Routing and Interworking Protocols for Next Generation Wireless Networks

By

Nadeem Akhtar

Submitted for the degree of Doctor of Philosophy

UNIVERSITY OF SURREY

Centre for Communication Systems Research
School of Electronics and Physical Sciences
University of Surrey
Guildford, Surrey, GU2 7XH, UK

October 2007

In the name of Allah, the Most Gracious, Most Merciful

"Seeking knowledge is obligatory upon every Muslim."

- Prophet Muhammad (peace be upon him)

Summary

Next Generation Internet (NGI) architectures aim to enable convergence of a multitude of wired and wireless systems. A common theme is the presence of an IP-based core network with heterogeneous access networks at the edge. Non-conventional systems such as ad hoc, mesh, sensor networks etc. are expected to be fully integrated into NGI. Two different yet related technical challenges must be addressed to create such an integrated networking infrastructure. First, protocols and mechanisms have to be designed for each type of network that will be part of NGI, according to its specific requirements. Second, interworking mechanisms between these networks have to be developed to support inter-operability and inter-network co-operation.

This thesis addresses both these challenges, albeit within a limited scope. First, position-assisted and multipath routing extensions are proposed for the Relative Distance Micro-discovery Ad hoc Routing protocol to minimise signalling overhead and increase data throughput. Simulation results show that these extensions improve the protocol's performance significantly. Next, the effect of using multipath routing in conjunction with different channel assignment algorithms on the capacity of wireless mesh networks is investigated, in relation to single path routing. For this purpose, an analytical framework for capacity estimation is proposed. The analysis indicates that the effect of routing algorithm is inter-linked with channel assignment schemes. Finally, mechanisms for interworking between heterogeneous wireless networks (such as ad hoc and mesh networks) based on Network Composition are investigated and a signalling protocol for establishing composition is proposed. Furthermore, the analysis of cost of composition in WLAN scenarios revealed that signalling load is relatively small but latency is high.

Key Words: Ad hoc Networks, Position-assisted Routing, Multipath Routing, Wireless Mesh Networks, Channel Assignment, Nominal Capacity, Ambient Network, Composition, Signalling Protocol.

Acknowledgements

I would like to express sincere and heartfelt thanks to my supervisors, Prof. Rahim Tafazolli and Dr. Klaus Moessner, for their support, advice and encouragement. I am forever indebted to them for giving me the chance to pursue this research.

This work and everything else I have achieved so far would not have materialized without the selfless love and unstinted backing of my parents and siblings. They have demonstrated tremendous patience and understanding and no amount of words can express my gratitude towards them. Despite the enormous physical distances between us, the warmth of their love and affection has always been a source of great comfort.

There is no easy way to describe the contribution of my dearest friend, Mahvash. It would have been impossible to come this far without her. She has been a constant source of inspiration and also helped me focus whenever my resolve wavered. The unique and special friendship that has developed between us during the last few years has made this long, and often difficult, journey truly worthwhile.

I'm grateful to everyone in CCSR for all the help, especially Mike, Stoytcho, Steph, Alice, Haitham, Shyamalie and Karann. Their useful and timely comments were instrumental in ensuring that my work progressed. Special thanks to Atta and Ahmed for helping navigate my way through here in the early years.

Thanks also to Rehan and Hena whose hospitality regularly motivated my escape from Guildford for much-needed rest and relaxation. Saif, Nivedita, Sunit, Mili and Kumar deserve a special mention simply for being such good friends. Last, but not least, thanks to everyone else who has helped me in myriad ways over the years.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

3GPP	3rd Generation Partnership Project
ACS	Ambient Control Space
AN	Ambient Network
ANAP	Ambient Network Attachment Protocol
ANI	Ambient Network Interface
AODV	Ad hoc On-demand Distance Vector
AODV-BR	Ad hoc On-demand Distance Vector Backup Routing
AP	Access Point
API	Application Programming Interface
APS	Ad hoc Positioning System
ARI	Ambient Resource Interface
ASI	Ambient Service Interface
BAN	Body Area Network
CA	Composition Agreement
CBR	Constant Bit Rate
C-FE	Composition Functional Entity
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
DASM	Diffusing Algorithm for Shortest Multipath

DCCP	Datagram Congestion Control Protocol
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
DYMO	Dynamic On-demand
FE	Functional Entity
FN	Failure Notification
FSR	Fisheye State Routing
FTP	File Transfer Protocol
GANS	Generic Ambient Network Signalling
GMR	Graph Multi-path Routing
GPS	Global Positioning System
GSLP	GANS Signalling Layer Protocol
GTLP	GANS Transport Layer Protocol
HAN	Home Area Network
HDE	Hybrid Distance Estimation
IARP	Intrazone Routing Protocol
IEEE	Institute of Electrical and Electronics Engineers
IERP	Interzone Routing Protocol
IETF	Internet Engineering Task Force
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
IST	Information Society Technologies
LAR	Location Aided Routing
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
MDSR	Multi-path Destination Source Routing

MNO	Mobile Network Operator
MPR	Multipoint Relay
MS	Media Server
MSR	Multipath Source Routing
MT	Mobile Terminal
MTA	Message Transfer Attributes
NGI	Next Generation Internet
NSIS	Next Steps In Signalling
OLSR	Optimized Link State Routing
OSPF	Open Shortest Path First
PAN	Personal Area Network
PDA	Personal Digital Assistant
PDM	Physical Distance Micro-discovery
PDR	Packet Delivery Ratio
PRNET	Packet Radio Network
QoS	Quality of Service
RD	Relative Distance
RDE	Relative Distance Estimation
RDM	Relative Distance Micro-discovery
RDMAR	Relative Distance Micro-discovery Ad hoc Routing
RERR	Route Error
RIP	Routing Information Protocol
RREP	Route Reply
RREQ	Route Request
RTS	Request To Send
RTT	Round Trip Time
SAE	System Architecture Evolution
SMR	Split Multipath Routing

SURAN	Survivable Adaptive Radio Networks
TBRPF	Topology Broadcast based on Reverse Path Forwarding
TC	Topology Control
TCP	Transmission Control Protocol
TLU	Time Last Updated
TORA	Topology Ordered Routing Algorithm
TTL	Time To Live
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
UTRAN	UMTS Terrestrial Radio Access Network
VAN	Vehicular Area Network
VoIP	Voice over Internet Protocol
VWR	Virtual Wireless Ring
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

Chapter 1

Introduction

Next generation communication networks will support many heterogeneous systems, both wired and wireless. Furthermore, convergence will be a key feature of such networks. Next Generation Internet (NGI) architectures will comprise a multitude of access networks, connected to a common core network. Multi-hop wireless access networks will form an integral part of future communication systems, besides the conventional single-hop access networks where base stations and access points are directly connected to the wired backbone via wired links. The growing use of ad hoc and mesh networking technology is already making this a reality, although on a limited scale in the form of isolated deployments. Furthermore, mobile access networks such as Vehicular Area Networks (VAN) will also be more widespread. Finally, in addition to the core and access networks, there will be end user devices, user-owned small networks such as Home/Personal/Body Area Networks (HAN/PAN/BAN) and special types of networks such as surveillance systems, sensor networks, multimedia entertainment systems etc. These will connect to the core network via access networks and sometimes directly attach to each other without traversing the core.

Figure 1.1 shows the logical view of how these different types of networks are connected in NGI architectures. Two different, yet related, technical challenges must be addressed in order to realize such an architecture. First, protocols and mechanisms have to be designed for the different types of networks that constitute NGI. This has to take into account the specific requirements of each network and extensive research is ongoing in this direction. This is particularly true for networks such as ad hoc and mesh, personal, vehicular, sensor etc. The main research issues here relate to network configuration and organisation, routing, mobility management, security etc. The second challenge is to design suitable mechanisms to enable flexible and dynamic interworking between these networks. In current networks, interworking and co-operation between networks is mainly restricted to data forwarding. Note that such mechanisms should be generic so that they can be applied diverse interworking scenarios.

The research presented in this thesis tries to address both these challenges, albeit within a limited scope. First of all, routing protocols for ad hoc networks are investigated. Then, the effect of routing and channel assignment on the capacity of

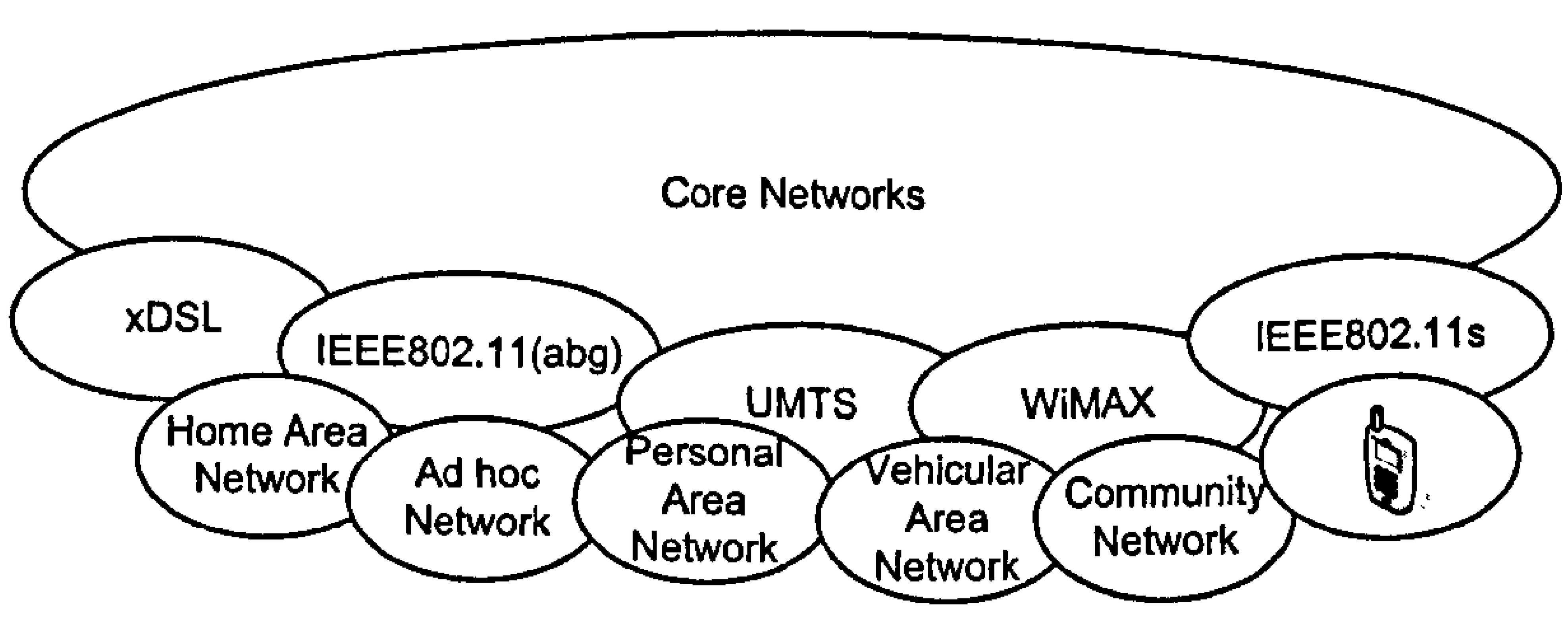


Figure 1.1: Next Generation Internet Architecture: Logical View

wireless mesh networks is analyzed. Finally, the design of a framework for flexible and dynamic interworking for network co-operation is studied.

The next section discusses motivations and objectives of the research and then the main contributions to the advancement of state-of-the-art are enumerated. In the end, the organisation of the rest of this thesis is briefly described.

1.1 Motivation and Objectives

This research addresses technical challenges towards the realization of next generation wireless networks. In particular, the investigation focusses on two aspects of interworking: i) interworking between nodes in multihop wireless networks for data forwarding and ii) interworking between networks to enable co-operation for resource and service access and sharing amongst heterogeneous networks. In the following, first the motivations behind this research are discussed with the help of a usage scenario. Then, the objectives of this study are explained.

1.1.1 Scenario

Figure 1.2 illustrates one specific NGI scenario. At the centre of this scenario is a Wireless Mesh Network (WMN) backbone, comprising several routers, inter-connected via multihop wireless links. The WMN is connected to two access networks, a WLAN hotspot and a WiMAX network, both of which are attached to the Internet via high-speed (wired) links. Finally, there is a Mobile Ad hoc Network (MANET) which consists of a number of end user terminals such as laptops, PDAs etc. Some of the MANET nodes are directly attached to a couple of WMN routers.

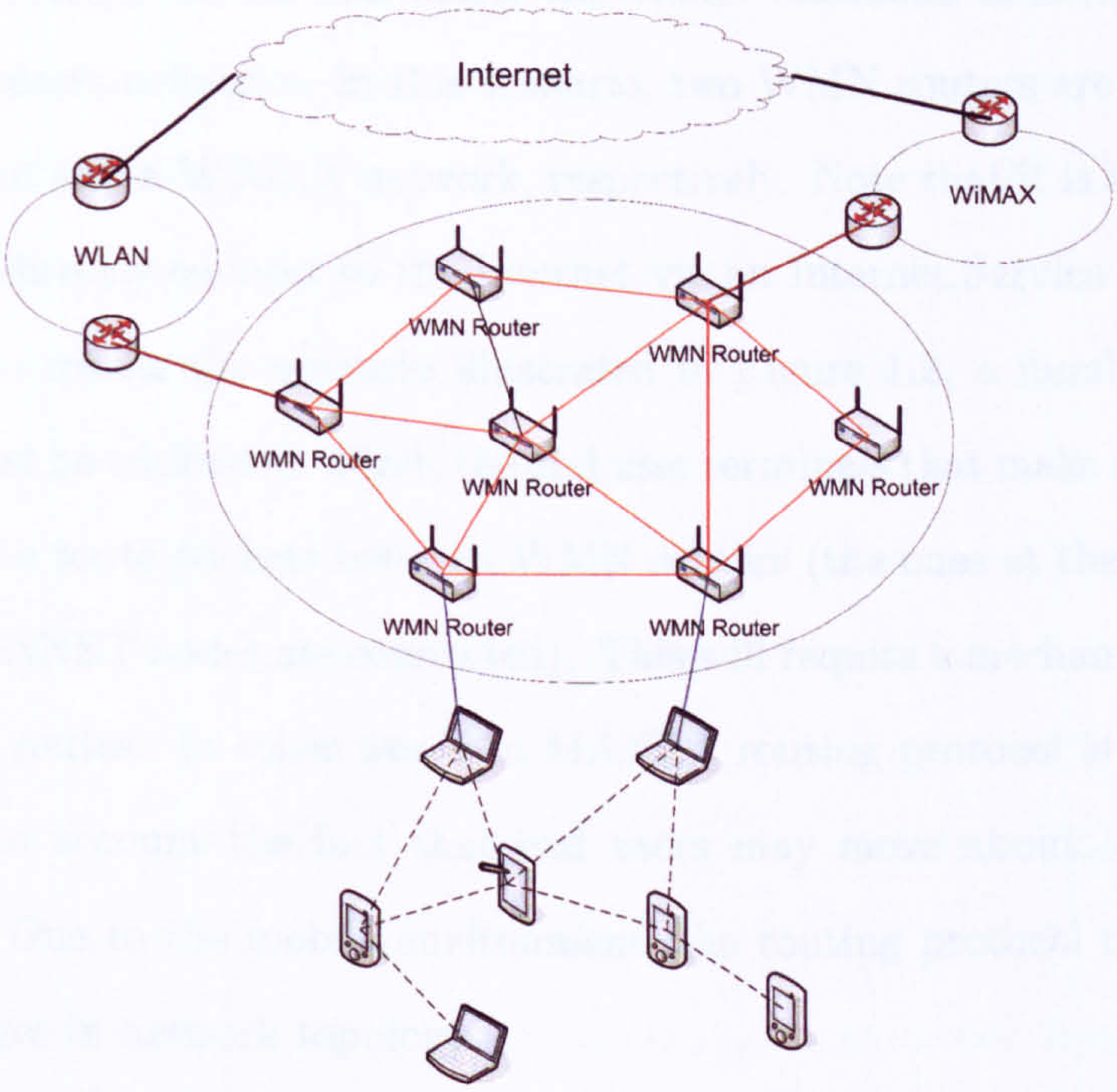


Figure 1.2: NGI Scenario

To put the scenario into proper context, the WMN can be seen as community mesh network deployed to cater to the needs of people living within a large residential campus (e.g. a housing colony). Since the radio range of WMN routers is limited, a large number of routers will be needed to enable all the residents to directly attach to one of them. A more viable option is to deploy a limited number of routers and extend their coverage by using ad hoc connectivity between end users. In other words, terminals belonging to end users can form MANET *islands*, allowing terminals that are not within the radio range of a WMN router to get connectivity to the WMN backbone via multihop paths traversing one or more end user terminals. This ensures that the end users are fully connected with each other. However, in order to provide

Internet connectivity to the end users, the WMN backbone must be connected to one or more access networks. In this scenario, two WMN routers are connected to a WLAN hotspot and a WiMAX network, respectively. Note that it is also possible for the WMN to directly connect to the Internet via an Internet Service Provider.

In order to realize the scenario illustrated in Figure 1.2, a number of technical challenges must be addressed. First, the end user terminals that make up the MANET must be able to route packets between WMN routers (the ones at the edge, to which some of the MANET nodes are connected). This will require a mechanism to establish and maintain routes. In other words, a MANET routing protocol is required. This must take into account the fact that end users may move about, albeit within a limited area. Due to the mobile environment, the routing protocol must be able to react to changes in network topology.

Second, the WMN backbone must be designed taking account technical and economic considerations. In particular, the number of WMN routers and the network topology must be determined in such a way that end user requirements (such as throughput, delay etc.) are met at a reasonable cost. In addition, mechanisms for establishing routes between the WMN nodes are also needed so that traffic between the end users and external networks can be routed. In addition, as the WMN routers have multiple radio interfaces, channels must be assigned to interfaces such that mesh connectivity is maintained whilst keeping co-channel interference down. In other words, the WMN topology, routing and channel assignment schemes must be selected in such a way that the network capacity must at least be enough to meet the traffic demands of the end users. For this, it must be possible to quantify the available capacity for different topologies, routing approaches and channel assignments.

Finally, the WMN has to establish co-operation with the access networks. This is not just limited to having the appropriate gateway mechanisms in place. The WMN should be able to set up service level agreements with the WLAN and WiMAX networks in order to guarantee that the traffic flowing to/from the end terminals meets users application requirements. In addition, the WMN may also want to use the services of WLAN/WiMAX network to authenticate the end users. Another example of such co-operation is the use of the DHCP server belonging to the WLAN (or WiMAX) network to assign IP addresses to the end terminals. Furthermore, the WLAN may offer to act as Mobile IP Foreign Agent to support mobility of end terminals. Such wide-ranging co-operation between heterogeneous networks requires a flexible and dynamic interworking framework.

The scenario described above provides the background for this research. Although a number of issues were highlighted, this study targets only a select few, as discussed below.

1.1.2 Research Objectives

The first item of study is routing protocols for mobile ad hoc networks. MANET is an autonomous system that consists of mobile nodes which can move around arbitrarily [1]. No assumptions are made about the availability of fixed infrastructure. In the most extreme case, a MANET is made up entirely of end user terminals such as laptops, PDAs, mobile phones etc, which are connected to each other via wireless links. However, some MANET usage scenarios have specialised devices such as wireless routers and APs in addition to end user nodes.

MANETs are different in many respects from other networks such as fixed, cellular and hotspot networks. To begin with, MANETs do not depend on fixed infrastructure. Furthermore, MANET nodes are not organised in a predetermined topology and nodes can move about arbitrarily and hence the network topology is dynamic. In the absence of fixed infrastructure, MANET nodes act as routers for relaying data and control messages on behalf of other nodes. These unique characteristics of MANETs pose a number of research challenges in the areas of channel assignment, MAC mechanisms, routing, quality of service, security and privacy etc.

Various aspects of MANETs have been investigated extensively during the past two decades. Among these, routing has attracted the maximum attention. The MANET Working Group of the Internet Engineering Task Force (IETF) [2] was constituted in 1986 to promote standardization of IP-based routing functionality for MANETs. Design of routing protocols for ad hoc networks has proved to be a challenging problem due to a number of factors. Firstly, network topology can change frequently due to node movements. Secondly, absence of fixed infrastructure means that deployment of dedicated routers is not always possible and hosts have to share routing and other network functions. Thirdly, nodes in the network have to share the same bandwidth-limited wireless channel. These factors impose certain requirements on MANET routing protocols, some of which are contradictory.

Dynamic topology results in short lifetimes for routes and necessitates frequent refreshing of routing databases in order to provide up-to-date information. However, bandwidth constraints imply that control overhead has to be minimised which puts limitations on the frequency of route updates. In general, the protocol must be lightweight so that it does not put excessive use of energy and bandwidth resources of the network. Therefore, it can be said that routing protocols for MANETs should be able to react swiftly to the changes in network topology and yet, be able to operate efficiently in a resource-constrained environment. In reality, it is nearly impossible to satisfy these requirements simultaneously and practically feasible solutions require a certain degree of trade-off between the conflicting design goals.

The research presented here addresses the problem of minimising control overhead incurred from routing-related signalling. The challenge is to reduce signalling overhead without degrading the overall protocol performance. The starting point of this investigation is the Relative Distance Micro-discovery Ad hoc Routing (RDMAR) protocol [3], designed to achieve high overall throughput whilst maintaining a low control overhead. The protocol was developed by Aggelou and Tafazolli at the University of Surrey. RDMAR restricts the scope of route search during the discovery phase, thus avoiding the overhead associated with the conventional approach of flooding the whole network with route query messages. *Query localisation* is made possible by estimation of relative distance between source and destination nodes. The goal is to further improve the overall performance of RDMAR protocol by reducing the signalling overhead and improving the throughput and delay aspects. This is achieved by introducing a set of extensions to the protocol.

The second study item addresses estimation of the capacity of wireless mesh networks. A wireless mesh network can be seen as a special case of MANET because it also consists of nodes interconnected via multihop wireless links. A key difference is that in most WMN use cases, only a few or maybe none of the nodes are mobile [4]. Client-based mesh networks that consist of end user terminals are very much like conventional ad hoc networks, although in general, connectivity to a (wired or wireless) backbone network is assumed. However, backbone or infrastructure mesh networks usually consist of fixed nodes connected via wireless links. In this case, WMN nodes are dedicated wireless routers and access points. These nodes can have more than one radio interfaces, thereby allowing the use of multiple radio channels for creating the mesh of wireless links.

Wireless mesh networks have attracted considerable attention as an alternative deployment model for access networks. In particular, the use of WMNs to provide last-mile access is proving quite popular. Furthermore, mesh-based metropolitan wireless broadband networks are also being rolled out. Other usage scenarios include enterprise networks, transportation systems, distributed video surveillance systems etc.

One of the challenging aspects of WMN design is the estimation of network capacity in order to dimension the network appropriately. Like ad hoc networks, the capacity of WMNs depends on a several different yet related factors. In particular, network size and topology, radio technology, traffic profile, routing protocol, channel assignment are some of the important factors that can affect WMN capacity. The work reported here addresses the problem of estimating the capacity of WMNs for a set of scenarios taking into account the different factors mentioned above. The focus of this study is on multi-radio multi-channel WMNs.

The third study item relates to interworking and co-operation between heterogeneous networks. The main research challenge is to design a flexible framework to enable dynamic and automatic interworking. This will facilitate co-operation between networks and also help realize full convergence of networks, beyond the current attempts such as Fixed-Mobile Convergence and integration of WLAN and 3GPP networks.

There are two important aspects of next-generation networks that must be taken into account. First, there will be a multitude of systems with different characteristics in terms of underlying networking technologies, network size and complexity etc. Second, there is a great diversity in the way control functions such as routing, mobility and QoS management, security etc. are organised and the control function that enables interworking must be able to handle this.

The IST Ambient Networks project [5] has proposed the idea of a unified control space to hide the heterogeneity in the underlying networking technologies by using a set of technology-agnostic reference points. Furthermore, a common control space is proposed to present a homogeneous view of the control plane to the outside world. The Ambient Network architecture includes a feature known as composition which is defined as a framework for flexible and dynamic interworking between diverse networks. It can be used in a wide range of scenarios involving end users, access providers, network operators, brokers etc for provisioning of access, control and sharing of network services and resources amongst heterogeneous networks. Network composition has been taken up a feasibility study item by the 3GPP [6].

The last part of this research is devoted to the study of network composition. A signalling protocol for supporting the composition framework has been proposed. Furthermore, a detailed study was carried out to identify the costs of composition in terms of signalling load and latency.

1.2 Main Contributions

The main contributions to the advancement of state-of-the-art are briefly summarised below.

1. A position-based route discovery method is added to RDMAR with the aim of improving the accuracy of distance estimation algorithm. The query localisation feature of RDMAR now works with physical distances whenever node position data is available and falls back on relative distance estimation otherwise. Modifications have been made to the protocol messages and various data structures so as to handle node position data. This add-on enhances the performance of RDMAR by minimising the control overhead.

2. A highly directional route discovery extension is proposed to limit the propagation of control messages to those regions of the network where the likelihood of finding the destination node is very small. Once again, this makes use of node position information when such data is available. This extension is integrated with the position-based discovery mechanism which is shown to be highly effective in minimising the amount of control overhead incurred for on-demand route discovery without any degradation in the overall protocol performance.

3. The third RDMAR extension is multipath routing. The protocol is modified to discover and use multiple routes between source-destination node pairs. Furthermore, a traffic-based data forwarding approach is proposed to take into account the diverse requirements of applications. Results show that multipath routing improves throughput performance and at the same time, leads to significantly smaller control overhead.

4. An analytical framework for estimating the capacity of wireless mesh networks has been developed, based on the concept of collision domains. Furthermore,

the capacity of multi-radio multi-channel WMNs in different scenarios is investigated to study the effect of different design parameters such as channel assignment scheme, routing algorithm, network topology and traffic profile.

5. A signalling protocol for network composition is proposed to enable control plane interworking and the detailed specification provided. Furthermore, a detailed analysis of the composition process is carried out to investigate the costs of composition in terms of signalling load and latency for a number of scenarios. Different strategies for composition negotiation are studied and the associated costs are computed.

1.3 Thesis Outline

The rest of this thesis is organised as follows. In the next chapter, the background to the research on ad hoc routing is presented which includes a survey of relevant literature. Chapter 3 introduces the position-assisted routing extension to RDMAR and in Chapter 4, the multipath extension for RDMAR is described. Chapter 5 focusses on capacity estimation of wireless mesh networks. Signalling for network composition is analysed in Chapter 6. Finally, conclusions and future directions of this research are discussed in Chapter 7. In addition, two appendices related to Chapter 6 are also included at the end.

Chapter 2

Routing in Mobile Ad hoc Networks

2.1 Introduction

The origins of mobile ad hoc networks can be traced back to the packet radio networks of the 1970s. The ALOHA system was developed in 1970 at the University of Hawaii to setup radio-based connectivity between user terminals and a central computing facility within the university [7]. It was essentially a single-hop packet broadcast network but provided the basis for a multihop multiple access packet radio network (PRNET) [8]. PRNET was followed by the Survivable Adaptive Radio Networks (SURAN) program in the early 1980s [9]. All these efforts were mainly directed towards developing highly resilient networking technologies for the military for deployment in battlefields. The real impetus for ad hoc networking came in the 1990s in the form of the mobile computing devices and economically viable radios and the term "ad hoc networks" was formally adopted by the IEEE 802.11 sub-committee.

Mobile ad hoc network is an autonomous system that can be created *on-the-fly* [10][11]. This type of network is self-configuring and does not depend on any fixed infrastructure such as access points, routers, switches etc. In the absence of such infrastructure, end hosts also act as routers to provide support for routing and other network functions in a cooperative and distributed fashion. MANET nodes communicate with each other over a wireless channel. They can be stationary or mobile and therefore, join or leave the network anytime.

There are two common MANET use cases: as a standalone network or as a *stub* network. In the first case, the network operates in isolation without being connected to a fixed backbone. Example usage scenario is a disaster recovery operation where members of the rescue team establish an ad hoc network to coordinate their operations. In the second case, one or more MANET nodes are attached to a fixed wireline/wireless network and thus act as gateways between other MANET devices and nodes in the fixed network or beyond. A typical scenario is Internet connection sharing where one of the nodes is attached to an Internet Service Provider and others use it as the default router.

There are two possible modes of communication with reference to node connectivity. In the first case, all nodes are within the radio range of each other, so that each node is able to reach every other node *directly*. This situation, although possible, is highly restrictive as nodes must be located close enough to ensure direct connectivity while using reasonable radio transmit power levels. Note that mobile MANET nodes have battery limitations and hence cannot use high transmit power. The second case arises when not all nodes lie within the transmission range of each other, which rules out direct reachability for some source-destination node pairs. To enable connectivity between a pair of nodes that do not share a direct radio link, *multi-hop* paths are required. In other words, such nodes have to use a chain of radio links passing through one or more *intermediate* nodes for sending and receiving data packets. Intermediate nodes perform the classical store-and-forward function of a router. Before such a forwarding chain can be used, the route which consists of a sequence of intermediate nodes, has to be determined.

The routing problem has been around for a long time and a large number of IP-based routing protocols are discussed in literature, some of which have found their way into the routing infrastructure in the global Internet [12][13][14]. Conventional IP routing protocols can be broadly classified into two categories: link-state and distance-vector. In the first one, every node maintains a topology map in the form of a graph, showing connectivity with other nodes. Each node uses its copy of the map for computing routes to every possible destination in the network by identifying the best next hop for it. The map is created by combining information gathered from reachability messages and link-state advertisements. Reachability messages are essentially *announcements of existence*, periodically transmitted by each node to neighbours and used to create link-state advertisements containing information about neighbour nodes. Each node floods the network with advertisements about its own link-state. After a node has received advertisements from all other nodes, it creates the topology map. The Open Shortest Path First (OSPF) [13] and the Intermediate System to Intermediate System (IS-IS) [15] protocols are examples of link-state routing.

The working principle behind distance-vector routing is that routers periodically inform their neighbours about local topology changes. Periodic update from a router contains either the full routing table or a part of it and is sent to all neighbours. Upon receiving this information, other routers modify their own routing tables to reflect the changes and then inform their neighbours as well. The metrics used to compute the best path for a network differ between different routing protocols but the basic operating principles remain the same. The complexity and overhead of distance vector protocols is generally less than that of link state protocols. Examples of distance-vector routing are the Routing Information Protocol (RIP) [12] and Interior Gateway Routing Protocol (IGRP) [16].

Protocols like RIP or OSPF could be used in MANETs as well, at least in theory. However, in practice, they are not suitable for ad hoc networks because of the highly dynamic and resource-constrained environment. These protocols depend on intensive signalling to ensure that routing state at each node is fresh and accurate. Link-state protocols require periodic exchange of reachability messages and link-state advertisements to build the topology map. Any changes in the link-state of a node requires flooding the network with fresh messages so that other nodes can update their routes. Similarly, distance-vector protocols require routers to send route updates containing the whole routing table or parts of it. Clearly, these operations generate a significant amount of signalling across the network. Such an approach is not feasible for MANETs where node mobility results in dynamic network topology and short-lived routes, thereby needing frequent route or link-state updates.

The unique characteristics of MANETs motivate the need for protocols that can fulfil the challenging requirements of ad hoc routing. In the rest of this chapter, first the important features of ad hoc networks are listed and then some high-level design requirements are discussed. Finally, a survey of ad hoc routing protocols is presented and their pros and cons analysed.

2.2 Requirements of MANET Routing Protocols

Mobile ad hoc networks have a number of unique features which differentiate them from traditional networks. Some of these features and their implications on routing are described below:

Device Heterogeneity: MANETs typically consist of portable communication devices. Given the huge variety in such devices available nowadays, it is clear that MANET nodes are heterogeneous in many respects. They can be of different type such as laptops, Personal Digital Assistants, mobile phones, digital cameras etc. In addition, there are differences in terms of battery lifetime, storage capacity, processing power and so on. Hence, ad hoc routing protocols have to take into account the diversity in device types. More specifically, protocols must be scalable and flexible to handle the differences in device capabilities.

Power Constraint: MANET nodes that are on the move do not have access to a stable power supply and hence, have to rely on battery power. Despite advances in battery technology, power is still a major limitation of mobile devices. It is possible to simplify routing by increasing transmit power which will increase the likelihood of the destination lying within the transmission range. The possibility of finding direct paths between nodes increases with high transmitted levels but this also requires considerable amounts of battery power. Multi-hop paths are a better way to work under battery constraints. However, establishing and maintaining routes requires control signalling which in itself is a drain on battery. Therefore, protocols must not create significantly large signalling overhead.

Node Mobility: In general, there are no limits whatsoever on the mobility profile of a MANET node. Hence, nodes can be stationary or mobile, depending on the usage scenario. Different degrees of node mobility are to be expected. A node maybe mobile at one point of time but stationary at another instant of time. When a node is mobile, existing links with neighbouring nodes are broken and new ones are set up with nodes in the vicinity of the new position. Frequent changes in link states, coupled with the fact that node movements are independent of each other, create a highly dynamic network topology. Therefore, protocols must be robust against node mobility.

Absence of Fixed Infrastructure: Availability of fixed infrastructure is not a pre-requisite for MANETs. As a result, usage scenarios with and without infrastructure have to be supported. In the absence of fixed infrastructure such as dedicated routers, switches, servers, etc., ordinary hosts share the responsibility of providing various network functions. The routing functionality has to be distributed across all nodes for robustness and resilience in the face of node mobility. Assigning too much importance to particular nodes for routing can lead to problems when one or more of these special nodes leave the network.

Variable and Constrained Bandwidth: MANET nodes are connected by wireless links which are subject to effects such as fading and shadowing. Furthermore, most scenarios require sharing a common channel between several nodes using some multi-access scheme. As a result, nodes have to operate in an environment where bandwidth is variable as well as constrained. Efficient use of available bandwidth requires that overhead must be kept to a minimum.

Based on the discussion above, a set of high-level design requirements for ad hoc routing protocols are abstracted:

- The protocol must be lightweight in terms of memory consumption, processing requirements and control overhead.

- The protocol must be able to find routes without significant delay.
- The protocol must be able to react to route changes quickly.
- The protocol must consume minimum amount of battery power.
- The protocol must be distributed in nature.
- The protocol must use the available bandwidth efficiently.

These requirements are, to some extent, contradictory. For a protocol to adapt quickly in the face of frequent route changes, intensive signalling is needed which results in high overhead. This, in turn, leads to battery drain as well as low bandwidth utilisation. Distributed operation improves robustness and resilience but also means that all nodes have to support routing functions. Such conflicting requirements have made ad hoc routing protocol design a very challenging task. Nevertheless, a large number of ad hoc routing protocols have been proposed in literature, as discussed in the next section.

2.3 Survey of Ad hoc Routing Protocols

2.3.1 Classification of Protocols

There are many different ways in which routing protocols can be classified. Below, some of these classification criteria are used to categorise protocols found in literature.

Ad hoc routing protocols can be broadly divided into two categories: *proactive* and *reactive*. Proactive protocols follow the same approach as conventional IP routing protocols in the sense that each MANET node has *a priori* knowledge of routes to other nodes in the network. The main advantage of this approach is that whenever a particular node wants to establish an application layer session with a peer, it only has to perform a routing table lookup to find the next hop node towards the destination. Therefore, data packets can be routed with minimal delay. The downside is that routing tables have to be kept fresh using frequent route update messages which contributes to the overhead and also causes congestion in the network, especially in high-mobility scenarios where topology changes are frequent. Maintaining exhaustive routing tables is also wasteful because of the short lifetimes of routes. Examples of such protocols include the Topology Broadcast based on Reverse-Path Forwarding (TBRPF) [17], Destination Sequenced Distance Vector routing [18], Wireless Routing Protocol [19], Fisheye State Routing (FSR) [20] etc.

The drawbacks of proactive routing suggest that protocols based on this approach are not well-suited for ad hoc networks. Reactive or *on-demand* routing has been proposed as an alternative. Here, MANET nodes discover routes only when required and keep them only as long as they are needed by higher layers. Thus, a node starts route discovery when it wants to establish an application session with another node. The route is active as while application data flows between them. The advantages of reactive routing is that there is no extra signalling for refreshing routes. In addition, routing tables are relatively smaller in size. The main drawback is that application data has to be buffered while a route is being discovered. Ad hoc On Demand Distance Vector (AODV) [21], Dynamic Source Routing (DSR) [22], Topology Ordered Routing Algorithm (TORA) [23], Relative Distance Micro-discovery Ad hoc Routing (RDMAR) [3] are some of the reactive protocols found in literature.

The pros and cons of both these routing approaches have motivated the development of *hybrid* protocols which include both reactive and proactive elements in order to exploit the advantages of both. The Zone Routing Protocol (ZRP) [24] is a prime example of hybrid routing.

Ad hoc routing protocols are also classified as *flat* or *hierarchical*. In flat routing, each node participates equally in routing and no node has any special responsibilities. Examples include AODV, DSR, RDMAR. Hierarchical protocols organise network nodes into a hierarchy. Nodes are grouped into clusters or zones and within each such group, certain nodes have special roles. ZRP employs hierarchical routing by dividing the network into zones. Flat routing is fully distributed and hence it is more flexible, robust and resilient. However, it suffers from scalability problems with respect to network size. Hierarchical routing protocols exploit device heterogeneity by taking advantage of superior capabilities of certain nodes in the network. In addition, clustering or zoning isolates local changes from affecting the whole network. At the same time, this approach introduces possible points of failure in the network and may even result in partitioning of the network.

Protocols can further be categorised as *location-aware* or *location-agnostic*, depending on whether information about network nodes' positions is used for computing routes or not. Although, in general, routing is intrinsically linked to physical location of nodes, most ad hoc routing protocols, such as AODV, TORA, DSR, DSDV, do not explicitly use location information when making routing decisions. In contrast, Location-aided Routing (LAR) [25] uses node position information when establishing routes while RDMAR uses relative node positions for the same purpose.

The classification presented above is not exhaustive. For instance, ad hoc routing protocols can also be categorised as distance-vector or link-state; unicast or multicast and so on. Rather than going deeper in classifying protocols, it is more instructive to compare and contrast some of the protocols mentioned above.

2.3.2 Protocol Examples

AODV is a reactive distance-vector protocol. In AODV, to discover a route, the source node broadcasts a Route Request (RREQ) message to its neighbours. The message contains addresses of the source and destination nodes and a sequence number. When an intermediate node receives this request, it installs a route towards the source node and then checks if a valid route to the destination is available in its route table. A Route Reply (RREP) message is sent to the source node if a route to the destination is found. Otherwise, the node rebroadcasts the RREQ and in this way, the message is relayed towards the destination node. Upon receiving the RREQ, the destination stores the newly-discovered route towards the source and sends back an RREP. The message is routed to the source by intermediate nodes using routes established during RREQ forwarding. As the RREP message progresses towards the source, intermediate nodes add/update routing table entries for the destination node. AODV ensures loop-free behaviour with the help of sequence numbers. Each node has its own sequence number which is incremented whenever there is a topology change in the immediate neighbourhood of a node. The sequence number also helps in selecting the fresh routes. A node's route table lists reachable destinations, the distance (in hops), the corresponding next hops and the sequence number of each destination node. A timer is also associated with each route table entry, which is updated whenever the particular route is used for routing application data. Routes are deleted when the associated timers expire. Nodes that sense a link break, delete the failed route(s) and initiate the *Failure Notification* procedure to inform all the affected nodes about this event. Thereafter, the *Route Maintenance* procedure is performed to find an alternative route between the source-destination pair. AODV eliminates the need for expensive routing table updates by establishing and maintaining routes as and when required. At the same time, nodes cannot establish application sessions until the route discovery is successfully completed. The protocol is flat and distributed and hence resilient and robust.

DSR uses the source-routing approach where the header of each data packet carries the full and ordered hop-by-hop route to the destination. To find a route to a particular destination, the source broadcasts an RREQ as in the case of AODV. As the message propagates towards the destination, intermediate nodes append their addresses to the *route record*. When the RREQ finally reaches the destination, the full route from source to destination is available in the message. The destination sends an RREP that also includes the route record. Upon receipt of the reply, the source creates a routing entry for the destination. If multiple routes are found, they are all installed in the cache. These additional routes provide redundancy in case of route failure. Furthermore, DSR has an aggressive caching strategy to discover routes while forwarding packets for other nodes and overhearing packets transmitted by other nodes. Source routing eliminates the need of keeping routes at the intermediate nodes. An obvious disadvantage is the overhead represented by the route record contained in the header. This can be quite significant if routes consist of several hops.

The Zone Routing Protocol includes both proactive and reactive features. The network is divided into overlapping routing zones with each network node at the centre of a zone. Within a particular zone, an *Intrazone Routing Protocol* (IARP) is used to proactively maintain routes between each node-pair within the zone. The size of a zone is defined by the zone radius parameter, expressed in number of hops. To find a route to a node which lies in a different zone, an *Interzone Routing Protocol* (IERP) is used. In this case, the source sends a route request to its border nodes which check their local route tables and if a route to the destination is available, a reply is sent back. Otherwise, the message is forwarded to their own border nodes and the procedure is repeated until the destination is found. The main advantage of ZRP is that the effect of topology changes is localised within the zones. Moreover, routes between nodes located within the same zone are available upfront and hence route acquisition delay is very small. ZRP does not specify the choice of IARP and in theory, any proactive protocol could be used. The choice of zone radius is an important design parameter. A small radius reduces the amount of signalling overhead due to the IARP procedures. At the same, it results in more frequent use of IERP for route discovery.

