direct communication. Hence, it gets the aid from Node2 which acts as an intermediate node in order to forward the packet from Node1 to Node3 by establishing the connection between these two nodes. Node2 behave as a router and these nodes that is Node1, Node2 and Node 3 together forms a Simple Mobile Ad-hoc Network.

The maturity of wireless transmissions and familiarity of portable computing devices have made the impossible thing possible of making the communication between devices at anyplace irrespective of time [2]. A MANET is an autonomous collection of mobile devices through which the communication occur with each other over wireless links and willing to help in a distributed manner in order to make use of the availability of the necessary network functionality even in the absence of a fixed infrastructure network. The mobile devices form a self-creating, self-organizing, selfadministering wireless network that can be rapidly deployed with minimum user intervention then this is called as MANET.

A. MANET Characteristics

The mobile ad-hoc network characteristics are listed as follows:

- **Distributed Operation:** The network is distributed and it does not have a centralized control on the network. This should implement the special functions for host configuration, routing and security purposes. Because of the absence of the centralized firewall.
- **Multi-Hop Routing:** When a source node wants to send information to the destination node and both these nodes are out of its communication range or radio range then there in of the intermediate nodes which acts as a router to forward the packet from source to destination.
- **Autonomous Terminals:** The nodes in the MANET functions as a host as well as the router. Because the nodes in the MANET are independent nodes.
- **Dynamic Topology:** The nodes are free to move in varying speeds so the network topology will also be changed randomly and continuously at unpredictable times. Being independent nodes the routing is been established dynamically among themselves as they travel around, establishing their own network.
- **Light-Weight Terminals:** The CPU capability of the nodes is very less. Then the power storage and the memory size of the nodes are also very low.
- **Shared Physical Medium:** Any entity can have the accessibility to the wireless communication medium by having the necessary equipment and adequate resources for accessing it.
- **Bandwidth-Constrained:** There will be fluctuation in the bandwidth of the wireless links. It is because of the reliability, efficiency, stability and capacity of wireless links are often inferior to the wired links.
- **Minimum Human Intervention:** The mobile nodes with the spontaneous behaviour which needs only minimum human intervention in order to configure the network.
- **Symmetric Environment:** Each and every node has the same features with similar responsibilities and capabilities. So it forms a symmetric environment.
- **Mobility:** There is a high user density and large level of user mobility. The nodal connectivity will be happening at irregular intervals.

B. MANET Advantages

The following are the advantages of ad-hoc network. They are

- Without considering the geographical area it provides the access to the information and services.
- There is no centralized control over network administration because it is a self-configuring network.
- It is less expensive when compared to wired network.
- It is scalable; the reason is it accommodates the addition of more nodes.
- Flexibility is been improved.
- Network can be set up at any place and any time.

C. MANET Challenges

The following are the challenges of MANET. They are

- **Limited Bandwidth:** The bandwidth used in this network is of lower capacity than the infrastructure networks.
- **Dynamic Topology:** Routing is established dynamically and this may disturb the relationship trust among the nodes.
- **Routing Overhead:** The stale routes are been generated in the routing table which leads to routing overhead. This happens due to the frequent change of the nodes location within the network.
- **Hidden Terminal Problem:** The nodes that are hidden from the sender of a data transmission session, but are reachable to the receiver of the session this results in the simultaneous transmission of those nodes which leads to collision of packets.
- **Packet Losses Due to Transmission Errors:** There is will be high packet loss due to increased collision, hidden terminals, interference, uni-directional links and frequent path breaks.
- **Mobility-Induced Route Change:** The frequent path breaks due leads to frequent route changes.
- **Limited Resources:** The mobile nodes are dependent on the battery power and the memory capacity and power are severely limited.
- **Limited Physical Security:** It implies on higher security risks such as peer-to-peer network architecture or a shared wireless medium accessible to both the justifiable network users and malicious attackers. So the attacks like eavesdropping, modification, jamming and denial-of-service and other attacks should be taken into concern.
- **Autonomous:** Managing the operation of various mobile nodes is not possible in the absence of centralized network administration.
- **Device Discovery:** The automatic optimal rote selection needs the dynamic updating by identifying the newly moved in nodes and providing information about their existence.
- **Poor Transmission Quality:** Many error sources that result in the degradation of the signal which is been received.

- **Ad-hoc Addressing:** The challenges in standard addressing scheme to be implemented.
- **Network Configuration:** The infrastructure is dynamic and leads to dynamic connection and disconnection of the variable links.
- **Topology Maintenance:** To maintain the updating information of dynamic links among nodes is a great challenge.

