Ph.D. in Electronic and Computer Engineering
Dept. of Electrical and Electronic

Modeling and Performance Evaluation of MANET Handover

Ing. Bernardo Leal

Advisor: Dott. Ing. Luigi ATZORI
Curriculum: ING-INF/03 - Ph.D. in Electronic and Computer Engineering

XXIII Cycle
March 2012

To my wife, … my support always.

Content

Chapter 1 - Introduction

A Mobile Ad Hoc Network (MANET) is an unstructured collection of wireless nodes that move arbitrarily and use multi-hop protocols to communicate between each other [1]. There is not a pre-defined infrastructure in a MANET as there is in other types of wireless networks, like WI-FI and WIMAX, so the topology of the network may change dynamically without prediction.

In a wireless structured network, every user register with an access point using a link layer protocol. There is not direct communication between users navigating on the same cell at this level. To may communicate with other users on the same cell, or other correspondent nodes on the structured network, the user has to run a network protocol, like the Internet Protocol (IP). In structured networks, users do not need to run any type of routing protocol as it is needed by MANET nodes. They need only to forward data packets to the access point, which handles packet routing. On the other hand, Ad hoc nodes do not need to register to any other node to may communicate with other users inside the same MANET, and even with nodes in the structured network. MANET nodes connect to each other in first place using a link layer protocol. Later, using the IP protocol, and with the help of an ad hoc routing protocol, it finds its way to forward data packets to its correspondent nodes.

The MANETs were initially proposed to operate as stand-alone networks, usually for temporary communications, such as conferences, emergency rescue, or military missions, restricting its traffic within the MANET premises [2]. In a way different to traditional fixed IP networks, all members in a MANET communicate over multi-hop relays by equally participating in the routing information distribution and maintenance running the same ad hoc routing protocol. Using the routing protocol, ad hoc nodes fill out routing tables that need to use to forward data packets to their destinations as it is done by routers. This is the behavior that differentiates MANET nodes from regular nodes. MANET nodes behave at the same time as regular nodes and as routers, and this behavior is necessary when there is not a structured network that may be used to navigate.

Now days, MANET networks integrate with other networks, like the Internet, permitting ad hoc nodes to communicate with hosts placed in any part of the world. Furthermore, Fourth-generation (4G) wireless systems assume ubiquitous computing and universal access for mobile users that wish to connect to the Internet through heterogeneous technologies, and wish to maintain connectivity globally without interrupting their ongoing communications, even when they cross from one type of network to another, or when their connection paths change the gateways their packets go through. One of the network types included in the 4G systems is the Mobile Ad Hoc Network (MANET) [3]. In such an integrated scenario, the MANET may help to extend the coverage of existing infrastructure networks, like Wireless LANs and 3G networks, as it is shown on Figure 1.1. Here, we may find the integration of different technologies (WI-FI, UMTS, CDMA, WIMAX and MANET in one unique IP network. In this scenario, a mobile user capable of running all these technologies may maintain a communication with a correspondent node, even if moves anywhere.

In the scenario represented in this figure we may see mobile users that being outside the coverage of any Wireless LAN Access Point (AP), or outside the coverage of any of the 3G network cells, may still communicate with their correspondent nodes on the Internet by means of the relays created by the multi-hop ad hoc nodes that reside in the same MANET coverage. This is how a mobile user may

keep its connection with the Internet even if it has lost direct contact with an access point in a structured network.

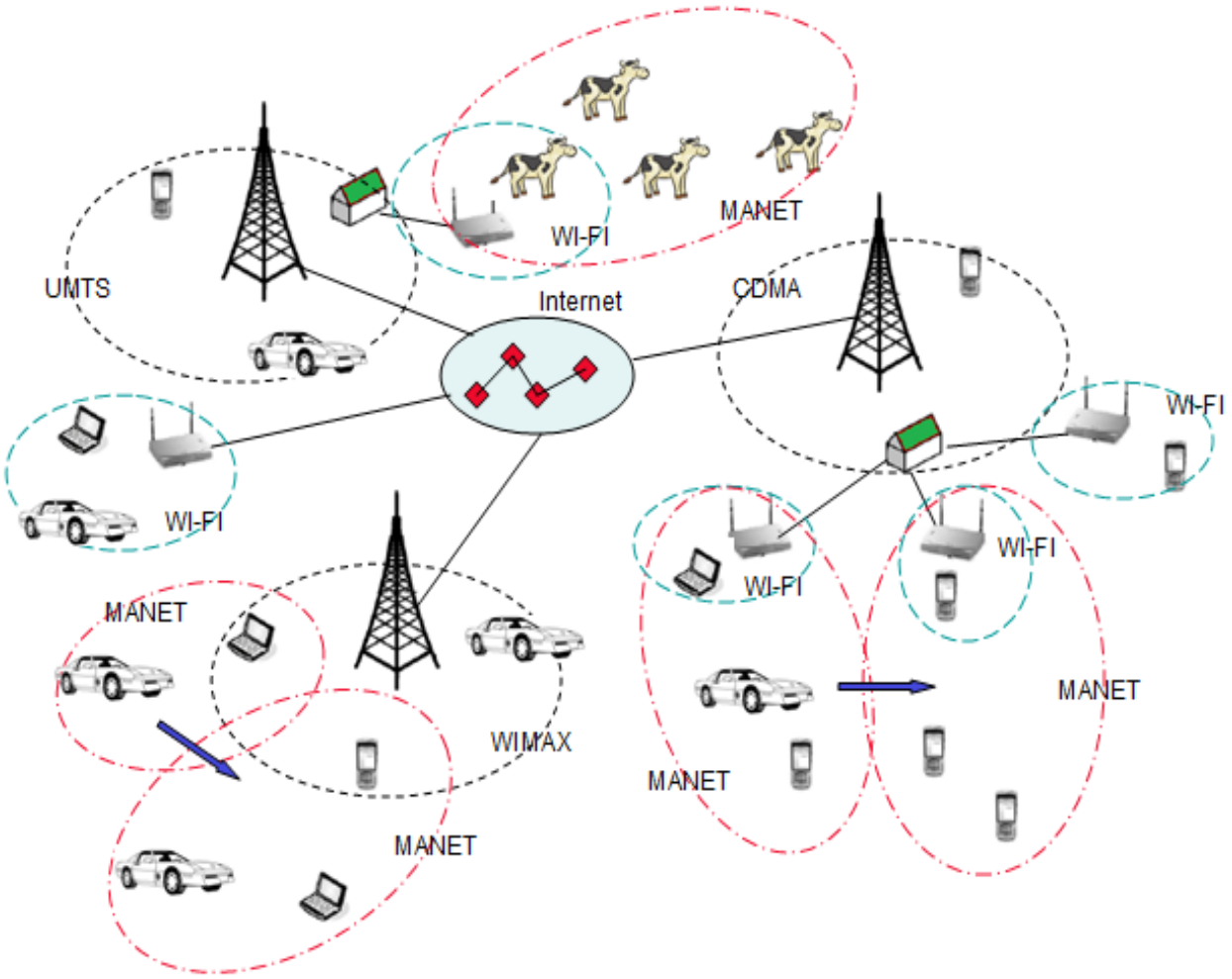

Figure 1.1 MANET Integration

1.1 Smart Objects on MANET's

The expression "Internet of Things" is used referring to the idea of a global infrastructure of interconnected physical objects [4]. This concept is mainly motivated by the growing adoption of the Radio Frequency Identification (RFID) technologies, which have been widely used for tracking objects, people, and animals, making use of an architecture that combines the use of simple RFID tags and extensive and complicated interconnection of RFID readers. This architecture optimally supports tracking physical objects within well-defined areas (such as stores), but it limits the sensing capabilities and deployment flexibility that other challenging application scenarios may require.

An alternative architectural model for the Internet of Things may be a more loosely coupled, decentralized system of smart objects with sensing, processing, and networking capabilities. In contrast to simple RFID tags, smart objects may carry segments of application logic that may let them

evaluate their local environment, and by means of a unique addressing scheme, probably IP, interact with other objects, and even with human users, wherever they are.

Several wireless technologies allow mobile smart objects to increase their pervasive presence around us. WI-FI, WIMAX, and Sensing and Cellular networks are examples of technologies that may support object interconnection, but when they move away from networks structures, MANET may be the recommended way to interconnect them to the Internet. Figure 1.1 shows an integration of different communication technologies, including MANETs, which permit objects ubiquitous communication. In such scenario, a farmer in his car may receive real-time information in his mobile phone or portable PC about data directly coming from his caw sensors in a different country. Neither the caw sensors nor the user device need to be in direct communication with an access point. It is enough that a multi-hop route is established, with the help of other ad hoc nodes, between them and their respective access point.

1.2 MANET's and the Internet

The integration of MANETs with fixed infrastructures must be carefully studied to evaluate how it performs. In such integrated scenario, commonly known as Hybrid Ad Hoc Network, a MANET can be seen as an extension to the existing infrastructure, whose mobile nodes may seamlessly communicate with nodes on the fixed network, forwarding packets throughout the gateways found on the edge that join both types of network. There is not a predefined limit for the size of a MANET. It depends mainly on the link layer technology, the node distribution, and on the traffic conditions, but it is possible to have MANET coverage areas of hundreds of Kilometers, and even more.

However, connecting MANETs to the Internet does not come without difficulties. Ad hoc routing protocols work different than the regular routing protocols used on the Internet, and their interoperability becomes an important issue. In first place, nodes on the Internet do not participate on the route learning and maintenance as it is done by ad hoc nodes on the MANETs. These tasks are left to specialized routers running routing protocols. In contrast, every ad hoc node must exchange routing information with other nodes in the MANET coverage area, which makes them perform, not only as end nodes, but as routers [5]. Communication between nodes on the Internet and mobile ad hoc nodes is done throughout specialized Internet Gateways (IG), that are routers located at the edge of a MANET and which have connections to both, the structured network and the MANET. The gateways must run the routing protocol used on the structured network and the ad hoc routing protocol used on the MANET, which should help them to know if the packets arriving to any of their interfaces must be routed to the opposite interface, or must remain local [6].

Since MANETs were envisioned as isolated non-structured networks, their nodes are not usually set with addresses that follow a structured plan, but when they want to communicate with nodes on the Internet, ad hoc nodes should use Internet Protocol (IP) addresses that follow a structure. One convenient way for assigning structured IP addresses to mobile nodes is to use the same network prefix that is used by the closest gateway. In this way, mobile nodes will be organized on sub-networks surrounding these gateways that share the same network prefix. This organization facilitates the routing tasks done by routers on the Internet, by mobile nodes in the MANET, and by gateways, which have interfaces facing both types of networks [7].

When MANET integrates with the Internet, a more demanding challenge emerges if node mobility is considered. In any moment, a moving node may lose routing information towards its actual MANET gateway. In this scenario, any ongoing communication held by the moving node with a

correspondent hosts on the Internet, will be interrupted. In order to resume the communication, the moving node may need to affiliate to a different MANET sub-network, but even if this is possible, during the time the node changes its affiliation from one gateway to another, some data packets may be lost. Even more, since the moving node will try to adopt a new IP address, whose prefix belongs to the visited MANET sub-network, the ongoing communication may not be resumed, unless an IP mobility management protocol is used.

In 4G systems, it is expected that mobile devices that require communicating with nodes in the Internet are allowed to maintain connectivity globally when moving from one network to another, without interrupting their ongoing communications. Mobile IP is a popular mobility protocol that permits mobile nodes dynamically enter or leave different networks using the same IP address they got on their home network, while still maintaining their ubiquitous communications [8]. However, even with the help of Mobile IP, there will be a brief communication interruption from the moment a mobile node changes its affiliation from one MANET sub-network to another (a handover). This is the research subject of this thesis.

1.3 Thesis Objectives and Organization

MANET integration with structured networks, like the Internet, is a research topic that has received great attention in recent years, but no so much has been argued about seamless handover between MANET sub-networks in a hybrid ad hoc scenario. This is an important topic when we think about ubiquitous and universal communication for mobile nodes on the Internet, as it is expected in 4G systems.

The main objective of this research is to develop a model that may be used to evaluate the performance of MANET handovers under different scenarios. Different issues about MANET integration with the Internet are considered. In first place, a review is made about the elements that mainly affect the execution of the handover procedure. Some of these elements are: the IP mobility protocol implemented, the external route computation procedure, the type of ad hoc routing protocol used, and may be the most important, the gateway discovery approach used. For this evaluation, a mobile node in a MANET holding a communication with a correspondent node in the Internet roams to a different sub-network, having to change its registration to a different gateway. The different scenarios considered to evaluate the handover performance include the use of different types of MANET protocols, the use of different gateway discovery approaches, and the use of different versions of the Mobile IP protocol. In first place, a review is made of the functioning condition of the proposed scenario. Special attention is given to the ad hoc protocol types and the Mobile IP protocol. Second, a handover model is proposed, which is used to develop some metrics that may be used to evaluate the MANET handover performance. Finally, these metrics are used to evaluate the different scenarios proposed before.

This PhD thesis is organized as follows: In Chapter 2 there are described the different types of ad hoc protocols: proactive routing protocols, reactive routing protocols, and hybrid routing protocols. In Chapter 3 it is presented how a MANET integrates with a structured network, like the Internet. It is described how IP addresses are assigned to mobile nodes, how the Mobile IP protocol helps mobile nodes to maintain its home address, and finally, how mobile nodes discover that a gateway is available in the same MANET. In Chapter 4 it is described the MANET handover procedure. In particular, it is shown the differences between the Mobile IP for IP_{v4} and Mobile IP for IP_{v6}. Additionally, the handover performance for each case is evaluated. In Chapter 5 it is described with more detail the proactive and reactive handover procedures. A description of the handover timing is shown for each one. In Chapter

6 it is presented a handover model that permits the evaluation of the MANET performance during a handover for the different gateway discovery approaches, for the different Mobile IP protocol versions and for the different ad hoc protocols. On Chapter 7, the handover performance results for the different scenarios are presented. Finally, the research conclusions are presented.

Related Papers

The content on this thesis is mainly based on the research work done during the PhD studies and that were published on the next papers:

- Bernardo Leal, Luigi Atzori. Objects Communication Behavior on Multi-Homed Hybrid Ad Hoc Networks. 20th Tyrrhenian International Workshop on Digital Communication. Pula, September 2-4, 2009.
- Bernardo Leal, Luigi Atzori. Performance Analysis of Multi-Homed Hybrid Ad Hoc Network. MOBIMEDIA 2009. London, September 7-9, 2009.
- Bernardo Leal, Luigi Atzori. MANET Average Communication Interruption Time Evaluation. IEEE International Conference on New Technologies, Mobility and Security, NTMS-2010. Paris, February 7-10, 2011
- Bernardo Leal, Luigi Atzori. Book Chapter. Connecting Moving Smart Objects to the Internet: Potentialities and Issues when using MANET Technologies. On: Mobile Ad Hoc Networks: Current Status and Future Trends. CRC Press, November 16, 2011. ISBN 9781439856505

Chapter 2 - MANET Protocols

The IP addressing scheme used in the Internet is hierarchical. This means that every IP address has a network ID component that identifies the network an Internet host belongs to. By using this feature, routers do not need to find routes to every possible destination host, but to the networks these hosts belong to. Traditionally, addresses on a MANET are not necessarily hierarchical, so MANET node addresses are independent to every other. In this scenario, traditional IP routing protocols do not work well and a MANET routing protocol should be used to find routes to hosts instead of finding routes to networks [9]. Since usually addresses used on MANET nodes do not include network identifications, there is no way to know if the destination host is on the same MANET or outside it by only inspecting the destination address. A search has to be made first inside the MANET, and if it is not found, it is guest that the destination is outside the MANET.

MANET nodes must use routing protocols to learn how to forward packets to its destinations, but efficient ad hoc routing protocols must be adaptive to topological changes and traffic demands [10,11]. In general, ad hoc routing protocols can be divided into proactive routing (table-driven) and reactive routing (on-demand). Some protocols may even use a hybrid routing approach. The earlier types of ad hoc routing followed a proactive scheme, similar as those used on the Internet, where routing tables are built based on the information routers exchange about the network topology. Proactive table-driven routing protocols maintain one or more routing tables in every node in order to store routing information about other nodes in the MANET. This type of routing protocol attempts to update the routing table information either periodically, or in response to changes in the network topology in order to maintain consistent and up-to-date routing information. The advantage of proactive protocols is that a source node does not need to initiate a route discovery procedure to find a route to a destination node each time it has packets to send, which would cause some delay to initiate packet forwarding. With proactive protocols, the route to a destination is always available from the routing table. One disadvantage with proactive routing is that the frequent exchange of routing information with other nodes produces excessive overhead over the MANET [5], especially in the case of a large number of high-mobility mobile nodes.

As an alternative, reactive ad hoc routing protocols have been developed to decrease the routing overhead produced with proactive protocols, and thus preserving the usually scarce bandwidth available on this type of networks. Reactive routing protocols begin a route discovery to a destination node when the source node has data packets to send to a destination. After discovering the route, the route maintenance is initiated to keep the route until it becomes no longer required, or the destination node is not reachable anymore. Thus, with reactive routing protocols two main phases are involved: Route Discovery phase and Route Maintenance phase. The advantage of this type of protocols is that routing overhead messaging is low since routing information is only exchanged when routes are needed. But reactive routing has an important drawback: since there are not permanent routing tables, there will be a long route discovering delay. From the moment the mobile node discovers it has to send some packets to a new destination, it may take a while before it may learn how to forward them.

As a compromise between the proactive and the reactive routing protocols, a hybrid ad hoc routing version may be used, which combines the proactive scheme for those nodes that are found in a certain region of the MANET close to the chosen gateway, and the reactive scheme for those nodes

found on the remaining region (farther from the chosen gateway). In this way, part of the MANET is set to work in a less congested environment, but their nodes will suffer from higher delays. The other part of the MANET is set to work in a more congested but more prepared to forward environment. On Table 2.1 is shown a list of some of the most popular ad hoc routing protocol classified according its type.

Table 2.1. Ad Hoc Routing Protocol Types

Protocol Type	**Protocol Name**
Proactive	Routing Information Protocol (RIP)
	Destination-Sequenced Distance-Vector (DSDV)
	Optimized Link State Routing (OLSR)
	Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)
	Open Shortest Path First (OSPFv3) with MANET extensions
Reactive	Ad-hoc On-Demand Distance Vector (AODV)
	Dynamic Source Routing (DSR)

2.1 RIP

RIP is a routing protocol based on the Bellman-Ford (or distance vector) algorithm. This algorithm has been used for routing computations in computer networks since the early days of the ARPANET [12]. RIP uses one of a class of routing algorithms known as Distance Vector algorithms. RIP is intended for use within the IP based Internet. This protocol does not solve every possible routing problem. RIP is primary intended for use as an Internal Gateway Protocol (IGP) in networks of moderate size. The protocol is limited to networks whose longest path (the network's diameter) is 15 hops. The protocol depends upon "counting to infinity" to resolve certain unusual situations, like routing loops. This protocol uses the numbers of hops as fixed metric to compare alternative routes. If used in a MANET, every node must propagate its routing table to every other neighbor periodically, which increases traffic congestion noticeably. Although it is a very simple protocol, RIP is not recommended for use in a MANET.

2.2 DSDV

DSDV is a modification of the conventional Bellman-Ford routing algorithm. It addresses the drawbacks related to the poor looping properties found on RIP in the face of broken links [13,14]. The modification adapted in DSDV makes it a more suitable routing protocol for ad hoc networks. It adds a new attribute, a sequence number, to each route table entry of the conventional RIP. Using the newly added sequence number, the mobile nodes can distinguish stale route information from the new ones and thus prevent the formation of routing loops. As in every proactive protocol, in DSDV, each mobile node of an ad hoc network maintains a routing table, which lists all available destinations in the network, the metric and next hop to each destination and a sequence number generated by the

destination node. Periodically or immediately when network topology changes are detected, each mobile node advertises routing information using broadcasting or multicasting a routing table update packet. However, with DSDV arises route fluctuation because of its criteria of route updates. At the same time, DSDV does not solve the common problem of all distance vector routing protocols, the unidirectional links problem.

2.3 OLSR

The Optimized Link State Routing Protocol (OLSR) is developed specially for mobile ad hoc networks [15,16]. It operates as a table driven, proactive protocol, i.e., it exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbor nodes as "multipoint relays" (MPR). In OLSR, only those nodes that were selected as MPR are responsible for forwarding control traffic, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required. Nodes which have been selected as multipoint relays by some neighbor node(s) announce declare link-state information for their MPR selectors periodically in their control messages. Thereby a node announces to the network that it has reachability to the nodes which have selected it as an MPR. In route calculation, the MPRs are used to form the route from a given node to any destination in the network. Furthermore, the protocol uses the MPRs to facilitate efficient flooding of control messages in the network.

2.4 TBRPF

The TBRPF routing protocol [17] is based on source trees and reverse path forwarding. Each node running TBRPF computes a source tree based on partial topology information stored in its topology table using a modification of the Dijkstra's algorithm. The tree provides paths to all reachable nodes on the MANET. To minimize overhead, each node reports only a part of its source tree to its neighbors. TBRPF uses a combination of periodic and differential updates to keep all neighbors informed of the reported part of its source tree. Each node also has the option to report additional topology information (up to the full topology), to provide improved robustness in highly mobile networks. Like OLSR, TBPRF uses a default route to announce reachability to the Internet. A MANET node that has Internet access over an external network, to which it is connected, operates as a gateway and advertises Internet connectivity as a 0.0.0.0/0 default route.

2.5 OSPFv3-MANET

$OSPF_{v3}$ with MANET extensions ($OSPF_{v3}$-MANET) [18] is an adaptation of the regular OSPF protocol used on regular IP structured network to be used on ad hoc networks. $OSPF_{v3}$ uses Hello messages for neighbor discovery. MANET Designated Routers (MDRs) are chosen based on the 2-hop neighbor information learned from Hello messages, and these designations are then distributed in subsequent Hello messages. As in OLSR, Hello messages track link connectivity. If a Hello message has not been received within a 6 seconds period, the link is declared to be down and a new Link State

Advertisement is distributed. Database Description and Link State Advertisements (LSAs) are distributed by MDRs to share the network's complete picture. $OSPF_{v3}$-MANET uses MDRs to control overhead, similar as how OLSR make use of its MPRs. A range for the overhead control messages is also available, so the LSA flooding can be made to vary from a minimal flooding that covers the MDRs only, to a full LSA flooding that covers all routers in the network, similar as how it is done with the $OSPF_{v2}$ protocol.

