HOME NETWORKING

The role of mobile ad hoc network in future home networking environments

Humayun Bakht, Madjid Merabti, and Bob Askwith
School of Computing and Mathematical Sciences, Liverpool John Moores University, U.K.

Abstract: Mobile ad-hoc networks are the networks that can be formed with the mutual coordination of two or more mobile devices without the intervention of any fixed infrastructure. Our future homes and Industrial environments are likely to be based on the networks which are easy to deploy with minimal installation and maintenance cost. Mobile ad-hoc networks have strong potential to fulfil the requirements of future computing. Where, on one hand mobile ad-hoc networks are able to give us a networking environment where we can form network on our convenience without involving much complexities. The other side shows that there are number of issues in this area which require satisfactorily solutions before we will be able to use mobile ad-hoc networks at a wider scale i.e. home, business, education and other environments. Routing can be seen as one of the important aspect of any networking environment. It is an unresolved issue in mobile ad-hoc networks. Work is going on since over a decade to invent an efficient routing mechanism for mobile ad-hoc networks. Numbers of different techniques and algorithm have been proposed. However, most of these solutions have certain limitation which makes them unable to operate in all environments. Moreover, very less attention has been given to obtain analytical results of these algorithms in a real environment. Our research shows, that most of the existing issues in mobile ad-hoc networks are interrelated with the routing mechanism of mobile ad hoc networks. On the basis of carried out research, we have also concluded that most of the proposed protocols, if good in addressing some issues besides routing, they are not very impressive in handling others. As deployment of mobile ad hoc networks in future home environment depend very much on the invention of a successful routing solution. We have proposed a novel algorithm 'mobile ad-hoc on demand data delivery protocol (MAODDP)' as a routing solution for mobile ad hoc networks. One of the important features of MAODDP is the fast communication by establishing route and delivering data simultaneously at the same time.

A. Sloane (ed.), *Home-Oriented Informatics and Telematics*

MAODDP follows an intermediate approach in between tables driven and on-demand routing protocols and can be used to save bandwidth and battery life of the participating nodes of mobile ad hoc networks. In this paper, we will discuss in details about various aspects of mobile ad hoc on demand data delivery protocol and its importance in our future computing environment.

Keywords: Wireless, networks, protocols.

1. INTRODUCTION

Mobile ad-hoc network is one of the new additions in the family of wireless networks[1]. It is an autonomous systems of mobile nodes connected together forming an ad-hoc or temporary network in the absence of fixed infrastructure[2-4]. Operating in the absence of fixed supporting structure poses several different challenges to mobile ad-hoc networks[5]. Some of those challenges include routing, security, hidden terminal problems and bandwidth constraints[5, 6]

Routing[7, 8] is the mechanism of information exchange between any two hosts in a network; it is an important aspect to be seen. Routing is one of the challenging issues in mobile ad-hoc networks. Existing Internet protocols were designed to support routing for environment with supporting structure. Their performances therefore, are not very impressive on mobile ad-hoc network.[9] This fact results in the development of new routing strategies for mobile ad-hoc networks. In mobile ad-hoc network a route between a pair of mobile nodes may go through several other mobile nodes. These routes can change when hosts change locations. One traditional way of achieving routing in mobile ad-hoc network is to consider each host as a router and running some conventional routing protocol. This approached is not feasible for mobile ad-hoc network, which suffer with unpredictable and frequent topology changes. Good numbers of papers have been reported proposing various routing solutions[10-14]. One of the main weaknesses in most of the proposed solutions is the lack of consideration given to other routing related issues. Moreover, these protocols do-not perform well in all environments[9, 15, 16] .In an ad-hoc network, all nodes cooperates each other in order to establish and maintains routing in the network, forwarding packets for each other to allow communication between nodes not directly within wireless transmission range. Rather then using the periodic or background exchange of routing information, as it is common in most of the routing protocols.

The contribution of this paper is to highlight in detail about the possible use of mobile ad-hoc networks in the future home environment. In this paper, we have also included a detail description of mobile ad-hoc on

demand data delivery protocol as a routing solution for mobile ad-hoc network. Rest of the paper has been organized as follows. Section 2 throws light on the possible implementation of mobile ad-hoc networks in future home networking environments. Section 3 details the brief description of mobile ad-hoc on demand data delivery protocol (MAODDP). Section 4 covers conclusion and future work while references are listed in section 5.