Optimized Link State Routing (OLSR) [26] protocol uses the proactive approach. In OLSR, each node selects some of its neighbour nodes as *multipoint relays* (MPRs). This subset is referred to as the MPRset of the node. Each MPR node maintains a MPR Selector set which is a list of all the nodes that have selected it as an MPR. A node's control traffic can only be forwarded by nodes that are in its MPRset. This prevents unnecessary transmissions of a message while it is being flooded into the network. Like other link-state protocols, in OLSR also, nodes use *Hello* messages to advertise one-hop neighbours and discover two-hop neighbours. However, the link-state is flooded into the network only by MPR nodes using Topology Control (TC) messages. Furthermore, an MPR node only has to advertise the links with nodes in its MPR Selector set. The information in TC messages is used to build routing tables in each node. OLSR optimises the classical link-state algorithm by decreasing the number of transmissions during message flooding and at the same time reducing the size of link-state advertisement messages. Compared to reactive protocols such as AODV and DSR, route acquisition delay is smaller but control overhead is higher. Advantages of OLSR are more pronounced in large-sized and dense networks.

The Location-aided Routing (LAR) protocol uses information about nodes' physical location for reducing control overhead. LAR assumes that nodes can obtain their position precisely using GPS or other means. If the source knows the previous location of the destination, then based on the time elapsed since the position information was acquired, it defines an *expected zone*, which is the area where the source expects the destination to be in. Further, the source also identifies a *request zone* that is defined to be the smallest rectangle that includes the present position of the source node and the expected zone. During the route discovery process, any intermediate nodes that do not lie in the request zone discard route request packets. Thus, unnecessary route requests are suppressed and control overhead is reduced. One problem with LAR is the assumption that all nodes have position information using GPS because it may not always be true as it is extremely difficult to get location information in certain situations, such as in built-up areas.

Relative Distance Micro-discovery Ad hoc Routing (RDMAR) is also a reactive protocol which uses information about node location for routing. The distinguishing feature of RDMAR is the concept of localised route discovery that tries to limit the scope of route discovery process to reduce the control overhead incurred. The RDMAR approach to ad hoc routing involves the use of the Relative Distance Estimation (RDE) algorithm. As the name indicates, RDE estimates the relative distance between a node-pair based on the last known value of the relative distance between the two and the time elapsed since this value was recorded. The distance is converted to hop count and used to limit the search area and thus reduce control overhead.

A recent re-chartering of the IETF MANET Working Group has resulted in efforts towards standardisation of one reactive and one proactive protocol. The Dynamic On-demand MANET routing protocol (DYMO) [27], derived from AODV, has been adopted as the reactive protocol.

2.4 Discussion

In this chapter, different aspects of ad hoc routing have been discussed. The characteristic features of these networks were described and analysed to yield a set of high-level requirements. In order to meet the unique challenges posed by ad hoc networks, routing protocols have to be:

- lightweight
- fast
- robust and resilient
- power-efficient
- bandwidth-efficient

The requirements listed above are contradictory in nature and hence, it is almost impossible to design protocols that meet all of them. Therefore, research effort has focussed on finding the right trade-off between these competing factors. A wide variety of protocols have been proposed in literature based on different routing approaches such as reactive/proactive/hybrid, flat/hieararchical, location-aware/location-agnostic etc. This classification yields insight into the pros and cons of these different protocols.

Chapter 3

Position-assisted Routing in Ad hoc Networks

3.1 Introduction

The Relative Distance Micro-discovery Ad hoc Routing (RDMAR) protocol was briefly described in the previous chapter. RDMAR is a reactive, distance-vector protocol, designed to minimise the control signalling overhead incurred for route setup and maintenance. This objective is achieved through *query localisation* which refers to limiting the spread of route request messages. RDMAR limits the scope of route discovery by estimating the *relative distance* between source and destination nodes which and then using it to set a parameter in the route request packet to control its indiscriminate forwarding by intermediate nodes. In this chapter, first the different elements of RDMAR are described in detail and then two extensions are proposed to further improve its localisation performance. These extensions rely on the use of node positions for routing purposes. Finally, results of a simulation-based evaluation of these extensions are presented.

3.2 Relative Distance Micro-discovery Ad hoc Routing Protocol

RDMAR comprises two main procedures: Route Discovery and Route Maintenance. The former is used for discovering the shortest-length route between source-destination pairs while the latter is invoked when active routes fail. These two procedures are common to all reactive distance-vector protocols [21][22][25]. The feature that distinguishes RDMAR from other protocols is the optimised route discovery mechanism referred to as Relative Distance Micro-discovery (RDM). The micro-discovery procedure includes a Relative Distance Estimation (RDE) algorithm to compute the relative distance between nodes. In the following, first a high-level overview of the protocol operations is given and then the RDE algorithm is described.

3.2.1 Route Discovery

The route discovery procedure is triggered when a data packet is received from upper layers for a destination to which there is no active route. At the source node, say S, the local route table is checked to determine if an active route to the destination node, say D, is available. The packet is forwarded to the appropriate next hop node if a valid route is found. Otherwise, the data packet is buffered and the RDM process is initiated.

The first step in RDM is to estimate the relative distance (*RD*) between nodes S and D. The *RD* is converted into number of hops and then a Route Request(RREQ) message is created, with the *Time-To-Live* (TTL) field set to the estimated RD, and broadcast to its neighbours. All nodes that lie within the transmission range of node S receive this packet. Such nodes are generally referred to as *intermediate* nodes. Each recipient checks the destination address field of the RREQ message to determine whether the request is intended for itself or some other node. Assuming that none of the neighbours is the target, they first install a *reverse* route towards the source and then rebroadcast the RREQ, after decrementing the TTL. Each intermediate node keeps a list of RREQs that have been forwarded previously and when an RREQ is received that matches one stored in the list, it is discarded. This is necessary to suppress duplicate requests from propagating in the network. In this way, the route query proceeds towards node D. When it finally receives the RREQ, the destination stores the route and sends a Route Reply (RREP) message to node S using the newly established route. The RREP is routed to the source via various intermediate nodes using the reverse routes learnt during the RREQ forwarding phase. Before sending the RREP to the next hop, intermediate nodes store the *forward* route towards the destination. It must be noted that unlike AODV [21] and DSR [22], in RDMAR, an RREP can only be generated by the destination node.

Figure 3.1 illustrates route discovery in an ad hoc network, where node S is attempting to find a route to node D, with the estimated RD equal to 2 hops. The RREQ broadcast by node S is intercepted by nodes 1 and 3 which forward it further after decrementing the TTL (now equal to 1). One of the recipients is node D which stores the route and sends RREP to the source. Nodes 2 and 4 also receive the RREQ forwarded by nodes 1 and 3, respectively. However, when they decrement the TTL, it becomes zero and hence they discard the RREQ. Had the original TTL been greater than 2, the RREQ would have been forwarded by nodes 2 and 4 to their neighbours (nodes 7 and 5, respectively) although the destination was only two hops

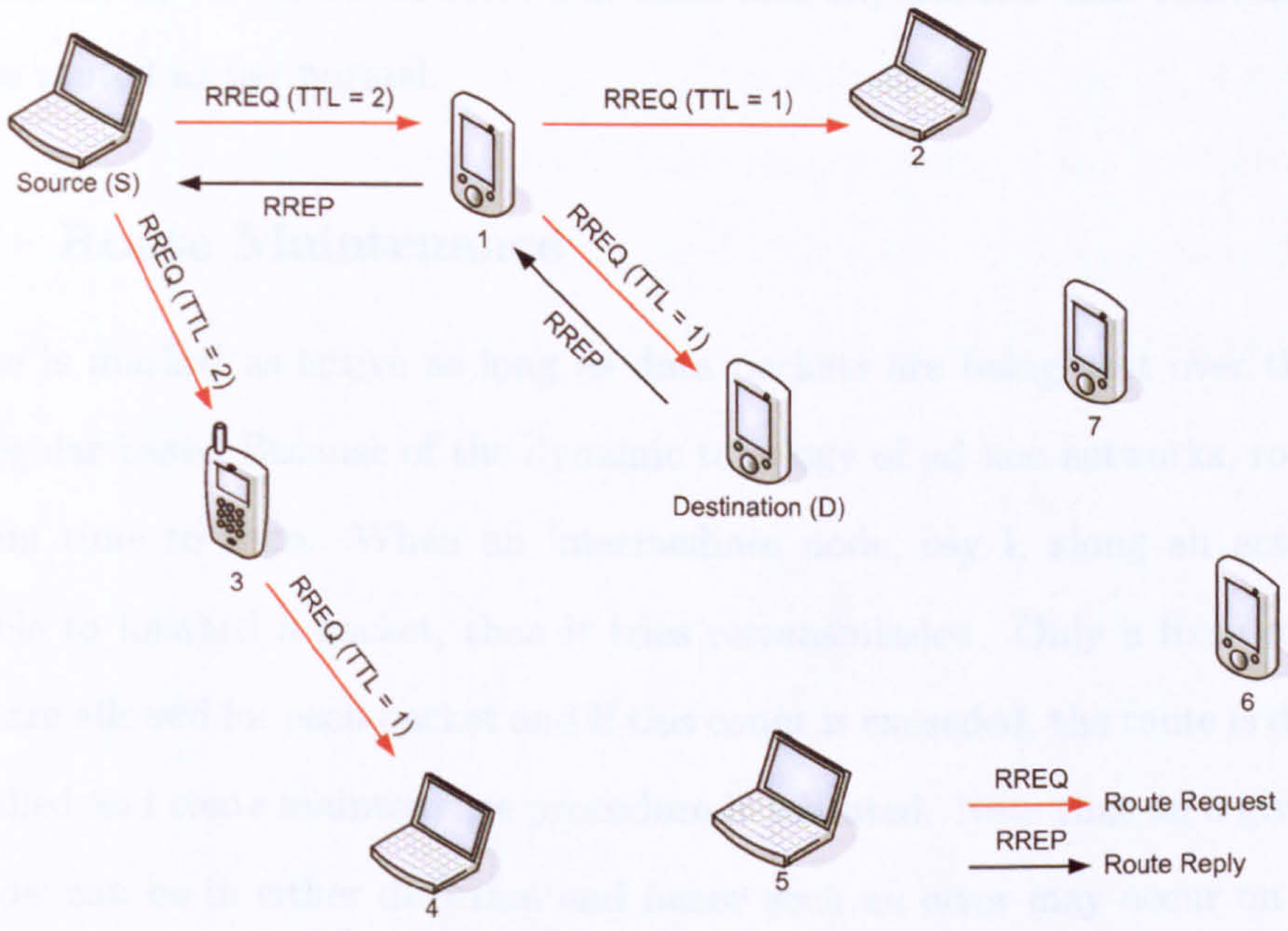


Figure 3.1: Route Discovery

away. Thus, the RDM mechanism ensures that the spread of RREQs is localised to a limited region of the network, in contrast to a pure flooding mechanism where RREQs are allowed to propagate throughout the network.

The routing table entries created at source, destination and intermediate nodes during the propagation of route discovery messages (both RREQ and RREP) include, besides next hop address and hop count for the routes, the time when the route was added in the *Time_Last_Updated* (TLU) field. This information is used during future RDM procedures, as will be clear later.

The route discovery procedure is completed when the RREP reaches node S and the newly discovered route to the destination is installed in the local routing table. Thereafter, data packets that were queued up while the route was being discovered, are transmitted on a First-In-First-Out basis and any packets that come afterwards are also routed as per normal.

3.2.2 Route Maintenance

A route is marked as active as long as data packets are being sent over that route on a regular basis. Because of the dynamic topology of ad hoc networks, routes may fail from time to time. When an intermediate node, say I, along an active route is unable to forward a packet, then it tries retransmission. Only a fixed number of retries are allowed for each packet and if this count is exceeded, the route is deemed to have failed and route maintenance procedure is initiated. Note that on a given route, data flow can be in either direction and hence such an error may occur on the path downstream from node S to node D or upstream from D to S. The response of node I (which detected the route failure) depends on its relative location with respect to the source and destination. If the distance of node I from D is less than that from node S, then it launches the RDM procedure directed towards the destination. However, if node I is closer to the source, a packet delivery failure notice is sent to the source and the *Failure Notification* (FN) is initiated. During this procedure, whenever node I receives a packet that in the normal course would have been routed over the failed route, the packet is dropped and an FN message is sent to the source which is added into the so-called *Dependent List.* This is done only once and any subsequent packets from that source are simply discarded. As the FN propagates towards the source, intermediate nodes delete the route towards the affected destination if it passed via the node that forwarded the FN. When node S receives the FN from node I, a fresh route discovery cycle is started.

Figure 3.2 illustrates the route maintenance process. In this case, there are three active routes (marked by red bidirectional arrows) between nodes 1-9, 4-8 and 3-6, respectively. All the routes traverse the link between nodes 2 and 5. When node 2 detects that the wireless link with node 5 has failed, it deactivates all the routes with node 5 as next hop. Furthermore, it sends Route Error (RERR) messages to nodes 1, 4 and 9 to inform them about the route failure.

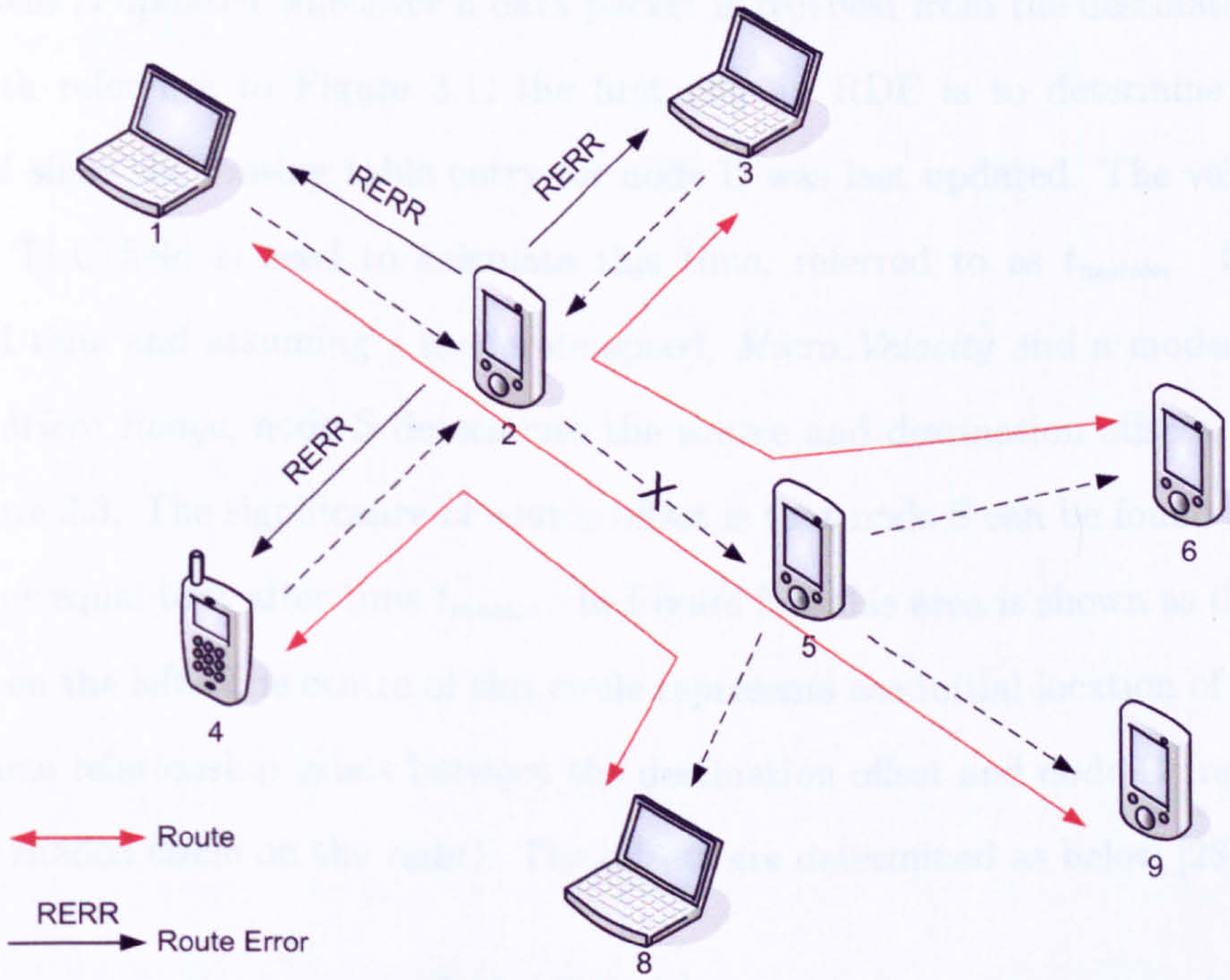


Figure 3.2: Route Maintenance

3.2.3 Relative Distance Estimation

The RDE algorithm is applied whenever a node wants to discover a route to another node in the network. Given the previously known distance between two nodes, a location prediction model is used to estimate the current relative distance. As mentioned earlier, each routing table entry has a TLU field which indicates the last time when routing information about the corresponding destination was received. Note that the TLU field is updated whenever a data packet is received from the destination.

With reference to Figure 3.1, the first step in RDE is to determine the time elapsed since the routing table entry for node D was last updated. The value stored in the TLU field is used to calculate this time, referred to as t_{motion}. Given the elapsed time and assuming a moderate speed, *Micro_Velocity* and a moderate radio range *Micro_Range*, node S determines the source and destination offsets, as shown in Figure 3.3. The significance of source offset is that node S can be found in a circle of radius equal to it after time t_{motion}. In Figure 3.3, this area is shown as the shaded region on the left. The centre of this circle represents the initial location of the node. The same relationship exists between the destination offset and node D (represented by the shaded circle on the right). The offsets are determined as below [28]:

$$s_{offset} = v_{\mu} * t_{motion}$$
$$d_{offset} = v_{\mu} * t_{motion} \tag{3.2.1}$$

where v_{μ} is the *Micro_Velocity*.

The new relative distance depends on the exact location of the nodes within the two circles that represent the sets of their possible locations. Based on source and destination offsets, the expected minimum and maximum possible relative distances

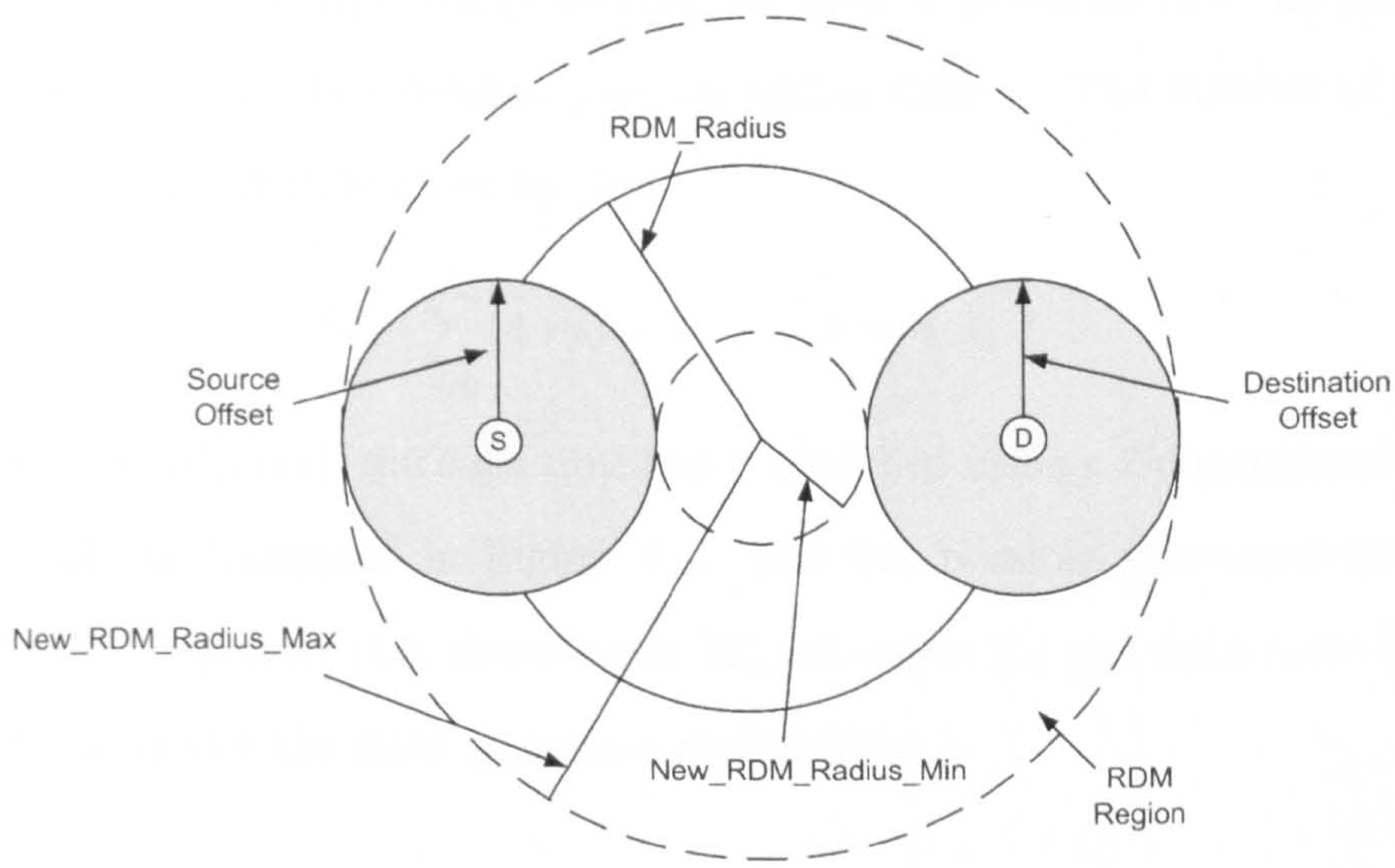


Figure 3.3: Relative Distance Estimation

between the two are given by:

$$New\_RDM\_Radius_{max} = RDM\_Radius + s_{offset}$$
$$New\_RDM\_Radius_{min} = RDM\_Radius - s_{offset} \quad (3.2.2)$$

The new relative distance falls between these two extremes. A stochastic model was presented in [3] to predict the new relative distance between the nodes, based on a two-dimensional random walk model. It makes two key assumptions: a) Time is divided into discrete units called *slots* and b) In each time slot, a node either moves one step (left, right, up or down) or stays stationary. The length of each step is the product of node velocity and slot duration. The analytical model uses the concept of *Virtual Wireless Ring* (VWR). Taking the position of a node at time $t = 0$ as the reference spot, VWR_t is defined as the circular region with the reference spot as centre and radius equal to the maximum distance that the node could have travelled in time t ($t \geq 0$). VWR_t encompasses all the possible positions that the node could have moved to from its reference position within time t. The number of all such positions, S_t for VWR_t is given by [28]:

$$S_t = \sum_{i=0}^{t}(4 * i) + 1 \qquad \text{t} = 0,\ 1,\ 2,\ ... \tag{3.2.3}$$

The movement of a node during a time slot is modelled using a 2-dimensional Markov walk model, as illustrated in Figure 3.4. The five possible movement states are: stationary (S), up-move (U), down-move (D), left-move (L) and right-move (R). The figure also indicates the state transition probabilities.

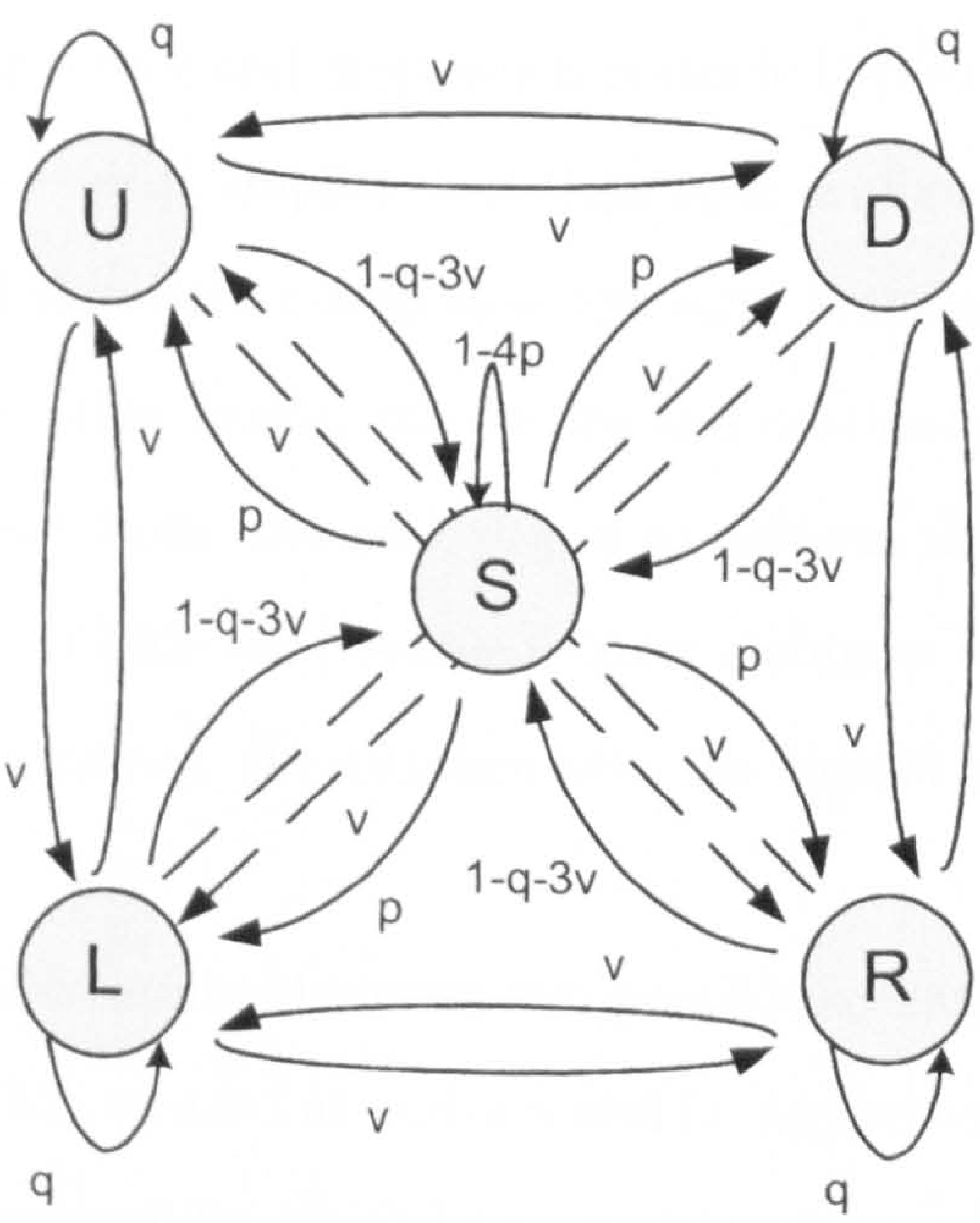


Figure 3.4: State diagram for node movements

Let the state space be denoted by $\Gamma = S, U, D, L, R$ and $\Gamma(t)$ be the state at time t. Furthermore, assuming that the distance between a node's reference spot and its location at time t is $d(t)$, the distance at time $t+1$ can take 4 possible values [28]:

$$d(t+1) = \begin{cases} d(t) & \text{if } \Gamma(t) = S; \\ d(t) + D & \text{if } \Gamma(t) = R; \\ d(t) - D & \text{if } \Gamma(t) = L; \\ \sqrt{d^2(t) + D^2} & \text{if } \Gamma(t) = U \ \text{or} \ \Gamma(t) = D \end{cases}$$

where D is the distance travelled during a single time slot.

$\{(D(t)), \Gamma(t), t = 0, 1, 2, ...\}$ is a Markov chain as $D(t+1)$ depends only on $D(t)$. The stationary probability distribution of this Markov chain, derived in [3], is used to find thea node's *spot configuration* which consists of the probabilities of different possible positions where it can be located relative to its reference spot. The model assumes that both the source and destination nodes in Figure 3.3 have same values for p, q and v respectively which implies that their spot configurations will be identical. It is further assumed that both nodes have the same transmission range and similar mobility patterns. In other words, the source and destination offsets will be equal. Given the spot configurations, the next step is to perform their convolution to determine the probabilities of different possible relative distances between the nodes. Once these probabilities are known, the distance with the highest probability is selected as the new RD.

This algorithm differentiates between two possible scenarios with reference to the two circles in Figure 3.3, centred at nodes S and D, respectively. In the first case, the two circles are non-overlapping which happens when s_{offset} (and d_{offset}) is less than half the previous relative distance. The second case is where the circles are overlapping which occurs when s_{offset} is greater than half the previous relative distance.

In the next section, some of the factors which influence RDMAR performance are discussed and then the position-assisted routing extension is described in detail.

3.3 Position-assisted Routing

The performance of RDMAR has been studied in detail and compared with other ad hoc routing protocols [3] [28]. These investigations revealed that localized route discovery results in improved overall protocol performance. The control overhead generated by RDMAR was found to be much less and this difference was accentuated as the transmission range increased. However, the route acquisition latency was higher on the average, because route discovery in RDMAR is an end-to-end process and only the destination is allowed to send RREP messages. This contrasts with AODV [21] and DSR [22] protocols where intermediate nodes can send RREPs on behalf of the destination if they have valid routes to it. The RDE algorithm holds the key to RDMAR performance. Accurate estimation of RD will lead to the discovery of a route to the destination in the first attempt with minimum overhead. Otherwise, two different types of anomalous situations arise. First, if the new RD determined by the algorithm is less than the actual RD, the first attempt at route discovery will fail because the RREQ is discarded before it reaches the destination as a result of TTL expiration. A new route discovery cycle is launched after incrementing the RD estimate by one hop. In the worst case, the discovery process may have to be repeated many times with increasing values of RD until the destination is found or the RD exceeds a pre-defined RD_{max} (which depends on network size). These repeated route discovery cycles result in considerable signalling overhead and also increase route acquisition delay. Second, if the estimated RD is more than the actual RD, the RREQ messages will travel to a much wider area than required, thereby leading to undesirable signalling.

The discussion above underlines the importance of RDE in the RDMAR protocol. The accuracy of RDE depends on a number of factors, first of which is the freshness of information about the last known RD value between the nodes. This is reflected by the value of t_{motion} which itself depends on the TLU parameter. On one hand, smaller the value of the t_{motion}, higher the chances that the estimate of the new RD is closer to the actual RD. On the other hand, a large value of t_{motion} means that the information about previous RD is outdated and may result in highly inaccurate estimate of new RD, especially if the destination node was moving at a high speed during this period. To avoid wildly inaccurate RD estimates (and hence incur high overhead), the RDE algorithm is not applied at all if t_{motion} exceeds a pre-defined maximum value. The second factor which influences RDE accuracy is the value of v_μ (*Micro_Velocity*) used to compute the offsets in Equation 3.2.1. This parameter represents node velocity and is assumed to be the same for all nodes. For a specific node, if v_μ is more than its actual velocity during the time period under estimation (which equals t_{motion}), the calculated offset will be an over-estimate. Conversely, if v_μ is less than the node velocity, the offset will be underestimated. In both cases, the end result will be inaccurate RD estimation. The third factor that affects the preciseness of the RDE algorithm is the choice of values for the probabilities of motion, i.e. p, q and v respectively.

It is clear that any improvement in the accuracy of the RDE will have a favorable impact on the overall protocol performance. The stochastic model used in RDE for movement prediction is based on relative positions of nodes, expressed as function of time, and iterates upon them to arrive at an estimate of the new relative distance between the two nodes. The RDE algorithm is executed at the source node but it assumes equal level of uncertainty in the relative positions of the two nodes. In Figure 3.3, the source node selects a possible location in its VWR and computes the probability of being found in that spot. Then, for each possible position of the destination (bounded by its VWR), it computes the associated probabilities. Finally, the RD corresponding to each destination position and the related probability are calculated. The same procedure is repeated for all possible positions of the source node. If a particular RD appears more than once, the related probabilities are added. The end result is a table of distances and associated probabilities out of which, the RD which has the highest probability is chosen.

The discussion above motivates the introduction of the position-assisted routing extension to RDMAR. There are two key features of the proposed extension: *Hybrid Distance Estimation* and *Directed Route Discovery*. The first one concerns the use of node positions in the RDE algorithm while the second one also makes use of position information for further narrowing the scope of route discovery.

3.3.1 Hybrid Distance Estimation

The Hybrid Distance Estimation (HDE) algorithm inherits the stochastic model of RDE for predicting node mobility. The key difference is that HDE is designed to work with both physical and relative distances. In the default case, HDE uses physical location of source and destination nodes to estimate the physical distance PD, which is then converted to TTL. When location information about either of the nodes (or both) is unavailable, the algorithm reverts back to RD estimation, as described in Section 3.2.3.

The physical distance is estimated by simplifying the RDE algorithm to take into account the fact that now there is no uncertainty in the source node's position. With reference to Figure 3.3, the circle around node S is reduced to a point located at its currently known (x, y) coordinates. The circle around node D is still there but centred at its previously known coordinates. The new situation is depicted in Figure 3.5.

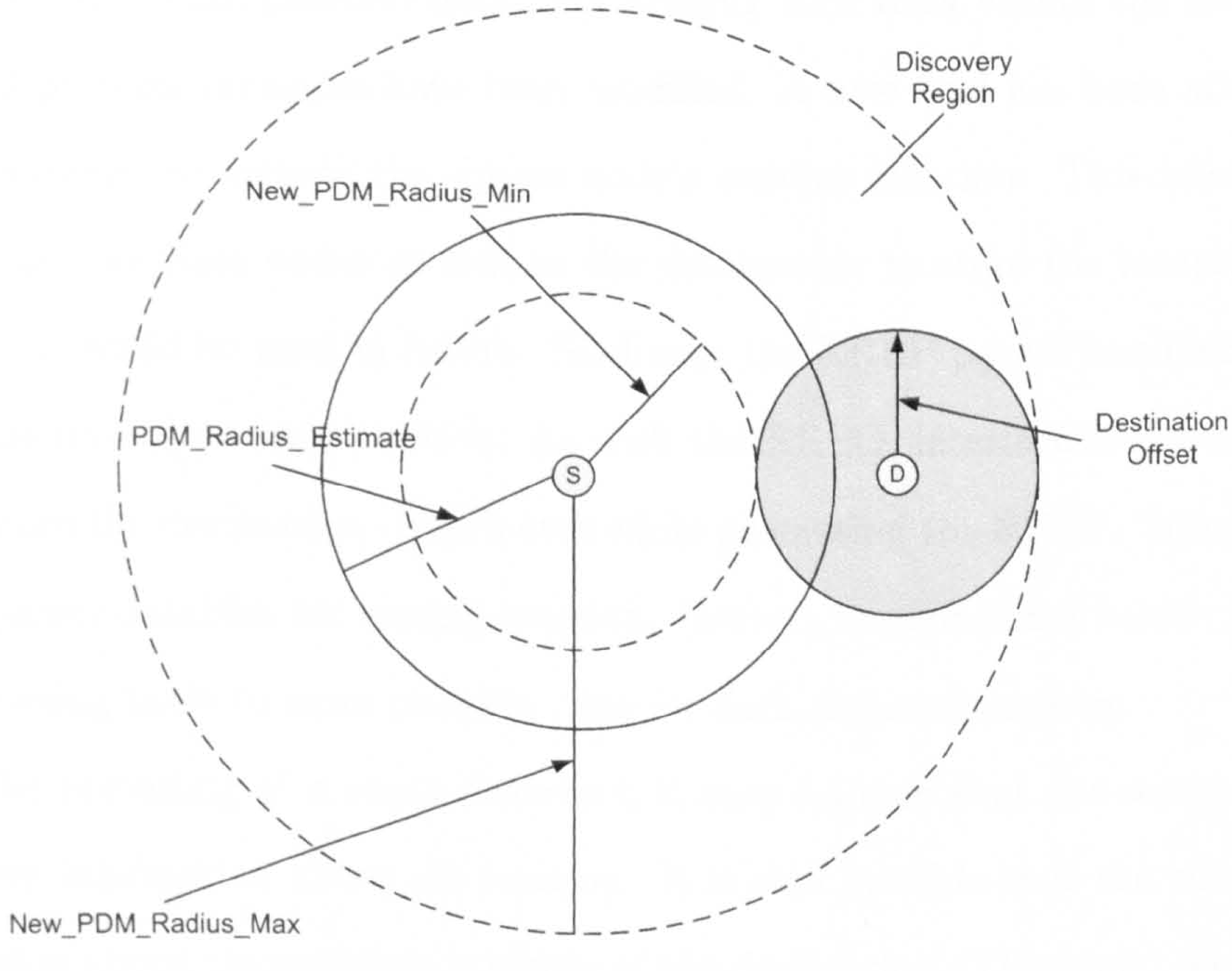


Figure 3.5: Physical Distance Estimation

The scope of route discovery is bounded by the two dashed circles. Note that *PDM* refers to Physical Distance Micro-discovery (cf. Relative Distance Micro-discovery). The actual scope of route discovery is determined by estimating the new *PD* between the nodes S and D, depicted by the solid circle (with radius equal to *PDM_Radius_Estimate*). With its own position already known, the stochastic model is used by the source node to determine probabilities of the possible (new) positions of the destination, given its last previously known location. It then calculates the probabilities of all possible distances between the two nodes. Finally, the most probable PD is chosen for determining the TTL to be used in the RREQ message.

Physical distance estimation will obviously work only if nodes know their own position as well that of other nodes. Therefore, each node must be equipped with a mechanism to obtain position data. For sharing such data within the network, the RDMAR protocol messages have been modified. A new field has been added to the RREQ message to include the source node's current location. This information is used by intermediate nodes as well as the destination to store the location of node S so that it could be used in future. Similarly, the RREP packet has been modified to include the destination position. As with the RREQ, intermediate nodes and the source store the destination coordinates while processing the RREP. Note that there is no separate database for storing location. Instead, an additional field is introduced in the routing table to store position data for each destination entry.

At the beginning of a route discovery, it may happen that the source is unable to acquire information about its position. It is also possible that the source has no information about the previous position of the destination. This could happen when the last received RREP/RREQ originating from the destination had no position data. In both these cases, the original RDE algorithm is used for getting the TTL value.

3.3.2 Directed Route Discovery

Directed route discovery exploits the knowledge of node positions to further optimize the protocol. More specifically, location information is used to limit the scope of the route discovery procedure further. Route discovery in native RDMAR is omni-directional i.e., the source (and intermediate) nodes broadcast route request packets and any node within their transmission range can receive the message and forward to its own neighbours as long as the TTL is greater than zero. Now, consider the network nodes to be lying in a 2-dimensional space with the source node at the origin. It is obvious that the destination can be located in only one of the four quadrants. Assume, for the sake of argument, that it is in the top-right quadrant, in which case, any route requests that propagate away from this quadrant will be of no use. Therefore, RREQ messages propagating away towards the edges of the remaining quadrants constitute an overhead and lead to inefficient use of bandwidth. This is evident from Figure 3.5 where the discovery region is a circle centred at node S although the destination is to be found on its right side.

Directed route discovery utilises position information to steer RREQ packets towards the quadrant in which the destination is located and thus avoids the wasteful situation mentioned above. When a route is to be discovered, the source node invokes the HDE procedure and sets the TTL field in the RREQ packet accordingly. In addition, it makes use of the previously known location of the destination to predict the approximate direction where the destination is located with respect to the source. Knowing its own position, the source node can determine the quadrant in which node D is located. This information is then inserted into the RREQ message.

When an intermediate node, say I, receives this message, it checks the quadrant it is situated in relative to node S. If node I is located in the same quadrant as the destination, it forwards the message to its neighbours. Otherwise, the reverse route to the source is stored but the RREQ is discarded. This procedure makes route discovery more localised to further reduce the control overhead. Once again, directed route discovery can be applied only when the source node known its own position, as well as that of the destination; otherwise route discovery follows the omni-directional approach. Figure 3.6 illustrates how directed route discovery is used.

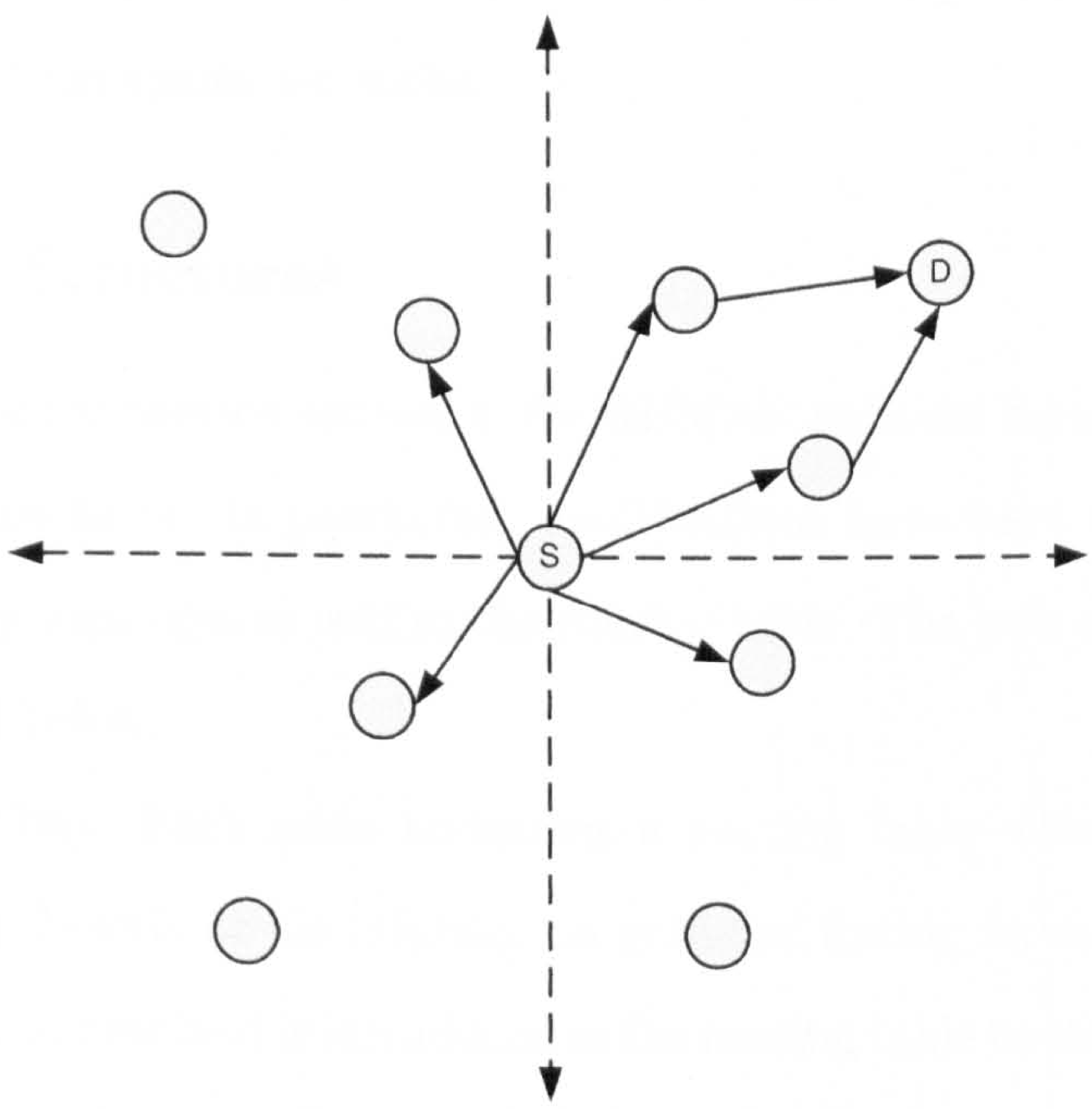


Figure 3.6: Directed route discovery

The figure above shows a MANET where node S wants to find a route to node D. After estimating the distance to node D, the source node determines that the destination node is located in the top right quadrant and this information is included in the RREQ packet. When the route request reaches nodes that are in quadrant 1, they decide to forward it to their neighbours. Nodes that are in other quadrants discard the message and the request propagates no further in those regions. Thus, unwanted route request messages are eliminated and the route request is steered towards the destination. Although, in general, this approach will help reduce signalling overhead, it must be pointed out that in certain situations, the reverse may happen. More specifically, with reference to Figure 3.6, if there are no other nodes (besides the destination) in the top-right quadrant, then route discovery will fail. This problem will be more acute in sparse networks.