2.6 AODV

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is particularly intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times [19,20].

When a source node running AODV attempts to send a packet to a destination, but it does not have a valid route in its routing table, it will broadcast a Route Request (RREQ) to discover a route for the destination. The traveling RREQ will set up reverse paths pointing from the nodes receiving the RREQ back to the source node. Each node processing the RREQ records its neighbor’s address from which the first copy of the RREQ is received, as the next hop towards the source node. If the destination or a node knowing the destination receives the RREQ, it wills unicast a Route Reply (RREP) back to the source node through the path established by the RREQ. Each node forwarding the RREP will also create a route entry from itself to the destination. To maintain route entries, each node keeps track of its active connectivity to its next-hop nodes by the use of local Hello messages. If a node detects a broken link to one of its neighbors, it may either broadcast or unicast a Route Error (RERR) message to all precursors.

2.7 DSR

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes [21]. One of the important features of DSR is the implementation of Source Routing, which permits that every node caches the complete hop-by-hop source routes from itself to other destinations in a Route Cache. Each data packet carries a complete source route in its DSR header, containing a list of hops through which, this data packet will travel. Using source routing, the source node can control the route its own data packets will take in its way to destination. Other nodes will forward these data packets using the source routing information found in the DSR headers and will cache it for later use. The Route Discovery occurs when a source node attempts to send a data packet to an unknown destination by broadcasting a RREQ flooding the network. Only the destination or an intermediate node knowing a route to the destination can send back a RREP to the source node. The Route Maintenance is implemented by each intermediate node transmitting data packets to confirm the reachability of its next-hop node specified in the source route.

2.8 Holding Time

After usable routes are found, both types of routing protocols keep track of them by means of aging timers. With proactive protocols, Hello packets are transmitted periodically between all neighboring nodes on the MANET. If Hello packets are no longer received from a known neighbor, new routes has to be computed. With reactive protocols, Hello packets are transmitted periodically only between intermediate nodes that are part of an active route. But with either type of protocol, a mobile node must wait a predefined holding time before declaring that a connection with a neighbor is lost. In Table 2.2 we may see some of the most important characteristics of three of the most popular ad hoc protocols.

Table 2.2. Ad Hoc Routing Protocol Waiting Time

	AODV	**OLSR**	**OSPF**
Route Management Messages	• Route Request • Route Reply • Hello (1 sec)	• Hello (2 sec) • TC (each 5 sec)	• Hello (2 sec) • LSAs (as needed)
Route Holding Time	No Hello within 2 seconds	No Hello within 6 seconds	No Hello within 6 seconds
Length of Messages	• Route Requests (24 bytes) • Route Replies (20 bytes) • Route Errors (20 bytes) • Hello messages (4-6 bytes)	• Hello (8 bytes + 4 bytes for each neighbor interface) • Topology Control (4 bytes + 4 bytes per advertised neighbor)	• Hello (36 bytes + 4 bytes per neighbor) • Router-LSAs (20 bytes + 40 bytes per neighbor)

One of the characteristics shown in this table is the route holding time, which is the time the router has to wait before declaring that a route (on reactive protocols), or a link (on proactive protocols) is lost. Paradoxically, even though reactive protocols have longer transmission delays, they tend to take less time than proactive protocols to recover when a route is lost as a consequence of node mobility. This is so because they take less time to declare lost routes than proactive protocols. We can see on the table that OLSR and OSPF hold routes for 6 seconds after they are lost. Instead, AODV holds routes only 2 seconds after they are lost.

In order to verify how the protocol holding time affects MANET performance, we simulate over the OPNET simulator a handover for two different MANET protocols: AODV and OLSR. The simulation scenario includes one mobile node and several fixed nodes on a MANET using 802.11b at 2 Mb/s with a radio range of about 250 meters on each node. The nodes are placed randomly in a rectangular area of approximately 1000 x 1000 m^2 and when the node moves, it loses and regains contact with its destination. On Figure 2.2 are shown the end to end delay for the two protocols when a mobile node transmitting data packets to a correspondent node in the same MANET has to change one intermediate node for another. The simulation is run for about 15 minutes, and we may see that approximately over the minute 10, the mobile node losses its link with one of the intermediate devices, but then establishes a new link with another one, and the end to end connection is retaken.

We may see that when AODV is used (the blue line), the end to end delay does not go over 2 seconds. Instead, when OLSR is used (the red line), it may be seen that the end to end delay reaches around 6 seconds. This result corresponds with the holding times shown on table 2.2. With OLSR, when a route is lost, it has to wait 6 seconds before it may initiate a new route search. With AODV, it only has to wait 2 seconds before it may initiate a new search when a link is lost.

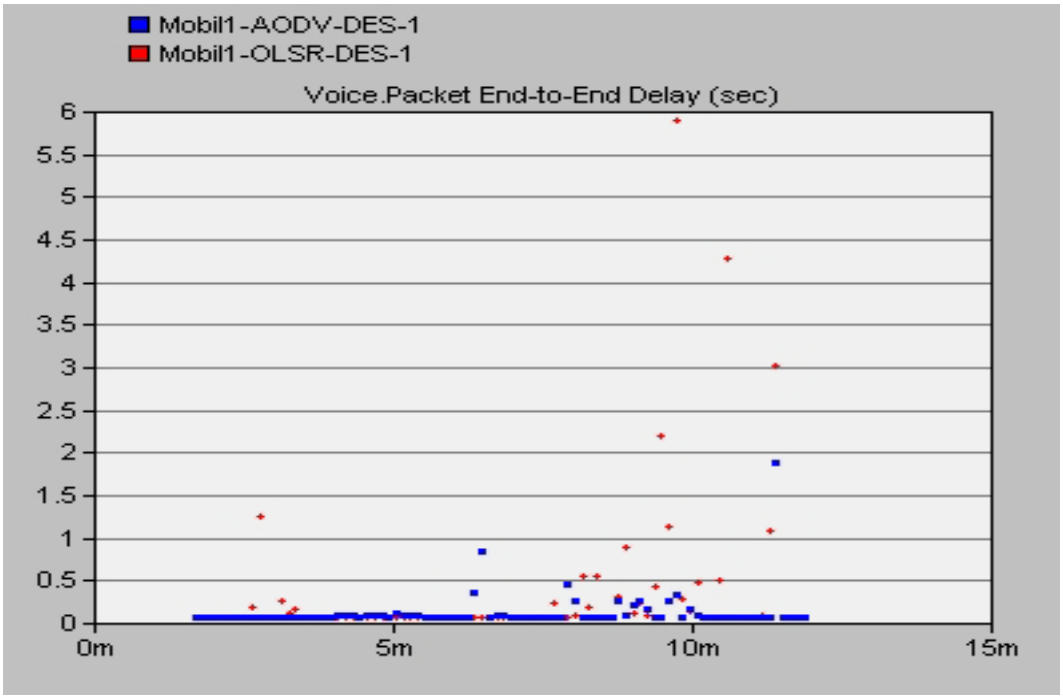

Figure 2.2 Handover End to End Delay for AODV and OLSR

Chapter 3 - MANET Integration with the Internet

Many solutions have been proposed to integrate mobile ad hoc networks with the Internet. In these integrated scenarios, different ad hoc routing protocols may be configured to maintain the intra-MANET communication, while Internet Gateways (IG) are used to forward packets back and for between the MANET and the Internet. The gateways are specialized nodes that act like an interface between the two types of networks and that implement both groups of protocol stacks, the Internet Protocol (IP) stack, and the ad hoc routing protocol stack. The link layer technology used in the MANET side is not defined, and may vary between different MANET sub-networks. On cellular networks, it is commonly used General Packet Radio Service (GPRS) and Universal Mobile Telecommunications Service (UMTS), while on data networks it is frequently found the use of Wireless Fidelity (WI-FI) and Worldwide Interoperability for Microwave Access (WIMAX) networks. Most of the time, the gateways are fixed, but sometimes selected mobile nodes on the MANET may behave as mobile gateways when they are in direct contact with the structured network. Additionally, when nodes move and roam between different MANET networks, a mobility protocol like Mobile IP have to be used to provide permanent Internet connectivity for MANET nodes. Even though other integration mechanisms, like Network Address Translation (NAT) had been previously used, now days most existing architectures connecting MANETs with the Internet are based on Mobile IP [22], but since this mobility protocol was originally designed to work in a one-hop network scenario, some expansions should be made to the ad hoc routing protocols in order to make them work properly with Mobile IP. Alternatively, a version of Mobile IP for MANETs could be developed.

An issue related to the integration of MANETs with the Internet is the way data traffic is forwarded between MANET nodes and correspondent nodes on the Internet. Possible alternatives can be classified according to the tunneling mechanism used: tunneling based integration routing solutions and non-tunneling based integration routing solutions. With the tunneling integration solution, if the destination address is not found in the MANET, the originating node encapsulates the data packets aimed to the Internet and routes them to the gateway. Later, the gateway decapsulates the packets and sends them to their destinations using standard IP forwarding. In order to reduce the routing labor of intermediate nodes is by using routing headers, which contain information about how to route data packets to the selected destination. By doing so, intermediate nodes do not have to do any route searching. The drawback of this approach is that it introduces significant overhead due to the additional headers added. With the non-tunneling integration solution, mobile nodes send packets directly to their default route expecting that intermediate nodes correctly forward them to the gateway in case the gateway has announced itself previously as the default gateway. With this solution, the ad hoc routing overhead is greatly reduced, but also the data forwarding efficiency gets reduced, since it is not guarantee that the shortest path to the gateway is chosen when data packets are forwarded. As with the tunneling solution, the gateway will forward the data packets to their final destinations using standard IP forwarding.

3.1 Ad hoc nodes address assignation

How IP addresses are set over MANET node interfaces has a great impact on how a MANET integrates to the Internet, specially, in a highly mobile scenario. In a MANET, traditionally, IP addresses are set in an autonomic way in every ad hoc node without follow any hierarchy, and for this reason MANET routing protocols deal with networks as flat address spaces, treating all nodes in a network as peers. This addressing approach make difficult to group nodes under a common network prefix, as it is normally done in structured wired networks, making more complicated the route tables filling process. When proactive routing protocols are used, the route tables of every ad hoc node must be filled with the addresses of every other node belonging to the same MANET. Additionally, if a MANET that uses this type of address configuration is integrated with the Internet by means of a gateway, the routing protocol used in the structured network will have to announce towards the Internet an enormous amount of addresses, which may affect negatively the network performance.

To overcome these issues, ad hoc nodes should be aggregated or grouped by means of sharing a common network prefix. This is an objective difficult to accomplish when using manual and statically address configuration, since MANET nodes are intrinsically mobile, besides that the time needed to perform the manual configuration on every node does not usually satisfy the common requirement for rapid network deployment. It has been proposed to use DHCP (Dynamic Host Control Protocol) servers for the automatic assignation of IP addresses, but it does not work well if a server happens to fall outside the local network. The DHCP address assignment scheme belongs to an address configuration type known as statefull auto-configuration. An alternative approach is to use a stateless address auto-configuration, a method in which every node sets by itself a global IP address. With stateless auto-configuration there is a risk of setting duplicate addresses in a network. If this is the case, a mechanism known as Duplicate Address Detection (DAD) may be used to correct the problem. DAD requires that the whole MANET be asked if a particular address is being used, in which case, a new stateless address must be set. There is a much smaller chance of address duplication with Ip_{v6} than with Ip_{v4} [7]. The main drawback of using the DAD mechanism is the control overhead that it introduces in the MANET, specially, if the procedure is repeated periodically to avoid address duplications when a partitioned MANET merges, or a MANET splits.

Neither the manual nor the stateless auto-configuration help nodes to be aggregated by means of sharing a common network prefix. To deal with this problem, Care of Address (CoA) may be used. CoA are stateless addresses that share the same prefix that is used by the gateway the node register to in order to communicate with hosts in the Internet. Once a node learns about the gateway prefix, it may use it to set its own IP address. A new CoA has to be set every time a node registers to a different gateway. With Ip_{v6}, a MANET node configures an address using a global prefix managed by one of the gateways, and uses this address as source IP address when communicating with external hosts on the Internet [7]. Return traffic from the external nodes on the Internet is therefore routed back to the gateway, which in turn forwards the packets to the MANET node. However, for IP_{v4} there is a great scarcity of global addresses, and those available may need to be share. Thus, to allow different MANET nodes to share an address for external communication, the gateway may need to implement some sort of Network Address Translation (NAT) in combination with the Mobile IP protocol. However NAT has two important problems. First, since NAT is mainly used to share a limited amount of global addresses, the brief temporal address assignation occurs only when a Mobile Node initiates a communication with a correspondent node on the Internet and not when the host on the Internet wants to communicate with a mobile node in the MANET. It means that mobile nodes will not always have fixed global addresses that correspondent nodes on the Internet may use to reach them. Additionally, when mobile nodes roam between different MANET sub-networks, they have to obtain different global addresses from other NAT servers, whose prefix must be associated to the visited MANET sub-

networks. Each time a node have to change its IP address without the assistance of a mobility protocol any ongoing communication held by the mobile node will be interrupted.

3.2 Mobile IP Architecture

Mobile IP was originally designed as an efficient and scalable mechanism that allows users to seamlessly roam among IP networks without changing their home IP addresses. Mobile IP has two versions, Mobile IPv4 and Mobile IPv6. The Mobile IPv4 network architecture was developed by IETF to provide continual Internet connectivity to mobile users, and includes three functional entities, as are shown in Figure 3.1. A Mobile Node (MN), which may be a host or a router, is a host that has a permanent home address (HoA) from its home network and may changes its access point from one subnet to another without changing its home address. A Home Agent (HA) is a server located on the mobile node home network, usually sharing the same access point device. Finally, the Foreign Agents (FAs) are also servers, but which are located in each foreign network, usually sharing the foreign network access point device. The FAs can enable the mobile nodes to access the Internet [6,7,23,24].

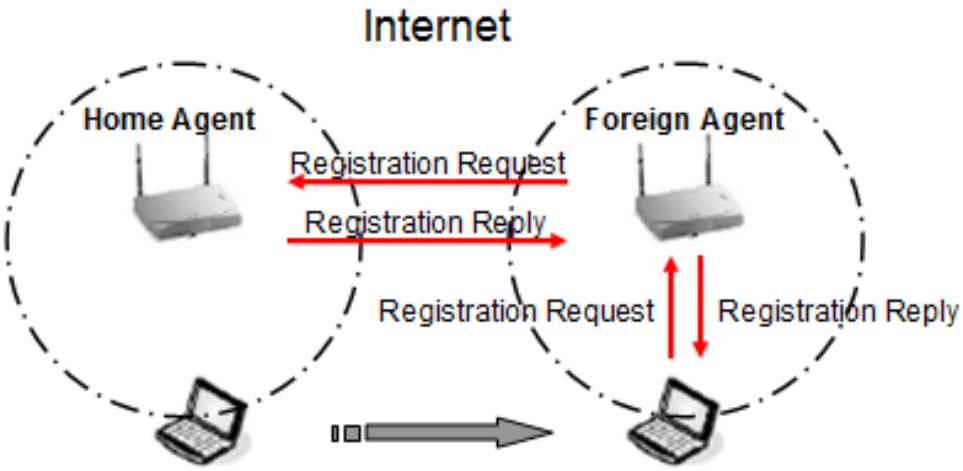

Figure 3.1 Mobile IP Architecture

To begin the Mobile IP process, a MN must set its IP address using the same network prefix that is used by its Home Agent. To advertise their presence, HAs and FAs broadcast periodically in their respective networks, Agent Advertisements via one-hop links. These Advertisements are used by the MNs to register to the HA, and to detect whether the MN still remains on its home network or has roamed to a foreign network. If the MN has roamed, it must set a new IP Care-of Address (CoA) using a prefix similar to the FA network prefix. This address is used to identify the MN in the visited local network. Finally, the CoA must be registered to the HA by means of the FA. By doing this registration, the HA creates a new entry containing the MN's CoA, or updates the existing entry in its Binding List, and then sends a Registration Reply to the FA. Upon receiving the Registration Reply, the FA records the MN's home address in a Visitor List, and relays the Registration Reply to the MN.

After the CoA registration, the HA knows how to reach the MN in the foreign network where the CoA is allocated. Packets destined to the MN's home address will be tunneled to the MN's CoA by the HA throughout the FA. Packets transmitted by the MN aimed to the Internet are forwarded by the

visited network gateway toward their destinations. This is how Mobile IP helps MNs navigate on the Internet by using their unique home IP addresses.

However, Mobile Ip_{v4} suffers from some drawbacks, like long handover time and the increase in signaling overhead. It suffers from a long handoff delay due to the triangle routing problem described before. Additionally, implementing Mobile IP over MANETs requires that some modifications be made over the original protocol because Mobile IP assumes that a MN must have direct link connectivity with an agent, but in a MANET a mobile node is generally multiple hops away from it. To solve this problem, it has been proposed that the following requirements should be satisfied [25]:

- Foreign agents should be able to forward packets using multi-hop routes, instead of delivering only via a directly connected link.
- Mobile nodes should be able to use Mobile IP care-of addresses multiple hops away from a foreign agent.

Additionally, when used in MANETs, it may be necessary to discover agents in a reactive way in order to avoid the periodic agent advertisements that increase network congestion, and to better adapt with the use of reactive routing protocols.

As an alternative, one way to use the original one-hop Mobile IP protocol in a multiple hop scenario, like a MANET, is by using Mobile Gateways [51]. A Mobile Gateway (MG) is a regular mobile node that becomes a MG when it is one hop away from a Foreign Agent. FAs are devices that are fixed to the Internet backbone and MGs register to them following the regular Mobile IP protocol. On the other hand, MNs that are not in direct contact with FAs register to the MGs using the regular ad hoc protocol. If there are multiple reachable mobile gateways, selection is usually made based on the minimal hop count.

3.2.1 Mobile IP – AODV Case

As a study case, we analyze an approach that utilizes AODV for discovery and maintenance of routes within the MANET, whereas Mobile IP is utilized to allow that mobile nodes may have Internet connectivity everywhere. We assume that Internet Gateways connect the MANET to the Internet and broadcast their own global prefix information to the MANET [25].

IG/FA Discovery. When a mobile node wishes to reactively discover a foreign agent, it does so by issuing a RREQ. The mobile node then broadcasts this RREQ to its neighbors. When a neighbor node receives this RREQ, it first checks its Foreign Agent List to determine whether it is currently registered with a FA. If the mobile node is not registered with any FA, then it re-broadcasts the request. If, on the other hand, the mobile node is currently registered with a FA and has a route to that FA, then it creates a route reply with the agent's IP address placed in the Foreign Agent IP Address field of the RREP extension. The RREP is then unicast back to the source node.

When the source node receives a route reply for a FA, it can then use that route to unicast an Agent Solicitation message to the FA. Upon receiving the Agent Solicitation message, the FA unicasts an Agent Advertisement back to the mobile node. After receiving the Agent Advertisement messages from different FAs, the mobile node proceeds to select the optimum gateway, usually that with the smallest hop count. From the selected gateway, the MN reads the network prefix which then uses to set its CoA.

After choosing an Agent Advertisement, the node creates a Registration Request message that unicasts to the foreign agent. The node should have a valid path to the foreign agent since it has just received an Agent Advertisement from that agent. In the event that the mobile node's route to the

foreign agent has become invalid, the node initiates a route discovery procedure to find a new route to the foreign agent. After receiving the registration request, the foreign agent processes the Registration Request and then unicasts a Registration Reply back to the mobile node.

Before sending data packets, a mobile node must have a route to its destination, but initially it does not know whether the destination node is within the ad hoc network, or whether it is reachable through the wired interface on the FA. All hosts homed in the ad hoc network must have the same network number as the gateway interface connecting to the ad hoc network. To learn a route versus any of those hosts, the mobile node broadcast a route request, to which intermediate nodes or the destination node itself will answer. But if the destination node has roamed to a different MANET network, the gateway will respond, after controlling its binding list that the route to the destination node is throughout the gateway. In a similar fashion, for destinations nodes with network numbers different to the originating node, a route request is broadcast. If the destination node resides on the same network, it, or any intermediate node will respond with a valid route. If not, the request packet will traverse the ad hoc network and eventually will be received by the gateway, which will respond if it has a valid route to the destination node.

3.2.2 Mobile IPv6

Mobile IP_{v6} offers a number of improvements over Mobile IP_{v4} mainly due to the capabilities inherited from IP_{v6}. To support mobile devices roaming in the Internet which dynamically change their access point, the IETF standardizes Internet protocol version 6 ($Ip_{\mathbf{v6}}$) that includes a built-in mobility support. Under the Mobile $IP_{\mathbf{v6}}$, built-in route optimization eliminates triangle routing, which is present in Mobile $IP_{\mathbf{v4}}$. The foreign agent is no longer necessary, packets are sent to the mobile agent that can then be tunneled to the mobile node using an $IP_{\mathbf{v6}}$ router header instead of IP encapsulation. According to the IETF Internet Draft, the basic operation of the Mobile $IP_{\mathbf{v6}}$ mechanism is as follows [7]:

1. MN uses IP_{v6} Neighbor Discovery to acquire a new CoA using $IP_{\mathbf{v6}}$ stateless address auto-configuration or statefull address auto-configuration (such as $DHCP_{\mathbf{v6}}$ or $PPP_{\mathbf{v6}}$). Since the CoA has the network prefix of the foreign subnet, there is no need for a foreign agent.
2. The mobile node (MN) discovers its home agent (HA).
3. When the mobile node moves to foreign network, obtains a care of address (CoA) and sends Binding Update (BU) messages to the HA and to the correspondent node (CN) to update its binding cache.
4. After receiving the BU message, the CN reply to the MN with a Binding Acknowledgement (BA) message, and sends packets directly to the MN.

3.3 Gateway Discovery

Gateways play a fundamental role in MANETs integration with the Internet, not only because gateways are used to route packets between the Internet and the MANETs, but because frequently the Mobile IP agents are installed in this same device. When a mobile node in an ad hoc network wants to communicate with a host on the Internet, it has to discover first an efficient and reliable Internet gateway. But the gateway discovery time has a strong influence on packet delay and network throughput. It means that the gateway discovery process is a key component for providing efficient Internet connectivity to ad hoc nodes.