II. APPLICATIONS OF MANET

The following table provides an overview of present and future MANET applications, partially based on [3, 4]:

- **Military Battlefield:** The military take advantage of the common place network technology to maintain information between the soldiers, vehicles, and military information headquarters.
- **Commercial Sector:** Electronic payments are made anytime and anywhere environments with the help of e-commerce. In the field of business the mobile offices and dynamic accessibility of the database is possible. It also provides vehicular services such as transmission of road and climatic conditions, network for the taxi cabs, inter-vehicle networks. It is also used for rescue operations for disaster relief efforts.
- **Local Level:** Ad-hoc networks can autonomously link an instant and temporary multimedia network using palmtop computers in order to share and spread information among participants at e.g. conference or classroom. Local level application might be in home or office wireless networking.
- **Personal Area Network (PAN):** The short-range of MANET can simply the intercommunication between various mobile devices. Ad-hoc network extend the access to the Internet or other networks by WLAN, GPRS and UMTS. It is a promising application field of MANET.
- **Collaborative Work:** For business environments, the need for collaborative computing might be more important outside office atmosphere than inside because the people do need to have outside meetings to cooperate and exchange information on a given project.
- **Civilian Sector:** Ad-hoc network in sports stadiums, trade fairs and shopping malls. And also in the networks of visitors at airports.
- **Education:** Ad-hoc communications during meetings or lectures, virtual classrooms, universities and campus environments.
- **Entertainment:** Multi-user games, wireless peer-to-peer networking, outdoor Internet access, robotic pets, and theme parks the ad-hoc network is of great use.
- **Sensor Networks:** Home applications such as smart sensors and actuators embedded in consumer electronics. The data tracking environmental conditions, animal movements, chemical or biological detection.
- **Context Aware Services:** Follow-on services such as call-forwarding, mobile workspace. Information services such as location specific services and time-dependent services. Infotainment such as tourist information.
- **Coverage Extensions:** Extending cellular network access. Linking up with the Internet.

III. MANET VULNERABILITIES

It is a weakness in security system. A particular system is also liable to unauthorized information manipulation as a result of the system doesn't verify a user is a licensed or unauthorized before permitting the info access [5].

Mobile ad-hoc network is vulnerable than a wired network. Some of the vulnerabilities are listed below:

- **Lack of Centralized Management:** MANET does not have a centralized network administration. Hence, there is no monitor server which results in the difficulty of detecting the attacks as well it is not an easy job to monitor traffic in a dynamic and large scale ad-hoc network. It will impede trust management for nodes.
- **No Pre-defined Boundary:** In mobile ad-hoc networks, to define a physical boundary of the network is impossible. The nodes in the ad-hoc network can join and leave the wireless network due the migrant environment that they work in.
- **Cooperativeness:** Routing algorithm for MANET's usually assumes that nodes are cooperative and non-malicious. This result a malicious attacker can easily become a vital routing agent and disturb the network operation fail to obey the protocol specifications.
- **Resource Availability:** It is a major issue in MANET. It is because of providing secure communication in a dynamic environment and also it protects specific threats and attacks, which leads to development of various security plans and architectures. The ad-hoc environments also permit the deployment of self-organized security mechanisms.
- **Scalability:** Due to the mobility of the nodes, scale of ad-hoc network changing all the time. So scalability is an issue that concerning with the security. Security mechanisms ought to be capable of handling an outsized network also as tiny ones.
- **Limited Power Supply:** The nodes in mobile ad-hoc network have to be compelled to think about restricted power provide, which is able to cause many issues. When there is limited power supply the nodes in the ad-hoc network behaves in a selfish manner.
- **Dynamic Topology:** Dynamic topology and adjustable nodes membership may interrupt the faith in relationship between the nodes. The trust may get interrupted if some nodes are detected as compromised. This dynamic behaviour might be higher protected with distributed and adaptive security mechanisms.

- **Bandwidth-Constraint:** The variable low capability links exists as compared to wireless network that are additional at risk of external noise, interference and also the strength of the signal gets reduced.
- **Adversary inside the Network:** The mobile nodes within the MANET can freely be a part of and leave the network. The nodes within the network may also behave as malicious nodes but it very difficult to detect. Thus this attack is more dangerous than the external attack.