3.3.3 Data Structures

The position-assisted routing extension for RDMAR requires certain changes to the protocol data structures. In particular, modifications have been made to the route request and reply messages as well as the routing table. The new data structures are briefly described below.

Routing Table: Each node maintains a routing table which contains routes discovered either directly or via information gathered during forwarding of RREQ or RREP messages. A new field is introduced in the routing table to store the coordinates of each destination. The modified routing table has the following fields:

1. Hop Count - distance between source and destination
2. Destination Address
3. Next Hop - neighbouring node via which destination can be reached
4. Time Last Updated - time when this entry was last updated
5. Position - coordinates of destination (New field)
6. Route Timeout - timer value for this route

Route Request: The RREQ message is extended with two new fields: one for storing the location of source node (originator of the RREQ) and another for indicating the quadrant in which the destination is expected to be found. In addition, a flag is added to indicate if the message carried source position information. The RREQ format is shown in Figure 3.7.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type</td><td colspan="2">Q</td><td>P</td><td colspan="13">Reserved</td><td colspan="8">Hop Count</td></tr>
<tr><td colspan="32">RREQ ID</td></tr>
<tr><td colspan="32">Source Address</td></tr>
<tr><td colspan="32">Source X Coordinate</td></tr>
<tr><td colspan="32">Source Y Coordinate</td></tr>
<tr><td colspan="32">Source Sequence Number</td></tr>
<tr><td colspan="32">Destination Address</td></tr>
<tr><td colspan="32">Destination Sequence Number</td></tr>
</table>

Figure 3.7: Route Request

The fields in the RREQ message are as follows:

1. Type - Indicates the message type ('1' for RREQ)
2. Q - 2-bit number indicating the quadrant in which the destination is located
3. P - Position flag which indicates if the message contains source coordinates
4. Reserved - Sent as 0; ignored at reception
5. Hop Count - Number of hops from the source to node currently processing the RREQ
6. RREQ Identifier - Unique number indicating the freshness of route request

7. Source Address - IP address of the RREQ originator

8. Source X Coordinate - X coordinate of source position

9. Source Y Coordinate - Y coordinate of source position

10. Source Sequence Number - Current sequence no. associated with source node

11. Destination Address - IP address of destination node

12. Destination Sequence Number - Last known sequence no. of destination node

Route Reply: The RREP has one new field to store the location of destination node (originator of RREP) and an extra flag to indicate if destination position is included in the message. The RREP format is shown in Figure 3.8.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type</td><td>P</td><td colspan="15">Reserved</td><td colspan="8">Hop Count</td></tr>
<tr><td colspan="32">Source Address</td></tr>
<tr><td colspan="32">Destination Address</td></tr>
<tr><td colspan="32">Destination Sequence Number</td></tr>
<tr><td colspan="32">Destination X Coordinate</td></tr>
<tr><td colspan="32">Destination Y Coordinate</td></tr>
<tr><td colspan="32">Lifetime</td></tr>
</table>

Figure 3.8: Route Reply

The fields in the RREP message are as follows:

1. Type - Indicates the message type ('1' for RREQ)

2. P - Position flag which indicates if the message contains source coordinates

3. Reserved - Sent as 0; ignored at reception

4. Hop Count - Number of hops from the destination to the node currently processing the RREP
5. Source Address - IP address of the RREQ originator
6. Destination Address - IP address of destination node
7. Destination X Coordinate - X coordinate of destination position
8. Destination Y Coordinate - Y coordinate of destination position
9. Destination Sequence Number - Last known sequence no. of destination node
10. Lifetime - The time in milliseconds for which nodes receiving the RREP consider the route to be valid

The remaining data structures have been left untouched. These include the Failure Notification message, the Dependent List and the RREQ Table [28].

3.3.4 Positioning Techniques

The RDMAR extension proposed here is critically dependent on the ability of network nodes to determine their positions because in the absence of such information, the protocol falls back to its original form. A number of methods have been proposed to determine the location of mobile nodes. Some of them are briefly summarised here.

The Global Positioning System (GPS) [29] is undoubtedly the most widespread means of obtaining position information. In GPS-based positioning, a node receives radio signals from multiple satellites and then applies triangulation to estimate its position, with an accuracy of 10m. GPS is an attractive option because of its accuracy and public availability. Nowadays, it is becoming increasingly common for mobile devices to have GPS functionality built-in. However, GPS suffers from some well-known limitations. The accuracy is significantly degraded when used indoors. GPS signals are subject to attenuation under adverse climatic conditions. A GPS receiver has its own radio for listening to satellite signals and will use battery power which is an important resource for nodes in mobile ad hoc networks.

A number of node positioning techniques using wide-area cellular systems have also been proposed in literature. These are typically based on direction, time and strength of signals received from cellular base stations [30]. Each measurement defines a locus on which the node can be positioned and the intersection point of the loci from multiple measurements reveals the location of the node. The node position can then be estimated by triangulation. The Time Difference of Arrival (TDOA) technique uses difference in propagation delays of the signals from the transmitter(s). In [31], a technique is proposed for mitigating the error in TDOA-based estimation of mobile position by using the direct link-up ability of the node in a hybrid ad hoc cellular system. This method uses nearby nodes with position information and direct linking ability to the targeted node to assist in positioning.

The proliferation of Wireless LAN (WLAN) has led to the development of several methods for node positioning based on measurements of radio signals from Access Points (APs). However, most of them are primarily targeted at indoor positioning. One such technique based on WLAN is discussed in [32] where a radio map is created after measuring the signal strengths of APs at different points within a building. The signal distribution is used to train a position-determination model. Mobile nodes employ this model to estimate their positions. A client-based WLAN indoor positioning technique is presented in [33]. It proposes enhancements to triangulation-based indoor positioning in WLANs using a radio propagation model to take into account signal distortion because of obstacles.

The Ad hoc Positioning Systems (APS) [34] is a distributed node positioning technique designed specifically for ad hoc networks. This method assumes the existence of at least 3 nodes (referred to as *landmarks*) which have access to GPS or some other wide area positioning method. These nodes can be stationary or mobile. Information about positions of the landmark nodes is distributed across the network via exchange of messages between one-hop neighbours. Once a node knows the positions of 3 or more landmark nodes, it is able to determine its own location.

In theory, any of the techniques mentioned above can be used for node positioning as long as the necessary conditions are met. Nodes in an ad hoc network situated in a building with WLAN can use one of the indoor WLAN-based positioning methods. Similarly, in outdoor scenarios, GPS can be used if all nodes are equipped with receivers. Otherwise, the APS could be deployed if only some of the nodes have GPS capability.

3.4 Performance Evaluation

The position-assisted routing extension for RDMAR is aimed at reducing control overhead incurred during route discovery procedures without affecting the route acquisition delay significantly. Its impact on RDMAR's performance has been investigated using simulation modeling. In the following, first the simulation environment is described and then, results of the simulation are presented and discussed.

3.4.1 Simulation Environment

The tool used for performance evaluation was GloMoSim [35]. The simulation model comprised a MANET consisting of 50 nodes distributed randomly over an area of $1000m \times 1000m$. All nodes are assumed to have the same transmission range and are considered to be similar in all other respects. Nodes move within the simulation area according to the well-known (and widely used by the ad hoc network research community) Random Waypoint mobility model. At the start of a simulation run, nodes are placed randomly in the simulation area and thereafter, each node selects a random position and moves towards it independently in a straight line with a fixed speed, selected from a predefined range. Once the destination is reached, it stops there for a pre-determined *pause time* and at the end of this period, another destination is selected and the process is repeated. Each node has a 802.11b radio, operating in *ad hoc* mode. Furthermore, the free space channel propagation model is used. The investigation focusses on two performance measures:

- **Control Overhead**: The number of control packets.
- **Route Acquisition Delay**: Time taken by a node to discover a route to a destination node.

During each simulation run, 15 application sessions were established between different source-destination pairs. The session start times were staggered and all sessions continued until the end of the simulation. Each session generated Constant Bit Rate (CBR) traffic at the rate of 4 packets per second with each packet of size 64 bytes. These parameters have been chosen after a careful study of several simulation studies of ad hoc routing protocols [36][37]. The simulation duration was set to 300 seconds.

The results presented here for each scenario were averaged over 50 simulation runs, each with a different seed.

3.4.2 Simulation Results

The first set of results shows the control overhead (in terms of number of packets) for the native RDMAR protocol and the extended version. For each case, the signalling overhead due to route discovery and maintenance procedures was measured. Figure 3.9 illustrates the overhead as a function of node speed when the transmission range is set to 200m. In this figure (and those that follow in this chapter), the legend 'RDMAR+' refers to the results for extended RDMAR.The minimum node speed is set to zero in this simulation. Although the overhead rises with speed for both versions of the protocol, it is clear that position-assisted routing helps reduce overhead.

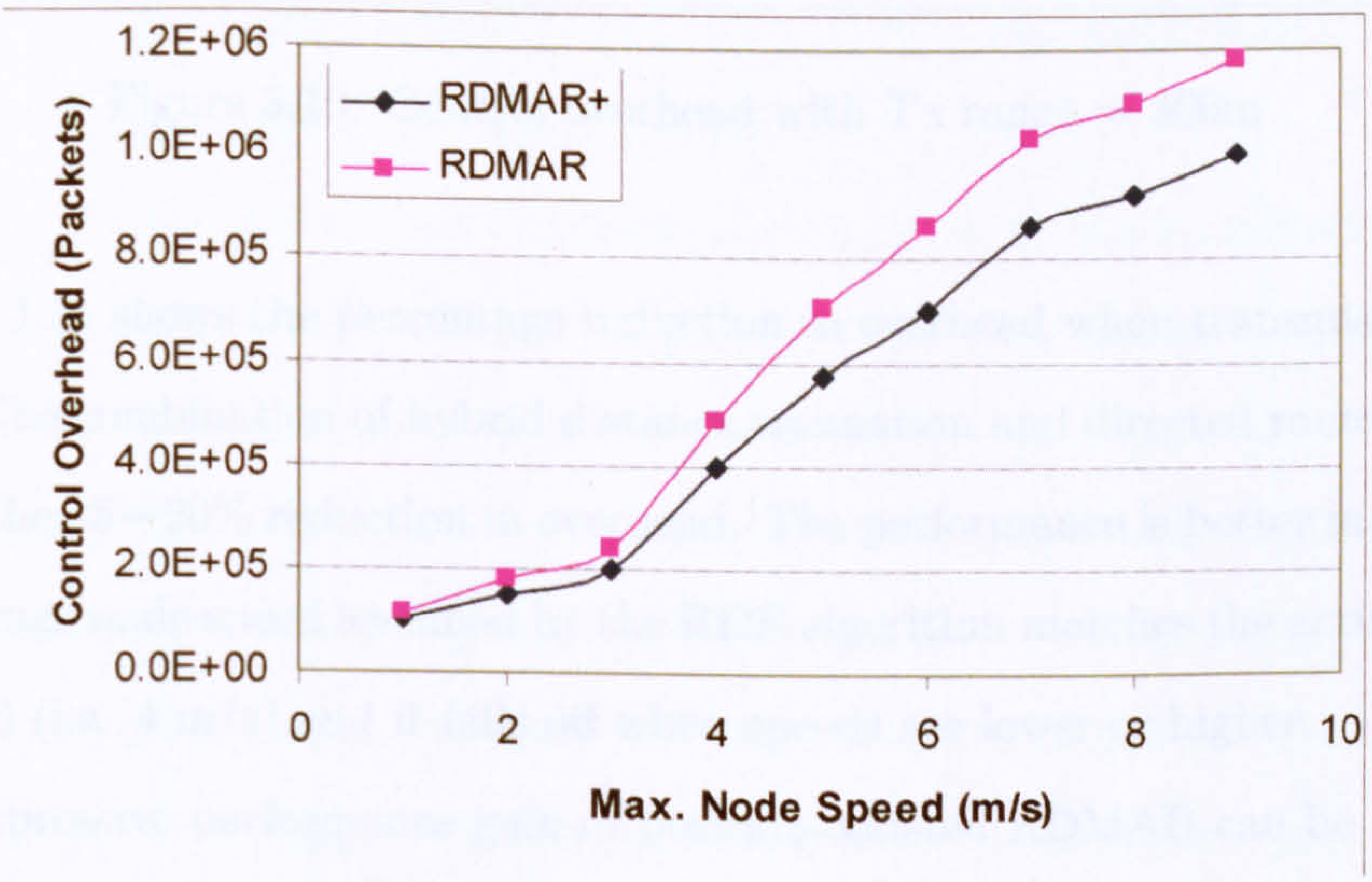


Figure 3.9: Control overhead with Tx range = 200m

Further simulations with the transmission range set to 300m confirm these findings, as evident from Figure 3.10. The actual overhead is slightly lower at higher transmission ranges but the general trend is the same.

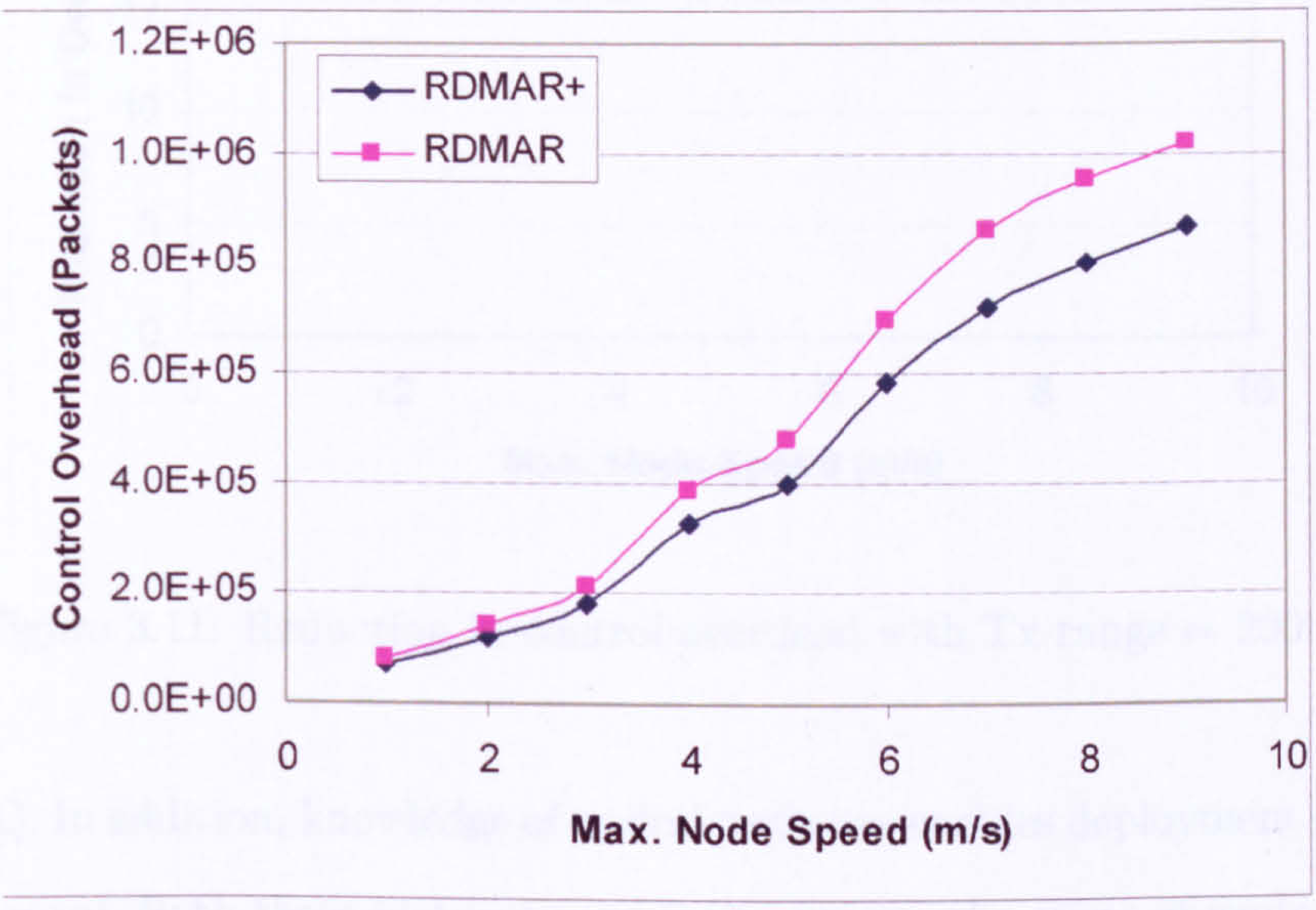


Figure 3.10: Control overhead with Tx range = 300m

Figure 3.11 shows the percentage reduction in overhead when transmission range is 200m. The combination of hybrid distance estimation and directed route discovery results in the 15 – 20% reduction in overhead. The performance is better in the region where average node speed assumed by the RDE algorithm matches the actual average node speed (i.e. 4 m/s) and it falls off when speeds are lower or higher.

The impressive performance gain of position-assisted RDMAR can be attributed to the twin-effects of improved distance estimation and increased localisation of route queries. Use of position information decreases the level of uncertainty in distance estimation which, in turn, increases the chance of reaching the destination with the

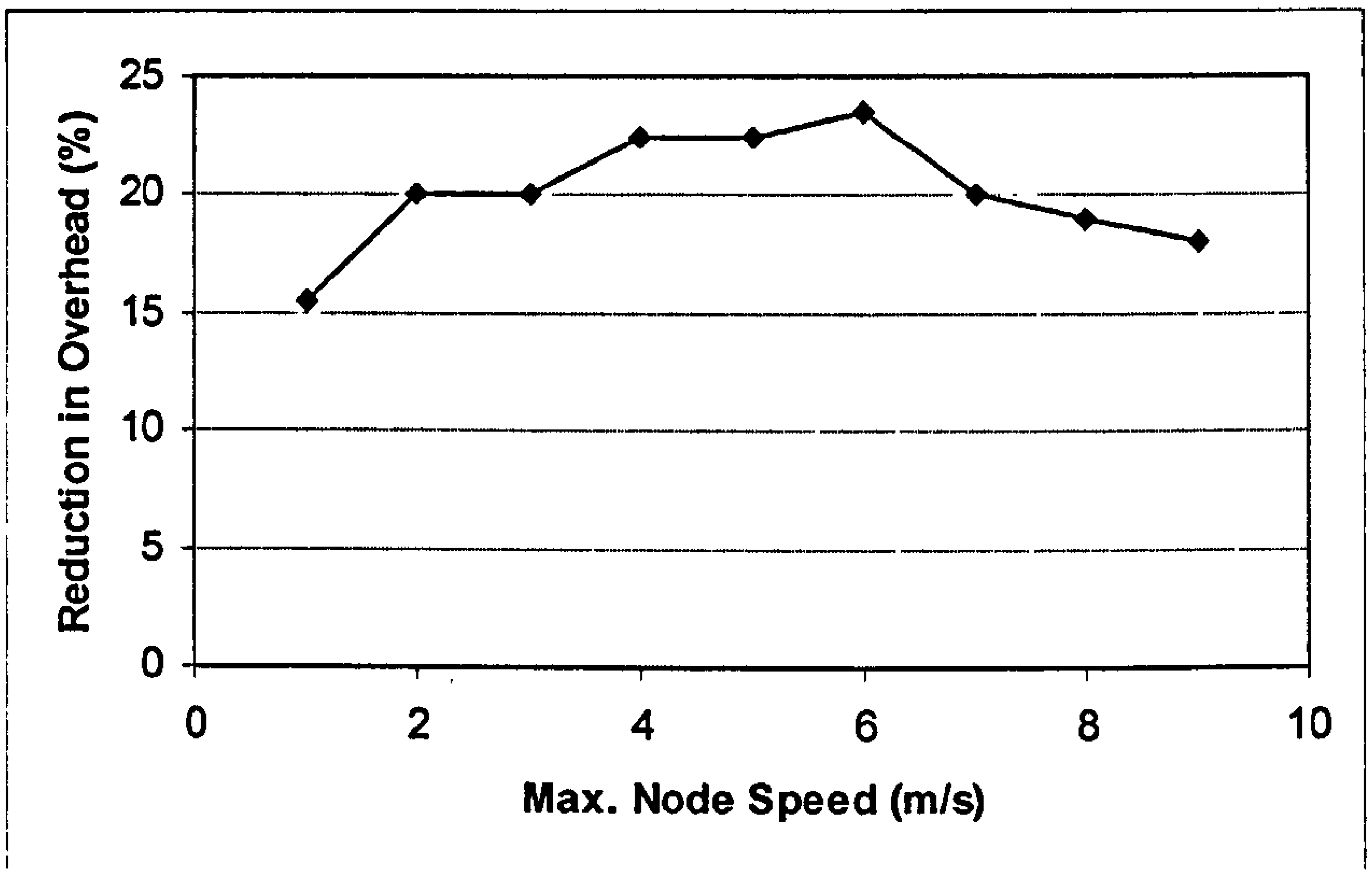


Figure 3.11: Reduction in control overhead with Tx range = 200m

first RREQ. In addition, knowledge of nodes' positions enables deployment of directed route discovery. Both these features combine to narrow the scope of route discovery. The net result is a decrease in control overhead.

Reduction in control overhead in itself is good but it is also important to look at route acquisition delay to get a better idea of the overall protocol performance. Figure 3.12 shows the average route acquisition delay plotted as a function of maximum node velocity. The delay initially decreases as node speed is increased and after reaching a minimum, it starts going up. Both versions of the protocol exhibit this trend. The main reason for this behavior is the inability of the distance estimation algorithm to make accurate estimates when the difference between node speed and the assumed *Micro_velocity* is large. As both RDE and HDE assume the same value for this parameter, they are more or less equally affected. The best performance is

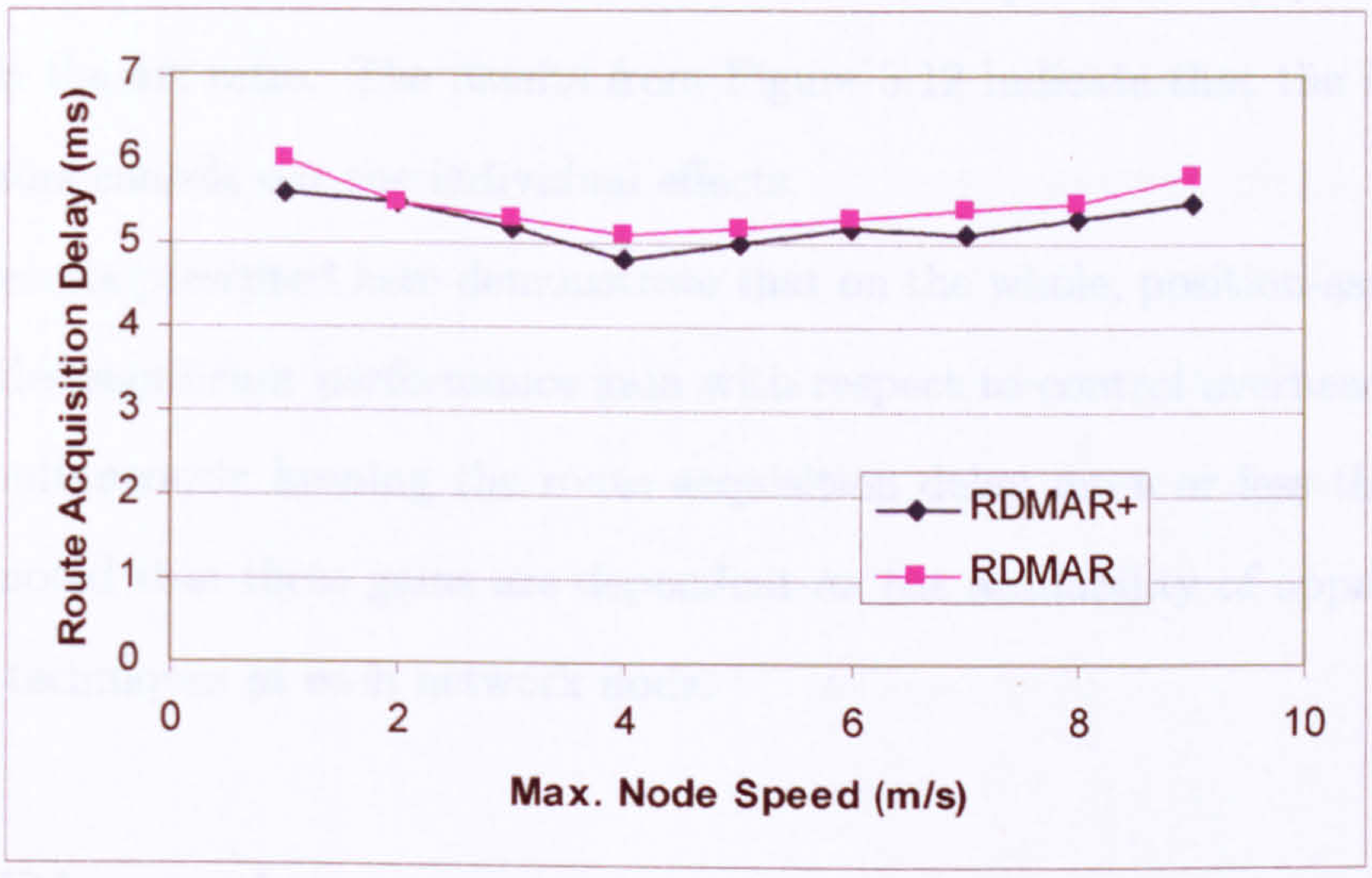


Figure 3.12: Average route acquisition latency

achieved when the average node speed is the same as the assumed node speed. In the simulation model, *Micro_velocity* is set to 2 m/s. Therefore, the delay is minimum when maximum node speed is 4 m/s (resulting in average speed of 2 m/s).

Figure 3.12 does show a slight performance gain for position-assisted RDMAR. There are three factors that have a bearing on the time it takes a node to find a route to a destination. Firstly, the extra computations and processing involved in position-assisted routing introduce an extra delay element which is added to the route acquisition delay. Secondly, increased accuracy in distance estimate should result in better *hit ratio*. That is to say, an RREQ launched with TTL based on a more accurate distance estimate has a higher chance of reaching the destination before the TTL reaches zero. Therefore, nodes are less likely to require multiple route discovery cycles with increasing TTL values before a route can be found. Finally, directed route discovery does not allow certain nodes to forward RREQs which can have a negative impact on the hit ratio. The results from Figure 3.12 indicate that the interplay of these factors cancels out the individual effects.

The results presented here demonstrate that on the whole, position-assisted routing provides significant performance gain with respect to control overhead reduction while simultaneously keeping the route acquisition delay more or less the same. It must be noted that these gains are dependent on the availability of appropriate positioning techniques at each network node.

3.5 Discussion

In this chapter, the RDMAR protocol was extended by adding position-assisted routing which uses information about nodes' positions to improve the localisation property of RDMAR. The proposed extension consists of two features: Hybrid Distance Estimation and Directed Route Discovery. HDE is responsible for estimating the physical or relative distance between a pair of nodes, depending on the availability (or the lack of it) of node position data for the two nodes. When the current position of source node and a recent position of the destination are known, HDE estimates the new physical distance between them using the stochastic model of native RDMAR. HDE falls back to relative distance estimation when position information is not available. In both cases, the distance estimate is converted to hop count and inserted in the Time-To-Live field of the RREQ packet. Directed route discovery also uses position data to steer route request packets towards the region where the destination is expected to be found. The proposed extension aims at cutting down control signalling needed to establish and maintain routes between nodes.

Performance comparisons of the extended and original versions of RDMAR have been made using simulations. The results presented here show that modified RDMAR provides significant benefits by suppressing unnecessary signalling messages without degrading route acquisition performance. The observed gains exist only in the presence of position data. This assumption may not be true all the time. However, recent advances in node positioning mean that this technology is maturing and this combined with Moore's Law will ensure that mobile nodes have access to widely available and relatively cheap positioning techniques in the near future.

Chapter 4

Multipath Routing in Ad hoc Networks

4.1 Introduction

Routing in ad hoc networks has thrown up many challenging issues and intense research effort in this area has yielded a wide variety of MANET routing protocols, some of which were briefly described in Chapter 2. These protocols are designed to be lightweight, loop-free and quick to react in the face of topology changes due to mobility or other reasons. Most ad hoc routing protocols ([21][22][24]) use the shortest path metric for route selection. For reactive protocols, it means that route replies which result in longer routes are discarded. This approach has the advantage of keeping routing tables small. In addition, maintaining many routes to the same destination may not be useful in scenarios where topology is highly dynamic. The main disadvantage is that when a route breaks, ongoing sessions are disrupted while a new route is being discovered. Furthermore, having only one route between a given source-destination pair means that all the traffic generated during application sessions involving these two nodes has to use the same path, irrespective of the specific requirements of particular applications. Therefore, this *one-path-fits-all* approach is more suited to best-effort traffic. However, it is clear that like any other network, MANETs will also support applications that have different QoS requirements.

The alternative to shortest-path routing is to maintain multiple routes towards each destination. There are many potential benefits of this approach. Knowledge of multiple routes provides extra information about the network topology. This could be exploited to ensure that connectivity between nodes is maintained for a longer duration, on the average. Any increase in average connectivity directly translates into reduction in the number of route query attempts and thus, leads to lower control overhead. Another advantage of multiple paths is the possibility of using more than one route simultaneously, thus distributing traffic load and reducing congestion. Furthermore, maintaining multiple routes provides redundancy in the face of route failure. In this case, one of the routes is used to forward traffic while the rest are kept as backup. When the active route fails, one of the backup routes is used. Even if the backup route is longer than the failed route, it can be used for ongoing sessions while a shorter route is being discovered. In the worst case, the backup route itself may have become invalid since it was first discovered but this is no worse than having no available route except for a small increase in the duration for which ongoing sessions are disrupted. Bearing these considerations in mind, a multipath routing extension has been proposed for RDMAR to further improve its performance. In the following, first the related work in this area is discussed, followed by a detailed description of the multipath routing feature for RDMAR. Finally, results of a simulation study on the effect of multipath routing on RDMAR performance are presented.

4.2 Related Work

The idea of using multiple paths is not really new and first originated in the context of traditional circuit switched networks. Several proposals are found in literature for multipath routing in packet-switched networks. In OSPF [13], multiple paths to a destination can be selected by a router if they all have minimum cost and [38] presents a link-state algorithm in which loop-free multipath routing is enabled. The Diffusing Algorithm for Shortest Multipath (DASM) [39] has been proposed for establishing multiple loop-free paths between nodes. In DASM, each node maintains a destination-oriented acyclic graph. Each destination entry in the routing table stores the next hops for the shortest and second-shortest path. However, only the shortest path is used for routing traffic and the second route is deployed only when the first one fails. The AODV-Backup Routing (AODV-BR) protocol [40] is an extension of the AODV protocol [21] for supporting alternate path routing where a backup route is used when the primary route fails. The Multi-path Destination Source Routing (MDSR) [41] protocol adds a multipath extension to DSR protocol [22]. In MDSR, when a destination receives multiple route requests from the same source consisting of different sets of intermediate nodes (resulting in *disjoint* routes), it stores all the routes and informs the source about them by sending a route reply for each path. For each destination, the path first discovered is labeled as *primary* while the rest are called *secondary* routes. Only the primary route is used for data forwarding and when it breaks, one of the secondary routes is used. The proposal also includes an alternative strategy where intermediate nodes are also allowed to maintain alternate paths to the destination which they can use when their primary path is disrupted. Graph Multi-path Routing (GMR) [42] is another DSR-based protocol. It follows the same principle as MDSR except that in this case, intermediate nodes collect route requests from the source and forward a single request containing all the paths obtained from the RREQs. This increases the chances of discovering *node-disjoint* routes. Split Multipath Routing (SMR) [43] is also derived from DSR. Unlike GMR, this protocol allows intermediate nodes to forward duplicate requests for the same destination. The destination selects the route obtained from the first route request as primary and then analyses the other requests to find the *maximally* disjoint route relative to the primary path and informs the source about both the routes.

Analytical results in [41] show that use of multiple paths can improve the performance significantly but this gain is reduced as the number of paths and/or length of the paths increases. In [44], the impact of using alternate routes for load balancing is analyzed with end-to-end delay as the performance criteria. A significant improvement was seen with multipath routing but the gain was affected by network topology and channel characteristics. The works cited above do not take into account the type of traffic itself and most of the algorithms presented are evaluated for UDP traffic. The performance of TCP over multipath routing was analyzed in [45] and results indicate that splitting TCP traffic over multiple paths results in degradation of performance, but use of alternate paths as back up routes is a better way of utilizing multiple routes.

4.3 Multipath Routing Extension for RDMAR

The original RDMAR protocol is based on shortest (single) path routing. In other words, during route discovery, the destination node replies only to the first route request from the source and all further RREQs from the same source and with the same sequence number are discarded. Therefore, the source and destination nodes end up with one route each, in either direction. During the course of an application layer session between them, when one of the links in the path fails, a new route discovery phase is started. It is clear from the discussion in the previous section that multipath routing can help mitigate the effects of frequent link breaks by providing alternate paths when the route currently in use becomes unavailable. Furthermore, this strategy may even reduce control overhead by suppressing unnecessary route requests. However, discovering multiple paths can also add to the signalling overhead. For example, in the DSR-based multipath routing protocols cited above, the destination has to send either multiple route replies or put multiple source routes in a single route reply, resulting in increased amount of signalling bits exchanged between nodes. Furthermore, in some protocols, route acquisition delay is increased. For example, in GMR [42], intermediate nodes accumulate route requests and then forward the collected routes in a single route request. Clearly, this adds to the delay as intermediate nodes wait for a finite period of time for several requests to arrive before processing them. Similarly, in MSR [46], the destination accumulates route requests before choosing the shortest path and the maximally disjoint alternate path.

The motivation for adding multipath routing to RDMAR is twofold. First, there are clear advantages of using multiple routes. Second, unlike many other reactive protocols, RDMAR was designed to localise route discovery and results show that it is successful in reducing control overhead [3]. In addition, the extensions proposed in the previous chapter have further reduced the overhead by narrowing the scope of discovery to a greater extent. Therefore, RDMAR is better-suited to cope with any potential increase in overhead when multipath routing is added.

The multipath routing extension is implemented on top of position assisted routing. There are three main elements of multipath RDMAR: Route Acquisition, Application Data Routing and Route Maintenance, as discussed below.

4.3.1 Route Acquisition

The route acquisition process of native RDMAR was designed to discover the shortest path to a destination. The protocol stipulates that when an RREQ is received by the destination, the sequence number is checked first and if it turns out to be a new request, the reverse route to the source is stored and an RREP is sent to the source. Subsequent RREQs received by the destination from the same source with the same sequence number are discarded. To implement multipath routing, this rule is relaxed. The destination is now allowed to reply back to more than one RREQ from the same source with the same sequence number but only if the previous hops of these requests are different. This rule ensures that the newly found routes are disjoint in least one link. When the destination starts replying to more than one RREQ from the same source, it will result in higher control overhead which is clearly undesirable. Keeping this in mind, intermediate nodes are allowed to forward only the first RREP they receive from the destination. However, intermediate nodes use the subsequent RREPs to create multiple routes to the destination. In this way, a set of multiple routes are established. The number of discovered paths depends on the network topology. It is not unreasonable to expect that sometimes only one route maybe discovered, especially when the network is sparse. The formal description of the route acquisition procedure is given below.

Route Request

The source node, say S, receives application data from higher layers to be sent to the destination, say node D. The local routing table is searched to find available route(s) to the destination. Assuming that no route is found, an RREQ message is created and broadcast. All the first-hop neighbours of node S receive the message and broadcast it to their neighbours. This way the request propagates towards the destination according to the normal RDMAR procedure, described in the previous chapter. Before forwarding, each node makes sure by checking the sequence number that it has not processed the same message before to eliminate duplicate RREQs.

Route Reply

Node D receives one of the possibly many RREQs originating from node S. The first RREQ is assumed to yield the shortest path. This is not unreasonable barring catastrophic congestion at some intermediate node which can delay the RREQ traversing the shortest path. Such a situation is not improbable but it is highly unlikely. Node D stores the shortest path and immediately sends an RREP back to the source. This ensures that route acquisition delay is no worse than in original RDMAR. When another RREQ is received later on from the same source with the same sequence number as before, node D compares the address of the node which forwarded the RREQ with the address of the next-hop node for the shortest path to node S. The RREQ is discarded if the addresses are same; otherwise, the hop count is compared with that of the shortest path. If new hop count is either equal to the length of the shortest path or longer by one hop, then another route is added to the routing table and a fresh RREP is sent towards the source. This strategy limits the number of routes and also make sure that the difference between the path lengths is not greater than one. At an intermediate node, the first RREP sent by node D is processed as per normal: a route to node D is installed in the routing table and the RREP forwarded towards the source. When another RREP is received for the same source with the same sequence number as before, the route is added to the table but the message is discarded. This limits propagation of RREPs and also increases disjointness of routes available at the source. At node S, multiple routes based on received RREPs (with the same sequence number) are stored in the routing table. Figures 4.1 and 4.2 illustrate the route acquisition procedure.

Figure 4.1 shows the first phase where node S initiates Route Discovery by sending an RREQ towards node D. This request progresses onwards as per the normal RD-MAR procedure. The arrows indicate the flow of RREQ messages via intermediate nodes.

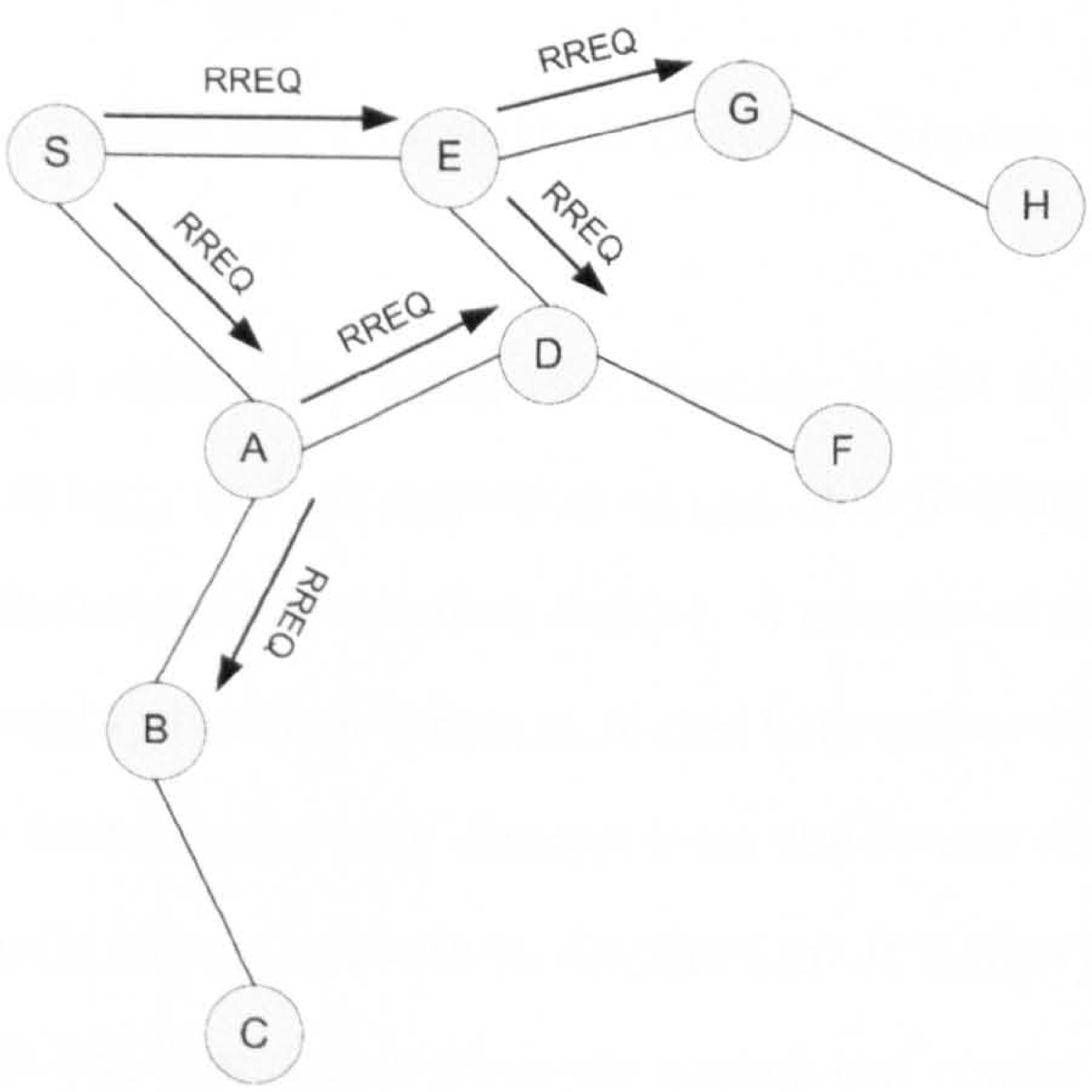


Figure 4.1: Propagation of Route Requests

As shown in Figure 4.2, when the RREQ is received by the destination, it sends back two RREPs, via nodes A and E respectively. Thus, node S is able to discover two valid routes to the destination.