2. MOBILE AD HOC NETWORKS IN FUTURE HOME NETWORKING ENVIRONMENT

Recent advancement such as Bluetooth[17, 18], WIFI and ad-hoc sensors networks[19] have reviewed an old concept of ad-hoc or peer-to peer networks. Mobile ad-hoc networks are the networks of two or more mobile devices connected with each other without the intervention of any fixed infrastructure. Where on one hand mobile ad-hoc networks offer benefits which cannot be avail from other networks technologies of similar kinds[20]. On the other hand, there are still number of different issues awaiting suitable solutions before we can expect to see their deployment at a wider scale.

The focus of the current ongoing research in this area is to invent various techniques to support different network controls. One of the main aims of ongoing research is to ease end-users jobs by reducing installation and maintenance hassles. At present, setting up a wireless environment in a home environment not only costly but also there are several other issues that are involved. Not every one has technical knowledge to choose the best wireless product which can fulfill one's needs at a lower rate. Moreover, if one is not an expert in setting up network systems, chances are the user's needs to communicate with technical peoples to resolve various problems which may arise with time. This issue not only causes extra cost but also create unnecessary burden on the end users. Likewise, very rarely we find people who are willing to learn different concepts of network terminologies. Setting up a wireless system at its present state requires end users to have at least basic networking knowledge in order to do minor changes on day to day basis whenever it requires. One final and important issue is the continuous updating of the installed system. It happens that the system hardware and the network supporting software could be outdated with time. Therefore, to achieve faster and better services, end users might require updating different parts of their system.

Therefore, there is a solid need of a network system which can easily be used by both technical and non technical users. The system can easily be available, easy to understand without involving too much complexity.

Mobile ad-hoc networks offer these features. Successful deployment of these networks could possibly create an environment where we can use various home objects such as washing machines, oven and cooker for networking purpose. Ad-hoc networks can easily be deployed and can be well suited in all environment i.e. home, Industrial, educational and banking. Another area that has attained a point of focus is how to connect an ad-hoc network with a larger network such as the Internet. Work is on its way to establish mechanisms that can possibly ease mobile ad -hoc networks connection with the larger networks. One final issue is the network security both for homes and business places. Ad-hoc sensor networks which are one of the implementation of mobile ad-hoc networks are currently in used to secure different places such as shopping malls, parking lots etc.

3. MOBILE AD-HOC ON DEMAND DATA DELIVERY PROTOCOL (MAODDP)

Based on the idea of faster and efficient data delivery, MAODDP established the route between the source and the potential destination on demand and deliver the data simultaneously at the same time. MAODDP provides loop-free routes through the use of sequence numbers associated to each route. In short, if A needs a route to B it broadcasts a ROUTE REQUEST and data delivery packet (RREQD). This packet contains the desire destination information the source node aware of and the packet to deliver. Each node that receives this packet, and does not have a route to B, rebroadcasts it. The node also keeps track of the number of hops the message has made, as well as remembering the source of the RREQD. If a node has the route to B it forwards the packet to B.

To achieve faster convergence in the network and thus higher mobility, a ROUTE ERROR message can be broadcasted on to the network in the case a link breakage occurs. Hosts that receive the error message remove the route and re-broadcast the error messages to all nodes with information added about new unreachable destinations.

3.1 Overview

When a route to a new destination is needed, the node uses a broadcast RREQD packet to find a route to the intended destination. A route can be determined when the RREQD reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is an unexpired route entry for the destination whose

associated sequence number is at least as great as that contained in the RREQD.

Once the data delivery accomplished successfully, an acknowledge message (ACK) is send back to the source of the message. Each node receiving the RREQD store a route back to the source of the request, so that the acknowledge message (ACK) can be unicast from the destination along the recorded path to that source, or likewise from any intermediate node that is able to satisfy the request. Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates which destinations are now unreachable due to the loss of the link. In order to enable this reporting mechanism, each node keeps a ``precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards the destination which is now unreachable.

Each node operating on MAODDP maintains a route table management. Route table information must be kept even for ephemeral routes, such as are created to temporarily store reverse paths towards source nodes broadcasting RREQDs. MAODDP uses the following fields with each route table entry:

- Destination IP Address
- Destination Sequence Number
- Hop Count (number of hops needed to reach destination)
- Last Hop Count
- Next Hop
- List of Precursors
- Lifetime (expiration or deletion time of the route)
- Routing Flags

Managing the sequence number is crucial to avoiding routing loops, even when links break and a node is no longer reachable to supply its own information about its sequence number. A destination becomes unreachable when a link breaks or is deactivated. When these conditions occur, the node detecting the condition increments the destination's sequence number and the metric in the route table entry is assigned to be infinite.

