INTERNET CONNECTIVITY FOR MOBILE AD HOC NETWORKS

A THESIS SUBMITTED IN PARTIAL FULFILMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Technology

in

Computer Science & Engineering

By

RAVINDRA KUMAR BIND

Department of Computer Science and Engineering
National Institute of Technology
Rourkela

2007

INTERNET CONNECTIVITY FOR MOBILE AD HOC NETWORKS

A THESIS SUBMITTED IN PARTIAL FULFILMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Technology

in

Computer Science & Engineering

By

RAVINDRA KUMAR BIND

Under the Guidance of

Dr. Ashok Kumar Turuk

Department of Computer Science and Engineering

National Institute of Technology

Rourkela

2007

National Institute of Technology
Rourkela

Certificate

This is to certify the thesis entitled, **Internet Connectivity for Mobile Ad Hoc Networks** submitted by Sri Ravindra Kumar Bind in partial fulfillment of the requirements for the award of Master of Technology Degree in *Computer Science Engineering* at the National Institute of Technology, Rourkela (Deemed University) is an authentic work carried out by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University / Institute for the award of any Degree or Diploma.

Place: NIT Rourkela
Date:

Dr. Ashok Kumar Turuk
Assistant Professor
Dept. of Computer Science & Engineering
National Institute of Technology
Rourkela - 760008

Acknowledgment

It will be simple to name all those people who helped me to get this thesis done, however it will be tough to thank them enough. I will nevertheless try...

I would like to gratefully acknowledge the enthusiastic supervision and guidance of Dr. Ashok Kumar Turuk during this work. He is my source of inspiration.

I thank Prof. S. Chinara for his constant encouragement and support during this thesis.I would like to express my special thanks to Prof.B.Majhi for being a great soul. He is always ready to help with a smile. I am very much indebted to Prof. S. K. Jena, Head-CSE, for his continuous encouragement and support. My sincere thanks goes to Prof. S. K. Rath (Dean-Academics) for motivating me to work harder.

I would like to thank Prof. B. D. Sahoo,Prof. R. Baliarsingh, Prof. D. P. Mohapatra, Prof. Sabuj K. Jena for their valuable suggestions.

I express my gratitude to Prof. P. K. Sa for generously sharing his time and knowledge and for making life fun while working.

I thank to all my friends for being there whenever I needed them. Thank you very much Dilip, Mrinal, Aser, Tony, Srikant, Sairam. I have enjoyed every moment I spent with you.

I must acknowledge the academic resource that I have got from NIT Rourkela. Last, but not least, I would like to dedicate this thesis to my family,for their love, patience, and understanding.

Ravindra Kumar Bind

Contents

Abstract

Ad hoc networking allows portable devices to establish communication independent of a central infrastructure. However, the fact that there is no central infrastructure and that the devices can move randomly gives rise to various kind of problems, such as routing and security. In this thesis the problem of routing is considered.

There are several ad hoc routing protocols, such as AODV, DSR, OLSR and ZRP, that propose solutions for routing within a mobile ad hoc network. However, since there is an interest in communication between not only mobile devices in an ad hoc network, but also between a mobile device in an ad hoc network and a fixed device in a fixed network (e.g. the Internet), the ad hoc routing protocols need to be modified.

In this thesis the ad hoc routing protocol AODV is used and modified to examine the interconnection between a mobile ad hoc network and the Internet. For this purpose Network Simulator 2, ns2, has been used. Moreover, three proposed approaches for gateway discovery are implemented and investigated.

The goal of the thesis project is twofold:

- To modify the source code of AODV in accordance with the Internet draft " Global connectivity for IPv6 Mobile Ad Hoc Networks " which presents a solution where AODV is used to provide Internet access to mobile nodes.
- To implement and compare different approaches for gateway discovery.

In this thesis, three different type of gateway discovery have been taken:

- The **proactive gateway discovery** is initiated by the gateway itself. The gateway periodically broadcasts a gateway advertisement message which is transmitted after expiration of the gateways timer .The time between two consecutive advertisements must be chosen with care so that the network is not flooded unnecessarily. All mobile devices residing in the gateways transmission range receive the advertisement and update information about gateway. After receiving advertisement, a mobile device just forward it broadcast it again. This process goes on within entire MANET.

- In **reactive gateway discovery** a mobile device of MANET connects by gateway only when it is needed. For that the mobile device broadcasts request message to the ALL_MANET_GW_MULTICAST address (the IP address for the group of all gateways in a mobile ad hoc network). Thus, only the gateways are addressed by this message and only they process it. Intermediate mobile nodes that receive the message just forward it by broadcasting it again up to gateway.

- To minimize the disadvantages of proactive and reactive gateway discovery, the two approaches can be combined. This results is a **hybrid gateway discovery**. For mobile devices in a certain range around a gateway, proactive gateway discovery is used. Mobile devices residing outside this range use reactive gateway discovery to obtain information about the gateway.

In comparing theses different gateway discovery, three matrices are used. These are packet delivery ratio,average end-to-end delay and overhead.

In case of proactive gateway discovery and hybrid gateway discovery, value of packet delivery ratio is larger than reactive gateway discovery. In case of proactive gateway discovery and hybrid gateway discovery, value of end to end delay is less than reactive gateway discovery.The overhead of proactive gateway discovery is greater than other two gateway discovery

As for the average end-to-end delay, the proactive and hybrid methods perform slightly better than the reactive method. Concerning the routing overhead, when the advertisement interval is short the reactive method generates much less overhead than the proactive method, which in turn generates much less overhead than the hybrid method.

List of Figures

List of Tables

Chapter 1

INTRODUCTION

Today, many expect one to be able to connect to the Internet. For example, email has become an important way for people from different parts of the world to keep in touch with each other. It is also an excellent way for scientists around the world to collaborate and share ideas with each other. However, to be able to connect to the Internet one has to find a stationary computer with a modem or a network card. This limits ones possibilities to connect to the Internet. Therefore, it is desirable to have access to the Internet from portable devices such as mobile phones, laptops or personal digital assistants (PDAs).

In view of the increasing demand for wireless information and data services, providing faster and more reliable mobile access is becoming an important concern. The widely deployed and successful mobile communication standard global system for mobile communication (GSM) has spoiled us by our expecting to reach, and be reached, by everyone at (almost) every place. Nowadays, not only mobile phones, but also laptops and PDAs are used by people in their professional and private lives. These devices are used separately for the most part; i.e. their applications do not interact. Sometimes, however, a group of mobile devices form a spontaneous, temporary network as they approach each other. This allows e.g. participants at a meeting to share documents and presentations. These kind of spontaneous, temporary networks are referred to as mobile ad hoc networks (MANETs) (sometimes just called ad hoc networks) or multihop wireless networks, and are expected to play an important role in our daily lives in the near future.

A mobile ad hoc network is a network formed and functioning without any established infrastructure or centralized administration and consists of mobile nodes that use a wireless interface to communicate with each other. These mobile nodes serve as both hosts and routers so they can forward packets on behalf of each other. Hence, the mobile nodes are able to communicate beyond their transmission range by supporting multihop communication.

The issue of routing in a mobile ad hoc network becomes a challenging task since the mobile nodes are free to move randomly. Ad hoc routing protocols can be classified into three classes 1: proactive, reactive and hybrid routing protocols. In proactive routing the routing table of every node is updated periodically. On the contrary, reactive routing is performed on-demand, i.e. the sending node searches for a route to the destination node only when it needs to communicate with it. Hybrid routing uses a mixture of these two routing approaches. That is, proactive routing is used in a limited area around the mobile node and reactive routing is used outside this area.

Mobile Ad Hoc Networking (MANET) is the name of a working group in the Internet Engineering Task Force (IETF) and it serves as a meeting place for people dealing with MANET approaches. The primary focus of the working group is to develop and evolve MANET routing specifications and introduce them to the Internet Standards track. The goal is to support networks scaling up to hundreds of routers according to the official web .

The layout of the thesis is as follows:
Chapter 1.2 describes the project goals. Chapter 2 gives an overview of the concept of mobile ad hoc networks in general. In addition, it presents some of several promising ad hoc routing protocols. Chapter 3 discusses interworking between mobile ad hoc networks and fixed networks (e.g. the Internet). It also discusses some problems that occur when these different networks are integrated and finally it presents conceivable solutions. Chapter 4 considers three approaches for gateway discovery and discusses advantages and disadvantages of them. Chapter 5

explains the simulation scenario and examine the results. Chapter 6 summarizes and concludes the thesis.

Some details of the implementation of the Internet draft " Global Connectivity for IPv6 Mobile Ad Hoc Networks " are presented .

1.1 MOTIVATION

Although an autonomous, stand-alone mobile ad hoc network is useful in many cases, a mobile ad hoc network connected to the Internet is much more desirable. So far, most of the research concerning mobile ad hoc networking has been done on protocols for autonomous mobile ad hoc networks. However, during the last few years, some work has been done concerning the integration of mobile ad hoc networks and the Internet.

In this thesis the access to the Internet from a multihop wireless network is investigated. To achieve this network interconnection, gateways that understand the protocols of both the mobile ad hoc network stack and the TCP/IP suite (see Figure 2.1, are needed. All communication between a mobile ad hoc network and the Internet must pass through the gateways.

The Internet draft "Global Connectivity for IPv6 Mobile Ad Hoc Networks" describes how to provide Internet connectivity to mobile ad hoc networks. In particular, it explains how a mobile node and a gateway should operate. Further, it proposes and illustrates how to apply a method for discovering gateways. In the case for reactive routing protocols, the idea is to extend the route discovery messaging, so that it can be used for discovering not only mobile nodes but also gateways.

1.2 PROJECT DESCRIPTION

The ad hoc routing protocol AODV is one of the promising routing protocols investigated by the MANET working group. It can be used in a mobile ad hoc

network to route packets between mobile nodes. However, it cannot provide Internet access to the mobile nodes because it does not support routing between a fixed network like the Internet and a mobile ad hoc network.

The goal of the thesis project is twofold:

- To modify the source code of AODV in accordance with the Internet draft " Global connectivity for IPv6 Mobile Ad Hoc Networks " which presents a solution where AODV is used to provide Internet access to mobile nodes.
- To implement and compare different approaches for gateway discovery.