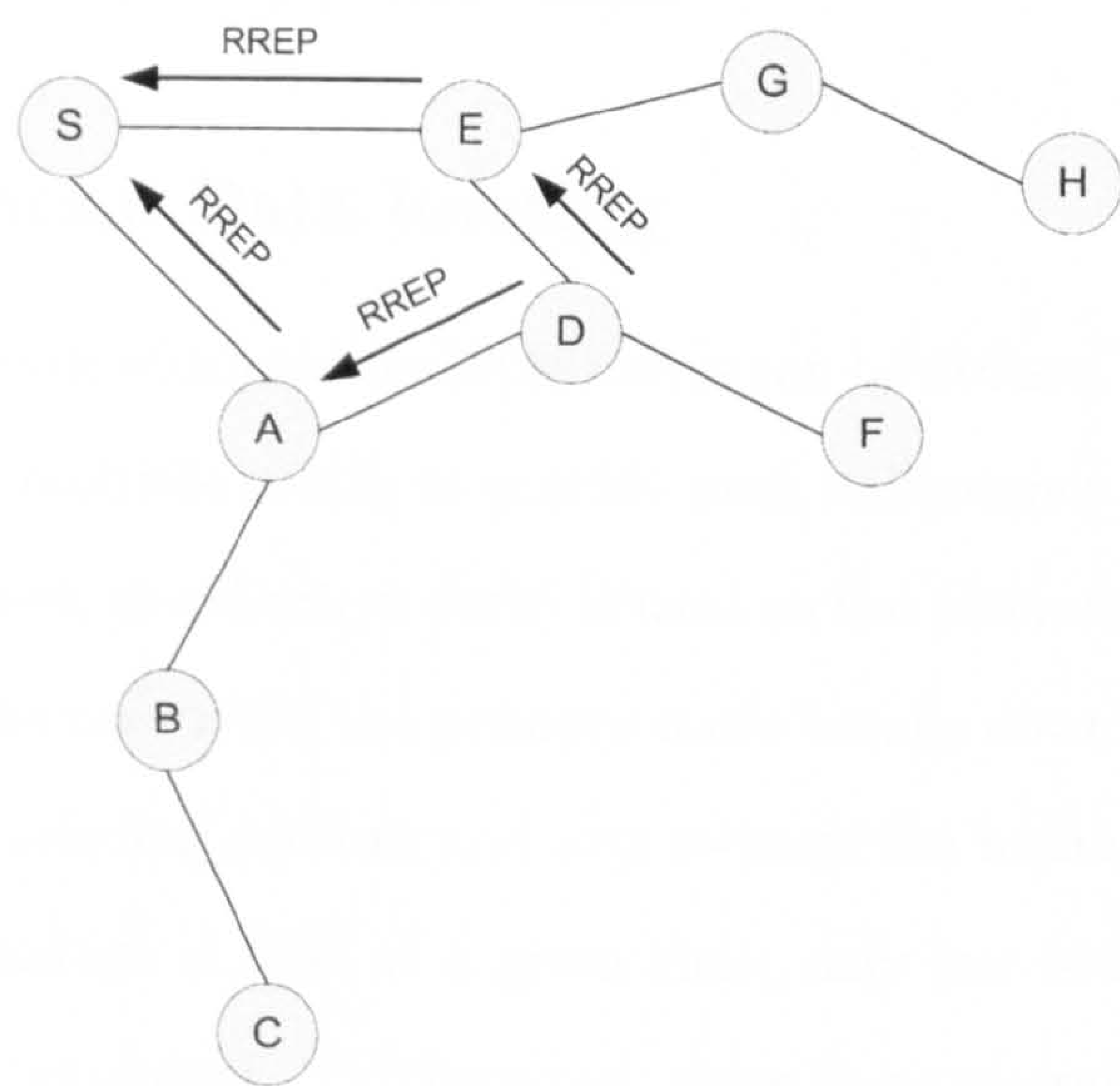


Figure 4.2: Propagation of Route Replies

The multiple paths discovered using this strategy might not be totally disjoint. Depending on node density and transmission ranges of individual nodes, it is possible that two or more paths may share common link(s). A number of possibilities exist with regards to the relationship between different routes between a source-destination pair. For example, two or more routes may diverge from the source and then join again at some intermediate node along the route to destination. It is also possible that there is only one link towards the destination from the source but routes start diverging from some intermediate node and meet again at the destination. Another possibility is the existence of routes that diverge at some intermediate node and converge again at another intermediate node downstream. In general, the end result of route discovery will be a mixture of such cases. The route acquisition procedure does not provide any explicit mechanism to ensure that the different paths are disjoint. This is done primarily to keep the discovery process simple.

4.3.2 Application Data Routing

There are many ways in which the multiple routes can be utilised. GMR, MSR, MDSR and AODV-BR use multiple routes to provide path redundancy. In other words, one of them (in most cases, the shortest path) is used as the *primary* route while the rest act as backup for the case when the primary route breaks down. This strategy helps avoid disruption of ongoing sessions and also reduces the number of route discovery cycles. The disadvantage is that at a given time, only one route is used and other routes are not fully exploited. Furthermore, there is no guarantee that the backup routes will be available when required unless there is some mechanism to refresh those routes whilst they are in inactive state. Note that most reactive protocols (including AODV and DSR) do not have an explicit route refresh method and use incoming data packets to refresh corresponding routes.

A second option is to 'grade' routes based on some quality metric and use different routes for different types of traffic, based on its requirements. Routes can be ranked on the basis of link quality, congestion level etc. However, this approach will require measurement or estimation of the quality parameter in question. Although there are ways to acquire such knowledge for the local link, using it end-to-end will require some mechanism to share the quality information with end nodes. This is not only difficult to achieve in MANET scenarios but also adds to the control overhead.

Another option is to use two or more available paths simultaneously for routing application data, primarily motivated by load-balancing considerations. This approach fully utilises all available paths, simultaneously ensuring that they stay refreshed. The disadvantage is that packets travelling through different paths may arrive at the destination out of order which may create problems for certain types of applications.

Instead of selecting one routing method for all types of traffic, the multipath version of RDMAR adopts a more sophisticated approach. Considering that TCP and UDP are the two dominant transport protocols used in the Internet, application data is divided into two classes according to the underlying transport protocol and then different route selection algorithms are applied for each data type.

UDP packets destined to a particular node are routed using a subset of the available paths which consists of routes with the shortest and second-shorted lengths. Routes are selected on a per-packet basis according to a round-robin scheme. It is assumed that there are sufficiently large buffers at the destination so that if some packets arrive out of sequence, they can be reordered. As the difference between the different paths is limited to one, the delay jitter will also be small. This is crucial for applications that are sensitive to delay and jitter, such as VoIP and video conferencing etc.

As pointed out earlier, an intermediate node sends only one RREP back towards the source. The implication is that in some cases, the source may not know that multiple routes exist and only intermediate node(s), where routes diverge, knows about it. Thus, it is not possible to choose the route simply at the source. Therefore, the responsibility for route selection is distributed over all the intermediate nodes along the route. Thus, if the source node has only one outgoing link to the destination but there is a node downstream having multiple routes to the destination, it is allowed to distribute packets over the multiple routes. If there is more than one such node, each of them applies the same rule. In this way, the packets are routed all the way to the destination.

Consider a node, say S, that wants to send a UDP packet to node D. Assuming that route discovery has already taken place, node S will search its route table to retrieve a route to D. The shortest path to node D is selected and the packet forwarded to the corresponding next hop and the route is marked as *used.* When the packet arrives at the next hop node, say N, it also searches the local routing table to find the shortest path to D that is not marked as used. The packet is forwarded to the next hop and the route marked as used. The procedure is repeated until the destination is reached. At node S, when the next UDP packet is generated by some application, it selects the next path (with length equal to the shortest path or one hop longer) to route this packet and then marks it also as used. Similar steps are taken at each intermediate node. When a node finds that all available routes have been used, then all the routes are unmarked and the shortest one is selected and remarked. This round-robin scheme is implemented at each intermediate node.

Routing TCP traffic in itself is a very challenging task in ad hoc networks because the unique characteristics of such networks like dynamic topology, fluctuating channel conditions and access contention have an adverse impact on TCP connections. The main reason for this degradation lies in the congestion control mechanism of TCP, originally designed for wired networks. In ad hoc scenarios, packet losses are frequent because of collisions and link breaks and this can trigger TCP to go into congestion avoidance phase. This is in addition to window reductions caused by actual congestion in the network. The condition is especially severe when there is a link break because it will lead to packet loss over a long period of time. Furthermore, TCP is also sensitive to round trip time (RTT). Routing TCP traffic on multiple paths simultaneously will impact the accuracy of the average RTT calculation algorithm. Finally, if packets use different paths, they may reach the destination out of order and thus, result in duplicate ACKs.

Bearing these considerations in mind, only one path is used at a time for TCP traffic and the alternate path(s) become active only when the main route fails. This will eliminate the problems associated with RTT as well as reduce the chances of out of order packet delivery. Thus, in case of TCP traffic, the shortest path is designated as the primary route and all data packets are routed on this path as long as it is active.

4.3.3 Route Maintenance

When a link break occurs on a particular route, the affected node inactivates the broken route. For UDP traffic, this means removing the affected route from the round-robin scheme and for TCP traffic, this means using the next best route. However, as long as at least one other route is available, no other action is required. The Failure Notification(FN) procedure is invoked only when either the source or an intermediate node has no route left to the destination. Although the procedure is same as in original RDMAR, there is one significant difference. At an intermediate node, when there is no route left to the destination, it sends a FN message towards the source. When this message is intercepted by another intermediate node (in the direction of the source), the notification is forwarded to the source only if this node also does not have any other route left to the destination. Thus, the impact of a local route failure is localised and at the same time the redundancy provided by multiple paths is exploited fully.

4.4 Performance Evaluation

The multipath routing extension for RDMAR has been designed to improve the overall protocol performance. The desired effect is reduction in control signalling overhead and increase in throughput as a result of higher route availability. A simulation analysis was done to determine whether multipath RDMAR performs as expected. The simulation environment was similar to the one described in the previous chapter. The scenario consisted of a MANET of 50 mobile nodes distributed randomly over an area of $1000m \times 1000m$ with transmission range set to 250m. Each simulation ran for 300 seconds and each data point in the graphs below represents the average over 50 simulation runs. The maximum node speed is 4 m/s and pause time is 30 seconds, unless otherwise stated.

Packet delivery ratio (PDR) and control overhead are used as performance indicators. PDR is defined as the ratio of data packets delivered to the destination to those generated by the source, expressed in percentage. Control overhead is the ratio of signalling messages created to the number of data packets generated by each node. All RREQ, RREP and FN messages are counted as part of the overhead.

The first set of results are for UDP traffic. During each simulation, nodes take part in CBR sessions characterised by packet rate of 10 per second and packet size 64 bytes. The sessions are staggered in time to avoid synchronisation effects. The PDR and control overhead are measured under different network loading conditions created by varying the number of sessions in the network.

Figures 4.3 shows the PDR variation with network load. It indicates that the PDR of multipath RDMAR is consistently higher compared to the native protocol. As the number of sessions increases, the performance deteriorates for both. However, the multipath version clearly copes better with increasing network load. The main reason for this behavior is that high load levels lead to increased bandwidth contention because many nodes attempt to transmit data packets over the same channel. By distributing load along different paths, multipath routing results in more efficient use of bandwidth and also relieves congestion.

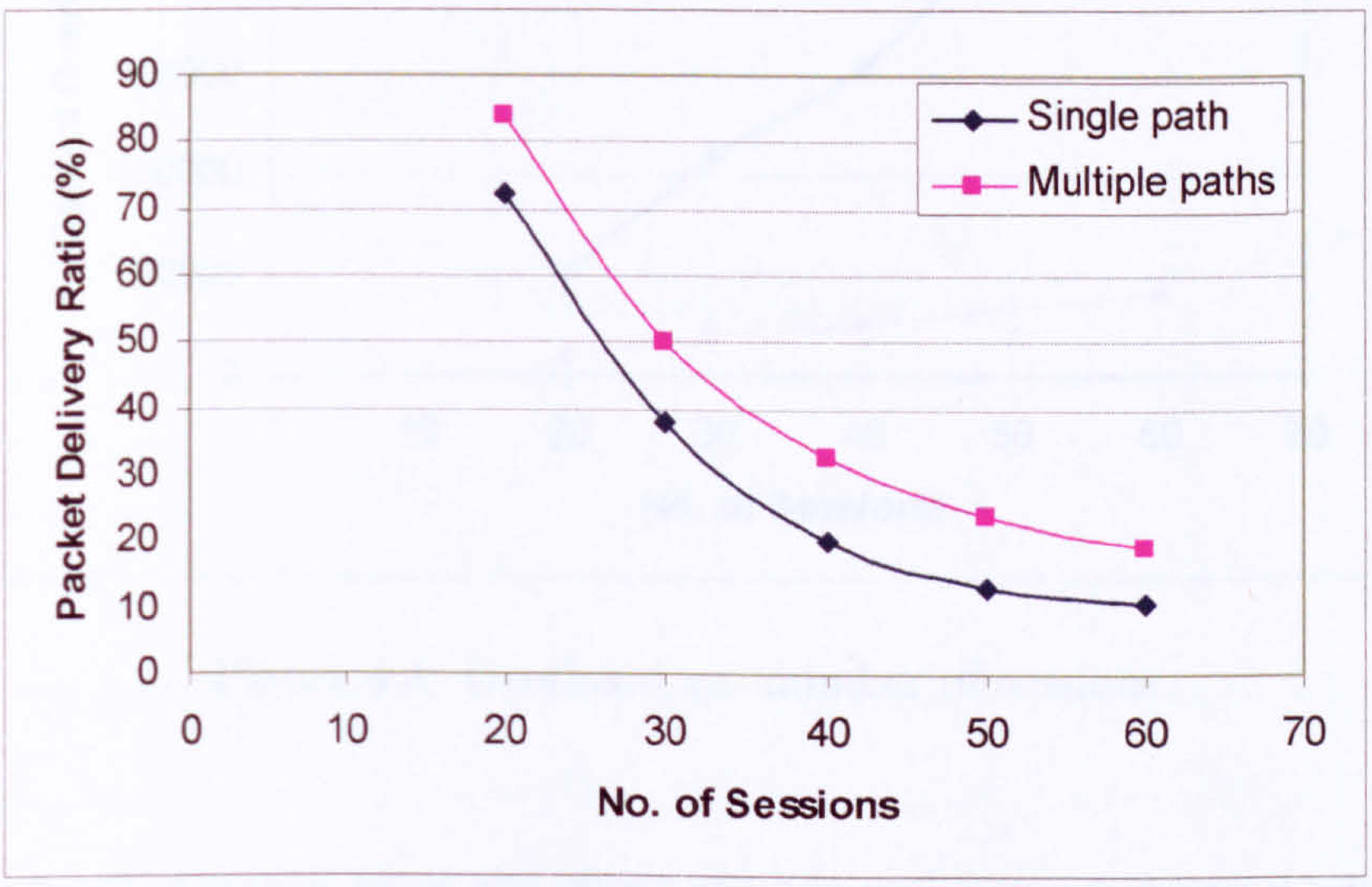


Figure 4.3: PDR vs. number of sessions

The control overhead from multipath routing is also much lower, as indicated by Figure 4.4. As mentioned earlier, when several paths are available, even if one of them fails, others may still be available to carry the traffic. Thus, the number of route discovery cycles is reduced. In contrast, every route failure results in a route discovery cycle when native RDMAR is deployed. As the number of sessions increases, more and more packets are dropped due to collisions. The MAC layer reads them as link failures and informs the network layer. The routing protocol then has to initiate a route discovery. Thus, increased network load contributes to more route failures and hence, signalling load of native RDMAR is much higher.

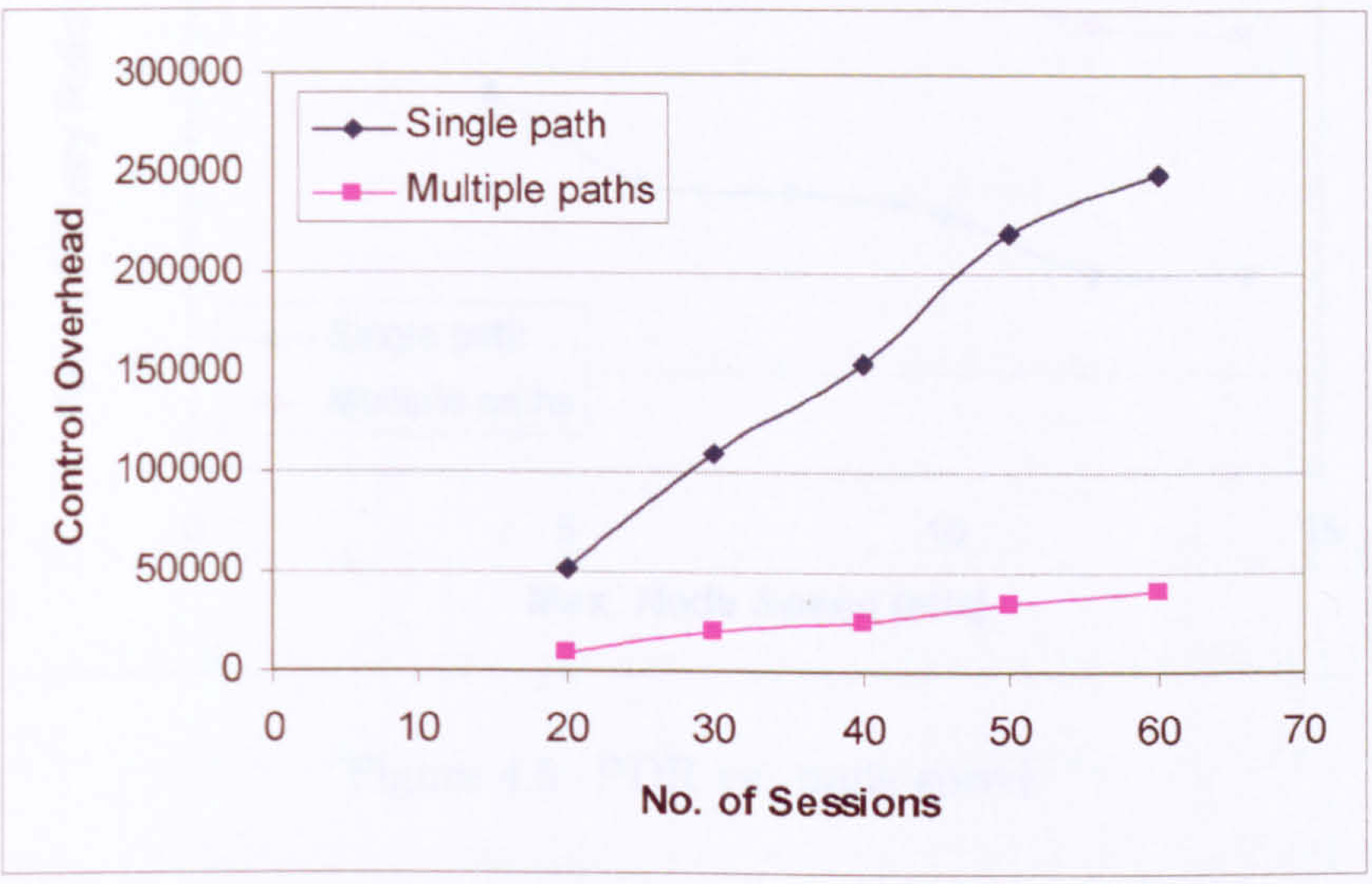


Figure 4.4: Overhead vs. number of sessions

The next set of results show the effect of node mobility on protocol performance. Mobility level is varied by changing the maximum node speed while keeping the minimum speed fixed (to zero). As per the Random Waypoint mobility model, incrementing maximum speed makes nodes more mobile as average speed is increased. During these simulations, pause time is set to 30 seconds. Furthermore, 20 application sessions are established between different node pairs at the beginning of a simulation and continue till the end.

Figure 4.5 shows the PDR as a function of maximum node speed. As speed increases, route disruptions become more frequent and hence the number of dropped packets goes up, leading to more retransmissions and reducing the PDR.

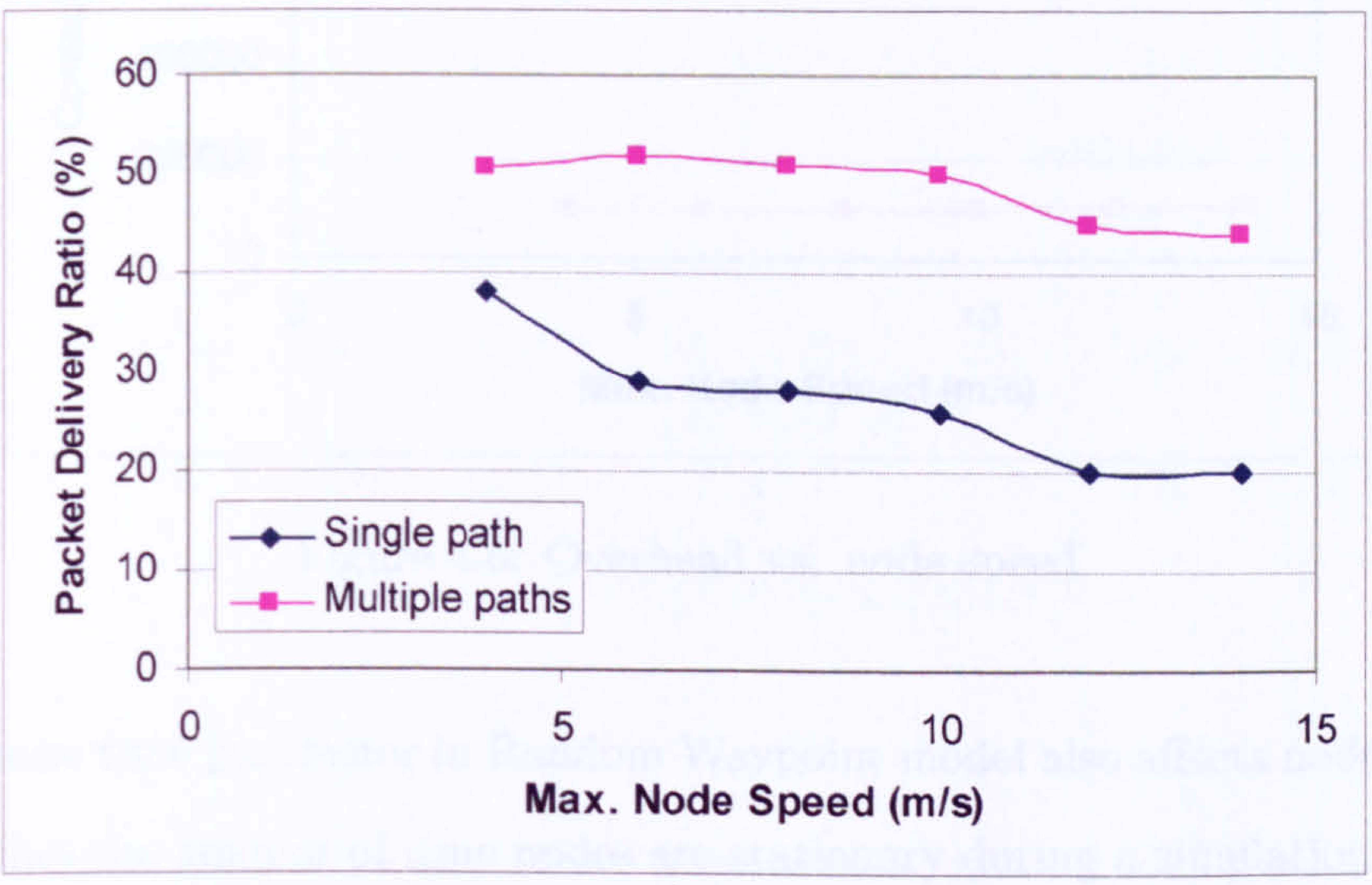


Figure 4.5: PDR vs. node speed

The same reason accounts for increase in overhead (see Figure 4.6). At high node speeds, route lifetimes are shorter, thereby requiring more signalling for route maintenance and discovery. It is clear from the results presented here that multipath RDMAR performs significantly better because it is able to handle route disruptions due to mobility more effectively by keeping PDR high while simultaneously limiting control overhead. It is important to note that the differences between the native and modified RDMAR are more pronounced at higher speeds.

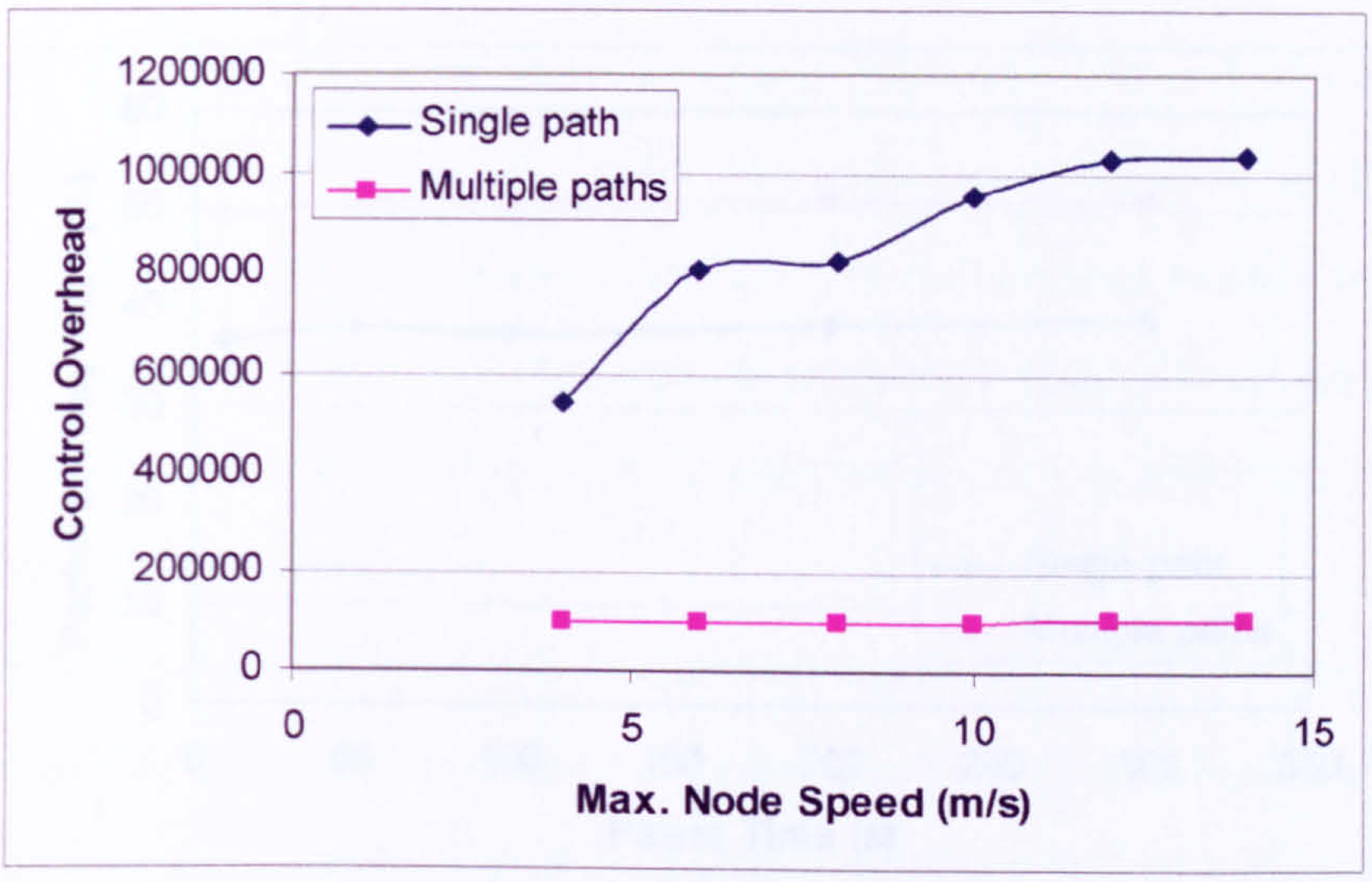


Figure 4.6: Overhead vs. node speed

The pause time parameter in Random Waypoint model also affects node mobility. It determines the amount of time nodes are stationary during a simulation. Another set of simulations was carried out to study the impact of pause time on the protocol performance. The node speed was set to 4 m/s. Once again, 20 applications sessions were established between different node pairs during each simulation.

Figures 4.7 and 4.8 indicate that the effect of pause time is marginal. The PDR stays almost unchanged as pause time increases and the same trend is observed in the case of control overhead. The reason for this behaviour is the interplay of competing forces. On one hand, higher pause times (low mobility) lead to fewer route breaks. On the other hand, when nodes are less mobile, the inherent load redistribution caused by changing topology is not so prominent. The effect of these two factors is canceled out. However, multipath RDMAR outperforms the native protocol.

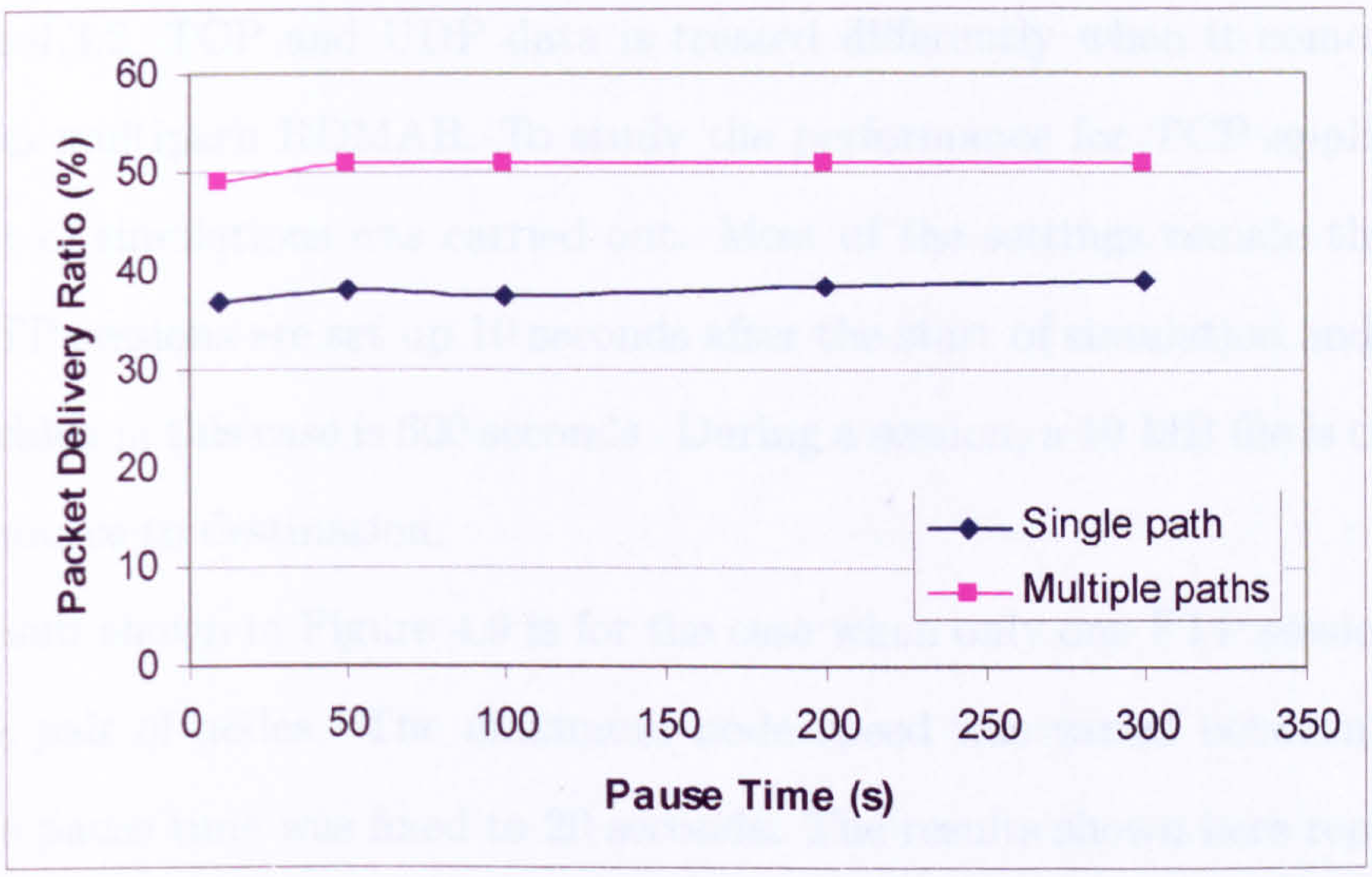


Figure 4.7: PDR vs. pause time

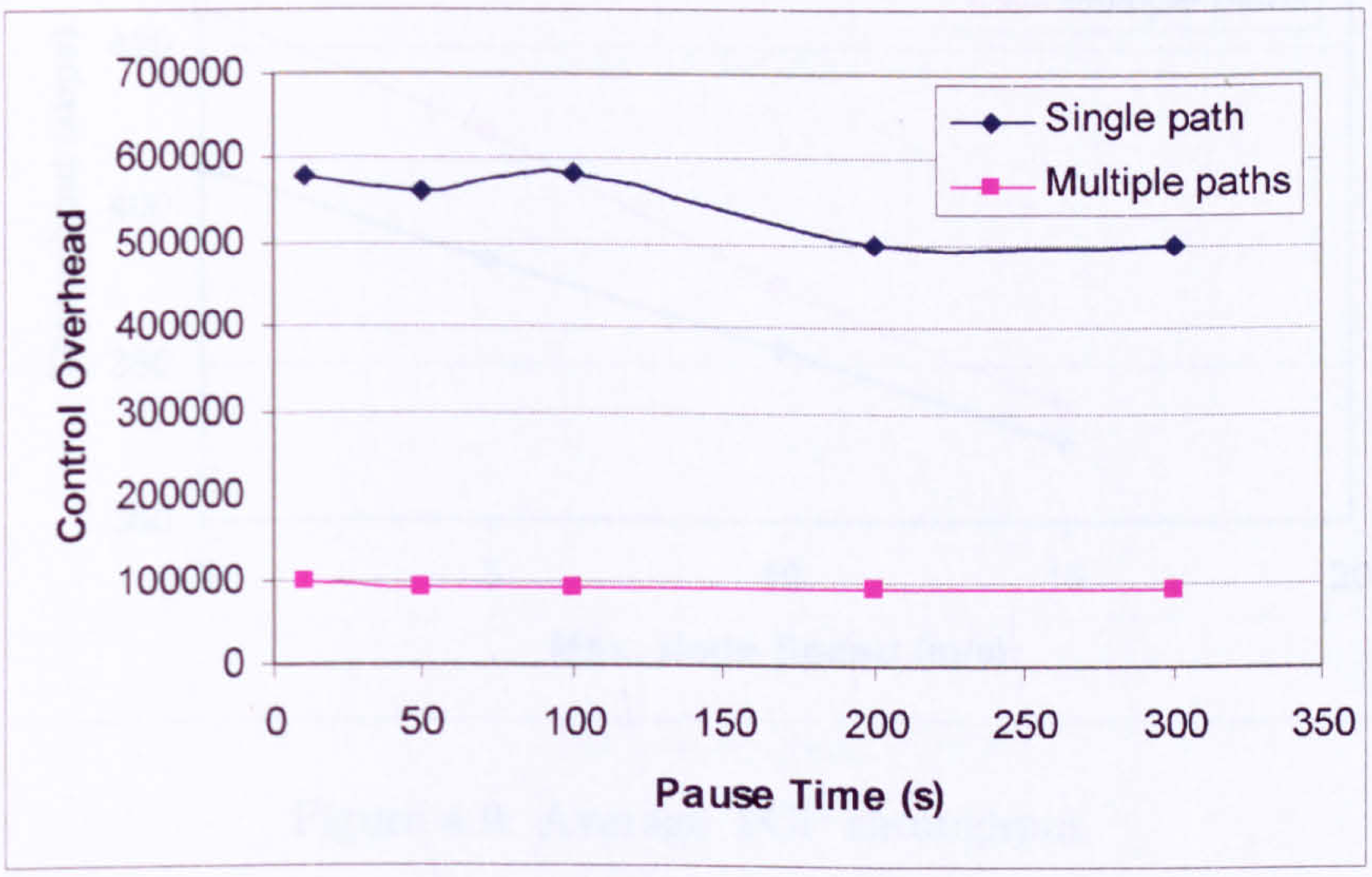


Figure 4.8: Overhead vs. pause time

The simulations have so far focussed on UDP-based applications. As described in Section 4.3.2, TCP and UDP data is treated differently when it comes to route selection in multipath RDMAR. To study the performance for TCP applications, a further set of simulations was carried out. Most of the settings remain the same as before. FTP sessions are set up 10 seconds after the start of simulation and last until the end, which in this case is 600 seconds. During a session, a 10 MB file is transferred from the source to destination.

The result shown in Figure 4.9 is for the case when only one FTP session is setup between a pair of nodes. The maximum node speed was varied between 0 and 15 m/s, while pause time was fixed to 20 seconds. The results shown here represent the average of 50 simulations runs.

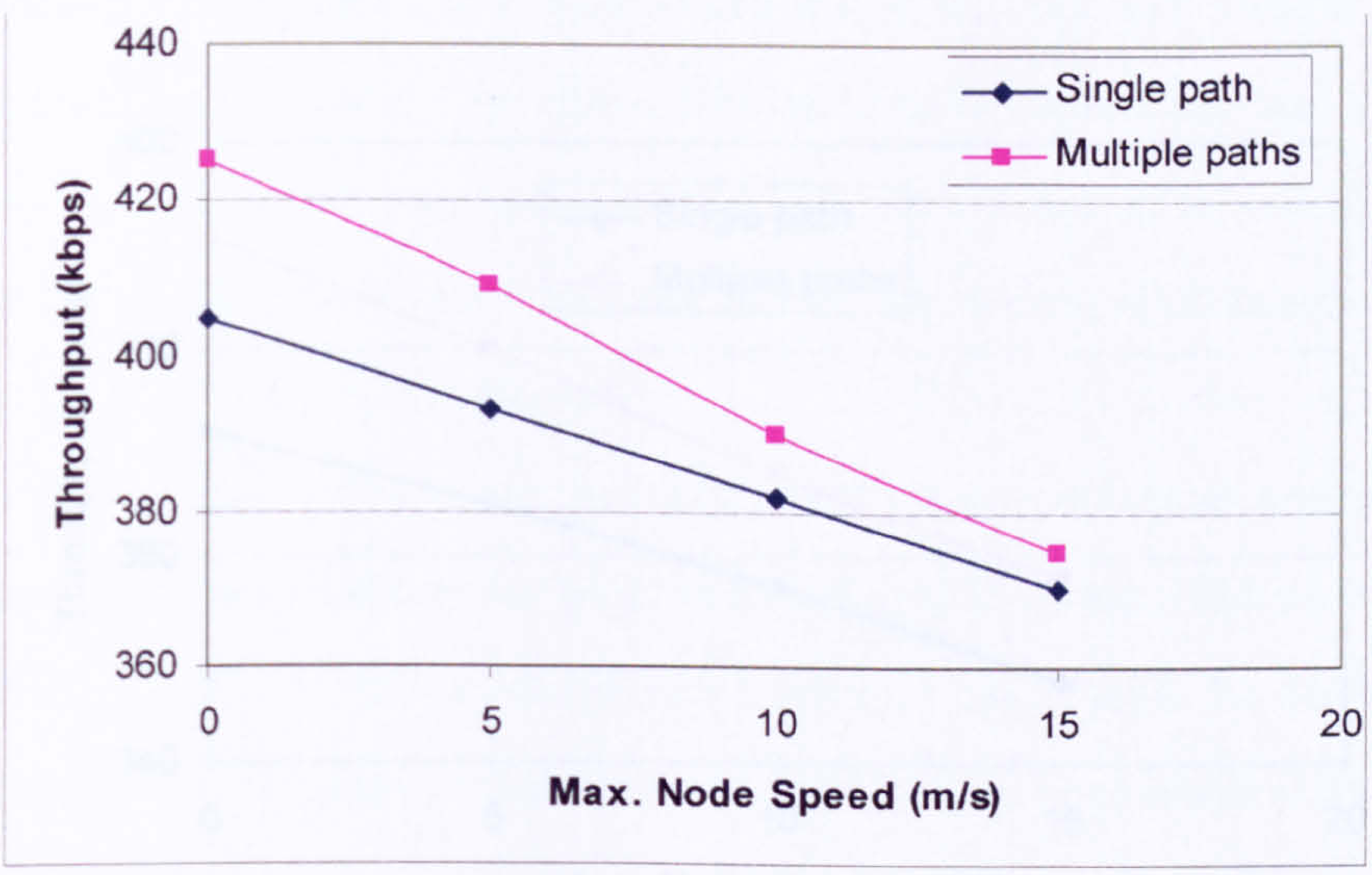


Figure 4.9: Average TCP throughput

The throughput decreases with node speed because of higher mobility. The throughput for multipath routing is generally higher and the difference in performance is more pronounced at lower speeds. A further set of simulations was done to study the effect of other ongoing sessions on the TCP throughput of a single session. Background traffic was introduced into the network in the form of three CBR sessions. These sessions, between three different source-destination pairs, are started 5, 10 and 15 seconds respectively, after the start of FTP session. The CBR sources generate 10 packets per second, each packet of size 64 bytes and the sessions continued till the end of simulation. The result of these simulations are shown in Figure 4.10. As a result of introducing CBR sessions, the TCP throughput drops but the general trend is almost the same. The performance of multipath RDMAR is again better compared to the native protocol.