A MANET node must discover an Internet gateway prior communicating with an Internet correspondent host. The gateway discovery approaches can be broadly divided into three categories [27,28]: proactive discovery approach, reactive discovery approach, and hybrid discovery approach. With the proactive approach, ad hoc nodes passively hear periodic advertisements that are transmitted from Internet gateways. On the contrary, with the reactive approach, ad hoc nodes solicit agent advertisements from nearby gateways when they need to communicate with nodes outside the local network. In either case, agent solicitations and agent advertisements will be relayed by other ad hoc nodes by means of a multi hop ad hoc protocol. The proactive discovery approach may be used with both, proactive and reactive routing protocols, but there is not much sense on using the reactive discovery approach with proactive routing protocols since every node in the MANET should be already aware about every other node in the same MANET, including available gateways. Using the proactive discovery approach with a proactive routing protocol increases the traffic congestion. In order to reduce the overhead produced by this combination, routing information may be piggybacked on agent advertisements. As a result, duplicate route discovery could be avoided, and thus, bandwidth resources may be saved. Another way to reduce the advertisement overhead with the proactive discovery approach is by reducing the frequency of the advertisement flooding. This frequency may be adjusted dynamically according to the traffic conditions in order to reduce this congestion.

The reactive discovery approach generates lower discovering overhead than the proactive approach, which is valuable in wireless networks, but that does not help mobile nodes on having routes to destination hosts available just when they are needed. Additionally, and even more important, if a node roams to a different MANET sub-network, to discover foreign gateways, it will surely take longer time when using the reactive discovery approach than when using the proactive one. Paradoxically, when a connection with a gateway is lost, the reactive discovery approach usually takes less time to recover to recover it than the proactive approach. The agent solicitation in the reactive approach is launched when the mobile node detects that certain event has taken place at a particular moment, i.e., the loss of a gateway registration, the loss of a gateway route, or even the detection of a certain roaming status.

It has been also proposed to use a hybrid discovery approach, which combines the proactive and the reactive discovery approaches. In this case, the proactive approach is usually implemented for mobile nodes that are closer to the gateway, limiting the scope of the advertisement flooding, reducing in this way the header overhead. Nodes that are farther away get to know about gateways by requesting them only when they are needed. Different criteria may be used to define the flooding scope. A popular one is by setting the maximum number of hops the advertisements are allowed to travel. Another one is by restricting on the intermediate nodes the relay of advertisements to only those that share the same address prefix.

It has been also argued that the hybrid discovery approach is not enough to reduce the discovery overhead when the network conditions change. So it has been proposed the use of an adaptive gateway discovery algorithm based on the dynamic adjustment of the scope of the gateway advertisement packets [29,30]. Thus, by just monitoring data packets, gateways may adaptively select the packets Time To Live (TTL) of their advertisement, in order to best suit the current network conditions. For instance, in a low traffic and/or low node density scenario, the TTL may be increased to allow farther away nodes receive periodic agent advertisements without affecting network conditions. On the other hand, in a high traffic and/or high node density scenario, the TTL should be reduced. In this case, nodes not receiving periodic agent advertisements need to get foreign agent information from one of the many available intermediate nodes. Even more, nodes that do not lie in the N-hop neighborhood of the foreign agents may learn about available gateways from unicast advertisement packets aimed to other nodes. This technique is known as eavesdropping. With eavesdropping, a single agent solicitation from any mobile node can potentially benefit all of the other nodes that are close to

the one that broadcasts the solicitation, as well as those nodes that lie along the path to the requesting node.

An alternative way to control the discovery overhead is by dynamically adjusting the frequency of the agent advertisements according to the traffic conditions. For instance, shorter routes are associated to longer route lifetimes, so the routes could be updated later, that is, the advertisement frequency could be reduced. It has been also proposed a restricted flooding scheme, which is based on the property of prefix continuity. Under this scenario, a MANET mobile node only forwards the gateway advertisement messages which it uses to configure its own IP address [31]. This property, additionally to help reduce flooding, guarantees that every node on the MANET shares the same prefix than its next hop to the gateway, so that the MANET gets divided in as many subnets as gateways are present.

When there are multiple gateways available in the MANET, a selection criterion must be defined to choose only one of them. A straightforward solution is to select the gateway that has the shortest number of hops to the mobile node from the default gateway. However, other metrics, like the gateway offered load can be used in order to select the most appropriate Internet gateway. The offered load can also be used to implement a traffic balancing mechanism. Internet gateways could advertise a metric of the load which passes across each one of them within the gateway discovery messages. MANET nodes could use this information to take a more intelligent decision than when only the number of hops to the gateway is considered.

3.3.1 Ipv6 Gateway Discovery

The Internet draft "Global Connectivity for Ipv6 Mobile Ad Hoc Networks" describes how to provide Internet connectivity to mobile ad hoc networks. In particular, it proposes and illustrates how to apply the two methods for Internet gateway discovery: the proactive approach and the reactive approach. The proposed methods target all MANET protocols regardless of whether they are reactive and proactive [7].

To may communicate on the Internet, a node should know the global prefix of the MANET and the address of the related Internet gateways(s). First, the node auto-generates a global IP_{v6} address by using the global prefix information and its 64-bit interface ID. The mobile node then uses this global address as its care of address when possibly performing a home registration. If no home registration is needed, the mobile node is at home in the MANET and the prefix of its home address belongs to its Internet gateway.

After configuring a global IP address and obtaining a route to the correspondent node, the mobile node starts to send it packets via the chosen gateway using the running ad hoc routing protocol. When the gateway receives the packets, it encapsulates them adding its own address as the source address and forwards them directly to the correspondent node bypassing the home agent. In the reverse route, the correspondent nodes encapsulate the packets using the MANET node care of address as the destination address, but are sent directly to the gateway, which forwards them to the mobile node using the ad hoc routing protocol.

3.4 Proposed Architectures

The integration of MANETs with the Internet is a topic that has been evaluated by researchers during the last few years, and as a consequence, a number of schemes for MANET integration have

been proposed. The majority of these schemes are based on the use of Mobile IP to manage mobile nodes IP mobility, but they differentiate between each other in a certain number of characteristics, between which, we may recall the ad hoc routing protocol that manage the intra-MANET communication, the gateway discovery approach used, and the route discovery procedures implemented, among others. On Table 3.1 is shown a list of some of the proposed schemes that use Mobile IP as their IP mobility protocol.

Table 3.1 Proposed schemes for MANET integration

Discovery Approach	Scheme	MIP version	Routing protocol	Route discovery	Other Characteristics
Proactive	Lei and Perkins [32]	v4	Modified RIP	Subnet	Nodes are compelled to register even if not needed
	Ergen and Puri [33]	v4	DSDV and TBBR	Subnet	The Agent advertisement contains care of address, source address and hop count
	Xie and Kumar [34]	v4	Enhanced DSDV	Know all internal nodes	EDSDV maintains all the features of standard DSDV but reduces the packet loss due to broken links and overcomes the stale route problem of standard DSDV
Reactive	Ammari and El-Rewini [35]	v4	DSDV	Subnet	Mobile Gateways one-hop away from Foreign Agents provide Internet connectivity to the rest of MANET nodes Load and hop distance are used as criteria for gateway selection
	Nilsson et al. [36]	v6	AODV	Search inside first	Modified AODV I-RREQ and I-RREP messages are used to discover the gateway
Hybrid	Broch et al. [37]	v4	DSR	Subnet	Slow gateway and route discovery
	Sun et al. [38]	v4	AODV	Search	Nodes are compelled to register even if not needed
	Tseng et al. [8]	v4	DSDV	Subnet	Mobile nodes within the gateway range receive periodic agent advertisements. Nodes outside this range must send agent requests
	Jonsson et al. [39]	v4	AODV	Search	Nodes are compelled to register even if not needed
	Ratanchandani and Kravets [29]	v4	Any on demand	Mixed	Mobile nodes use an arbitrary address within the MANET and use a care-of-address for external communication, as specified by Mobile IP

					Mobile nodes within the gateway range receive periodic agent advertisements. Nodes outside this range must send agent requests
	Benzaid et al. [40]	v4	OLSR	Know internal nodes	Mobile nodes within the gateway range receive periodic agent advertisements. Nodes outside this range must send agent requests
	Shin et al. [41]	v4	Any	Subnet	The coverage of IGWs is extended by WRs. Only the WRs can rebroadcast periodic Agent Advertisements. The mobile nodes out of the backbones' coverage have to broadcast Agent Solicitations
	Xi and Bettstetter [42]	v6	Any on demand	Subnet	Mobile nodes configure themselves with new stateless address when they roam to a different network
	Wakikawa et al. [43]	v6	Any	Know all internal nodes	Nodes are compelled to register even if not needed

In this table, the schemes are grouped according the gateway discovery approach used, and are identified by the name of their proponents. Most network models include several MANET sub-networks, each of which is attached to the Internet backbone by means of a gateway. Gateways define MANET ranges. Usually, related with each gateway is associated a parameter N. Any mobile node within N wireless hops from the gateway is said to be within the service range of this gateway. This range is achieved by setting TTL = N in each gateway's agent advertisement. In case a mobile node is within the service range of multiple gateways, it can choose closest one as its default gateway. Each gateway has two Network Interface Cards (NICs), one wireless interface and one wired interface. Gateways are connected to the Internet through their wired interface. Hence, gateways cannot move but non-gateway hosts are free to roam around.

We may also notice in this table that most of the schemes use the hybrid gateway discovery approach in order to profit from the advantages of both, the proactive and the reactive discovery approaches. By using the proactive approach within a predefined range, nodes closer to the gateway receive periodic agent advertisements, which permits them to be always aware of the most convenient gateway to be registered to. Additionally, periodic advertisements can be used for acquiring CoA information, for default route creation, to define MANET diameter, and to make handover decisions. On the other hand, nodes farther away from gateways need to request agent advertisements when they want to connect with hosts in the Internet. This approach will increase the data forwarding delay, but these nodes will suffer from less of the traffic congestion caused by the periodical agent advertisement coming from the gateways.

There is not a dominant ad hoc routing protocol type used on these schemes, but we may see that AODV is the preferred reactive routing protocol and DSDV is the preferred proactive routing protocol. The type of routing protocol is highly related to the type of gateway discovery approach. With the use of proactive protocols, ad hoc nodes have information about every possible route on the MANET in their routing tables. If a route is not found in the routing table, a default route is used to

forward packets outside the MANET. We may notice that in the schemes where proactive discovery approach is used, a proactive routing protocol is implemented. With reactive routing protocols, a destination route is discovered only when it is needed, which is similar to the behavior of the reactive gateway discovery approach, where agent advertisements are requested only when needed. That is the reason why in some schemes, to speed up data packet forwarding to the Internet, proactive discovery approach are used in combination with reactive routing protocols.

Finally, it´s found on these schemes some variations on the methods used for mobile node address assignation. In most of them the mobile node sets a home and CoA address by matching the network prefixes of the chosen gateways. This helps mobile nodes recognize if the destination host is outside the current MANET. In some schemes, mobile nodes have two addresses: one that uses for communicating inside the MANET, and one that uses for communicating with hosts on the Internet. When the IPv6 protocol is used, the node generates a global IPv6 address by using the global prefix information coming from the gateways. The node uses then its 64-bit interface ID to construct a valid address with the acquired prefix.

Chapter 4 - MANET Handover

Usually, the Internet backbone offers sound data delivery as a single “best effort” class of service, but when we care not only about if data is just delivered, but about how it is delivered, we talk about Quality of Service (QoS). QoS is a measure of how good a delivery service is according to some predefined parameters. The quality of a delivery service in a network is especially important for real time communication, like full duplex voice communication, and videoconferences. On wireless networks, and particularly on ad hoc multi hop networks, it is not easy to accomplish the QoS requirements. Some of the QoS parameters that could be used in a Hybrid Ad Hoc Network environment are: maximum round-trip delay, available bandwidth, bit error rate, packet loss, end to end delay, and jitter, between others [44].

One of the factors that affect the QoS on Hybrid Ad Hoc Networks is the handover between MANET sub-networks. When nodes travel through different MANET networks, they usually have to change the gateway they are registered to (a handover). When a handover occurs, there may be packet losses and also increase on the end to end delay and jitter. If the end to end delay grows above a predefined amount, there may even be connections losses with correspondent nodes on the Internet. In comparison with other wireless networks, QoS on MANETs is specially affected by handover occurrences, specially, because ad hoc nodes do not receive handover signaling messages from gateways as mobile nodes do in structured networks to perform seamless handovers. According to the mobility detection mechanisms used by standard the Mobile IP protocol, such as Lazy Cell Switching (LCS), Prefix Matching (PM), or Eager Cell Switching (ECS), a mobile node is capable of detecting whether it has roamed to a new network via one hop link connectivity. Instead, nodes in a MANET, which usually are multiple hops away from a gateway, have to make their handover decisions based on metrics they have to collect by themselves in this multiple hop scenario.

In Figure 4.1 is shown a generalized handover procedure when a mobile node roams between MANET different sub-networks. As it may be seen in the figure, we may define three main phases: the gateway discovery phase, the agent registration phase, and the packet forwarding phase. The time required to execute each one of these phases varies depending on several factors, one of which is the handover triggering mechanism used. The most frequently triggering factor used on MANETs is the distance to gateways measured in number of hops. With this mechanism, mobile nodes may decide to handover when the packets received from the actual gateway arrive after a predefined number of hops, or when advertisements from a closer gateway are received. When any of these events occurs, a new association may be established with a closer gateway.

On MANETs, a handover is highly sensitive to the type of agent discovery approach used. With the proactive discovery solution, the agent advertisement messages are broadcast by gateway nodes and forwarded to the whole ad hoc network. The agent advertisement messages may be used for mobile movement detection and for handover decision based on the number of hops to gateway nodes. For example, the MIPMANET Cell Switching algorithm (MMCS) establishes that an already registered visiting node should register with another foreign agent if it is at least two hops closer to this foreign agent than to the foreign agent that it is currently registered to for two consecutive agent advertisements. Alternatively, a handover may be also triggered if the visiting node loses contact with

its registered agent and saved advertisements from other agents are still valid. Otherwise, it will have to send and agent solicitation, as it occurs with the reactive discovery approach. However, these mechanisms have an important limitation. This type of handover is not adaptive to highly dynamical network topologies. The time a mobile node takes to learn that it has lost its gateway registration, and the time taken to establish a new registration may render the network useless.

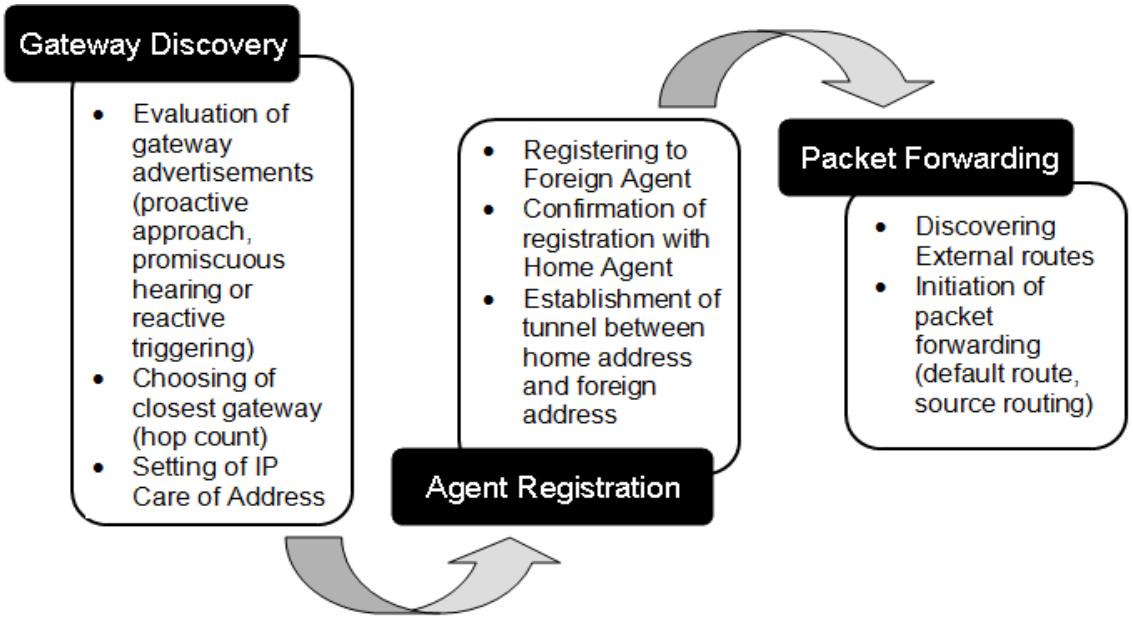

Figure 4.1 Handover Procedure

In some circumstances, the handover mechanism implemented when the reactive agent discovery approach is used may result more efficient than the mechanism used with the proactive discovery approach because in the former a mobile node is allowed to reactively discover a Mobile IP agent whenever necessary. Thus, instead of waiting for periodic agent advertisements, the mobile node can promptly discover a new agent as soon as it detects that it has lost connectivity with its registered agent. In response to the solicitation, an agent may unicast an advertisement to the mobile node, instead of broadcasting it, to significantly reduce the routing overhead. The main challenge of this alternative concerns with the efficient design of handover triggers that can optimize the handover performance. Additionally to the loss of a gateway registration, mobile nodes may also utilize invalidate gateway route entries for movement detection and gateway discovery initiation. However, the main drawback of this kind of solution is that of not being good for detecting mobile node movements to other MANET networks in order to make fast handover decisions. Finally, we have to remember that with the reactive discovery approach, before packets may be sent to the Internet, it is required first to discover adequate agents and gateway routes, which will increase the transmission delay.

Hop count is not the only metric that may be used as a trigger to initiate a handover. Some authors have proposed using a combination of hop counts and gateway load [45,46]. With this type of scheme, a dynamic gateway algorithm is provided to calculate an optimal gateway to handover when there are multiple gateways to choose from. With this metric combination, if a gateway is heavily loaded forwarding data from other mobile nodes, it may not be chosen as the actual gateway, even if it closer to the requesting node than others gateways. With the use of this type of algorithm, the handover time may become reduced, but with the use of other metrics, like the round trip delay, the handover performance may be improved even more.

MANET handovers do not depend only on the type of gateway discovery approach used, or the handover triggering mechanism. MANET handovers are also sensible to the type of ad hoc protocol used. On Table 4.1 is shown a comparison list of the main effects that the different types of MANET protocols produce over a MANET handover.

Table 4.1 Ad Hoc Routing Protocol Effects over a MANET Handover

Protocol Type	**Advantages**	**Disadvantages**
Proactive Protocol	• Permanent availability of Internal and External Routes • Easier IP Mobile prefix identification • Compatibility with proactive gateway discovery	• Significant congestion • Longer time to recover broken routes • Reactive triggers not available
Reactive Protocol	• Low congestion • Lower time to recover broken routes (lower time to find gateways) • Possibility for proactive agent advertisements	• Routes not available (long time to find routes) • In some cases, non IP Mobile prefix identification • In some cases, non-permanent availability of Agent Advertisements

From this table, we can see that proactive routing protocols produce more congestion than reactive protocols when handovers occur between different MANET sub-networks. But most important, proactive protocols take more time to recover a gateway route when it becomes lost than reactive protocols. On the positive side, proactive protocols offer a better route availability than reactive protocols, which reduces the end to end delay. On the other hand, when reactive protocols are used, mobile nodes have to search destination routes only whenever they are needed. The most valuable advantage of reactive protocols is that nodes have to wait less time to search new routes whenever one is lost, and this makes a big difference.

In order to overcome some of the disadvantages that characterize each type of routing protocol, some modifications can be made to improve the MANET performance during a handover. In Table 4.2, we may find summarized some of the proposals made on the schemes listed on Table 3.1 about how to improve handover performance.

Table 4.2 Mechanisms for improving handover performance

Protocol Type	**Mechanism for improving inter-MANET handover**
Proactive Protocol	Mechanisms implemented to reduce congestion: • Unicast advertisement to those specific nodes that register with agents • Route piggybacking to avoid route rebroadcasting • TTL rebroadcasting control to cover only the desired physical area

	• Maintain Agents List • Computation of multiple routes to a single destination • Multiple Agent Registration
Reactive Protocol	Mechanisms implemented to reduce congestion (when broadcasting advertisements): • Unicast advertisement to those specific nodes that register with agents • Maintain Agent List • Use tunneling instead of default routes • Computation of multiple routes to a single destination

We may see on this table that some of the mechanisms are implemented for both type of routing protocols. These are unicasting instead of broadcasting agent advertisements, maintaining an agent list, and computation of multiple routes to a single gateway. The computation of multiple routes to a single destination permits to have alternative routes available immediately, when a gateway route is lost. This mechanism makes a route search unnecessary. On the other hand, maintaining an agent list may help nodes to register faster to another agent when the actual registration is lost.

With proactive routing protocols it is possible to add routing information (piggybacking) on the periodic agent advertisements in order to avoid ulterior routes search. This mechanism is not necessary with the reactive protocol since the route is learned when the agent responds to an agent solicitation. Finally, one of the most important mechanisms used with proactive routing protocols is the use a TTL rebroadcasting control to cover only a desired physical area.

4.1 Ip_{v6} Handover

In IP_{v6} Mobile Ad Hoc Networks the two methods for Internet gateway discovery are considered: proactive gateway discovery that periodically disseminates Internet gateway advertisements to all nodes in the MANET; and reactive gateway discovery that utilizes solicitation and advertisement signaling between a MANET nodes and the Internet gateway. The handover procedure varies slightly according the discovery approach in effect. If the mobile node has not received any gateway advertisements from the current Internet gateway or other Internet gateways in a predefined period of time, it will initiate an Internet gateway discovery (reactive approach). When this happens, the mobile node broadcast gateway solicitation messages, to which nearby gateways may respond. Gateways receiving solicitations with hop count greater than a predefined threshold, do not respond. If a closer than the current gateway responds, the handover is initiated while the current gateway is notified in order that it begins to send pending data packets and mobile node authentication information to the new gateway. Additionally, the mobile host sends binding update to corresponding host in the Internet to notify about its new Care-of Address. This permits the corresponding node to forward packets directly to the mobile node, instead that to the Home Agent.

With the proactive discovery approach, a mobile node may trigger a handover without losing contact with its actual gateway and without requesting gateway advertisements. If a mobile node receives an advertisement from a gateway that is closer than the current one, it wills handover to the closer gateway following a similar mechanism used in the reactive approach. In either case, when a handover is executed, the mobile node constructs a new CoA based on the mobile host's interface ID and the new Internet gateway's network prefix. Since the older gateway sends pending data packets

and mobile node authentication information to the new gateway before the actual handover is executed, no user data is lost, resulting in a seamless handover.