1.3 BACKGROUND

While much research has been done on routing protocols for autonomous mobile ad hoc networks during the last few years, there has not been much work published in the field of Internet access for mobile nodes in a mobile ad hoc network. There are some works where Mobile IP is used to provide Internet access to the mobile nodes.

In "Global Connectivity for IPv4 Mobile Ad hoc Networks" (often simply referred to as "Global4") a solution is presented where AODV cooperates with the Mobile IP protocol. Mobile IP is used for mobile node registrations with a foreign agent, while AODV is used for routing within the mobile ad hoc network and for obtaining routes to the foreign agent. In this solution, the foreign agent discovery mechanism is incorporated into the ad hoc routing protocol.

There are also some works in which mobile IP is not used. The paper "Wireless Multihop Internet Access: Gateway Discovery, Routing and Addressing" discusses interesting issues like gateway discovery and different kinds of routing policies. The master's thesis, "Gateway Detection and Selection for Wireless Multihop Internet Access" , (which reminds of the former paper) discusses gateway detection and selection in more detail.

The leading and most promising work in the field is the Internet draft "Global Connectivity for IPv6 Mobile Ad Hoc Networks" (often simply referred to as "Global6" compared to "Global4" mentioned above) . Hence, in this project, the necessary parts of this draft have been implemented in ns2, in order to provide Internet access to mobile nodes. However, some issues are not considered in this draft. These issues are discussed and conceivable solutions are presented in Section 3.5.

This thesis also considers gateway discovery. In particular, a solution for implementing the different approaches has been presented. In "Gateway Detection and Selection for Wireless Multihop Internet Access" and "Wireless Multihop Internet Access: Gateway Discovery, Routing and Addressing" gateway discovery is discussed but none of them goes into deep with it and they do not consider the question of duplicated broadcast messages.

In the Internet draft "Global6", the term Internet Gateway is used instead of the term gateway that is used throughout this text. The reason to why the shortened term have been used is that no other kind of gateway is of importance in this project.

Chapter 2

MOBILE AD HOC NETWORKING

This chapter gives an overview of Mobile Ad Hoc Networking. Section 2.1 introduces the protocol stacks used in the Internet and MANET and compares them with the Open Systems Interconnection (OSI) model. Section 2.2 describes the different routing concepts. In Section 2.3 and 2.4 two reactive routing protocol are presented. Section 2.5 presents a proactive routing protocol and finally, in Section 2.6, a hybrid routing protocol is described.

2.1 THE PROTOCOL STACK

In this section the protocol stack for mobile ad hoc networks is described. This gives a comprehensive picture of, and helps to better understand, mobile ad hoc networks. Figure 2.1, shows the protocol stack which consists of five layers: physical layer, data link layer, network layer, transport layer and application layer. It have similarities to the TCP/IP protocol suite. As can be seen the OSI layers for session, presentation and application are merged into one section, the application layer.

On the left of Figure 2.1, the OSI model is shown. It is a layered framework for the design of network systems that allows for communication across all types of computer systems.

In the middle of the figure, the TCP/IP suite is illustrated. Because it was designed before the OSI model, the layers in the TCP/IP suite do not correspond

exactly to the OSI layers. The lower four layers are the same but the fifth layer in the TCP/IP suite (the application layer) is equivalent to the combined session, presentation and application layers of the OSI model.

On the right, the MANET protocol stack -which is similar to the TCP/IP suite -is shown. The main difference between these two protocol stacks lies in the network layer. Mobile nodes (which are both hosts and routers) use an ad hoc routing protocol to route packets. In the physical and data link layer, mobile nodes run protocols that have been designed for wireless channels. Some options are the IEEE standard for wireless LANs, IEEE 802.11, the European ETSI standard for a high-speed wireless LAN, HIPERLAN 2, and finally an industry approach toward wireless personal area networks, i.e. wireless LANs at an even smaller range, Bluetooth . In the simulation tool used in this project, the standard IEEE 802.11 is used in these layers.

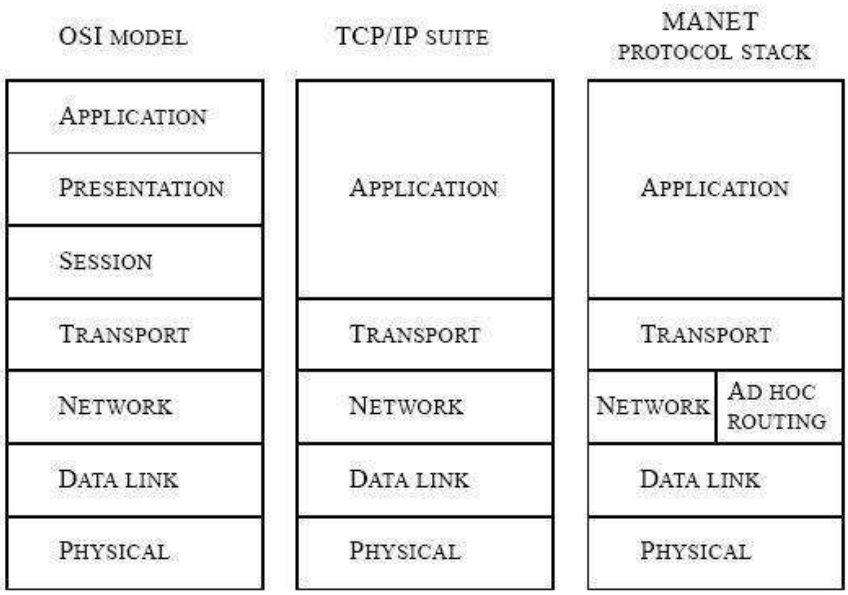


Figure 2.1: The OSI model, TCP/IP suite and MANET protocol stack.

This thesis focuses on ad hoc routing which is handled by the network layer. The network layer is divided into two parts: Network and Ad Hoc Routing. The

protocol used in the network part is Internet Protocol (IP) and the protocol used in the ad hoc routing part is Ad hoc On-Demand Distance Vector (AODV). Other ad hoc routing protocols that can be used in this part of the network layer are discussed in Sections 2.4, 2.5 and 2.6. One of the reasons to why AODV has been used in this study is that it is one of the most developed routing protocols for mobile ad hoc networks. A second reason is that the Internet draft "Global6" uses AODV as an example when illustrating how to extend the route discovery messaging of a reactive routing protocol for discovering gateways.

In the transport layer the User Datagram Protocol (UDP), is used in this study. The Transmission Control Protocol (TCP) is not used because there are some research showing that TCP does not perform well in mobile ad hoc networks. One reason to this is that in wired networks, lost packets are almost always due to congestion but in mobile ad hoc networks lost packets are more often caused by other reasons like route changes or transmission errors .

2.1.1 Interworking

Whenever a mobile node is to send packets to a fixed network, it must transmit the packets to a gateway . This will be discussed in more detail later in Chapter 3, but here the protocol stacks involved during communication between a mobile ad hoc network and the fixed Internet node are shown. A gateway acts as a bridge between a MANET and the Internet. Therefore, it has to implement both the MANET protocol stack and the TCP/IP suite, as shown in the middle of Figure 2.1, Although the figure shows that all the layers are implemented for the gateway, it does not necessarily need all of the layers.

The protocol stack used by the mobile node is the MANET protocol stack discussed previously and shown on the right of Figure 2.1 The fixed Internet node uses the TCP/IP suite. A gateway, that must be able to translate between these two "languages", must understand the both architectures.

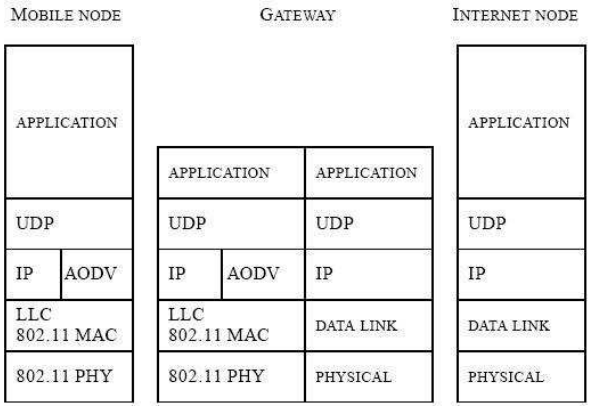


Figure 2.2: The protocol stacks used by mobile nodes, gateways and Internet nodes.

2.2 PROACTIVE, REACTIVE AND HYBRID ROUTING PROTOCOLS

Traditional distance-vector and link-state routing protocols are proactive in that they maintain routes to all nodes, including nodes to which no packets are sent. For that reason they require periodic control messages, which leads to scarce resources such as power and link bandwidth being used more frequently for control traffic as mobility increases. One example of a proactive routing protocol is Optimized Link State Routing Protocol (OLSR) . OLSR, which has managed to reduce the utilization of bandwidth significantly, is described in Section 2.5.

Reactive routing protocols, on the other hand, operate only when there is a need of communication between two nodes. This approach allows the nodes to focus either on routes that are being used or on routes that are in process of being set up. Examples of reactive routing protocols are Ad hoc On-Demand Distance Vector (AODV) , and Dynamic Source Routing (DSR) . AODV is described in Section 2.3 and DSR in Section 2.4.

Both proactive and reactive routing have specific advantages and disadvantages that make them suitable for certain types of scenarios. Proactive routing protocols have their routing tables updated at all times, thus the delay before

sending a packet is minimal. However, routing tables that are always updated require periodic control messages that are flooded through the whole network -an operation that consumes a lot of time, bandwidth and energy. On the other hand, reactive routing protocols determine routes between nodes only when they are explicitly needed to route packets. However, whenever there is a need for sending a packet, the mobile node must first find the route if the route is not already known. This route discovery process may result in considerable delay.

Combining the proactive and reactive approaches results in a hybrid routing protocol. A hybrid approach minimizes the disadvantages, but also the advantages of the two combined approaches. The Zone Routing Protocol (ZRP) is such a hybrid reactive/proactive routing protocol. Each mobile node proactively maintains routes within a local region (referred to as the routing zone). Mobile nodes residing outside the zone can be reached with reactive routing. ZRP is discussed in Section 2.6.

