The Effect of the Access Point Selection Method on Reachability between a Mobile Ad hoc Node and a Fixed Node

Master's Thesis

Tuulia Kullberg

Helsinki University of Technology
Department of Computer Science and Engineering
Telecommunications Software and Multimedia Laboratory
Espoo 2005

Teknillinen korkeakoulu
Tietotekniikan osasto

Tietoliikenneohjelmistojen ja Multimedian Laboratorio

HELSINKI UNIVERSITY OF TECHNOLOGY

ABSTRACT OF MASTER'S THESIS

Author: Tuulia Kullberg

Name of thesis:
The effect of the access point selection method on reachability between a mobile ad hoc node and a fixed node

Date: 4th May 2005 **Pages:** 60

Department: Department of Computer Science and Engineering **Chair:** T-79

Supervisor: Professor Hannu H. Kari
Instructor: M.Sc. Mikko Särelä

Mobile ad hoc networks have typically been considered as self-sufficient, closed networks, where no connections outside its boundaries have been possible. For the military and rescue applications, where no reliance can or wants to be made on existing network infrastructures, that assumption is probably enough. The situation is, however, different with civilian applications, which will more than likely require connections also with the fixed Internet and the services it has provide. The global connectivity can be offered by introducing additional routers at the edge of the ad hoc network. These routers act as the gateways between the closed ad hoc network and the fixed network by forwarding packets between the two.

This thesis analyses the impact of the selection of that router by proposing and implementing two selection methods, Break-Before-Make and Make-Before-Break, and studying their effect on the reachability between a mobile ad hoc node and a fixed node. The analysis is performed using simulations and DSDV as the ad hoc routing protocol.

The simulations showed that Make-Before-Break performs constantly better than Break-Before-Make, if the effect of using DSDV is eliminated. When the impact of DSDV is taken into consideration, no differences can be seen, as the performance of the DSDV protocol becomes the dominant factor.

Keywords: mobile ad hoc network, global connectivity, reachability, access point selection
Language: English

Kirjoittaja: Tuulia Kullberg

Otsikko:
Yhdyskäytävän valintatavan merkitys liikkuvan ad hoc solmun ja kiinteän solmun väliseen tavoitettavuuteen

Päivämäärä: 4. toukokuuta 2005 **Sivuja:** 60

Osasto: Tietotekniikan osasto **Professuuri:** T-79

VALVOJA: Professori Hannu H. Kari
OHJAAJA: DI Mikko Särelä

Liikkuvat ad hoc verkot on tyypillisesti mielletty itsenäisiksi, suljetuiksi verkoiksi, jotka eivät ole tarjonneet mahdollisuuksia verkon ulkopuolisiin yhteyksiin. Tämä on oletus on luultavasti riittävä armeija- sekä pelastussovelluksille, jotka eivät perusluonteensa takia ole voineet tai halunneet luottaa olemassa oleviin verkkokomponentteihin. Lukumäärältän jatkuvasti kasvavien siivilisovellusten kanssa tilanne on kuitenkin toinen, sillä ne enemmän kuin todennäköisesti tulevat haluamaan yhteyden ad hoc verkon sisäisten solmujen lisäksi esim. Internettiin ja sen tarjoamiin palveluihin. Nämä yhteydet voidaan tarjota lisäämällä ad hoc verkon reunoille tähän tarkoitettuja reitittimiä, jotka toimivat yhdyskäytävinä välittämällä paketteja suljetun ad hoc verkon ja kiinteän verkon välillä.

Tämä diplomityö analysoi yhdyskäytävänä toimivan reitittimen valinnan merkitystä liikkuvan ad hoc solmun ja kiinteän solmun väliseen tavoitettavuuteen. Se ehdottaa ja toteuttaa kaksi erilaista valintatapaa, joiden vaikutusta tutkitaan käyttämällä simulaatioita. DSDV on valittu ad hoc verkon sisäiseksi reititysprotokollaksi.

Simulaatioiden tulokset osoittavat, että kahdesta valintamallista Make-Before-Break toimii kaikissa ympäristöissä paremmin kuin Break-Before-Make, jos DSDV:n vaikutus tuloksiin eliminoidaan. Jos DSDV:n vaikutus otetaan huomioon, ei eroja valintamallien kesken nähdä, koska tällöin DSDV:n suorituskyky nousee hallitsevaksi tekijäksi.

Keywords: liikkuva ad hoc -verkko, tavoittavuus, Internet-yhteys, yhdyskäytävän valinta
Kieli: englanti

Acknowledgements

First of all I would like to express my gratitude to both my supervisor professor Hannu H. Kari and my instructor M.Sc. Mikko Särelä for giving me invaluable ideas, advice and guidance during the process of writing this thesis.

I would also like to thank GO-CORE and Samoyed projects for funding my master's thesis.

Finally I want to thank my husband Kristian Kullberg for all his support and encouragement throughout my studies at HUT.

Espoo, 4th May 2005
Tuulia Kullberg

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The wireless communication has experienced considerable changes during the last few years as the communication devices have gained remarkable improvements both in convenience and performance. The technology has enabled longer battery powers and bigger memory capacities while at the same time the amount of applications targeted at wireless communication has risen. As wires no longer tied users at their desks, new possibilities and needs within wireless networking were identified. One of them was the concept of ad hoc networks, networks that can be formed without any pre-existing and supporting infrastructure, on-the-fly.

The idea of ad hoc networks originates already from DARPA (Defence Advanced Research Projects Agency) packet radio network's days early 1980's. They are based on the idea that every mobile node must participate not only as a host, but also as a router and forward packets between the source and destination nodes. As the topology allowed to go through continuous changes, the task of completing the routing efficiently and correctly is demanding. Many different routing protocols based on diverse assumptions and intuitions have been proposed and implemented.

For the military and rescue applications, where no reliance can or want to be made on existing network infrastructures, closed and self-sufficient ad hoc networks are generally enough. But the situation is different with civilian applications, which will more than likely require connectivity also with the fixed Internet and the services it has provide. The global connectivity can be offered by introducing additional routers at the edge of the ad hoc network. These routers act as access points between the closed ad hoc network and the fixed network by forwarding packets between the two.

This thesis studies the importance of the selection of that router and proposes a couple of selection methods for it. The main focus is on the effect of the selection

methods on performance of the communication between the mobile node and the fixed node, which is examined using simulations.

The rest of this thesis is organized as follows. Chapter 2 defines the problem statement in more detail. The criteria for the evaluation of the selection methods are listed in Chapter 3. Chapter 4 presents the existing literature relevant to this thesis. Chapter 5 explains the selection methods and Chapter 6 the simulations used in this thesis. The results for the simulations are presented and analysed in Chapter 7. Chapter 8 concludes the paper and gives propositions for future work.

Chapter 2

Problem statement

The purpose of this chapter is to introduce the research problem. First some basic concepts about computer networks are briefly explained after which the actual problem statement is defined.

2.1 Internet Protocol

Internet Protocol version 4 (IPv4) [26] was developed in 1970's and has since remained as the dominant network layer protocol. The introduction of world wide web (www), however, resulted in an exponential increase in the amount of Internet users and popularity never imagined 30 years ago. Internet Protocol version 6 (IPv6) [7, 8] is a next version of IPv4.

As the most significant improvements IPv6 offers larger address spaces, an integral part for support of mobility and an option to extend the protocol further in order to correspond to the changed needs of future times. The mass transition from IPv4 to IPv6 in the Internet is possible but not yet of current interest as some of its features including security still need further considerations and solutions. In the future, when high speed Internet access will be widely provided by the mobile phones for billions of users, IPv6 will nevertheless remain as the best possible option. Nowadays IPv6 is mainly deployed in research studies and test networks.

2.2 Fixed network

A computer network is a structure consisting of data sources and destinations called hosts and computers forwarding the messages between the hosts called

routers. Every network has a unique network identifier, which is presented as the prefix of nodes' IP address. This enables the correct routing between any two separate networks. As every host and router of the same network have the same prefix as part of their IP addresses, routes can be stored pointing to networks rather than to individual hosts. With large networks containing thousands or even milliards of users, it is a huge advantage and results in reasonably sized and manageable routing tables, which would otherwise grow out of control.

Fixed network is often heard to be used as a synonym for Internet, a worldwide network composed of a collection of interconnected smaller networks. Term fixed, however, relates more to the features the network has. In a fixed network, the topology can be considered nearly static, which makes the routing information long-lived and therefore relative easy to collect and maintain.

2.3 Mobile ad hoc network

Fixed networks, consisting of stationary backbones and routers, do not however exist in all places and all situations. Therefore a new idea called ad hoc networks was developed. Ad hoc networks are autonomously operating clusters, which enable the formation of a functional communication network without any help from pre-existing infrastructures. Combined with wireless transmission media like infrared or radio waves that allow users to have total freedom of movement, they are assumed to offer great possibilities e.g. in military or disaster relief areas where no reliance can or want to be made on available network components.

Mobile ad hoc networks (manets) consist of a collection of arbitrarily located independent wireless platforms, usually simply referred to as mobile nodes, within the transmission range of some other participant. They are closed networks having dynamic and arbitrarily changing, multihop topologies. As the topology is allowed to go through continuous changes, the task of completing the routing efficiently and correctly becomes demanding.

2.3.1 Routing in Ad Hoc networks

Routing in ad hoc networks can be divided into three parts. First, when a network is newly formed and no route yet exists between source and destination nodes, route discovery has to be completed. After a successful route discovery begins the maintenance of the active routes, which means noticing link failures and taking corrective actions to repairing the affected routes. The last phase includes the deletion of unnecessary routes.

Routing protocols for ad hoc networks can be divided into three categories named proactive, reactive and hybrid. Proactive routing protocols (e.g. [24, 35]) spread the routing information of all nodes in the network using periodic control messages. Reactive routing protocols (e.g. [6, 23]), on the other hand, operate only when routing information is needed, i.e. on demand. A hybrid protocol (e.g. [13]) is a combination of these two using proactive approach within a small zone and reactive beyond this.

DSDV

Destination Sequence Distance Vector routing protocol (DSDV) [24] is a proactive manet routing protocol, which uses two kinds of message types, periodically sent advertisements and immediate update messages.

All the mobile nodes using DSDV are required to maintain a list of all the available destinations in their routing tables and advertise them periodically. In an optimal situation every mobile has therefore an image of the topology of the network in memory and at the time of receiving data, forwarding can start immediately as every manet node is able to locate every other node in the network. However, with frequent link failures, the periodical advertisements can not really keep up with the changing routes, which is why immediate update messages were introduced to the protocol. They are sent immediately to all neighbouring nodes as a response to node movements and link breakages. They also try to decrease the amount of extra load the periodical advertisements tend to produce.

2.4 Global connectivity

The nodes in ad hoc networks can communicate and deliver data only between other nodes within the reach of that network. Providing communication within the closed network is not, however, always sufficient as some of the manet nodes will more than likely require connectivity with the fixed Internet and the services it has provide. This is referred to as global connectivity.

This thesis uses the principles of Globalv6 protocol [38] to achieve global connectivity. Globalv6 introduces additional components called access points to the architecture of an ad hoc network. Access points are routers that are capable of understanding both the routing protocol used inside the ad hoc network as well as sending packets to and receiving them from the Internet or some other fixed network. By forwarding all the packets through these access points the nodes can reach destination nodes located in the Internet.

2.5 Mobility management

The characteristics of wireless ad hoc networks support the idea of mobility by their nature and the ad hoc routing protocols have therefore been designed to perform better under continuously changing topologies than the traditional routing protocols designed for fixed networks. However, by utilizing merely ad hoc routing protocols, the nodes are restricted to migrate only within the boundaries of a single ad hoc network. Additionally, if global connectivity is provided, the nodes must stay within the reach of the access points they use. Mobile IP, which is specified for both IPv4 [10] and IPv6 [15], can be used to enable the migrations between two access points while at same time preserving all the existing connections and providing always-on reachability for the mobile nodes.

The general architecture of Mobile IPv6 consists of a mobile node (MN), a correspondent node (CN) and a home agent (HA). The mobile node and the correspondent node are the two communicating peers, whereas the continuous connectivity is provided by the home agent, which catches all the packets destined to the mobile node and tunnels them to the mobile node's current location whenever the mobile node is visiting some foreign network. It is therefore extremely important for the mobile node to update its location information with the home agent whenever it changes its current point of attachment.

Mobile IP is not the only possibility to mobility management. Other solutions include e.g. link layer mechanisms [3], Host Identity Protocol (HIP) [19], Stream Control Transmission Protocol (SCTP) [32] and Session Initiation Protocol (SIP) [27].

2.6 Reachability

Reachability is a key factor when analysing the performance of any network as it defines whether the destination can receive data packets sent by the source node or not. This thesis is interested in reachability between a mobile node locating in an ad hoc network and a stationary node in a fixed network, a situation where all the messages must travel through some access point. The selection of the access point in use can therefore be predicted to have an impact on the communication properties between the two, which is in fact the main interest in this thesis.

2.7 Simulation

Simulating is a widely used method in performance studies of ad hoc networks because of its low costs and high availability of well-known tools. It means creating an artificial environment which has similar behaviour and characteristics as a real network would have. A simulator is usually a computer program that can quite easily be enhanced with both new features, i.e. newly developed protocols, as well as a variety of test runs. It can therefore be customized to meet the needs of different behaviour studies.

This thesis uses Network Simulator 2 [21] as the simulation tool, because it already provides some of the features needed to accomplish this thesis successfully. Other alternatives for simulating ad hoc networks would have been e.g. Scalable Wireless Ad hoc Network Simulator [34], GloMoSim [11] or OPNET [22].

