Bandwidth Efficient Multicasting Operation in AODV Protocol for Mobile Ad-Hoc Networks

Gurpreet Singh Bagga¹, Mritunjay Kumar Rai²

¹Student
Department of Electronics and Communication
Lovely Professional University
Phagwara, Punjab, India

²Associate Professor
Department of Electronics and Communication
Lovely Professional University
Phagwara, Punjab, India

ABSTRACT

Multicasting technique provides an important service for improving throughput, bandwidth and delay of distributed systems and applications. In unicast and broadcast transmissions there is wastage of bandwidth, so multicasting transmission approach is used to deliver the data from sender to group of destinations. Reactive routing protocol is used for the route establishment from source to destination only when it is required. AODV and DSR are the reactive routing protocols which uses flooding approach for establishing the route from source to destination. In this approach network resource like bandwidth, node energy has been wasted. To overcome this problem, flooding approach will be replaced with the multicasting approach and outcomes are efficient in reducing delay, improving throughput.

Keywords: Adhoc Network, Analysis, AODV, DSR, MANET

1. INTRODUCTION

1.1 AD HOC NETWORK

Ad hoc wireless networks are the decentralized type of network. In ad hoc network resource management and routing between source to destination is done using distributed approach in which coordination of each node requires to enable communication. ad hoc network is used in urgent situation. No fixed infrastructure like base station is needed in ad hoc network. Ad hoc use multi hop technique for communication [1].

1.2 CHARACTERISTICS OF AD HOC NETWORKS

The main characteristics [1] of ad hoc networks are as follows:

I. A temporary network consists of collection of mobile nodes.
II. Network topology can change regularly and suddenly.
III. No centralized administration is present.

IV. Each host is able to act as an independent router.
V. As network interfaces hosts use wireless RF transceivers.
VI. It is self-organizing network in nature.
VII. Ad hoc wireless network use multi-hopping technique.

1.3 CLASSIFICATION OF AD HOC NETWORKS

Two types of classification in ad networks are:

I. Single-hop
II. Multi-hop

I. Single-hop In the single hop there is direct path between source and destination nodes and both nodes are in range of each other and more chances of link failure [1].

II. Multi-hop

In the multi hop source and destination nodes are communicating with the help of intermediate nodes not directly.

1.4 ADVANTAGES

I. It becomes very easy and fast for setting up a wireless system and it vanish the need of wires and cables.

II. Wireless networks is able to extended to those places where wired cannot be.

III. It adapts easily, flexibility to make changes in the configuration of network.

Fig. 1: Infrastructure less Mode
1.5 TYPES OF AD HOC NETWORK
There are different types of ad hoc network available. These are following:
I. MANET
II. Wireless Sensor Networks (WSN)
III. Wireless Mesh Networks (WMN)
I. MANET (mobile ad hoc network) consists of self-configuring nature of mobile nodes. It is infrastructure less network. In Manet different numbers of mobile nodes are connected through wireless medium. Each mobile node is free to move anywhere in network i.e. no central controller is available [7].

Fig.2: Diagram of MANET

II. WIRELESS SENSOR NETWORK
Wireless sensor networks provide the infrastructure less wireless communication among sensors which is deployed for particular application. It consists of sensors (sensing devices) that can be wirelessly communicated. Each sensing device has capability to talk to its peer, sense the physical Parameters, and process the gathered data.

III. WIRELESS MESH NETWORK
Wireless mesh network is used to provide the alternate communication network to the fixed or mobile clients without the use of network planning and spectrum reuse concept. Mesh topology provides many alternate paths for communication between sources to destination. When existing path fails then it reconfigure new path quickly.

1.6 ISSUES IN AD HOC WIRELESS NETWORKS
Major issues and challenges that affect the performance of ad hoc wireless network are as follows [5]:
I. Mobility: in ad hoc network due to mobility of nodes it results in frequent path breaks, packet collision and difficulty in resource reservation.
II. Distributed operation: ad hoc network needs to operate in an environment where no Centralized coordination is possible.
III. Robustness: multicast routing protocol must be able to reconfigure its path quickly from frequently path breaks due to mobility of nodes.
IV. Efficiency: efficiency is very important in multicast routing protocol because bandwidth is limited efficiency is total number of packet received by receiver to total number of packet transmitter.
V. Quality of service: certain qos parameter which are demanded are bandwidth, delay, jitter, packet delivery ratio and throughput.
VI. Efficient group management: the process of accepting multicast session members and maintaining connectivity among them until session expires.
VII. Scalability: routing protocol should be able to perform efficiently in a network with large number of nodes.
VIII. Security: multicast protocol must have capability to avoid resource consumption and prevent non-members from gaining unauthorized information.
IX. Resource management: mobile nodes have limited battery so multicast routing protocol should use minimum power by reducing number of packet transmission and node should go to sleep mode when not in use.

