Volume 6, Issue 4, April 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Multicasting in Mobile Adhoc Networks

Amandeep Chhabra, Geeta Arora

Department of Computer Science and Engineering, U.I.E.T, K.U.K,
Haryana, India

Abstract: Multicast enables efficient large scale content distribution by providing an efficient transport mechanism for one to many and many to one communication. Multicast communication is an efficient means to support key network applications such as real-time teleconferencing and data dissemination. The success of wireless ad hoc networks and the increasing interest in multimedia applications explain the need of multicast protocols adapted to the wireless environment. In the paper, we first introduce the design considerations for a multicast protocol in a wireless ad hoc network. We then present a classification of multicast protocols.

Keyword: CIDR, RFC, BCP, DNS

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs)[8] are increasingly employed in both military and commercial network situations where fixed infrastructure is too costly or dangerous to deploy. Multicast plays an important role in MANET. Many ad hoc network applications need the nodes to work as a group to carry out a given job. This kind of application is efficient due to the broadcast nature of wireless network for it can improve the efficiency of the wireless links. As a result, multicast routing has become a research focus recently, and various multicasting protocols in MANET have been proposed. Multicast communication as defined in [1] is an efficient means of distributing data to a group of participants. In contrast to unicast communications, multicast routing permits a single IP datagram to be routed to multiple hosts with minimal redundant transmission within a network. Membership in a multicast group is often highly dynamic, with receivers entering and leaving the multicast session without the permission or explicit knowledge of other hosts. The inherent cost and resource benefits of multicast routing and data delivery are clear; however, the group-oriented communication paradigm presents new and unique technical challenges beyond traditional network security approaches.

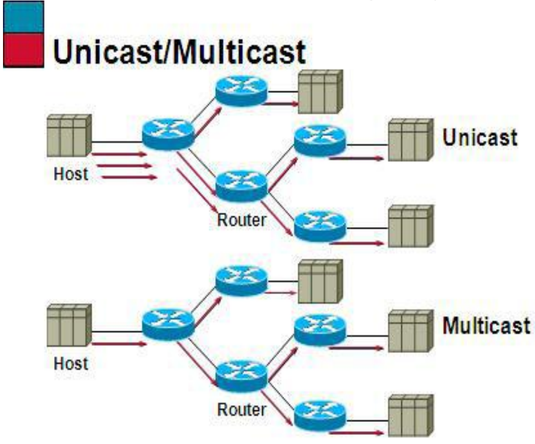


Fig 1: Unicast & Multicsat Routing

II. PROPERTIES OF MULTICAST

The definition of the host group model [10] provides a summary of the key properties of multicast: a host group is a set of network entities sharing a common identifying multicast address, all receiving any data packets addressed to this multicast[9] address by senders (sources) that may or may not be members of the same group and have no knowledge of the groups and membership. This definition highlights the three main properties of multicast:

- All members receive all packets sent to the address: Multicast routing delivers all packets sent to the multicast address to all members of the multicast group.
- Open group membership: Multicast provides an open group model and allows group membership to be transparent to the source.
- Open access to send packets to the group: Any host can send data to the multicast address, and it will be delivered to the multicast group without regard for the source of these packets.

Multicst Addressing

IPv4 multicast addresses are defined by the leading address bits of 1110, originating from the class D network design of the early Internet when this group of addresses was designated as Class D. The classless Inter-Domain Routing (CIDR) prefix of this group is 224.0.0.0/4. The group includes the addresses from 224.0.0.0 to 239.255.255.255. Address assignments from within this range are specified in an Internet Engineering Task Force (IETF) [2], Best Current Practice document, BCP 51, also known as RFC 3171.

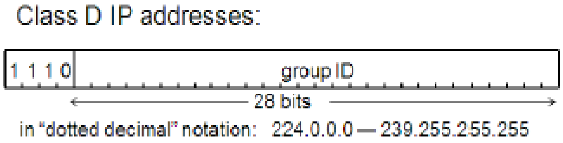


Figure 2: Class D IP Address.

The address block 224.0.0.0/24 (224.0.0.0 to 224.0.0.255) is designated for multicasting on the local local area network only. For example, the Routing Information Protocol (RIPv2) uses 224.0.0.9, Open Shortest Path First (OSPF) uses 224.0.0.5, and Zeroconf m DNS uses 224.0.0.251. The notion of group is essential to the concept of multicasting.. In IP multicasting, multicast groups have an ID called multicast group ID. The format of class D IP addresses is shown in Figure 2.