3.2 MAODDP Terminology

Active route: A routing table entry with a finite metric in the Hop Count field. A routing table may contain entries that are not active (invalid routes or entries). They have an infinite metric in the Hop Count field. Only active

entries can be used to forward data packets. Invalid entries are eventually deleted.

Broadcast: Broadcasting means transmitting to the IP Limited Broadcast address. A broadcast packet may not be blindly forwarded, but broadcasting is useful to enable flooding.

Forwarding node: A node that agrees to forward packets destined for another destination node, by re-transmitting them to a next hop which is closer to the uni-cast destination along a path which has been set up using routing control messages.

Forward route: A route set up to send data packets from a source to a destination.

Source node: A node that initiates an MAODDP message that is the processed and possibly retransmitted by other nodes in the ad-hoc networks. For instance, the node initiating a RREQD and flooding the RREQD message is called the source node of the RREQD message.

Reverse route: A route set up to forward an acknowledged (ACK) packet back to the source from the destination or from an intermediate node having a route to the destination.

Flood: Flooding means to send a message to every node of the ad-hoc networks or to every node in an region of the ad-hoc network. In MAODDP, a message is flooded by iterated use of broadcast, for which receivers must also rebroadcast after their processing steps have been completed for that message.

3.3 MAODDP Operations

Route request and data delivery packet (RREQD), acknowledged message (ACK) and Route Error (RERR) messages for uni-cast communication towards a destination, and how the message data are handled. In order to process the messages correctly, certain state information has to be maintained for the route table entries for the destinations of interest.

3.3.1 Maintaining Sequence Numbers

MAODDP depends on each node in the network to own and maintain a sequence number to guarantee the loop-freedom of all the routes towards that node. A node increments its own sequence number in two circumstances:

- Immediately before a node originates a RREQD flood, it MUST increment its own sequence number. This prevents problems with deleted reverse routes to the source of a RREQD.

- Immediately before a destination node broadcast an acknowledged (ACK) message in response to a route request and data delivery packet (RRQED), it MUST update its own sequence number to the maximum of its current sequence number and the destination sequence number in the acknowledged packet (ACK).

Every route table entry at every node MUST include the latest information available about the sequence number for the IP address of the destination node for which the route table entry is maintained. This sequence number is called the "destination sequence number". It is updated whenever a node receives new information about the sequence number from RREQD data delivery packet, acknowledged packet, or RERR messages that may be received related to that destination.

The only other circumstance in which a node may change the destination sequence number in one of its route table entries is in response to a broken or expired link to the next hop towards that destination. The node can easily determine which destinations use a broken next hop by consulting its precursor lists for the next hop. In this case, for each destination which uses the next hop, the node increments the sequence number and puts the Hop Count to be "infinity"

In summary, a node may change the sequence number for a particular destination only if:

- It is itself the destination node, and offers a new route to itself
- It receives an MAODDP messages i.e. RREQD OR ACK, with new information about the sequence number for some other destination node
- The path towards the destination node expires or breaks.

3.3.2 Maintaining Route Table Entries and Route Utilization Records

For each valid route maintained by a node (containing a finite Hop Count metric) as a routing table entry, the node also maintains a list of precursors that may be forwarding packets on this route. These precursors will receive notifications from the node in the event of detection of the loss of the next hop link. The list of precursors in a routing table entry contains those neighboring nodes to which a route reply was generated or forwarded.

When a node receives an MAODDP control packets from a neighbor, it checks its route table for an entry for that neighbor. In the event that there is no corresponding entry for that neighbor, an entry is created. The sequence number is either determined from the information contained in the RREQD, or else it is initialized to zero if the sequence number for that node can not be determined. The lifetime for the routing table entry is either determined

from the RREQD, or it is initialized to MY_ROUTE_TIMEOUT. The hop count to the neighbor is set to one.

Each time a route is used to forward a data packet, its Lifetime field is updated to be no less than the current time plus ACTIVE_ROUTE_TIMEOUT. Since the route between each source and destination pair are expected to be symmetric, the Lifetime for the previous hop, along the reverse path back to the IP source, is also updated to be no less than the current time plus ACTIVE_ROUTE_TIMEOUT.