2.8 The Problem Statement

The main objective of this thesis is to design access point selection methods and study their impacts on reachability between a mobile node of a wireless ad hoc network and its corresponding node in a fixed network.

The impact will be studied using simulation. IPv6 is used as the network layer protocol and DSDV as the manet routing protocol. Globalv6 and Mobile IPv6 are used to provide global, continuous connectivity for the mobile nodes.

Chapter 3

Design criteria

This chapter defines the criteria that will be used in evaluating the proposed access point selection methods. The criteria are designed to allow a comparison between the selection methods, and they will be verified by evaluating the results gathered from the simulation runs.

3.1 Consistency

Consistency is based on two things. First, the results from the simulation runs for one set of parameters should have only small variance between each others. The results should also be similar in all simulations. If this is not the case, then the results can not be said to reliably indicate one of the solutions to perform better than the other one.

Consistency is a basic criteria that the simulations must satisfy in order to make the rest of the criteria worth analysing.

3.2 Packet delivery fraction

Packet delivery fraction means the ratio between the data packets delivered to the destinations and those originated by the source nodes. It tells how many of the packets are dropped because of the lack of route either in the source nodes or nodes along the route, and shows how well the candidate protocol is performing.

3.3 Delay

Delay in computer networks means the amount of time passed between the source node's decision to send data and the actual time of receiving the data at the destination. Real time services expect it to be within some application dependent pre-defined boundaries in order to be able to provide the service at all. Even if the application has no special delay requirements, shorter delays result in faster service and higher user satisfaction.

3.4 Jitter

Jitter means the variation in time between the arriving packets and should be kept small in order to be able to provide quality service. The existence and amount of jitter can be revealed by examining the successful packet deliveries in the simulations.

With non-interactive applications, the effect of jitter can be reduced by using buffers. Especially the transport layer protocol TCP [25] is sensitive to variance in delays, which can seriously deteriorate its performance. Buffers and the performace of the TCP are, however, out of scope of this thesis.

3.5 Control overhead

Even though communication devices have gained remarkable improvements both in battery power, bandwidth and memory capacity, the resources are still scarce and must be consumed economically. Therefore, the load the access point selection method causes on the network must be taken into consideration. The load, i.e. the total amount of control messages needed in order to enable the global connectivity, becomes an especially important factor when considering the efficiency and scalability properties of a selection method.

Chapter 4

Previous work

This chapter describes existing research and theory relevant to this thesis and is organized as follows. Fixed networks are explained first, after which mobility and its successful management are studied. Ad hoc networks and means to provide global connectivity are introduced next. Finally, simulation studies end the chapter.

4.1 Fixed Network

Traditionally computer networks have been quite static consisting of stationary routers and hosts connected to them. A network like this is often referred to as a fixed network, as it does not go through any large changes in its topology after the initial configuration. The reason behind the static topology has mainly been the large and heavy computers and the usage of copper wire or optical fiber as the transmission media.

The object of a computer network is to enable the communication between any two hosts. Therefore all the hosts within the network must be given a unique identity, so that the routers, whose task is to act as the data forwarding entities between the hosts, know who the destination is. At the time of the development of the networking concepts, it was thought to be a good idea to tie the identity of a host to its IP address, which also has to be unique as it defines the location of the host. This causes, however, problems as is explained in Section 4.2.

An IP address was designed to consist of a network part identifying the network and a host part identifying a specific host within that network. By separating the two, routing could be made much more efficient as routes could be stored pointing to networks rather than to individual hosts. This helps the routing tables to stay

reasonably sized and manageable as host specific routes are needed and used only within the home network or access network, where the number of nodes is limited (e.g. tens or hundreds).

However, the amount of available IPv4 addresses [26] is about run down because of the massive increase in the number of Internet users. IPv6 [7, 8] responds to this challenge by increasing the address space from 32 to 128 bits, but before it becomes widely used, other solutions proposed are be utilized. Subnetworking [4] is of them. It allows multiple physical networks to share the same network address, which causes changes both in the structure of the IP address and routing. The host part has to be now divided into two parts, where the first one identifies the subnetwork and the second one the host. The length of the subnetwork part may vary depending on the organization's needs and has to be therefore explicitly announced as a subnetwork mask together with the whole address. As a result of subnetworking we get a hierarchical address system, where routing decisions have to be made based on both the network part and the subnetwork part.

4.2 Physical mobility

The strict binding between the identity of a host and its IP address works well with fixed networks and stationary hosts. However, it makes it impossible for a host to change its home network and still be reachable without getting a new, topologically correct IP address. Today's available wireless transmission media like radio waves and infrared have, however, given the users a different kind of freedom than before and introduced a new dimension called mobility to networking.

There are three types of mobility, which all set their own requirements for communication networks. We have networks, which support node mobility, mobile networks, and mobile ad hoc networks [17].

Networks supporting node mobility have a topology consisting of a few to several mobile nodes in otherwise more or less static environment. Each mobile node is assumed to handle its own mobility including both noticing the movements between networks and as well initiating the needed actions in order to be able to continue the data communication. Mobile IP [10, 15] is a protocol developed to handle this kind of mobility and is studied later in Section 4.3.1 in more detail.

With mobile networks, the topology inside the network remains nearly static as the nodes themselves are not mobile but the entire network instead. An example of a mobile network could be a bus, where users sit on their places with their computers as the bus at the same time carries the whole network of users with it. In this case mobility management for all the nodes of the network can be handled

by selecting a few nodes called mobile routers responsible for the task. It might therefore even be possible for the other nodes to be unaware of the mobility of the network. Solutions for mobility management in mobile networks are based on extending Mobile IP protocols.

A mobile ad hoc network resembles a combination of the two previous as it supports mobility of individual nodes, but can also form together moving clouds of nodes, i.e. mobile networks. Unlike the two, however, it does not need any pre-existing infrastructure to rely on, which allows ad hoc networks to have highly dynamic topologies. This thesis concentrates on fixed networks supporting node mobility and mobile ad hoc networks, which are explained in Section 4.4.

4.2.1 Node mobility

Usually node mobility is regarded as a node's transition between different sub-networks or domains. This kind of mobility always creates a need for re-addressing as the prefix of the network changes. This kind of mobility is called *macro-mobility* [33], and it is one of the three possible types of mobility a node can perform. The other two are *micro-* and *nano-mobility*. As opposed to macro-mobility, in micro- and nano-mobility the IP address does not need to be changed. Micro-mobility refers to mobility within the same network, which in fixed networks means rerouting. Nano-mobility, on the other hand, refers to changing routes in wireless network.

Mobility described above considers the communicating node, i.e. the terminal, to be the mobile subject. The subject can, however, also be a user or even an application. Furthermore, the identity of a user on a terminal may either be changed meaning multiple user accounts or a user may physically change from one terminal to another. Application mobility means changing the execution location of the application between separate terminals. All of these have special requirements to consider, but this thesis is only interested in terminal mobility.

4.2.2 Mobility Models

The performance in mobile ad hoc networks is not affected only by the efficiency of routing protocols and data processing techniques but also by other parameters including node density, topology and movement of individual nodes related to each others. Unfortunately the exact routes of nodes in real usage situations are not really known, so the best that can be done is to create estimations called mobility models and study the performance based on them.

Mobility models can be divided in two categories: entity and group mobility models [2]. Entity models are based on randomized mobility of each node individually whereas group mobility models randomize the mobility of a cloud of nodes staying close to each other and moving as a group. This thesis uses an entity mobility model to model the topology of ad hoc networks, the most well-known of which are described next shortly.

Random walk

Random walk is first of the simple mobility models presented in this thesis. Term simple refers to the fact that a node's behaviour does not depend on the past movement history in any way. In random walk each node selects a random direction from a uniform distribution between 0 and 2π and a random speed from a uniform distribution between $Speed_{min}$ and $Speed_{max}$, after which it moves in a straight line according to the selected parameters for a predefined time *t*. Direction and speed are randomized again after *t* seconds.

Random walk tends to produce localized mobility instead utilizing of the whole simulation area and is often referred to as Brownian motion.

Random direction

Random direction [28] is second of the simple mobility models. It resembles random walk as it also uses a random direction from a uniform distribution between 0 and 2π and a random speed from a uniform distribution between $Speed_{min}$ and $Speed_{max}$ as two of the parameters defining mobility. However, instead of stopping after some predefined *t* seconds, the movement is continued in a straight line until the node meets the edge of the simulation area, where the it pauses for a time t_{pause} before choosing another direction and speed. This can lead to a situation where the nodes have the tendency to remain at the edges for rather long times. Pause time t_{pause} is selected from a uniform distribution between $Pause_{min}$ and $Pause_{max}$.

Random direction produces global mobility as the nodes move between the edges of the simulation area. It is able to maintain the initial node density approximately constant throughout the simulations [29], which is why it was chosen to be the mobility model used in this thesis.

Random waypoint

Random waypoint [14] is third of the simple mobility models. In random waypoint, each node selects a random destination point from the simulation area, where to it moves in a straight line with a random speed from a uniform distribution between $Speed_{min}$ and $Speed_{max}$. At the destination the node pauses for a pause time t_{pause}, which is selected from a uniform distribution between $Pause_{min}$ and $Pause_{max}$. After t_{pause} seconds, another destination, speed and t_{pause} are randomized.

Gauss-Markov

Gauss-Markow is a more complex mobility model as it randomizes the speed and direction of each node based on their current values and standard deviation. New values are updated at a fixed frequency and taken into use without no separate pause times. Additionally, the nodes are kept away from the edges of the simulation area by changing the direction whenever they get too close.

Gauss-Markow produces smooth curves covering most of the simulation area.

Boundless simulation area

Boundless simulation area model [12] resembles the Gauss-Markow model explained above, as it assumes each node to make continuous changes to speed and direction based on their current values with a fixed frequency. The difference is that the simulation area is modelled as a toroid shaped. Thus the nodes are not kept away from the edges but are instead immediately transferred to other side of the area with edge hits.

In boundless simulation area the nodes move with few sudden turns and smooth curves covering the whole simulation area.

4.3 Mobility Management

Mobility management protocols allow nodes to change their location in fixed networks or, when ad hoc networks are considered, change their point of attachment to the fixed network and still maintain their existing connections. The readdressing related to the mobility could in fact be solved without the mobility management protocols using e.g. stateful and stateless address autoconfiguration for IPv6

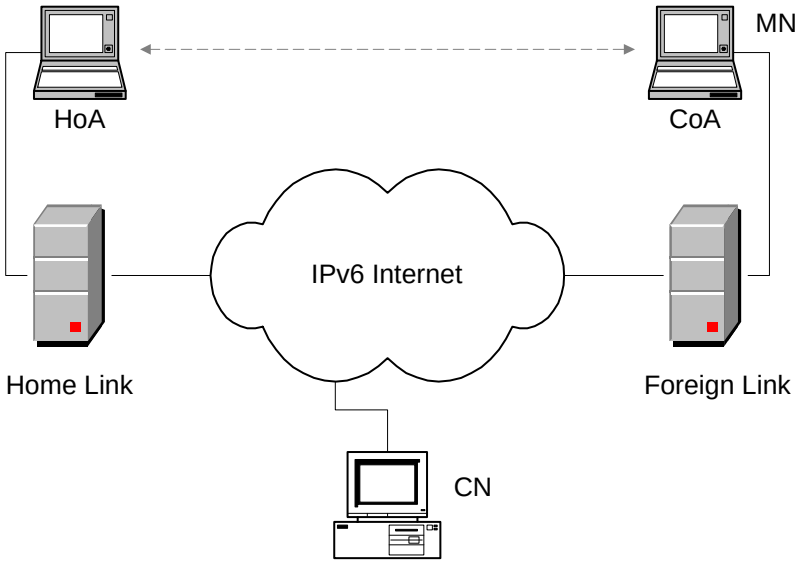

Figure 4.1: Mobile IPv6 architecture.

networks [9, 36], but the need for connection preservation leads to the solutions presented next with Mobile IP as the most significant regarding this thesis.

4.3.1 Mobile IP

Mobile IP has two versions: Mobile IPv4 [10] for IPv4 and Mobile IPv6 [15] for IPv6, where the latter one is an integral part of Internet Protocol as opposed to Mobile IPv4, which was developed on top of IPv4 after the need for mobility had emerged. It uses two kinds of addresses: permanent or at least semi-permanent home addresses, by which the mobile nodes can always be reached regardless of their actual location, and temporary care-of addresses specific for the foreign network the node is visiting. The change of addresses is handled at the Internet layer, which allows both the transport layer and the application protocols to be unaware of the mobility. Layers on top of the IP thus use home addresses for the communication whereas IP and layers below it use care-of addresses.

Mobile IPv6 architecture consists of seven parts: home and foreign links with home (HoA) and care-of addresses (CoA), the communicating nodes named Mobile Node (MN) and Correspondent Node (CN), and finally Home Agent (HA). All of them are presented in Figure 4.1 and explained next.

Mobile node forms the permanent home address at start up when it receives the network prefix advertised by some of the home routers on the home link. Alternatively the home address can be permanently configured in the memory. Therefore no mobility management is performed as long as the mobile node stays at home except at the beginning of the return to the home network. Whenever the mobile node moves out of the reach of the home link, it has to gain information about the global address of the foreign link, which it uses to form a care-of address. The newly formed care-of address is link specific and can be used only as long as the mobile node stays attached to the link in question.

Home Agent is a router locating on the home link and responsible for maintaining the mappings between the home and care-of addresses of the mobile nodes' current foreign links. It provides the always on reachability for the mobile node while it is away from home by capturing all the packets with node's home address as the destination and tunnelling them to the correct location using care-of address as the destination. It is therefore extremely important that the mobile node updates the care-of address with the home agent using a message called Binding Update as soon as the new CoA is available.