III. MULTICAST PROTOCOL DESIGN CONSIDERATIONS

Designing a new multicast protocol[4] or selecting an existing one is not an easy task. The first thing to do is to define precisely the multicast problem that must be solved. For this purpose, we propose here a list of criteria organized as follows:

1. Size of the multicast problem: these criteria aim at quantifying the multicast groups and their members. If, for instance, near all nodes belong to the considered multicast group, an optimized broadcast (i.e., a protocol minimizing the number of retransmissions in the network, see SMOLSR [5] for an example) can provide good performance. Moreover, a high number of multicast groups and sources are not in favor of multicast protocols maintaining a structure per pair (multicast source, multicast group). These criteria are:

- Number of multicast groups.
- Client density per multicast group: this is defined as the ratio between the number of clients and the total number of nodes within the network.
- Number of sources per multicast group.
- Traffic rate that must be sustained by the multicast protocol.
- QoS (Quality of Service) requirement: QoS requirement is generally expressed in terms of throughput or delay. With a QoS requirement, interferences can no longer be neglected: the transmission of a packet consumes bandwidth not only on the sender and its one-hop neighbors but also on all nodes up to a distance of two transmission ranges from the sender.
- Adaptativity and reactiveness: how does the considered multicast protocol, running in a wireless ad hoc network, adapt to frequent topology changes? How long does it take to recover? Similarly, new sources can be added in the multicast group, others can depart. Multicast group members can join or leave. How does the multicast protocol react? With which latency?
- Reliability: does the application expect from the multicast protocol a delivery guarantee with regard to all multicast clients, provided they are reachable? If the answer is yes absolutely or yes with a high probability, a reliable multicast protocol is required: a deterministic one in the first case and a probabilistic one in the second case.
- Mobility support: is the network static or do some nodes move? In case of mobility, what is the pertinent mobility model (i.e., pause time, speed,direction). Mobile nodes considerably increase the frequency of topology changes that the multicast protocol must be able to cope with. Most multicast protocols are able to support a pedestrian mobility, but nodes embedded in moving vehicles require specific consideration.
- Control overhead and scalability: a multicast protocol based on retransmissions by the sender of the lost messages is adapted to small multicast groups but is unable to scale to large groups. The control overhead induced by the multicast protocol must be kept small because of the limited resources in wireless ad hoc networks.
- Requirement on the underlying unicast routing protocol: some multicast routing protocols are totally independent from the unicast routing protocol; others rely on it and have specific requirement on its type (e.g., a reactive protocol like AODV [6] or DSR, or on the contrary a proactive protocol like OLSR [7])

In order to select the best multicast protocol among several candidates or to improve the design of a new multicast[4] protocol by choosing the best variant, we can compare their performance according to the following criteria:

- Delivery rate,
- Sustained throughput,
- End-to-end transmission delay,

- Control overhead: it can be evaluated:
    - At the bandwidth level, by the messages exchanged per second to maintain the multicast structure or by the redundant messages that would be useless in the absence of message loss.
    - At the memory level, by the amount of memory needed to store the control information maintained by the multicast protocol.
    - At the processing level, by the complexity of the multicast algorithm used.
- Time needed by the multicast protocol to:
    - Add a new client or source joining the multicast group,
    - Remove a client or source leaving the multicast group,
    - Recover from topology changes (i.e., breakage of an existing link, creation of a new link, appearance of a new node, disappearance of a neighbor node).

These comparisons will be made on scenario representative of the environment in which the multicast protocol will run:

- Number of multicast groups and multicast group size.
- Client density.
- Various traffic rates.
- Various mobility scenario.
- Frequencies of group membership and topology changes, etc.

The goal is to determine the best candidate for the multicast problem that has been previously defined.

IV. MULTICST ROUTING PROTOCOLS

MANET is a highly dynamic environment, so the traditional well established multicasting protocols cannot be deployed directly to it. Some modification and extension should be made while considering all the constraints, such as dynamic network topology, limited bandwidth and power. The new protocols should avoid global flooding, should dynamically build the routes, and should update both routes and memberships periodically[3].The Protocols are classified below:

Tree based multicasting protocols

This tree-based concept is borrowed from the multicasting protocols in wired networks. Since efficiency can be achieved and robustness is not a critical issue in the stable wired network, most multicast methods are tree-based, either *source-* or *shared-tree-based*. The former one will construct a multicast tree among all the member nodes for each source node; usually this is a shortest path tree. This kind of protocol is more efficient for the multicast, but has too much routing information to maintain and has less scalability. The latter one constructs only one multicast tree for a multicast group including several source nodes. Every source uses this tree to do multicast. Usually the shared tree constructed is a minimum spanning tree. Since the path between a sender and a receiver is not necessarily the shortest path, the shared-tree-based protocol is less efficient than the source-based protocol in doing multicast, but it reduces the overhead greatly by maintaining less routing information. To let these multicasting protocols work in MANET, some modification and extension should be made. The following two protocols are developed for MANET.