3.3.3 Generating Route Requests

A node floods a RREQD when it determines that it needs a route to a destination and does not have one available. This can happen if the destination is previously unknown to the node, or if a previously valid route to the destination expires or is broken (i.e., an infinite metric is associated with the route). The Destination Sequence Number field in the RREQD is the last known destination sequence number for this destination and is copied from the Destination Sequence Number field in the routing table. If no sequence number is known, a sequence number of zero is used. The Source Sequence Number in the RREQD is the node's own sequence number. The Flooding ID field is incremented by one from the last Flooding ID used by the current node. Each node maintains only one Flooding ID. The Hop Count field is set to zero.

Before flooding the RREQD, the source node buffers the Flooding ID and the Source IP address of the RREQD for FLOOD_RECORD_TIME milliseconds. In this way, when the node receives the packet again as it is flooded by its neighbours, it will not reprocess and re-forward the packet.

A source node often expects to have bi-directional communications with a destination node. In such cases, it is not sufficient for the source node to have a route to the destination node; the destination must also have a route back to the source node. In order for this to happen as efficiently as possible, any generation of an acknowledge packet by the destination node for delivery to the source node, should be accompanied by some action which notifies the destination about a route back to the source node. The source node selects this mode of operation in the intermediate nodes by setting the 'G' flag. After broadcasting a RREQD, a node waits for a acknowledged packet (ACK). If the acknowledged packet is not received within NET_TRAVERSAL_TIME milliseconds, the node MAY try again to flood the RREQD, up to a maximum of RREQD_RETRIES times. Each new attempt MUST increment the Flooding ID field.

Data packets waiting for a route (i.e., waiting for a acknowledged packet after route discovery and data delivery packet has been sent) SHOULD be

buffered. The buffering SHOULD be FIFO. If a (RREQD) has been flooded RREQD_RETRIES times without receiving any ACK, all data packets destined for the corresponding destination SHOULD be dropped from the buffer and a 'Destination Unreachable' message delivered to the application.

3.3.4 Processing and Forwarding RREQD

When a node receives a flooded RREQD, it first checks to determine whether it has received a RREQD with the same Source IP Address and Flooding ID within at least the last FLOOD_RECORD_TIME milliseconds. If such a RREQD has been received, the node silently discards the newly received RREQD. The node always creates or updates a reverse route to the Source IP Address in its routing table. If a route to the Source IP Address already exists, it is updated only if either

- The Source Sequence Number in the RREQD is higher than the destination sequence number of the Source IP Address in the route table, or
- The sequence numbers are equal, but the hop count as specified by the RREQD, plus one, is now smaller than the existing hop count in the routing table.
- This reverse route would be needed in case the node receives an eventual ACK back to the node which originated the RREQD (identified by the Source IP Address). When the reverse route is created or updated, the following actions are carried out:
- The Source Sequence Number from the RREQD is copied to the corresponding destination sequence number.
- The next hop in the routing table becomes the node transmitting the RREQD (it is obtained from the source IP address in the IP header and is often not equal to the Source IP Address field in the RREQD message).
- The hop count is copied from the Hop Count in the RREQD message and incremented by one.

3.3.5 Generating Acknowledge (ACK) by the Destination

If a RREQD is successfully deliver to the intended destination. It is the responsibility of the destination node to issue acknowledge packet (ACK) back to the source node. Destination node MUST update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQD packet. The destination node places the value zero in the Hop Count field of the ACK message.

The destination node copies the value MY_ROUTE_TIMEOUT into the Lifetime field of the ACK. Each node MAY reconfigure its value for MY_ROUTE_TIMEOUT.

3.3.6 Forwarding Acknowledge packet

When a node receives an ACK message, it first increments the hop count value in the ACK by one, to account for the new hop through the intermediate node. It then compares the Destination Sequence Number in the message with its own copy of destination sequence number for the Destination IP Address in the ACK message. The forward route for this destination is created or updated only if:

- The Destination Sequence Number in the ACK is greater than the node's copy of the destination sequence number, or (ii) the sequence numbers are the same, but the route is no longer active or the incremented Hop Count in ACK is smaller than the hop count in route table entry. If a new route is created or the old route is updated,
- The next hop is the node from which the ACK is received, which is indicated by the source IP address field in the IP header; the hop count is the Hop Count in the ACK message plus one; the expiry time is the current time plus the Lifetime in the ACK message; the destination sequence number is the Destination Sequence Number in the ACK message.