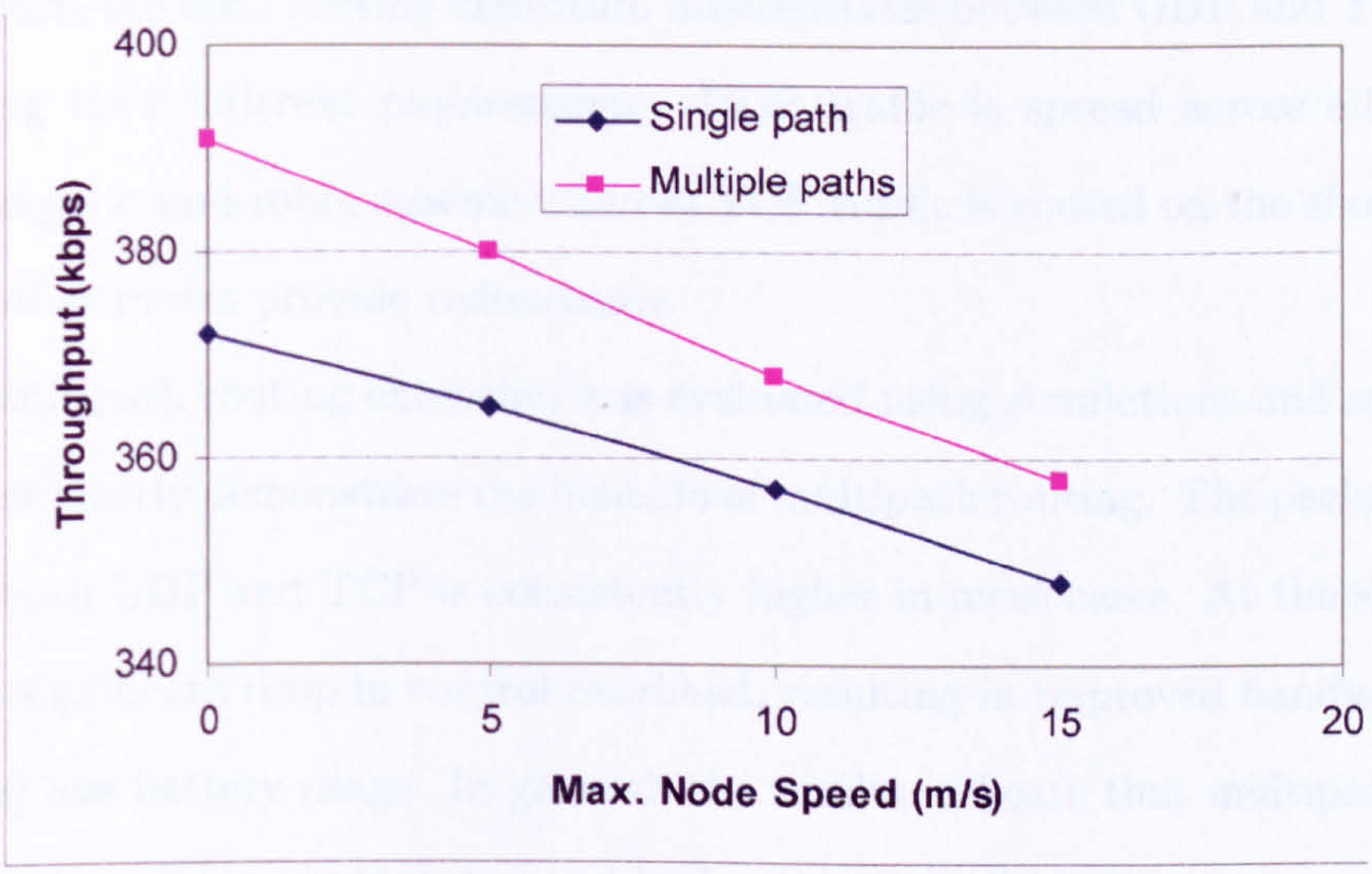


Figure 4.10: Average TCP throughput in presence of background traffic

4.5 Discussion

A multipath routing extension for the RDMAR protocol was presented in this chapter. It comprises three components:

1. Procedure for discovering multiple routes between nodes in an ad hoc network using RDMAR route request and reply messages;

2. Algorithm for routing application data;

3. Mechanism for handling route failures.

Each of these has been carefully designed keeping in mind the unique properties of ad hoc networks and requirements of different applications. In particular, the route discovery and maintenance procedures strive to limit the control overhead. Furthermore, the data routing algorithm differentiates between UDP and TCP traffic considering their different requirements. UDP traffic is spread across all available routes using a round-robin scheme whereas TCP traffic is routed on the shortest path and the other routes provide redundancy.

The multipath routing extension was evaluated using simulations and results presented here clearly demonstrate the benefits of multipath routing. The packet delivery ratio for both UDP and TCP is consistently higher in most cases. At the same time, there is a significant drop in control overhead, resulting in improved bandwidth utilisation and less battery usage. In general, the results indicate that multipath routing is able to cope with node mobility and high network load better.

Chapter 5

Capacity of Wireless Mesh Networks

5.1 Introduction

Wireless mesh networks have generated a lot of interest in recent years, both in the industry as well as the research community. These networks can potentially be used in a wide range of applications such as last-mile access, enterprise networks, Metropolitan Area Networks (MAN), transportation systems, video surveillance systems [4] [47]. WMNs can be deployed by Internet Service Providers for last-mile connectivity. In this case, one or more WMN nodes have wired Internet connectivity while the remaining nodes get network access via multi-hop wireless paths terminating at the wired nodes. The MAN scenario is realised by replacing the conventional wired backhaul with a city-wide WMN using wireless routers. Similarly, in the enterprise case, access points are connected together in mesh topology with a wireless backbone. In all these scenarios, replacement of wired infrastructure with WMN drives down the overall deployment cost. Furthermore, the resulting network is more flexible as wireless routers can be redeployed without any need for extensive re-cabling.

A common feature of the WMN deployment scenarios mentioned above is a wireless backbone connected to the fixed infrastructure via one or more wired links. This is the most commonly used mesh architecture, also referred to as *infrastructure* or *backbone* WMN. It consists of a set of nodes connected by wireless links, with one or more of the nodes directly connected to the global Internet. The latter are referred to as *gateways*. Nodes in a backbone WMN can be of three types: a) client devices such as PDAs, laptops etc. (configured to forward packets from/to other clients); b) wireless access points (to which client nodes attach) and c) wireless routers (can also have access point functionality). Wireless routers and access points are typically fixed and hence, WMNs made up entirely of such devices will have a stable topology whereas WMNs made up of client devices only will be dynamic in general. In the following, unless mentioned otherwise, the term WMN refers to backbone mesh networks comprising wireless access points and routers with one or more client nodes at the edge.

Wireless mesh network can be seen as a special type of MANET where most nodes are stationary. Paths between client and gateway nodes are made up of one or more wireless links, as in ad hoc networks. However, there are a couple of crucial differences. First, nodes in WMN backbone do not have battery constraints as they are powered from the mains supply. In general, these devices are more powerful than end user terminals (which are the typical constituents of MANETs) in terms of processing power, on-board memory, software and hardware capabilities etc. Second, the traffic pattern in WMNs is predictable because most of it is the result of client nodes exchanging application data with correspondent nodes located beyond the gateway nodes. From an ad hoc networking perspective, this is akin to a scenario where data flows always terminate at the same node (or subset of nodes). As in MANETs, use of multi-hop wireless paths results in a challenging radio environment with many nodes contending for a shared channel. However, MANET nodes are generally assumed to have a single radio interface whereas backbone WMN nodes can have more than one radio, especially when dedicated wireless access points or routers are used. Multiple radios per node make it possible to use more than one channel in the same WMN, unlike the single-radio case where only one channel can be used, even if many are available.

The design and deployment of a WMN for any application scenario is challenging because there are several interlinked factors that can impact the performance of the network. Some of them are network-related, such as network architecture (size, density, topology etc.), traffic and node mobility patterns and so on. Other factors are radio related, for example, operating frequency band, channel bandwidth, number of available channels, number of radios per node etc. Different metrics can be used to quantify the performance of mesh networks. These include capacity, throughput, goodput, delay etc. Among these, capacity is without doubt one of the most important indicators. In this chapter, the capacity of multi-radio, multi-channel WMNs is estimated for different scenarios to study the effect of the factors mentioned above.

5.2 Related Work

Capacity analysis of multi-hop wireless networks has proven to be an interesting and challenging research topic which is reflected in the wide body of related literature [48] [49] [50] [51] [52]. In [48], lower and upper bounds of network capacity were determined. This work also provided the important result that there is a significant decrease in throughput capacity per node as node density increases. However, the analysis does not capture routing-related effects and assumes that all paths follow straight lines. Thus, it can only be applied to WMNs in which nodes are organised in a chain topology. A theoretical framework for determining the nominal capacity of WMNs was described in [53]. The concept of *collision domains* is used to determine the bottleneck link in the network and upper bound on capacity calculated. The analytical model was validated using simulations. However, only single channel WMNs were considered.

The capacity of WMNs depends on the available radio capacity. In ad hoc networks, it is common to assume a single-radio (and consequently, single-channel) scenario where all nodes use the same channel for transmitting messages even if the underlying radio technology supports multiple channels. As a result, the channel contention problem is acute and packet collisions are frequent. Early work in WMN research also used the same assumption. However, given the fact that, in most cases, nodes in backbone WMN are dedicated wireless routers and access points, it is reasonable to assume that these nodes have multiple radios which makes the use of multiple channels possible. [54] [55] propose an integrated channel assignment and routing algorithm for multi-radio multi-channel WMNs. An iterative algorithm based on greedy channel assignment is used. The performance metric used to evaluate the performance of the algorithm was network cross-section goodput, defined as the sum of useful bandwidth assigned between communicating node pairs. However, the topology used in this study had ingress-egress node pairs distributed randomly. This maybe true when the WMN is operating in an ad-hoc networking scenario but in backbone WMNs, the ingress-egress pairs are not randomly distributed. A new routing metric for multi-radio WMNs was defined in [56] to capture loss rate and link bandwidth. This metric is then used to select the best paths for routing packets. Although, the research cited above studied the capacity of WMNs, the scenarios used tend to be rather specific. There is a need to determine WMN capacity for a wide range of scenarios so as to provide insights into the impact of different design factors such as network topology, network size, routing methods, channel assignment schemes etc on the capacity of WMNs. In this work, the relationships between these design parameters and the capacity of multi-radio, multi-channel WMNs is explored.

In the following, first the model proposed in [53] to determine the capacity of WMNs is introduced. Then it is used as the basis for developing an analytical framework to estimate the capacity of WMNs organised in grid topology. Finally, the capacity of WMNs is computed for different network scenarios.

5.3 Analytical Model for Capacity Estimation

The model presented in [53] uses nominal MAC throughput and the concept of collision domains for estimating capacity of wireless mesh networks. The former is defined as the throughput achieved at the MAC layer in a one-hop IEEE 802.11 network operating in infrastructure mode. It depends on a number of factors such as MAC layer characteristics, channel conditions, network topology and packet size distribution etc and can be determined if the relevant parameters are known [57].

Collision domains result from the shared nature of wireless links that connect WMN nodes. Use of a common channel implies that when a node is transmitting, all other nodes in the immediate vicinity must not transmit at the same time, assuming that there are no other means of providing isolation between simultaneous transmissions. Several techniques have been proposed in literature for preventing collisions between parallel transmissions. In the Carrier Sense Multiple Access (CSMA) protocol, nodes avoid collisions by listening to the carrier to ensure that no other node is transmitting. The main problem with CSMA is that when the sensing phases of two neighbouring nodes coincide, both start transmitting which causes collisions without either node knowing about it, thereby causing wastage of bandwidth and drop in throughput. An extension of the protocol, called CSMA with Collision Detection (CSMA/CD), enables a sender to detect collisions by comparing a copy of the transmitted frame with data received during the same period. Upon detection of collision, the sender backs off for a random period, thus reducing wastage of bandwidth. However, CSMA/CD is not suited for wireless environments because nodes cannot listen while transmitting. Another extension to CSMA, referred to as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), has been designed for packet radio networks. In CSMA/CA, when a node senses that the channel is busy, it defers the transmission using a random back-off. CSMA/CA suffers from the well-known *hidden node* and *exposed node* problems. The RTS/CTS (Request to Send/Clear to Send) handshake has been proposed to address these issues. In RTS/CTS, when a node wants to send data, it transmits an RTS frame. Upon receiving the RTS, the destination replies by sending a CTS frame. Neighbouring nodes that receive the CTS back-off from sending data for a period of time specified in both the RTS and CTS frames. Nodes that received only the RTS frame can transmit to other nodes (excluding the node which sent the RTS frame). RTS/CTS is generally used in tandem with CSMA/CA, for example in the IEEE 802.11 WLANs. The result of using CSMA/CA in conjunction with RTS/CTS is the creation of an isolation zone in which only a single node-pair can transmit/receive at a given time and all other nodes inside the zone stay silent. This gives rise to the concept of collision domains.

In the rest of this chapter, the following notation is used:

- R - Transmission range of a network node (assumed to the same for all nodes)
- I - Interference range of a network node (assumed to the same for all nodes)
- B - Nominal MAC capacity

Consider a wireless network with N nodes and the associated graph G(V,E), where V is the set of nodes and E is the set of virtual links connecting the nodes. E is defined as

$E = \{l_{ij} \mid d_{ij} \leq R, \ \forall i,j \in V, \ i \neq j\}$

where d_{ij} is the distance between nodes i and j.

The collision domain C_{ij} corresponding to link l_{ij} is the set of links consisting of l_{ij} and all other links that must be inactive to enable collision-free transmission and reception between nodes i and j. The size of a collision domain is directly related to the interference range of wireless nodes. C_{ij} will contain all links that terminate on nodes within the interference range of either node i or j.

Figure 5.1 shows 7 nodes organised in chain topology, connected via wireless links. Adjacent nodes are assumed to be just within the transmission range of each other. Furthermore, the interference range is assumed to be twice the transmission range.

Consider link l_{45} which connects nodes 4 and 5. Other links that have at least one of their end nodes within the interference range of nodes 4 or 5 must be inactive whilst transmission is taking place in either direction on link l_{45}. The dashed arrows indicate these transmission constraints. The set of links that lie within the dashed region

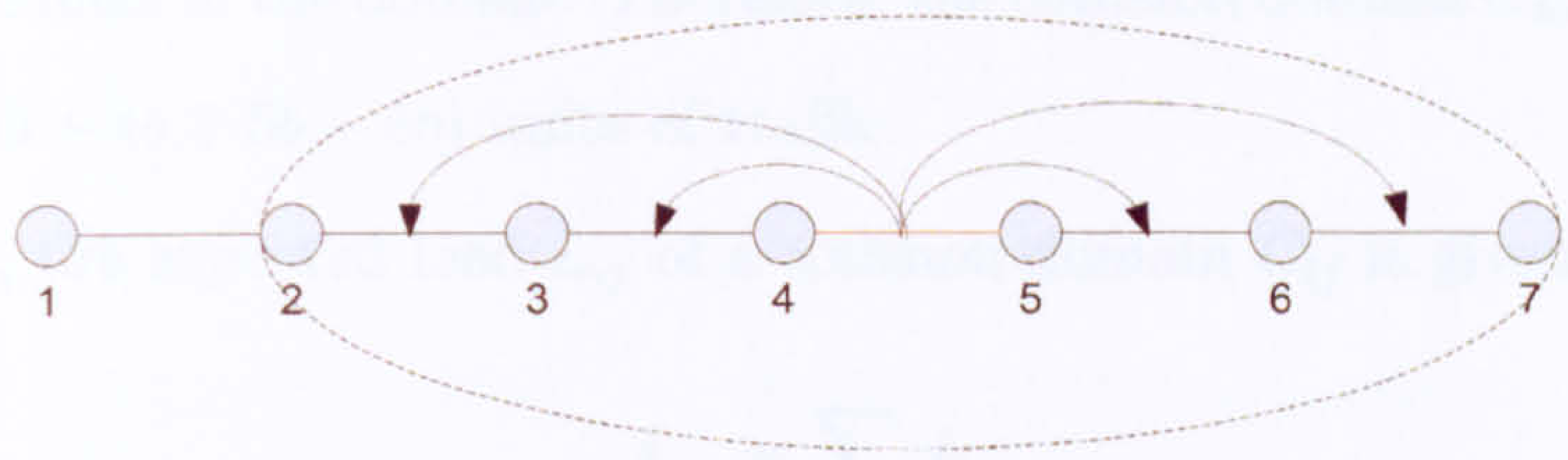


Figure 5.1: Collision domain

correspond to the collision domain of link l_{45}. Similarly, the collision domains of other links can be determined by identifying the corresponding transmission constraints. For example, the collision domain of l_{12} consists of l_{12}, l_{23} and l_{34}.

Now, consider the network shown in Figure 5.2. The node at the rightmost position is assumed to be the gateway while the remaining nodes generate b units of traffic destined it and also relay traffic received from the preceding node. In other words, nodes act as traffic generators as well as traffic aggregators. The numbers at the bottom of each link indicate the expected load on the link.

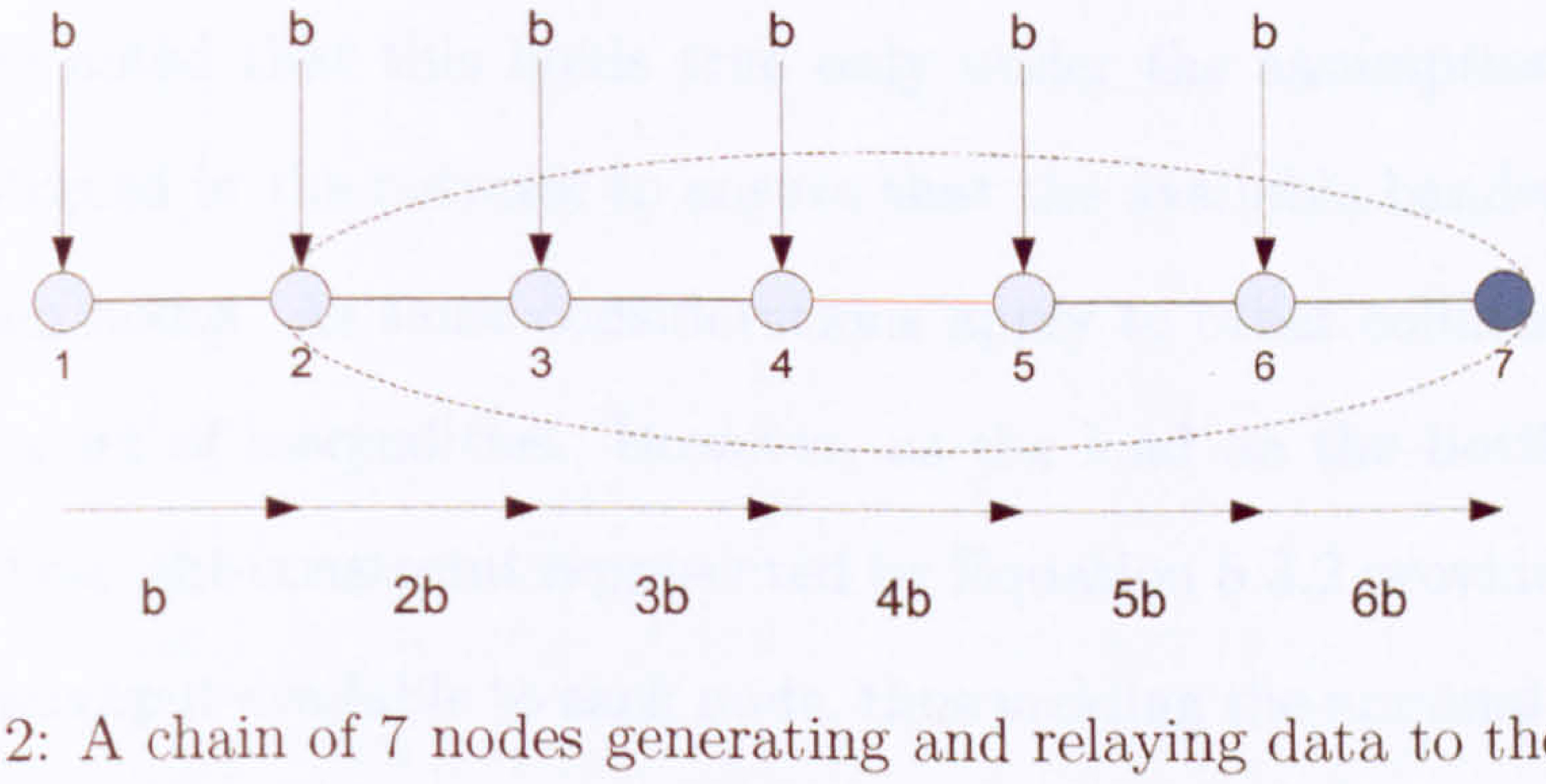


Figure 5.2: A chain of 7 nodes generating and relaying data to the gateway

The dashed region in the figure shows the collision domain C_{45} which corresponds to link l_{45}. Now, each collision domain must be able to carry the sum of the expected loads of all the links in the domain. Therefore, the collision domain C_{45} has to forward $20b$ $(= 2b + 3b + 4b + 5b + 6b)$ units of traffic.

In general, the expected load L_{ij} of a collision domain C_{ij} is given by

$$L_{ij} = \sum_{l \epsilon C_{ij}} f_l \tag{5.3.1}$$

where f_l is the aggregate flow rate on link l.

The maximum capacity of each collision domain is limited by nominal MAC throughput and hence, there exists a collision domain that will create an upper bound on the capacity of the whole network. A *bottleneck* collision domain is defined as the one that needs to forward the maximum amount of traffic [53]. It is possible that a network may have more than one bottleneck domain. For the network of Figure 5.2, it can be shown that C_{45} constitutes the bottleneck collision domain. Therefore, in this case, the maximum bandwidth available to each node is given by

$$b_{max} \leq B/20 \tag{5.3.2}$$

It must be noted that this holds true only under the assumption that *absolute fairness* is enforced in the network to ensure that the available bandwidth is equally shared between nodes. As same considerations apply to other collision domains, the end result is a set of inequalities. However, as the load on the bottleneck collision domain is highest, the constraint represented by Equation 5.3.2 provides the strongest bound on throughput available to each node, thus yielding the nominal capacity of the network. In [53], this method was validated by simulation and the observed capacity closely matched the theoretical results.

The method used for calculating the capacity of a chain network can be extended to arbitrary topologies. Consider, once again, a network of N wireless nodes represented by the graph G(V,E) where V is the set of nodes and E is the set of virtual links between these nodes. Each node is assumed to have p radio interfaces and q available channels. An arbitrary channel assignment algorithm allocates channels to radio interfaces of each network node. One of the network nodes is designated as gateway. Furthermore, K out of the remaining $N-1$ nodes generate application traffic with the gateway node as destination. A routing protocol establishes end-to-end paths between each traffic generator and the gateway node.

The first step is to calculate the expected load on each link in the network. Let b_i be the rate of traffic generated by node i. The expected load on an arbitrary link l in the WMN is given by

$$\phi_l = \sum_{i=1}^{K} b_i * \lambda_{i,l} \tag{5.3.3}$$

where $\lambda_{i,l}$ is the fraction of traffic originating from node i which traverses link l.

The routing protocol forwards traffic generated by node i over M paths ($M \geq 1$) in the direction of gateway node. No assumptions are made regarding the way traffic is distributed over different routes in case of multipath routing. $\lambda_{i,l}$ is calculated as below

$$\lambda_{i,l} = \sum_{j=1}^{M} \alpha_{j,i} * \beta^l_{j,i} \tag{5.3.4}$$

where $\alpha_{j,i}$ is fraction of node i's traffic routed over the jth path and $\beta^l_{j,i}$ is a binary variable which indicates whether the jth path passes through link l. The equation above can be simplified for some specific scenarios. When only one route is used, then $\lambda_{i,l}$ is a binary variable indicating whether the route between node i and the gateway traverses link l. In case of multipath routing with load equally shared between available paths,

$$\lambda_{i,l} = M_l/M \tag{5.3.5}$$

where M_l is the number of routes which include link l.

The next step is to determine all collision domains of the network. Assuming a multi-radio multi-channel network, the collision domain C_l of link l is given by

$$C_l = \{l\} \cup \{m \mid Q_l = Q_m \ and \ d_{xy} \leq I, \ xy = in, ik, jn, jk, \ \forall n, k \in V, \ nk \neq ij\} \tag{5.3.6}$$

where i, j and n, k are the end nodes of links l and m respectively; Q_l and Q_m are the channels assigned to links l and m respectively.

Given the set of all collision domains C and the per flow capacity of each domain, the bottleneck collision domain for the network (represented by the graph G(V,E)) is the one which has the lowest per flow capacity. Note that, in general, there may be more than one bottleneck collision domain in a network. In a homogeneous network, where the available bandwidth of all domains is same, the bottleneck domain is the one with the highest expected load. Therefore, C_l is a bottleneck collision domain if

$$\sum_{i \in C_l} \phi_i = \max_{C_j \in C} \sum_{k \in C_j} \phi_k \tag{5.3.7}$$

Having determined the bottleneck collision domain, the next step is to use the resulting inequality, i.e.,

$$\sum_{j \in C_B} \phi_j \leq B_l \tag{5.3.8}$$

The left-hand side of this inequality can be expressed as the weighted sum of the ingress flow rates b_i. The exact relationship depends on the routing and channel assignment algorithms. In the analysis that follows, it is assumed that the steady state rate of the flows emanating from the aggregator nodes is same.

Therefore, Equation 5.3.3 can be simplified as below

$$\phi_l = b * \sum_{i=1}^{K} \lambda_{i,l} \tag{5.3.9}$$

where b is the flow rate of an aggregator node.

Using this in Equation 5.3.8 yields

$$b * \sum_{j \in C_B} \alpha_j \leq B_l \tag{5.3.10}$$

where $\alpha_j = \sum_{i=1}^{K} \lambda_{i,l}$

Therefore,

$$b \leq \frac{B_l}{\sum_{j \in C_B} \alpha_j} \tag{5.3.11}$$

Equation 5.3.11 provides upper bound on the flow rate of each aggregator node and hence yields the WMN capacity.

In the next section, the method described above is used to estimate the capacity of WMNs organised as 2-dimensional grids. First, key aspects of the system under investigation are described and then results of capacity analysis are presented.

5.4 Scenarios for Capacity Analysis

Design of WMNs has to take into account a number of factors such as network architecture, size and topology, expected traffic profile, radio characteristics, channel assignment scheme, routing algorithm etc. The performance of a WMN is characterised by a number of metrics such as capacity, throughput, cross-section goodput

[54], delay. Although capacity is just one of the performance indicators, it is nevertheless very important. Capacity analysis can provide valuable insights on the overall performance of the network. In order to study the effect of different network parameters on WMN capacity, a set of scenarios have been designed. The key elements which constitute these scenarios are described below.

5.4.1 Network Topology

The topology of a WMN ultimately depends on the deployment scenario but some features are common. There are one or more gateway nodes with connectivity to the global Internet via wired links while the remaining nodes are wireless routers or access points (or hybrid nodes that can work as both). Access points act as aggregators of traffic originating from client nodes attached to them. Figure 5.3 shows one possible WMN deployment scenario.

The aggregators and gateways are explicitly marked and the remaining nodes are wireless routers (one of which is labelled) that forward traffic in either direction between gateways and aggregators. The figure also shows the wireless links connecting the WMN nodes. Note that multiple routing paths available between a given aggregator-gateway node pair.

The WMN topology illustrated in Figure 5.3 is arbitrary and any analysis based on it will not be valid for other scenarios. Therefore, a more general topology needs to be selected so that a wider range of scenarios can be investigated. WMNs organised in grid topology have been widely used in literature for performance analysis. Although it is not realistic to assume that grid-based WMNs can be used in all scenarios, it is reasonable to expect it to be used, at least, in urban environments. Note that

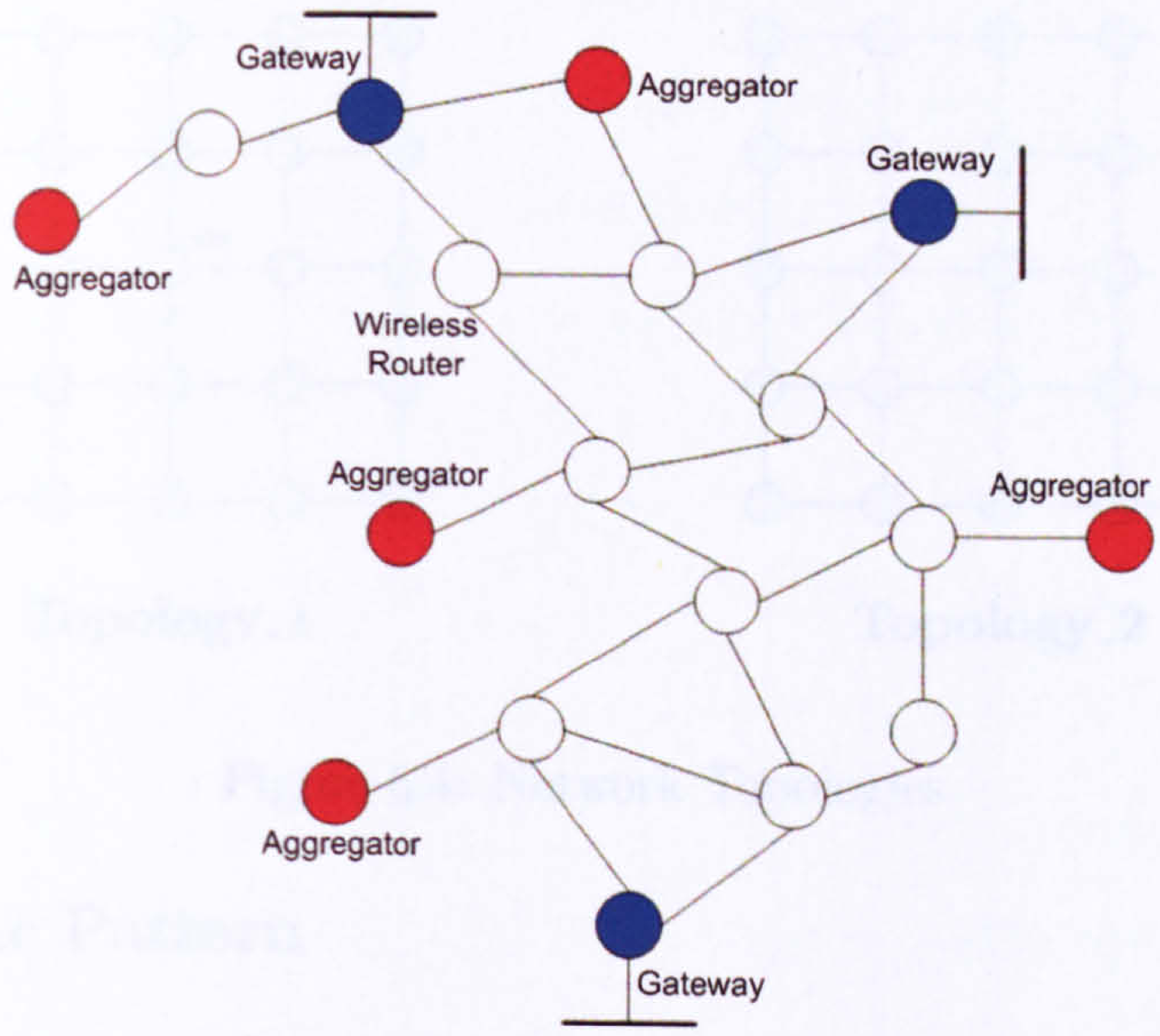


Figure 5.3: An example WMN topology

grids can also be used to generate more random topologies by removing some nodes. Bearing these considerations in mind, the analysis here focusses on WMNs organised in grid formation. Furthermore, it is assumed that there is only one gateway node.

Two network topologies are considered for capacity analysis, as shown in Figure 5.4, referred to as Topology_1 and Topology_2 respectively. The primary difference between the two is location of gateway node. In the first case, the gateway node is located at the center of the grid whereas in the second case, the gateway is at one of the corners. The other nodes are located at remaining grid points with aggregators distributed along the edges and wireless routers located at either the edges or interior grid points.

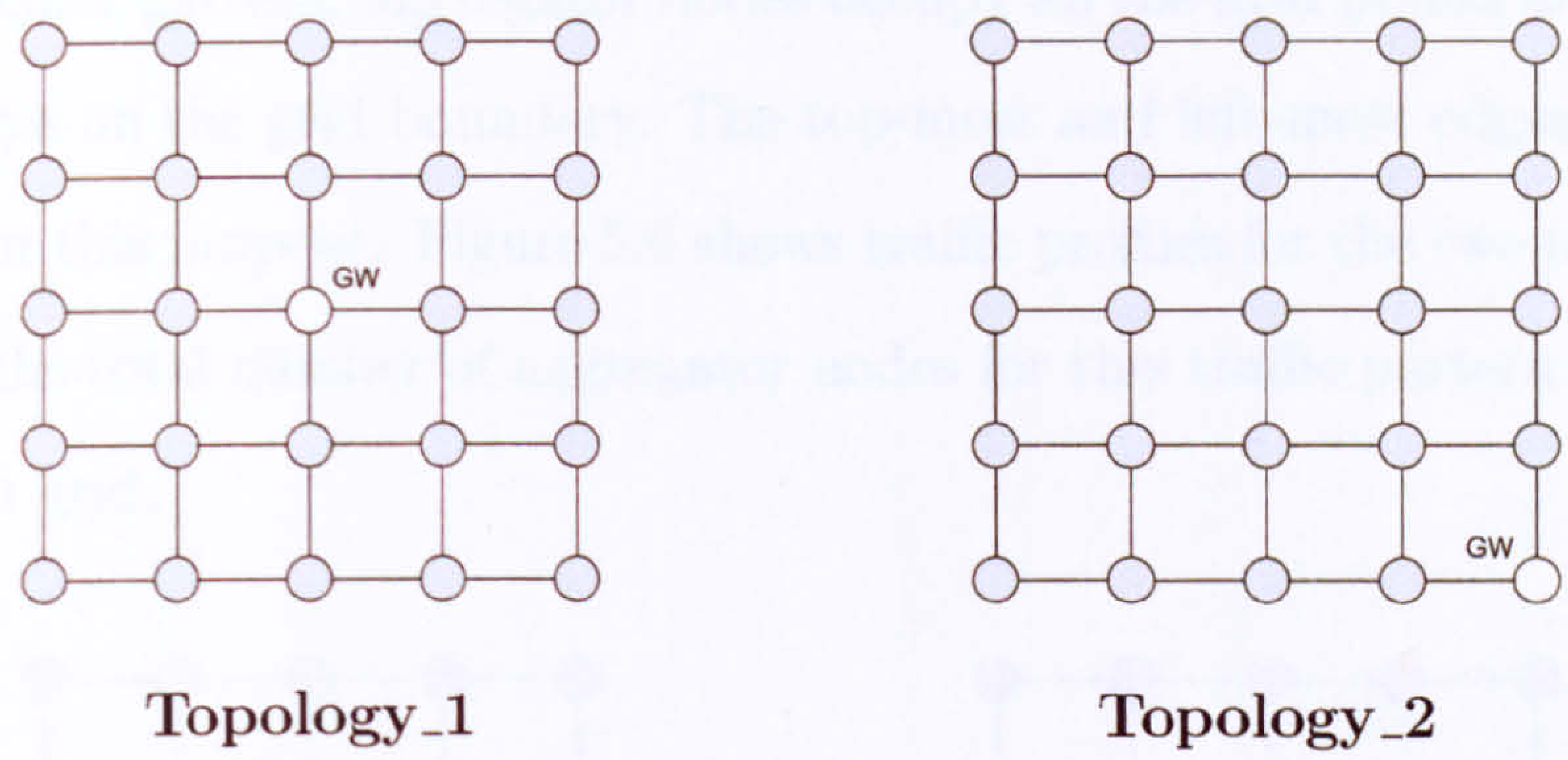


Figure 5.4: Network Topologies

5.4.2 Traffic Pattern

The analysis considers three different traffic patterns which are distinguished from each other by the location of aggregator nodes along the grid edges. In the first case, the aggregator nodes are placed at the four corners of the grid. The dark-shaded circles in Figure 5.5 indicate aggregator nodes' positions for Topology_1 and Topology_2 respectively.

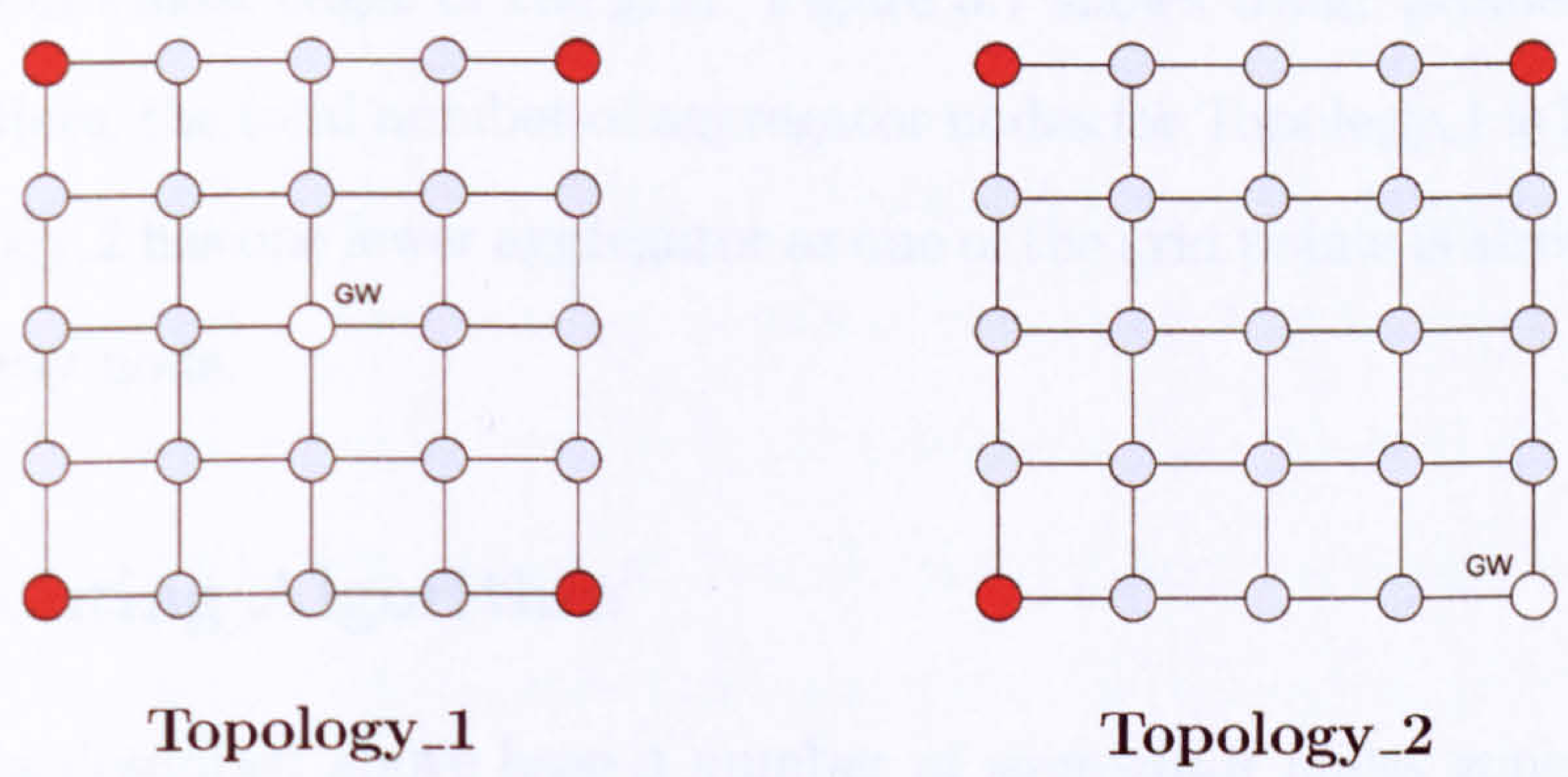
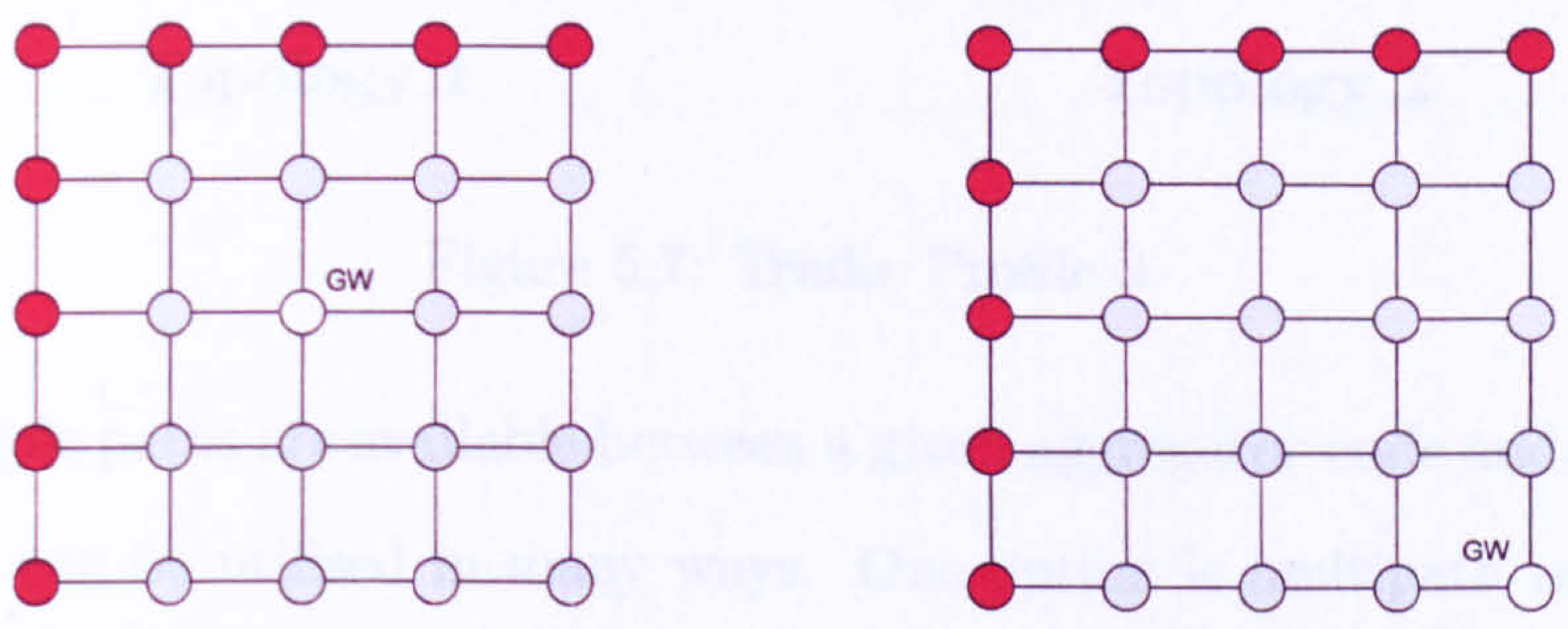


Figure 5.5: Traffic Profile 1

In the second pattern, aggregator nodes occupy all the grid points along a pair of adjacent edges on the grid boundary. The top-most and left-most edges respectively are chosen for this purpose. Figure 5.6 shows traffic profiles for the two topologies. In both cases, the total number of aggregator nodes for this traffic pattern is $m + n - 1$ for an $m \times n$ grid.