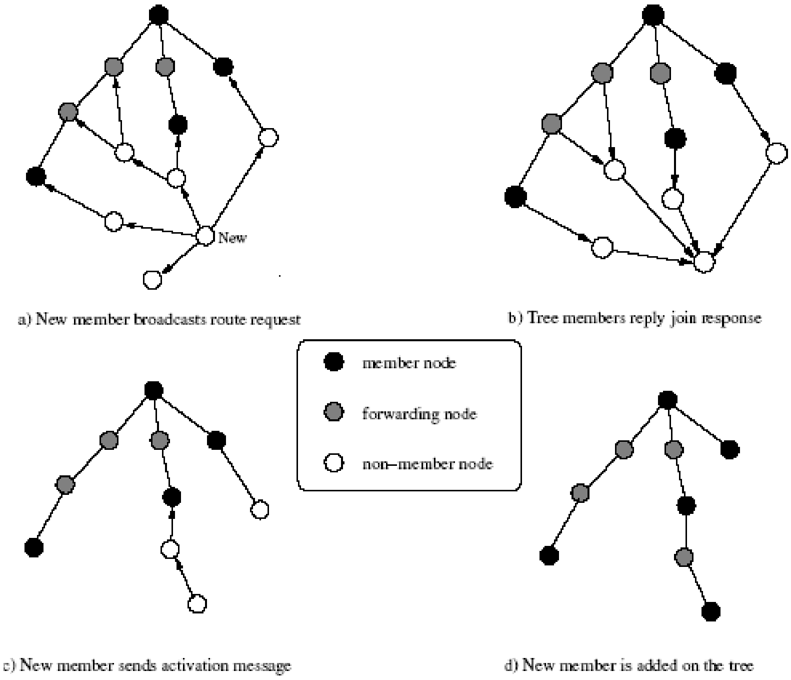
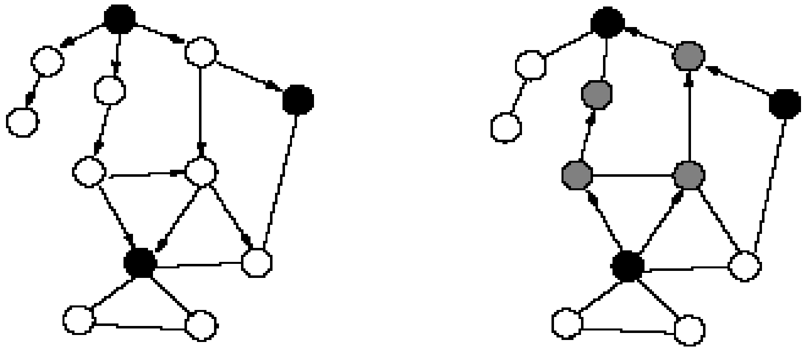

New
a) New member broadcasts route request
b) Tree members reply join response
● member node
● forwarding node
○ non–member node
c) New member sends activation message
d) New member is added on the tree

Fig 3 - Member join procedure of MAODV

MAODV (Multicast On-demand Distance Vector routing protocol) [19]. This protocol uses broadcast to find the route in an on-demand way and constructs a shared routing tree. The node who wants to join a multicast group or has data to send will broadcast a *Route Request (RREQ)* message. This message will be rebroadcasted by all the intermediate nodes until it reaches an on-tree (this group's multicast tree) node. This on-tree node can then reply a *Request Response (RREP)* message by unicast along the reverse path to the sender. The sender node may get more than one RREP, if so, it will select the best one based on sequence number and hop count, then unicast an *activation message* along this selected path. Every intermediate node on this path will be a forwarding node. It sets up entry in its routing table to add the sender and itself on the tree (see Figure 3). In this way, the multicast tree has only a single path to any tree node. This protocol uses hard state in its routing table, that is to say, the state information is updated when failure occurs, contrary to soft state, in which routing table is updated periodically. When a link failure occurs, it will be detected and some kind of repair will be done.