IV. SECURITY GOALS

The goals to evaluate the mobile ad-hoc network are secure or not are listed below [1, 3]:

- **Confidentiality:** It ensures that the computer related assets are accessed only by authorized parties. It is the protection of information that is exchanged via MANET. It should be protected against the disclosure attack like eavesdropping that is unauthorized reading of the message.
- **Availability:** It means the assets are accessible to authorized parties at appropriate times. It applies both the data and services. It ensures the durability of network service despite denial of service attack.
- **Integrity:**It means the assets can be modified only in an authorized way by the authorized parties. It should ensure that the message being transferred is not corrupted.
- **Authentication:** It is essential to assure that the participants in the communication are authenticated and not impersonators. The resources of network must be accessed only by the authenticated nodes of the network.
- **Authorization:** This is a property that assigns various access rights to users of various types. For example, a network management can be performed only by the network administrator only.
- **Resilient to attacks:** It is required to sustain the network functionalities even when a portion of nodes is compromised or destroyed.
- **Freshness:** It should ensure that the malicious node does not resend previously captured packets.
- **Non-repudiation:** It ensures that the sender and receiver of a message cannot deny any responsibility that they have ever sent or received such a message. This is helpful when we need to recognize difference if node with some undesired function is compromised or not.
- **Anonymity:** It means all information that can be used to identify current user of the node by default it should kept private and not to be distributed by the node itself.

V. SECURITY ATTACKS

Based on the behaviour the attacks are classified into two types. They are passive and active attacks [1].

A. Passive Attacks

The data is not modified when it is transmitted within the network but it leads to the unauthorized listening to the network traffic. The passive attacker will not interrupt in the operation of a routing protocol but tries to discover the important information form routed traffic.

B. Active Attacks

It is a very severe attack on the network because it prevents the flow between the nodes. Active attacks are classified into two types. They are active internal attacks and active external attacks. The active internal attacks are caused by the malicious nodes which are a part of the network and this is severe attack and very hard to detect when compared with the active external attack. The active external attacks are carried out by the sources available outside that is which is not belonging to the network. These attacks provide the unauthorized access to network that helps attacker to make changes like modification of packets, congestion and so on. The active attacks are further classified into three groups.

1) Dropping Packets: The selfish nodes can drop all the packets that are not destined to them. This prevents the end-to-end communication between the nodes.

2) Modification Attacks: These attacks modify the packets and disturb the overall communication between the nodes in the network.

3) Fabrication Attacks: In this type of attack, the fake message is send to the neighbouring nodes by the attacker.

VI. PRELIMINARY CLASSIFICATION OF ROUTING PROTOCOLS

The dynamic nature of a mobile ad-hoc network results in frequent and dynamic network topology, adding difficulty and complexity to the routing between the mobile nodes. There are numerous routing protocols and algorithms have been introduced to perform under different network environments and traffic conditions. According to the property which is termed as type cast the routing protocols are classified they are Unicast, Geocast, Multicast or Broadcast forwarding [6].

- **Unicast:** The unicast routing protocols means a one-to-one communication that is one node transmits data packets to another node. This the largest class of routing protocols found in the ad-hoc networks.
- **Multicast:** The multicast routing protocols means a one-to-many communication that is one node wants to send the same message or stream of data to multiple destinations. The nodes may join or leave the network in the multicast group as desired.
- **Geocast:** These types of routing protocols are the special case of multicast routing protocols that is used to deliver the data packets to a group of nodes that is presented inside the specified geographical area. The nodes can join or leave a geocast group either by entering or leaving the corresponding geographical region.

VII. AN OVERVIEW OF UNICAST ROUTING PROTOCOLS

The primary goal of the unicast routing protocols is the correct and efficient route construction and maintenance between a pair of nodes are the messages are delivered correctly and in a timely manner. The MANET routing protocols operate in networks with dynamic topologies where routing algorithms run on resource constrained devices. The MANET routing protocols must have to optimize the limited resources and cope with dynamic topologies. The other vital features for a routing protocol are: scalability, supporting unidirectional links, security and reliability, and Quality of Service support [6].

MANET unicast routing protocol are mainly classified into two categories. They are proactive routing protocols and reactive routing protocols. There is another class of unicast routing protocol is hybrid routing protocol.

A. Proactive Routing Protocols

The proactive routing protocols are same as the Internet routing protocols such as Routing Information Protocol (RIP), Distance-Vector (DV), Open Shortest Path First (OSPF) and link-state [3]. Each node has to maintain one or more tables to store routing details and any changes in the network topology need to be reflected by generating updates in every part of the network in order to maintain a consistent network perspective. They attempt to maintain consistent, up-to-date routing information of the whole network. It minimizes the waiting time of communication and allows nodes to determine which nodes are available in the network. The route construction and maintenance are performed through both periodic and event-driven messages.