2.3 AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV is a reactive mobile ad-hoc routing protocol. It joins the mechanisms of DSDV and DSR. The periodic beacons, hop-by-hop routing and the sequence numbers of DSDV and the pure on-demand mechanism of Route Discovery and Route Maintenance of DSR are combined.

Message Format

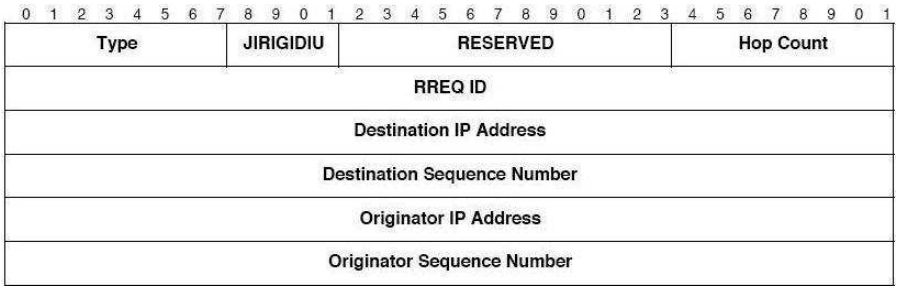


Figure 2.3: AODV: Route Request (RREQ)

As an important feature AODV uses a destination sequence number for each route entry. This destination sequence number is generated by the destination node and is sent to the requesting node. This trivially insures loop-freedom by simply selecting the route with the highest sequence number as the actual one.

AODV has four types of messages: Route Requests (RREQ), Route Replies (RREP), Route Errors (RERR), and Route Replies Acknowledgment(RREP - ACK). All these messages are received via UDP using normal IP hader processing. AODV uses the IP limited broadcast address (255.255.255.255) to broadcast messages.

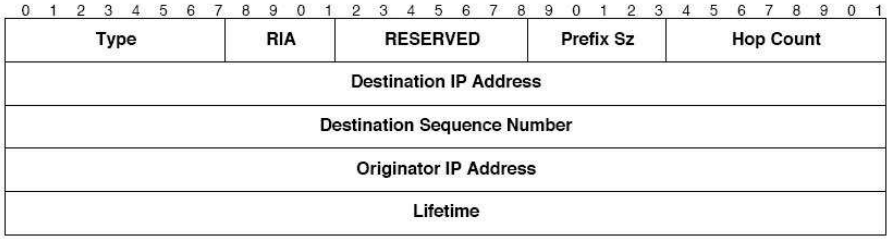


Figure 2.4: AODV: Route Reply (RREP)

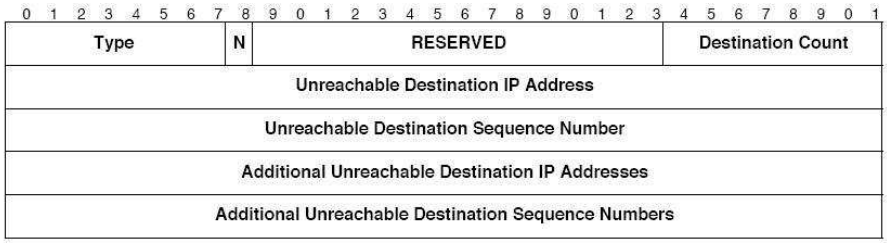


Figure 2.5: AODV: Route Error (RERR)

Figure 2.6: AODV: Route Reply Acknowledgment (RREP - ACK)

Type 1 for RREQ

2 for RREP

3 for RERR

4 for RREP -ACK

J Join Flag; reserved for multicast.

R Repair Flag; reserved for multicast.

G Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the destination node.

D Destination only flag; only the destination node may answer to this RREQ, no intermediate node is allowed of answering with a RREP.
U Unknown sequence number.

A Acknowledgment required; used, if there is a danger of unidirectional links. It causes the receiver of the RREP message to send back a RREP -ACK message. The reception of such an acknowledgment provides assurance that the link is currently bidirectional.

N No delete flag; set if upstream nodes should not delete the route, although a node has performed a local repair of a link.

2.3.1 Sequence Number and Routing Table Management

It is crucial for AODV to properly handle the sequence numbers. A node has to update its own sequence number in two cases:

- Before starting a route discovery process, the node has to increment its own sequence number.
- A destination node has to update its own sequence number to the maximum of its current sequence number and the destination sequence number in RREQ packet immediately before transmitting the RREP packet.

The sequence numbers in the routing table entries may be changed by the node only in the following circumstances:

- Offer of a new route to itself, if it is the destination node.
- Reception of an AODV message with new information about the sequence number for a destination.
- Expiration of path or path breaks.

When a node receives an AODV control message, either to create or to update a route for a particular destination, it searches its routing table for an entry to the destination. If there is no route entry, it creates a new one with the sequence number contained in the control packet, or else the sequence number is set invalid. Otherwise, the node compares the existing entry with the new information and updates it if either

- the new sequence number is higher than in the routing table entry,
- the sequence numbers are equal and the new hop count plus one is smaller than in the existing route, or
- the sequence number is unknown.

Besides the destination sequence numbers, the routing entry for each valid route contains a precursor list. This list contains all precursor of the node which are able to forward packets on this route. All neighboring nodes to which a RREP was generated or forwarded are included in this list. In the event of a next hop link breakage, notifications are sent to those nodes. The routing table entries of AODV consist of the following entries:

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Routing and state flags
- Network Interface
- Hop Count (distance in hops to reach the destination)

- Next Hop
- List of Precursors (as mentioned above)
- Lifetime (deletion time of the route entry)

2.3.2 Route Discovery

If a valid route exists between two communication peers, AODV takes no action. When a new route is needed, the Route Discovery mechanism is started. The source node has to send a RREQ message. The sequence number field in the RREQ is set to the last known destination sequence number or if not available the unknown sequence number field is set. The own sequence number is incremented and included in the Originator Sequence Number field of the message. The RREQ ID field is incremented by one of the node's current RREQ ID. The hop count is set to zero. The node buffers the RREQ ID and the Originator IP address of RREQ before broadcasting it. The source node waits now for a RREP message. If it does not retrieve one within a certain time, it may broadcast another RREQ. If the maximum number of retries has been reached, all data packets for this destination are dropped and a destination unreachable message is delivered to their originators

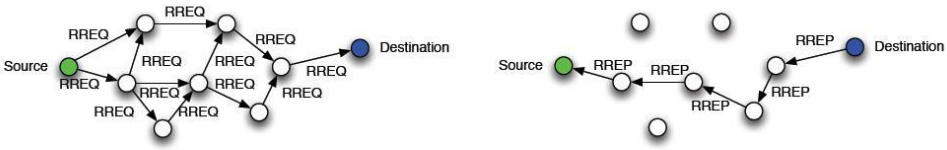


Figure 2.7: AODV: Route Discovery

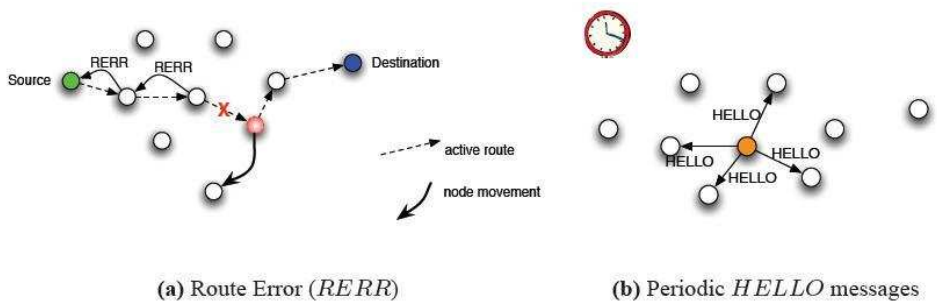
The intermediate node which is receiving the RREQ checks if it has already received a message with the same Originator Address and RREQ ID within a certain time. If a RREQ has been already received, the newly received message is discarded. Otherwise, the node increments the hop count in the RREQ and searches for a reverse route to the originator and creates or updates its route entry in the routing table. The destination sequence number of the reverse route in the routing table is set to the Originator Sequence Number if it is greater, the

sequence number is set valid, the hop count is copied from the RREQ and the next hop is changed. If the intermediate node has a fresh enough valid route to the destination, it unicasts a RREP, whose hop count is set to the hop distance of the current node to the destination, to the source node and discards the RREQ. Otherwise, it broadcasts the RREQ.

When the RREQ reaches the destination node, the node sends a RREP back towards the source of the RREQ using the reverse route. The destination node increments its own sequence number and puts it in the Destination Sequence Number field. The hop count is reset to zero. Each intermediate node forwarding the RREP always increments the hop count. As soon as the source node retrieves the RREP , it is able to transmit the data packets to the destination.

2.3.3 Route Maintenance

Nodes which are part of an active route can deliver connectivity information by broadcasting HELLO messages. A HELLO message is a RREP message with TTL = 1. By listening for packets from its neighbor nodes a node can determine the connectivity. If it receives neither HELLO nor other messages from a certain node during a certain interval, it has to assume a link break. Local connectivity can also be surveyed by using link layer notification. The node sends a RERR to all nodes in the precursor list of the concerned route, if it has detected a link break for the next hop of an active route, or if it gets data packets for a node for which it does not have an active route, or if it receives a RERR from a neighbor for an active route.



(a) Route Error ($RERR$) **(b)** Periodic $HELLO$ messages

Figure 2.8: AODV: Route Maintenance

2.4 DYNAMIC SOURCE ROUTING (DSR)

Dynamic Source Routing, DSR, is a reactive routing protocol that uses source routing to send packets . It is reactive like AODV which means that it only requests a route when it needs one and does not require that the nodes maintain routes to destinations that are not communicating. It uses source routing which means that the source must know the complete hop sequence to the destination.

Each node maintains a route cache, where all routes it knows are stored. The route discovery process is initiated only if the desired route cannot be found in the route cache.

To limit the number of route requests propagated, a node processes the route request message only if it has not already received the message and its address is not present in the route record of the message.