The mobile node and the correspondent node are the two communicating peers. Both of them are IPv6 nodes, but only the mobile node is required to be Mobile IPv6 capable. In a case that the correspondent node does not support Mobile IPv6, home address is used for all communication, which causes data packets to be exchanged via home agent using bi-directional tunnelling. In a more optimal situation a correspondent node supporting Mobile IPv6 uses mobile node's home address only when it is on the home link and care-of address at other times. This allows a direct communication between the two without any interceptions by home agent, and is called *route optimization*. Route optimization can be started when the mobile node and/or the correspondent node receive packets tunnelled by the home agent.

Route optimization consists of the following three phases. When a mobile node tries to establish a direct communication with a correspondent for the first time, return routability procedure is performed. The idea of the procedure is to verify that the mobile node can be reached by both via home agent using the home address as well as directly using the care-of address. This verification is done to prevent spoofing of home address/care-of address binding messages, which could result in false care-of addresses and denial-of service attacks. After a successful return routability procedure, both the mobile node and the correspondent node have created respective entries in their binding caches. The mobile node then sends a Binding Update (BU) message containing the care-of address to the correspondent node, which it acknowledges with a Binding Acknowledgement (BA)

message. After the BU/BA exchange the direct communication can finally begin. If both of the communicating peers can be considered as mobile nodes, the situation gets more complex, as Mobile IPv6 and route optimization has to be carried out both ways.

The correct usage of route optimization requires the correspondent node to always have an up-to-date information about the current care-of address of the mobile node in its binding cache. Otherwise packets are returned with ICMPv6 [5] error message, as the destination can not be reached. As only the mobile node is capable of noticing the link changes and forming a new temporary address, it is up to the mobile node to inform both the home agent as well as all the correspondent nodes it has active connections with of the change with a Binding Update. Only so does Mobile IPv6 act as has been intended.

Homeless Mobile IPv6 [20] is a variation of MobileIP, where the home link exists only virtually and can never be visited. It does not require any explicit home addresses, as the mobile node is always on a foreign link using a temporary care-of address. The solution therefore resembles the situation with mobile ad hoc networks, where the home agents for the manet nodes are located in the fixed network.

4.3.2 Other solutions

Mobile IP provides a solution to manage mobility on the Internet layer of the TCP/IP protocol stack [4] presented in Figure 4.2. Other solutions are based on different layer modifications and include e.g. Session Initiation Protocol, End-to-End Mobility, Stream Control Transmission Protocol, Host Identity Protocol and link layer mechanisms, which are briefly explained next.

Session Initiation Protocol

Session Initiation Protocol (SIP) [27] is an application layer protocol that is designed for creating, modifying and terminating sessions including e.g. multimedia distribution or conferences. It supports personal mobility by separating the location of the node from its identity, which allows users to have a single externally visible identifier with which they can always be reached regardless of their topological location. The mappings between the location and the identifier are stored by SIP registrar servers in databases called location services, which are periodically updated with REGISTER messages sent by the users. This mapping information is used by proxy servers in the users domain, when they help in routing the packets to the destination.

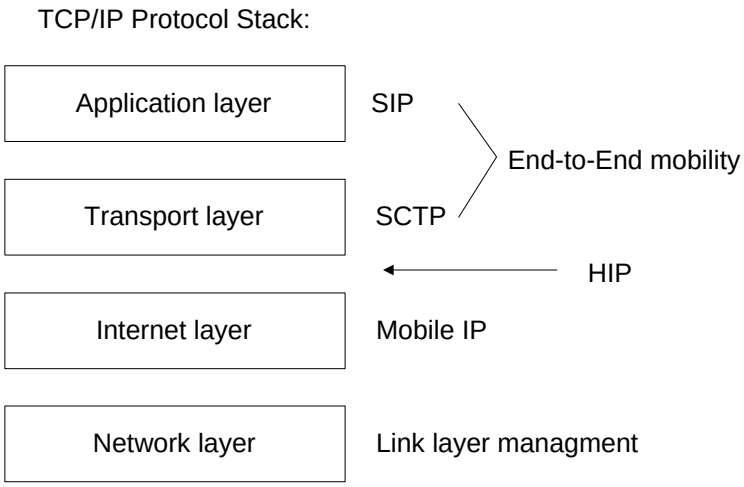

Figure 4.2: Layers of the TCP/IP protocol stack with corresponding mobility management solutions.

SIP can be run on top of several different transport protocols, but in order to be able to provide complete multimedia services to the users, it should be combined with other architectures like Real-time Transport Protocol (RTP) [30] or Real-Time Streaming Protocol (RTSP) [31].

End-to-end mobility

End-to-end mobility [1] is a framework developed to provide mobility services that are located in communication end points instead of using network layer or proxy based solutions. It aims to leverage the existing architectures to allow the hosts to dynamically update the address information contained in name servers whenever the IP address has changed.

The solution is based on two ideas. Firstly, an optional session layer is introduced to provide mobility aware applications and means to handle the connections and disconnections in a controlled way. Secondly, it adds new migrate options to the Transmission Control Protocol (TCP) [25] to enable the mobile hosts to renegotiate the IP addresses after the initial connection establishment.

Stream Control Transmission Protocol

Stream Control Transmission Protocol (SCTP) [32] is a connection-oriented transport protocol that operates on top of the IP layer. As the basic services it offers reliable packet transfer, congestion avoidance features similar to TCP and support for multihoming for either one or both of the communicating peers.

A connection between source and destination nodes is referred to as an association, which in SCTP is a broader concept than in TCP. A TCP association defines the IP addresses for the source and destination nodes as well as the port numbers of the application in use. SCTP, on the other hand, provides means for both the source and destination nodes to provide the other endpoint during the connection establishment with a list of all the possible IP addresses the node can use for either reception or delivery during the communication. An association in SCTP therefore consists of all the possible source/destination combinations that can be generated from the lists of the endpoints.

Host Identity Protocol

Host Identity Protocol (HIP) [18, 19] adds a new protocol layer between the internetworking and transport layers. It is based on the idea of separating the node's identity from its IP address, which in HIP merely acts as the temporary locator of the node. This kind of approach creates a possibility to support rapid changes of IP addresses caused by e.g. mobility or rehoming.

A host using HIP is allowed to have multiple identities, some of which can be well-known and some anonymous. All the identities, which are referred to as Host Identifiers (HI), are stored in a new namespace called Host Identity. HIs can either be generated and asserted by the hosts themselves or received from some third-party authenticator. Theoretically the only requirement for the HIs is that they have to be statistically globally unique, which is why their length is designed to be at least 100 bits. However, according to the authors, a public key of a public/private key pair makes the best HI as it could also be used to provide authentication services. In fact, the existing HIP specifications do not define the usage of any other types of HIs but public keys.

Link layer mobility management

The previously presented mobility management techniques can be used with any kind of networks without regard to link-layer techniques employed. Link-layer mobility, on the other hand, is only supported in homogenous networks, which is

why it is not thought to offer useful mechanisms with nodes locating and moving in the Internet. Link-layer mobility management is, however, used e.g. in GSM and WLAN networks, where it consists of handoffs and roaming [3].

GSM network consists of areas with different radio frequencies called cells next to each other. Handoff occurs, when the user moves from the coverage area of one cell into the coverage of an adjacent cell, and the signal is passed from the base station of the first cell to the second. The communication continues without any or only with minor interruptions as long as the user stays within the coverage of some cell. Roaming, on the other hand, means movements between different service providers and always requires cooperative agreements.

4.4 Mobile Ad Hoc Network

Ad hoc networks [37] introduce a totally new kind of mobility and freedom to networking as they allow nodes to form closed, functional networks anywhere, any time and, most importantly, without the need for any pre-existing infrastructure or maintenance. They are expected to offer great possibilities among e.g. military or disaster areas, where fast deployability of temporary networks and quick adaptation to the changing environment is needed and no reliance can or want to be made on existing network components.

As opposed to the basic networking concepts represented earlier in this paper, identity in ad hoc networks is not tied to the node's IP address. In fact the nodes do not even need to have any globally routable addresses as ad hoc networks are basically closed networks, where no data can be delivered outside its boundaries. As long as the identity is unique within the network, it is sufficient for the routing purposes.

A mobile ad hoc network is formed by arbitrarily located, typically wireless, mobile nodes often referred to as manet nodes, that are within the transmission range of some other participant. Because there are no specific routers, the nodes have to be capable of handling the routing tasks themselves, which includes exchange of routing information and forwarding data packets based on it. The mobility of the nodes typically leads to highly dynamic topology, where routing is hard to be performed efficiently and correctly. In addition, the fusions of smaller networks or separations of larger ones are not uncommon, which complicates the situation further.

Routing protocols for ad hoc networks can be divided into three categories: proactive, reactive and hybrib. Proactive routing protocols like Destination Sequence Distance Vector [24] (DSDV) or Optimized Link State Routing Protocol [35]

(OLSR) gather the routing information before it is needed. They rely on periodic advertisements, which are flooded to all nodes in the network. In an optimal situation the sending node has an up-to-date route to destination it has data for, and the packet delivery can be started immediately. However, this kind of approach consumes the scarce resources of ad hoc networks to spread routes that are never even used. Additionally, with increasing mobility, it may be hard for the proactive routing protocols to keep up with the changing routes, because they can only be announced periodically.

As opposed to the proactive approach, reactive routing protocols like Ad Hoc On-Demand Distance Vector (AODV) [23] or Dynamic Source Routing (DSR) [6] do not maintain any routing information before a communication between some two nodes is requested, but the requesting node performs a discovery for the route. Reactive routing protocols thus try to minimize the amount of control messages delivered and save the resources by focusing only on the truly needed information. They also have a faster response to the changed routes than proactive protocols. However, the delay caused by the route discovery can be unacceptable for some applications.

Hybric routing protocols like Zone Routing Protocol (ZRP) [13] try to minimize the disadvantages of the proactive and reactive routing protocols by combining the two approaches. It uses the proactive approach to discover the routes only to the nodes located within a small zone around it and reactive approach beyond this.

This thesis uses DSDV as the routing protocol inside the ad hoc network. The functionality and features of DSDV are described next.

DSDV

DSDV has two main objectives. Firstly, it enables route establishment between a source and a destination node by using periodically sent route advertisements. Secondly, it tries to keep the routing tables of the manet nodes as updated and accurate as possible by introducing immediate update messages to react to significant changes in the network topology. In order to reach these objectives, every manet node using DSDV is required to both maintain a routing table that lists all available destinations as well as to advertise its routing table to all neighbouring nodes.

In addition to the destination address, an entry of the routing table contains hop count information and a sequence number stamped by the original destination, both of which are used as the selection criteria when multiple routes choices are received to a single destination. Routes with most recent sequence numbers for the destinations are always preferred and selected. Hop count information is used

only to select between routes with same sequence number. The address of the advertising node is also stored as next hop information.

Periodical advertisements contain all the routing information a manet node has in memory, which is why they tend to cause a lot of control overhead and extra load on the network. The timing between the advertisements has to be therefore considered with extra care. Advertisements need to be sent frequently enough to fulfil the main purpose of the routing protocol, i.e. to ensure that every manet node can almost always locate every other node in the network, with the same time keeping in mind that too frequent sending rate might deteriorate the overall performance of the network by causing network congestion and packet collisions. Immediate update messages were added to help to reduce the overhead. They are sent whenever a new, significant information is added to the manet node's routing table and include only the information relevant to the change. New sequence number with no changes to hop count is not usually considered as significant information that should be broadcasted immediately.

Detection of link failures is an important part of the routing protocols. With DSDV broken links can be determined by means offered by layer-2 protocols, or, alternatively, if no advertisements from a former neighbouring node has been heard for a specific period of time, using that to conclude the manet node to be out of the reach of the transmission range. A broken link is immediately assigned an ∞ as the hop count, and its sequence number is incremented. After the updates the information concerning the broken link is immediately informed to neighbours.

Like most of the ad hoc routing protocols, DSDV has been designed to be used in networks, where all the participating nodes are considered to be friendly and trust each other. No security features has been designed to it because of this.

4.5 Global connectivity

Even though an autonomous and closed ad hoc network might be sufficient in some situations, it is more than likely that some of the manet nodes will at some point request an additional connection to the Internet or some other fixed network. As ad hoc networks have not originally been designed to provide this global connectivity, a new protocol called Globalv6 [38] was developed to offer the interconnection functionality. It is not a separate protocol but rather an extension to the existing manet routing protocols.