3.3.7 Route Error Messages

A node initiates a RERR message in three situations:

1. if it detects a link break for the next hop of an active route in its routing table or
2. if it gets a data packet destined to a node for which it does not have an active route, and has already made an attempt at local repair, or
3. If it receives a RERR from a neighbor for one or more active routes.

For above given two cases, for each unreachable destination the node copies the value in the Hop Count route table field into the Last Hop Count field, and marks the Hop Count for this destination as infinity, and thus invalidates the route.

4. CONCLUSION

In this paper, we have presented our thoughts about future deployment of mobile ad hoc networks in a home environment. We have also discussed

routing problem in general and have g covered a brief description of mobile ad-hoc on demand data delivery protocol as a routing solution for mobile ad hoc networks.

Unlike fixed wireless networks, mobile ad hoc networks operate without the aid of any fixed infrastructure. This approach could make it possible in near future to have networking environment in our home, business and other environment at a much reduced cost. However there are several issues which need to be resolved in order to see successful deployment of mobile ad hoc network under various environments. Our next step is to further investigate the possible use of MAODDP for mobile ad hoc networks in their deployment for future home networking environments.

REFERENCES

[1] Humayun Bakht, Madjid Merabti, and Robert Askwith. Centralized frame for routing in mobile ad-hoc networks. in International Conference on Computer Communication (ICCC2004). September, 2004. Beijing, China.

[2] Humayun Bakht, Understanding mobile ad hoc network, in Computing Unplugged. June 2004. p. 2.

[3] Humayun Bakht, Data Communication in mobile ad-hoc networks, in Computing Unplugged. September 2004. p. 2.

[4] Humayun Bakht, Group communications in mobile ad hoc networks, in Computing Unplugged. November 2004. p. 1.

[5] Humayun Bakht, Technical aspects of mobile ad-hoc networks, in Computing Unplugged. June 2004. p. 2.

[6] Humayun Bakht, A focus on the challenges of mobile ad hoc network, in Computing nplugged. August 2004. p. 2.

[7] Humayun Bakht, et al. Multicasting in mobile ad hoc networks. in 9th CDMA International Conference. 25-28 October 2004. Seoul , Korea.

[8] Humayun Bakht, Importance of secure routing in mobile ad hoc networks, in Computing Unplugged. August 2004. p. 2.

[9] Humayun Bakht, Some characteristics of mobile ad-hoc networks, in Computing Unplugged. July 2004. p. 2.

[10] Sulabh Agarwal, et al., Route-Life time Assessment Based Routing (RABR) Protocol for Mobile Ad-Hoc Networks. IEEE International Conference on Communications (ICC), June 2000.

[11] Stefano Basagni, Imrich Chlamtac, and Violet R. Syrotiuk, A Distance Routing Effect Algorithm for Mobility (DREAM). Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Dallas, TX,, October 25-30, 1998: p. 76-84.

[12] Tsu-Wei Chen and Mario Gerla, Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks. In Proceedings of IEEE ICC '98, 1998.

[13] M.S. Corson and A. Ephremides, Lightweight Mobile Routing protocol (LMR)A distributed routing algorithm for mobile wireless networks. Wireless Networks, 1995. 1.

[14] Benjie Chen, et al., Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks. the 7th ACM International Conference on Mobile Computing and Networking, Rome, Italy, July 2001.

[15] Nitin Vaidya., Tutorial on Mobile Ad Hoc Networks: Routing, MAC and Transport Issues. 2001 MobiCom (Rome) and 2000 MobiCom (Boston), 2000.

[16] Humayun Bakht, Routing protocols for mobile ad hoc networks, in Computing Unplugged. July 2004. p. 2.

[17] Humayun Bakht, Bluetooth a commercial application of mobile ad hoc networks, in Computing Unplugged. November 2004. p. 2.

[18] Humayun Bakht, Future of mobile ad hoc networks, in Computing Unplugged. October 2004. p. 1.

[19] Humayun Bakht, Sensor networks and ad hoc networking, in Computing Unplugged. Oct 2004. p. 1.

[20] Humayun Bakht, Some applications of mobile ad-hoc network, in ComputingUnplugged. September 2004. p. 1.