4.2 Handover Performance

There are some metrics that we can use to measure the performance of An Hybrid Ad Hoc Network. One of them is The Packet Delivery Ratio (PDR), which is a ratio between the amount of packets that arrived to its destination and the amount of packets that were transmitted. Traditionally, the PDR is mainly influenced by the type of routing protocol under consideration. As the node mobility increases, proactive protocols have shown a much lower performance results compared to reactive routing protocols. The reason is that proactive protocols usually have a higher convergence time compared to reactive protocols as the link break rate increases. Additionally, when a link is broken it is marked as “lost” for a longer period of time than in reactive protocols. During this time packets using this link are dropped. This behavior also affects the routes towards Internet gateways, which helps on reducing the PDR.

Another important metric that may be used to measure performance of Hybrid Ad Hoc Networks is the Gateway Discovery Overhead (GDO), which refers to the number of messages bytes associated to gateway discovering. This metric is also greatly influenced by node mobility. With the proactive discovery approach, GDO remains more or less constant regardless of the node mobility since gateways broadcast its agent advertisements periodically. However, with the reactive discovery approach, the GDO increases noticeably with node mobility because the link break rate increases and nodes send agent solicitations as soon as they lose contact with their actual gateway. On the other hand, GDO is also affected by the type of routing protocol used since they are responsible of gateway route discovering and maintenance. Since reactive routing protocols react faster than the proactive protocols to topology changes, they tend to generate more overhead traffic as the link break rate increases.

The normalized control overhead (NCO) is a metric which is computed as the relation between the total number of data packets successfully received plus the whole control overhead, over the total number of data packets successfully received. The control overhead usually considers messages related to the routing and auto configuration protocol. We have to add the overhead related to the agent discovery process. It is well known that schemes based on proactive routing protocols need to send a lot of control traffic to deliver data packets to their destinations that grows with node mobility. On the other hand, reactive routing protocols are characterized for having a low NCO, even in high mobility scenarios.

One metric that helps evaluate how well a network may adapt to certain level of QoS is the average end-to-end delay for mobile node communications with hosts in the Internet. When a proactive routing protocol is used, the delay of the communications is quite short thanks to the proactive creation and update of the routes. On the other hand, with reactive routing protocols data packets are delivered with a low average delay when the mobility is low, but when it is high, the links break more often and new route discoveries must be performed, which increases the latency of the communications. Additionally, it has been found a short delay with the use of proactive gateway discovery approach than with the reactive one because they update the routes to the Internet at periodic intervals of time.

In the cases considered so far, a single gateway serves alone a whole MANET, and its simultaneous use by several MANET nodes may result in heavy traffic congestion around the gateway

node. Additionally, the use of a single gateway has the drawback of being a single point of failure. In order to solve these problems, multiple gateways can be used for a particular MANET domain. The availability of multiple gateways provides the network with higher robustness and more flexibility for global Internet connectivity. In this scenario, additional to increase the overall throughput of the MANET to the global Internet, if any one of the gateways fails, another one can take over the failed condition. With the addition of new gateways, handovers will appear when mobile nodes roam between the different MANET sub-networks formed. The MANET performance will be reduced as a consequence of handovers. The GDO, the NCO, and the average end to end delay will increase with the appearance of handovers.

Related with the MANET robustness and greater flexibility for global Internet connectivity is the possibility of having multiple routes to the same gateway. Link failures is highly probable in a highly dynamic ad hoc network, and losing only one link of a multi hop route to a gateway will mean triggering a handover to find routes to anew gateway. One way to avoid unnecessary handovers is by having multiple routes form the originating node to the chosen gateway. In this way, when a route or a fraction of it is broken, a backup route may be used. To maintain multiple routes to a same destination in a MANET, a multiple route ad hoc routing protocol, like AODV Multiple Alternative Paths AODV-MAP [47] may be used.

Additionally, the handover performance may be improved if multiple foreign agents are available. But to manage multiple foreign agents covering the same ad hoc network, the visitor information lists need to be synchronized between all of them. The information must be synchronized whenever an entry is added or deleted from the visitor list in any of the gateways. All gateways will then be able to see if a visiting host is within the mobile ad hoc network, even if has not directly registered with some of the gateways receiving the registration request.

4.3 Ip_{v6} Handover Performance

In IP_{v6} Mobile Ad Hoc Networks, the handover process may be split into different phases that vary according the discovery approach used. With the reactive discovery approach we may differentiate a detection phase, a discovery phase, a request phase and a reply phase. During the detection phase the node evaluates the need to handover when contact with its actual gateway is lost. It occurs when no more advertisements are received from the current gateway and this may trigger a search to find a new gateway. During the search phase gateway advertisements are requested and necessary information is gathered to perform the handover. During the request phase, a reconnection solicitation is send to the chosen gateway, and finally, during the reply phase the handover is performed when a registration confirmation is received from this gateway. We can compute the handover time $Tr_{handover}$ for the reactive case as follows

$$Tr_{handover} = T_{detect} + T_{search} + T_{request} + T_{reply} \quad (4.1)$$

In the proactive case there are not detect and search phases. Mobile nodes decide to handover solely based on the periodic gateways advertisements received, so we can compute the handover time $Tp_{handover}$ for the proactive case as follows

$$Tp_{handover} = T_{request} + T_{reply} \quad (4.2)$$

With the proactive case, mobile nodes are not forced to handover as they are with the reactive case only when gateway registration is lost, but since MANETs are multi-hop networks with fast variable topological conditions, excessive handovers may results in QoS degradation and increasing connection dropping probability. For this reason, it is recommended then, that mobile nodes maintain their registration to their current gateways as long as possible. It is recommended [43] to define a gateway advertisements scope range by controlling the TTL count on the advertisements packets, and to not trigger a handover until the distance to a new gateway be several hop counts less than the distance to the current gateway.

Chapter 5 - Handover Procedure Analysis

In a Multi Homed Hybrid Ad Hoc Networks, each gateway and its registered mobile nodes form separated MANET sub-networks. As shown on Figure 5.1, for this analysis it is considered a generic network architecture where a MN engaged in a communication with a correspondent node on the Internet roams between two different MANET sub-networks. When the MN finds itself in the foreign MANET, it wills handover by changing its registration to the visited gateway. The time a MN takes to handover from one sub-network to another is mainly affected by the gateway discovery approach used and by the running ad hoc routing protocol.

For this analysis, we will evaluate two different handover scenarios over which we elaborate a mobility model that we will use for the performance evaluation. In one scenario, the proactive agent discovery approach is used, leaving the reactive approach for the other scenario. Also, in both scenarios it is considered the utilization of both versions of the Mobile IP protocol, MIP_{v4} and MIP_{v6}, to support node mobility on the Internet. Depending on the MIP version used, the visited network agent will perform either, as a Foreign Agent or as an Access Router. Finally, in both scenarios it is considered the utilization of both types of routing protocols: the reactive routing protocol and the proactive routing protocol.

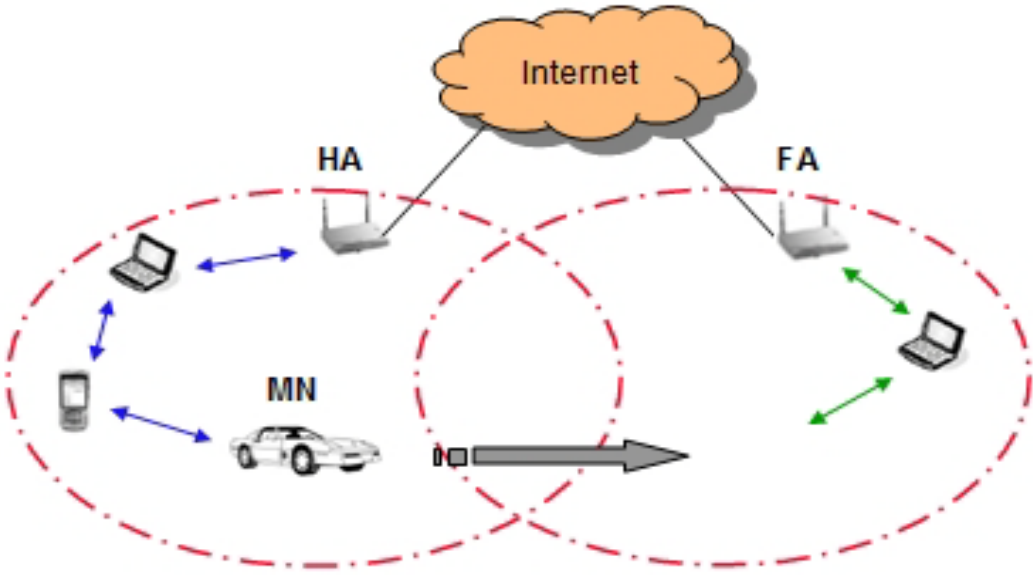

Figure 5.1 Handover Scenario

The scenario initiates whit a MN registering with a Home Agent in order to establish a communication with a correspondent in the Internet. After the communication is established, the MN moves, and a moment later it finds itself closer to a Foreign Agent than it is to its Home Agent. Under this circumstance the MN may be triggered to handover to the visited sub-network. The triggering mechanism is highly dependent on the agent discovery approach implemented. With the proactive

approach, a MN may be triggered to handover when agent advertisements from a closer gateway arrive. Instead, with the reactive approach, a MN is usually triggered to handover when the agent registration or the route to the current agent/gateway is lost. It follows a detailed description of these two handover scenarios.

5.1 Proactive Approach.

With the proactive approach mechanism, (see Figure 5.2) periodic agent advertisements provide mobile nodes with permanent information about agent presence. This gives the MN the opportunity to choose and register to the most convenient agent/gateway, usually the nearest one (measured in hops count) to the MN. In other words, every time a new agent advertisement is received by the MN, a handover may be triggered if this advertisement corresponds to a FA whose hop distance is smaller than the distance to the actual agent. On Figure 5.2 is shown a handover signaling diagram for the proactive gateway discovery approach when a handover occurs.

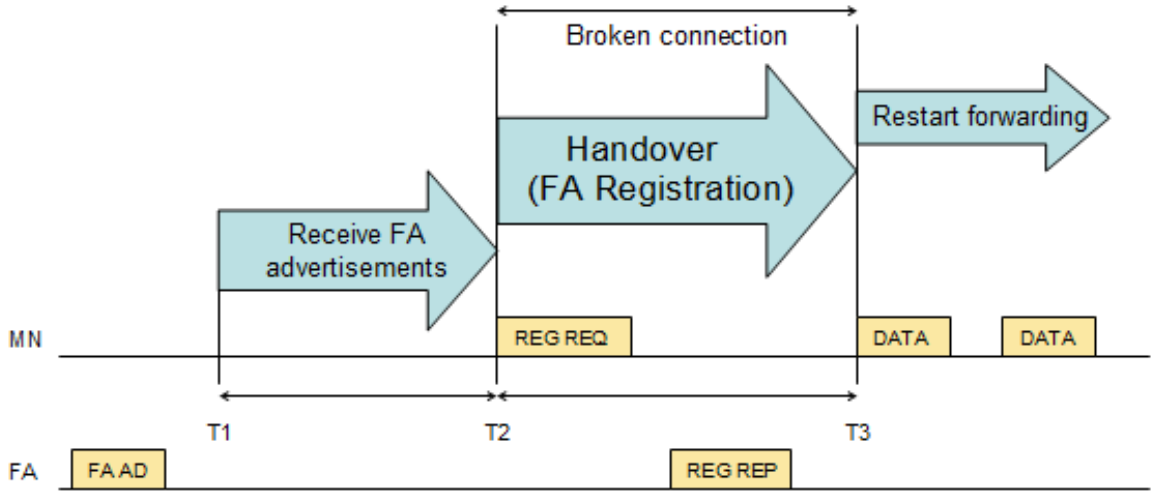

Figure 5.2 Proactive Handover Signaling Diagram

It may be seen that when new agent advertisements (FA AD) arrive to the MN from a FA, the MN takes the time from T_1 to T_2 to evaluate if these advertisements came from a gateway that is closer to the MN than the gateway the MN is currently registered to or not. If it is closer, a handover may be immediately triggered by setting in first place, a new CoA using a network prefix similar to the visited gateway address prefix. Immediately, the MN initiates the handover by unicasting a registration request (REG REQ) to the originating FA. In our case it occurs at time T_2. When the FA receives the REG REQ, it updates the MN binding information with the MN´s Home Agent. Next the FA unicasts a registration reply (REG REP) to the MN. This occurs sometime between T_2 and T_3. The handover is complete when the REG REP arrives to the MN, which occurs at time T_3. At this moment the MN is ready again to resume forwarding data packets to its correspondent node, but now throughout the visited MANET gateway, instead that throughout the Home Agent.

The duration of the time periods ($T_2 – T_1$) and ($T_3 - T_2$) is not fixed and depends mainly on the running ad hoc protocol and the hop distance between the MN and the FA. During the time from which the MN sends the registration request until it begins again forwarding data packets ($T_3 - T_2$), any

ongoing communication with correspondent nodes in the Internet will be interrupted, and any data packet sent between the MN and the CN may be lost. This time will be defined here as the broken connection time, and we may see that for the proactive agent discovery approach, the broken connection time equals the handover time. Thus, with the proactive discovery approach, the broken communication time and the handover time is (T_3 - T_2).

5.2 Reactive Approach.

Alternatively, with the reactive discovery approach, mobile nodes receive agent advertisements only when they require them. Particularly, a mobile node that maintains a communication with a correspondent node on the Internet is triggered to handover when the current agent registration expires, or when the route to the current gateway is lost. When the handover is triggered, the mobile node initiates a search for a new gateway that it can use to continue forwarding data packets versus its destination on the Internet. But if the mobile node is not engaged in a communication with host on the Internet, even if it moves to a different MANET sub-network, it will not initiate a gateway search because it does not have data packets to send. On Figure 5.3 is shown a MIP_{v4} handover signaling diagram for the reactive agent discovery approach.

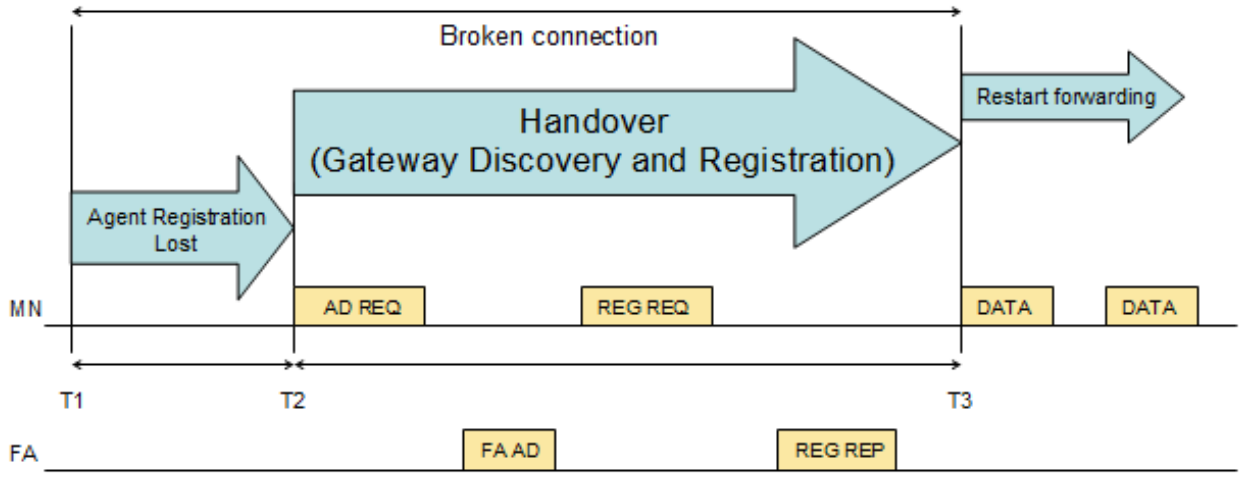

Figure 5.3 Reactive Handover Signaling Diagram

If a mobile node engaged in a communication with a correspondent node on the Internet looses contact with its actual gateway, may be caused for a broken link in an intermediate node, it will take some time before the MN realizes about this lost. In our scenario, the contact with the actual gateway is lost at time T_1. Then, the MN waits until time T_2 before initiating a new gateway discovery. The duration of the waited time ($T_2 - T_1$) depends on the holding time defined by each routing protocol to declare that a route is lost or that an agent registration has expired. On Table 2.2 are shown the holding times for some of the most popular MANET routing protocols. After realizing that the gateway route is lost, the handover is triggered at time T_2, moment in which the MN broadcasts an agent advertisement request (AD REQ). This request is propagated by other MANET nodes until one or more gateways are reached. In our scenario, one gateway answers the request by unicasting to the soliciting node an agent advertisement (FA AD). If agent advertisements from several gateways arrive to the MN, the MN chooses the one corresponding to the gateway with the smallest hop count. Next, the

mobile node sets a new CoA using an address prefix matching that of the chosen gateway. Next, the mobile node sends an agent registration request (REG REQ) to this gateway. The handover ends when the MN receives from this gateway a registration reply message (REG REP), which in our case occurs at time T_3.

We may see on Figure 5.3, that from the time the MN loses contact with the gateway at time T_1 until it begins again forwarding data packets at time T_3, any ongoing communication with correspondent nodes on the Internet will be interrupted, and any data packet sent between the MN and the CN may be lost. In a way different to the proactive discovery approach, with the reactive approach, the broken connection time is not equal to the handover time. With the reactive approach, the connection with the actual gateway is broken even before the handover is initiated. Additionally, the handover time with the reactive discovery approach is longer than with the proactive approach because in the later, there is no need to search for available gateways, since foreign agents periodically broadcast agent advertisements.

The handover signaling time diagrams when the version 6 of the Mobile IP protocol, MIP_{v6}, is used do not differ much from those corresponding to the MIP_{v4} version. One of the important differences is that in MIPv6 there is no data tunneling between the Home agent and the Foreign Agent (Access Router in the case of MIP_{v6}) when packets are exchanged between the MN and its CN. After the CN binding is updated, packets are exchanged directly between them.

Chapter 6 - Handover Modeling

Based on the handover signaling diagrams shown on Figure 5.2 and Figure 5.3, an analytical model is developed to evaluate the communication performance during a MANET handover. The MANET performance is evaluated by measuring the handover delay, the broken communication time, the handover failure probability, and the average communication interruption time. The handover delay was described on sections 5.1 and 5.2 for the proactive and for the reactive agent discovery approaches respectively, and even being the components of each approach different, the handover delay may be defined as the time a MN takes to change or recover an agent registration. The broken communication time measures the time an ongoing communication becomes interrupted when a handover occurs. For the proactive discovery approach, the handover time equals the broken communication time, but for the reactive approach, to the handover time we have to add the ad hoc protocol holding time. The handover failure probability measures the probability a handover may result in a loss of communication. Finally, the average communication interruption time measures the average time an ongoing communication becomes interrupted.

6.1 Handover Delay

As shown on Figures 5.2 and Figure 5.3, the handover delay is defined as the time taken by a MN to change its affiliation from one agent to another. This delay is not the same for the proactive and for the reactive discovery approaches. In the former, the handover time expands from the moment the mobile node sends a registration request to the chosen foreign agent until it receives the binding acknowledgment from it. On the other hand, with the reactive approach, the handover expands from the moment the MN broadcast an agent request to find a usable gateway until it receives the binding acknowledgment from the chosen foreign agent.

The handover delay time corresponding to each of the agent discovery approaches, to each MIP version, and to each ad hoc routing protocol type can be derived from the handover signaling diagrams shown on Figures 5.2, on Figure 5.3, and with the help of the parameter definitions shown on Table 6.1.

Handover Delay for the proactive discovery approach and MIP_{v4}, D_{pv4}

$$D_{pv4} = N_{h1}(T_{r3} + T_{pq3} + T_{r4} + T_{pq4} + 2T_{p1}) + N_{h2}(T_{r5} + T_{pq5} + T_{r6} + T_{pq6} + 2T_{p2}) \quad (5.1)$$

Handover Delay for the reactive discovery approach and MIP_{v4}, D_{rv4}

$$D_{rv4} = N_{h1}(T_{r1} + T_{pq1} + T_{r2} + T_{pq2} + 4T_{p1}) + N_{h1}(T_{r3} + T_{pq3} + T_{r4} + T_{pq4}) + N_{h2}(T_{r5} + T_{pq5} + T_{r6} + T_{pq6} + 2T_{p2}) \quad (5.2)$$

Handover Delay for the proactive discovery approach and MIP_{v6}, D_{pv4}

$$D_{pv6} = (N_{h1} + N_{h2})(T_{r5} + T_{pq5} + T_{r6} + T_{pq6}) + 2N_{h1}T_{p1} + 2N_{h2}T_{p2} \quad (5.3)$$

Handover Delay for the reactive discovery approach and MIP_{v6}, D_{pv4}

$$D_{rv6} = N_{h1}(T_{r1} + T_{pq1} + T_{r2} + T_{pq2}) + (N_{h1} + N_{h2})(T_{r5} + T_{pq5} + T_{r6} + T_{pq6}) + 4N_{h1}T_{p1} + 2N_{h2}T_{p2} \quad (5.4)$$

Table 6.1 Parameter Definitions

T_{p1}	Propagation Time / Hop (Wireless Hop)
T_{p2}	Propagation Time / Hop (Wired Hop)
T_{lr}	Link Recovery Time Reactive Protocols
T_{lp}	Link Recovery Time Proactive Protocols
N_{h1}	Number of wireless hops
N_{h2}	Number of wired hops

The numbers of wireless hops N_{h1} a packet have to go through when traveling form a mobile node to the gateway depends on the mobile node distribution. For this evaluation we are considering that the mobile nodes follow a two-dimensional uniform distribution. The number of wired hops N_{h2} a packet have to go through in this analysis is fixed to 1 assuming that the Home Agent and the Foreign Agent are directly connected. The wireless and wired propagation delay T_p depends on the hop distance between mobile nodes and agents, and between the Home agent and the Foreign Agent respectively. It means that to calculate the total propagation time we have to consider the number of wireless hops N_{h1}. The Link Recovery Time T_l refers to the ad hoc routing protocol holding time shown on Table 2.2. In Table 6.2 are shown the different time components associated with the handover signaling messages.