Globalv6 introduces a new component called an access point (AP) (see Figure 4.3), often also referred to as a gateway, to the architecture of an ad hoc network. Access points are routers that are located at the edge of the ad hoc network having

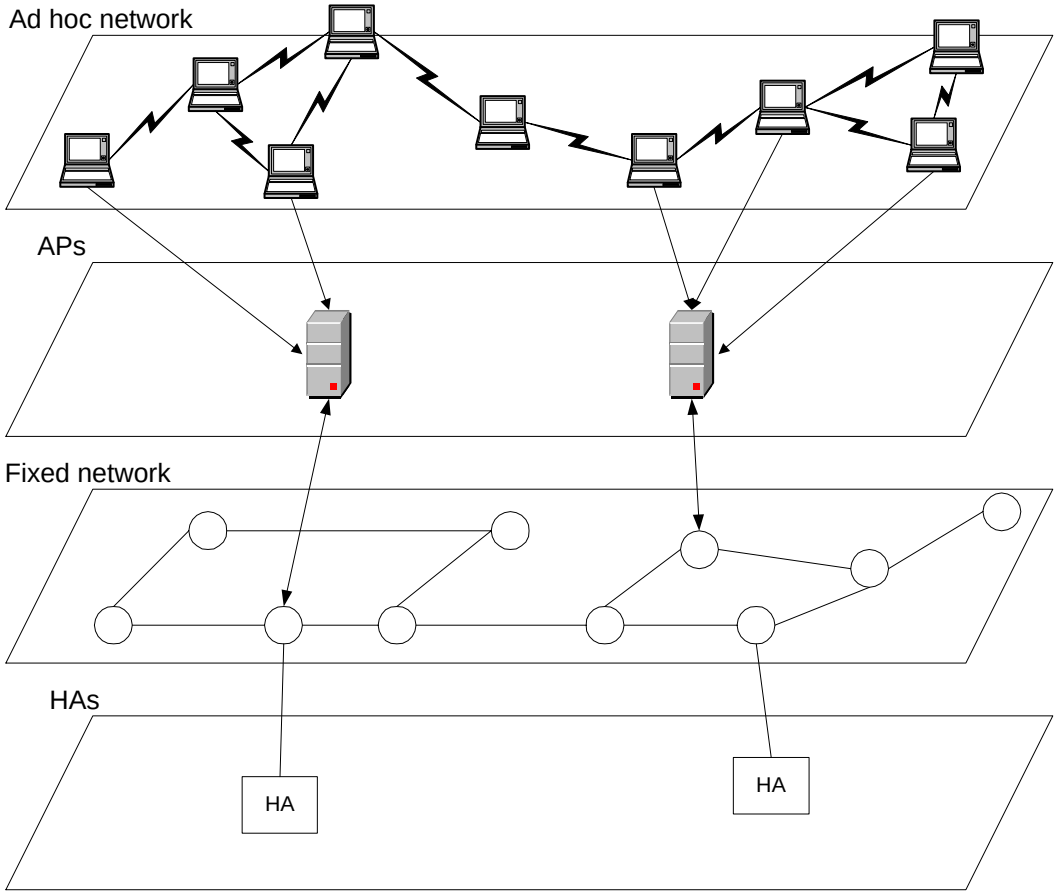

Figure 4.3: Access ad hoc network architecture.

a connection to both the fixed network and the manet nodes. By forwarding all the packets through these access points the manet nodes can reach destinations located in the fixed network.

The functionality of Globalv6 can be divided into access point discovery, data delivery and connection maintenance. All the three phases will be explained next, after which a few alternative solutions are proposed.

4.5.1 Access point discovery

When a manet node starts up or enters a new location, it first performs a router discovery to find if there are any routers in the same subnetwork.[1] If it finds any, it sets the found router as its default router towards the Internet, otherwise the node assumes to be in a closed network, where it can communicate with nodes within the boundaries of the same network by using the ad hoc routing protocols. However, as mentioned earlier, this communication is rather limited. Therefore Globalv6 proposes the manet node now to start another router discovery, this time for the access points of the ad hoc network, which successful completion would provide the node a global connectivity despite the original specifications of the ad hoc network.

The manet node has three possibilities to obtain the information about the possible access points. It can benefit the proactive approach, in which the access points themselves periodically broadcast advertisement messages throughout the network. The advertisement message includes the information about the identity of the access point in ad hoc networks as well as the global address and the corresponding network prefix along with its length. It also contains a lifetime for which the manet node can consider the information valid. Even though duplicate messages caused by message flooding can be deleted by the receiving nodes, the amount of control message overhead still remains high in the proactive approach. However, if the advertisement messages could be piggybacked with the beacon messages, they would not cost any extra control messages but only slightly longer beacon messages.

The second approach for access point discovery is reactive, where manet nodes send access point solicitation messages to a special ad hoc network access points multicast address. All the access points receiving the query reply with an access point advertisement message similar to proactive approach. The replying node can alternatively be some of the intermediate nodes, at which time a gratuitous reply is delivered also to the access point in order to provide a bi-directional communication. As all the access points of the ad hoc network listen to the requests, the manet node is likely to receive multiple replies, from which it can select the one it wants. If it receives no replies, it concludes that there are no access points and continues communication only with other nodes within the ad hoc network.

The third approach, hybrid, tries to combine the best characters of both of the previous by using the proactive discovery in a small zone around the access points

[1] The discovery is link-local, which makes it highly unlikely for the manet node to be in reach of some router. Additionally, the notification of the change of the location when using wireless transmission media is much more harder and complicated than with wired media as the signal deterioration takes place gradually instead of reconnecting the network cable.

and reactive beyond this. A variation of a hybrid approach is proposed in Section 4.5.4.

After the manet node has received the advertisement information about the access point, it can finally form a globally routable care-of address and add a default route via the access point towards the Internet in its routing table. If Mobile IP is used as the mobility management protocol, the new care-of address has to be now updated with the home agent.

4.5.2 Data delivery

When the manet node has successfully discovered an access point, the next question it faces is how to separate the manet nodes it can reach using ad hoc routing protocols, from the fixed nodes. It can not make any assumptions from the addresses of the destinations as they are allowed to be arbitrary inside the ad hoc network. The globally routable addresses can, however, be used in determination.

For proactive manet routing protocols, the situation should be pretty straight forward, as the basic assumption behind these protocols is that every mobile node and access point have a complete list of all nodes locating in the same ad hoc network in memory. Therefore if a match for the destination can be found, packets are sent following that host route. If no match is found, but the prefix of the destination is equal to the prefix of the global address of the source node, the packet is transmitted as if the destination was a neighbouring node. Only if they do not match, the destination is concluded to be a fixed node.

With reactive manet routing protocols, the situation is more complex. Globalv6 proposes the nodes to first assume that the destination node is a manet node from the same network. Given this assumption, the manet node initiates a route discovery, which follows the principles of ad hoc network routing protocols. The discovery is continued until either a reply is received, at which time the destination is concluded to be another manet node, or at least one network-wide search without a reply is performed. In the latter case the destination is assumed to be a node locating in a fixed network that can only be reached through the access point. Because of this no intermediate nodes are allowed to reply to the queries about fixed nodes even though they would know the route as it would indicate that the destination can be reached through the replying node instead of the access point. If the access point at some instant would receive any packets that it knows are destined to another manet node and not a fixed node, it can notify the source node of this and request it to initiate a route discovery for a direct route. However, some mechanisms might be needed to allow the manet nodes to communicate via access point for some reason. This kind of situation is possible because of some

failure occurrence during the route discovery process, or if the destination would happen to move to the same network after the initial route establishment. An alternative for manet node fixed node separation for the reactive manet routing protocols is proposed in Section 4.5.4.

Every fixed node will get its own route entry in the manet node's routing table, so that the search does not have to be performed separately for every packet transmission. The situation is same for the manet node entries, but as the number of fixed nodes is drastically larger than the amount of manet nodes, the routing tables now have a change to grow out of control. In order to avoid this, the entries are set expiration timers that take care of the deletion of unused routes.

4.5.3 Connection maintenance

The dynamic nature of ad hoc network makes it possible that the route to the current access point is either temporarily or permanently lost because of e.g. mobility or other errors. In that case it is inevitable for the manet node to try to retrieve the global connection by some means. It can either use the ad hoc network routing protocols to find an alternative route to the lost access point, or, if it assumes better choices to be available or the loss to be lasting, perform a new access point discovery. The latter, however, again requires binding updates with home agent and all the correspondent nodes due to change of CoA.

4.5.4 Alternative solutions

Two alternative solutions for Globalv6 functionality are proposed. One for the access point discovery and another for the data delivery.

Variation of a hybrid access point discovery

The hybrid approach for access point discovery uses periodical advertisements in a small zone (typically max 3 hops) around the access point and expects the manet nodes beyond the advertisement zone to initiate access point discoveries by sending a request to access points' multicast address. However, it might not be efficient approach to limit the size of the advertisement zone to some predefined value, but it might be better to change it dynamically.

A fourth approach might therefore be to flood the access point advertisements as far as the hop count or some other selection criteria for the advertising access point at the receiving node is better than for the other access points advertised.

Whenever the criteria gets worse, the flooding is stopped. Preferably, the advertisements might be flooded a few hops beyond this limit to allow the nodes to get information about the other alternative access points that can be taken into use in case the current access point fails or multipathing is utilized.

This thesis uses this approach to deliver the access point information throughout the ad hoc network.

Data delivery to fixed and manet nodes

After a successful access point discovery, Globalv6 assumes the manet nodes to treat every new destination as it would be another manet node and initiate a route discovery inside the boundaries of the ad hoc network. As the reactive manet routing protocols use the Expanding Ring Search technique for route discoveries, a lot of time is wasted in useless attempts if the destination finally turns out to be a fixed node instead.

If the assumption would be turned around, and every new destination would be assumed to be a fixed node that can be reached only through some access point, the Expanding Ring Search would no longer be automatically utilized and the delays experienced when communicating with fixed nodes would drop. If in this situation the access point would then notice that both of the communicating peers are actually in the same ad hoc network, it could notify the source node and request it to initiate a route discovery for a direct route. No drastically larger delays would therefore be experienced even when starting communication with other manet nodes. The drawback with this kind of solution is that it would require all the manet nodes to use globally routable addresses, which was not the original idea of the ad hoc networking. The load on access points would also increase as every packet would by default be directed to them.

4.6 Simulation

There are three possible methods to performance modelling: formal analysis, real life measurements and simulation. However, the dynamic properties of ad hoc networks make them hard to be studied by formal analysis. Real life implementations, on the other hand, are still rare and hard to get hold of. The low cost and high availability of simulation tools has therefore made simulating a widely used method when studying performance of different protocols. As mentioned earlier, this thesis uses Network Simulator 2 (NS2) [21] as the simulation tool.

Network Simulator 2

NS2 is an object-oriented, discrete event simulator. It provides a wide range of existing features including e.g. support for routing in both wired and wireless networking. Additionally, it has an open source code, which allows users to modify and extend it further.

NS2 is implemented using two languages: OTcl for generation of new simulation scenarios and C++ for the detailed protocol implementation. This kind of approach was developed to allow quick and easy formation of frequently changing and large simulation configurations, but still be able to keep the underlying simulator as fast and efficient as possible. Unfortunately, this also makes the modifications and extensions to the protocols slower and more complex as programming of new systems needs to be done in both languages at the same time.

Link life time distribution

A simulation network consists of a set of mobile nodes and links, which are physical connections between the nodes. A link between two mobile nodes therefore exists whenever they are within the transmission range of each others. The time that a link is continuously up from its formation to destruction is called link life time (*llt*). However, *llt*, as it is defined, is hard to measure, as there are no signs that would indicate us the exact points of time when some two nodes have emerged to each others transmission ranges or left them. Instead, we have the time when the first communication message was successfully delivered between the nodes and also the time when the first message delivery fails. For the analysis in this thesis it is sufficient to estimate *llt* to be equal to the successful communication time.

Link life time distribution describes the probability of the remaining *llt* of a randomly chosen link at any given time *t*.

Chapter 5

Access point selection

As stated in Section 4.5, communication messages between a manet node and a fixed node are delivered through access points located at the edge of the ad hoc network. The route from the fixed node to the access point can be considered fairly stable as opposed to the route between the access point and the manet node, where the mobility of the manet node or some of the intermediate nodes may cause the connection between the two to be broken at any time. The connection may also be lost as a result of some inner failure, which prohibits the access point from continuing to act as the data transmitter. This thesis, however, considers the access points to be available for the whole duration of the simulation time, which makes the selection of the route between the manet node and the access point to be a significant factor affecting the reachability from the manet node to the fixed node and vice versa.

Four different selection methods are explained next, after which hypothesis of expected is proposed.

5.1 Selection methods

This thesis studies the impact of two different access point selection methods: Break-Before-Make (BBM) and Make-Before-Break (MBB). They are both relatively simple and easy to understand as well as implement, which were the main reasons they were chosen for this thesis. Other possible selection methods might include e.g. multipathing or utilization of cost functions. BBM and MBB are covered in more detail next, after which the two alternative selection methods are briefly explained.

5.1.1 Break-Before-Make

The simulations use the proactive DSDV as the manet routing protocol, which gives the manet nodes two different possibilities to obtain the information about the existing access points, namely *advertisements* and *solicitations*. Periodically flooded access point advertisements allow all the manet nodes within the reach of that ad hoc network to become aware of the advertising nodes even though no need for a global connection would exist at that time. As an ad hoc network presumably contains more than just one access point, a manet node is likely to receive multiple advertisements, from among which it then selects an access point to act as its gateway towards the fixed network. This thesis uses an implementation where the first advertising access point is selected, but in a case further advertisements from closer access points are received, the access point information is always updated to closest in terms of hop count.

It is also possible for a manet node to require a global connection before it has received any advertisements or immediately after a connection break-down. In such situation, the manet node is able to initiate an access point discovery by broadcasting a solicitation message, which is received by all access points located in the ad hoc network. They reply by unicasting advertisements to the requesting node.

These alternative series of events are marked as *AP DISCOVERY BY ADS* and *AP DISCOVERY BY SOL* in Figure 5.1. The following *LOCATION UPDATE* includes the compulsory mobility management part, where the manet node informs its home agent (HA) about the new access point, and has to be performed every time a manet nodes changes its access point. [1] The latency before the data transmissions with the fixed node (FN) can be started therefore consists of the times consumed for these two phases.

The selected access point is used to relay the data packets until the connection is broken or an advertisement from a closer access point is received. With BBM, no information about alternative access points is stored in memory at the time of receiving advertisements. The communication is therefore unable to continue until either a route to the previously selected access point is rediscovered or some new access point is taken into use.

