Realtime communication in a mobile ad-hoc network

IT455: Network Protocols Term Paper

Sagar Mohite
ID: 200901076
Dhirubhai Ambani Institute of Information and Communication Technology
Gandhinagar, India.
200901076@daiict.ac.in

Jiten Thakkar
ID: 200901075
Dhirubhai Ambani Institute of Information and Communication Technology
Gandhinagar, India.
200901075@daiict.ac.in

***Abstract*—This paper deals with the problems that occur typically in a scenario where the nodes in a wireless mesh network are mobile and demand a real-time QoS. To present a detailed approach, we assume a defense scenario and define the requirements, after which we concentrate on developing a feasible network infrastructure for the situation.**

***Keywords*—Wireless mesh networks, mobile nodes, distributed networking, real-time communication.**

I. Introduction

Wireless mesh networks (WMNs) have gained a significant momentum these days with their eminent advantages especially their capabilities of self-forming, self-healing and their fault tolerant nature. It is relatively easy to establish meshes in areas where it is strategically difficult to create other conventional networks. Not only that, mesh networks have become very inexpensive as far their building up is concerned. But when the nodes of the mesh become mobile, it adds to the complexity in managing the network. Mobile meshes or the so-called mobile ad-hoc networks are

In this paper, we assume a typical defense scenario of mobile military units moving in a cluster and requiring a digital channel of communication to replace the analog walkie-talkies or other such communication channel. We stress on a digital medium because of its apparent advantages over the analog medium from the point of view of security, reliability etc. But that is not a focus of attention in this paper and we choose not to discuss this further. That being said, a digital communication channel that will allow soldiers moving together as a cluster to *talk* with each other on a secure line. Further details about the scenario are as given in the following section of this paper.

II. Scenario

This section describes the specific details in the scenario, the related assumptions and the requirements. It, however, does not specify how the requirements are going to be satisfied. That is mentioned in the subsequent sections.

A group of military vehicles is on a mission of exploring a particular terrain of which some areas are inaccessible. Each vehicle has a wireless node. A wireless node, in this case, consists of a wireless router and an antenna equipped to work on the 802.11 standards.

The vehicles need a mesh network established among themselves. It is assumed that all the vehicles move and explore the land until a point where the terrain is not accessible.

Each vehicle has about 20 soldiers. Since the entirety of the terrain is not accessible to the vehicle (hereafter referred to as ‘tank’, in certain places), the soldiers have to get down after a point and spread out as a unit to cover certain other areas (maybe for attack or defense or other situations). This is when a network has to be created ad-hoc amongst the soldiers. Each of them has to be connected to the vehicle, while the vehicle remains connected with other vehicles. As the soldiers move ahead, the network that is hence created needs to sustain itself even when the soldiers venture out of the range of the tank. The network needs to be *modified and managed* and hence sustained in ways that can still serve a minimal understanding of the purpose of communication from the perspective of the soldiers. Thus this ad hoc mobile wireless network is inherently self-creating, self-organizing and self-administering.

A. Assumptions related to the vehicular node

The vehicle, as claimed above, has a wireless mesh node that consists of a wireless router and an antenna that operates on the IEEE 802.11 standards.

B. Assumptions related to the soldier node

Every soldier is a node once he’s out of the vehicle. A soldier is assumed to carry in his bag – a router with wireless capabilities that is able to operate on the IEEE 802.11 standards. A soldier has an earpiece plugged in his ear (or an equivalent handheld device) that is directly connected to a signal transducer which is further connected to the router in his bag. The earpiece (or the handheld device) has no interface other than a button.

C. Requirements

Since the primary data that has to be transmitted via the channel is voice data, the medium has to provide a real time quality of service (QoS). QoS is the performance level of a service offered by the network, in general [4].

The protocol thus, must guarantee the timeliness and reliability constraints of real-time events by minimizing the percentage of packets that miss their end-to-end deadlines. Since all the members should receive the voice messages from every other member it should be imperative for the protocol to be of a multicast nature. The first objective of such a multicast protocol is to convey packets from a source to the members of a multicast group with an acceptable quality of service (QoS)[2], [3].

D. Network Infrastructure

The absence of a *fixed* infrastructure means that nodes in this ad hoc network communicate directly with one another in a peer-to-peer fashion. The mobile nodes themselves constitute the communication infrastructure – a node acts as both a real-time event router and an end host. As nodes move in and out of range of other nodes, the connectivity and network topology changes dynamically.

Unlike other networks where the link failures are not as frequent, mobility leads to an increase in the rate of link failure primarily because of varying signal strength. This is one of the main obstacles to routing in such networks.

Also link failures stand as primary obstacles in the aim of catering to real-time events.

In such networks the available bandwidth is limited and the wireless devices in the vehicles and those with the soldiers have severe energy constraints, relying for example on battery power. Therefore, real-time communication in a mobile ad hoc network is an expensive operation in mobile ad hoc wireless networks in terms of bandwidth and energy consumption. So we need to limit the control packet overhead to a minimum because addition of such control packets increases the overall network load for the transmissions. In addition, the routing and resource reservation protocol for guaranteed real-time class constraints might be limited by the capacity and power limitations of the wireless device.