As mentioned before, DSR uses source routing, i.e. the source determines the complete sequence of hops that each packet should traverse. This requires that the sequence of hops is included in each packet's header. A negative consequence of this is the routing overhead every packet has to carry. However, one big advantage is that intermediate nodes can learn routes from the source routes in the packets they receive. Since finding a route is generally a costly operation in terms of time, bandwidth and energy, this is a strong argument for using source routing. Another advantage of source routing is that it avoids the need for up-to-date routing information in the intermediate nodes through which the packets are forwarded since all necessary routing information is included in the packets. Finally, it avoids routing loops easily because the complete route is determined by a single node instead of making the decision hop-by-hop.

2.4.1 Route Discovery

Route Discovery is used whenever a source node desires a route to a destination node. First, the source node looks up its route cache to determine if it already contains a route to the destination. If the source finds a valid route to the destina-

tion, it uses this route to send its data packets. If the node does not have a valid route to the destination, it initiates the route discovery process by broadcasting a route request message. The route request message contains the address of the source and the destination, and a unique identification number.

An intermediate node that receives a route request message searches its route cache for a route to the destination. If no route is found, it appends its address to the route record of the message and forwards the message to its neighbors. The message propagates through the network until it reaches either the destination or an intermediate node with a route to the destination. Then a route reply message, containing the proper hop sequence for reaching the destination, is generated and unicast back to the source node.

2.4.2 Route Maintenance

Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache.

Acknowledgment messages are used to verify the correct operation of the route links. In wireless networks acknowledgments are often provided as e.g. an existing standard part of the MAC protocol in use, such as the link-layer acknowledgment frame defined by IEEE 802.11. If a built-in acknowledgment mechanism is not available, the node transmitting the message can explicitly request a DSR-specific software acknowledgment to be returned by the next node along the route.

2.5 OPTIMIZED LINK STATE ROUTING PROTOCOL (OLSR)

Optimized Link State Routing Protocol, OLSR, is another routing protocol developed for mobile ad hoc networks . It is a proactive protocol, which means that the mobile nodes exchange topology information with each other regularly.

As mentioned earlier , there is a big disadvantage of proactive routing protocols. To keep the routing tables updated the network is flooded and every mobile node receives the same message from each of its neighbors. Thus, bandwidth and energy are wasted for useless messages. To avoid too many redundant retransmissions, the flooding process is optimized in OLSR. In OLSR, only some selected nodes forward the broadcast messages during the flooding process. These selected nodes are referred to as multipoint relays (MPRs).

2.5.1 Multipoint Relays

The use of Multipoint Relays (MPRs), as the only nodes that forward broadcast messages, substantially reduces the message overhead as compared to a classical flooding mechanism, where every node retransmits each message when it receives the first copy of the message. Another optimization is achieved by minimizing the set of links flooded in the network. As contrary to the classic link state algorithm, a mobile node declares only the MPR links to its neighbor nodes, rather than all links to all neighbors. In summary, multipoint relaying allow to reduce the utilization of bandwidth in two following ways:

1. The number of redundant retransmissions when flooding the network is greatly reduced.

2. Redundant topology advertisements are reduced.

2.6 ZONE ROUTING PROTOCOL (ZRP)

Zone Routing Protocol, ZRP, is a routing protocol that is designed for mobile ad hoc networks . It is a hybrid protocol that is part proactive and part reactive.

The proactive part, uses a modified distance vector scheme within the routing zone of each node. The routing zone is determined by a zone radius, which is the minimum number of hops it should take to get to any node. Thus, each node has a routing zone, which is composed of nodes within its local area. This proactive component is called Intrazone Routing Protocol (IARP). The reactive component is called Interzone Routing Protocol (IERP), and uses queries to get routes when

a node is to send a packet to a node outside of its routing zone.

ZRP uses a method called bordercasting in which a node asks all nodes on the border of its routing zone to look for the node outside of its routing zone.

2.6.1 Intrazone Routing Protocol (IARP)

The Intrazone Routing Protocol (IARP) proactively maintains routes to destinations within a local neighborhood, which is referred to as a routing zone. More precisely, a node's routing zone is defined as a collection of nodes whose minimum distance in hops from the node in question is no greater than a parameter referred to as the zone radius. Note that each node maintains its own routing zone. An important consequence is that the routing zones of neighboring nodes overlap.

2.6.2 Interzone Routing Protocol (IERP)

The operation of the reactive Interzone Routing Protocol (IERP) is quite similar to standard route discovery process of reactive routing protocols. An IERP route discovery is initiated when no route is locally available to the destination of an outgoing data packet. The source generates a route query message, which is uniquely identified by a combination of the source nodes address and request number. The query is then relayed to a subset of neighbors as determined by the bordercast algorithm. Upon receipt of a route query message, a node checks if the destination lies in its zone or if a valid route to it is available in its route cache. If the destination is found, a route reply is sent back to the source. If not, the node bordercasts the query again.

2.6.3 Bordercast Resolution Protocol (BRP)

Since the topology of the local zone of each mobile node is known (this information is provided by IARP), global route discovery is simplified. Rather than broadcasting a route query from neighbor to neighbor, ZRP uses a concept called bordercasting. Bordercasting means that the route query is directed toward regions of the network that have not yet been covered by the query. A covered node is the one that belongs to the routing zone of a node that has received a

route query. Hence, the route query traffic is reduced by directing route queries outwards from the source and away from covered routing zones.

Chapter 3

INTERNET CONNECTIVITY FOR MOBILE AD HOC NETWORKS

This chapter investigates interworking between mobile ad hoc networks and the Internet. Section 3.1 motivates the need of Internet connectivity for MANETs . In Sections 3.2 and 3.3 the extended route request and route reply messages of the reactive ad hoc routing protocol AODV are described. Section 3.4 describes how a mobile node can obtain a default route. Section 3.5 discusses some important issues that must be considered when trying to integrate a MANET to the Internet.

3.1 THE EXTENDED ROUTE REQUEST

The extended RREQ message contains exactly the same fields with the same functions as the ordinary RREQ message, except for a flag. This flag is called Internet-Global Address Resolution Flag and is referred to as the I-flag. Hence, the RREQ message extended with the I-flag is referred to as the RREQ_I message throughout this text. Figure 3.1 shows the format of the RREQ_I message.

The I-flag is used for global address resolution and it indicates that the source node requests global connectivity. The RREQ_I message plays the same role as the router solicitation message of ICMP. Section 4.2 describes how the RREQ_I message is used to reactively discover a gateway.

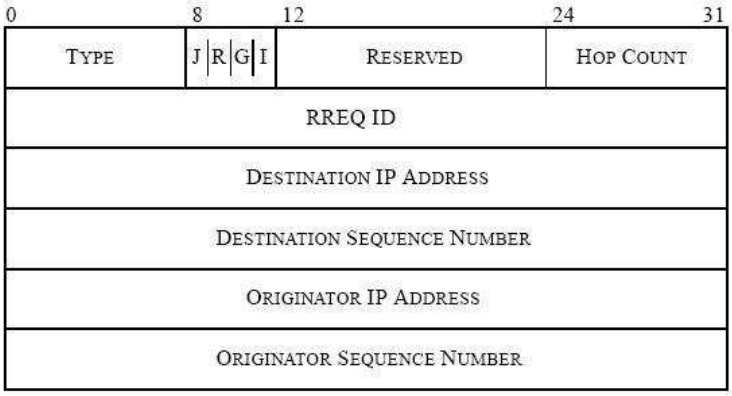


Figure 3.1: The format of a Route Request message extended with the I-flag.

3.2 THE EXTENDED ROUTE REPLY

The extended RREP message contains exactly the same fields with the same functions as the ordinary RREP message, except for a flag. This flag is the same flag that has extended the RREQ message to the RREQ_I message, namely the Internet-Global Address Resolution Flag (or the I-flag). Hence, the RREP message extended with the I-flag is referred to as the RREP_I message throughout this text. Figure 3.2 shows the format of the RREP_I message.

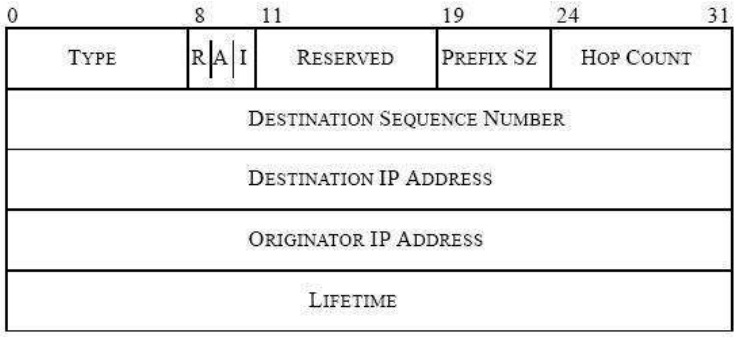


Figure 3.2: The format of a Route Reply message extended with the I-flag.

The I-flag is used for global address resolution and, if set, it indicates that this RREP contains information about a gateway. The RREP_I message plays the same role as the router advertisement message of ICMP. Section 4.1 describes why the RREP_I message cannot be used to proactively discover a gateway. Instead Section

4.3 describes how RREP_I messages can be used by the gateways to proactively advertise information about themselves in a limited zone around the gateway.

3.3 OBTAINING A DEFAULT ROUTE

A mobile node needs to learn the location and address of a gateway to be able to have access to the Internet. In other words, the mobile node needs a route to a gateway, which it uses as its default route, to be able to send packets to the Internet. This gateway information can be obtained in a few different ways:

- By relying on periodic advertisement messages broadcasted by the gateway (proactive gateway discovery)
- By sending a RREQ_I to the ALL_MANET_GW_MULTICAST address (reactive gateway discovery)
- By sending a RREQ which is received by a gateway

When a mobile node discovers a gateway, i.e. when it receives some message that, among other things, contains the address of the gateway, it creates a default route with the address of the gateway as the next hop. Chapter 4 describes three different methods for gateway discovery.

3.4 PROBLEMS AND CONCEIVABLE SOLUTIONS

Assume that a mobile node (S) wants to communicate with another node (D) and that S does not have any route to D in its routing table. Hence, S does not know whether D is a mobile node (located within the MANET) or a fixed node (located on the Internet). Using AODV (see Section 2.3) as the ad hoc routing protocol, S broadcasts a RREQ, requesting for a route to D. If D is a mobile node, the node itself or another mobile node with a fresh route to it will unicast back a RREP to S. However, if D is a fixed node, no mobile node will send a reply to S. So, how can S find a route to D if D is a fixed node? According to "Global6", if S broadcasts a RREQ but no corresponding RREP is received, S assumes that D

is a fixed node. Hence, the packets are sent to the Internet by using the default route.