This thesis proposes the manet node after a break always to perform a new access point discovery as it gives the manet node the possibility to select a closer

[1] The chosen access point itself does not receive any kind of confirmation from the manet node, which makes it unaware of the group of manet nodes using it as their gateway towards the fixed network. Only when the access point receives a Binding Update intended for HA, it can conclude that this MN has chosen the access point as its gateway.

access point with a shorter route, if such exists. In dynamic environments like ad hoc networks the shorter routes should be preferred to longer ones in terms of hop count as smaller amount of intermediate nodes tends to predict higher link life time probabilities. Secondly, the delays experienced with unsuccessful route rediscovery attempts to old AP quickly grow over the delay caused by updating the information with HA.

5.1.2 Make-Before-Break

The functionality of MBB is presented in Figure 5.2. It is an approach that is possible only in ad hoc networks, which include multiple access points. As was with BBM, the manet nodes again have two possibilities to receive information about existing access points. *AP DISCOVERY BY ADS* and *AP DISCOVERY BY SOL* phases look similar to BBM's, but a manet node using MBB is allowed and required to take advantage of the multiple advertisements it is to receive with both alternatives. From among all the advertising access points manet node selects one to act as its primary access point, which it will use for global communication as long as the connection stays valid or a closer access point is discovered. All the other advertising access points are stored in memory with expiration timers. These entries are reset every time a node receives an advertisement from the access point in question. With a proactive routing protocol like DSDV, the periodically broadcasted advertisements therefore ensure that the list of alternative access points is always up-to-date and valid. No extra control messages are needed, which would be the case with reactive routing protocols.

Whenever a connection with the primary access point is lost, a new one can be quickly selected from the list in memory. The closest in terms of hop count, most newly advertised or optimal in some other way can be selected. Simulations run for this thesis select always the latest advertiser even though it can lead to a situation where the chosen access point is, in fact, very far and others in memory just few hops away. As no time consuming AP discovery takes place and only updates with the home agent are needed, the communication should be expected to be able to continue quicker compared to BBM.

As an extension to the MBB's approach, the change of the access point might also take place even when the primary access point is still functional but the disconnection seems obvious in the near future. This is, however, out of the scope of this thesis.

5.1.3 Alternative methods

Both of the alternative methods are valid only in ad hoc networks containing more than one possible access points. Their evaluation is left to future work.

Multipathing

With BBM and MBB all the packets between the manet node and the fixed node are delivered using the same route and the same access point. However, if the used route encounters a failure, all the packets will be lost and have to be resent after a route rediscovery. In dynamic environments like ad hoc networks the high probability of link break downs can therefore disturb the communication considerably. One possibility to avoid this is multipathing. It duplicates all the packets to be delivered and sends them through two separate routes and access points. This increases the probability that at least one of the duplicated packets will reach the destination. [2] However, the duplicated amount of data packets to be delivered may cause problems in networks with scarce resources and high traffic loads.

Cost function

Usually the first of the replying access points is selected for task. However, the selection can also be performed using some other predefined criteria based on the information advertised by the replying access point. The criteria might be e.g. a combination of priorities, hop counts, processing power, the amount of served manet nodes or available energy. The nodes using cost function always select the first advertising access point and change it according to selection criteria after receiving more alternatives.

5.2 Hypothesis

Before any simulations are run, a short hypothesis of the differences in performance between the two selection methods is made. According to the writer's intuition, no significant differences should be visible in static environments as the routes last throughout the simulations and no rediscoveries of access points are needed. On the contrary, as the topology becomes more dynamic, the performance of the MBB should exceed BBM's as the information about a new access point already exists in memory. Therefore the amount of successfully delivered

[2] This is highly important especially with real-time data transfers like VoIP.

data packets should be larger. With MBB no extra control messages should neither be needed. Additionally, as neither of the selection methods buffer data packets in a case no route exists to the destination, higher mobility should not dramatically affect the delays experienced.

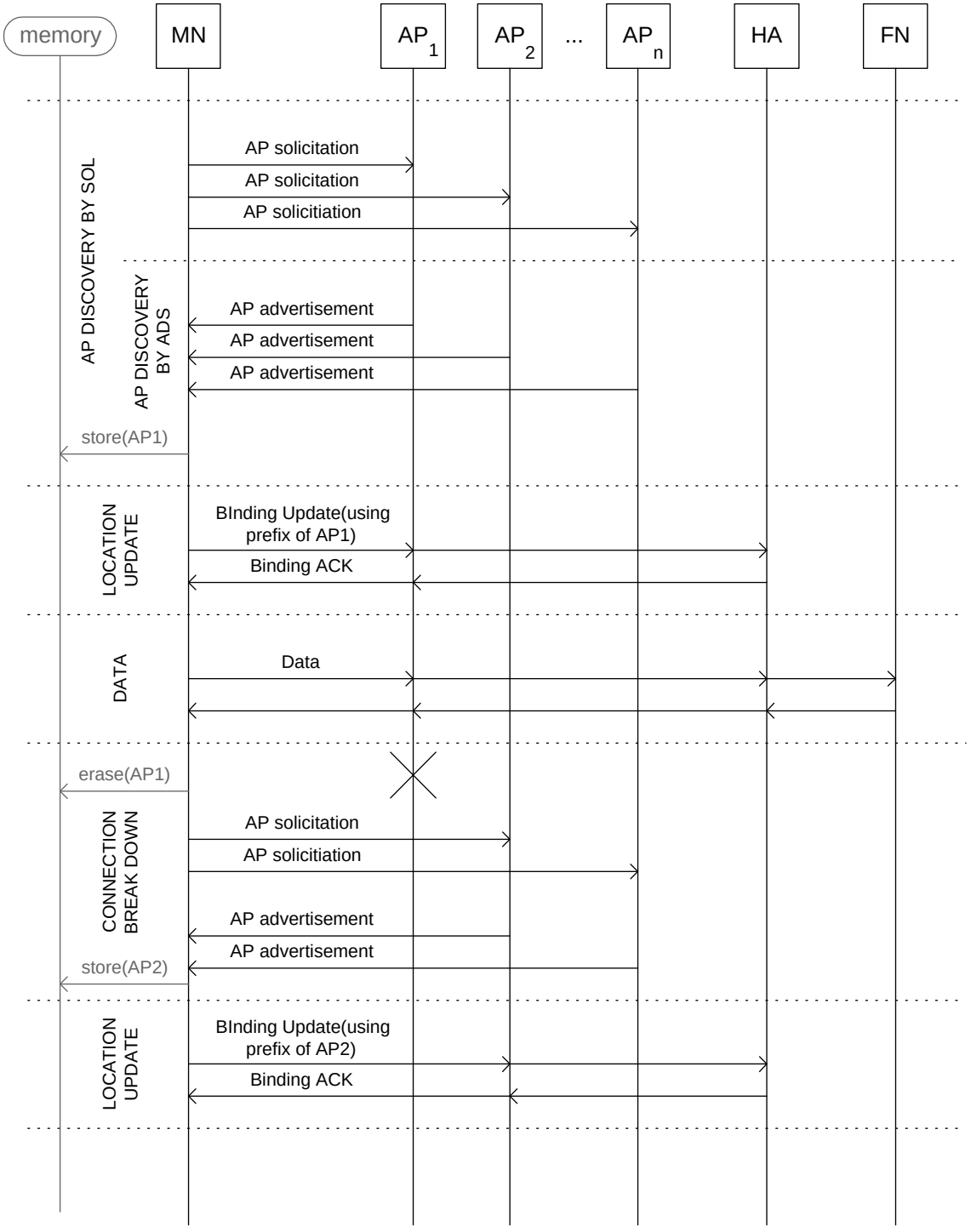

Figure 5.1: Break-Before-Make.

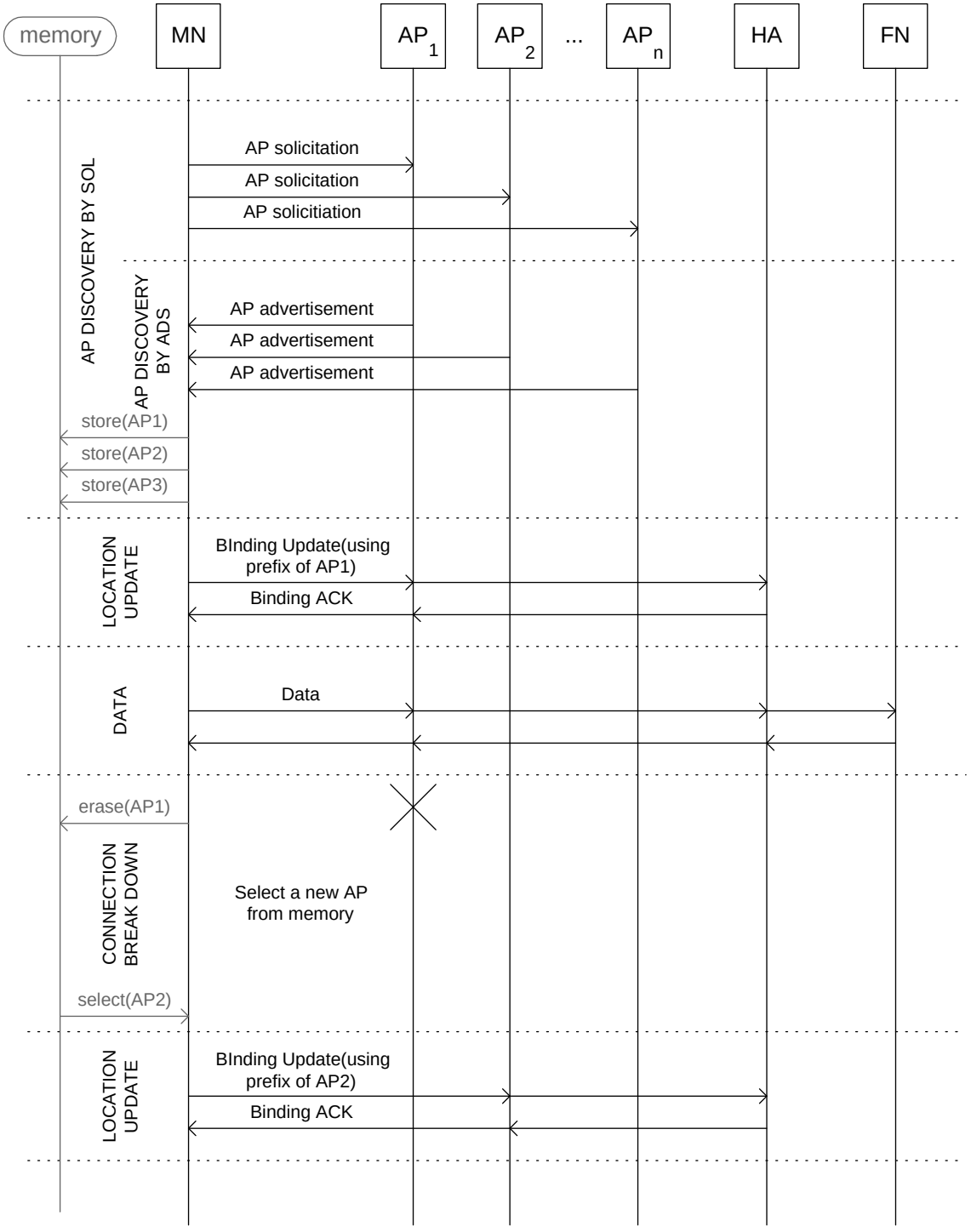

Figure 5.2: Make-Before-Break.

Chapter 6

Simulations

This chapter presents the simulation scenarios that were run in order to study the impact of the access point selection methods proposed in the previous chapter.

6.1 Scenarios

Before the actual scenarios were specified, the purpose of the simulations was reconsidered in more detail. The following three goals were identified.

1. To study how increased mobility affects reachability between the communicating nodes from an ad hoc network and a fixed network when using the proposed selection methods.
2. What is the point at which the differences between the selection methods become apparent and/or significant?
3. To study how the situation changes if predefined positions are used for the access points as opposed to random positioning.

The simulation scenarios were designed to meet these three goals. All of the them are run using both of the proposed selection methods, BBM and MBB.

Scenario 1 was designed to meet the first of the simulation goals. To measure the effect of mobility, a variety of speeds were selected for the mobile nodes in order to simulate the communication first in a nearly static environment, and then increasing the speed until a highly dynamic topology is achieved. The following four speeds were selected: 1, 2, 4, and 10 m/s. The number of access points was

chosen to be 10 in order to provide link distance distribution, where 95 % of the manet nodes are within 4 hops or less from the nearest access point. The positions of the access points were randomly selected across the 300 m * 300 m simulation area.

Scenario 2 is a special scenario, which aimed to figure out the differences in communication if the positions of the access points were fixed as opposed to randomly selected. This scenario describes the real life situation where the global connectivity would be provided by e.g. some Internet Service Provider (ISP) with predefined access point positions. Scenario 2 uses 4 evenly positioned access points and a fixed speed of 4 m/s for the mobile nodes.

All the simulation parameters used in scenarios are summarized in Table 6.1.

	Scenario	Parameter	Value
General	All	Simulation time	900 sec
		Initialization time	3000 sec
		Simulation area	300 m * 300 m
		Amount of mobile nodes	50
		AP advertisement interval	1.0 sec
		Pause time	0 sec
Communication related	All	Radius of transmitter	50 m
		Bandwidth	2 Mbps
		Traffic type	CBR
		Packet rate	4 packets/sec
		Packet size	64 byte
		Amount of flows	10
Scenario specific	1	Amount of access points	10
		Speed	1 m/s 2 m/s 4 m/s 10 m/s
	2	Amount of access points	4
		Speed	4 m/s

Table 6.1: Summary of the parameter values used in scenarios.