[1] A trade-off may exist where the ability to guarantee real-time constraints is limited by the overhead involved. For example, the benefit of proactive routes and resource reservations for guaranteed event transmission might be reduced by the additional overhead to discover and maintain the routes, particularly in a limited resource environment.

III. Approach

[5] There are many multicast routing protocols designed for mobile ad hoc networks and they can be categorized into two broad categories: tree-based approaches and mesh-based approaches. Tree-based approaches create trees originating at the source and terminating at multicast group members with an objective of minimizing a cost function. In a typical tree based approach, a shared delivery tree rooted at one of the nodes is constructed, with IDs increasing as they radiate from the source. Local route recovery is made possible due to this property of the IDs, hence, reducing the route discovery time and also confining route recovery overhead to the proximity of the link failure.

Mesh-based multicasting is better suited to highly dynamic topologies, simply due to the redundancy associated with this approach. In mesh-based approaches, there is more than one path between the source and the multicast group members (i.e., a redundant multicast tree). One such mesh-based multicast protocol, On-Demand Multicast Routing Protocol (ODMRP) [5], is based on periodic flooding of the network by the source node through control packets to create a multicast mesh. This basic operation is used both to create the initial multicast forwarding state and to maintain the mesh in case of node mobility and other network dynamics.

Because our case has a relatively low mobility we propose to a hybrid tree and based multicast methodology for mobile ad hoc networks to carry the voice data. The essence here is that the system chooses to switch between a tree based topology and a mesh based topology depending upon certain parameters.

We initially establish a star topology among the soldiers and the vehicle (with the vehicle as the center) as soon as they get down. As they move out of the range of the vehicle, the multicast ad hoc on demand distance vector routing protocol (MAODV) takes over and forms optimized trees amongst the soldiers and also handles route requests. Furthermore, as and how the nodes start moving, each node has its eccentricity (in the resulting tree) calculated. If it exceeds a certain value then the topology switches to that of a mesh based approach.

IV. Initiating the network

Just as the soldiers get down it is assumed that there is a central entity for a short period of time, in our case a tank or a jeep. This is used to initiate the network by relaying messages to all nodes in its range to join it. The message contains the address of the central entity. It transmits these messages for a short period of time, say 10-20 seconds, in which it transmits the message thrice. Interested nodes (soldiers' routers in our case) receive this invitation and request the central to connect to the network. On receiving a request to join the network, the central entity assigns an address to each node and sends an acknowledgement. As this process concludes we have a star topology constructed with the tank as the center.

A. Defining the connection state of a node:

It is important for a node to be aware if it's still in the range of the central entity that it was connected to. Instead of all the connected nodes pinging central entity to know the connection status, central entity sends out *I am Alive* (IMA) messages. The connected nodes expect to receive this message at a certain interval, so upon receiving the IMA message, the nodes can be sure that they are still in the network range.

If a node doesn't receive the IMA message for more than the certain decided interval, it assumes that it is out of the range of the network and transmits a message that it wishes to to join a network.

V. MAODV taking over

A. Tree creation

Any node that wants to join a network , selects itself as a group leader. Every network group is assign a sequence

number. It is the responsibility of the group leader to keep count of the sequence number. It sends periodic Hello messages to the group containing group sequence and group leader address. Group Hellos help to keep the nodes updated and also for repairing possibly partitioned multicast trees.

Anyone who wants to join the multicast group or wants to send messages to the group, uses RREQ or RREP message formats.

B. Route Request:

RREQ is used to discover a route for multicast destination. The important fields for multicasting of the message are set as follows:

• Source address; the address of the sourcing node.

• Destination address; the address of the multicast group that is the target of the discovery.

• Join-flag; if this is set, then the node originating RREQ wants to join the multicast tree(a multicast network). If it is unset, then the originator is a source of multicast transmission.

• Group Leader Extension; if the originator of RREQ knows the group leader (it has heard

Group Hello messages for this multicast group), then the RREQ can be sent towards the group

leader with this extension. This helps in joining the tree since it is probable that the tree is found from the direction where the leader is.

• Sequence number; the last sequence number known to this multicast group.

• Hop count; set to zero.

When the node sends this message, it initiates a timer. The value of the timer should be latency of single hop times the diameter of the network times two. If the node doesn't get the answer, then it tries twice by default. If there is still no answer, the node can choose itself as a group leader if it wants. However, if it only wants to send the data to the network which it can't connect to, it discards the message.

RREQs are sent using broadcasts through the network. It uses expanding ring search technique, where RREQ is first sent with a limited TTL and then the TTL is incremented in subsequent RREQs to cover all the nodes. This way we can prevent broadcast message being sent in a never ending cycle.

C. Route replies

When a node receives a RREQ for a multicast route, it first checks the Join-flag in the message. If the Join -flag is set, then the node may answer only if it is itself a member of the multicast tree and its sequence number for this tree is at least as great as the number in the RREQ. If the Join -flag is not set, then the node may answer, if it has an unexpired route to the multicast tree and its sequence number is at least as great as the number in the RREQ. If neither of the above is true, then the node must find the route towards the multicast tree itself. This means that it must rebroadcast the RREQ towards the neighbors of itself. In this case, it modifies that RREQ as follows:

• The source IP address of the RREQ is the one of the node rebroadcasting it.