As the routing information is maintained in the form of tables, these protocols are sometimes referred to as Table-Driven protocols. The following are the few types of the proactive ad-hoc routing protocols are: Destination-Sequenced Distance-Vector, Optimized Link State Routing, Topology Broadcast Based on Reverse-Path Forwarding, Cluster-Head Gateway Switch Wireless Routing Protocol, Fisheye State Routing [6].

- **Destination-Sequenced Distance-Vector (DSDV):** It is a distance-vector protocol. Every node maintains a routing table with one entry for each destination in which the shortest path route that is recorded. The destination sequence number is used in order to avoid routing loops. A node increases its sequence number whenever a change occurs in its nearby node. This number is used to select among the alternatives routes for the same destination. The route which contains the greatest number is selected by the nodes which are used in selecting the latest information.
- **Optimized Link State Routing (OLSR):** It is an IP routing protocol optimized for MANETs also used in WANET. It is a proactive link state routing protocol. The important point of the optimization is the multipoint relay (MRP). The MRP is identified by each node. When exchanging link-state routing information, a node contains the list which has the connections to those neighbours only and that have been selected it as MRP that is Multipoint Relay Selector Set. The protocol selects the bi-directional links for routing, hence avoiding packet transfer over the unidirectional links.
- **Topology Broadcast Based on Reverse-Path Forwarding (TBRPF):** It uses distance vector routing and there is no data available about routing. It is a link-state routing protocol for wireless mesh networks and it is similar to OLSR. Each node computes a shortest path tree to all other nodes, only a part of the tree is propagated using its bandwidth.
- **Cluster-Head Gateway Switch Routing (CGSR):** It is a protocol where nodes are grouped into clusters. In on-demand routing protocols, a route creation is initiated by the source when the source wants to communicate to the destination. It increases the scalability of the protocol. The priority token scheduling method and gateway code scheduling method and path reservation method are used as additional methods in order to increase the performance. The performance is affected because of the dynamic environment.
- **Wireless Routing Protocol (WRP):** It is a loop-free protocol and destination based protocol. It belongs to the class of path finding algorithms. This algorithm that utilizes the information about the distance and second-to-last hop (predecessor) along the path to each destination. It consists of four tables to maintain the details such as distance, link cost, routes and message transmission information.
- **Fisheye State Routing (FSR):** The routing details are based on the closer and far away nodes. The accuracy of the route is less for the far away nodes and accuracy of the route increases for the closer nodes. It is used for intra-group routing.

B. Reactive Routing Protocols

It is also known as source-initiated on-demand driven routing protocol since they do not maintain routing information will be in the network nodes if there is no communication. It uses a route discovery process to overflow of the network with route query requests when a packet needs to be routed using source routing or distance vector routing. Some of the reactive ad-hoc routing protocols are: Dynamic Source Routing, Ad-hoc On Demand Distance Vector, Temporally Ordered Routing Algorithm , Associativity Based Routing, and Signal Stability Routing [6].

- **Dynamic Source Routing (DSR):** This protocol is used for wireless mesh networks and the packet forwarding depends on source routing. It is a source based, on demand routing protocol and also loop-free. It has the route cache contains the source routes learned by the node. The route discovery occurs if and only if the route cache has an invalid route. The route cache is updated consecutively. It needs larger control overhead and memory requirements than AODV. Because DSR packets carry full routing information. It uses both asymmetric and symmetric links during routing. The route cache maintains multiple routes which help in the link failure.

- **Ad-hoc On Demand Distance Vector (AODV):** It is an improvement of DSDV and used in MANET and WANET. The route creation is based on-demand. It does not have a complete route list details like DSDV. The route discovery process is similar to the DSR. There is no larger control overhead and memory requirements than DSR. Because AODV packets contain only the destination address. At times this will create a problem during link failure. It works only on symmetric links.
- **Temporally Ordered Routing Algorithm (TORA):** It is localization of control messages to a very small set of nodes near the happening of a topological change. To finish this, nodes need to maintain the routing details about adjacent (one hop) nodes. This protocol performs three functions: route creation, operation and maintenance. It is a source-initiated and on-demand routing and also loop-free protocol. It has efficient bandwidth with highly adaptive and quickly do the route repair during the link failure and multiple routes are available. It is suitable for large, highly dynamic mobile ad-hoc environments.
- **Associativity Based Routing (ABR):** It is also a loop-free protocol. It has the new routing metric used in route selection that is degree of association stability. The route is discovered using the longer-lived route, stable and requiring less updates.
- **Signal Stability Based-Adaptive Routing (SSA):** It presents a totally different appeal from most other routing algorithms. The most important criteria is the usage of signal and also the stability of the location. The routing framework that works like on-demand routing algorithms that is route requests are broadcast through the network, the destinations provides the route replies, routes are set up accordingly. The route selection uses an added property called signal strength of the link.