6.2 Simulation runs

The simulations were done in two phases. First, consistency of the simulation system is verified and simulation related parameters are defined. Then, actual reachability analysis is done with simulation.

Measuring consistency

Consistency of the simulations was verified using the following four environments. The results for each are analysed in Section 7.1.

1. Simulation time.

   These simulations are run in order to specify earliest time in the simulation system when it stabilizes so that measurements can be started.

   The simulations were run using the slowest speed, i.e 1 m/s, and MBB as the selection method. The slowest speed was chosen because with slowest speed it takes the longest time to reach the stable state and faster speeds can therefore be expected to stabilize earlier.

2. Random data delivery.

   These simulations aim to ensure that the results are not dependent on the random time when packets are sent.

   Same set of initial positions, mobility files and communicating nodes are used, but the time of sending data is randomized between 0 to 0.25 seconds. Ten simulations were run for MBB with speed of 10 m/s.

3. Random communicating nodes.

   These simulations aim to ensure that communication pairs do not impact results.

   Same set of initial positions and movement patterns are used, but the communicating nodes are randomized from among all the manet nodes. Ten simulations were run for both MBB and BBM with speed of 10 m/s.

4. Randomized mobility.

   These simulations aim to ensure that randomized mobility does not impact results.

   Same set of initial positions and communicating nodes are used, but the files defining the mobility of the manet nodes are changed. Again ten simulations were run for both MBB and BBM with speed of 10 m/s.

Measuring reachability

After the consistency analysis, the final reachability simulations were run in order to analyse the packet delivery fraction, experienced delay, jitter and the amount of control overhead produced. To get the final results, both of the selection methods were simulated 30 times for each scenario using randomly chosen initial positions, movement patterns and communicating pairs. The results for the reachability are presented and analysed in Section 7.2.

Chapter 7

Analysis

This chapter presents the results gained from the simulations and analyses them. Analysis is performed against the design criteria introduced in Section 3.

7.1 Consistency analysis

The purpose of these simulations was to verify the consistency of the results before the actual reachability analysis could be performed. During the analysis it became, however, evident that the packet delivery fraction (shortened as *pdf* for the rest of this chapter) on its own was not able to verify the consistency of the results. The simulations namely showed that even though a manet node had all the needed information about a functioning access point in memory, in most situations data could still not be delivered to the waiting fixed node because of the inability of the DSDV protocol to deliver correct routing information quickly enough between the manet nodes, and most of the sent data packets ended up dropped somewhere along the route. Therefore in order to be able to compare the selection methods, another fraction was added to calculations.

The new fraction is called packet sending fraction (shortened as *psf*), and it means the ratio between the amount of data packets sent by source nodes and the amount of all data packets created during the simulations. Psf is used in the final reachability analysis as the indicator of the ranking order between the selection methods.

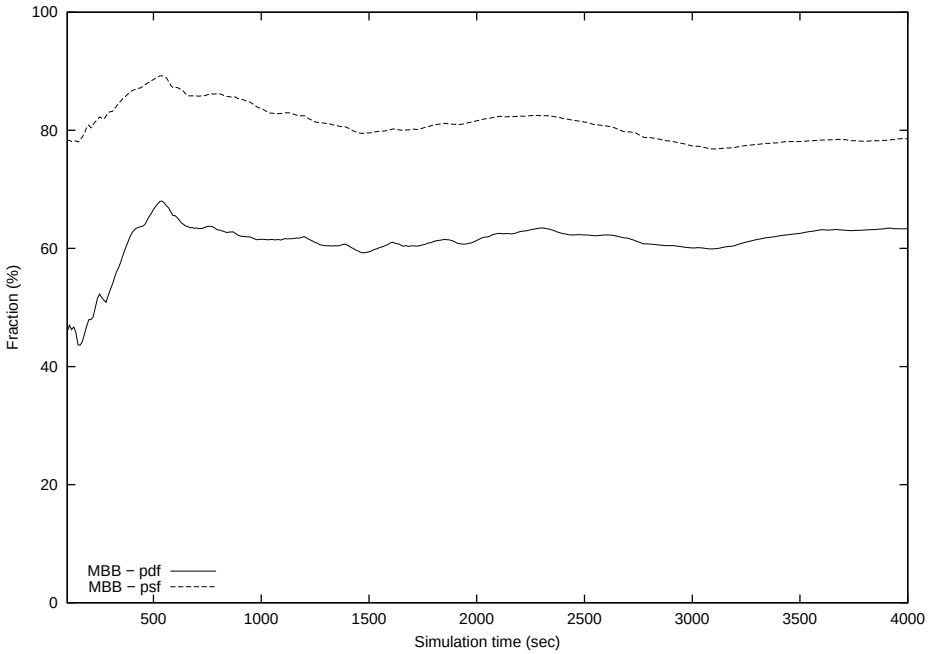

Figure 7.1: Pdf and psf as function of simulation time.

Simulation time

Simulation time measurements aimed at defining the point in time at which the reachability stabilizes. Pdf and psf values for the duration of the simulation time of 4000 seconds for the MBB selection method are shown in Figure 7.1.

Based on this figure, the initialization time for the following simulations was set to 3000 seconds, after which the reachability seems stable enough for our purposes. However, with more time and resources to use, it would be a good idea to run the simulations for e.g. 10000 seconds and see whether longer initialization time would provide more stable reachability fractions.

Random data delivery

The purpose of the random data delivery simulations was to check that the results are almost the same regardless of the sending time. The sending time was incremented by 0.02 seconds for every simulation run, i.e. simulation run 1 used sending time of .00 seconds, run 2 of .02 seconds, run 3 of .04 seconds etc.

Figure 7.2 shows the pdf and psf fractions measured for ten simulation runs. With

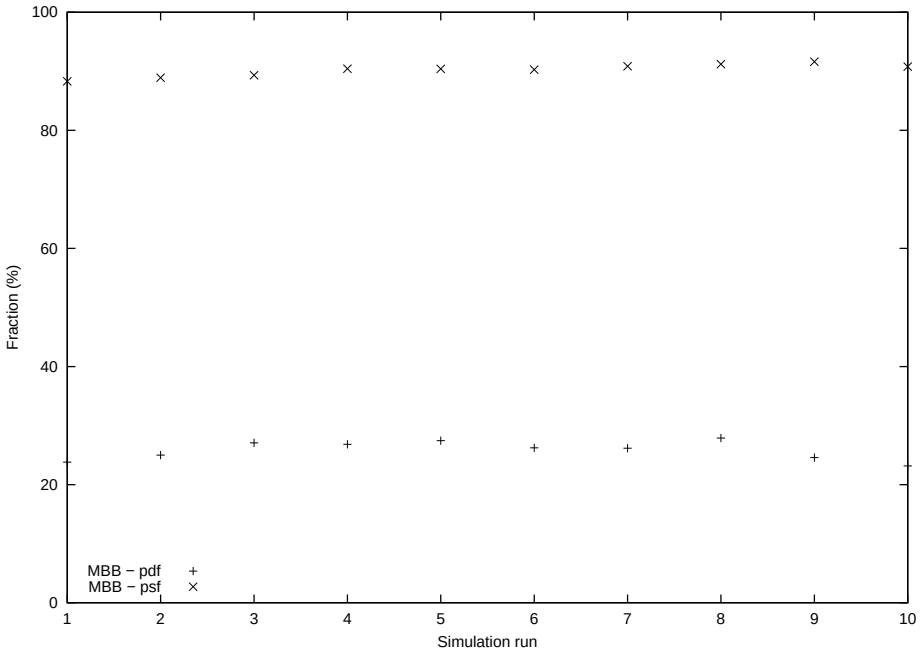

Figure 7.2: Pdf and psf as function of randomized data sending times.

the results being so similar to each others and the standard deviations calculated to be 1.6 for pdf and 1.05 for psf, the time of sending data packets can be said not to have any results affecting impact on the simulations. Standard deviations also show that psf is more stable than pdf.

Random communicating nodes

The simulations for random communicating nodes had two purposes. As with random data delivery simulations, they aimed to verify that the results for the ten simulation runs are almost the same. In addition to this, they also aimed to check that the results are consistent so that the ordering between the selection methods remains constant.

Figure 7.3 shows the results for both of the selection methods and ten simulation runs. From the figure it can be seen that the psf values are almost the same with standard deviations calculated to be 1.18 and 1.28 for BBM and MBB. If the pdf values are compared, no real consistency can be seen, as neighter of the selection methods consistently performs better than the other one. These results therefore indicate that no ordering between BBM and MBB can be made based on the pdf values as the results vary as a function of random communicating nodes.

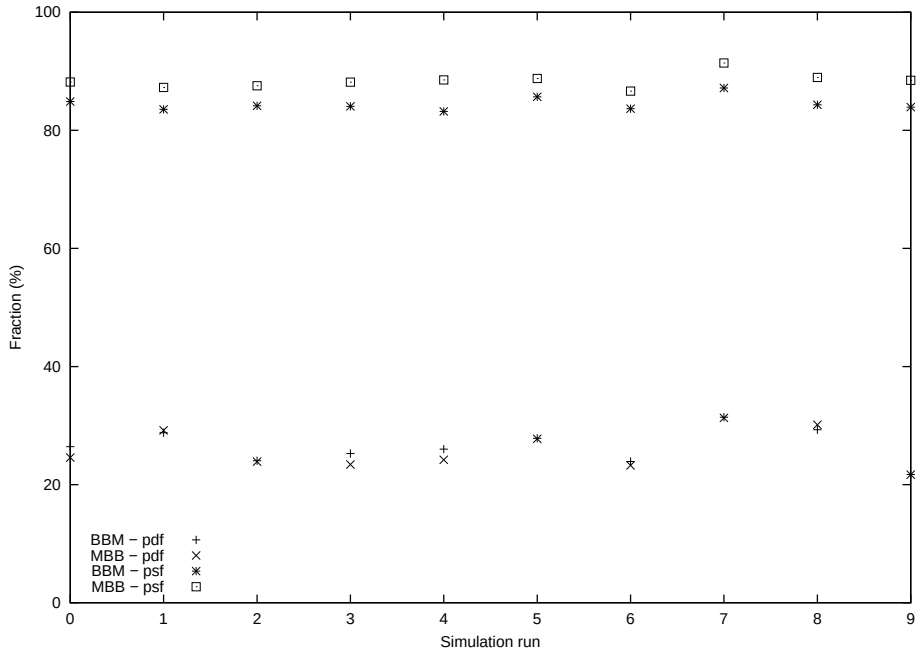

Figure 7.3: Pdf and psf as function of randomized communicating nodes.

Based on the psf values, it is, however, reasonable to regard the results consistent as MBB consistently produces better psf than BBM in all simulation runs even though the absolute values for the psf vary a little. The variation is natural as the communicating nodes are chosen randomly.

Randomized mobility

The purpose of the randomized mobility simulation was the same as with the simulations with random communicating nodes.

Figure 7.4 shows again the pdf and psf values for both of the selection methods and all ten simulation runs. With standard deviations of 0.99 (BBM) and 1.05 (MBB) and results with only few percentage units differences among the simulation runs, random mobility files using random direction can be concluded not to have an impact on the consistency of the results.

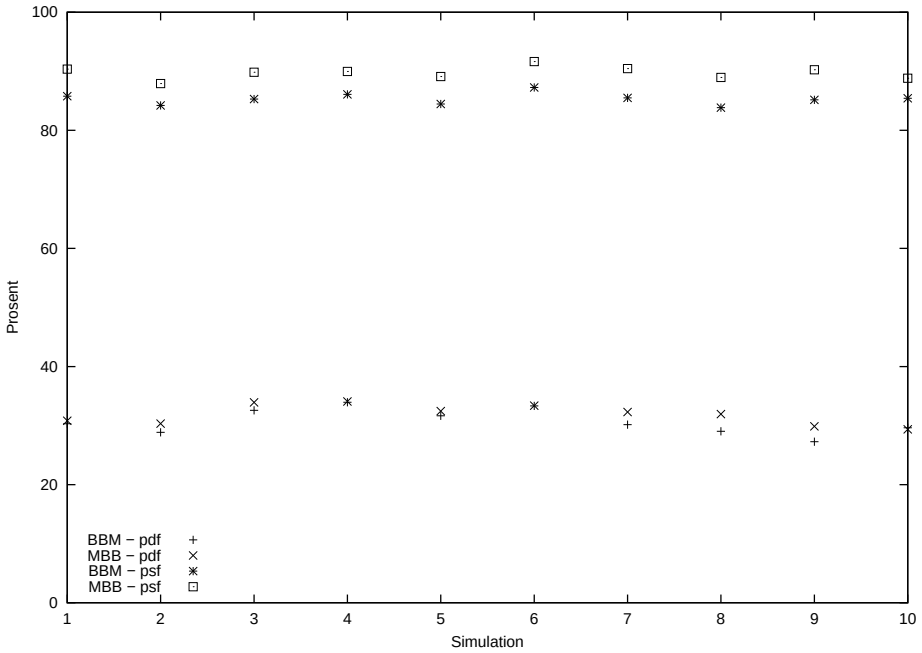

Figure 7.4: Pdf and psf as funciton of randomized mobility patterns.

Summary

Consistency simulations showed that it takes 3000 seconds for the system to stabilize so that the collection of data for the reachability analysis can be started. The data sending times, communicating nodes and mobility files defining the movements of the manet nodes can also be randomized without that it would affect the consistency of the results.