1.7 TYPES OF MANET
1. Vehicular Ad Hoc Networks (VANETs): It is used for the communication among the mobile vehicles. Thus the communication being carry on even if the vehicles are moving in the different direction with in a particular area[1].
2. Intelligent vehicular ad hoc networks (InVANETs): It is used in case like collision of vehicles or any other types of mobility problems. It uses the scheme intelligently and the flow less communications goes on.
3. Internet Based Mobile Ad hoc Networks (iMANET): It is an ad hoc networks that connection mobile nodes and fixed nodes of Internet-gateway. Ad hoc routing algorithms don’t apply directly in such type of networks.

1.8 ATTACKS ON MANET
There are two types of attacks are present in MANET which break the security of the networks. These attacks are as follow:
Passive Attacks
Active Attacks
1. Passive Attacks: A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection. In its, operations are not affected. The operations supposed to be accomplished by a malicious node ignored and attempting to recover valuable data
during listens to the channel. Examples of Passive Attacks are eavesdropping, snooping [8].

2. Active Attacks:

An active attack is that attack which any data or information is inserted into the network so that information and operation may harm. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing [8].

Other types of attack are as follow:

1. Internal Attack: Internal attacks are as of compromised nodes that are part of the set of connections. In an internal attack from the network the malicious node gains unauthorized access and behave as a genuine node. Traffic can be analyze between other nodes and may participate in the activities of other networks [9].

2. External Attack: The external attack is concealed out by the nodes which do not belong to network. It may cause unavailability and congestion by sending false information for the network.

3. Denial of Service Attack: The aims of attack are to hit the accessibility of a node and all the nodes in the entire network. The services will not be accessible if the attack is successful. The attacker generally uses battery exhaustion method and radio signal jamming [9].

4. Wormhole Attack: It is a network layer attack. In wormhole attack, a malicious node, at one location in the network receives packets and to another location in the network tunnels them, to the location where packets are present into the network. The two colluding attacker’s tunnel between them is referred as wormhole [10]. When the control messages are routing are tunneled it create disrupted.

5. Black hole Attack: In this type of attack the requests is listen by an attacker for the routers in a flooding based protocol. When a request is received by the attacker to the destination node for a route, it creates a reply for the short route and enters into the passageway to do something with the packets passing between them [10].

6. Byzantine Attack: In this attack, a intermediate compromised node carries out attacks such as creating collision forwarding packets on non-optimal paths, routing loops, and dropping packets selectively which result in interruption or dreadful conditions of the routing services [11].

7. Replay Attack: In this type of attack an attacker performs a replay attack are repeatedly re-transmitted the valid data to the network injection fort routing traffic that has been previously captured. This attack targets the routes freshness and determines poor security design [11].

8. Jamming: In this attack, attacker wireless medium keep monitoring initially in sort to verify frequency at which destination node is getting signal from sender. Signal is transmit on that frequency to hindered error free receptor.

9. Man-in-the-middle attack: In this attack, an attacker sits between the sender and receiver and any information being sent between two nodes sniffs by him. In some cases, attacker may masquerade as the sender to communicate with receiver or masquerade as the receiver to reply to the sender.

10. Gray-hole attack: This attack is also known as routing misbehavior attack. It leads to messages dropping. It has two phases. In the first phase a valid route to destination is advertise by nodes itself. In second phase, with a certain probability nodes drops intercepted packets

11. Eavesdropping: It is another kind of attack that often happens in the mobile ad hoc networks. Eavesdropping is done to obtain some information that is confidential and keep secret during the communication. The confidential information may consist of the public key, location, private key and id passwords of the nodes. It should be kept away from the unauthorized access because such data are very important to the security state of the nodes.

1.9 ROUTING PROTOCOLS IN MANET

Routing protocol indicates that how to communicate with the help of routers. It shares information among intermediate nodes then with the whole network. It helps to search shortest path from source to destination. There are mainly two types of routing protocol available[ 4].

I. Proactive Protocol (Table-driven)

II. Reactive Protocol (On-demand)

1.9.1 PROACTIVE ROUTING PROTOCOL

In Proactive protocol all nodes maintain fresh list of the route and their destination from source in the form of tables. Routing information is flooded in whole network and path finding algorithm applies when source wants path to destination. All the nodes are updating their table regularly. If the topology frequently changes than update information propagate to each node and table is updated.