C. Hybrid Routing Protocols

It combines the approaches of both proactive and reactive protocols. It is used to combine a set of nodes into zones in network topology. The network is then partitioned into zones. The route to destination within the same zone is established without any delay. In case of other zones, it needs a route discovery and route maintenance procedure to establish a connection to the destination to route packets. It is used for large networks. The hybrid ad-hoc protocol is Zone Routing Protocol (ZRP) [6].

- **Zone Routing Protocol (ZRP):** It is a Zone Based Hierarchical Link State Routing Protocol. It is the combination of proactive and reactive protocols. It has the advantage of both protocols. It defines that each node with a zone and it contains the neighbours within the number of hops. The proactive and reactive algorithms are used to route the packets both in and out of the zones.

VIII. CONCLUSION

The reactive protocols are more powerful than the proactive protocols. Because the reactive protocols reduce the control overhead and power consumption the reason is the routes are only established on requirement basis. In reactive protocols the source node needs to wait for the route discovery process before communication occurs. The time taken for the route discovery process is high and mostly not applicable for the real-time communications. It works well in medium sized networks. This protocol results in more scalable solution. In contrast, the proactive protocols need periodic route updates to keep information current and consistent and also it contains multiple routes which are not needed results in routing overheads. It provides a better quality of service than the reactive protocols. The routing information is constantly updated and the routes to every destination are available always and up-to-date which reduces the end-to-end delay. It is suitable for only a small-scale static network. The hybrid protocol is used for large scale network and it has the advantages of both reactive and proactive protocols. Based on the network size and usage the protocols are used. The following table shows the comparison of the unicast routing protocols [7].

TABLE I COMPARISON BETWEEN PROACTIVE, REACTIVE AND HYBRID ROUTING PROTOCOLS

Parameters	**Proactive**	**Reactive**	**Hybrid**
Routing Philosophy	Flat or Hierarchical	Flat	Hierarchical
Routing Techniques	Table driven	On-demand	Combination of both
Overhead in Routing	High	Low	Medium
Route availability	Always Available	Set up when needed	Depends upon the destination's location
Latency	Low	High	Zone dependent
Periodic Updates	Yes	No	Required inside the zone
Storage need	Low	Depends upon the number of routes kept	Depends upon the size of the zone
Scalability	Scalable	Not scalable, suitable only for small network	Scalable to large network

REFERENCES

[1] Aarti and Dr. S.S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Secutiry Attacks," International Journal of Advanced Research in Computer Science and Software Engineering, Volume-3, Issue-5, May 2013.

[2] Ilyas, "The Hand Book of Ad-hoc Wireless Networks", CRC Press LLC.

[3] EshaSehgal and SohanGarg, "Mobile Ad-hoc Networks (MANETs): Challenges, Applications and Security Goals with Minute Introduction of Routing Protocols," International Journal of Advanced Research in Computer Science and Software Engineering, Volume-3, Issue-8, August 2013.

[4] Vikas Kumar, AmitTyagi, Amit Kumar, "Mobile Ad-hoc Network: Characteristics, Applications, Security Issues, Challenges and Attacks," International Journal of Advanced Research in Computer Science and Software Engineering, Volume-5, Issue-1, January 2015.

[5] PriyankaGoyal, VintiParmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Applications," International Journal of Computational Engineering and Management, Volume-11, January 2011.

[6] ImrichChlamtac, Macro Conti and Jennifer J.N. Liu, "Mobile Ad-hoc Networking: Imperatives and Challenges," Elsevier, Ad-hoc Networks 1(2003) 13-64.

[7] Anil Saini, Vinod Kumar, "Mobile Ad-hoc Networking Routing Protocols: Comparative Study," International Journal of Enhanced Research in Science Technology & Engineering, Volume-2, Issue-12, Decemeber 2013.