3.4.1 Mobile Nodes versus Fixed Nodes

As already said, if a mobile node (S) broadcasts a RREQ but does not receive any corresponding RREP, S assumes that the destination (D) is a fixed node located on the Internet. But how many RREQs does S have to send, without receiving any corresponding RREP, before it can assume that D is located on the Internet? This issue is not discussed in "Global6".

As described in 2.3.1, S uses expanding ring search to find a route to D. To be absolutely sure that D is not a mobile node located within the MANET, S must do, at least, one network-wide search. Since a network-wide search consumes a lot of time and link bandwidth, it is not a good idea to do this search more than once. The idea can be summarized:

A mobile node assumes that a destination node is a fixed node located on the Internet, if the mobile node has done one network-wide search without receiving any corresponding RREP for the destination node.

In this study, the expanding ring search of AODV is used, without any modifications, as described in Section 2.3.1. It should be mentioned that, using the expanding ring search technique results in a considerable route discovery delay if the destination is a fixed node. Modifying the TTL_START, TTL_INCREMENT and TTL_THRESHOLD parameters can decrease the route discovery delay if the destination is a fixed node, but at the same time, the modification can result in increased routing overhead if the destination is a mobile node. The modification could for example be to increase TTL_START. Because, assuming the destination is a fixed node, increasing TTL_START would result in less number of broadcasted RREQs (and consequently less delay) before the source assumes that the destination is a fixed node. Thus, different approaches are preferable depending on whether a mobile node is to communicate mostly with the MANET or the

Internet.

3.4.2 Gateway Operation upon Reception of RREQs

According to "Global6", when a gateway receives a RREQ, it looks in its routing table searching for the destination IP address specified in the RREQ message. If the address is not found in the routing table, the gateway has to send a RREP_I back to the originator of the RREQ. On the other hand, if the gateway finds the host route in its routing table, it should not unicast back a RREP_I to the originator of the RREQ "because the destination is then assumed to be inside the manet" . However, if the host route is found, not sending neither a RREP_I nor a RREP back to the originator of the RREQ, is not a good idea. The gateway must send a RREP and optionally also a RREP_I back to the originator of the RREQ. After pointing out the problem to the authors of the draft, they agreed on changing this. Hence, in the implementation used in this project:

If a gateway receives a RREQ and finds the host route in its routing table, the gateway unicasts a RREP -and optionally also a RREP_I -back to the originator of the RREQ.

In this way, a mobile node may obtain a default route although it has not requested this route. If the mobile node is to communicate with the Internet later, this default route can be used and hence, the mobile node does not have to send another request message in order to find a route to a gateway.

Another issue that must be considered is how a gateway should react when it receives several RREQs for the same destination. As already said, a gateway should send a RREP_I if it receives a RREQ and it does not find the destination address in its routing table. But since expanding ring search is used, a gateway may receive several RREQs for the same destination address. The question is, should the gateway reply every RREQ with a RREP_I or only some of them?

The chief advantage of sending a RREP_I for every received RREQ is that the

route to the gateway and the default route is updated. The chief disadvantage is that network resources are used. However, since the RREP_Is are unicast and not broadcasted to the requesting node, there will not be that much traffic generated. Hence, in the implementation used in this project:

A gateway replies every received RREQ with a RREP_I.

3.4.3 The Routing Table

Another issue that is worth discussing is how the routing table should change after a network-wide search without receiving any corresponding RREP. Assume that a source mobile node has done a network-wide search, without receiving any corresponding RREP. Hence, the source node assumes that the destination node is a fixed node located on the Internet.

According to "Global6", the source node sends its data packets using the default route. What the source node actually has to do is to create a route entry for the destination node in its routing table, see Table 3.1. If the route entry for the fixed destination node would not be created in the routing table, the source node would not find the address to the fixed node in its routing table when the next data packet would be generated and hence, the source would have to do another time consuming network-wide search.

Although it is necessary for the source node to create a route entry for the fixed node in its routing table, there is a disadvantage. The disadvantage is that a mobile node will have to create a route entry for every fixed node that it wants to communicate with, in its routing table. One might think that a mobile node already has to create a new route entry for every mobile node in the mobile ad hoc network it communicates with, so there should not be anything strange about that. The problem is, however, that the number of fixed nodes is much greater than the number of mobile nodes. If a mobile node desires to communicate with many fixed nodes, its routing table will grow rapidly. However, this is not as alarming as it sounds. In AODV the routes that are not used will expire and

eventually be deleted after a certain time, preventing the routing table to grow without control.

To summarize the idea:

Although a default route is used, a mobile node has to create a new route entry in its routing table, not only for every mobile node, but also for every fixed node that it communicates with.

DESTINATION ADDRESS	NEXT HOP ADDRESS
FN(0.0.1)	DEFAULT(-10)
DEFAULT(-10)	GATEWAY(1.0.0)
GATEWAY(1.0.0)	MN_A(1.0.3)

Table 3.1: The routing table of a mobile node after creation of a route entry for a fixed node. The values in the parentheses are examples of IP addresses used in ns2.

Table 4.1 shows how the routing table of a mobile node (S) should look like after creation of a route entry for a fixed node. If S wants to communicate with the fixed node FN, S sends its data packets to MN_A. When MN_A receives the data packets it searches its routing table to see if it has a valid route to FN. If a valid route to FN is found, the data packets are sent to the next hop specified by the route entry. On the other hand, if a valid route is not found, the packets would normally be dropped because MN_A does not know to which node the packets should be forwarded. "Global6" does not mention how this case should be handled. In the implementation used in this project, if MN_A does not find a valid route to FN and if the destination is a fixed node located on the Internet, MN_A creates a (or updates the) route entry for FN in its routing table. Next, it forwards the data packets to a gateway which forwards them toward their destination. To summarize the idea:

If an intermediate mobile node receives a data packet, it searches its routing table looking for a valid route to the destination. If a valid route to the destination is not found and the destination is a fixed node located on the Internet, the inter-

mediate mobile node creates a new route entry (or updates the old invalid route entry) for the fixed node and forwards the data packet toward the gateway.

3.4.4 Intermediate Node Operation upon Reception of RREQs

According to "Global6", when an intermediate mobile node receives a RREQ_I message, it must not send a RREP_I to the originator of the request message, even if the intermediate node has a route to a gateway. Instead, the intermediate mobile node rebroadcasts the received RREQ_I message. So far everything is correct, but the draft does not mention how an intermediate mobile node should react when it receives a RREQ message destined for a fixed node. The idea used in the implementation used in this study, is described below.

When an intermediate mobile node receives a RREQ message, it searches its routing table for a route to the destination. If the destination is a fixed node, the intermediate node must not send a RREP back to the originator of the request message even if the route is found. Because if the intermediate node sends a RREP back to the originator of the RREQ message, the originator thinks that the destination is a mobile node that can be reached via the intermediate node. It is important for the originator of the RREQ to know that the destination is a fixed node and not a mobile node, because sometimes these are processed differently. Hence, in the implementation used in this study:

If an intermediate mobile node receives a RREQ message destined for a fixed node, it must not send a RREP back to the originator of the RREQ even if the intermediate mobile node knows a route to the destination.

3.4.5 Unreachable Gateway

An interesting issue to consider is what a mobile node should do if it cannot reach any gateway, although the destination is a fixed node. This issue is not discussed in "Global6".

Assume that a mobile node (MN) is sending data packets to a fixed node through a gateway (GW). Assume further that MN moves away from GW such that GW becomes unreachable for MN, i.e. MN cannot reach GW or any other gateway -not even through another intermediate mobile node. What shall MN do?

In the implementation used in this study, MN broadcasts a RREQ_I message to the ALL_MANET_GW_MULTICAST address (see Section 3.4), i.e. the IP address for the group of all gateways in the mobile ad hoc network. However, since GW is unreachable for MN, the RREQ_I message is not received by GW (or any other gateway). MN uses the expanding ring search technique when it broadcasts RREQ_I messages, but not even a RREQ_I message with the TTL value set to NET_DIAMETER is received by any gateway, because MN cannot reach any intermediate mobile node that can forward the RREQ_I message on its behalf.

After doing a network-wide search without receiving any corresponding RREP_I message from any gateway, MN pauses for a while. When the pause is finished, MN does another network-wide search and pauses again if no RREP_I is received. This procedure continues until MN moves close to a gateway or an intermediate mobile node so it can receive a RREP_I from a gateway. When a gateway is found, MN sends its data packets to the fixed node through the found gateway.

Letting the mobile node to broadcast RREQ_I messages until it finds a gateway might not be the best solution. An alternative solution would be to drop all buffered data packets destined for the destination and send an ICMP Destination Unreachable message to the application. There might exist better solutions than the two mentioned above, but due to lack of time this issue was not investigated further. To summarize the idea behind the implementation used in this study:

If a mobile node cannot reach any gateways, it broadcasts RREQ_I messages until it finds one.

Chapter 4

GATEWAY DISCOVERY

The question of whether the configuration phase with the gateway should be initiated by the gateway (proactive method), by the mobile node (reactive method) or by mixing these two approaches (hybrid proactive/reactive method) has been discussed lately. In the following, the mechanisms of these three approaches are discussed. Proactive gateway discovery is discussed in Section 4.1, reactive gateway discovery is discussed in Section 4.2 and finally, hybrid gateway discovery is discussed in Section 4.3. The question of packet formats is also considered.

4.1 PROACTIVE GATEWAY DISCOVERY

The proactive gateway discovery is initiated by the gateway itself. The gateway periodically broadcasts a gateway advertisement (GWADV) message which is transmitted after expiration of the gateway's timer, ADVERTISEMENT_INTERVAL (see Table 5.2). The time between two consecutive advertisements must be chosen with care so that the network is not flooded unnecessarily. All mobile nodes residing in the gateway's transmission range receive the advertisement.