Table 6.2 Handover Time Components

Signaling Message	**Size (bytes)**	**Transmission Time / Hop**	**Proc. & Que. Time / Node**
Agent Solicitation	28	T_{r1}	T_{pq1}
Agent Advertisement	48	T_{r2}	T_{pq2}
Router Solicitation	48	T_{r3}	T_{pq3}
Router Advertisement	56	T_{r4}	T_{pq4}
Binding Update	74 (MIPv4) 112 (MIPv6)	T_{r5}	T_{pq5}
Binding Acknowledgement	48 (MIPv4) 96 (MIPv6)	T_{r6}	T_{pq6}
Link Error Reactive	20	T_{r7}	T_{pq7}
Link Error Proactive	8	T_{r8}	T_{pq8}

In particular, in this table are shown the signaling message sizes (in number of bytes), the transmission time identification T_r per hop corresponding to each different message, and the processing and queuing time identification T_{pq} corresponding to each different message. The transmission time T_r corresponds to only one hop. Since it is assumed a uniform node distribution, in order to compute the total transmission time for each message, we have to know the number of hops N_{h1} and N_{h2} the messages have to go through. Additionally, the signaling messages transmission delay component T_r depends on the transmitted packet length and the transmission speed. The different signaling packet lengths are defined on Table 6.2, and the transmission speed depends on the network technology used (WIFI, UMTS, GPRS, etc.).

Finally, the process and queuing time T_{pq} depends on the traffic and mobility pattern followed by mobile nodes. The traffic pattern of a mobile node is represented by the arrival process of a communication session to a mobile node and the session duration time. The T_{pq} shown on the table corresponds to just one node, so to compute the total processing and queuing time we have to consider the number of nodes N_{h1} and N_{h2} the messages have to go through. The process and queuing delay T_{pq} is a random variable that depends on the traffic load in the network and the queue length at each participating node. It's assumed the use of an M/M/1 queue model for the message transmission process and queuing at each mobile node [48]. This means that packets arrival to any mobile node follows a Poisson probability density function, but they are later forwarded following an exponential distribution. If λ_n and μ_n represents the average packet arrival rate and the average service rate at each node respectively, we may express the average process and queuing time as

$$T_{pq} = 1 / (\mu_n - \lambda_n) \tag{5.5}$$

We will consider for this evaluation that the mobility pattern of a mobile node is represented by the residence time that the mobile node spends in a MANET sub-network. We assume that the sub-network residence time T_R is a random variable with exponential distribution with mean 1/μ. That is, the average residence time T_R = 1/μ.

This analysis is not limited to the traffic and mobility patterns chosen. As long as the probability distribution functions of the session-arrival process, the session-duration time, and the subnet-residence time are given, this analysis can be applied to evaluate the impact of traffic and mobility over MANET handovers performance.

6.2 Broken Communication Time

It is possible that more important than the time a mobile node takes to handover is the broken communication time, which is the time a mobile node must wait to resume transmitting data packets after an ongoing communication becomes interrupted when a handover occurs. We must remember that for the proactive agent discovery approach, the broken communication time equals the handover time. It means that the broken communication time may be expressed as (5.1) and (5.3), which corresponds to D_{pv4} and to D_{pv6} respectively. On the other hand, for the reactive discovery approach, on top the handover time we have to add the ad hoc routing protocol holding time, so the broken communication T_b may be expressed as

$$T_{b\ v4} = D_{r\ v4} + T_{r\ e} \qquad \text{for MIP}_{v4} \tag{6.1}$$

$$T_{b\ v6} = D_{r\ v6} + T_{r\ e} \qquad \text{for MIP}_{v6} \tag{6.2}$$

where T_{re} represents the time taken by the running ad hoc routing protocol to recognize the loss of the actual agent route, and trigger a new route search (the holding time). T_{re} depends on the type of MANET protocol used. We have to recall that reactive routing protocols define the transmission of Hello packets between neighboring nodes participating in a valid route. Any intermediate node that is part of a valid route must inform to the originating node about any link failure. The time that a route failure message takes to arrive to the originating node varies according to the amount of hops there are between the reporting node and the originating node. In these scenarios we are setting the T_{re} value equal to half the hop count for the route between the mobile node and its gateway. That is $N_{h1}/2$. This represents the average T_{re} value if we use a uniform node link failure distribution. Thus we may express T_{re} for reactive ad hoc protocols as

$$T_{rer} = N_{h1}/2(T_{r7} + T_{pq7}) + N_{h1}T_{p1} + T_{lr} \tag{6.3}$$

With proactive routing protocols, any link error on any node MANET must be informed to every other node in the network in order to rebuild the routing tables. Intermediate nodes are responsible for propagating this information to farther away nodes. The time a link error message takes to arrive to any mobile node varies according to the amount of hops it takes. If we consider a uniform node link failure distribution, the average T_{re} value may be set as half the hop count for the route between the mobile node and its gateway. That is $N_{h1}/2$. Thus, we may express the broken route recognition time T_{re} for the proactive routing protocols as

$$T_{rep} = N_{h1}/2(T_{r8} + T_{pq8}) + N_{h1}T_{p1} + T_{lp} \tag{6.4}$$

6.3 Probability of Handover Failure

When an ongoing communication between a mobile node and a correspondent node on the Internet is interrupted during a handover, the service quality may be compromised. QoS criterion establishes that certain parameters, like the end to end delay, should not exceed a maximum given amount. We may define then that a handover fails if the broken communication time during a handover is longer that a certain predefined threshold value TH. By doing so, we may know how much the QoS is affected. We may evaluate the handover failure by computing the probability that an ongoing communication becomes interrupted for a time longer than the predefined threshold value TH. The probability of a handover failure may be expressed as

$$\mathbf{P}_{f\,\Gamma_{\alpha}\ i\overline{T}} \int_{T\ H}^{\infty} f_{T\ \&}(t)d \tag{6.5}$$

where $f_{Tb}(t)$ represents the broken communication distribution function. From (5.1) to (6.4) we were able to see that the formula representing the broken communication time T_b depends on some components, like the transmission time T_r, the propagation time T_p, and the MANET protocol holding time T_l, that are generally constant. These components also depend on other parameters that do not change over the time, like the wireless link speed, the wired speed, the average hop distance between the mobile node and the actual gateway, the wired hop distance between the Home Agent and the Foreign Gateway, and the signaling message lengths.

On the other hand, the processing and queuing time T_{pq}, which is determined by the traffic load and the queue lengths at each network node, may vary from time to time. Therefore, the service and the queuing times will be the random variables that we will use to calculate the broken communication time probability density function. Now, as we mentioned before, we assume an M/M/1 queuing system on every MANET node. That is, the packet arrival time (including both data packets and signaling messages) to a mobile node follows a Poisson distribution, and the service time of each packet follows an exponential distribution. Thus, the process and queuing time distribution function may be expressed as [49]

$$f_{Tpq}(t) = (\mu_n - \lambda_n)e^{-(\mu n - \lambda n)t} = \gamma e^{-\gamma t} \tag{6.6}$$

where λ_n and μ_n represents the average packet arrival and the average service rate at each node respectively, and where we are letting $(\mu_n - \lambda_n) = \gamma$. By so doing, the broken communication time T_b may then be written as the sum of two components. One component is constant and includes the parameters number of hops N_h, transmission time T_r, propagation time T_p, and holding time T_l. The other component is variable and depends on the process and queuing time T_{pq}. If we now exclude temporarily the constant components, we may express the broken communication distribution function $f_{Y1}(t)$ for the proactive agent discovery approach, according to (5.1) and (5.3) as

$$f_{Y1}(t) = (\gamma^2/(N_{h1} + N_{h2})^2)te^{-(\gamma/(Nh1 + Nh2))t} \tag{6.7}$$

Following the same procedure, the broken communication distribution function $f_{Y2}(t)$ for the reactive agent discovery approach, according to (5.2) and (5.4), may be expressed as

$$f_{Y2}(t) = (\gamma^2/(2N_{h1} + N_{h2})^2)te^{-(\gamma/(2Nh1 + Nh2))t} \tag{6.8}$$

If we call C_1, C_2, C_3, and C_4 the sum of the constant components of the handover delay for each case on (5.1) to (5.4), and we add them to $f_Y(t)$, we get the broken communication distribution function $f_{Tb}(t)$ for each agent discovery approach. For the proactive cases, we have to use the constant components C_1 and C_3, and then $f_{Tb}(t)$ may be expressed as

$$f_{Tb}(t) = (\gamma^2/(N_{h1} + N_{h2})^2)(t-C)e^{-(\gamma/(Nh1 + Nh2))(t-C)} \qquad \text{proactive cases} \tag{6.9}$$

where $C_1 = N_{h1}(T_{r3}+T_{r4}+2T_{p1}) + N_{h2}(T_{r5}+T_{r6}+2T_{p2})$ and $C_3 = (N_{h1}+N_{h2})(T_{r5}+T_{r6}) + 2N_{h1}T_{p1} + 2N_{h2}T_{p2}$

For the reactive cases, we have to use the constant components C_2 and C_4, and $f_{Tb}(t)$ may be expressed as

$$f_{Tb}(t) = (\gamma^2/(2N_{h1} + N_{h2})^2)(t-C)e^{-(\gamma/(2Nh1 + Nh2))(t-C)} \quad \text{reactive cases} \tag{6.10}$$

where $C_2 = N_{h1}(T_{r1}+T_{r2}+4T_{p1}) + N_{h1}(T_{r3}+T_{r4}+T_{pq4}) + N_{h2}(T_{r5}+T_{r6}+2T_{p2})$ and $C_4 = N_{h1}(T_{r1}+T_{r2}) + (N_{h1}+N_{h2})(T_{r5}+T_{r6}) + 4N_{h1}T_{p1} + 2N_{h2}T_{p2}$

6.4 Average Communication Interruption Time

In the previous section we evaluated the probability of a handover failure, that is, the probability that a handover exceeds a predetermined threshold time TH, which we declare is above the maximum required to maintain a certain QoS level. But the probability of a handover failure only tell us if a handover fails (causes a communication interruption). It tells us nothing about the chances a handover occurs. We will evaluate now the average communication interruption time. This metric tell us about how much time a mobile node maintain running communications broken as a consequence of handovers between different sub-networks. We have to recall that the occurrence of a handover depends mainly on node mobility, and in our simple model shown on Figure 5.1, a mobile node changes its affiliation form one gateway to another while it is engaged in a communication with a correspondent node on the Internet. To evaluate the average communication interruption time, we need to know about the possibilities that a handover occurs, and about how much time the ongoing communication remains interrupted when a handover occurs. By doing so, we may express the average communication interruption time as

$$T_{ci}^{avg} = P_{ci}T_b \tag{6.11}$$

where P_{ci} is the probability that a communication becomes interrupted, and T_b is the broken communication time as was described before in (5.1), (5.3), (6.1) and (6.2), for the proactive and for the reactive discovery approaches respectively. We have to recall that T_b is not the same for the proactive and for the reactive discovery approaches, and that T_b additionally will also depends on the running MIP version and on the running MANET routing protocol type.

6.4.1 Communication Interruption Probability - Proactive Approach

With the proactive agent discovery approach, gateways broadcast periodic agent advertisements, which permit nodes to be always aware if they move into a different sub-network, independently of the running MANET protocol, even if they are not currently engaged in communications with any correspondent node on the Internet. In this scenario nodes handover when they realize that they are closer to a different gateway.

To evaluate the average communication interruption time, we have to know when the mobile node remains in its actual network, and when the mobile node has roamed to a different one. The time that a mobile node remains in its actual network will be called the mobile node residence time. As expected, the residence time depends on node mobility, which will be characterized by a mobility

pattern. We will assume that the residence time T_R is a random variable that follows an exponential distribution function with mean 1/μ. Now, we need to evaluate the probability that there is an ongoing communication at the moment that a handover occurs. If a handover occurs, but at this moment there is not any ongoing communication, then there will not be any communication interrupted. Communication sessions in any node appear in a randomly fashion and sessions duration is also considered a random variable. As we may see on Figure 6.1, an ongoing communication will be interrupted if the session duration is longer than the remaining residence time. The remaining residence time is the time between the arriving of a session and the time a node leaves its actual network (handover). That is, there will be a communication interruption if at the moment of a handover occurrence there is still an ongoing communication running.

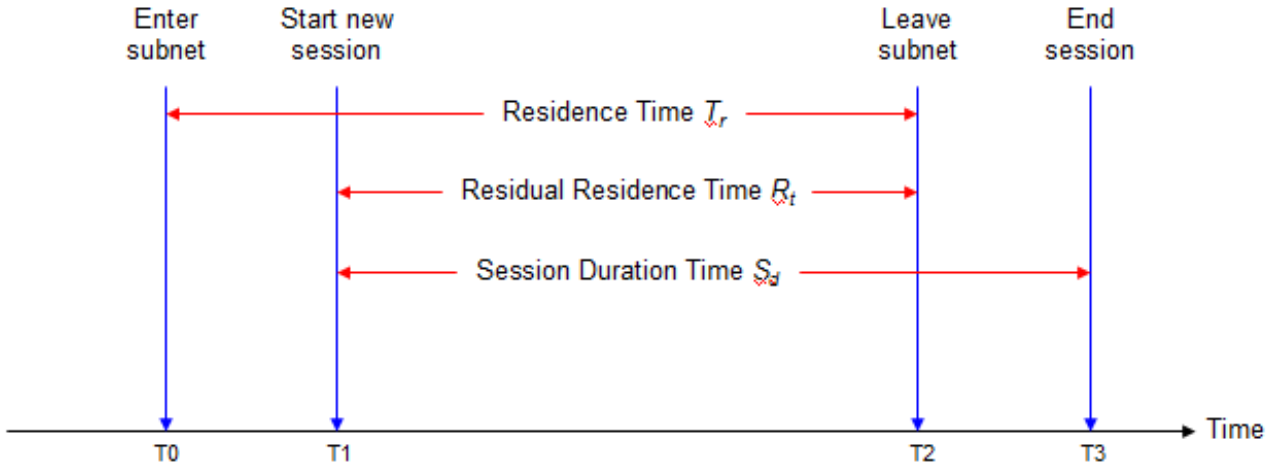

Figure 6.1 Communication Interruption Timing Diagram

As proposed in [50], we may say that the probability that a communication becomes interrupted as a consequence of a node handover depends not only on that there is a communication session during the remaining residence time, but that the session duration be longer than this remaining residence time. Combining these conditions, the probability of communication interruption P_{ci} may be expressed as follows:

$$P_c = P(S_d > R_t) P(\text{session arrival in } R_t) \quad (6.12)$$

where S_d represents the session duration time, and R_t represents the remaining residence time, which from now on we will call residual residence time. We may see on Figure 6.1 that the residual residence time R_t represents the time existing between a session arrival and the handover time. Now, we will assume that the session arrival process to a mobile node follows a Poisson distribution with average rate λ_u, that the session duration S_d follows a Gamma distribution with mean $1/\eta$ and variance V, and that, as stated before, the mobile node actual sub-network residence time follows an exponential distribution with mean $1/\mu$. Then, according to (6.12), the probability of a communication interruption P_{ci} can be expressed as [50]:

$$P_{ci} = \int\int f_{Sd}(y) f_{Rt}(t) dy dt \int \lambda_u t e^{-\lambda_u t} f_{Rt}(t) dt \quad (6.13)$$

where $f_{Sd}(y)$ represents the session duration probability distribution function, $fR_t(t)$ represents the distribution function for the residual residence time remaining between the session arrival and the handover time, and λ_u is the average session arrival time.

6.4.2 Communication Interruption Probability - Reactive Approach

If the reactive agent discovery approach is used, a mobile node which is engaged in communication with a correspondent node in the Internet only receive agent advertisements if they require them at the moment they loose registration with its actual gateway. If the mobile node registers to a different gateway, then a handover occurs. We have to recall that, even if the mobile node may be physically closer to a different gateway, it won't initiate a handover until it definitively looses registration with its actual gateway. Now, the analysis previously made for the proactive discovery approach also applies to the reactive approach. The probability of a handover occurrence for the reactive discovery approach also depends on node mobility, but since in this case, nodes may decide to handover even after they have already moved into neighboring sub-network controlled spaces, normally the average residence time is longer than the correspondent for the proactive approach. For this scenario, it also applies the same time diagram shown on Figure 6.1. The difference with the proactive discovery approach will be on the residence time. With the reactive discovery approach, mobile nodes will have a longer residence time, so they will have a longer mean value $1/\mu$. Hence, the probability of communication interruption for the reactive discovery approach may also be calculated using (6.12) and (6.13).

Chapter 7 - Perfomance Analysis

We will now use the handover modeling formulas found on chapter 6 to evaluate the broken communication time, the handover failure probability, and the average communication interruption time using the scenario shown on Figure 5.1. For this evaluation are considered the two types of discovery approaches: the proactive agent discovery approach and the reactive agent discovery approach. Also are considered in this evaluation the two different types of MANET routing protocols: the proactive ad hoc routing protocols and the reactive ad hoc routing protocols. Finally, in this evaluation are also considered the two versions of the Mobile IP protocol: MIP_{v4} and MIP_{v6}.

7.1 Broken Communication Time

7.1.1 Broken Communication Time as a function of packet arrival rate

As we defined before, the broken communication time measures the time an ongoing communication becomes interrupted as a consequence of a mobile node that handovers between two MANET sub-networks. The broken communication time is not the same for the proactive discovery approach than for the reactive discovery approach. As shown on Figure 5.3 for the reactive agent discovery approach, if we add to the handover time, the time that a mobile node has to wait to recognize that its agent registration is lost, we get the broken communication time T_b. On the other side, for the proactive discovery approach, the broken communication time is the same as the handover time, as we may see on Figure 5.2. We may use the handover expressions found in (5.1) and (5.3) to calculate T_b for the proactive discovery approach, and may use the expressions found in (6.1) and (6.2) to calculate T_b for the reactive discovery approach.

For the analysis of the broken communication time we consider two possible scenarios: one in which the packet arrival rate λ_n is left variable, and one in which the wireless link speed is left variable. That is, in one case we want to evaluate the broken communication time as the packet congestion increases, and in the other case we evaluate the broken communication time as the packet transmission rate increases. The rest of the components included in (5.1), (5.3), (6.1), and (6.2) are set as follows: the wireless MANET speed is set to 2 Mbps. The wired links speed is set to 10 Mbps. These speed values are used to calculate the packet transmission delay T_r. On each node, the average packet service time $1/\mu_n$ is set to 100 µs. The average one hop propagation delay T_{p2} over a wired link is set to 2.5 µs, and the average one hop propagation delay T_{p1} is set to 1 ms for the wireless links [T1]. The number of wireless hops and wired hops N_{h1} and N_{h2} were fixed to 10 and 1 respectively. We consider the utilization of two different MANET protocols, one proactive and one reactive. The proactive protocol used is OLSR, which has a link recovery time (holding time) T_{lp} = 6 ms. On the other hand, the

reactive protocol implemented is AODV, which has a link recovery time T_{l2} = 2 ms. The results found for this evaluation are shown on Figure 7.1.

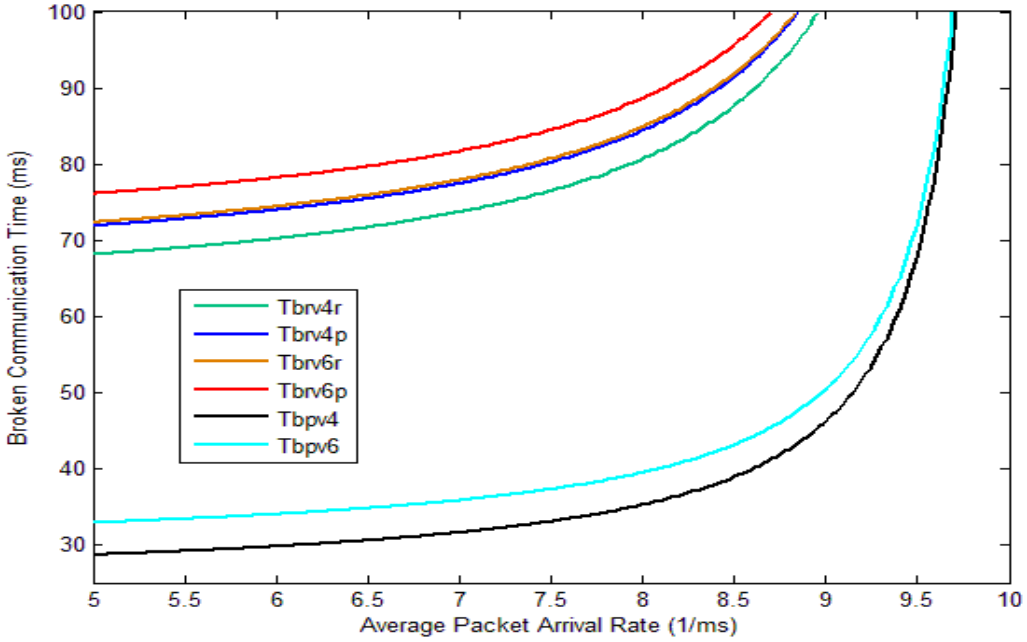

Figure 7.1 Broken Communication Time as a function of packet arrival rate

In this figure, the broken communication times T_{bpv4}, T_{bpv6}, T_{brv4p}, T_{brv6p}, T_{brv4r}, and T_{brv6r} are plotted as a function of the average packet arrival rate λ_n. T_{bpv4} and T_{bpv6} are the broken communication times for the proactive discovery approach for MIP_{v4} and MIP_{v6} respectively. T_{brv4p} and T_{brv6p} are the broken communication times for the reactive discovery approach when it is running OLSR for MIP_{v4} and MIP_{v6} respectively. T_{brv4rp} and T_{brv6} are the broken communication times for the reactive discovery approach when it is running AODV for MIP_{v4} and MIP_{v6} respectively. Note that the routing protocol used does not make any difference on the broken communication time when the proactive discovery approach is used, and for that reason we do not show differentiate results for them. This is so because with the proactive discovery approach the mobile node handovers when it finds a better gateway, and not when it looses a gateway route.

For this evaluation, the average packet arrival rate λ_n is made to vary from 5000 to 10.000 packets/seg. As it can be seen on the figure, the broken communication time for all cases grow slowly as the average packet arrival rate approaches the mobile nodes service rate μ_n, which in this case is 10.000 packets/seg. When the packet arrival time approaches this value, the broken communication grows exponentially. On the other hand, we may also see that for packet arrival rate values lower than about 8.000 packets/seg, the broken communication time does not change much. We may conclude from these the results that as long as the packet arrival rate does not approach the node service rate, the broken communication time will maintain a constant value near the minimum possible.