Packet delivery fractions for the consistency simulations can not be considered consistent as the the results showed no constant ordering between the selection methods. Pdf can not therefore be used reliably as an indicator in the reachability analysis.

MBB's packet sending fraction, on the other hand, was systematically better than BBM's regardless of the randomized parameters. Psf can therefore be used as a reliable indicator in the reachability analysis.

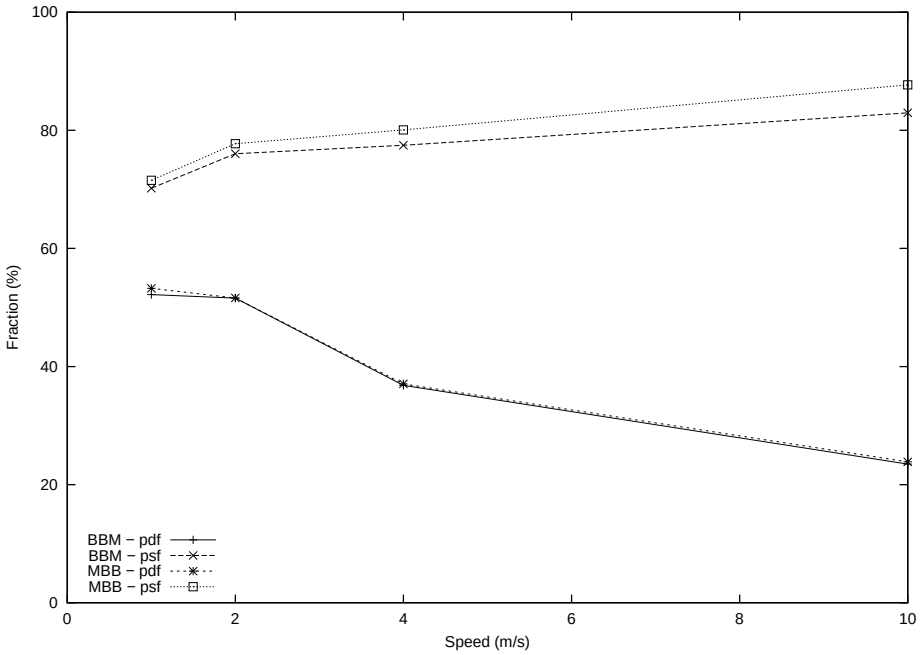

Figure 7.5: Packet delivery and packet sending fractions.

7.2 Reachability analysis

The final reachability analysis is divided into two parts. The first part analyses the results received for scenario 1 and the second part for scenario 2.

7.2.1 Scenario 1

Scenario 1 studied the impact of mobility on BBM and MBB selection methods.

Fractions

Packet delivery and packet sending fractions for both of the selection methods and four speeds are presented in Figure 7.5. Pdf shows the performance of the access point selection method when combined with DSDV as the manet routing protocol. Psf, on the other hand, presents the amount of time during which the sending manet nodes have an unexpired access point information in memory and are should to be able to reach their fixed node destination. Because the routing information can be partly expired in the network, not all packets reach their desti-

nation but are dropped somewhere along the route, as pdf shows. As the routing information is delivered by the means offered by DSDV, this huge difference between the fractions can be taken as a sign of the inability of the DSDV protocol to spread the routing information correctly and quickly enough and to all nodes along the route. It is not enough that the sending manet node has a route to the node acting as the access point in its routing table, but all the intermediate nodes need than information too. Therefore as the mobility increases, the task of keeping the routing tables up-to-date becomes really challenging for DSDV, which is why the pdf decreases to just 25% with speed of 10 m/s. However, the situation is not good even in a more stabile environment as even with very low speeds, i.e. 1 m/s or 2 m/s, only about 50% of all the data packets produced are successfully delivered to their destinations. Therefore the combination of the proposed selection methods and DSDV can not really be considered as a true option for mobile ad hoc networks that require global connections. The performance of the DSDV protocol has shown poor results in research done before too [16], so this could be expected.

Based on the pdf values, no ranking between the selection methods can be made as the results for both of the selection methods are almost identical. With low speeds (1 m/s) it could possibly be said that MBB perfoms better, but the small difference can, however, be within the statistical error marginals.

Based on the psf values, it is reasonable to claim the MBB selection methods to perform better as it consistently gives better results than BBM. As was expected, the difference is smaller with lower mobility, but it increases always up to 5% with higher speeds, which means nearly 2000 successfully delivered data packets more. The increasing difference can be explained by the charasteristics of the flooding behaviour of the selection methods. The access point advertisements are forwarded only as far as there are no shorter routes to other access points, which in stable environment easily leads to situation, where every manet node has information only about one or maximum of two access points. When the speed of the manet nodes increases, the propability of a manet node receiving advertisements from more than just one access points increases. This helps MBB, which now has more access points in memory and can start using one of them in a case the current access point is lost. Unfortunately this does not help as the data packets are lost along the route.

The interesting and unexpected in Figure 7.5 is that the packet sending fraction increases as the speeds get higher, instead of decreasing, which would have been the hypothesis. The reasoning given above could explain it for MBB, but BMM does not take advantage of multiple advertisements. Additionally, the delivery of access point information is nearly 100% in static environments, but the sending

fraction reaches only 70%. The only explanation for this is the performance of the DSDV protocol. Data packets can be sent if the sending manet node has both the access point information and a route to that node in routing table. With higher speeds, DSDV is able to deliver the routing information more widely as the manet nodes move quicker and are able to hear advertisements from more manet nodes. The simulations namely showed that even in nearly static environments, DSDV is not able to keep the routing information up-to-date in all nodes in the network, but routes expire before they are readvertised. As psf does not take into consideration the correctness of the routes, a large amount of data ends up dropped along the route, which leads to the situation with 10 m/s, where 85% of the packets can be sent but only quarter of them reach the destination.

Delay and jitter

Packets are not buffered by source nodes in a case no route to some access point is found in memory. The intermediate nodes are, however, allowed to store the packets until the route is found or the buffer runs out of free space. The increasing delays can therefore be a result of both longer routes or buffering along the route.

Table 7.1 list the delay distributions for the selection methods. During the simulations there were few (0.2% of all delays) very large delays (over 50 seconds) measured. These can not, however, be considered as outliers, as the intermediate nodes are allowed to buffer data packets for very long times. The long delays do not either occur during any special simulation run, but randomly in all runs. Therefore they have to be included in the analysis. The average delays and jitters along with the skew and kurtosis are also shown in the table.

Average delays and jitter are analysed first. As was expected, the average delays increase with the mobility. The interesting notification is that the difference in delays between the selection methods also increases as the speeds get higher. The differences are not, however, significant. The pattern with jitters looks very much like the delay averages', as they also seem to triple when the speed is brought up to 10 m/s from 1 m/s.

In order to be able to analyse the reason behind the increasing delays and averages, the hop count distribution for succesfully delivered data packets was calculated, and it is shown in Table 7.2. The hop count count distributions for both of the selection methods are the same, which means that neither of the selection methods tends to choose longer routes than the other one. The averages show that with higher speeds, the length of the routes, through which data packets were successfully delivered, decreases. Therefore the only reason for increasing delays is that the buffering times of the intermediate nodes increase as the nodes move faster.

As the mobility increases, the amount of hops that the successfully delivered data packets have traversed decreases considerably as more links are broken because of the higher speeds.

Based on the measured delay and jitter no ordering between the selection methods can be done as the delay distributions for both look so similar. Again the results were too much affected by the performance of the DSDV protocol in order to make any clear analysis of th eimpact of selection methods.

Control overhead

The amount of control packets produced for both of the selection methods and all four speeds are showed in Table 7.3. It presents the amount of forwarded advertisements, solicitations, registrations to home agent and registration acknowledgements. Around 70% of the control overhead is composed of the access point solicitations and advertisements, and 30% of home agent registrations and acknowledgements.

The amount of sent data packets during the simulations is 36 000 while the total amount of all control packets is as high as 600 000 to 700 000, 20 times the amount of data packets. If we additionally compare it to the number of successfully delivered data packets, 40-70 control packet forwards are needed for every successful data delivery. This can cause serious problems in networks with higher loads than in the simulation environment, where the load was kept really low in order to avoid the network congestion and packet collisions. With this high amount of control overhead, the efficiency and scalability of the selection methods combined with proactive DSDV can be predicted to be poor.

BBM seems to produce 10 000 to 30 000 control packets more than MBB for all the speeds. This difference is generated mainly by the amount of forwarded access point advertisements. The amount of periodically sent advertisements is same for both of the selection methods. The amounts of sent solicitation messages, which differs only 300 - 1000 packets with BBM being the more active one, can neighter explain this large gap, which leads to the the following explanation. With BBM the advertisements are forwarded longer than with MBB, which is pretty reasonable as with BBM only one access point is kept in memory at time. The expirations of current access points cause the manet nodes to flood the advertisements further than if they would have an alternative with shorter route already in memory.

The registration requests and acknowledgements together comprise the compulsory mobility management part. Interesting here is that registration requests are sent with low speeds 2, higher speeds even 4 times more freguently than replying

acknowledgements. This is again the sign of the incorrectness of the routes stored in routing tables, as two thirds of the sent registration messages never reach the home agent within the expiration time and have to be therefore re-sent. With Mobile IPv6 this means that on the average it takes longer than 10 seconds for the first acknowledgement to reach the mobile node. With higher speeds it is therefore likely that the mobile nodes change their access point to new one before the acknowledgement is received from the old one.

With MBB the amount of sent registration requests is consistently 2000 - 3000 messages bigger than with BMM. This is logical, as a new route is taken into use immediately after the expiration of the old one and the home agent has to be informed of the change. It is, however, likely that the route taken from memory is not optimal in terms of hop count and if an advertisement of shorter route is received, the access point is changed to that and the registration has to be sent to the home agent. As BBM does not have access points in memory, it skips the first phase and only performs the second one.

7.2.2 Scenario 2

Scenario 2 was a special scenario that aimed to study the effect of using predefined positions for the access points on instead of randomizing them.

Packet delivery fractions and packet sending fractions for the scenario 2 are presented in Table 7.4. The situation is very similar to previously analysed scenario 1 with speed 4 m/s. Pdf values are same for both of the selection methods, so no ordering can be done based on them. But when psf values are compared, MBB again performs slightly better.

Delay and hop count distributions for scenario 2 are listed in Tables 7.5 and 7.6. The distributions for both of the selection methods are very much alike, which is why, based on the distributions, both of the selection methods can be said to perform similarly when delays and jitters are considered. If the distributions are, however, compared to the results gained for scenario 1, significant differences are observed. In scenario 2, the fewer amount of access points leads to approximately 10% longer routes on the average than what were measured in scenario 1. Longer routes, on the other hand, result in longer average delays, where the difference is 0.4 seconds, increasing almost 50%. Longer routes have also impact on the pdf and psf values, where the gab between the fractions in scenario 2 is 20% larger than what it was in scenario 1.

If the amount of control overhead produced was high already in scenario 1, it is even 1.4 times higher for scenario 2. Control overhead is listed in Table 7.7.

Total amount of control messages reaches 950000 with BBM, and for MBB it is near 900000. The difference between the selection methods is larger than what is was with scenario 1, and is entirely caused by forwards of advertisements. Like with scenario 1, MBB can be said to perform better when control overhead is considered.

The effect of longer routes can also be seen in control overhead, as the amount of solicitation messages is nearly 2 times higher in scenario 2 than what it was in scenario 1. As routes are longer, the expected link life time is shorter and link break downs more common. In addition to solicitation messages, more frequent link failures can also be seen from the amount of received registration acknowledgements, which is decreased to half of the scenario 1's.

	MBB				BBM			
Delay (s)	1 m/s	2 m/s	4 m/s	10 m/s	1 m/s	2 m/s	4 m/s	10 m/s
0.1	71.71	73.46	73.38	72.56	72.21	72.71	72.37	70.93
0.2	10.54	9.23	7.41	3.47	10.9	9.46	7.43	3.45
0.3	3.62	3.16	2.52	1.27	3.68	3.19	2.45	1.27
0.4	1.86	1.69	1.3	0.82	1.83	1.75	1.32	0.82
0.5	1.39	1.26	1.07	0.72	1.38	1.27	1.03	0.79
0.6	0.89	0.75	0.67	0.54	0.81	0.79	0.67	0.58
0.7	0.79	0.7	0.59	0.53	0.71	0.7	0.65	0.59
0.8	0.69	0.55	0.52	0.49	0.61	0.59	0.53	0.53
0.9	0.52	0.47	0.41	0.42	0.46	0.48	0.45	0.47
1.0	0.54	0.46	0.45	0.47	0.48	0.48	0.48	0.54
1.1	0.4	0.35	0.33	0.38	0.35	0.36	0.35	0.37
1.2	0.36	0.35	0.35	0.38	0.32	0.34	0.38	0.4
1.3	0.36	0.3	0.32	0.35	0.31	0.32	0.33	0.38
1.4	0.29	0.28	0.27	0.32	0.25	0.26	0.29	0.35
1.5	0.32	0.27	0.32	0.35	0.28	0.29	0.33	0.37
1.6	0.25	0.23	0.22	0.28	0.2	0.22	0.26	0.32
1.7	0.23	0.23	0.26	0.29	0.2	0.23	0.26	0.35
1.8	0.23	0.21	0.24	0.29	0.2	0.23	0.25	0.3
1.9	0.17	0.19	0.22	0.25	0.17	0.19	0.22	0.31
2.0	0.22	0.21	0.24	0.29	0.19	0.21	0.24	0.31
2.1	0.15	0.16	0.18	0.24	0.15	0.15	0.2	0.26
2.2	0.16	0.16	0.19	0.26	0.15	0.17	0.2	0.28
2.3	0.17	0.17	0.19	0.24	0.15	0.16	0.21	0.26
2.4	0.12	0.14	0.18	0.23	0.11	0.14	0.19	0.26
2.5	0.15	0.16	0.19	0.23	0.14	0.17	0.21	0.25
2.6	0.12	0.12	0.16	0.19	0.11	0.13	0.17	0.23
2.7	0.12	0.13	0.17	0.21	0.11	0.13	0.17	0.24
2.8	0.12	0.14	0.16	0.22	0.11	0.13	0.18	0.23
2.9	0.09	0.11	0.14	0.19	0.09	0.12	0.16	0.23
3.0	0.12	0.13	0.17	0.22	0.11	0.14	0.2	0.23
> 3.0	3.3	4.23	7.17	13.31	3.22	4.48	7.81	14.11
Average delay (s)	0.44	0.56	0.85	1.46	0.45	0.52	0.79	1.39
Average jitter (s)	0.65	0.86	1.33	2.22	0.65	0.79	1.25	2.07
Skew	5.37	5.41	5.41	5.31	5.36	5.40	5.40	5.27
Kurtosis	29.4	29.74	29.76	28.79	29.33	29.64	29.62	28.44

Table 7.1: Delay distribution for successfully delivered data packets.