Upon receipt of the advertisement, the mobile nodes that do not have a route to the gateway create a route entry for it in their routing tables. Mobile nodes that already have a route to the gateway update their route entry for the gateway. Next, the advertisement is forwarded by the mobile nodes to other mobile nodes residing in their transmission range. To assure that all mobile nodes within the mobile ad hoc network receive the advertisement, the number of retransmissions is determined by NET_DIAMETER defined by AODV . However, this will lead to

enormously many unnecessary duplicated advertisements. A conceivable solution to the problem that occurs due to these duplicated advertisements, is presented in Section 4.1.1.

Although the problem of duplicated broadcast messages can be solved, one disadvantage remain. This disadvantage, which is general for all proactive approaches, is the fact that the message is flooded through the whole mobile ad hoc network periodically. This a very costly operation. Limited resources in a mobile ad hoc network, such as power and bandwidth, will be used a lot.

4.1.1 Duplicated Broadcast Messages

The problem of duplicated broadcast messages in mobile ad hoc networks is well known. In AODV, RREQ messages are broadcasted. To avoid duplicated RREQs, a RREQ ID is used (see Section 2.3.1). When a RREQ is received by a mobile node, it first checks to determine whether it already has received a RREQ with the same originator IP address and RREQ ID. If such a RREQ already has been received, the node discards the newly received RREQ.

In this thesis, the idea of comparing the RREQ ID with the originator IP address is used to solve the problem of duplicated advertisements. An advertisement is approximately a RREP_I message and since this message does not contain any field similar to the RREQ ID field in RREQ messages, a new AODV message has been introduced: the gateway advertisement (GWADV) message. This new AODV message is basically a RREP message extended with one field from the RREQ message, namely the RREQ ID field. Figure 4.1 illustrates the GWADV message format which can solve the problem of duplicated broadcast messages.

When a mobile node receives a GWADV, it first checks to determine whether a GWADV with the same originator IP address and RREQ ID already has been received during the last BCAST_ID_SAVE seconds . If such a GWADV message has not been received, the message is rebroadcasted. Otherwise, if such a GWADV message has been received, the newly received GWADV is discarded. Hence, du-

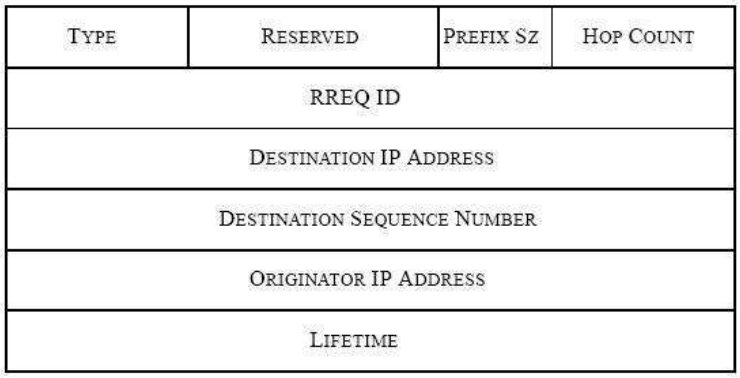


Figure 4.1: The format of a gateway advertisement (GWADV) message.

plicated GWADVs are not forwarded and the advertisement is flooded through the whole network without causing too much congestion. However, the disadvantage with this solution is the fact that a new AODV message is introduced which requires AODV to be modified.

It is worth mentioning that the mobile nodes randomize their rebroadcasting of the GWADV in order to prevent synchronization and subsequent collisions with other nodes rebroadcasts.

4.2 REACTIVE GATEWAY DISCOVERY

The reactive gateway discovery is initiated by a mobile node that is to initialize or update information about the gateway. The mobile node broadcasts a RREQ_I (see Figure 3.1) to the ALL_MANET_GW_MULTICAST address , i.e. the IP address for the group of all gateways in a mobile ad hoc network. Thus, only the gateways are addressed by this message and only they process it. Intermediate mobile nodes that receive the message just forward it by broadcasting it again. Since the message format is RREQ, which has a RREQ ID field as discussed in Section 4.1.1, duplicated RREQ_Is are discarded. Upon receipt of a RREQ_I, a gateway unicasts back a RREP_I which, among other things, contains the IP address of the gateway.

The advantage of this approach is that RREQ_Is are sent only when a mobile

node needs the information about reachable gateways. Hence, periodic flooding of the complete mobile ad hoc network, which has obvious disadvantages as discussed in 4.1, is prevented. The disadvantage of reactive gateway discovery is that the load on forwarding mobile nodes, especially on those close to a gateway, is increased.

4.3 HYBRID GATEWAY DISCOVERY

To minimize the disadvantages of proactive and reactive gateway discovery, the two approaches can be combined. This results in a hybrid proactive/reactive method for gateway discovery. For mobile nodes in a certain range around a gateway, proactive gateway discovery is used. Mobile nodes residing outside this range use reactive gateway discovery to obtain information about the gateway.

The gateway periodically broadcasts a RREP_I message (see Figure 3.2) which is transmitted after expiration of the gateway's timer, ADVERTISEMENT_INTERVAL (see Table 5.2). All mobile nodes residing in the gateway's transmission range receive the RREP_I. Upon receipt of the message, the mobile nodes that do not have a route to the gateway create a route entry for it in their routing tables. Mobile nodes that already have a route to the gateway update their route entry for the gateway. Next, the RREP_I is forwarded by the mobile nodes to other mobile nodes residing in their transmission range. The maximal number of hops a RREP_I can move through the mobile ad hoc network is ADVERTISEMENT_ZONE (see Table 5.2). This value defines the range within which proactive gateway discovery is used.

When a mobile node residing outside this range needs gateway information, it broadcasts a RREQ_I to the ALL_MANET_GW_MULTICAST address. Mobile nodes receiving the RREQ_I just rebroadcast it. Upon receipt of this RREQ_I, the gateway unicasts back a RREP_I.

Chapter 5

SIMULATION

To be able to evaluate the implementation of the Internet draft Global Connectivity for IPv6 Mobile Ad Hoc networks in ns2, some simulation scenarios must be run. This chapter describes what have been simulated, how the simulations have been set up and finally it presents the results of the simulations.

The simulations were conducted on an Intel Pentium IV processor at 2.4 GHz, 128 MB of RAM running Linux.

5.1 SIMULATION SETUP

This section describes the scenario, the movement model and the communication model used in this study. Moreover, it presents the parameters used in the simulations.

5.1.1 Scenario

The studied scenario consists of 14 mobile nodes, 2 gateways, 2 routers and 2 hosts. The topology is a rectangular area with 800 m length and 500 m width. A rectangular area was chosen in order to force the use of longer routes between nodes than would occur in a square area with equal node density. The two gateways are placed on each side of the area; their x,y-coordinates in meters are (100,250) and (700,250). All simulations are run for 110 seconds of simulated time.

Four of the 14 mobile nodes are constant bit rate traffic sources. They are distributed randomly within the mobile ad hoc network. The time when the five

traffic sources start sending data packets is chosen uniformly distributed within the first ten seconds of the simulation. After this time the sources continue sending data until one second before the end of the simulation. The destination of each of the sources is one of the two hosts, chosen randomly.

A screenshot of the simulation scenario is shown in Figure 5.1. The five mobile nodes that are marked with a ring, are the sources. The two hexagonal nodes are the gateways and the four square nodes are the two hosts and the two routers.

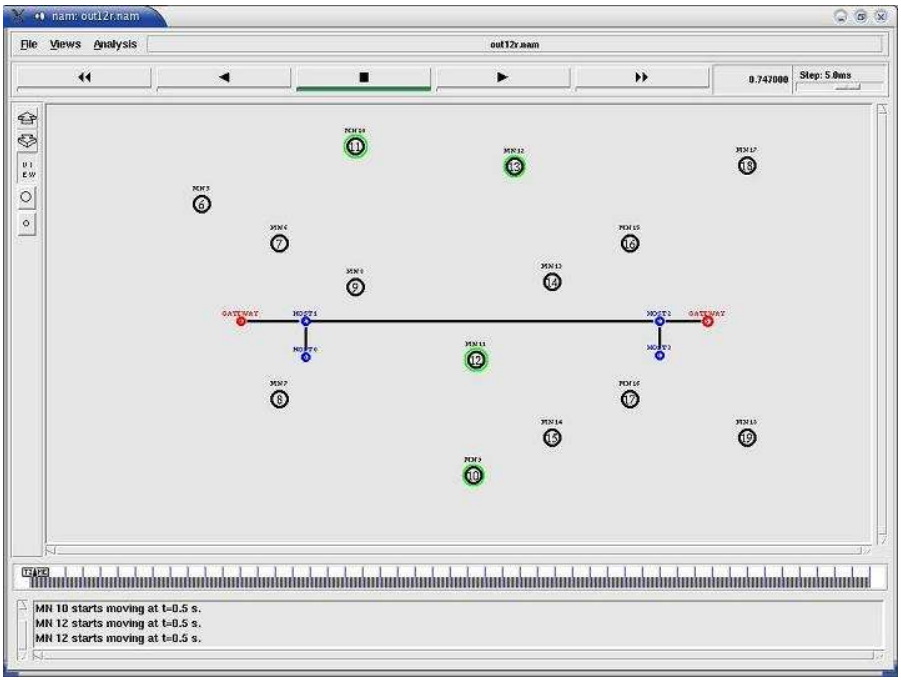


Figure 5.1: Screenshot of the simulation scenario.

5.1.2 Movement Model

The mobile nodes move according to the "random waypoint" model. Each mobile node begins the simulation by remaining stationary for pause time seconds. It then selects a random destination in the defined topology area and moves to that destination at a random speed. The random speed is distributed uniformly between zero (zero not included) and some maximum speed. Upon reaching the destination, the mobile node pauses again for pause time seconds, selects another

destination, and proceeds there as previously described. This movement pattern is repeated for the duration of the simulation.

The movement patterns are generated by CPU's movement generator (setdest). The chosen values for pause time and maximum speed are shown in Table 5.1.

5.1.3 Communication Model

In the scenario used in this study, five mobile nodes communicate with one of two fixed nodes (hosts) located on the Internet through a gateway. As the goal of the simulations was to compare the different approaches for gateway discovery, the traffic source was chosen to be a constant bit rate (CBR) source. Each source mobile node generates packets every 0.2 seconds in this study. In other words, each source generates 5 packets per second. Since each packet contain 512 bytes of data, the amount of generated data is 5*512*8 bit/s = 20 kbit/s, for each source.