We may also see that the broken communication time values expand from near 30 ms to around 80 ms considering all cases. These values may not be disrupting for regular voice communication, but echo suppressors may be required. As expected, the broken communication time is superior for all the reactive discovery approach cases, because the mobile node does not begin the handover process until it finally realizes that have loosen contact with its actual gateway. For low congested networks, the

broken communication time value for the reactive discovery approach cases is about 40 ms bigger than for the proactive ones. For the reactive cases, the broken communication time goes around 70 ms. On the other hand, it goes around 30 ms for the proactive cases. Finally, it may be seen that there are not big differences between the MIP_{v4} and MIP_{v6} scenarios and when the different routing protocols are used. As a matter of fact, T_b is about 4 ms bigger when MIP_{v6} is used than when MIP_{v4} is implemented, and another 4 ms bigger when OLSR is used instead of AODV. This behavior occurs because signaling packets for MIP_{v6} are longer than those for MIP_{v4}, and the link recovery time in AODV is about 4 ms bigger than in OLSR.

7.1.2 Broken Communication Time as a function of the wireless speed

On Figure 7.2, the broken communication times T_{bpv4}, T_{bpv6}, T_{brv4p}, T_{brv6p}, T_{brv4r}, and T_{brv6r} are plotted as a function of the MANET wireless speed. For this evaluation the average packet arrival rate λ_n is set to 5000 packets/seg, while the mobile nodes service rate μ_n is maintained at 10.000 packets/seg.

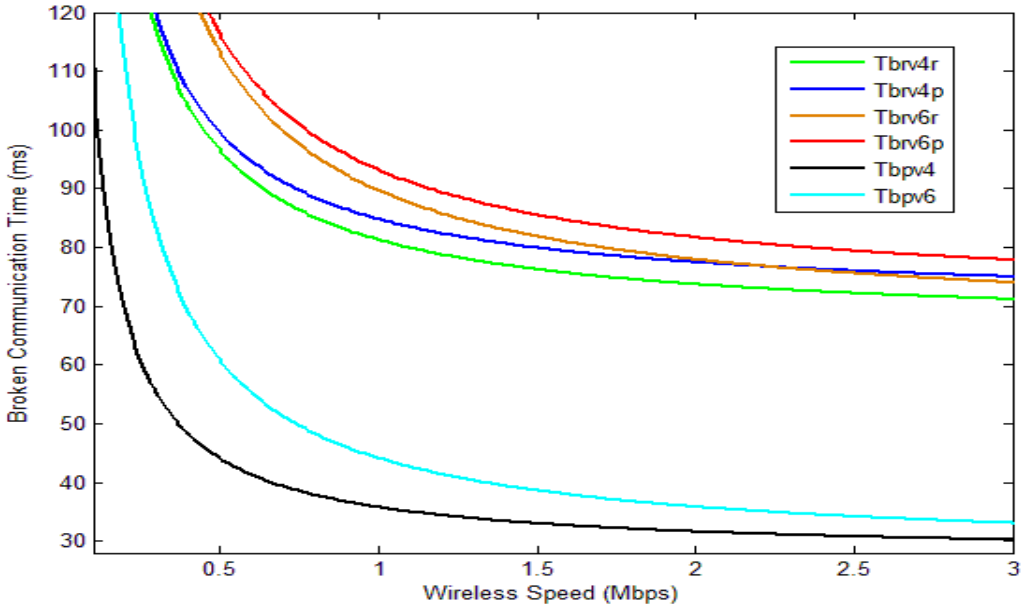

Figure 7.2 Broken Communication Time as a function of wireless speed

It may be seen that for all cases, the broken communication time grows exponentially when the MANET wireless speed descends from 1 Mpbs. This result is not unexpected. If mobile nodes take longer to transmit their data packets, the chances that a handover occurs during a packet transmission grows. On the other hand, for wireless speeds above 1 Mbps, the broken communication time decrease slowly with the increasing wireless speed. For a wireless speed of near 3 Mbps, the broken communication time expands from about 30 ms to around 70 ms. As with the scenario where the average packet arrival rate was made variable, there is a difference of about 40 ms between the reactive and the proactive agent discovery approaches for speeds superior to 1 Mbps, resulting the proactive approach with a lower broken communication time. At 3 Mbps, the proactive approaches have a T_b around 30 ms, while the reactive approaches have a T_b around 70 ms. Also, it may be seen that there are not big differences on the results between the MIP_{v4} and the MIP_{v6} scenarios, neither when there are used the different types of routing protocols. In particular, the broken communication

time is about 3 ms bigger when MIP_{v6} is used than when MIP_{v4} is implemented, and about 4 ms bigger when OLSR is used instead of AODV. As mentioned before, this is so, because signaling packets for MIP_{v6} are longer than for MIP_{v4}, and because the link recovery time in AODV protocol is about 4 ms bigger than in OLSR.

7.1.3 Broken Communication Time as a function of the number of wireless hops

On the other hand, on Figure 7.3, the broken communication times T_{bpv4}, T_{bpv6}, T_{brv4p}, T_{brv6p}, T_{brv4r}, and T_{brv6r} are plotted as a function of the number of wireless hops. For this scenario the average packet arrival rate λ_n is set to 5000 packets/seg while the mobile nodes service rate μ_n is maintained at 10.000 packets/seg, and the wireless speed is set to 2 Mbps. It may be seen that in all cases, the broken communication time grows linearly when the number of wireless hops increase from 0 to 30 hops. This result is not unexpected. More wireless hops mean that every transmitted packet will have to suffer the transmission and propagation delays of more links. It grows linearly because we are using a bi-dimensional uniform node distribution. In this case there is a growing difference between the reactive and the proactive discovery scenarios. The broken communication time grows about 4 ms/hop faster for the reactive approach than for the proactive approach. For 30 hops, the reactive approach reaches a broken communication time of almost 200 ms, making it useless for voice communication. For the same number of wireless hops, the proactive approach reaches a broken communication time of about 70 ms. Also here, it may be seen that there are not big differences between the MIP_{v4} and MIP_{v6} scenarios, and neither when we use the different types of routing protocols. However, the performance is better (lower T_b) when MIP_{v4}, and when AODV are used.

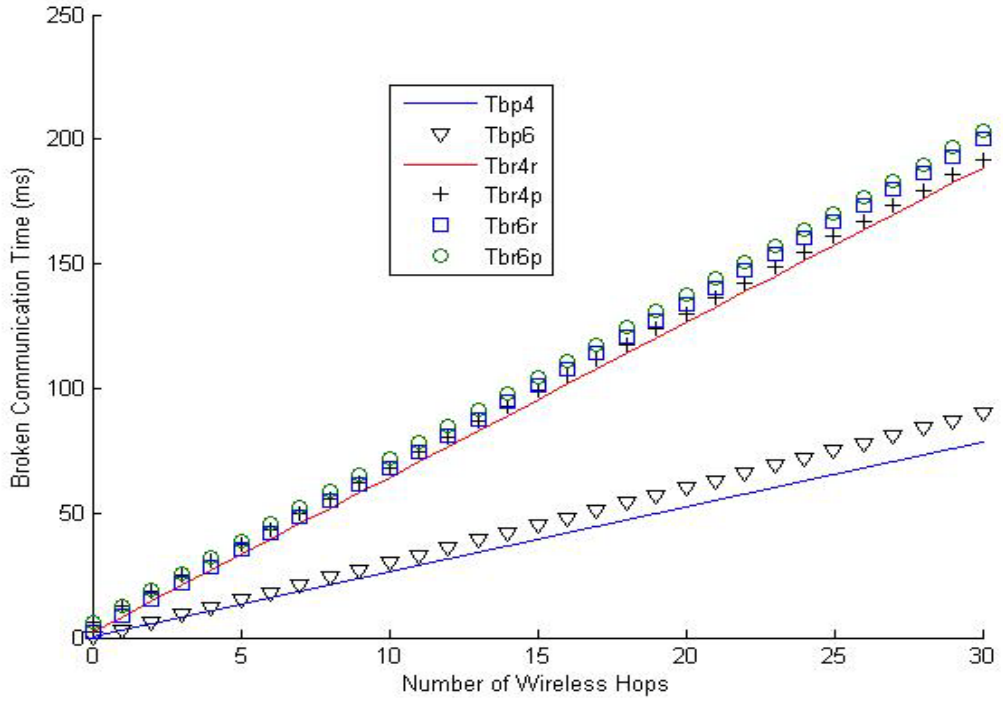

Figure 7.3 Broken Communication Time as a function of the number of wireless hops

7.1.4 Broken Communication Time as a function of the prosess and queuing time

On Figure 7.4, the broken communication times T_{bpv4}, T_{bpv6}, T_{brv4p}, T_{brv6p}, T_{brv4r}, and T_{brv6r} are plotted as a function of the processing and queuing time. For this scenario the average packet arrival rate λ_n is set to 5000 packets/seg. It may be seen that also here, in all cases, the broken communication time grows linearly with the increase on the processing and queuing time. This result is not unexpected. More processing and queuing time on each hop will increase the broken communication time. The behavior is similar to when the number of hops is increased. As before, there is a difference between the results found for the reactive discovery approach and the proactive discovery approach. The broken communication time grows about 20 ms faster for each millisecond of processing and queuing time for the reactive discovery approach than for the proactive approach. We may see that for a processing and queuing time of 10 ms, the reactive approach reaches a broken communication time of about 280 ms, making it useless for voice communication, but for the same processing and queuing time, the proactive approach reaches a broken communication time of about 140 ms. As before, it may be seen that there are not big differences between the results corresponding to the MIP_{v4} and the MIP_{v6} scenarios and when the different types of routing protocols are used. However, the performance is better (lower T_b) when the MIP_{v4} version, and when the AODV protocol are used.

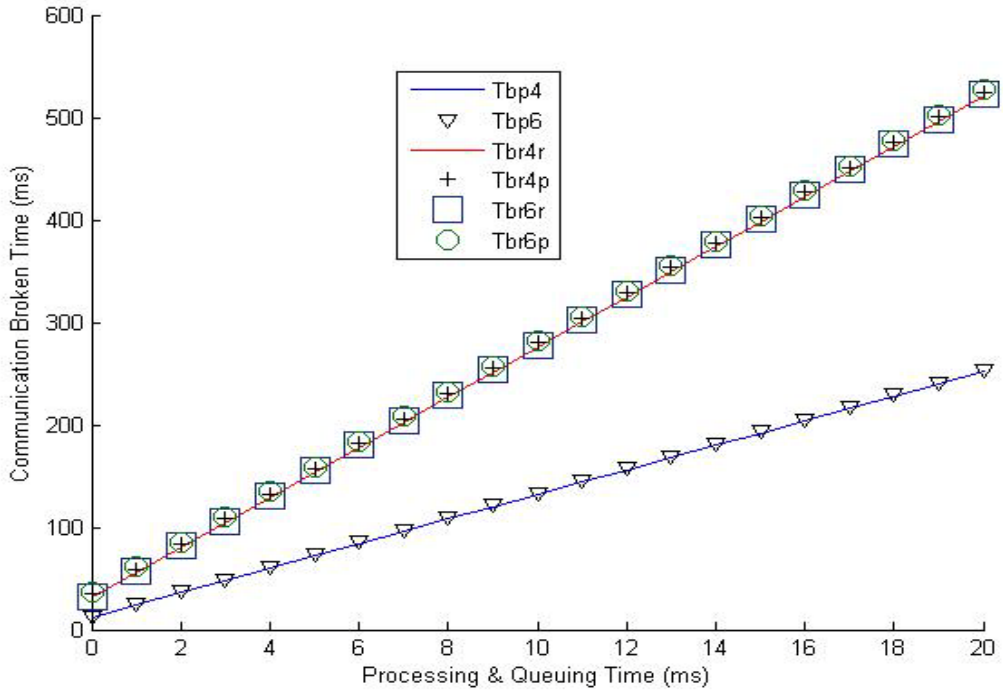

Figure 7.4 Broken Communication Time as a function of the processing & queuing time

7.2 Handover Failure Probability

7.2.1 Handover Failure Probability as a function of the number of hops

We have defined before that a handover fails if, as a consequence of the handover, an ongoing communication is interrupted for a time above a predefined threshold. On (6.5) we presented an expression that permit us to calculate the handover failure probability if we know the broken communication distribution function. For this evaluation we have set the average packet arrival rate λ_n to 5000 packets/seg and the average service time to 100 µs in every node. The wired number of hops is set to 1. The MANET wireless speed is set to 2 Mbps. The wired speed for the link that joins the Home Agent and the Foreign Agent is set to 10 Mbps. The average one hop propagation delay is set to 2.5 µs for the wired link and is set to 1 ms for the wireless links. For this evaluation, we want to know about the handover failure probability if we define a communication interruption threshold of 200 ms, which corresponds to the end to end delay accepted limit for voice communication. On Figure 7.5, the handover failure probability T_{pv4}, T_{pv6}, T_{rv4p}, T_{rv6p}, T_{rv4r}, and T_{rv6r} are plotted as a function of the number of wireless hops N_{h1}. T_{pv4} and T_{pv6} are the handover failure probabilities for the proactive agent discovery approach for the MIP_{v4} and for the MIP_{v6} scenarios. T_{rv4p} and T_{rv6p} are the handover failure probabilities for the reactive agent discovery approach when OLSR is used for the MIP_{v4} and for the MIP_{v6} scenarios. Finally, T_{rv4r} and T_{rv6} are the handover failure probabilities for the reactive agent discovery approach when AODV is used for the MIP_{v4} and for the MIP_{v6} scenarios.

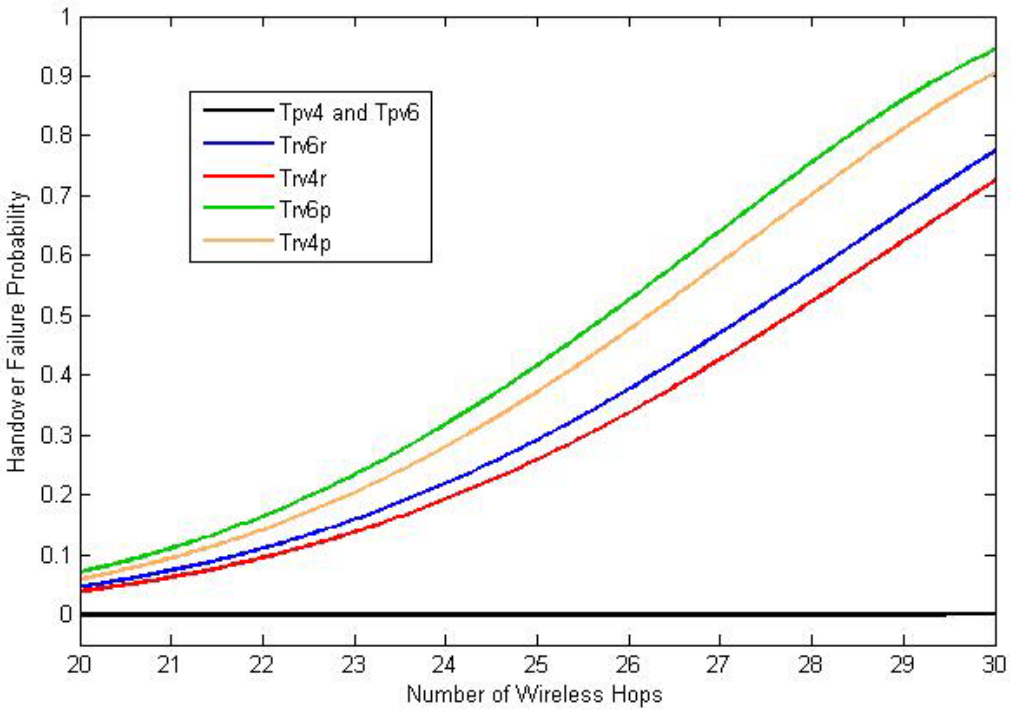

Figure 7.5 Handover Failure Probability as a function of the number of hops

Notice in the figure that there in not difference between the proactive discovery approach cases T_{pv4} and T_{pv6}. The reason is that for the range of number of hops N_{h1} chosen (20 to 30), the communication interruption time for the proactive discovery approach is well below the chosen threshold value (200 ms) to declare a failed communication, as it may be seen on Figure 7.2. The broken communication time for the proactive discovery approach cases for 30 wireless hops is about

70 ms.

It is clear that the handover fail probability must grow with the increase on the number of wireless hops, and this is the behavior we see with the reactive discovery cases for N_{h1} values between 20 and 30. In this range, the fail probability grows from near 5% to around 80%. For values of N_{h1} below to 20, the handover fail probability tends to zero. This is so because for less than 20 hops, also the broken communication time for the reactive discovery approach is well below 200 ms. Finally, we can see that, as before, there is not very much difference between the utilization of MIP_{v4} and MIP_{v6}. On the other hand, there is a small difference on the handover failure probability when we change the type of routing protocol. With the use of AODV we may see a handover fail probability of about 20% lower than with the use of OLSR. More precisely, for 30 wireless hops, the handover failure probability is about 90% per the reactive routing protocol and about 75% for the proactive protocol.

7.2.2 Handover Failure Probability as a function of the average packet arrival rate

On Figure 7.6, the handover failure probability T_{pv4}, T_{pv6}, T_{rv4p}, T_{rv6p}, T_{rv4r}, and T_{rv6r} are plotted as a function of the average packet arrival rate. T_{pv4} and T_{pv6} are the handover failure probabilities for the proactive agent discovery approach for the MIP_{v4} and for the MIP_{v6} scenarios. T_{rv4p} and T_{rv6p} are the handover failure probabilities for the reactive agent discovery approach when OLSR is used for the MIP_{v4} and for the MIP_{v6} scenarios. Finally, T_{rv4r} and T_{rv6} are the handover failure probabilities for the reactive agent discovery approach when AODV is used for the MIP_{v4} and for the MIP_{v6} scenarios.

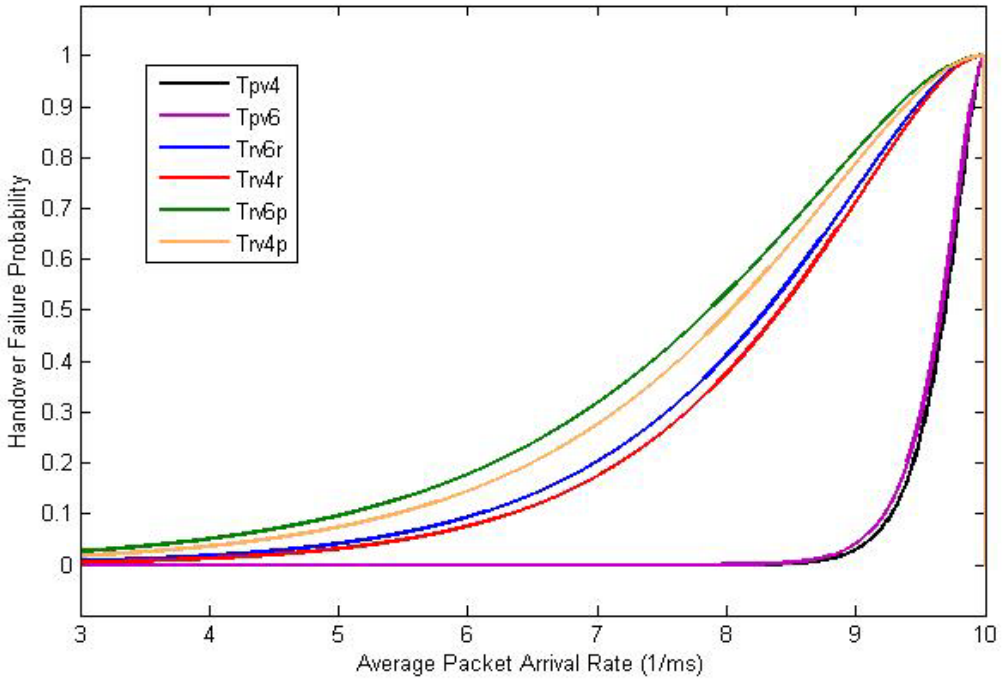

Figure 7.6 Handover Failure Probability as a function of the packet arrival rate

Also here, the handover fail probability must grows with the increase on the average packet arrival rate, and this is the behavior we see with the reactive discovery cases for average packet arrival rates values between 4 and 10 packets/ms. In this range, the fail probability grows from near 2% to around 100%. This behavior is normal. As more packets attend to be served, the probability of a

broken communication increase, and also the probability of a handover failure. On the other hand, for the proactive discovery approach, the failure probability remains low until the packet arrival rate approaches 10 packets/ms, which is the packet service rate on every mobile node. Notice in the figure that there in almost no difference between the proactive discovery approach cases T_{pv4} and T_{pv6}. The reason is that the communication interruption time for the proactive discovery approach is low in comparison with the chosen threshold value (200 ms) to declare a failed communication, as it may be seen on Figure 7.2. For average packet arrival rate values bellow 9 packets/ms, the failure probability is near zero for the two proactive discovery approach cases.

Finally, we can see that, as before, there is not very much difference between the utilization of MIP_{v4} and MIP_{v6}. On the other hand, there is a bigger difference on the handover failure probability when we change the type of routing protocol. With the use of AODV we may see a handover fail probability lightly lower than with the use of OLSR. More precisely, for an average packet arrival rate of 7 packets/ms, the handover failure probability is about 10% lower for the reactive routing protocol than for the proactive protocol.

7.2.3 Handover Failure Probability as a function of the wireless speed

On Figure 7.7, the handover failure probability T_{pv4}, T_{pv6}, T_{rv4p}, T_{rv6p}, T_{rv4r}, and T_{rv6r} are plotted as a function of the wireless speed. T_{pv4} and T_{pv6} are the handover failure probabilities for the proactive agent discovery approach for the MIP_{v4} and for the MIP_{v6} scenarios. T_{rv4p} and T_{rv6p} are the handover failure probabilities for the reactive agent discovery approach when OLSR is used for the MIP_{v4} and for the MIP_{v6} scenarios. Finally, T_{rv4r} and T_{rv6} are the handover failure probabilities for the reactive agent discovery approach when AODV is used for the MIP_{v4} and for the MIP_{v6} scenarios.