I. Destination sequence distance vector (DSDV).

It is table driven protocol in which route to all the destinations are present at each node. At a regular interval of time tables are exchanged between the neighbors. Every node maintains a routing table that has lists of all available destinations, the assigned sequence number by the destination node and the number of hops to reach the destination. The sequence number is used to distinguish old routes from new ones and to avoid the loops formation. The periodically stations transmit their routing tables to their instant neighbors. If a significant amount of change has occurred in its table from the last update then station
also transmits its routing table. If two routes have the same sequence number then the route with the shortest route is used. DSDV does not support multi-path routing. It provides shortest path of good quality, trustworthy and cooperative.

Tables are updated with two types, incremental and full dump.

Incremental update is used when nodes do not observe changes in local topology.

Full dump is used when there is a change in local topology.

1.9.2 REACTIVE ROUTING PROTOCOL

It is an on-demand routing protocol. It finds the path only when it is required. These protocols do not maintain network topology information and do not exchange information periodically. It maintains a table only on demand. Route discovery is followed to find the path. These are bandwidth efficient protocols. In this protocol, route request packet is sent across the network and route reply message comes from intermediate nodes. Route error message is issued by nodes if the link is broken. Its disadvantage is when flooding is excessive then congestion occurs [2].

I. AD HOC ON-DEMAND DISTANCE VECTOR

It is an on-demand routing protocol, meaning that a path from source to destination is created only when it is required. It uses the destination sequence number to find the up-to-date path to the destination and to find the most recent path. In AODV, source and intermediate nodes store the next hop information [3]. If the destination sequence number of the current received packet is greater than the previous number only then the node updates itself.

Three messages define in AODV: Route Requests (RREQ), Route Errors (RERR) and Route Replies (RREP). These messages are used to discover the route and maintain routes across the network from source node to destination [2].

2. OVERVIEW TO MULTICAST

In multicasting technique, it sends the information just once to multiple users and it can produce large savings in bandwidth. Copies of the message are made only when the paths diverge at a router, as when the message is supposed to be passed on to another router. Nodes use the IGMP (internet group management protocol) to inform multicast-aware routers of any multicast sessions in which they want to participate or terminate. If all members of a multicast group on a particular network segment leave the group, then the router ceases to forward multicast data to that segment.

Without support of multicasting technique, multiple copies of the same message are transmitted again and again on the same link. In this way, more bandwidth is required for transmission.

By using multicasting technique, only a single copy of the same message is transmitted from the source. Multicast routers have the capability to duplicate the packets.
2.1 MULTICAST PROCESS

The client node sends an IGMP (internet group management protocol) join message to its designated multicast router. The destination MAC address maps to the Class D address of group being joined, rather being the MAC address of the router. The router receives the join message and uses multicast routing protocol to add this client to the multicast distribution tree. The switch receives the multicast packet and examines its forwarding table. If no entry exists for the MAC address, the packet will be flooded to all ports within the broadcast domain. If an entry does exist in the switch table, the packet will be forwarded only to the designated ports. Multicast routers also periodically send an IGMP query to the “all multicast hosts” on the subnet to determine which groups are still active within the subnet.

2.2 APPLICATIONS

Teleconferencing (audio, video, shared White board, text editor), news, sports, weather updates, stocks, distance learning, Web-cache updates, Push-based systems, Software distribution, Multi-player games, Server/service location, Other distributed applications [6].

3 CONCLUSION

The path from the source to destination is established with the routing protocols such as Proactive and Reactive protocols. In the Proactive routing protocols each node maintain the information of network topology in the form of tables and it exchanges the routing information periodically. In the whole network routing information is flooded and when it requires path uses path-finding technique. In the MANET, it is very difficult to maintain such tables-driven routing protocol due to its self-configuring nature of nodes. In such cases another type of routing protocol, i.e. Reactive routing protocols is used for the route establishment. In reactive routing protocols routes are established between source and destination only when required. AODV and DSR are two most common type of protocols which are used for the route establishment. In AODV routing protocol dijkstra's algorithm is implemented. Protocols like DSR and AODV use the flooding approach for the route establishment. The RREQ messages are flooded into the network, and intermediate nodes which are having the path to destination reply with the RREP message and best path is selected on the basis of sequence number and hop-count. In this approach, the network resources like bandwidth, node energy get wasted. To overcome the problem, of flooding approach will be replaced with the multicasting approach.

4. REFERENCES