The traffic connection pattern is generated by CMUs traffic generator (cbrgen.tcl). The main parameters in cbrgen.tcl are "connections" (number of sources) and "rate" (packet rate); see Table 5.1.

Parameter	Value
Transmission range	250 m
Simulation time	110 s
Topology size	800m x 500m
Number of mobile nodes	14
number of sources	4
Number of gateways	2
Traffic type	constant bit rate
Packet rate	5 packets/s
Packet size	512 bytes
Maximum speed	10 m/s

Table 5.1: General parameters used in all simulations.

5.1.4 Parameters

The parameters that are common for all simulations are given in table 5.1 and the parameters that are specific for some simulations are shown in table 5.2.

The transmission range is the maximum possible distance between two communicating mobile nodes. If the distance between two mobile nodes is larger than 250 m they cannot communicate with each other directly.

Parameter	Value
ADVERTISEMENT_INTERVAL	varied from 2-60 seconds
ADVERTISEMENT_ZONE	3 hops

Table 5.2: Specific parameters used in some simulations.

ADVERTISEMENT_INTERVAL is used when proactive and hybrid discovery methods are used . ADVERTISEMENT_ZONE is used for hybrid gateway discovery method and defines the range within which proactive gateway discovery is used.

5.2 PERFORMANCE METRICS

The second goal of this project was to "implement and compare different approaches for gateway discovery". Comparing the different methods is done by simulating them and examining their behavior. In the simulations in the following section, the effect of different gateway advertisement intervals are evaluated.

In comparing the gateway discovery approaches, the evaluation has been done according to the following three metrics:

- The packet delivery ratio is defined as the number of received data packets divided by the number of generated data packets.
- The end-to-end delay is defined as the time a data packet is received by the destination minus the time the data packet is generated by the source.
- The overhead is defined as the total number of AODV messages transmitted during the simulation. For AODV messages sent over multiple hops, each transmission of the message (each hop) counts as one transmission.

5.3 SIMULATION RESULTS

In this section the effect of varying gateway advertisement intervals is evaluated. Since gateway advertisements are not sent in the reactive gateway discovery approach, the results for this approach are constant and independent of the advertisement interval. Each data point is an average value of 10 runs with the same communication model, but different randomly generated movement patterns.

5.3.1 Packet Delivery Ratio

Figure 5.2 shows the packet delivery ratio with advertisement intervals between 2 and 60 seconds. As the figure shows, the packet delivery ratio is very high (above 99.8 %) for all three gateway discovery approaches. The figure also shows that the difference between the three approaches are very small. However, the proactive and hybrid approaches have some larger packet delivery ratio than the reactive approach, especially with short advertisement intervals. The reason is that the short advertisement intervals result in more gateway information (RREP_I and GWADV packets).

As described in Sections 4.1 and 4.3 a mobile node that receive a RREP_I or a GWADV message, update its route entry for the gateway. Therefore, it is more likely for the mobile nodes to have fresher and shorter routes to a gateway and thereby minimizing the risk for link breaks. Link breaks can result in lost data packets since the source continues to send data packets until it receives a RERR message from the mobile node that has a broken link. The longer the route is (in number of hops), the longer time it can take before the source receive a RERR and hence, more data packets can be lost.

When the advertisement interval increases, a mobile node receives less gateway information and consequently it does not update the route to the gateway as often as for short advertisement intervals. Therefore, the positive effect of periodic gateway information is decreased as the advertisement interval increases.

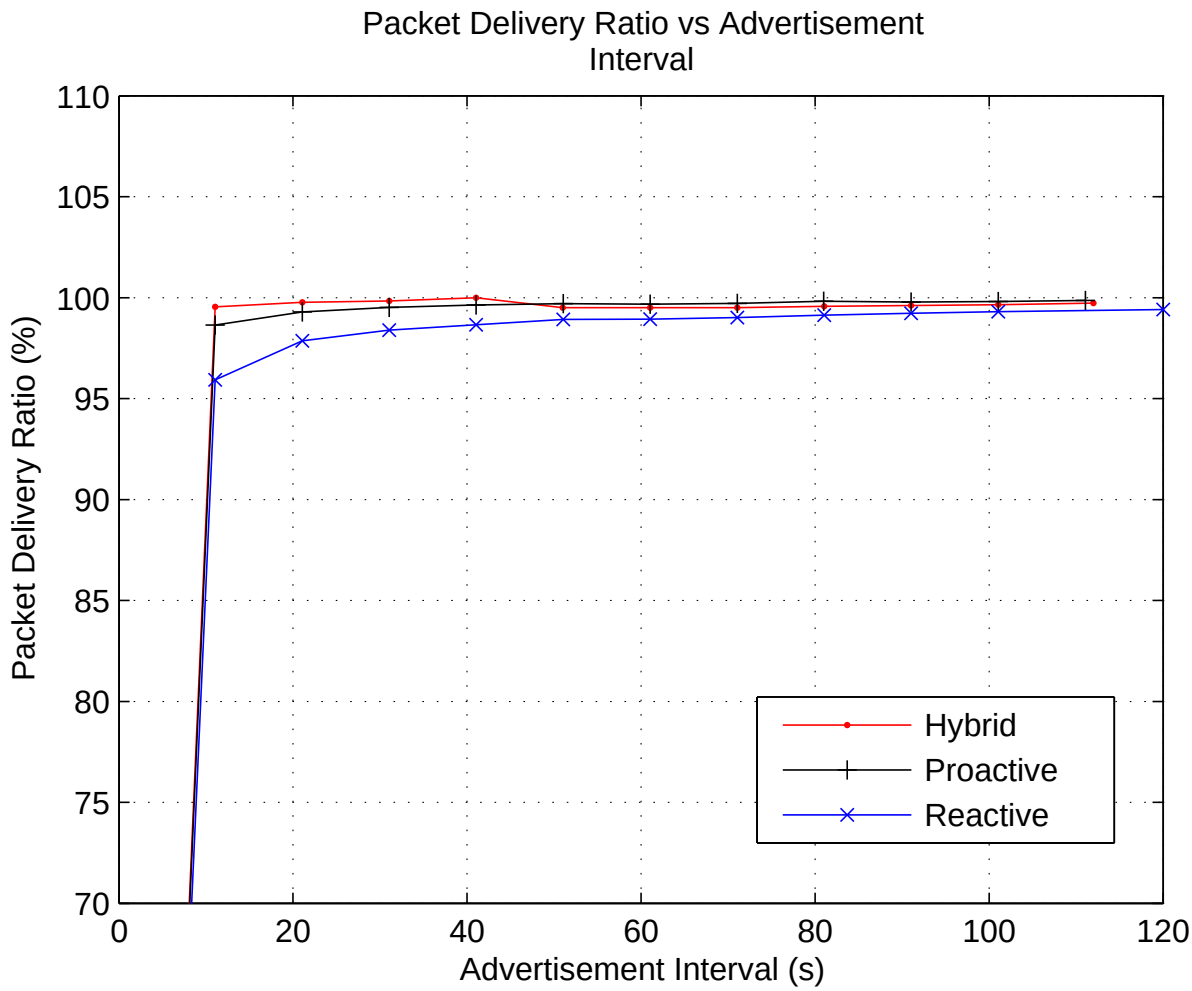


Figure 5.2: Packet delivery ratio

5.3.2 Average End-to-end Delay

Figure 5.3 shows the average end-to-end delay with advertisement intervals between 2 and 60 seconds. As the figure shows, the average end-to-end delay is less for the proactive and hybrid approaches than for the reactive approach. The reason is that the periodic gateway information sent by the gateways allow the mobile nodes to update their route entries for the gateways more often, resulting in fresher and shorter routes. With the reactive approach a mobile node continues to use a route to a gateway until it is broken. In some cases this route can be pretty long (in number of hops) and even if the mobile node is much closer to another gateway it does not use this gateway, but continues to send the data packets along the long route to the gateway further away until the route is broken. Therefore, the end-to-end delay increases for these data packets, resulting in

increased average end-to-end delay for all data packets.

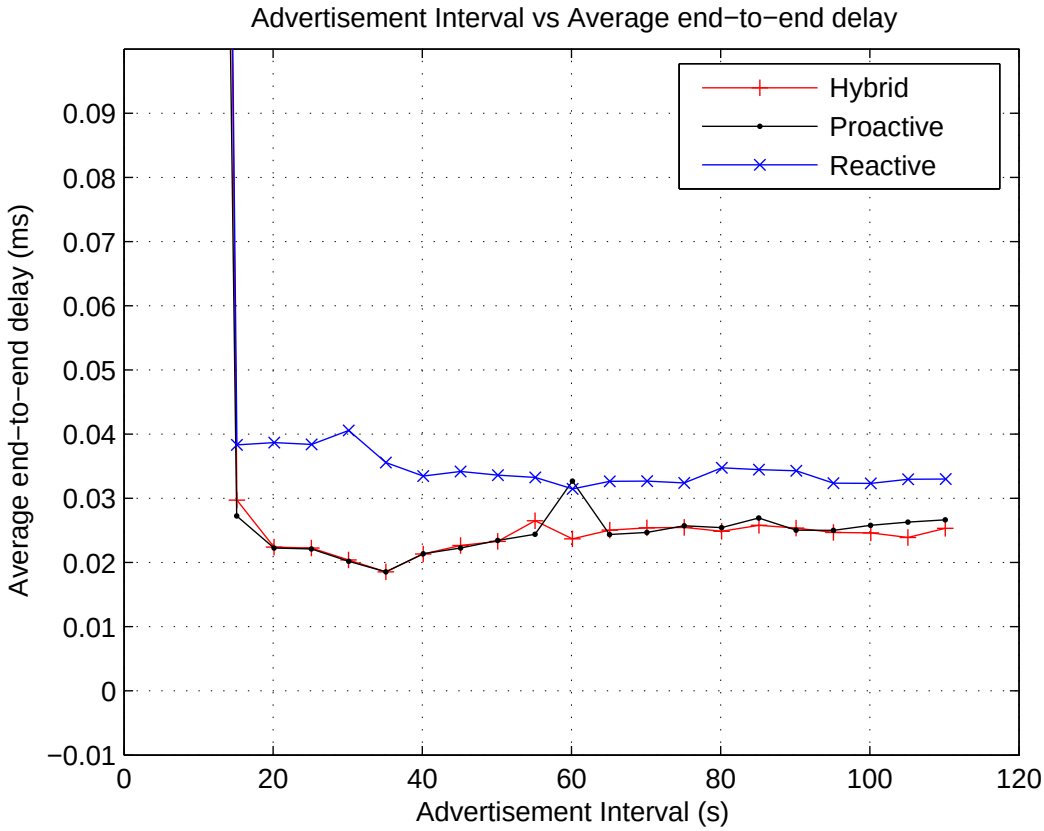


Figure 5.3: Average end-to-end delay

The figure also shows that the average end-to-end delay is decreased slightly for short advertisement intervals when the advertisement interval is increased. At the first thought this might seem unexpected. However, it can be explained by the fact that very short advertisement intervals result in a lot of control traffic which lead to higher processing times for data packets at each node. Moreover, since the AODV messages are prioritized over data packets, these have to wait in the routing queue until the AODV messages are sent, resulting in higher end-to-end delay.