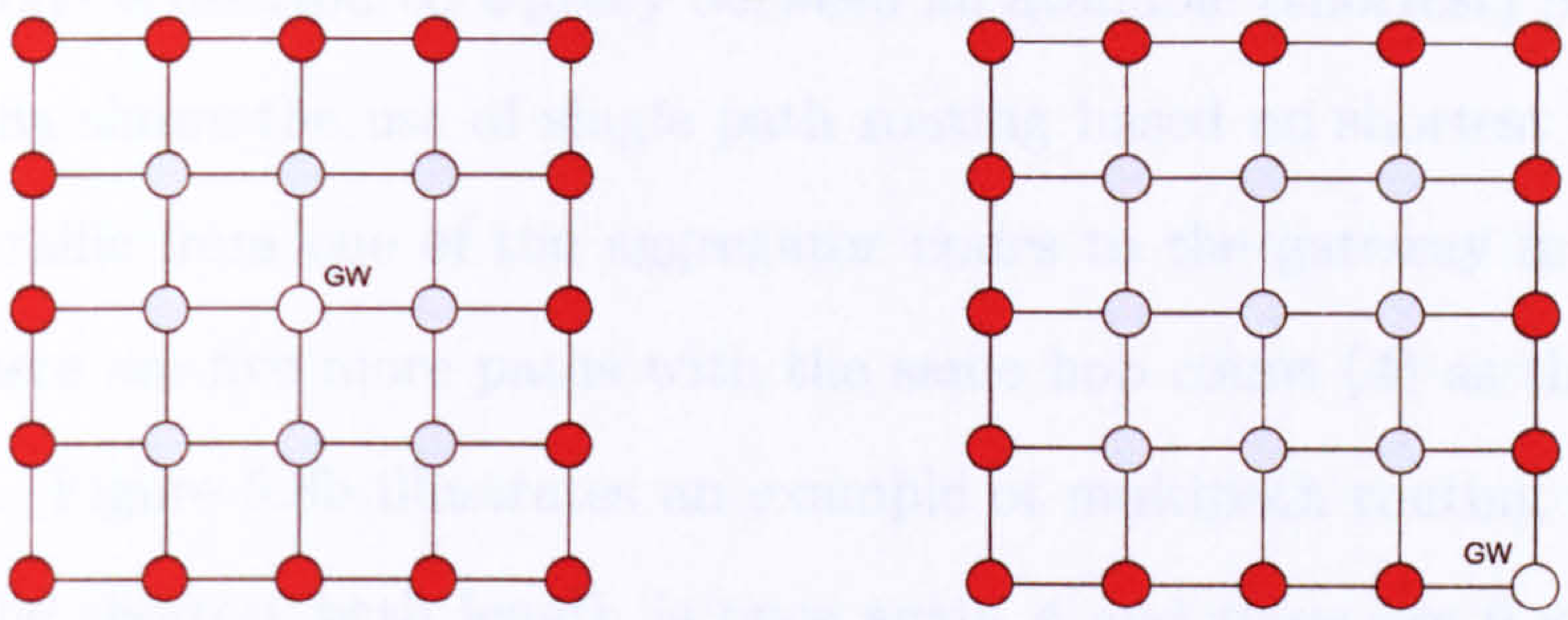
Topology_1 **Topology_2**

Figure 5.6: Traffic Profile 2

Finally, in the third traffic pattern, aggregator nodes occupy all available positions on the four outermost edges of the grid. Figure 5.7 shows traffic profiles for the two topologies. Here, the total number of aggregator nodes for Topology_1 is $2*(m+n-4)$ while Topology_2 has one fewer aggregator as one of the grid points is already occupied by the gateway node.

5.4.3 Routing Algorithm

The scenarios described above have a number of aggregator nodes generating traffic with the gateway node as the destination. A routing protocol is required to establish routes between the different source-destination node pairs. As seen from the figures



Topology_1 **Topology_2**

Figure 5.7: Traffic Profile 3

before, multiple paths are available between a given aggregator node and the gateway. These paths can be utilised in many ways. One option is multipath routing where all available paths are used simultaneously by distributing the traffic over them. Furthermore, distribution of traffic can be even or uneven. Another multipath routing strategy is to shortlist a few of the available routes based on some suitable criteria and distribute the traffic over this subset of paths. A special case is the single path approach in which only one of the available routes is selected and all the traffic is forwarded along it.

All these approaches have their pros and cons which were discussed in the previous chapter. Since the choice of routing algorithm is part of WMN design, the analysis is performed for both approaches in order to investigate the effect of using single and multiple routes on network capacity. The single path routing algorithm selects the shortest available path from a given aggregator node to the gateway. Path length is measured in number of hops. If more than one route fits the shortest path criteria, then one of them is randomly chosen. When multiple path routing is used, the list of all paths that have the shortest path length is constructed and traffic from the aggregator node is distributed equally between all available (shortest) paths.

Figure 5.8a shows the use of single path routing based on shortest path criteria for routing traffic from one of the aggregator nodes to the gateway in Topology_1. Note that there are five more paths with the same hop count (4) as the one shown in the figure. Figure 5.8b illustrates an example of multipath routing for the same topology. The shortest path length is once again 4 and there are 6 such paths in total. Therefore, traffic originating from the aggregator node is equally distributed along all the 6 paths.

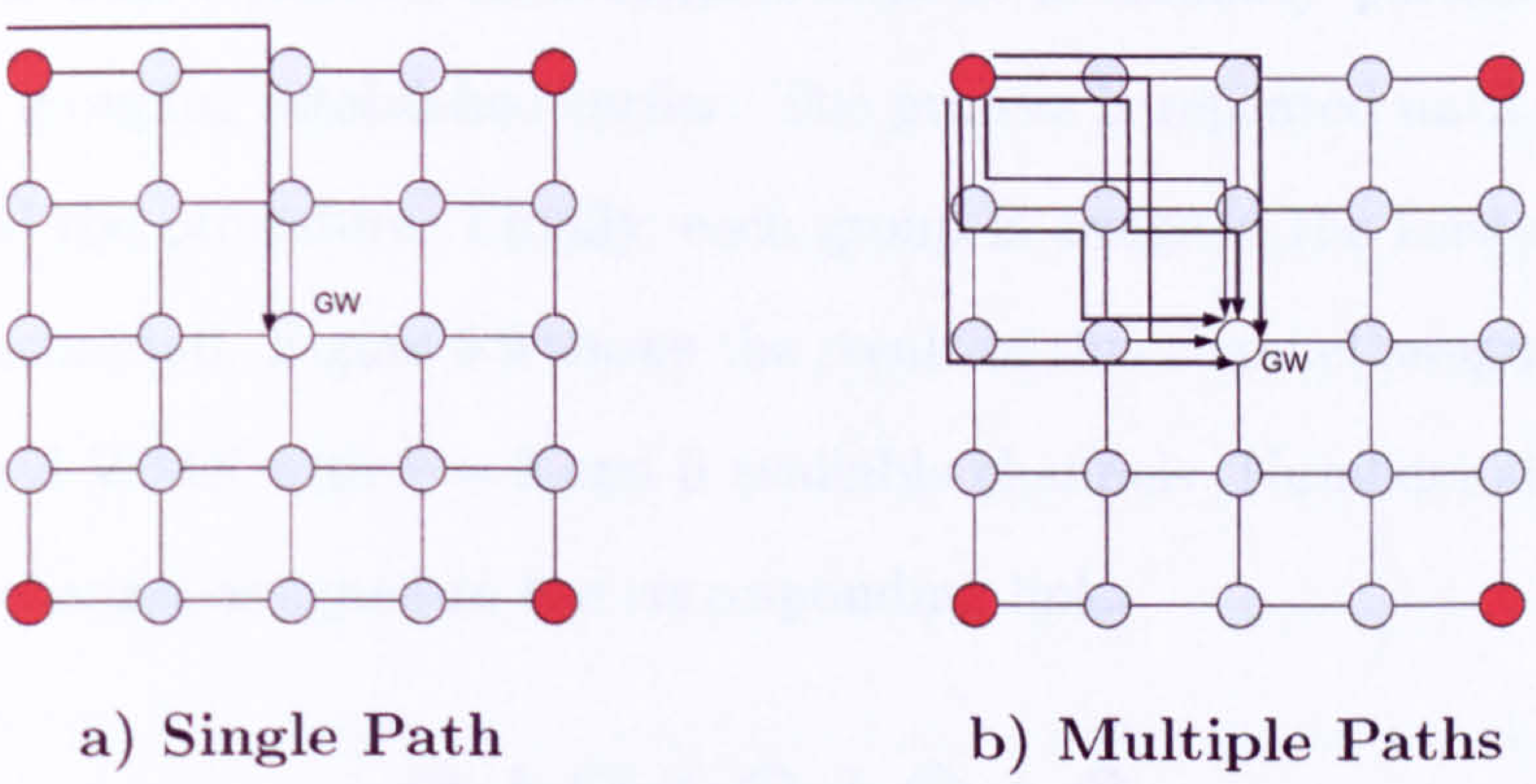


Figure 5.8: Routing Algorithms

5.4.4 Channel Assignment

Single-radio WMNs can use only one channel even if several are available to ensure that the network does not become partitioned. However, in multi-radio WMNs, it is possible to utilise multiple channels simultaneously. In such scenarios, channels must be assigned to radio interfaces in such a way that there is at least one path between every pair of nodes to avoid partitioning. Furthermore, the assignment must also take into account performance objectives such as interference reduction, fair distribution of load and throughput maximisation.

Three different channel assignment schemes are considered. The first is relatively simple where all interfaces are assigned the same channel. This is essentially a baseline case against which other cases are compared. In the second scheme, the partitioning algorithm proposed in [54] is used for *uniform* channel assignment across the network. Assuming that each node has k interfaces, the algorithm starts by selecting one node and dividing its neighbours into k groups. Each interface of the node is assigned a group. In the next iteration, each neighbour node is similarly partitioned without violating the grouping established earlier. The process is repeated until all the nodes have executed the procedure. Finally, each group is assigned the least-used channel in the neighbourhood. Figure 5.9 shows the result of this channel assignment scheme for a 5×5 grid WMN with $k = 2$ and 6 available channels. Numbers along the lines indicate the channel assigned to the corresponding link.

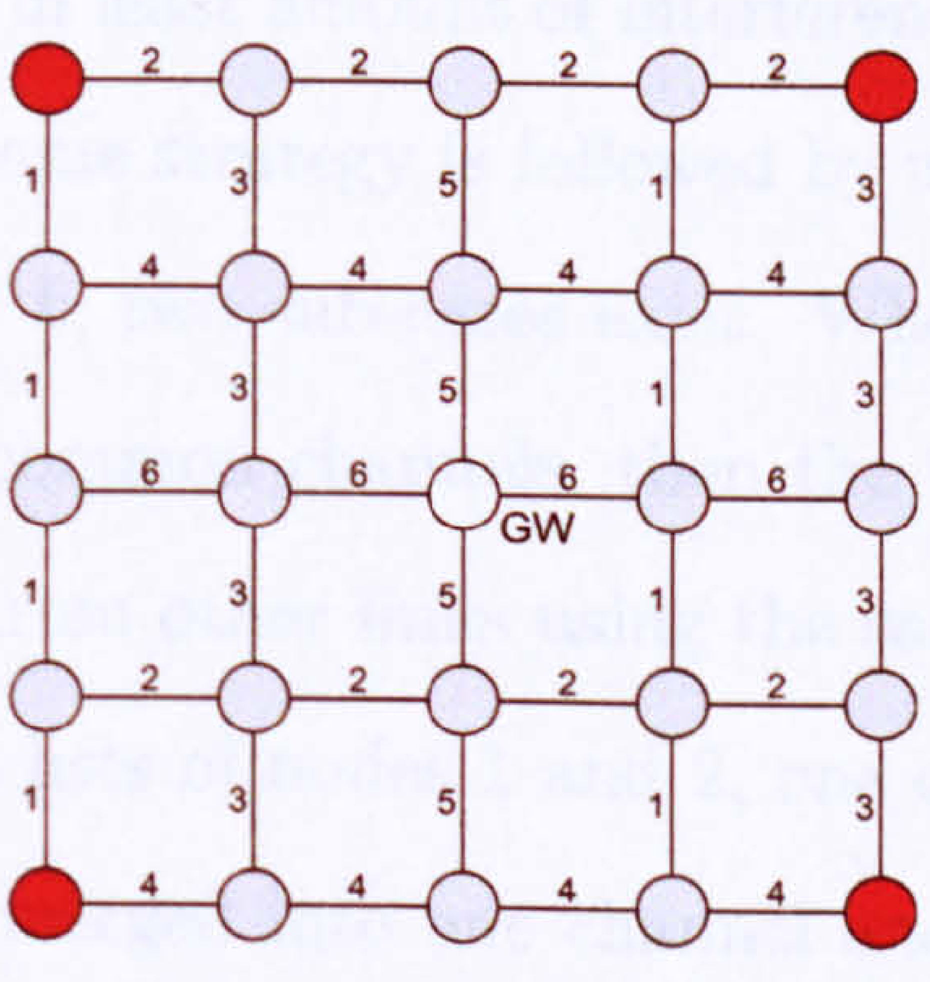


Figure 5.9: Channel assignment based on partitioning

The third scheme assigns channels to interfaces based on the condition that available bandwidth on the interfaces is at least equal to the expected load on the associated links [54]. The scheme uses a *greedy* load-aware algorithm where channels are assigned to links one-by-one in the decreasing order of expected load. When a link is traversed, a channel assigned to it such that prior assignments are not violated. Consider a virtual link with nodes 1 and 2 forming the two ends. Assume that each node has k network interfaces. Each node maintains a list of channels that have already been assigned to its interfaces (corresponding to other virtual links terminating at the node). Let K_i be the size of the channel list of node i. Now, for the link between nodes 1 and 2, three possibilities exist. First, if $K_1 < k$ and $K_2 < k$, then an unused channel (not present in the channel lists of both nodes 1 and 2) is assigned to the link such that it attracts least amount of interference from other links that use the same channel. Second, if $K_1 = k$ and $K_2 < k$, then the link is assigned a channel from the list of node 1 and added to the list of node 2. Once again, the channel is selected such that it results in least amount of interference from other links operating on the same channel. The same strategy is followed by node 2 if $K_2 = k$ and $K_1 < k$. Third, if $K_1 = k$ and $K_2 = k$, two sub-cases exist. When the channel lists of nodes 1 and 2 have one or more common channels, then the link is assigned the one that minimizes the interference from other links using the same channel. When there are no common channels in the lists of nodes 1 and 2, one channel each is selected from the two lists. The two are merged into one channel and assigned to the link. Note that in this case, the renaming operation is repeated for all other instances of the merged channels previously assigned to nodes 1 and 2. The choice of channels to be merged is again made such that the interference from other links is minimized.

Further details of this scheme can be found in [54]. Since links with higher loads are visited first, it is expected that they will be allocated a channel that suffers from less interference and therefore, get a greater share of the available bandwidth.

5.4.5 Scenario Synthesis

The different design aspects described above have been combined to generate several scenarios. The following assumptions are applicable to all scenarios:

1. All nodes on the grid are stationary;
2. Traffic in the network is generated by aggregator nodes only and all other nodes, including wireless routers and the gateway, do not generate any traffic;
3. Traffic generated by aggregator nodes is destined for the gateway;
4. Interference range is assumed to be 2 hops.

The last condition implies that nodes that are within 2 hops distance of a particular node will cause interference to it if one or more of their interfaces use the same channel. In addition, the assumptions mentioned in [53] also apply here. In particular, absolute fairness is assumed. Furthermore, the MAC layer supports RTS/CTS handshake mechanism resulting in symmetric link constraints for collision domain determination.

The elements that characterise the different scenarios are as follows:

- Topology (including type and size of grid)
- Traffic Pattern

- Routing Algorithm
- Channel Assignment Scheme
- No. of available channels

By varying these elements, several scenarios are synthesised and the capacity of resulting networks estimated.

5.5 Capacity Evaluation

5.5.1 Scenario Settings

The capacity of WMNs corresponding to the scenarios presented above was estimated using the analytical model presented in Section 5.3. For this analysis, the WMN nodes were assumed to have two radio interfaces. Furthermore, two values were used for the number of available channels - 3 and 12. The former corresponds to the number of non-overlapping channels in IEEE802.11b while the latter equals the number of channels available in IEEE802.11a. Two grid sizes are considered: 5×5 and 9×9, with each grid used to realise the two topologies discussed in Section 5.4. All the aggregator nodes in each scenario generate the same amount of traffic. Depending on the particular scenario, traffic is routed towards the gateway node using either single path or multipath routing. In the case of single path routing, when multiple paths have the shortest path length, one is selected at random. For multipath routing, traffic is distributed evenly across all the routes in use. Without loss of generality, the nominal MAC capacity is assumed to be 1 and the capacity available to each WMN node is calculated as percentage of the nominal MAC capacity.

In the analysis that follows, the following notation is used to describe the scenarios and results:

- T1: Topology_1 and T2: Topology_2
- R1: Multipath routing and R2: Single path routing
- C: Channel assignment scheme (scheme 1 is uniform assignment, scheme 2 is partitioning-based assignment and scheme 3 is load-aware assignment)
- c: Number of available channels

For each scenario, the topology, traffic profile, routing algorithm and channel assignment scheme constitute the input parameters. A MATLAB program was used to first determine the expected load on each link and then find collision domains corresponding to each link of the WMN. The amount of traffic handled by each domain was calculated and the bottleneck domain(s) computed. Finally, Equation 5.3.11 was used to compute the maximum available throughput per aggregator node.

5.5.2 Results

The first set of results are for a 5×5 grid WMN. Figure 5.10 shows the nominal capacity of the network for single path and multipath routing when Topology_1 is being used while Figure 5.11 corresponds to Topology_2. For each case, capacity (as percentage of nominal MAC throughput) is plotted against the number of aggregator nodes, which is a function of the traffic pattern. As three traffic patterns are used in the analysis, there are three sample points on each curve in the graphs.

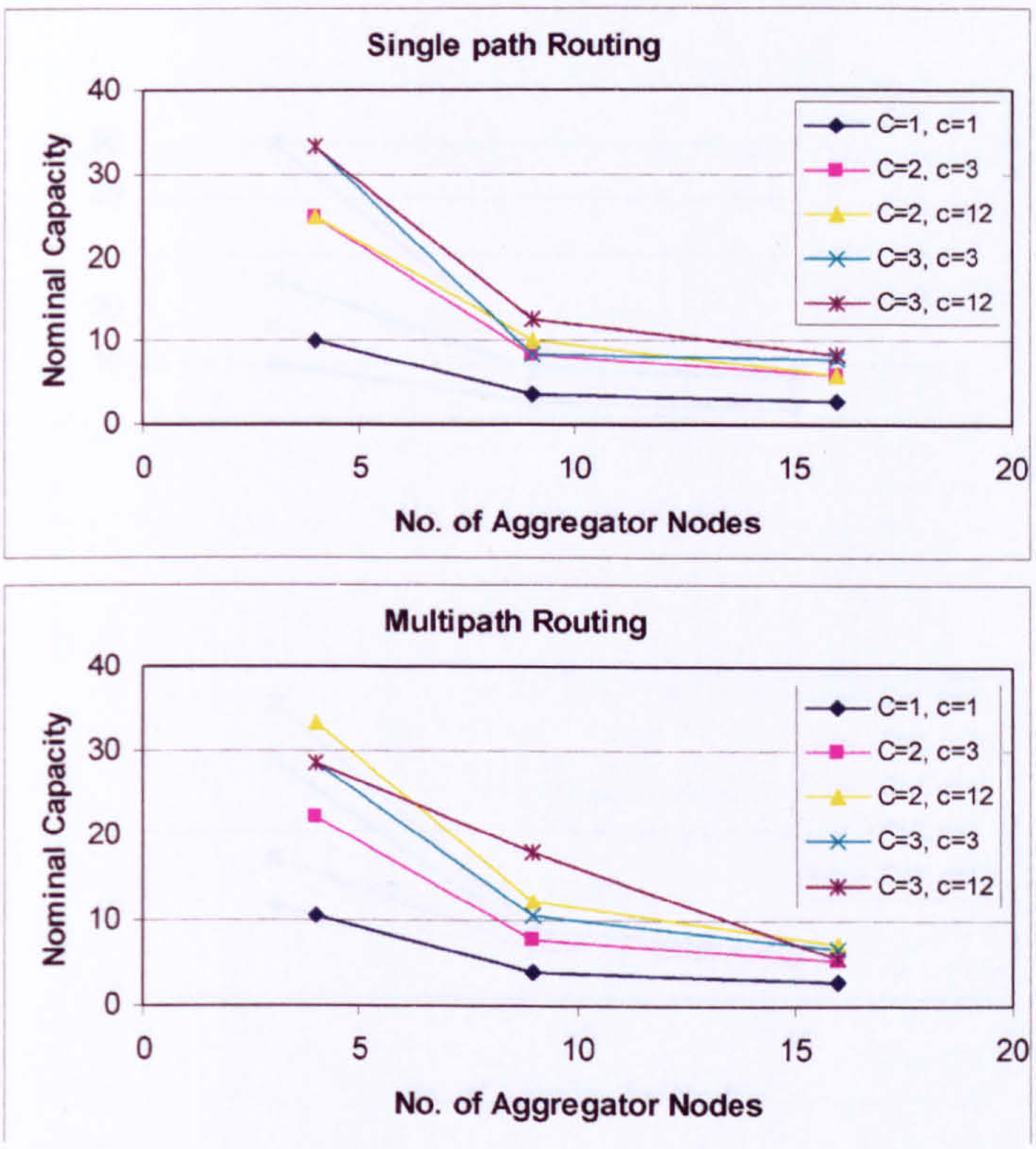


Figure 5.10: Capacity for 5x5 grid (Topology_1)

The results shown in Figures 5.10 and 5.11 provide insight into the effect of number of available channels and the channel assignment scheme on capacity. Scenarios where only one channel is used have the lowest capacity per aggregator node and constitutes the baseline case. The results clearly indicate that the capacity of WMN nodes is increased when multiple channels are used. However, the capacity gain decreases as the number of aggregator nodes increases. Furthermore, the channel assignment scheme appears to be an important factor in determining the capacity. For the same number of available channels, the load-aware scheme results in capacity increase of

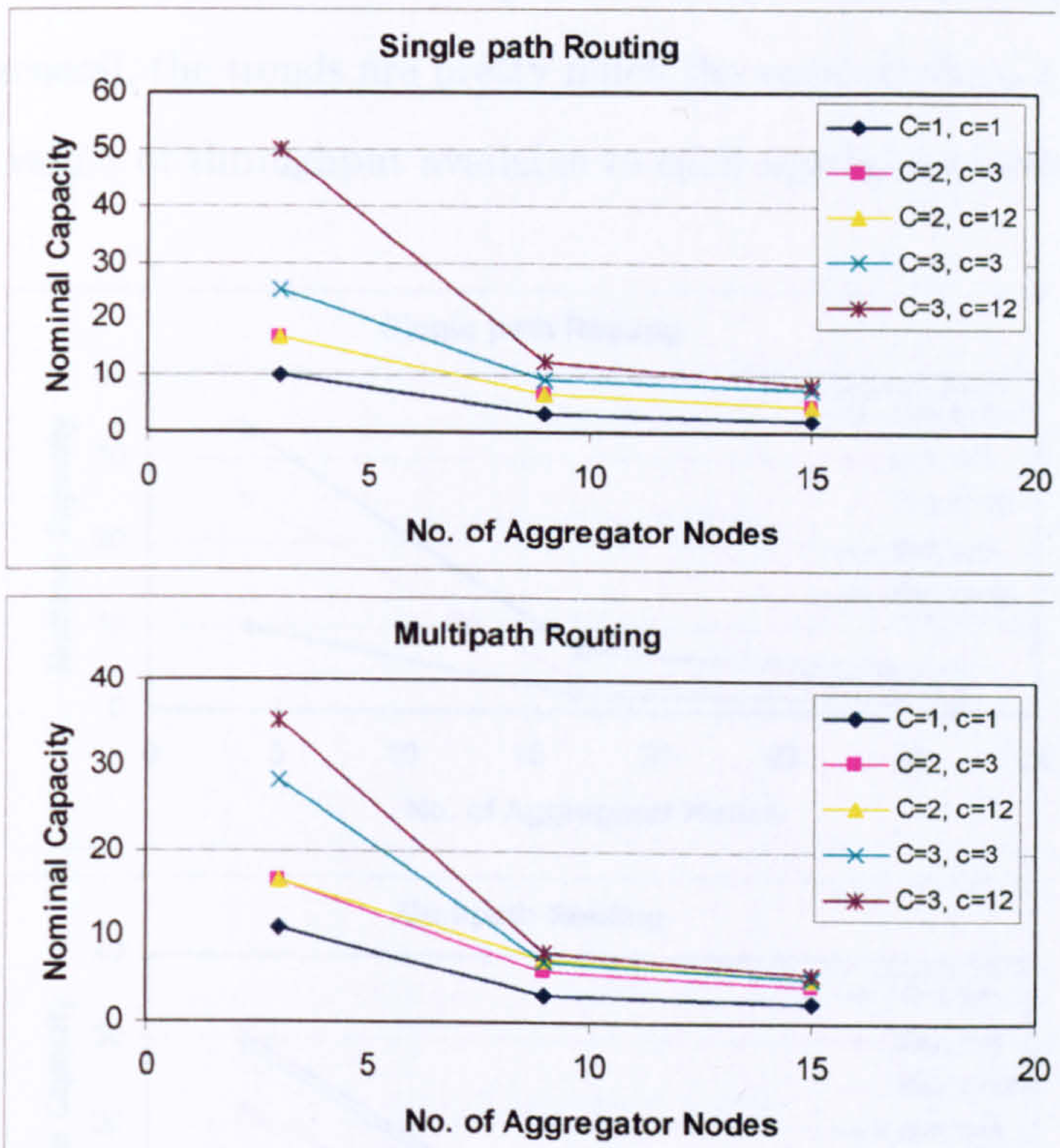


Figure 5.11: Capacity for 5x5 grid (Topology_2)

almost 10 per cent when single path routing is used in Topology_1. On the whole, load-aware channel assignment outperforms the partitioning-based method but the gain is diminished as the number of aggregator nodes increases. Differences between various assignment schemes are clear in Figure 5.10 for the first traffic pattern (which corresponds to 4 aggregator nodes). It can also be seen from the graphs that capacity falls sharply as the number of aggregator nodes increases, especially for multi-channel scenarios. In general, multipath routing seems to provide capacity improvement although once again it is less pronounced when there are a lot of aggregator nodes.

The second set of results, shown in Figures 5.12 and 5.13, shows the capacity for a 9×9 grid. In general, the trends are pretty much the same as the 5×5 grid scenario but the actual values of throughput available to each aggregator node are not same.

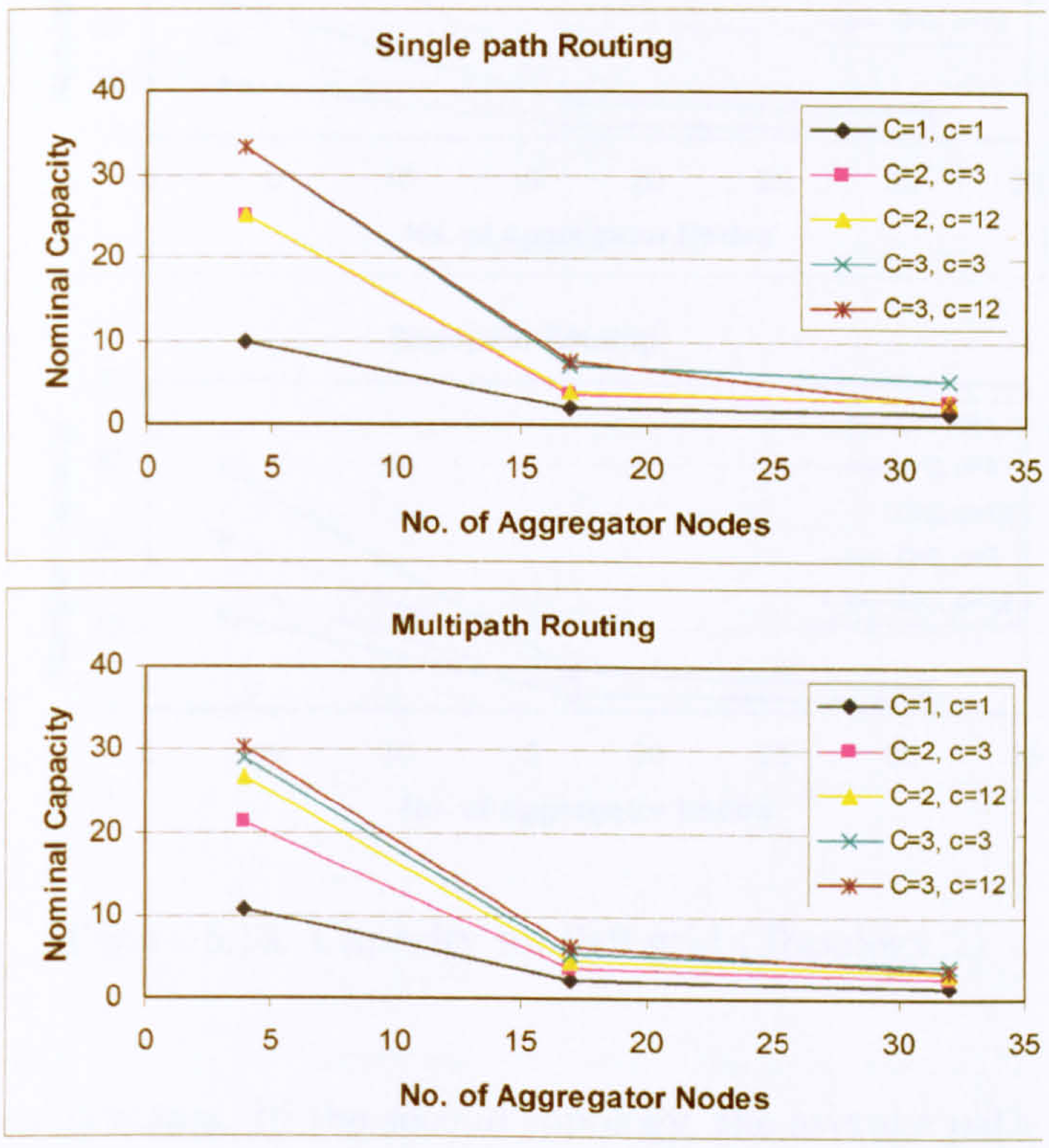


Figure 5.12: Capacity for 9x9 grid (Topology_1)

5.6 Discussion

The results presented here illustrate the impact of different factors on WMN capacity. The maximum available throughout per aggregator node in Topology_1 is generally higher than in Topology_2 although the differences tend to diminish as the number of

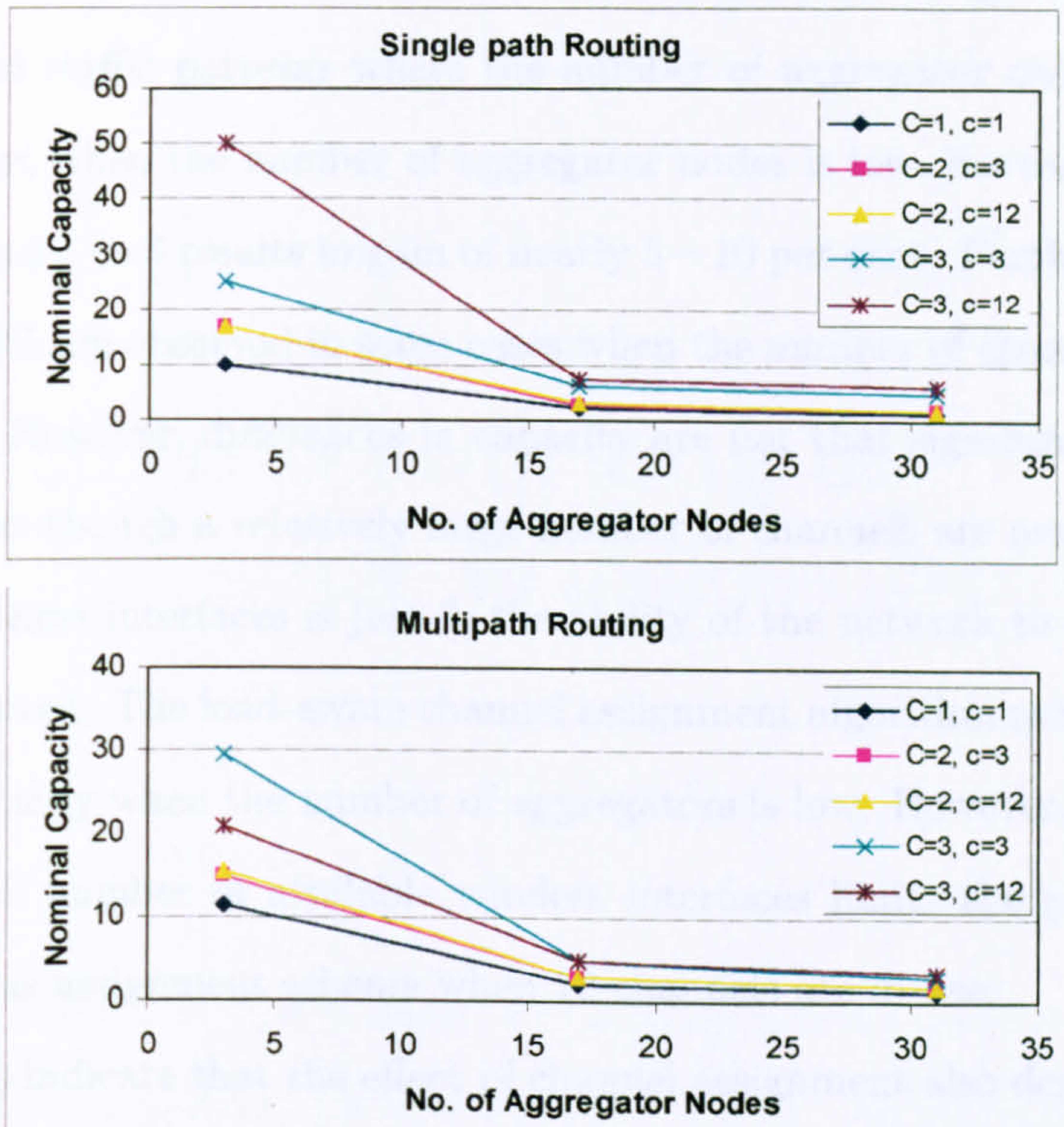


Figure 5.13: Capacity for 9x9 grid (Topology_2)

aggregator nodes increases. In the second topology, the average path length between aggregators and the gateway is greater compared to the first topology. As a result, the number of active links is higher and hence, interference levels increase resulting in lower capacity. For the same topology, as network size increases, capacity decreases because of longer paths. An inverse relationship exists between the number of aggregator nodes and capacity because increasing the number of such nodes leads to higher expected load.

The effect of increasing the number of available channels is significant for the first and the second traffic patterns where the number of aggregator nodes is moderate. On the average, when the number of aggregator nodes is low, increasing the number of channels from 1 to 3 results in gain of nearly $5-10$ per cent. Furthermore, gains of almost $20-30\%$ are observed in some cases when the number of channels is increased from 3 to 12. However, differences in capacity are not that significant for high load scenarios. Even though a relatively large number of channels are available, since the number of wireless interfaces is just 2, the ability of the network to use all available channels is limited. The load-aware channel assignment algorithm results in improved capacity, especially when the number of aggregators is low. However, once again, the relatively small number of available wireless interfaces limits the gain that can be achieved by this assignment scheme when 12 channels are in use.

The results indicate that the effect of channel assignment also depends on several factors such as network topology, network dimensions, routing algorithm and traffic profile. For Topology_2, load-aware assignment gives the same capacity as the partitioning-based scheme for moderate and high traffic scenarios, independent of the network dimension. However, capacity gain is achieved when load-aware assignment is used in Topology_1 if traffic load is low or moderate. In general, it can be seen from the results that capacity can be improved by using multiple channels and intelligent channel assignment. At the same time, building a dense mesh network is not such a good idea because of the dramatic decrease in throughput when the number of aggregator nodes increases. As far as routing is concerned, it must take into account channel assignment so that load is evenly distributed on each channel.

Chapter 6

Dynamic Interworking of Heterogeneous Wireless Networks

6.1 Introduction

The work presented so far has focussed on multihop wireless networks. First, routing in MANETs was considered, particularly the RDMAR protocol and its extensions. Then, the effect of routing and channel assignment algorithms on multi-radio multi-channel WMNs was investigated. Both MANET and WMN are relatively recent developments and the related technology is still maturing. Therefore, current deployment of these networks is limited and patchy. However, it is foreseen that they will be integral components of the so-called Next Generation Internet (NGI) architectures.

Within the NGI vision, MANETs can be seen as stub networks, attaching to the core network via heterogeneous radio access networks (RAN). Clearly, this will require some form of interworking between the ad hoc and core networks. In the simplest case, one of the MANET nodes can use a suitable mobile or wireless network operator (e.g. UMTS or WLAN) to attach to the Internet and let others share the connection. This is a non-optimal solution because it will give rise to problems such as single point of failure, bandwidth bottleneck etc. Therefore, it would be desirable to establish an interworking relationship between the MANET and the operator network. Note that in this case, the MANET as a whole is treated as peer by the operator network. However, this does not necessarily mandate that all the MANET nodes be directly attached to the access network. Furthermore, the dynamic nature of MANETs implies that this relationship should be flexible enough to cope not only with node mobility but also situations where nodes may leave or join the network from time to time. Similar considerations apply to client-based WMNs that comprise of only end user terminals.

Even within an ad hoc network, network nodes co-operate for data forwarding and they have to "agree" on the protocol to use and the particular features of the selected protocol to deploy. Take the example of RDMAR where position-assisted routing is useful only if all nodes agree to share location data. Similarly, multipath routing will be beneficial if all the nodes agree to deploy this feature. These can be manually configured at each node but it is highly desirable that nodes mutually select them based on pre-configured policies and preferences. Note that MANET nodes may belong to different administrative entities (e.g. users) and hence, it may not be possible to manually configure all of them in a centralised manner unlike conventional scenarios where network administrators are in charge of such tasks. In case, QoS-enabled routing is to be used, nodes must agree on the type of QoS guarantees to be provided as well as the details of compensation to be paid, if any. Furthermore, for security reasons, nodes must be able to authenticate each other but before that they must decide the type of credentials (e.g. cryptographic keys). Therefore, it would help to automate such transactions as well as the subsequent configuration process.

The examples above provide two use cases where interworking between networks as well as between nodes will be mutually beneficial. A third case is that of interworking between an end host and network operator. Currently, end users typically subscribe to operators in order to be able to make voice calls or browse the Internet. However, a more flexible interworking relationship between the two is required so that end users have more choice and operators can offer tailored service offerings.

A common feature of the use cases mentioned above is the need for a flexible framework of cooperation covering both technical and business aspects. The research presented in this chapter addresses this challenge. The research scope of the work documented in this chapter is very different compared to the previous chapters where only interactions between network nodes were considered. Here the emphasis is on network-network interactions, aiming at exploiting the features of the protocols investigated in earlier chapters, to achieve aforementioned interworking. In particular, the focus is on the concept of network composition, developed as part of the Ambient Networks research project. Composition can be defined as a framework for dynamic and automatic cooperation between networks. The term cooperation is used here in a broad sense to refer to a wide range of interactions between networks to achieve specific communication-related objectives. There are two main contributions here: a protocol for enabling network composition and the analysis of composition process itself with respect to signalling overhead and delay.

In the rest of this chapter, first the main networking concepts of Ambient Networks, especially composition, are introduced. Then the signalling protocol for network composition is described, followed by detailed analysis of the composition process.