Mesh based multicasting protocols

Correspondingly, the mesh-based method is much more suited for MANET, which demands more robustness of the protocol. That is, when a route fails, which is common in mobile ad hoc networks, there should be another route to deliver the data. It is the redundancy of the routes that provides the fault tolerance.



a) Source sends out join data

b) Receivers reply join tables / forwarding nodes turn on

Fig 4 - Creation of forwarding mesh in ODMRP.

ODMRP (On-Demand Multicast Routing Protocol) [14]. This protocol uses the concept of 'forwarding node' to do the multicasting. It finds some nodes (group member nodes or non-member nodes) to be 'forwarding node' in the whole network, and only these nodes will forward multicast messages. The source on-demand establishes the routes by broadcasting the *JoinData* message with TTL. This message is periodically generated to refresh both the membership and routes. Every intermediate node will add the upstream node's ID in its own routing table upon receiving this message. The message will be forwarded until it reaches a group member. The group member then creates a *JoinTable* message and broadcasts this message to its neighbors. Every neighbor node will know that itself is on the path between the source and the group member if the next hop ID in one of the entries of the *JoinTable* message meets its own ID. This neighbor node then establishes itself as a *forwarding node*. It sets the *Forwarding Group Flag* on. Then it builds its own *JoinTable* message based on routing table and propagates it on until the message reaches the source via the shortest path (see Figure 4). The mesh of forwarding nodes is established in this way. This forwarding group supports the shortest paths between any member pairs. The source can send data to all the group members with the help of the mesh. Only the forwarding nodes will forward the multicast data. It is a soft state protocol and there is no need for the group members to send explicit messages to leave the group. Members can stop working at any time, and this change can be detected by the periodic refreshment.

Hybrid multicasting protocols

There is a hybrid approach named AMRoute (Ad hoc Multicast Routing) [3]. This protocol is a combination of tree-based and mesh-based methods to seek both efficiency and robustness. It has two main procedures. One is mesh creation, the other is tree creation. It first creates the virtual mesh links among the group members based on the physical links. A logic core will be selected from the members in this procedure. It then uses this mesh to establish the multicast tree. The logical core will initiate the tree creation. The tree can stay unchanged even if the topology of the network changes, as long as the links between the core node and tree members still work with the help of virtual mesh. The neighbors on the multicast tree are connected by the underlying unicast tunnels which have the responsibility to deal with dynamic network topology. Both the tree and mesh are quite static.

V. CONCLUSION AND FUTURE SCOPE

In the Paper firstly a brief summary of Multicast Design protocol Considerations have been proposed according to which we can design protocol according to th need,then summary of Traditional Multicasting protocols have been given and then we lay emphasis on new technologies and trends in this field. The future work is the design of multicasting protocols in MANET to reduce the overall control overhead to support the scalability and robustness. Some key issues of this goal, such as the control of the spreading of the state information and the reliability mechanism, need further study.

REFERENCES

[1] Peter S. Kruus , Joseph P. Macker,” TECHNIQUES AND ISSUES IN MULTICAST SECURITY”.

[2] M .V.VIJAYA SARADHI, BH.RAVI KRISHNA**,”** A GROUP KEY MANAGEMENT APPROACH FOR MULTICAST CRYPTOSYSTEMS” in **J**ournal of Theoretical and Applied Information Technology.

[3] SHUHUI YANG , AND JIE WU,”New technologies of multicasting in manet’s”.

[4] Pascale Minet and Anis Laouiti,” Multicasting in Mobile Ad Hoc Networks”.

[5] Hipercom project, ‘‘Simple Multicast OLSR (SMOLSR)’’, http://hipercom.inria.fr/ SMOLSR-MOLSR/

[6] C. Perkins, E. Belding-Royer, S. Das, ‘‘Ad hoc on-demand distance vector (AODV) routing’’, RFC 3561, 2003.

[7] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Muhletaler, P.Minet, A. Qayyum, L. Viennot, ‘‘Optimized link state routing protocol’’, RFC 3626, 2003.

[8] Mansoor Alicherry ,Angelos D. Keromytis, Angelos Stavrou,” Mansoor Alicherry Angelos D. Keromytis Angelos Stavrou” Columbia University& George Mason University.

[9] Paul Judge and Mostafa Ammar,” Security Issues and Solutions in Multicast Content Distribution: A Survey” Georgia Institute of Technology.

[10] D. Cheriton and S. Deering, ÒHost Groups: A Multicast Extension for Datagram Internetworks,Ó Data Commun. Symp., Sept. 1985, pp. 172Ð79.