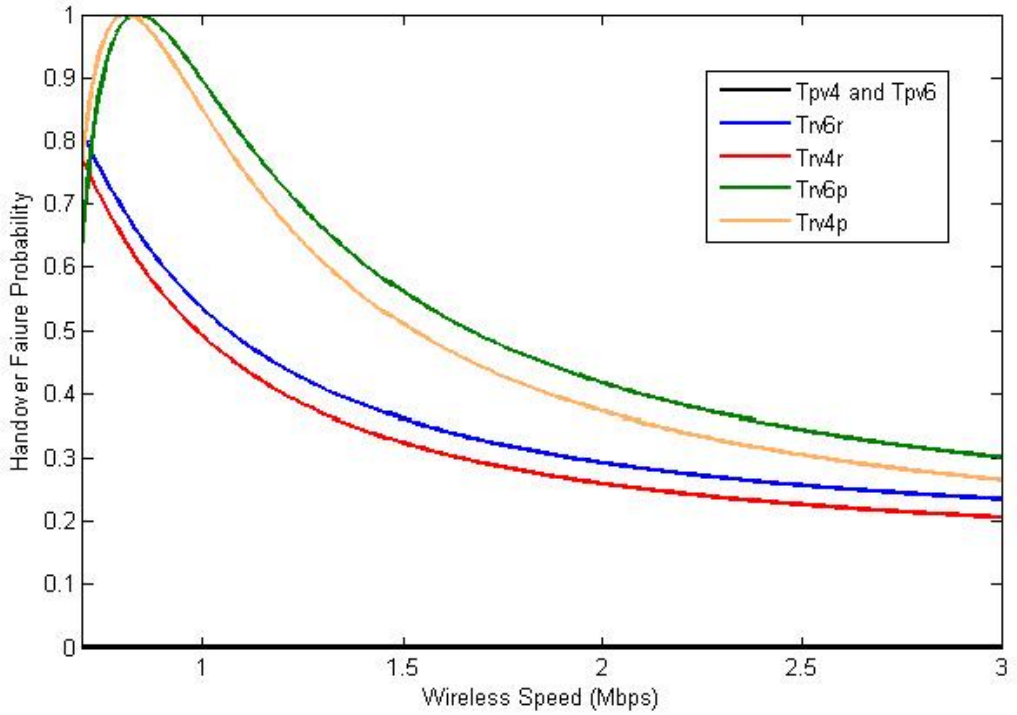

Figure 7.7 Handover Failure Probability as a function of the wireless speed

In this case the handover fail probability descends with the increase on the wireless speed, and

this is the behavior we see for the reactive discovery cases for wireless speed values between 0.5 and 3 Mbps. In this range, the fail probability descends from near 100% to around 30%. With the increase on the wireless speed, the probability of a broken communication decreases, and also the probability of a handover failure. On the other hand, for the proactive discovery approach cases, the failure probability is always zero for the chosen threshold level. Neither here there is any difference between the proactive discovery approach cases T_{pv4} and T_{pv6}. The reason is that the communication interruption time for the proactive discovery approach is very low in comparison with the chosen threshold value (200 ms) to declare a failed communication for the chosen speed range, as it may be seen on Figure 7.2.

Finally, we can see that, as before, there is not very much difference between the utilization of MIP_{v4} and MIP_{v6}. On the other hand, there is a bigger difference on the handover failure probability when we change the type of routing protocol. With the use of AODV we may see a handover fail probability lightly lower than with the use of OLSR. More precisely, for a wireless speed of 1 Mbps, the handover failure probability is about 40% lower for the reactive routing protocol than for the proactive protocol.

7.2.4 Handover Failure Probability as a function of the threshold

On Figure 7.8, the handover failure probability T_{pv4}, T_{pv6}, T_{rv4p}, T_{rv6p}, T_{rv4r}, and T_{rv6r} are plotted as a function of the threshold level. T_{pv4} and T_{pv6} are the handover failure probabilities for the proactive agent discovery approach for the MIP_{v4} and for the MIP_{v6} scenarios. T_{rv4p} and T_{rv6p} are the handover failure probabilities for the reactive agent discovery approach when OLSR is used for the MIP_{v4} and for the MIP_{v6} scenarios. Finally, T_{rv4r} and T_{rv6} are the handover failure probabilities for the reactive agent discovery approach when AODV is used for the MIP_{v4} and for the MIP_{v6} scenarios.

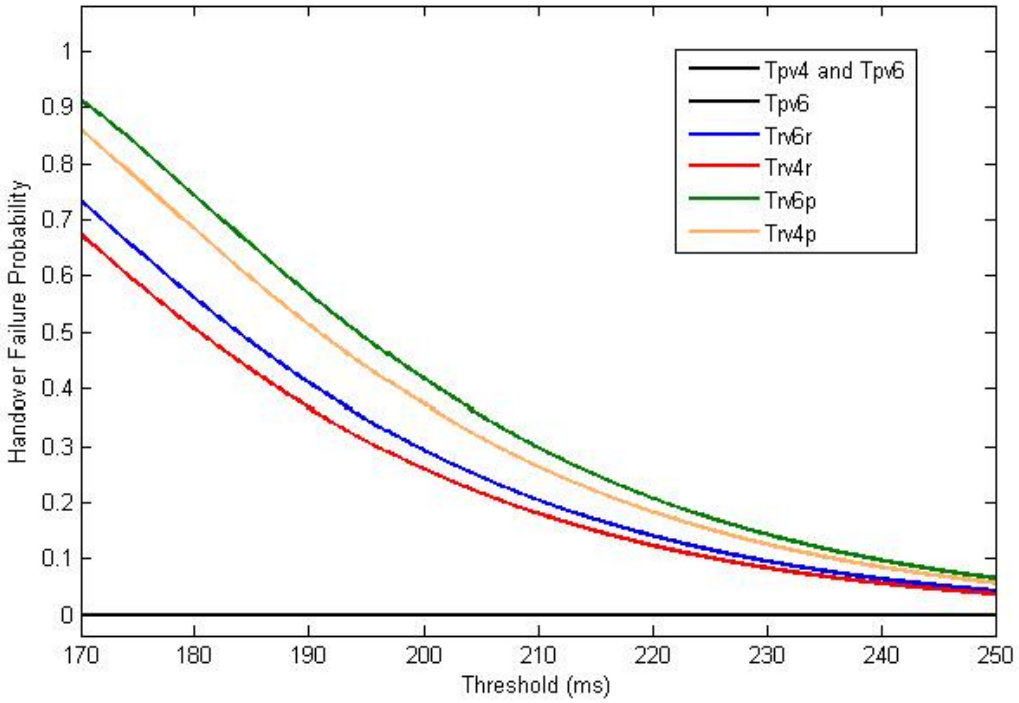

Figure 7.8 Handover Failure Probability as a function of the threshold

Also in this case the handover fail probability descends with the increase on the threshold level, and this is the behavior we see for the reactive discovery cases for threshold level values between170 and 250 ms. For this range, the fail probability descends from around 80% to near 5%. With the increase on the threshold level, the probability of a broken communication decreases, and also the probability of a handover failure. On the other hand, for the proactive discovery approach cases, the failure probability is always zero for the chosen threshold range. Neither here there is any difference between the proactive discovery approach cases T_{pv4} and T_{pv6}. The reason is that the communication interruption time for the proactive discovery approaches is noticeably lower in comparison with the reactive discovery approaches to declare a failed communication for the chosen parameters, as it may be seen on Figure 7.2.

Finally, we can see that, as before, there is not very much difference between the utilization of MIP_{v4} and MIP_{v6}. On the other hand, there is a bigger difference on the handover failure probability when we change the type of routing protocol. With the use of AODV we may see a handover fail probability lightly lower than with the use of OLSR. More precisely, for threshold level of 170 ms, the handover failure probability is about 20% lower for the reactive routing protocol than for the proactive protocol.

7.3 Average Communication Interruption Time

7.3.1 Average Communication Interruption Time as a Function of the Session Arrival Rate

Until now, we have evaluated the consequences of a handover occurrence when there is an ongoing communication between a mobile node and a correspondent node on the Internet. That is, the broken communication time and the handover failure probability. Now, we will evaluate the chances that a communication becomes interrupted as a consequence of a handover occurrence. More specifically, we will evaluate the average communication interruption time, which we will calculate using the expressions shown on (6.11) to (6.13). In these expressions we may see that the average communication interruption time depends on the broken communication time, on the session arrival rate, on the session duration time, and on the mobile node residence time. For this evaluation, we will set the average session duration time to 4 minutes, the average residence time to 2 minutes, and the broken communication time may be read for all cases from the Figure 7.2, when the wireless network speed is set to 3 Mbps. That is, T_{bpv4} = 30 ms, T_{bpv6} = 33 ms, T_{brv4p} = 76 ms, T_{brv6p} = 78 ms, T_{brv4r} = 71 ms, and T_{brv6r} = 74 ms.

On Figure 7.9, the average communication interruption times P_{v4}, P_{v6} , R_{v4r}, R_{v6r}, R_{v4p} and R_{v6p} are shown as a function of the average session arrival rate, which is made to expand from 0 to 5 session per minute. P_{v4} and P_{v6} represents the average communication interruption times for the proactive agent discovery approach when MIP_{v4} and MIP_{v6} are used respectively. R_{v4r} and R_{v6r} represents the average communication interruption times for the reactive agent discovery approach while AODV is running when MIP_{v4} and MIP_{v6} are used respectively. Finally, R_{v4p} and R_{v6p} represents the average communication interruption times for the reactive discovery while OLSR is running when MIP_{v4} and MIP_{v6} are used respectively.

On this figure we may see that for all cases, the average communication interruption time, after

growing from zero to a maximum value, at an average session arrival rate of about 0.5 sessions per minute, decreases again gradually as the average session arrival rate increases. It is logical to expect that with the increase on the session arrival rate, it should be a correspondent increase on the average communication interruption time, but this does not occur for values of average session rate above around 0.5 sessions per minute. To understand this behavior, lets image that the mobile node is not moving. In this scenario, if more sessions arrive, it does not mean that more sessions will be broken, because there will not be any handover with a stationary node. On the contrary, the average communication interruption will decrease as a consequence that there will be more sessions with less probability of being interrupted. In our case, if more and more sessions arrive, keeping the same node mobility, means that the percentage of broken communication will decrease.

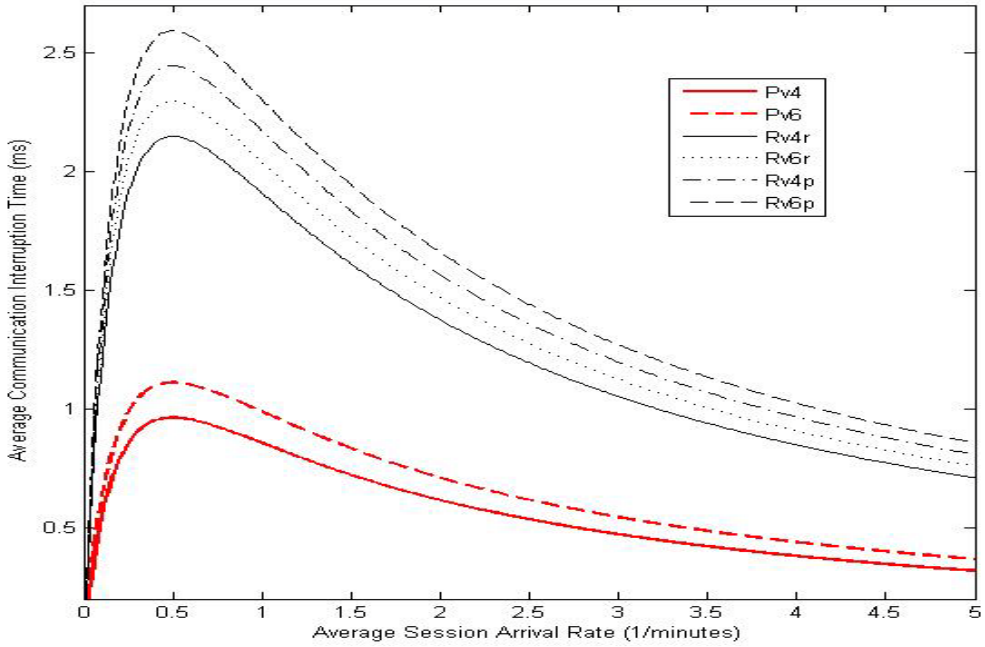

Figure 7.9 Average Communication Interruption Time as a Function of the Session Arrival Rate

One important observation that we can make about the Figure 7.9, is that the proactive agent discovery cases (P_{v4} and P_{v6}) have a lower average communication interruption times than the reactive agent discovery cases (R_{v4r}, R_{v6r}, R_{v4p} and R_{v6p}). The average communication interruption time for the proactive discover approach scenario reaches a maximum of around 1 ms, while for the reactive discovery approach scenario, the average communication interruption time reaches a maximum between 2 and 2.5 ms. As before, this is so, because the proactive agent discovery approach has a lower broken communication time than the reactive discovery approach. Finally, we may observe that there is not a great difference between the results corresponding to the MIP_{v4} and MIP_{v6} scenarios, and when the routing protocol is exchanged between AODV and OLSR. However, the best performances (lower average communication interruption time) are obtained when AODV and MIP_{v4} are used.

A different behavior of the broken communication interruption time is shown on Figure 7.10. In this case, the average session arrival time is let variable. The average communication interruption time

is evaluated for three different broken communication times, independently of the agent discovery approach used, the MIP version implemented, and the running MANET protocol.

For this evaluation, the session arrival time is made to vary from 0 to 5 sessions per minute for three broken communication time values: 20 ms, 50 ms, and 100 ms respectively. It may be noticed on Figure 7.10 the same average communication interruption time behavior found on Figure 7.9. The curves first grow fast from zero until reaching a maximum value, after which the average interruption time begins to descend slowly until reaching a low near constant value. We may notice however, that for low T_b values (20 ms in our case), there is almost not growing, reaching only a maximum value near the same that later will keep for bigger session arrival times. Thus, if the broken communication time is low, it does not matter much if the probability of a handover is high or low, the average communication interruption time will be fairly constant. We may say from the figure that if T_b is less than 50 ms, the average communication interruption time will be bellow 4 ms. Finally, we may notice that for any value of $T_{b,}$ the maximum average interruption time values occurs for an average session arrival of about 0.5 sessions per minute.

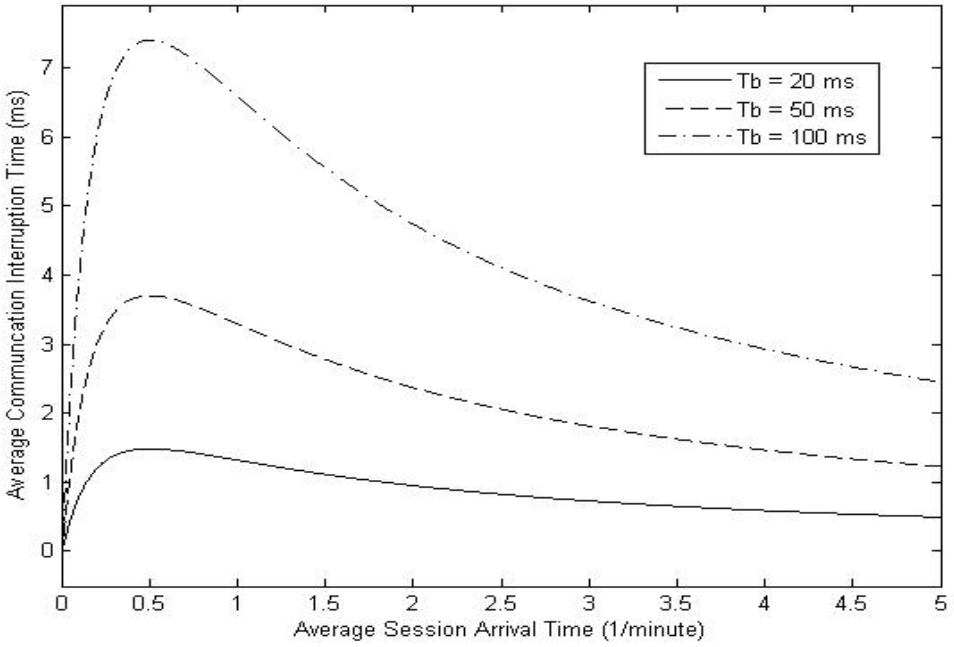

Figure 7.10 Average Communication Interruption Time as a Function of the Session Arrival Rate and the Broken Communication Time

7.3.2 Average Communication Interruption Time as a Function of the Session Duration Time

Another behavior of the broken communication interruption time is shown on Figure 7.11. In this figure are shown the average communication interruption times P_{v4}, P_{v6} , R_{v4r}, R_{v6r}, R_{v4p} and R_{v6p} as a function of the average session duration, which is made to expand from 0.1 to 100 minutes. For this evaluation, we will set the average residence time to 2 minutes, the average session arrival rate to 1 min^{-1}, and the wireless network speed to 3 Mbps. On this figure we may see that for all cases, the average communication interruption time grows slowly from near zero to around 1 ms (for the

proactive discovery approach), and to around 3 ms (for the reactive discovery approach) when the average session duration grows from 1 to 10 minutes. For session duration values longer than about 10 minutes, the average communication interruption time tends to remain constant. It is clear that as the session duration grows, there will be more chance that ongoing communications become interrupted, but as the session duration approaches the average node residence time, almost all sessions will be interrupted, and even longer session durations will not increase the average communication interruption time any more. Of course, very low session durations (bellow 1 minute) will result with a very low average communication interruption time.

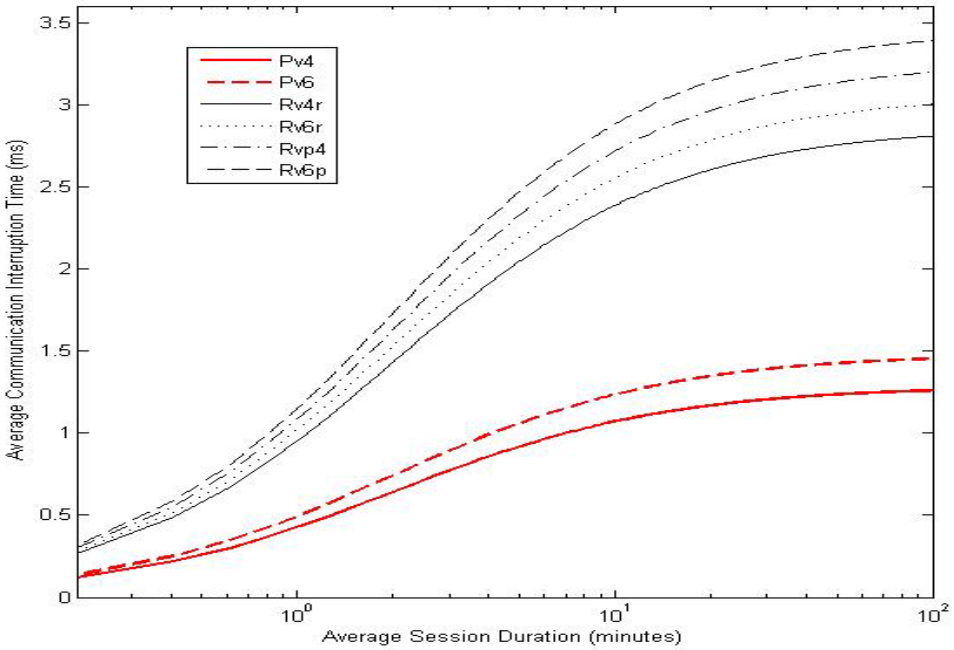

Figure 7.11. Average Communication Interruption Time as a Function of the Session Duration Time

We may also see on Figure 7.11 that the proactive discovery scenarios (P_{v4} and P_{v6}) have a lower average communication interruption times than the reactive discovery scenarios (R_{v4r}, R_{v6r}, R_{v4p} and R_{v6p}). The average communication interruption time for the proactive discover approach reaches a maximum value of around 1 ms, while for the reactive approach, it reaches a maximum above 3 ms. As before, this is so because the proactive agent discovery approach has a lower broken communication time than the reactive one. Finally, we may see that there is not a great difference between the scenarios where MIP_{v4} and MIP_{v6} are implemented and between the scenarios where AODV and OLSR are running. However, we may see that the best performances are obtained when AODV and MIP_{v4} are used.

As a variation of the evaluation shown before, on Figure 7.12 different communication interruption times are considered. In this case, the average session duration time is again let as a variable, independently of the agent discovery approach, the MIP version, and the running MANET protocol used. The average session duration time is made to change from 0.1 to 100 minutes, and we use three different broken communication time values: 20 ms, 50 ms, and 100 ms. It may be noticed on Figure 7.12 the same behavior found on Figure 7.8 for the average communication interruption time. We may see that it grows from a low value when the session duration is low (around 0.1 minute),

to a value that depends on the broken communication time when the session duration is high (around 100 minutes). When the session duration is low, the average communication interruption time does not change much with T_b (less than 1 ms), but when the session duration is about 100 minutes, then the average communication interruption time becomes about 2 ms for a T_b of 20 ms and near 10 ms for a T_b of 100 ms. When T_b is low, the average interruption time almost does not grow because low duration sessions have low probability of interruption.

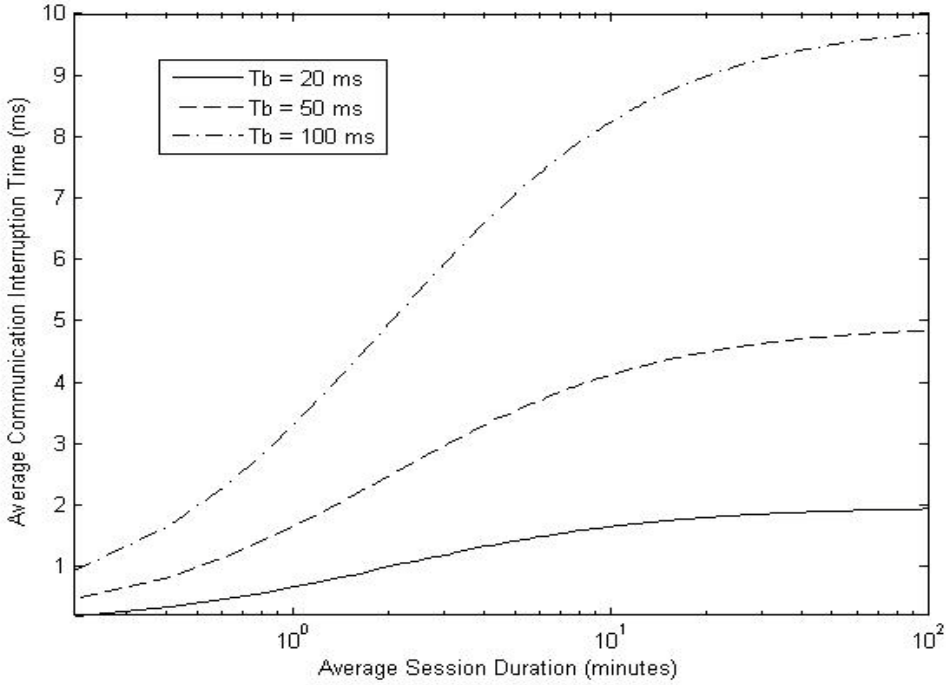

Figure 7.12 Average Communication Interruption Time as a Function of the Average Session Duration and the Broken Communication Time

7.3.3 Average Communication Interruption Time as a Function of the Session Average Residence Time

On Figure 7.13 are shown the average communication interruption times P_{v4}, P_{v6}, R_{v4r}, R_{v6r}, R_{v4p} and R_{v6p} as a function of the average residence time, which is made to expand from around 0.2 to 4 minutes. For this evaluation, we will set the average session duration to 4 minutes, the average session arrival rate to 1 min-1, and the wireless network speed to 3 Mbps. On this figure we may see that for all cases, the average communication interruption time decreases exponentially from about 100 ms, when the average residence time is around 0.4 minutes (fast nodes), to near zero when the residence time is longer than 3 minutes (slow nodes). This is an expected result because higher residence time means that mobile nodes will have a lower mobility, and thus lower chances to handover. On the contrary, values of residence time lower than 0.4 minutes will produce extreme high values of average communication interruption time because all the communication sessions will tend to be interrupted.