6.2 Ambient Networks

Scenarios for next generation communication networks are characterised by four main features. First, there will be a multitude of networks with a plethora of access technologies underneath. Second, inter-networking between networks will go beyond what we have today (mainly at the data forwarding level). Interworking between landline and cellular networks is already happening and there is a growing impetus towards Fixed-Mobile Convergence as well as convergence of wireless and cellular networks. Third, traditional business roles will disappear and provision of services will be democratized, instead of the current situation where the number of providers is relatively small. In other words, there will be more players besides big operators and providers, as we can already see from the emergence of municipal WLANs, community-based networks. Finally, the relationship between end users and service providers will be much more flexible and dynamic unlike the current subscription-based models. In a highly competitive market, end users would not only like to make the most of what is available but at the same time, choose the best of what is available.

From the future networking vision outlined above, it can be inferred that the dominant themes are growing heterogeneity, greater choice of service providers and increased levels of interworking between networks. The networking environment will consist of a multitude of networks in the core, access as well as user segments:

- Cellular networks
- Metro-scale networks
- Enterprise networks
- Hotspot networks

- Community networks
- Ad hoc networks
- Vehicular networks
- Personal networks
- Sensor networks
- Body area networks

Note that some of these are low-complexity networks, potentially owned by end users. In the long run, they will play the same role as that of end user terminals nowadays. In addition, some of them will also act is service providers in certain scenarios. This also highlights a shift from the current paradigm of predominantly user-network relationships towards network-network interactions.

The networks listed above will be inter-connected by heterogeneous wireless technologies and interworking between them will crucial in realizing convergence of different types of wired and wireless systems. Interworking of UMTS and WLAN-based networks has been studied [58] by 3GPP. The System Architecture Evolution (SAE) initiative of 3GPP is taking this one step further by considering architectures where different types of access networks such as UTRAN, WLAN and WiMAX can attach to the UMTS core network. However, these efforts are mainly directed towards static and "one-time" interworking for specific types of networks. Therefore, a technology-agnostic framework for dynamic and flexible interworking is required for next generation networks.

The main challenge towards such a framework comes from heterogeneity of networking technologies as well as the diversity in the way network control functions are implemented and organised in different networks. The latter refers to the significant differences in the way services are controlled and provisioned in different types of networks, e.g., UMTS and WLAN.

6.2.1 Architecture

The Ambient Networks [5] project is developing concepts and solutions to realize a unified network architecture based on a common control plane that hides the heterogeneity in access technologies and also presents a homogeneous control plane. Two key principles that guide Ambient Network design are: open architecture and network composition. The first manifests itself in the form of a set of open interfaces to enable richer interconnections between networks. The second principle aims to enable self-managed and dynamic composition of control plane functions.

The Ambient Networks approach aims to create a networking environment which hides the heterogeneity of underlying access and transport networks and at the same time, also ensures that applications and services are presented with a homogeneous control plane. 'Network' is the basic element of AN architecture. In other words, the notion of 'network' includes end user terminals and small networks such as BAN, PAN etc in addition to conventional networks such as LANs, WANs etc. This contrasts sharply with the current practice of looking at communication systems in terms of networks and end user devices. This artifice allows the application of Ambient Network concepts and solutions to a whole range of networks.

Ambient Network concepts are built around Internet design principles and follow, in particular, the all-IP networking approach with strong emphasis on separation of transport and control functions. An Ambient Network, by definition, consists of an IP-based transport abstraction called Ambient Connectivity, a control plane abstraction, referred to as Ambient Control Space (ACS) and three Reference Points. Figure 6.1 shows the logical view of an Ambient Network [59].

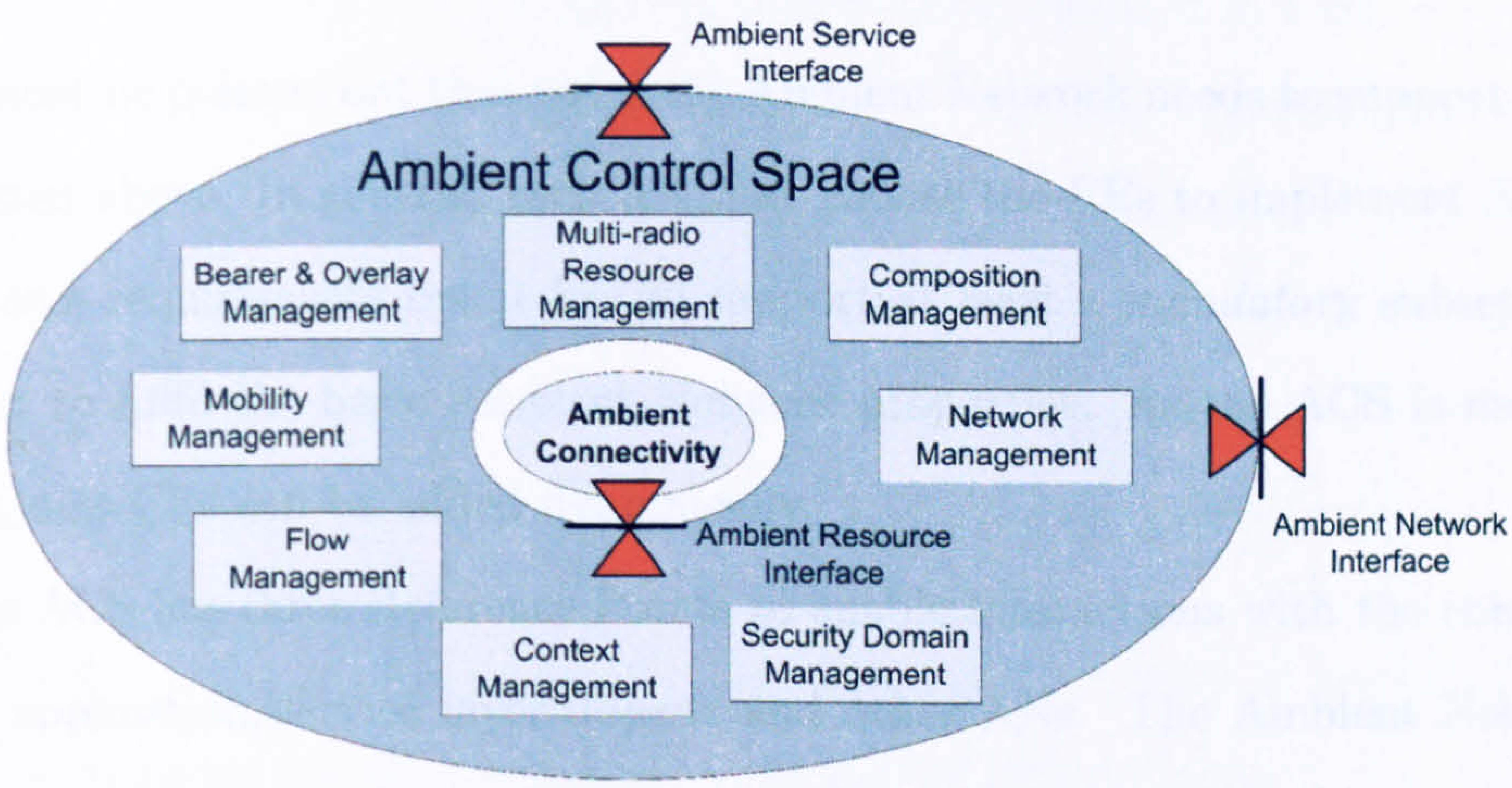


Figure 6.1: Ambient Network: Logical View

The ACS is a modular construct comprising a well-defined but flexible set of control functions or Functional Entities (FEs). Some of the FEs currently defined are:

- Bearer and Overlay Management
- Multi-Radio Resource Management
- Connectivity Management & Generic Link Layer

- Flow & Mobility Management
- Network Advertisement & Discovery
- Composition Control
- SLS Management & Compensation
- Network Management

It must be pointed out that not every Ambient Network needs to support all of the FEs listed above. In general, each AN may choose the FEs to implement depending on its own requirements but it has to support at least a *mandatory* subset of them in order to fulfil the basic Ambient Network properties. As the ACS is modular in nature, new FEs can be added dynamically.

The ACS has three Reference Points to enable interactions with the connectivity plane, application/service layer objects and other ANs. The Ambient Network Interface (ANI) is used to connect control spaces of different ANs. Besides facilitating *inter-ACS* communication, it can also be used for *intra-ACS* communication between different FEs of the same ACS. The Ambient Service Interface (ASI) supports interactions between the ACS and application layer entities. It enables applications and services to use ACS functions for establishment, maintenance and termination of end-to-end connections. The Ambient Resource Interface (ARI) is situated inside an Ambient Network node between the ACS and the connectivity plane and provides technology-independent mechanisms for the ACS to control and manage connectivity resources such as routers, switches, radio elements (terminals, relays, access points), media gateways, middleboxes etc.

6.2.2 Network Composition

Network Composition is one of the fundamental principles that underpin the Ambient Network architecture. The primary goal of Composition is to enable *plug and play* interworking between Ambient Control Spaces as well as sharing of control among Ambient Networks. Composition goes beyond what Internet and mobile networks can provide today where control-plane cooperation happens primarily for packet forwarding. Furthermore, it also goes beyond interworking possible in today's commercial mobile networks, where control interworking, e.g. roaming agreements, need to be negotiated and realized manually. Composition also enables sharing and delegation of control over physical and logical resources if so desired, e.g. a WLAN operator may decide to give up authentication and charging control and hand it over to the operator of a UMTS network [58]. Composition is characterised by the following features:

- Generic - the process is not dependent on the presence of particular control functionality, nor is it specific to a particular network type.
- Scalable - provides both upwards and downwards scalability.
- Extendable - can be easily extended to include new type of control functions and resources
- Plug and Play - automatic operation that functions without (or with minimal) human interaction.
- Adjustable - operation whose behavior can be configured based on context such as preferences, ambient awareness etc.
- Controllable - operation can be limited and controlled by policies.

These properties imply that Composition is well-suited to facilitate dynamic cooperation in future heterogeneous networking environments characterised by the presence of networks of different types and sizes. It is desirable to support different levels of interworking between networks so that a wide variety of technical scenarios and business models can be realised. Bearing this in mind, three different types of Compositions are defined:

Network Interworking: The composing ANs maintain full control of their own resources and continue to stay as separate networks after composition.

Control Sharing: The composing ANs stay separate, but share some or all of their individual resources. In this case, a new virtual AN is created with its own ACS alongwith the physical and/or logical resources being shared. A special case is *control delegation* where one AN delegates the control of certain resources to another AN.

Network Integration: The composing ANs merge to create a new AN that consists of the control functions and resources from both networks. In this case, from the point of an external observer, only the unified network is visible.

The process of creating different types of Compositions is coordinated and orchestrated by the Composition-FE (C-FE) which is one of the mandatory control functions of the ACS that each Ambient Network must have. In the next section, the different procedures that constitute the Composition process are described in detail.

6.3 Composition Process

Network Composition is an operation involving two Ambient Networks. The Composition process consists of a number of phases:

- Media Sense
- Advertisement & Discovery
- Network Attachment
- Composition Negotiation
- Composition Realization

Note that during a particular instance of Composition, it is not necessary that these phases are passed one-by-one. This is particularly true of the first 3 as will be clear from the description of the various phases below.

6.3.1 Media Sense

Composition between two networks requires that there is a communication medium between them. Therefore, media sensing is the starting point of the process. It can be triggered by different types of events, depending on the specific scenario being considered. For example:

- A WLAN-enabled laptop automatically starts scanning for access points when it is switched on;
- PANs belonging to two friends detect each other when they come in range;
- A train's mobile router detects a WLAN access point as it arrives at a station.

6.3.2 Advertisement & Discovery

This phase is used by an Ambient Network to advertise itself to the other AN or to discover more information about it (or both) in order to make a decision whether to proceed with composition. This information may relate to capabilities, resources and services. Depending on the specific scenario, tariff-related information may also be exchanged. For example, a *provider* AN may advertise QoS-enabled communication links to potential *customer* ANs. Similarly, a PAN may advertise willingness to share its Internet connection.

The discovery process takes two forms: passive and active. The former refers to the situation where an AN listens to *advertisement* messages sent out by others whereas in the latter case, advertisements are requested by sending *solicitation* messages. Typically, a mixture of legacy and AN-specific mechanisms are used during this phase. Several possibilities exist with respect to distribution of advertisements:

- Embed information in Layer 2 (L2) beacons of the particular wireless technology in use;
- Send special L2 control messages using distribution mechanisms supported by the underlying wireless technology;
- Embed in messages exchanged during network attachment phase (further discussed below);
- Send as ACS signalling across the ANI.

The choice of method depends on a number of factors such as the size and nature of information to advertise, security requirements, level of trust with potential recipients etc. Note that the first two options require modifications for each wireless technology concerned. Furthermore, because of size and security considerations, beacons can only carry small amount of advertising information. However, additional Information Elements can be inserted into other L2 control messages which typically use unicast or multicast mechanisms unlike beacons which are generally broadcast messages. The most flexible option is to use special ACS signalling messages designed specifically for this purpose. However, this can only be done after AN attachment procedure is completed. Alternatively, some advertising information can be inserted into the attachment messages, as described below.

6.3.3 Network Attachment

The purpose of this phase is to establish a secure communication link between the two networks so that ACS signalling messages can be exchanged. The AN Attachment Protocol (ANAP) [60] has been designed to setup connectivity and security association. ANAP enables the two ANs to perform mutual authentication and authorization using cryptographic identifiers and establish a security association. The process involves a 4-way handshake derived from the Host Identity Protocol (HIP) base exchange [61]. Additional data can be piggybacked on to the ANAP messages. Thus, advertising information can be inserted, if required, as illustrated in Figure 6.2. Note that different levels of protection are available for the advertising information, depending on the ANAP message used for piggybacking. Furthermore, the final two messages (shown as dashed arrows) are optional.

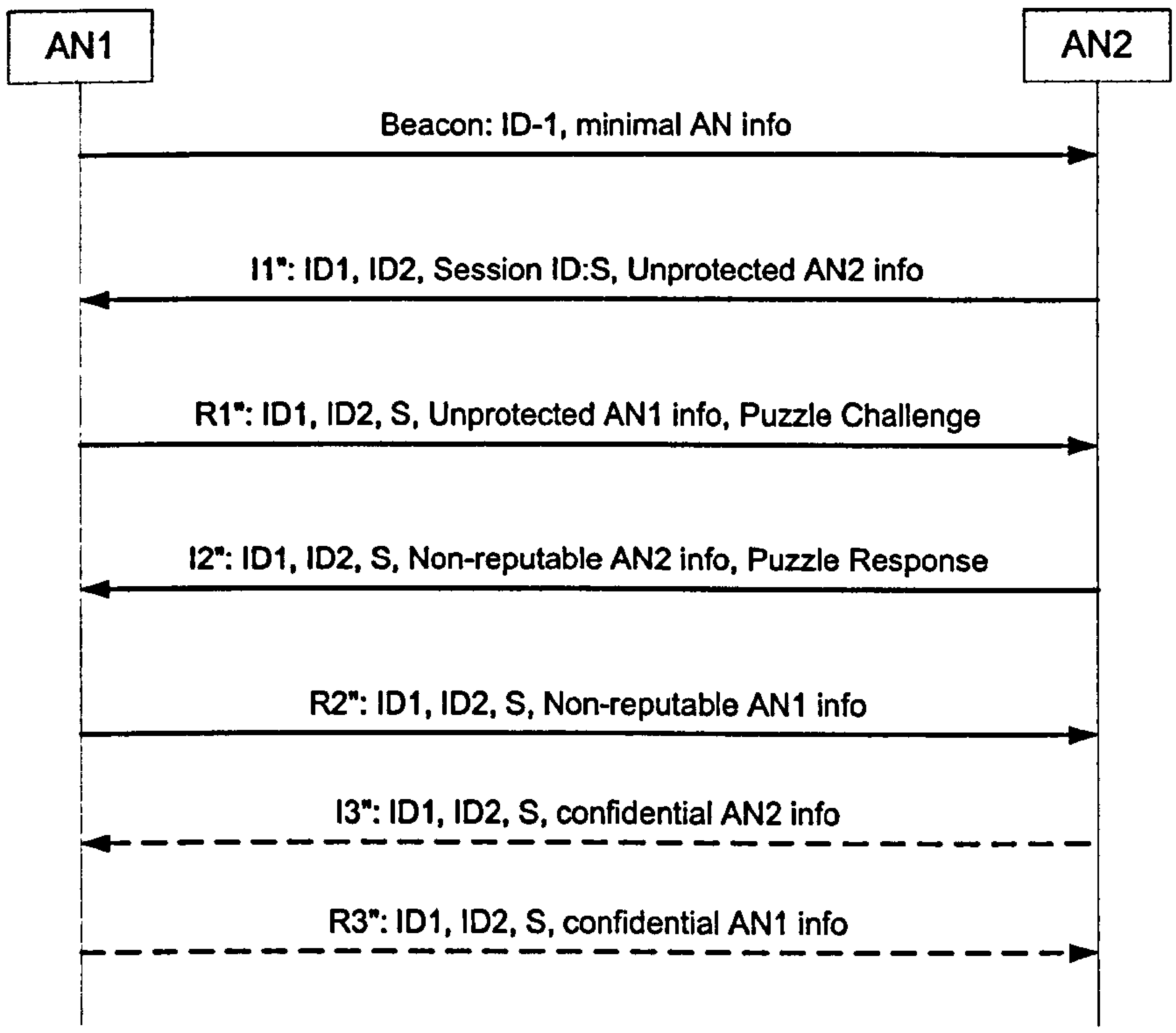


Figure 6.2: Ambient Network Attachment Protocol

6.3.4 Composition Negotiation

Information exchanged via advertisements using the different mechanisms described above is used in conjunction with policies to decide whether to start composition negotiation. As mentioned earlier, composition is a mechanism to enable cooperation between networks regarding usage and control of network resources and services. The parameters of this cooperation are defined in a Composition Agreement (CA) which is negotiated during this phase by the two composing ANs. The CA includes identifiers of the two ANs, the policies to be followed in the composed AN about access and control of logical as well as physical resources, compensation information etc. Each network will typically maintain a database of CA templates and *off-the-shelf* CAs for use during composition negotiations.

Composition negotiation is coordinated and orchestrated by a special control function called Composition-FE. The process starts with the selection of a CA template. A template usually has some of the data fields pre-defined while other fields are either blank or a range of values is provided. The C-FE fills some of them and consults other local FEs to put suitable information into other fields. Finally, the remaining fields are left to be provided by the other AN. The negotiation process is flexible in the sense that the recipient of a CA proposal is also allowed to offer a counter proposal of its own.

6.3.5 Composition Realization

Realization is the final phase of the composition process during which the negotiated CA is implemented by the two networks. This involves configuration of logical and physical network elements to comply with the CA. For example, if the CA includes an SLS for bandwidth guarantees, the appropriate routers and switches will be configured to provide the desired QoS to data flows.

The lifetime of a composition is defined in the CA itself. Upon expiry of a CA, two outcomes are possible: i) the CA is re-negotiated which in the simplest case may involve extending the validity of the original CA without modifying its contents; ii) the CA is deleted and the configurations made in the realization phase are *undone*.

6.4 Composition Use Cases

The preceding sections described the composition process in detail. Here, a set of scenarios is presented to illustrate how composition can be used to enable dynamic interworking between networks in real-world scenarios.

6.4.1 Composition between Personal Area Networks

Consider a scenario with two PANs belonging to users A and B respectively. PAN-A is already composed with the home wireless broadband network of A. User A wants to share its Internet access, printer and music library with user B. In today's world, this will require that each of the three resources are configured separately in both PANs. For instance, the Internet gateway device of PAN-A has to be configured to allow Internet connection sharing, the access rights of the printer have to be changed and directory permissions of the music library have to be modified. Similarly, the Internet gateway node of PAN-B has to be configured to use the Internet connection sharing facility provided by PAN-A and so on.

Network composition provides an automatic and dynamic mechanism to facilitate such cooperation. In this particular case, the CA between PAN-A and PAN-B will specify the resources being shared and additional information required for configuration. Compensation parameters may also be included if user A wants to charge user B for the services provided as part of the composition. In the realization phase, the resource-related parameters provided in the CA are used to configure the network elements. The different FEs of the ACS which control the aforementioned resources are responsible for configuring them.

6.4.2 Composition between End Users and Public Hotspot Networks

The proliferation of public hotspot networks, mainly based on WLAN technology, has made it easier for end users to get high-speed access to the Internet. However, quite often, these hotspots are tied to some ISP or MNO and users either need to use their existing subscriptions with these networks or setup a short-term subscription agreement with the hotspot operator using pre-paid vouchers or usage-based credit/debit card payments. Such agreements are currently pretty basic, offering best-effort Internet access. End users are often interested in getting more than that, for example, QoS guarantees, enhanced security for certain types of application data and so on. In addition, users are also interested in comparing offers from multiple hotspot networks wherever possible to find the one which best matches their individual needs. Such wide-ranging relationships between end users and operators is difficult to realize using current technology.

Network composition provides the framework for supporting more flexible interworking between hotspots and end users. The advertising process can be used by hotspots to provide information about the basic and value-added services being offered, thereby helping users make more intelligent network selection. The CA between the two will define the services and associated guarantees provided by the hotspot to the user. Furthermore, compensation details will also be in the CA.

6.4.3 Composition between WLAN and 3GPP Network

The last scenario comprises two access networks, one of which is a WLAN hotspot while the other is a 3GPP network providing global access to its subscribers. The networks are assumed to belong to independent business and legal entities. The WLAN operator wants to expand its customer base by extending access to users subscribed to different 3GPP operators. Currently, this is done by pre-defined business agreements and in most cases, this is restricted to one or two operators because scalability reasons preclude the possibility of having agreements with every 3GPP network.

Network composition enables establishment of dynamic agreements between a WLAN hotspot and multiple 3GPP networks. When a subscriber of 3GPP network A detects a WLAN hotspot and requests Internet access, the WLAN initiates composition with network A, if no CA with it exists currently. Once the two network agree on a CA, it is realized and Internet access granted to the user based on its subscription with network A. The charging relationship between the two networks is defined in the CA. Subsequent Internet access requests from other subscribers of network A are granted on the basis of the existing CA. Similar CAs can be negotiated and realized as and when required with other 3GPP networks. Note that these dynamic CAs will be in addition to other more 'permanent' agreements with *friendly* and *popular* 3GPP networks whose subscribers are more frequent users of the hotspot.

6.5 Signalling for Composition

The different phases of composition procedure involve exchange of control signalling between composing Ambient Networks. This includes broadcast of beacons, distribution of AN advertisements using unicast, multicast or broadcast mechanisms, unicast signalling for AN attachment, composition negotiation, realization and decomposition. The signalling requirements during the various phases of the composition process are different. Therefore, a number of protocols have been defined to cater to these requirements. Of these, ANAP has already been described briefly earlier. Here, the protocol used for composition negotiation and realization is presented.

Signalling between peer C-FEs during the composition process is carried in a protocol designed specially for this purpose, referred to as the Composition GANS Signaling Layer Protocol (C-GSLP). GANS or Generic Ambient Network Signalling is a suite of protocols designed for signalling between Ambient Control Spaces over the Ambient Network Interface. In the following, first a brief overview of GANS is presented and then the Composition-GSLP is described briefly. Note that the detailed protocol specification is provided in Appendix A.

6.5.1 Generic Ambient Network Signalling Protocol Suite

The GANS protocol suite has been designed to support different types of inter-ACS signalling between dynamic and heterogeneous networks. It follows the design philosophy adopted by the Next Steps In Signalling (NSIS) Working Group in the IETF by adopting a two-layer model, as shown in Figure 6.3

The lower layer, GANS Transport Layer Protocol (GTLP), takes care of tasks

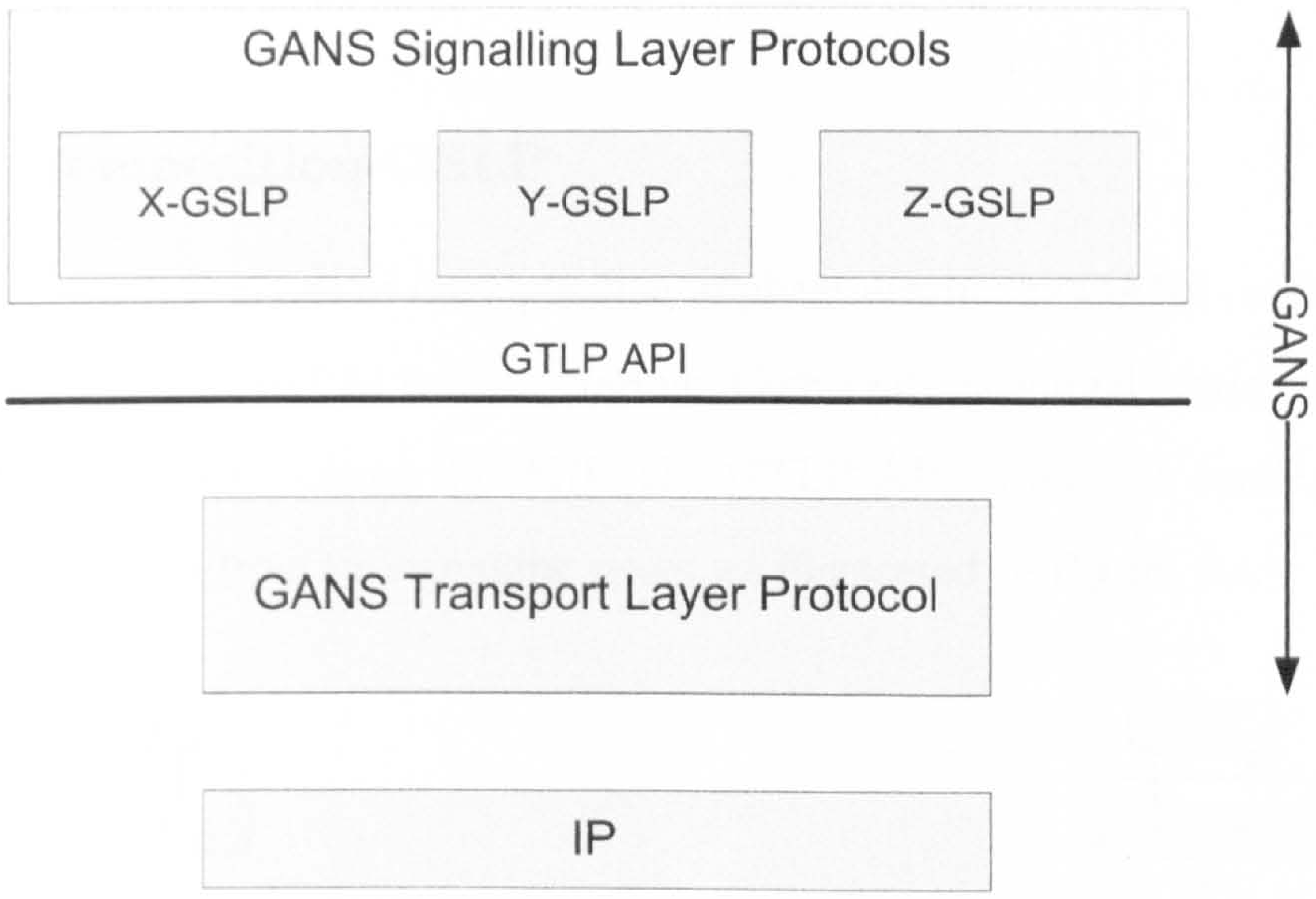


Figure 6.3: 2-layer Model for GANS

common to all signalling applications: signalling peer discovery, security relation establishment between peers, and bi-directional message transportation between them. The upper layer consists of a number of GANS Signalling Layer Protocols (GSLPs), each designed to meet specific requirements of signalling applications. Examples of GSLPs include protocols for Inter-Network QoS Agreements, Compensation and Composition signalling, respectively.

The GTLP offers a well-defined Application Programming Interface (API) to GSLPs for sending and receiving messages. GSLPs can specify a set of Message Transfer Attributes (MTA) when passing a message over the interface to indicate how it should be transported by the GTLP. Currently three attributes are defined: Security, Reliability and Priority. Based on the MTA, GTLP decides the transport protocol (TCP, UDP, DCCP etc.), the type of security mechanism and priority scheme. Further details on the GTLP can be found in [62].

6.5.2 Composition-GSLP

Composition-GSLP is one of the signalling applications in the GANS protocol suite. The protocol is designed to transfer various Composition-related payloads between peer Composition-FEs across the ANI. The GTLP API is used to send/receive C-GSLP messages to/from its signalling peers, as illustrated in Figure 6.4.

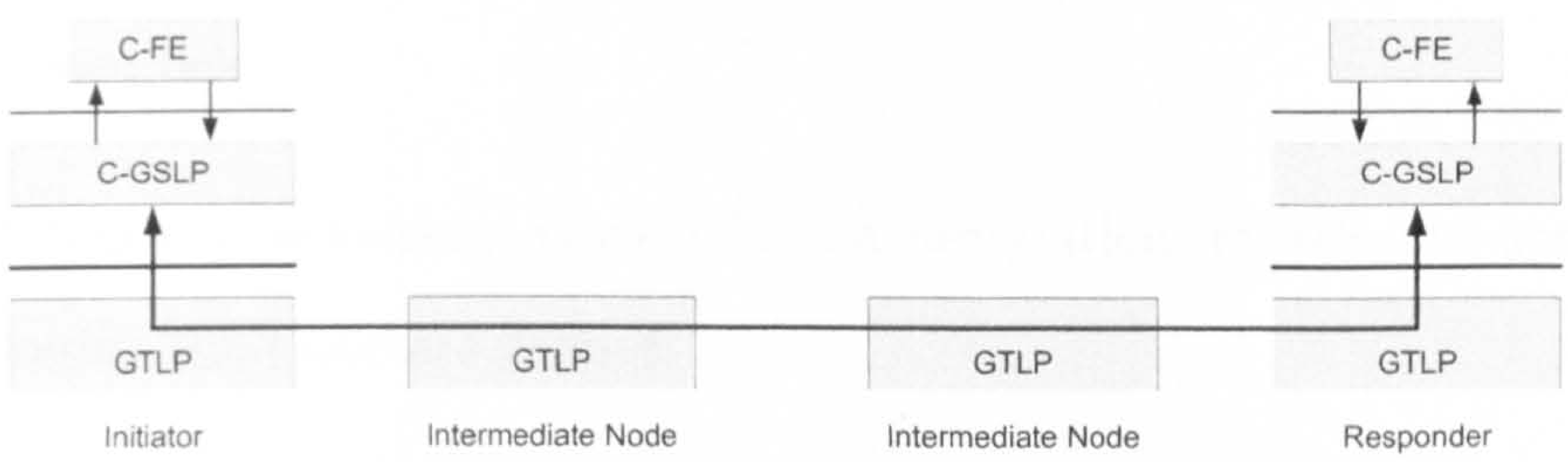


Figure 6.4: C-GSLP Operation

C-GSLP signalling involves two nodes: Initiator and Responder. Initiator is the C-GSLP instance which starts the signalling session while Responder is the destination C-GSLP. Since composition is essentially a bilateral process, signalling is typically end-to-end. In other words, although a signalling message, in general, may traverse a number of intermediate nodes, the message is terminated only at the Responder. The forwarding of messages happens at the GTLP layer and the contents of C-GSLP payload are not visible to the intermediate nodes.

When the C-FE wants to send control data to its peer, it is encapsulated in a C-GSLP message and passed alongwith other information such as the MTA, destination address, session identifier, to GTLP using the API. GTLP first checks if there is an existing signalling association with the destination, based on the information received over the API and if one is found, the C-GSLP message is encapsulated in a GTLP packet and sent towards the signalling peer using appropriate transport protocol and security mechanisms. Otherwise, a new signalling association is setup first using the 3-way GTLP handshake [62] and then the message is sent. At the destination, the message is delivered to GTLP and after performing necessary security checks, it is passed to C-GSLP over the GTLP API.

C-GSLP defines three basic message types, each of which has two or more sub-types as listed below:

- **CANEG**: This message is used for CA negotiation, refresh and update. The following sub-types are defined:
  1. CANEG_Negotiate
  2. CANEG_NegotiateAck
  3. CANEG_Validate
  4. CANEG_ValidateAck
  5. CANEG_Cancel
- **CARLZ**: This message is used to coordinate the CA realization process, after the CA has been successfully negotiated. The message sub-types are:
  1. CARLZ_Prepare
  2. CARLZ_Ready
  3. CARLZ_Commit

4. CARLZ_Cancel

- **CADEL**: This message is used during decomposition procedures. It could either be sent after the CA lifetime has expired or when either AN wants to terminate the composition while the CA is still active. This message has the following sub-types:

  1. CADEL_Delete
  2. CADEL_DeleteAck

The C-GSLP messages listed above have to carry diverse signalling payloads. The control data carried depends on the type and purpose of the message. For instance, in case of CA negotiation, the payload will typically include a CA but in some cases, it may only have some high-level CA-specific information such as CA identifier. Therefore, flexible and extensible formats have been defined for these messages. All C-GSLP messages consist of a common header and one or more Type-Length-Value (TLV) style objects of varying length. The detailed message specification is available in Appendix A.

6.5.3 Example Signalling Sequences

The usage of C-GSLP messages during different phases of the composition process is illustrated here with the help of a set of message sequence charts. An example of the composition negotiation process is illustrated in Figure 6.5. Besides the C-FE, both ANs are also shown to have an 'X-FE' which serves as an example of one or more real FEs that are called by the C-FE for consultation during the negotiation process. The C-FE, after selecting a CA (or template), sends it to X-FE so that the latter can either provide information about resources and services under its control or simply acknowledge that the pre-defined information is correct. Thereafter, the CA is sent to the peer C-FE in the other AN which, in turn, consults its own FEs for input in preparing the response which can take three forms: i) unconditional acceptance of the received CA; ii) conditional acceptance based on information provided in the empty/pre-filled fields of the CA and iii) rejection of the CA proposal. In the figure, the second outcome is shown and the revised CA is returned back after which the C-FE of AN1 again consults its FEs and sends a new CA proposal to its peer C-FE. This time, after consulting the local FEs, the C-FE of AN2, accepts the new CA. Finally, the CA is digitally signed by the two ANs.

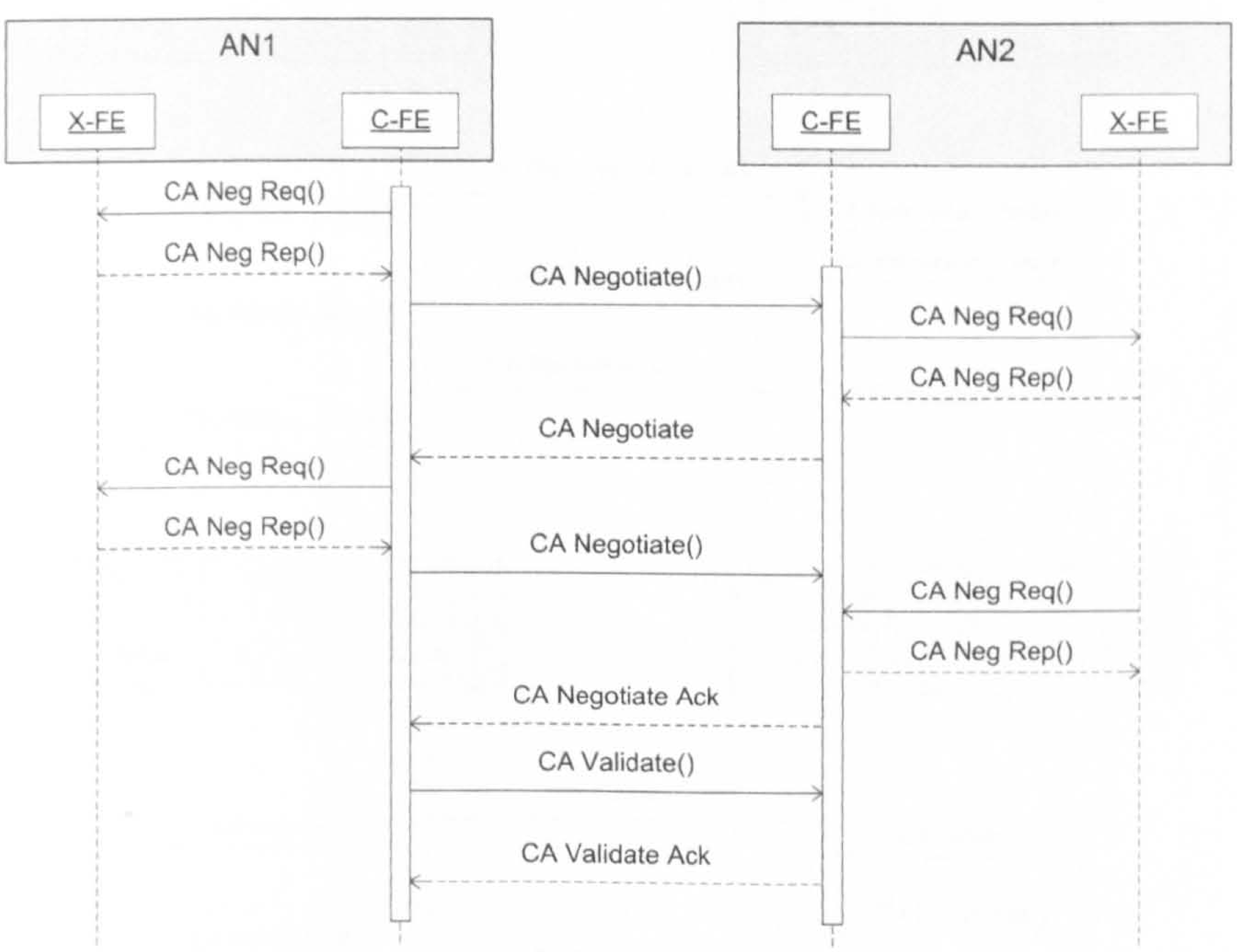


Figure 6.5: Composition Negotiation

Note that Figure 6.5 illustrates only one possible message sequence for a composition negotiation process and many different variations are possible. The C-FE may not consult the same set of FEs in each iteration, e.g. the Compensation-FE will typically be asked to provide input only in later stages of negotiation. In fact, the C-FE may not need to consult with other FEs at all in situations where it has access to all the required information about resources, services and policies . Furthermore, the negotiation may require one or more round-trips. It may even be aborted after a certain number of round-trips, based on pre-defined negotiation policy. The CA realization and decomposition processes are illustrated in Figure 6.6.

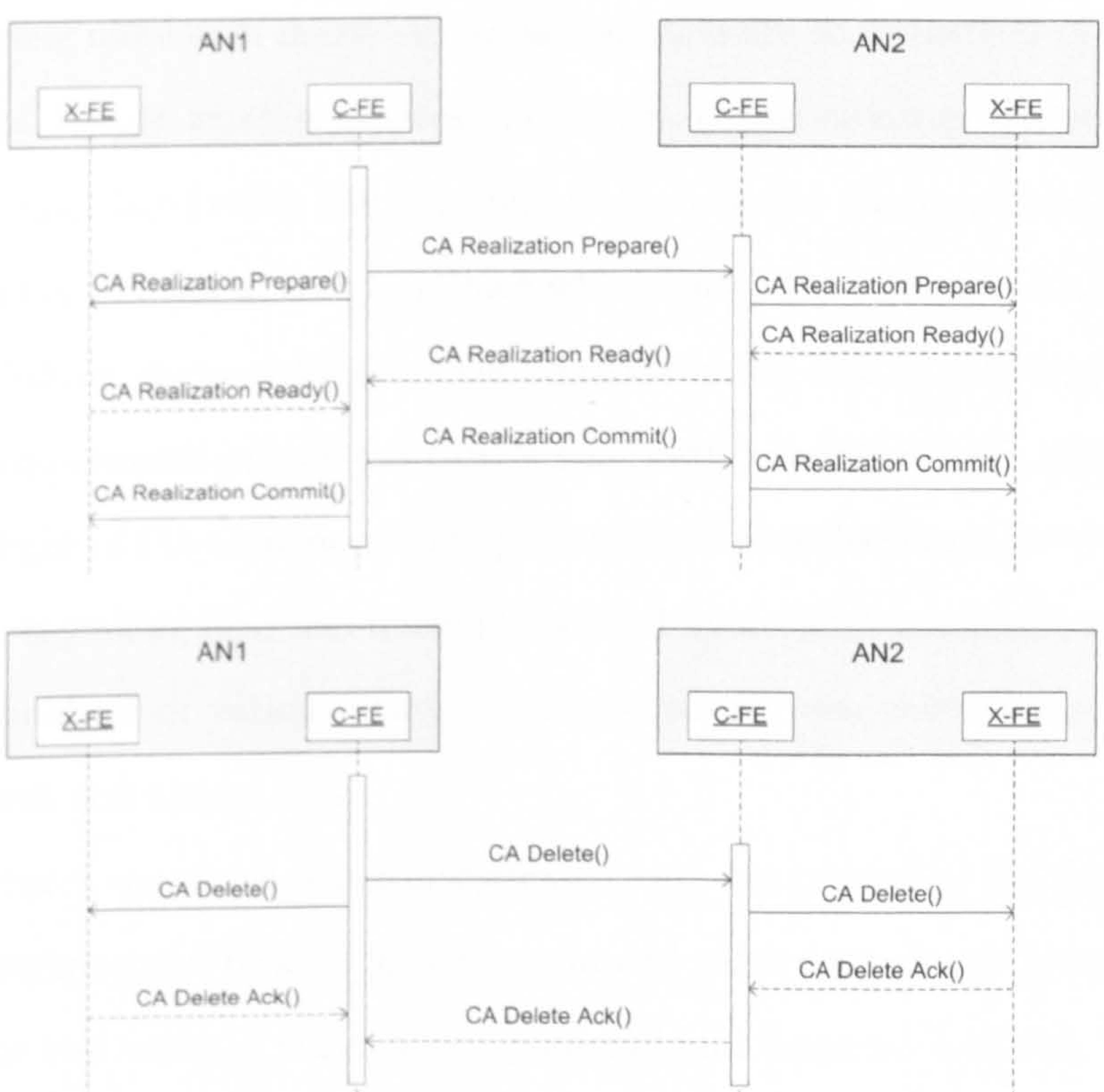


Figure 6.6: Realization and Decomposition

6.6 Analysis of Signalling Load and Delay

The composition process described in the previous sections has been designed to bring more flexibility to interworking between networks. Composition provides a framework to enable inter-network cooperation in the dynamic and heterogeneous scenarios envisaged for future communication networks. Although the procedures are independent of underlying networking technologies, it is clear that they will be applied predominantly in wireless environments. Furthermore, the vast majority of compositions will involve user and access ANs. In the latter case, given the increasing penetration of wireless technology, it is important that the composition process scales with increasing number of users. As far as user ANs are concerned, they are expected to consist of mainly wireless devices and hence, conservation of battery power and wireless channel bandwidth will continue to be a major concern. Furthermore, the diversity in capabilities of user terminals will require that composition scales accordingly. In addition, support for seamless handoffs in the face of user mobility will put stringent requirements on the amount of composition-related delay that can be tolerated. In light of the aforementioned performance considerations, it is important to analyze the signalling load and delay introduced by network composition. Therefore, a detailed analysis of various composition procedures was carried out for scenarios involving user and access ANs.