5.3.3 AODV Overhead

Figure 6.4 shows the AODV overhead with advertisement intervals between 2 and 60 seconds. The AODV overhead is dominated by the periodically broadcasted RREP_I and GWADV messages. As the figure shows, the AODV overhead

is larger for the proactive and hybrid approaches than for the reactive approach, especially for short advertisement intervals. This is an expected result since the proactive and hybrid approaches periodically broadcast gateway information no matter if the mobile nodes need them or not, while the reactive approach broadcasts gateway information only when a mobile node sends a request for it. Moreover, the figure shows that the AODV overhead decreases for the proactive and hybrid approaches as the advertisement interval increases. This is due to less frequent gateway information transmissions.

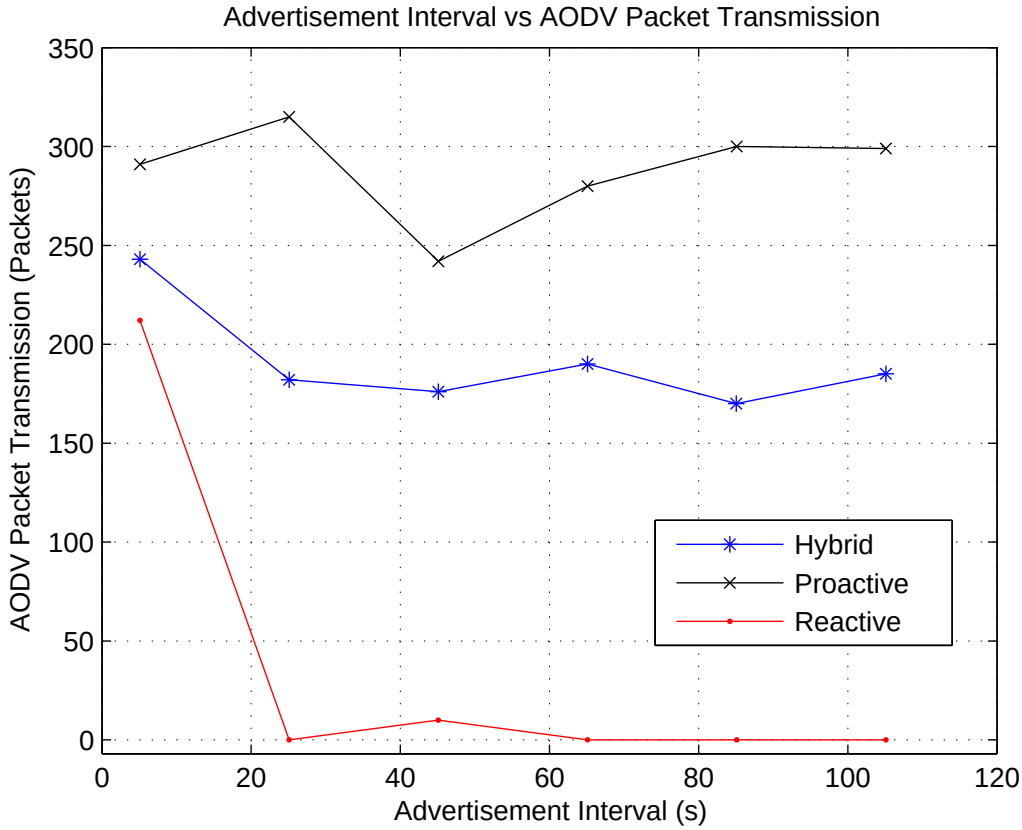


Figure 5.4: AODV overhead

Finally it can be noticed that the overhead for the hybrid approach is much greater than for the proactive approach when the advertisement interval is short. This is due to duplicated messages as described in Section 4.1.1. In the hybrid method, gateways broadcast RREP_I messages which are forwarded by mobile nodes until the TTL (time to live) value for the messages are decreased to zero. Hence, there are some amount of duplicated RREP_I messages, i.e. a mobile node

can receive the same RREP_I several times. On the other hand, in the proactive method, gateways broadcast GWADV messages which are forwarded by mobile nodes only if they have not forwarded the messages before. Hence, there are no duplicated broadcast messages generated when the proactive approach is used.

In the simulations where hybrid gateway discovery has been used, the TTL value has been set to ADVERTISEMENT_ZONE which is defined as 3 in this study. This implies that a RREP_I message is received by all mobile nodes within a range of 3 hops from the gateway. The discussion above and Figure 5.4 illustrates why RREP_I messages cannot be used for a proactive gateway discovery method unless it is modified. Because in the proactive approach the TTL value would have to be set to NETWORK_DIAMETER, which equals 30 hops in the AODV implementation in NS. The figure shows namely that a lot of duplicated RREP_I messages are generated when TTL is set to 3; then one can imagine how much overhead a TTL value of 30 would have generated.

Chapter 6

CONCLUSIONS

The thesis has considered the Internet access of mobile nodes in a mobile ad hoc network. The ad hoc routing protocol AODV has been extended to route packets, not only within a MANET but also between a wireless MANET and the wired Internet. To be able to achieve this, some nodes must act as a mixture of a mobile node and a fixed node. The communication between the wireless and the wired network must pass through these nodes, which are referred to as gateways. In this project, three methods for detection of these gateways have been presented, implemented and compared. The three methods for gateway detection are referred to as reactive, proactive and hybrid gateway discovery. The comparison between these methods provides us useful information.

Regarding the packet delivery ratio, the result is largely the same, regardless of which gateway discovery method is used. As for the average end-to-end delay, the proactive and hybrid methods perform slightly better than the reactive method. Concerning the routing overhead, when the advertisement interval is short the reactive method generates much less overhead than the proactive method, which in turn generates much less overhead than the hybrid method. When the advertisement interval increases, all three methods generate virtually the same routing overhead.

The results presented are valid for the specific scenario used in this project. Therefore, one cannot tell which of the gateway discovery methods is the best one for every possible scenario. There are many factors that can be changed and

their impact should be investigated. Unfortunately the scope of this project made it impossible to deal with more than a part of these interesting issues. The aim in future work will be to examine them in greater detail. For example, changing the number of mobile nodes and the size of the topology changes the mobile node density. Its impact should be investigated. Another issue that should be examined is the impact of the number of gateways and the distance between them. Certain other questions of interest are the number of traffic sources, the number of packets sent per second, the size of the data packets, and the speed of the mobile nodes.

Bibliography

[1] Murthy C. Siva Ram and Manoj B. S., *Ad Hoc Wireless Networks: Architectures and Protocols*. Pearson Education, 2005.

[2] Belding Royer E.M., Sun Y., and Perkins C, "Global Connectivity for Ipv4 Mobile Ad Hoc Networks," *IETF Internet Draft Work in progress*, November 2001.

[3] Wakikawa R., Malinen J., Perkins C., Nilsson A., and Tuominen A.J., "Global Connectivity for Ipv6 Mobile Ad Hoc Networks," *IETF Internet Draft*, November 2001.

[4] Perkins C., Belding Royer E.M., and Das S., "Ad Hoc On-Demand Distance Vector (AODV) Routing," *IETF Internet Draft*, January 2002.

[5] Haas Z.J., Pearlman M.R., and Samar P., "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," *IETF Internet Draft, work in progress*, July 2002.

[6] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing, Kluwer Acadamic Publisher*, vol. 353, pp. 153–181, 1996.

[7] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector (AODV) Routing," *Proceedings of IEEE Workshop on Mobile Computing System and Application 1999*, pp. 90–100, February 1999.

[8] M. Joa Ng and I. T. Lu, "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," *IEEE Journal on Selected Area in Comminications*, vol. 17, no. 8, pp. 1415–1425, August 1999.

[9] T. H. Clausen, G. Hasen, L. Christensen, and G. Behrmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments and

Simulation," *Proceedings of IEEE Symposium on Wireless Personal Mobile Communications*, September 2001.

[10] Rui TENG, Hiroyuki MORIKAWA, and Tomonori AOYAMA, "A Low Overhead Routing Protocol for Ad Hoc Networks with Global Connectivity," *IEEE.*, 2005.

[11] Vinh Dien HOANG, Zhenhai SHAO, Masayuki FUJISE, and Hoang Minh NGUYEN, "A Novel Solution for Global Connectivity in Manet," *IEEE*, 2004.

[12] Clausen T., Jacquet P., Laouiti A., Minet P., Muhlethaler P., Qayyum A., and Viennot L., "Optimized Link State Routing Protocol," *IETF Internet Draft*, July 2002.

[13] Xi J. and Bettstetter C., "Wireless Multihop Internet Access: Gateway Discovery," *Routing and Addressing, in Proceedings of the International Conference on Third GenerationWireless and Beyond (3Gwireless'02), San Francisco*, May 2002.

[14] Hong X., Xu K., and Gerla M., "Scalable routing protocols for mobile ad hoc networks," *IEEE Network*, August 2002.

[15] M. Canne S. and Floyd S., *ns Network Simulator*, Fall K.; Varadhan K., and the VINT project, July 2005.