Finally, we may also see on Figure 7.13 that the proactive discovery cases (P_{v4} and P_{v6}) have a lower average communication interruption times than the reactive discovery cases (R_{v4r}, R_{v6r}, R_{v4p} and

R_{v6p}). An average communication interruption time of 100 ms for the proactive discover approach results for an average residence time around 0.3 ms, while for the reactive approach, to reach the same average communication interruption time, an average residence time value of around 0.5 ms is required. That is, slower nodes. As before, this is so because the proactive discovery approach has a lower broken communication time than the reactive discovery approach. Finally, we may see that there is not a great difference between the scenarios where MIP_{v4} and MIP_{v6} are used and between the scenarios where AODV and OLSR are running. However, the best performances are obtained when AODV and MIP_{v4} are used.

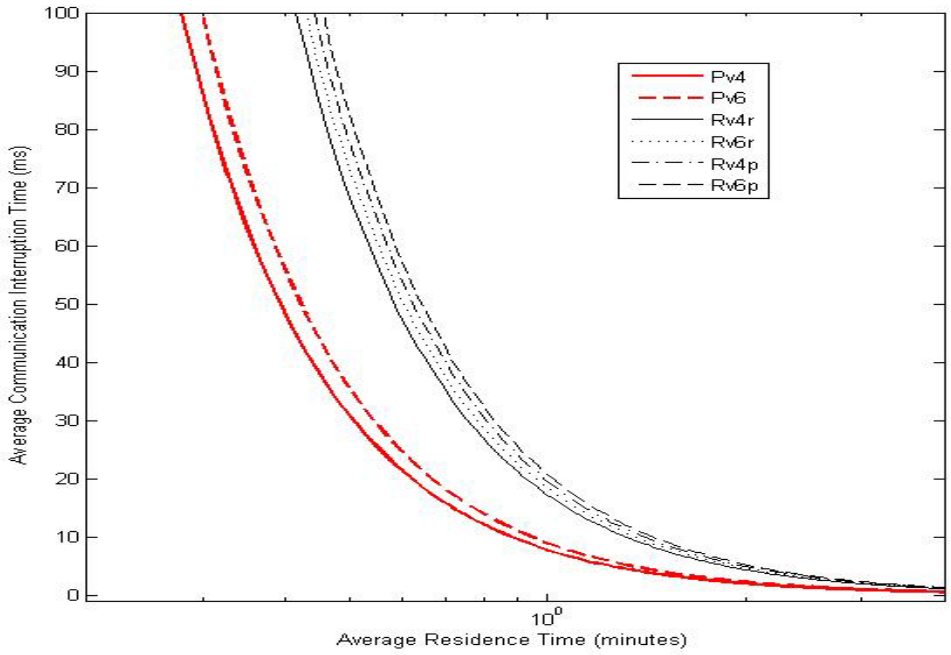

Figure 7.13 Average Communication Interruption Time as a Function of the Session Average Residence Time

A different behavior of the broken communication interruption time is shown on Figure 7.14, where different broken communication times are considered. In this case, the average residence time is let as a variable, independently of the agent discovery approach, MIP version, and running MANET protocol used. The average residence time is made to change from 0.3 to 10 minutes for three broken communication time values: 20 ms, 50 ms, and 100 ms respectively. It may be noticed on Figure 6.14 the same behavior found on Figure 6.10. The average communication interruption time decreases from very high values when the node mobility is high (residence time less than 1 minute), to near zero when the node mobility is low (residence time larger than 5 minutes). We may notice that for low mobility nodes, the T_b value makes no difference. That is, the average communication interruption time will always tend to zero for any value of T_b. On the other hand, when node mobility is high, higher T_b values will produce higher communication interruption times. For instance, a 100 ms average communication interruption time requires a residence time of 0.35 ms for a T_b value of 20 ms. On the other hand, to get the same average communication interruption time, it is required a residence time of 0.8 ms for T_b value of 100ms.

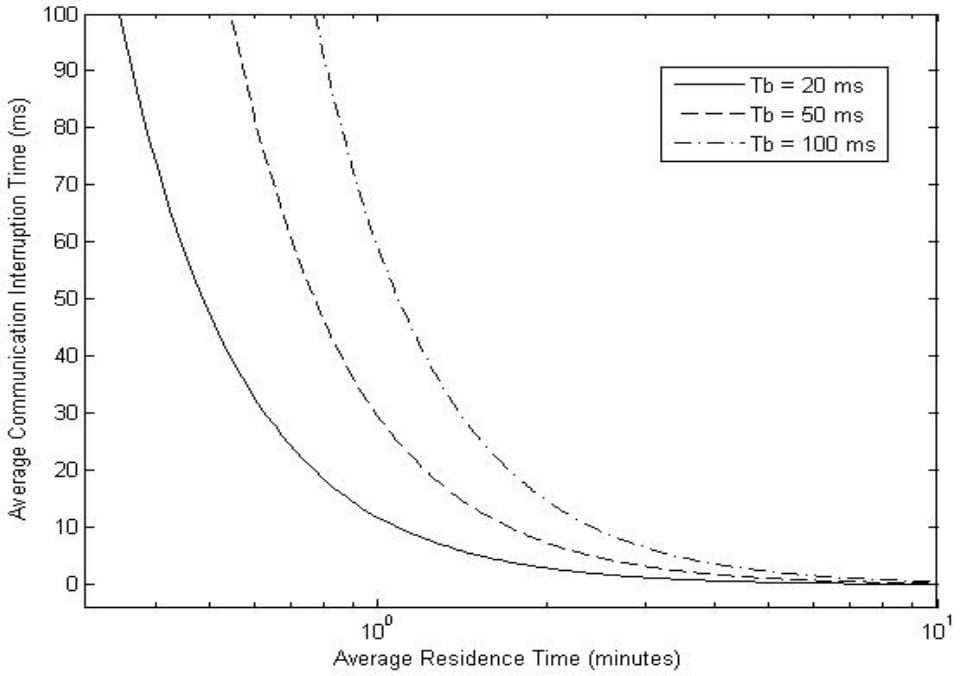

Figure 7.14 Average Communication Interruption Time as a Function of the Average Residence Time

Conclusions

It was explained in this thesis how MANET networks integrate with the Internet, permitting ad hoc nodes to communicate with hosts placed in any part of the world. In such an integrated scenario, the MANET may help to extend the coverage of existing infrastructure networks, like Wireless LANs and 3G networks. But it was pointed out that connecting MANETs to the Internet does not come without difficulties. Ad hoc routing protocols work different than regular routing protocols used on the Internet, and their interoperability becomes an important issue. For this reason communication between nodes on the Internet and ad hoc nodes is done throughout specialized Internet Gateways (IG). But a more demanding challenge emerges when node mobility is considered. In a multi-homed integrated ad hoc network, a moving node may need to change its gateway affiliation (a handover) while holding a communication with a correspondent hosts on the Internet, possibly causing communication interruptions. That is way the main objective of this research was to develop a model that may be used to evaluate the performance of MANET handovers.

Different issues affect MANET integration, some of which are the IP mobility protocol implemented, the running of ad hoc routing protocol, and the gateway discovery approach used. It was first described in detail how the Mobile IP protocol works. Mobile nodes must register to Home Agents and Foreign Agents to keep always connected to the Internet. Second, it was explained that MANET routing protocols are classified in proactive and reactive routing protocols according to how they discover destination routes. Finally, the different agent discovery approaches were explained. Agents may be discovered proactively or reactively. With proactive discovery, agents periodically send Agent Advertisements. With reactive discovery, mobile nodes require Agent Advertisement when they need them.

For this analysis we evaluated two different handover scenarios over which we elaborated a mobility model that was used later for the MANET performance evaluation. In one scenario, the proactive agent discovery approach was used, leaving the reactive approach for the other scenario. In both scenarios were considered the utilization of both versions of the Mobile IP protocol, the MIP_{v4} and the MIP_{v6}. Finally, in both scenarios was considered the utilization of both types of routing protocols: the reactive routing protocol and the proactive routing protocol. The developed handover model permitted us to propose some metrics that we used later to evaluate the MANET handover performance. These metrics are the broken communication time, the probability of a handover failure, and the average communication interruption time.

After evaluating two of the most popular MANET routing protocols (AODV and OLSR), the first one reactive, and the second one proactive, in order to know how they react when MANET nodes move between different MANET sub-networks, we have conclude that, even when OLSR, and in general all the MANET proactive routing protocols, has a lower transmission delay than AODV, and in general all the MANET reactive routing protocols, it has a lower performance. This may be verified from the evaluations made in this research: the broken communication time and the average communication interruption time. In all cases, AODV has a lower broken communication and average communication interruption time than OLSR. This occurs because AODV has a lower holding time than OLSR. More precisely, AODV has a holding time of 2 milliseconds and OLSR has a holding time of 6 milliseconds. Another drawback of OLSR in comparison with AODV is the higher signaling overhead it

adds to the MANET network. For these reasons we may conclude, and especially for high congested networks, AODV, and in general all the reactive routing protocols, has a better handover performance than OLSR and in general all the proactive routing protocols.

It could be seen that there is almost no differences between the handover performances when the two versions of Mobile IP were used. However, the broken communication time, the probability of a handover failure, and the average communication interruption time are lightly bigger when the MIP_{v6} is used than when the MIP_{v4} is used. This is so because the signaling packets for the MIP_{v6} are longer than those for MIP_{v4}. This permit us conclude that since there is almost no difference between the two Mobile IP versions performance, it is recommended to use MIP_{v6}, since it has a lower transmission delay than MIP_{v4}.

We finally investigated the impact that the different agent discovery approaches have on the handover MANET performance. It was found a noticeably difference on the handover performance between the different agent discovery approaches. In the scenarios considered, the proactive discovery approach resulted with a better performance. As shown on Figure 5.2 and Figure 5.3, and later verified on the evaluation results, the reactive discovery approach has a longer broken communication time than the proactive discovery approach. With the proactive approach, a roaming node request new agent registration (a handover initiation) as soon as it finds a more convenient gateway. On the other hand, with the reactive discovery approach, a roaming node has to loose contact with its actual gateway first, then it has to find a convenient gateway, before a new agent registration may be requested.

To analyze the agent discovery approach impact over MANET handovers, the broken communication time was evaluated as a function of the wireless speed, the number wireless hops, the process and queuing time, and the average session arrival rate. The probability of handover failure was evaluated as a function of the number of wireless hops, the average packet arrival rate, the wireless speed, and the threshold value. Finally, the average communication interruption time was evaluated as a function of the average session arrival rate, the average session duration, and the average residence time. In all results we could confirm that the proactive discovery approach has a better handover performance than the reactive discovery approach, which permit us conclude that regardless the MANET routing protocol, and the Mobile IP version, the proactive agent discovery approach should be used in highly mobile scenarios. But in a highly mobile scenario is recommendable to use a reactive routing protocol, so we recommend the combination of proactive agent discovery approach and reactive routing protocol.

In particular, we noticed that the reactive agent discovery approach may have a broken communication time and an average communication interruption time that in some scenarios may render the network useless. In general, in the considered scenarios, values of wireless speed lower than 0.5 Mbps, average residence time lower than 0.5 minutes, average process and queuing time bigger than 5 ms, and number of wireless hops bigger than 20, may produce broken communication times bigger than 200 ms, and average communication interruption times bigger than 10 ms. For these cases, the proactive discovery approach is recommended.

Acknowledgements

I want to thanks the whole staff from the Department of Electrical and Electronic Engineering at the University of Cagliari for the support given during my PhD studies. Special thanks go to Dr. Luigi Atzori, for his constant support and valuable advices during my working activities.

This PhD research was conducted at the CNIT Multimedia Communications Laboratory at the University of Cagliari.

References

[1] C. R. Dow, P. J. Lin, S. C. Chen, J. H. Lin, and S. F. Hwang , A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks, Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05) , 2005.

[2] S. Corson, J. Macker, Mobile Ad hoc Networking (MANET): routing protocol performance issues and evaluation considerations, RFC2501, January 1999.

[3] J. Qaddour, R. Barbour, Evolution to 4G wireless: problems, solutions, and challenges, The 3rd ACS/IEEE International Conference on Computer Systems and Applications, 2005, pp. 78 – 81.

[4] G. Kortuem, F. Kawsar, D. Fitton, V. Sundramoorthy. Smart Objects as Building Blocks for the Internet of Things. IEEE Internet Computing, vol. 14, no. 1, pp. 44–51, 2010.

[5] M. Abolhasan, T. Wysocki, E. Dutkiewicz, A review of routing protocols for mobile ad hoc networks, Ad Hoc Networks 1 (2), 2004, pp. 1 – 22 .

[6] K. Rahman, R. Zaman, A. Gopal, Integrating Mobile Ad Hoc Networks and the Internet: challenges and a review of strategies , Communication Systems Software and Middleware and Workshops (COMSWARE 2008), January 2008, pp. 536 – 543.

[7] H. Cha, J. Park, and H. Kim, Extended Support for Global Connectivity for IPv6 Mobile Ad Hoc Networks, Internet-Draft "draft-cha-manet-extended-support-globalv6-00.txt", October 2003.

[8] Y. Tseng, C. Shen, W. Chen, Integrating mobile IP with ad hoc networks, Computer 36 (5), 2003, pp. 48 – 55.

[9] H. Kumar, R.K. Singla, S. Malhotra , Issues & Trends in AutoConfiguration of IP Address in MANET , Int. J. of Computers, Communications & Control, Vol. III, 2008, pp. 353-357 .

[10] C. Perkins, E. Royer, Ad-hoc on-demand distance vector routing, Proceedings of the Mobile Computing Systems and Applications (WMCSA'99), 1999 , pp. 90 – 100.

[10] E. Royer, C. Toh, A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks, IEEE Personal. Communication. Magazine, 1999, pp. 46 – 55.

[11] S. Sesay, Z. Yang, J. He, A Survey on Mobile Ad Hoc Wireless Network, Information Technology Journal, vol. 3, no. 2, 2004, pp. 168 – 75

[12] G. Malkin, B. Networks, RIP Version 2, Request for Comments: 2453, November 1998

[13] E. Mahdipour, A. Rahmani, E. Aminian, Performance Evaluation of Destination-Sequenced Distance-Vector (DSDV) Routing Protocol, International Conference on Future Networks, 2009, pp. 186,190

[14] C. Perkins, P. Bhagwat, Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers, Proceeding SIGCOM '94, Conference on Communication, Architecture, Protocols and Applications, August 1994, pp. 234 – 244.

[15] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), Request for Comments: 3626, October 2003

[16] P. Jacquet et al, Optimized Link State Routing Protocol for Ad Hoc Networks, Proceeding 5th IEEE Multi Topic Conference (INMIC 2001), 2001.

[17] R. Ogier, F. Templin, M. Lewis, Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), IETF Internet draft, draft-ietf- manet-tbrpf-11.txt, October 2003

[18] P. Spagnolo, T. Henderson, Connecting Ospf Manet To Larger Networks. Military Communications Conference. Milcom 2007

[20] C. Perkins, E. Royer, Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, July 2003.

[21] D. Johnson, D. Maltz, J. Broch, DSR: The dynamic source routing protocol for multihop wireless ad hoc networks, Ad Hoc Networking, Addison-Wesley, 2001, Ch. 5 , pp. 139 – 172.

[22] C. Perkins, Mobile-IP, ad-hoc networking, and nomadicity, Computer Software and Applications Conference (COMPSAC'96), 1996, Proceedings of 20th International, 1996, pp. 472–476.

[23] F. M. A. Abduljalil, S. K. Bodhe, A Survey Of Integrating Ip Mobility Protocols and Modile Ad Hoc Networks, IEEE Communications Surveys & Tutorials, 1st Quarter 2007 , Volume 9, No. 1.

[24] C. Perkins, IP Mobility Support for IPv4, IETF RFC 3344, Aug. 2002.

[25] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson, G.Q. Maguire, First Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC) 2000, 2000, pp. 75 – 85.

[27] Z. Lin, L. Yuanan, L. Kaiming, Z. Linbo, Y. Ming, A Hybrid Internet Gateway Discovery Scheme in Mobile Ad Hoc Networks, WASE International Conference on Information Engineering, ICIE '09. 2009, pp. 367 – 370.

[28] B. Lu, B. Yu, B. Sun, Adaptive Discovery of Internet Gateways in Mobile Ad Hoc Networks With Mobile IP-based Internet Connectivity. 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom '09), 2009. pp. 1 – 5.

[29] P. Ruiz, A. Gomez-Skarmeta, Enhanced Internet connectivity for hybrid ad hoc networks through adaptive gateway discovery, 29th Annual IEEE International Conference on Local Computer Networks, 2004, pp. 370 – 377.

[30] P. Ratanchandani, R. Kravets, A hybrid approach to internet connectivity for mobile ad hoc networks, Wireless Communications and Networking (WCNC 2003), 2003 , vol. 3, pp. 1522 - 1527.

[31] C. Jelger, T. Noel, A. Frey, Gateway and Address Autoconfiguration for IPv6 Ad Hoc Networks, Internet- Draft draft-jelger-manet-gateway-autoconf-v6-02.txt. Apr. 2004.

[32] H. Lei, C. Perkins, Ad Hoc Networking with Mobile IP, Proceedings of the 2nd European Personal Mobile Communication Conference, 1997.

[33] M. Ergen, A. Puri, Mewlana-Mobile IP Enriched Wireless Local Area Network Architecture, Proceedings of the Vehicular Technology Conference (VTC 2002-Fall), 2002 , vol. 4, pp. 2449 - 2453.

[34] B. Xie, A. Kumar, A Framework for Integrated Internet and Ad Hoc Network Security, Proceedings of Ninth International Symposium on Computers and Communications (ISCC 2004), 2004, pp. 318–324.

[35] H. Ammari, H. El-Rewini, Integration of mobile ad hoc networks and the internet using mobile gateways, Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS04), 2004

[36] A. Nilsson, C. Perkins, A. Tuominen, R. Wakikawa, J. Malinen, AODV and IPv6 internet access for ad hoc networks, SIGMOBILE Mobile Computer Communication Review 6 (3) (2002), pp. 102 – 103 .

[37] J. Broch, D. Maltz, D. Johnson, Supporting hierarchy and heterogeneous interfaces in multi-hop wireless ad hoc networks, Proceedings of the 1999 International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'99), 1999, pp. 370

[38] Y. Sun, E. Royer, C. Perkins, Internet connectivity for ad hoc mobile networks, International Journal of Wireless Information Networks special issue on ''MANETs: Standards, Research, Applications, Volume 9, (2), pp. 75 - 88.

[39] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson, J. Maguire, MIPMANET - mobile IP for mobile ad hoc networks, Proceedings of the Mobile and Ad Hoc Networking and Computing (MobiHOC 2000), 2000, pp. 75–85.

[40] M. Benzaid, P. Minet, K. Agha, Integration of Mobile-IP and OLSR for a universal mobility, Wireless Networks 10 (4), 2004, pp. 377 – 388.

[41] J. Shin, J. Na, H. Lee, A. Park, S. Kim, Mobile IP support in ad hoc networks with wireless backbone, Proceedings of the Vehicular Technology Conference (VTC 2004-Spring), vol. 4, 2004, pp. 2136 – 2139.

[42] J. Xi, C. Bettstetter, Wireless multi-hop internet access: gateway discovery, routing, and addressing, International Conference on Third Generation Wireless and Beyond (3Gwireless'02), 2002.

[43] R. Wakikawa, J. Malinen, C. Perkins, A. Nilsson, A. Tuominen, Global connectivity for IPv6 mobile ad hoc networks, Internet Draft, draft-wakikawa-manet-globalv6-05, March, 2006.

[44] S. Ding, Mobile IP handoffs among multiple internet gateways in mobile ad hoc networks, Communications, IET, Volume 3, pp. 752 – 763.

[45] B. Lo, B. Yu, B. Sun, Adaptive Discovery of Internet Gateways in Mobile Ad Hoc Networks With Mobile IP-based Internet Connectivity ,

[46] R. Kumar, M. Misra, A. Sarje, An Efficient Gateway Discovery in Ad Hoc Networks for Internet Connectivity, International Conference on Computational Intelligence and Multimedia Applications, 2007

[47] T. Kim, S. Yeo, J. Park, B. Vaidya , Performance Evaluation of Hybrid Multipath Mobile Ad hoc Network , 6th IEEE Consumer Communications and Networking Conference, CCNC 2009, 2009.

[48] J. Xie, I. Howitt, I. Shibeika, IEEE 802.11-based Mobile IP fast handoff latency analysis, Proceedings of IEEE ICC, Jun. 2007, pp. 6055–6060

[49] L. Ping, Y Peiyan, An Approach to Calculate Queue Delay in Mobile Ad Hoc Networks, International Conference of Information Science and Management Engineering (ISME), 2010

[50] J. Xie, U. Narayanan, Performance Analysis of Mobility Support in IPv4/IPv6 Mixed Wireless Networks, IEEE Transactions On Vehicular Technology, Vol. 59, No. 2, Feb. 2010

[51] M. Denko, W. Chen, An architecture for integrating mobile ad hoc networks with the Internet using multiple mobile gateways, Canadian Conference on Electrical and Computer Engineering, May 2005, pp. 1097 - 1102