• The hop count is incremented by one.

• The original TTL is decremented by one.

In addition to this rebroadcast, a node does two things;

1. It creates a reverse unicast route for the node which originally send the RREQ.
2. It creates a multicast table entry for the multicast group in question.

The RREPs are send as a unicast message towards the originator of the RREQ message. This is done using the information that was learned when the RREQ was rebroadcasted and a unicast reverse route was created. Intermediate nodes increment the hop count of the message. The contents of the RREP messages are as follows;

• Hop count; set to zero if the sending node is a member of the multicast tree, otherwise set to

the value which is the sending node´s distance towards the multicast tree.

• Source address; the address of the node that originated the RREQ.

• Destination address; the multicast group address

• Destination sequence number; the responding node´s knowledge of the sequence number.

D. Tree partitions

The changes in the network topology may lead to two different situations;

1) A link is broken

2) Multicast tree is partitioned

Lets look at each of these cases separately. A node discovers a link breakage if the node has not heard from its neighbor for a while. In this case, it might try to ping the neighbor or ask a route towards it via RREQ. Be it either case, when the node discovers connectivity loss with the multicast tree neighbor, then if it is the downstream neighbor, it is responsible for correcting the situation. What the node does is that it sends a RREQ with a Multicast Group Leader Extension. This extension contains the old distance of the node to the group leader. Only multicast tree member nodes that have distance to the group leader equal or less than the one set in the extension may answer with RREP. This prevents the nodes on the same side of the break as the initiator of the RREQ from answering and thus creating possible loops. If the repair leads to a situation, where the node´s new distance to the group leader is greater than the old one, then it must inform its downstream nodes about this. This is done with MACT message where the update-flag is set. This MACT message is multicasted to all of the tree members, also upstream. But upstream members see that this message came from a downstream node and therefore discards the message.

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE and SI do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

E. Merging partitions

When the two network partitions become united once again, there is two multicast group members for a single multicast group. Since this is an illegal situation, it must be corrected.

What happens is that the group leader that has numerically lower IP address joins the tree of the other group leader. It does this by sending a RREQ with repair -flag set. This RREQ is unicasted to the other group leader and all the nodes along the way must update their multicast routing tables so that also they begin to use the group leader that has numerically higher IP address. The rest of the tree that was formed with the originator of RREQ is given knowledge of the group leader change by issuing a group hello with update-flag set.

VI. Tree Diameter

The distance between two vertices in a graph is the number of edges in a shortest path connecting them. This is also known as the geodesic distance because it is the length of the graph geodesic between those two vertices. If there is no path connecting the two vertices, i.e., if they belong to different connected components, then conventionally the distance is defined as infinite.

The concept of eccentricity is fundamental distance measuring unit in graph theory. If G = (V, E) is a connected graph, the distance d(u, v) between two vertices u and v of G is defined as the minimum length of a u-v path of G. The eccentricity e(v) of v is $\max_{u \in V} d(u, v)$. That is, e(v) is the distance between v and a vertex farthest from v. The radius rad(G) of G is the minimum eccentricity among the vertices of G, and the diameter diam(G) of G is the maximum eccentricity. It is well known that the radius and diameter are related by the inequality

$$rad\ G \leqslant diam\ G \leqslant 2\ rad\ G.$$

We evaluate this distance in our graph in terms of the RTT of the response messages that are received by the nodes. The essence here is about connecting the node with the highest eccentricity with the center of the tree and thus forming redundant connections and creating a mesh topology.

The center of a graph is the set of all vertices of minimum eccentricity, that is, the set of all vertices A where the greatest distance d(A,B) to other vertices B is minimal. Equivalently, it is the set of vertices with eccentricity equal to the graph's radius. Thus vertices in the center (central points) minimize the maximal distance from other points in the graph.

VII. Conclusion

Thus we proposed a method has a number of advantages of the tree based multicast routing protocols as well as the mesh based multicast routing protocols.

Acknowledgments

We would like to thank Professor Sanjay Srivastava for his guidance all through.

References

VIII. References

[1]Hughes, B., & Cahill, V. (n.d.). *Achieving Real-time Guarantees in Mobile Ad Hoc Wireless Networks.*

[2]Janssen, J., Vleeschauwer, D., Petit, G., Windey, R., & Leroy, J. (2002). Delay Bounds for Voice over IP Calls Transported over Satellite Access Links. *Mobile Networks and Applications*, 79-89.

[3]Murthy, C., & Manoj, B. (2004). *Ad Hoc Wireless Networks: Architectures and Protocols.* Prentice Hall.

[4]Tavli, B., & Heinzelman, W. (2006). *Mobile Ad Hoc Networks: Energy-Efficient Real-Time Group Communications.* Springer.

[5]Tavli, B., & Heinzelman, W. B. (2011, May). Energy-Efficient Real-Time Multicast Routing in Mobile Ad Hoc Networks. *IEEE Transactions on computers, Vol 60*.