	BBM				MBB			
Hops	1 m/s	2 m/s	4 m/s	10 m/s	1 m/s	2 m/s	4 m/s	10 m/s
1	61.17	73.38	70.95	80.65	60.73	73.2	70.67	80.75
2	24.22	19.45	21.58	16.09	24.79	19.52	21.45	15.89
3	8.46	5.1	5.8	2.72	8.51	5.18	6.13	2.78
4	5.02	1.74	1.32	0.5	4.89	1.82	1.38	0.54
5	0.83	0.21	0.29	0.04	0.79	0.17	0.29	0.04
6	0.23	0.09	0.06	0	0.19	0.06	0.07	0.01
7	0.04	0.01	0	0	0.06	0.01	0.01	0
8	0.02	0.01	0.01	0	0.04	0.02	0	0
9	0	0	0	0	0.02	0.01	0	0
>10	0	0	0	0	0	0	0	0
Average	1.64	1.37	1.38	1.23	1.64	1.37	1.4	1.24
Skew	4.52	5.05	4.91	5.26	4.49	5.04	4.91	5.27
Kurtosis	21.64	26.44	25.21	28.37	21.27	26.38	25.19	28.44

Table 7.2: Hop count distribution.

	BBM				MBB			
	1 m/s	2 m/s	4 m/s	10 m/s	1 m/s	2 m/s	4 m/s	10 m/s
Adv	447916	535093	520538	405644	415679	517502	509876	390795
Sol	24779	23484	19784	14663	24265	23199	19236	13694
Reg	96857	103475	117597	131385	98689	106574	119157	134488
RegAck	56534	48371	40804	32512	57573	49134	41022	32602
Sum	626086	710423	698723	584204	596206	696409	689291	571579

Table 7.3: Control overhead.

	BBM	MBB
Pdf (%)	15.24	15.79
Psf (%)	63.05	65.51

Table 7.4: Pdf and psf for scenario 2.

Delay (s)	BBM	MBB
0.1	65.25	64.68
0.2	7.11	6.8
0.3	2.75	2.74
0.4	1.69	1.74
0.5	1.4	1.39
0.6	0.86	0.99
0.7	0.92	0.9
0.8	0.72	0.75
0.9	0.64	0.62
1.0	0.64	0.64
1.1	0.47	0.51
1.2	0.52	0.5
1.3	0.44	0.46
1.4	0.39	0.42
1.5	0.43	0.43
1.6	0.32	0.35
1.7	0.36	0.36
1.8	0.33	0.37
1.9	0.32	0.33
2.0	.035	0.34
2.1	0.36	0.3
2.2	0.32	0.28
2.3	0.27	0.28
2.4	0.29	0.27
2.5	0.3	0.29
2.6	0.23	0.23
2.7	0.26	0.24
2.8	0.23	0.24
2.9	0.23	0.23
3.0	0.27	0.23
> 3.0	11.42	12.08
Average delay	1.24	1.27
Average jitter	1.87	1.89
Skew	5.26	5.24
Kurtosis	28.43	28.23

Table 7.5: Delay distributions succesfully delivered data packets in scenario 2.

Hops	BBM	MBB
1	61.39	62.19
2	27.27	26.13
3	9.13	9.77
4	1.78	1.44
5	0.35	0.43
6	0.08	0.03
7	0	0
8	0	0
9	0	0
>10	0	0
Average	1.53	1.52
Skew	4.40	4.45
Kurtosis	20.29	20.9

Table 7.6: Hop count distributions for scenario 2.

	BBM	MBB
Adv	767567	709065
Sol	36897	35788
Reg	128341	130774
RegAck	22397	23324
Sum	955202	898951

Table 7.7: Control overhead for scenario 2.

Chapter 8

Conclusions

Ad hoc networks have typically been considered as closed, self-sufficient networks where no connections outside its boudnaries have been possible. Connections to fixed networks can, however, be offered by adding special routers called access points at the edge of the ad hoc network. As all packets between the two networks must travel through some access point, the selection method used to choose the right access point can be guessed to have some impact on the communication between the manet node and a fixed.

This thesis proposed and studied the effect of two selection methods, Break-Before-Make (BBM) and Make-Before-Break (MBB). MBB takes advantage of multiple advertisement the manet nodes are to receive as all of them stored in memory and can be from there taken into use in a case the connection to the current access point is lost. BBM discards all additional advertisements, which is why it has to perform an access point discovery whenever the connection is lost. DSDV was used as the ad hoc routing protocol and MobileIPv6 to provide mobility management solution.

The performance of the two selection methods was studied using simulation and two scenarios. Scenario 1 aimed to find out how increased mobility of the manet nodes affects the reachability with both of the selection methods. Scenario 2, on the other hand, was a special scenario that aimed to find out how how the situations changes if predefined positions are used for access points as opposed to random positioning used in scenario 1. First the consistency of the results was verified, after which the reachability analysis was peformed using packet delivery fraction (pdf), packet sending fraction (psf), delay, jitter and control overhead as indicators.

The consistency simulations showed that data sending times, communicating nodes and mobility files defining the movements of the manet nodes can also be random-

ized without that it would affect the consistency of the results. They also showed that pdf can not be considered consistent as the results no constant ordering between the seelction methods, which is why it could not be used as a reliable indicator in the reachability analysis. Psf, on the other hand, could be as a reliable indicator, as there MBB was systematically better than BBM regardless of the randomized parameters.

Based on the psd values gained from the simulations, it is reasonable to claim the MBB selection method to perform better as it gives better results for all of the four speeds used. The difference is smaller at lower mobility, but increases up to 5% with highest mobility. If pdf values are compared, no ranking can be done as the performance of the DSDV protocol becomes a dominant factor affecting the results. This can be concluded from the fact that even though 85% of all data packets are sent towards the access point, only 17% of them reach the destination and over 80% are dropped somewhere along the route.

Delay distributions and jitters are similar for both of the selection methods, so none of the selection methods can be said to perform better when delays and jitters are considered. The reason behind the similarity is the fact that sending nodes are not allowed to buffer data packets in a case no route to an access point is found in memory. Therefore the faster recovery of the MBB only affects fractions, not delays.

The amount of control overhead was huge using both of the selection methods, which is why their scalability and efficiency can be concluded to be poor. However, as BMM produced 15 000 - 30 000 control packets more than MBB for all the speeds, it can be said that MBB perfoms better when the amount of control overhead is considered. With BBM the advertisements are forwarded longer as with expiration of the current route no alternatives are in memory, which would restrict the flooding of the advertisements.

The results for scenario 2 did not differ from the results presented above for scenario 1.

8.1 Future work

Clearly the combination of proposed selections methods and DSDV as the manet routing protocol as used in this thesis is not really a true option. It would, therefore be interesting to see if the performance would be improved if the access point advertisements would be piggypacked with DSDV advertisements or a reactive manet routing protocol like AODV would be used instead. Also the third selection method, multipathing, is definitely worth analysing, as the probability that at least

one of the used access point is functional is higher than if we only use one at a time.

Bibliography

[1] Olli Aalto. The migrate internet mobility project. *Research Seminar on Middleware for Mobile Computing*, February 2002.

[2] T. Camp, J. Boleng, and V. Davies. Survey of mobility models for ad hoc network research. *Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, 2(5):483 – 502, 2002.

[3] Imrich Chlamtac and Yin-Bing Lin. *Wireless and Mobile Network Architectures*. Wiley, 1st edition, 2000.

[4] Douglas E. Comer. *Internetworking with TCP/IP Principles, Protocols and Architectures*. Prentice Hall, 4th edition, 2000.

[5] A. Conta and S. Deering. Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. RFC 2463, IETF, December 1998.

[6] Yih-Chun Hu David B. Johnson, David A. Maltz. The dynamic source routing protocol for mobile ad hoc networks (dsr). *IETF Internet draft, draft-ietf-manet-dsr-10.txt*, July 2004.

[7] S. Deering and R. Hinden. Internet protocol, version 6 (ipv6). RFC 2460, IETF, December 1998.

[8] S. Deering and R. Hinden. Internet protocol version 6 (ipv6) addressing architecture. RFC 3513, IETF, April 2003.

[9] R. Droms. Stateless dynamic host configuration protocol (dhcp) service for ipv6. RFC 3732, IETF, April 2004.

[10] C. Perkins Ed. Mobility support for ipv4. RFC 3344, IETF, August 2002.

[11] Global mobile information systems library glomosim. See URL: http://pcl.cs.ucla.edu/projects/glomosim/, 2004.

[12] Z. Haas. A new routing protocol for reconfigurable wireless networks. In *IEEE International Conference on Universal Communications (ICUPC)*, pages 562–565, October 1997.

[13] Zygmunt J. Haas, MarcR Pearlman, and Prince Samar. The zone routing protocol (zrp) for ad hoc networks. *IETF Internet draft, draft-ietf-manet-zone-zrp-04.txt*, July 2002.

[14] D. Johnson and D. Maltz. Dynamic source routing in ad hoc wireless networks. In *Mobile Computing*, pages 153–181, 1996.

[15] D. Johnson, C. Perkins, and J. Arkko. Mobility support in ipv6. RFC 3775, IETF, June 2004.

[16] Rima Khalaf, Ali El-Haj-Mahmoud, and Ayman Kayssi. Performance comparison of the aodv and dsdv routing protocols in mobile ad hoc networks.

[17] Ed. M. Kojo and Ed. J. Manner. Mobility related terminology. RFC 3753, IETF, June 2004.

[18] R. Moskowitz and P. Nikander. Host identity protocol architecture. *IETF Internet draft, draft-moskowitz-hip-arch-06*, June 2004.

[19] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host identity protocol. *IETF Internet draft, draft-ietf-hip-base-00.txt*, June 2004.

[20] P. Nikander, J. Lundberg ans C. Candolin, and T. Aura. Homeless mobile ipv6. *IETF Internet draft, draft-nikander-mobileip-homelessv6-01.txt*, February 2001.

[21] The network simulator - ns-2. See URL: http://www.isi.edu/nsnam/ns/, 2004.

[22] Opnet. See URL: http://www.opnet.com/home.html, 2004.

[23] C. Perkins and E. Belding-Royer. Ad hoc on-demand distance vector (aodv) routing. RFC 3561, IETF, July 2003.

[24] Charles Perkins and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, pages 234–244, 1994.

[25] J. Postel. Transmission control protocol. RFC 793, IETF, September 1981.

[26] John Postel. Internet protocol. RFC 791, IETF, September 1981.

[27] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. Sip: Session initiation protocol. RFC 3261, IETF, June 2002.

[28] E. Royer, P. Melliar-Smith, and L. Moser. An analysis of optimum node density for ad hoc mobilenetworks. In *IEEE International Conference on Comminications (ICC)*, 2001.

[29] Elizabeth M. Royer, P. Michael Melliar-Smith, and Louise E. Moser. An analysis of the optimum node density for ad hoc mobile networks. In *Proc. IEEE International Conference on Communications*, Helsinki, Finland, June 2001.

[30] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. Rtp: A transport protocol for real-time applications. RFC 1889, IETF, January 1996.

[31] H. Schulzrinne, A. Rao, and R. Lanphier. Real time streaming protocol (rtsp). RFC 2326, IETF, April 1998.

[32] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. Stream control transmission protocol. RFC 2960, IETF, October 2000.

[33] Jun-Zhao Sun and Jaakko Sauvola. Mobility and mobility management: A conceptual framework. In *Proc. 10th IEEE International Conference on Networks*, pages 205 – 210, Singapore, 2002.

[34] Scalable wireless ad hoc network simulator. See URL: http://jist.ece.cornell.edu/, 2004.

[35] Ed. T. Clausen and Ed. P. Jacquet. Optimized link state routing protocol (olsr). RFC 3626, IETF, October 2003.

[36] S. Thomson and T. Narten. Ipv6 stateless address autoconfiguratio. RFC 2462, IETF, December 1998.

[37] C.K. Toh. *Ad Hoc Mobile Wireless Networks: Protocols and Systems*. Prentice Hall, 1st edition, 2001.

[38] Ryuiji Wakikawa, Jari T. Malinen, Charles E. Perkins, Andreas Nilsson, and Antti J. Tuominen. Global connectivity for ipv6 mobile ad hoc networks. *IETF Internet draft, draft-wakikawa-manet-globalv6-03.txt*, October 2003.