The research questions being investigated here are related to the expected benefits of the composition process for end users and service providers: greater choice of networks for end users, a wider set of potential end users for operators and in general, more flexible business relations between end users and service providers. These benefits must not come at too high a price in terms of additional latency and consumption of network resources for communication and information exchange within the network. From a dimensioning and scalability perspective, the following questions need to be answered:

1. How does signalling load increase with number of users and providers and also with the "greediness" of users?

2. How large is the load of business related signalling compared to user data ?

3. How much delay is introduced by composition procedures?

The main elements of the scenario used for this analysis are: multiple access networks in a given geographical area, each network advertising its services periodically; a number of users who discover available networks by listening to advertisements, evaluate competing offers, shortlist one or more providers based on their requirements, negotiate and finally select the one that best fits the requirements (both technical and non-technical) to establish connectivity. Figure 6.7 illustrates the scenario used for analysis. Note that each access point represents a service provider. The investigation was done using a combination of mathematical analysis and simulations.

6.6.1 Signalling Load

The analytical approach was used to estimate signalling load due to the composition process for the scenario shown in Figure 6.7. The starting point was to identify the sequence of events when a user attempts to compose with an access AN. The process starts with the user listening to advertisements broadcast by the access networks, which are then evaluated according to the user's requirements and AN1 is selected.

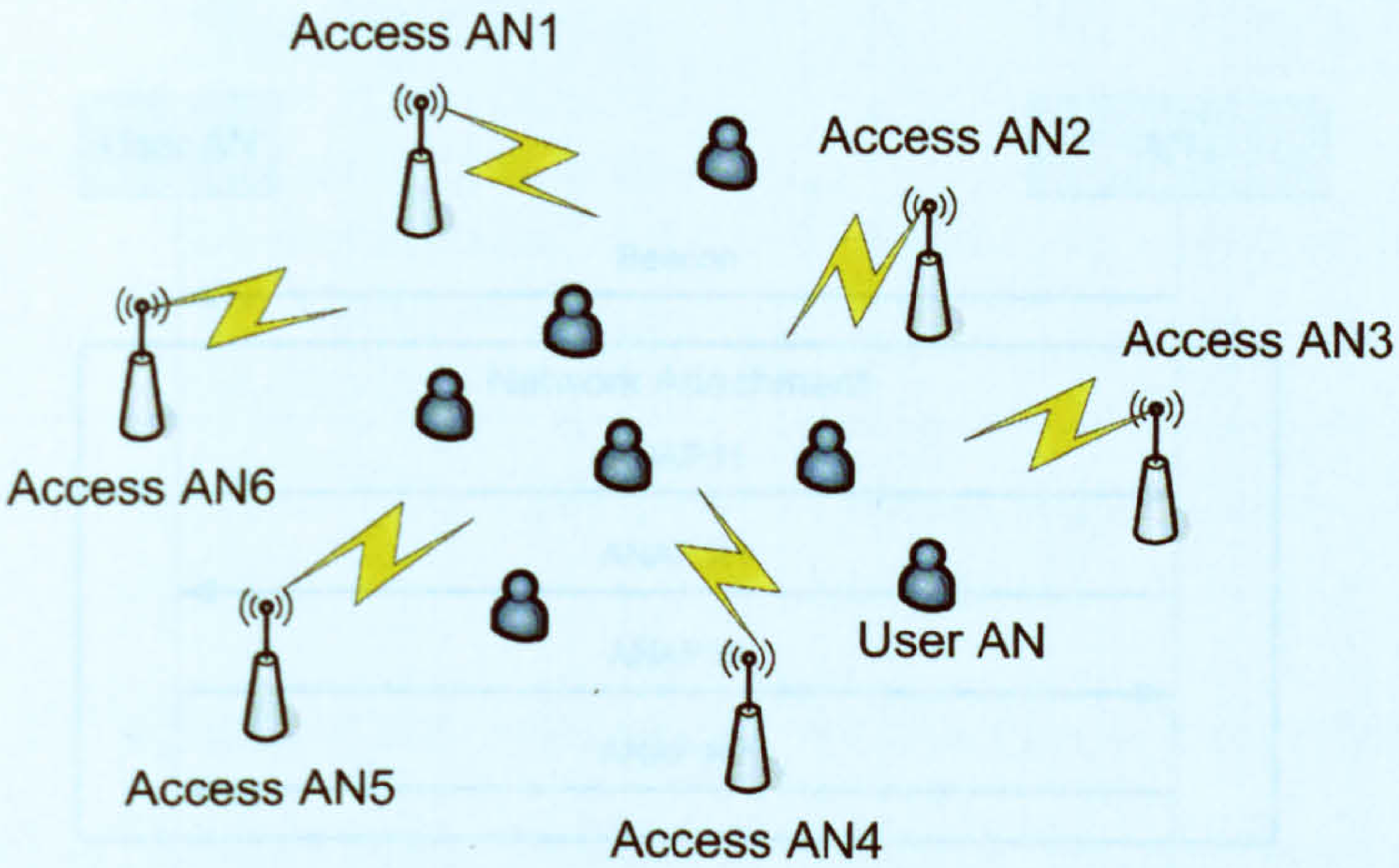


Figure 6.7: Scenario for Analysis

The user AN and AN1 then perform network attachment, followed by composition negotiation and realization and then an application session is established over this connection.

The complete signalling sequence is shown in Figure 6.8. It is divided into several phases, in accordance with the composition phases described in Section 6.3. After advertising using beacons, the 4-way ANAP handshake takes place and then a GANS signalling association is established using the 3-way GTLP handshake. Composition negotiation is shown to take only one round-trip, followed by CA Validation and Realization.

The signalling bits required for each message in Figure 6.8 were computed with the help of the protocol specifications of ANAP and Composition-GSLP were used to determine the payload size, assuming IEEE802.11b as the underlying wireless technology. Details of these calculation are available in Appendix B. Table 6.1 shows the number of bits exchanged over air during each signalling phase.

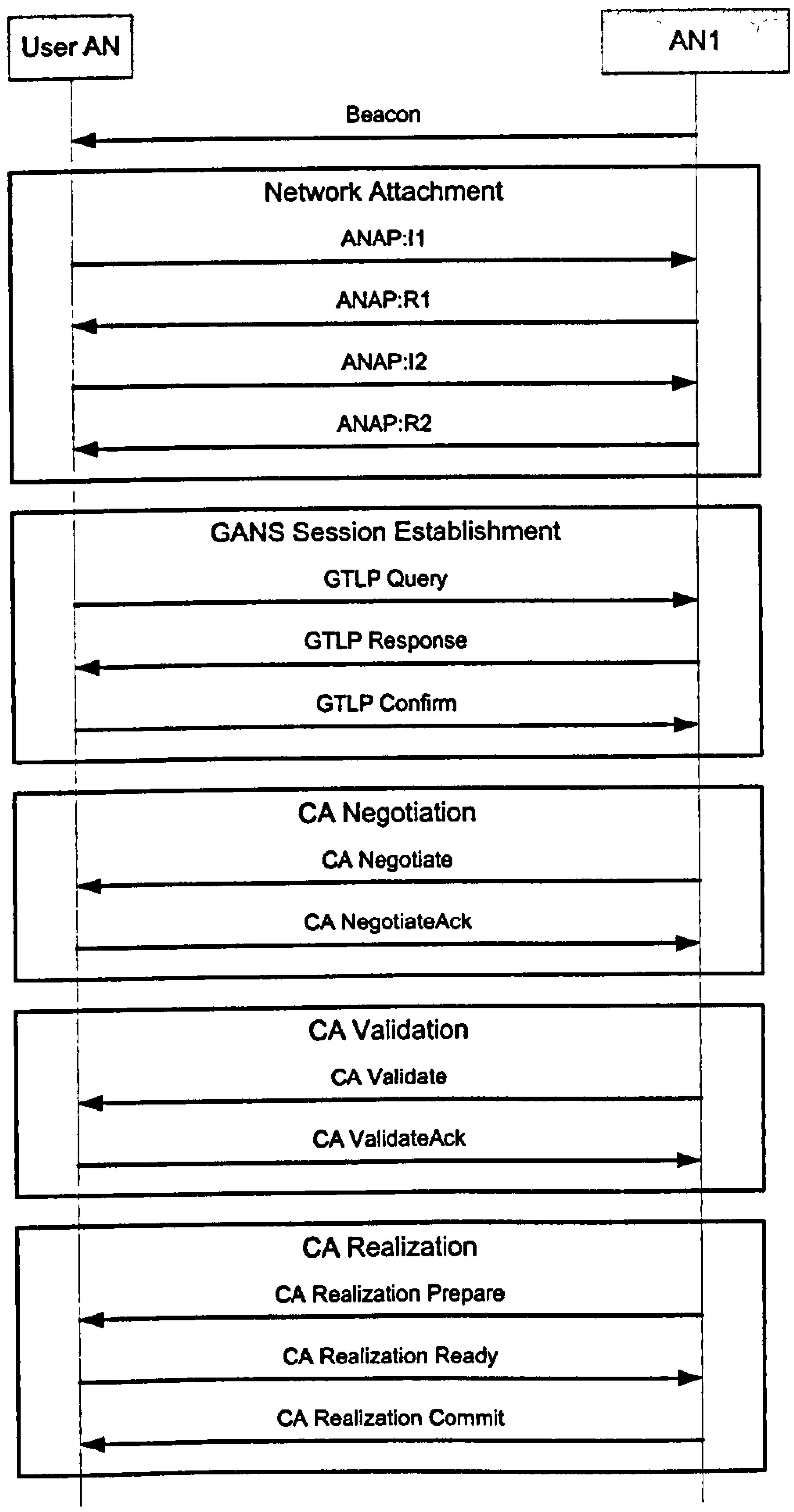


Figure 6.8: Signalling Sequence

Signalling Phase	No. of Bits
Network Attachment (l_a)	13328
GANS Signalling Association (l_g)	4587
CA Negotiation (l_n)	$(2q-1)*2999+1591$
CA Validation (l_v)	3182
CA Realization (l_r)	4773

Table 6.1: Signalling bits in composition phases

Note that the signalling bits required for negotiation is a function of the number of round-trips, q. Furthermore, beacons are ignored because they are transmitted periodically and not on a per-composition basis. The total load for the composition process is

$$l = l_a + l_g + l_n + l_v + l_r \tag{6.6.1}$$

The first scenario consists of a single user AN and multiple access ANs. The user makes a number of "access attempts" per unit time, at the end of which, it successfully completes the composition process with one of the access ANs. Here, two cases are possible: 1) the user attaches to all available networks (during it which it receives further advertisement information), initiates composition with each of them but accepts only one CA proposal, which is then validated and realized; 2) based on the advertisement information received during the attachment phase, the user decides to start composition negotiation with only one access AN.

Assuming that the number of access ANs is M and n is the number of access attempts per unit time, the total signalling load is:

Case 1:

$$L = (M-1)*n*(l_a + l_g + l_n) + n*l \tag{6.6.2}$$

Case 2:

$$L = (M - 1) * n * l_a + n * l \tag{6.6.3}$$

The first part of analysis looks at signalling load as a function of user activity and level of "greediness". The activity level is expressed in terms of number of access attempts per unit time while greediness translates into parallel compositions with several network providers. Figures 6.9 and 6.10 show the signalling load when CA negotiation takes only one round-trip. The results show that for a given number of access ANs, increase in user activity level leads to a linear rise in signalling load. Similarly, for a given user activity level, the load increases linearly with the number of access ANs. When the number of users is N (where $N > 1$), signalling load is uniformly scaled up by a factor of N.

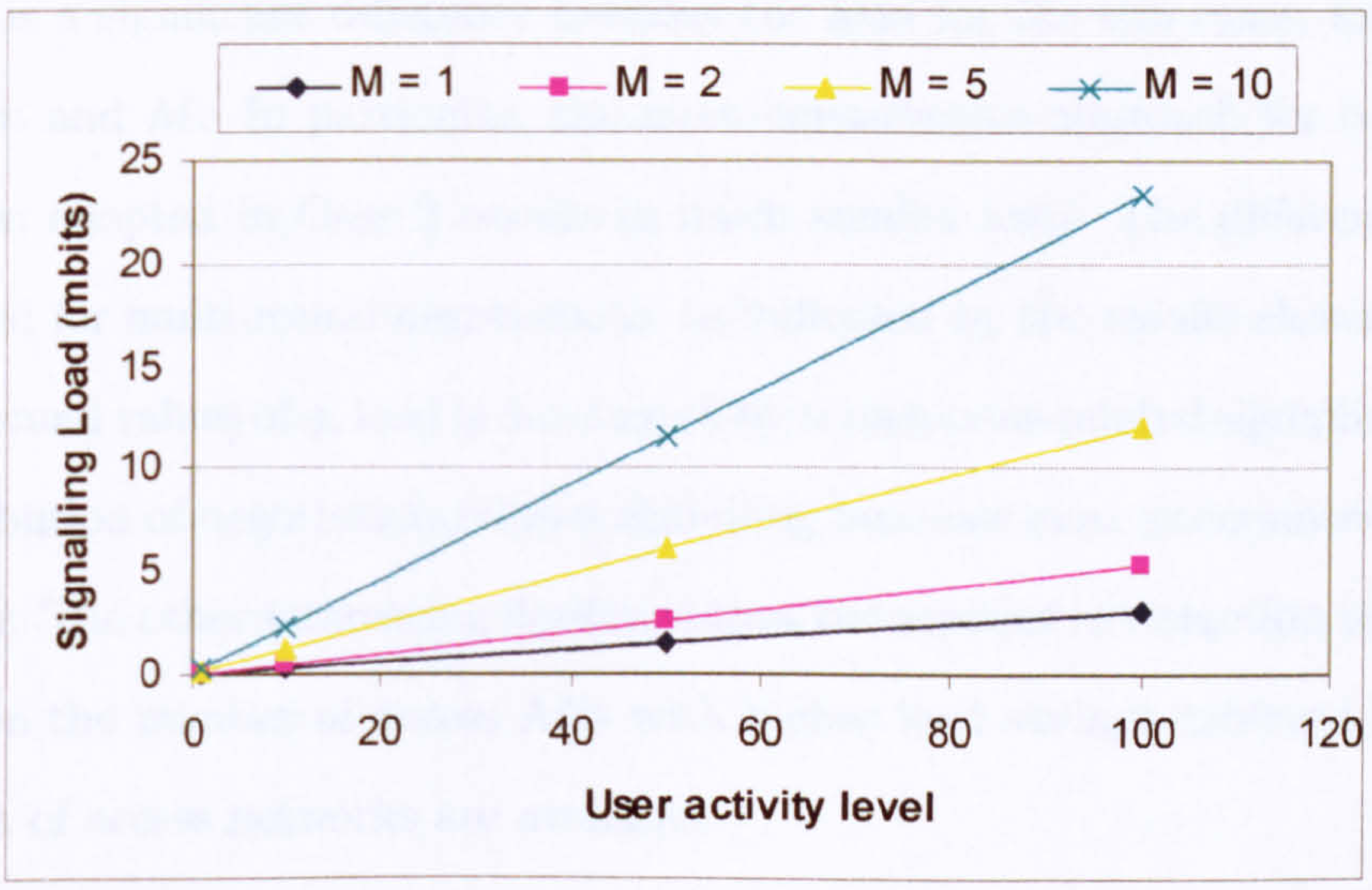


Figure 6.9: Signalling Load for Case 1, q = 1

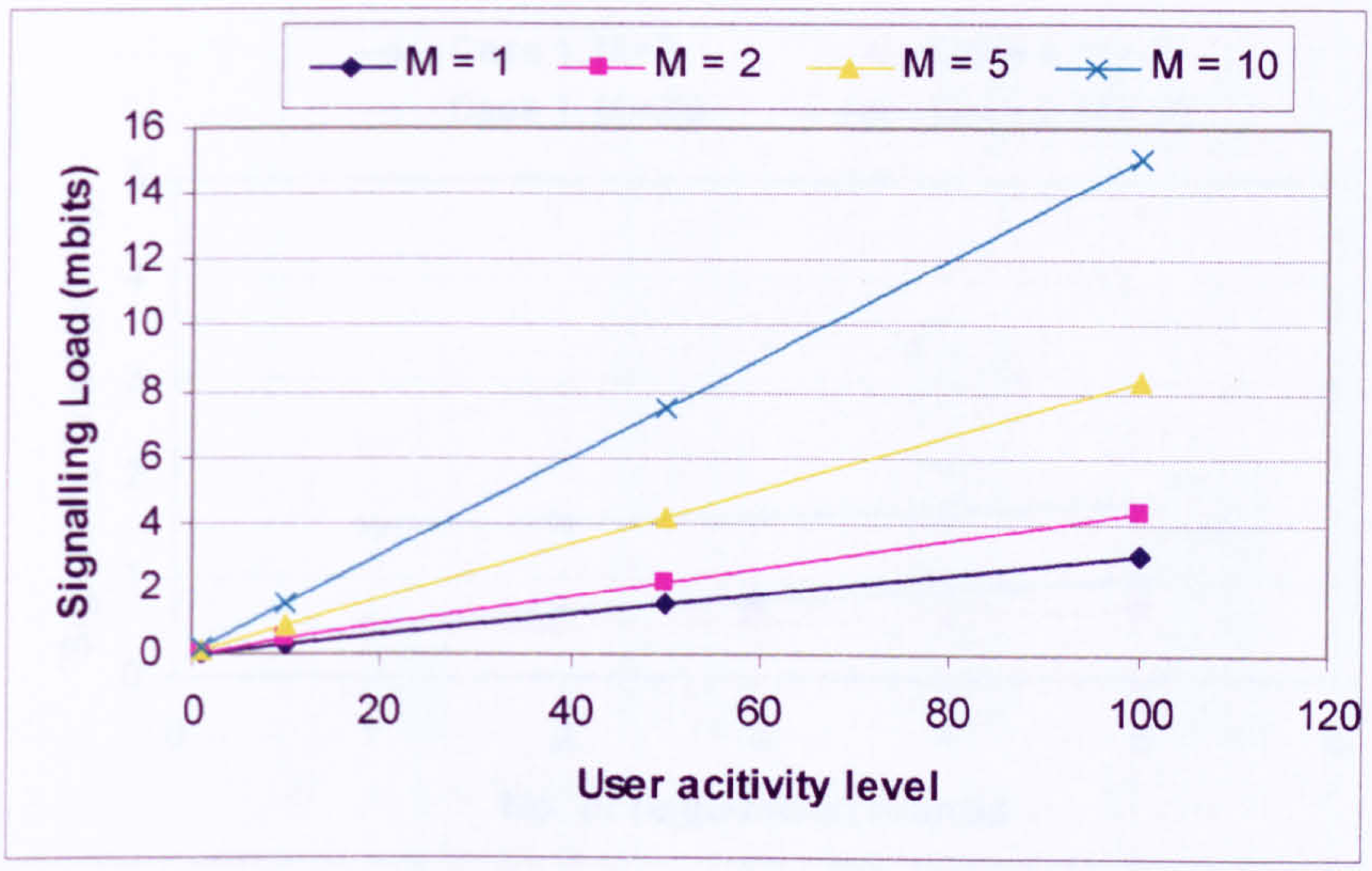


Figure 6.10: Signalling Load for Case 2, q = 1

There is a significant difference between the load for the two cases, for the same values of n and M. In particular, the more conservative approach for composition negotiation adopted in Case 2 results in much smaller load. The difference is more pronounced for multi-round negotiations, as indicated by the results shown in Figure 6.11. For small values of q, load is dominated by attachment-related signalling whereas the contribution of negotiation-related signalling becomes more pronounced at higher values of q. The other interesting finding is that the amount of reduction in signalling depends on the number of access ANs with higher load savings achieved for Case 2 when a lot of access networks are available.

Next, the effect of different negotiation strategies on the signalling load is studied. For a fair comparison, the product of M and q is fixed and then different pairs of values of these variables selected. Figure 6.12 shows the results for Case 1.

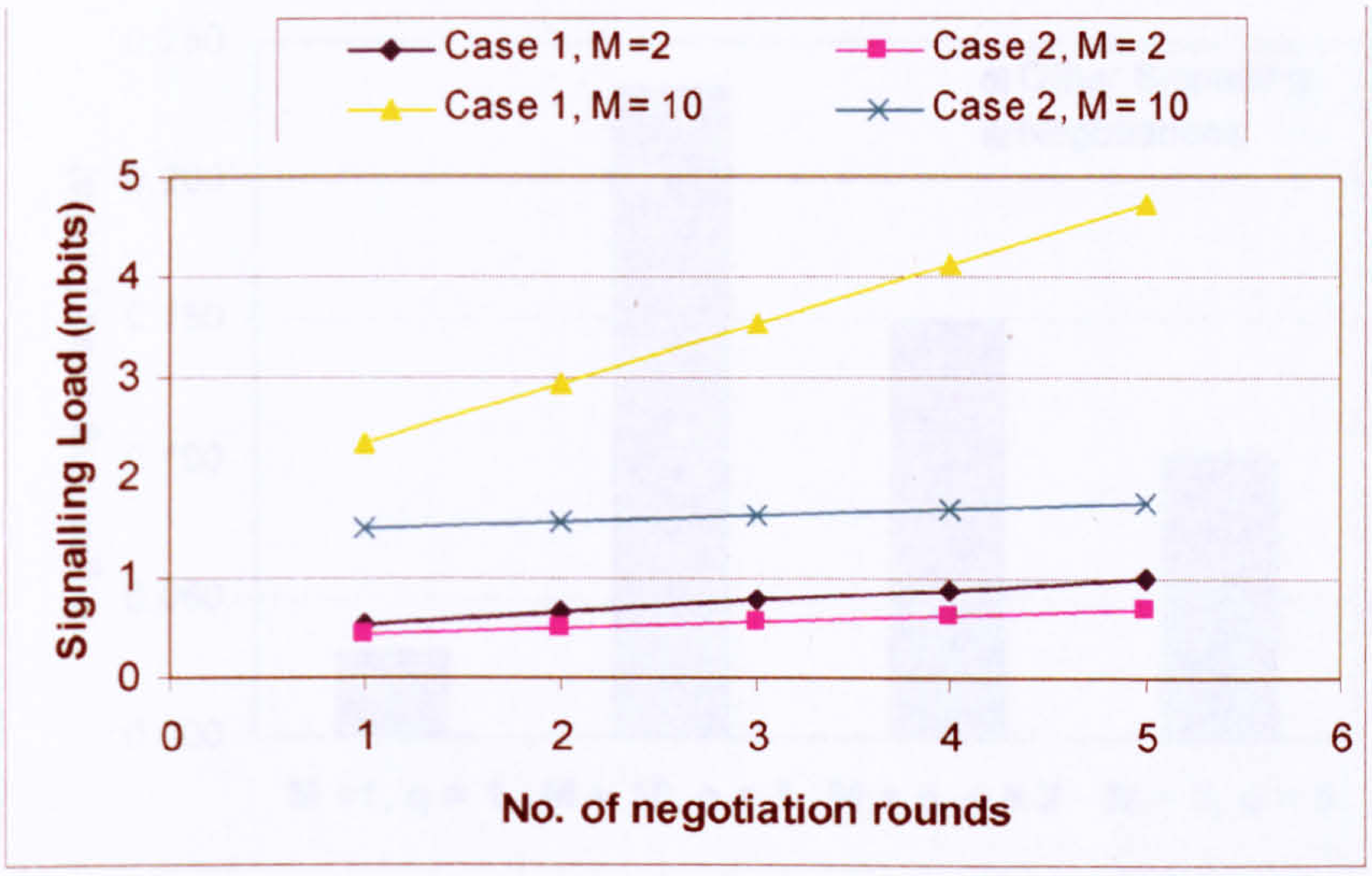


Figure 6.11: Impact of negotiation rounds

The load is split into two components: CA negotiation and all other procedures which include network attachment, GANS session establishment, CA validation and realization. The case of a single-round negotiation with 1 access network represents a low "willingness to negotiate" (WTN) while other cases represent correspond to a relatively high WTN. The results provide lower and upper limits for negotiation load as well as an estimate of the relative load of additional negotiation rounds. The conclusion is that negotiating with many networks consumes more resources compared to the strategy of "negotiating more" with fewer networks. The explanation is that attachment and other "one time" signalling require more bits than multiple negotiation rounds. These findings are corroborated by the results for Case 2, as shown in 6.13.

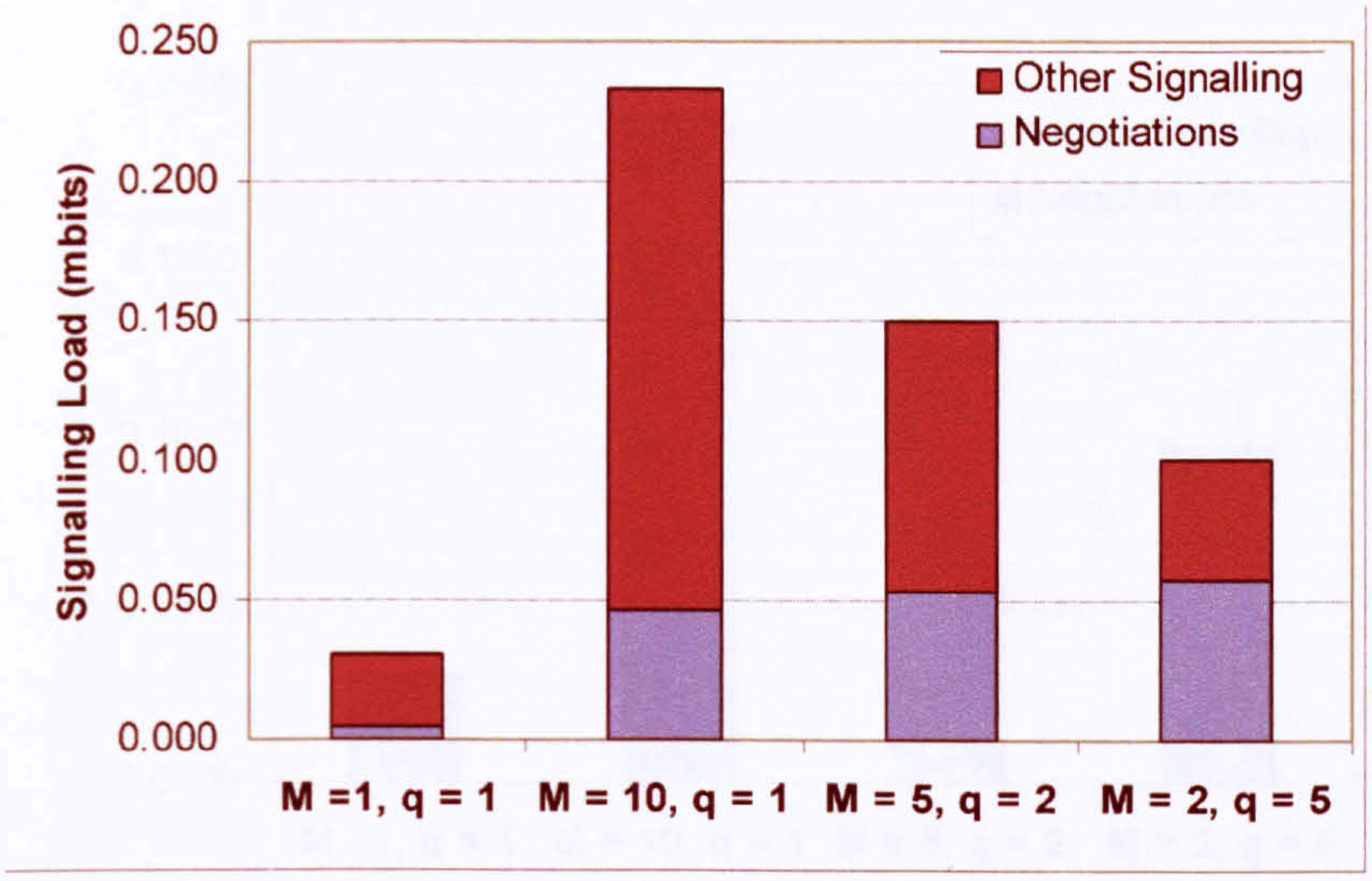


Figure 6.12: Negotiation Load (Case 1)

The results presented so far have looked at signalling load in isolation. In order to put it in context, the load is now compared to the amount of data bits transferred between the user and the selected access AN (with which composition was realised) during application sessions after successful access attempts. The traffic source is a CBR application generating data at 128kbit/s. The session duration is assumed to be exponentially distributed with a mean value of 5 minutes. Figure 6.14 shows the resulting relative signalling load for the case where 100 access attempts per unit time are made with each involving 5-round negotiations for various number of available access networks. Note that the the results are for Case 1 which is the worst-case scenario because the user negotiates in parallel with multiple access networks. It is obvious that the signalling load is very small, even though negotiations last 5 rounds.

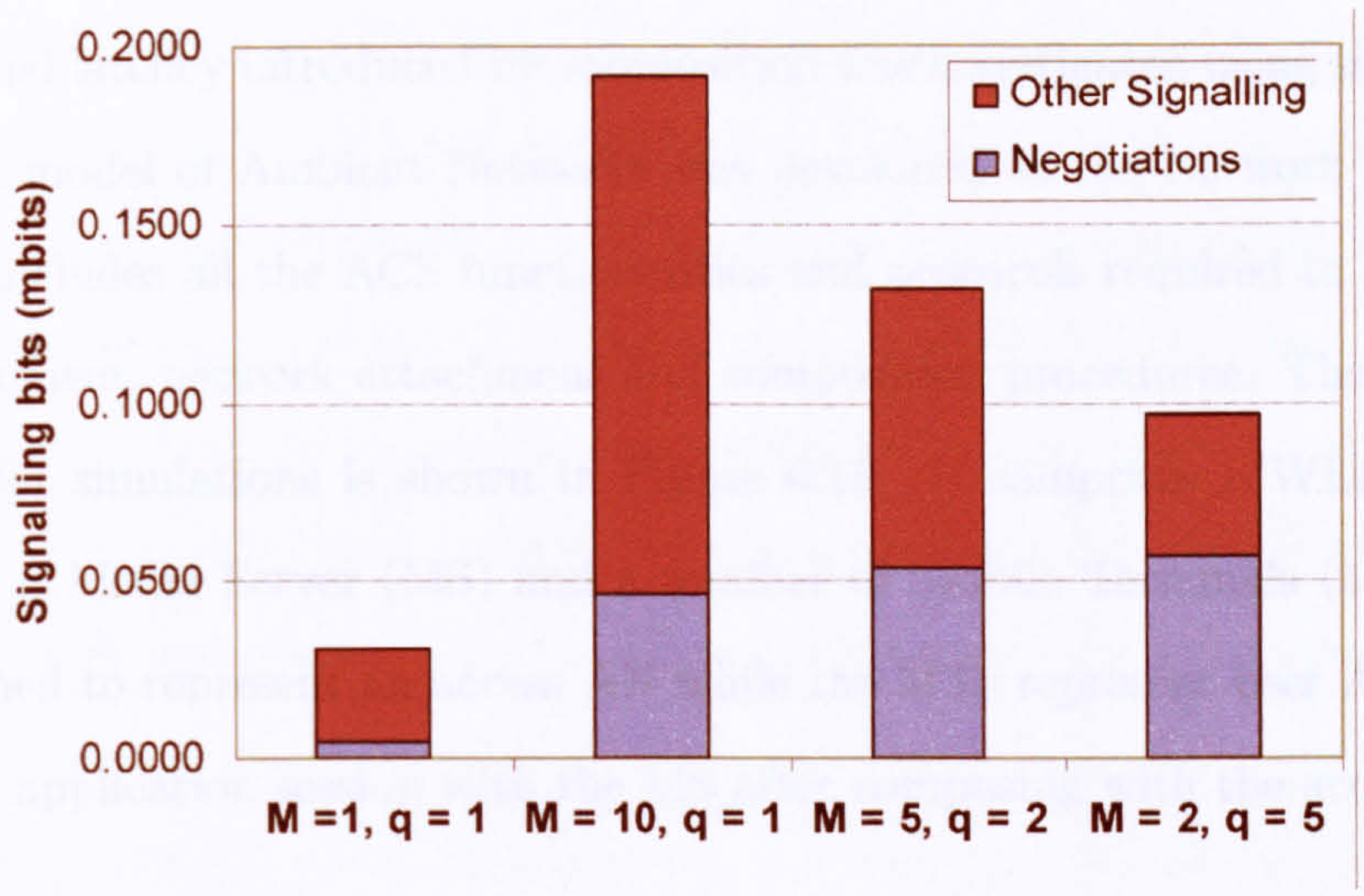


Figure 6.13: Negotiation Load (Case 2)

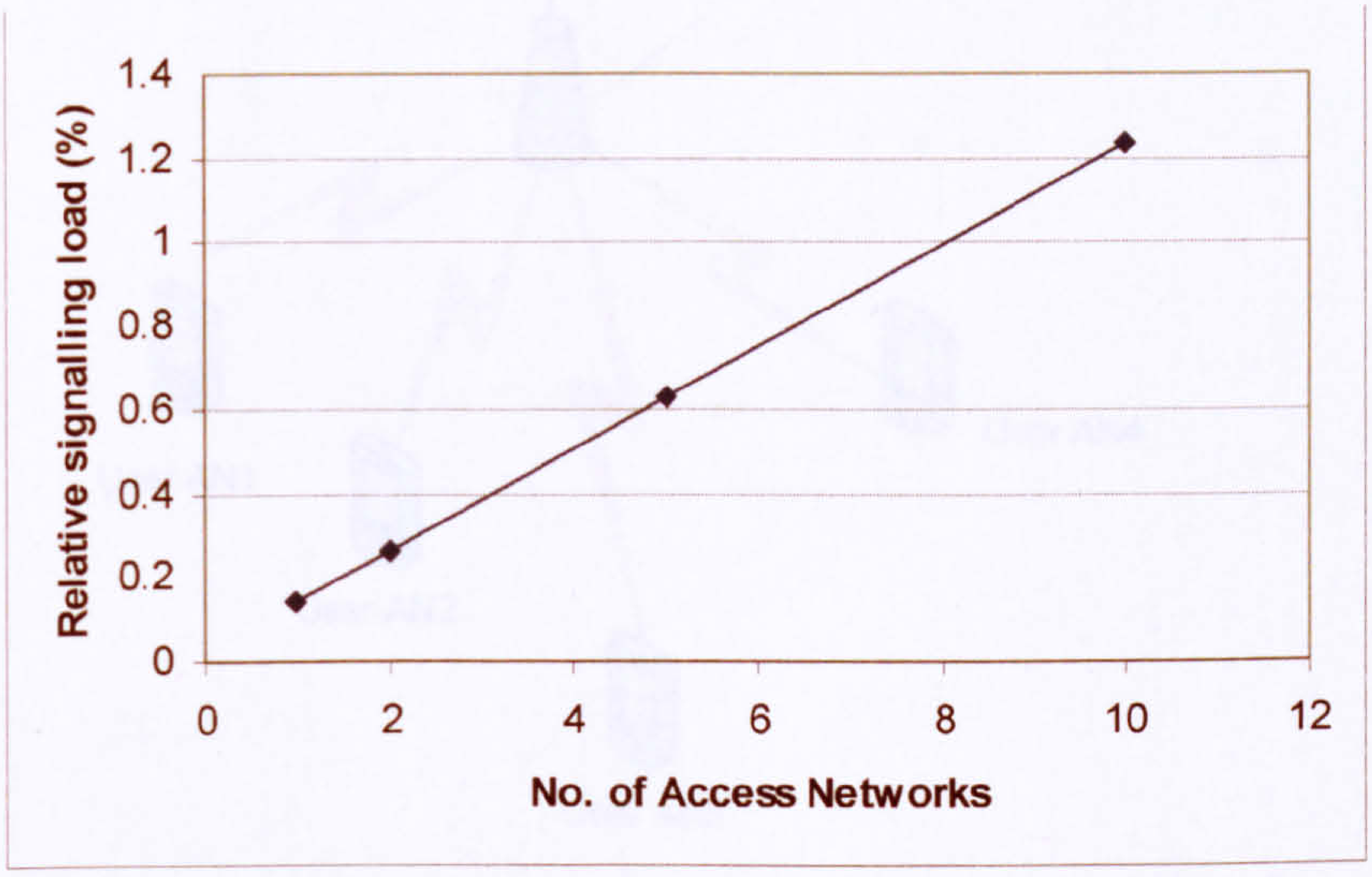


Figure 6.14: Relative Signalling Load

6.6.2 Composition Delay

The additional latency introduced by composition was investigated using simulations. A simplified model of Ambient Networks was developed in the Network Simulator. The model includes all the ACS functionalities and protocols required to implement the advertisement, network attachment and composition procedures. The basic scenario used for simulations is shown in Figure 6.15. It comprises a WLAN Access Point (AP), a Media Server (MS) and a number of Mobile Terminals (MTs). The AP is assumed to represent an access AN while the MTs represent user ANs, which establish an application session with the MS after composing with the access AN.

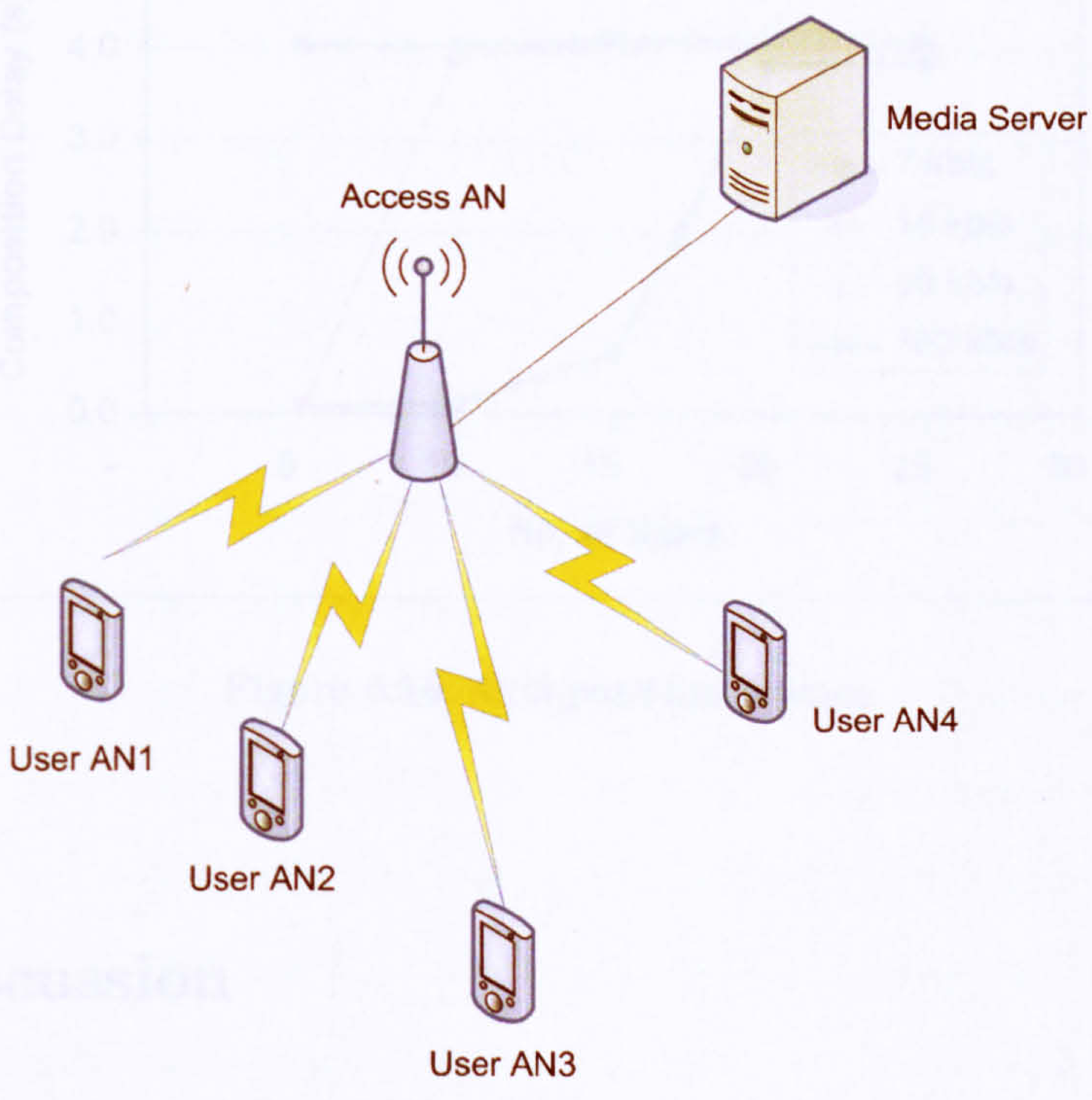


Figure 6.15: Simulation scenario

The simulation model was used to measure composition latency for a scenario characterised by different number of MTs and variable data rates for the application sessions. The scenario has N users, with the first $N-1$ users composing with the AP and then establishing a CBR session with the MS, at the beginning of the simulation. When the Nth user is activated, it discovers the AP, then performs network attachment, followed by a single-round CA negotiation. The results are shown in Figure 6.16. The delay is quite small in lightly loaded conditions but increases rapidly as the load increases and reaches a stable value when the network is fully saturated.

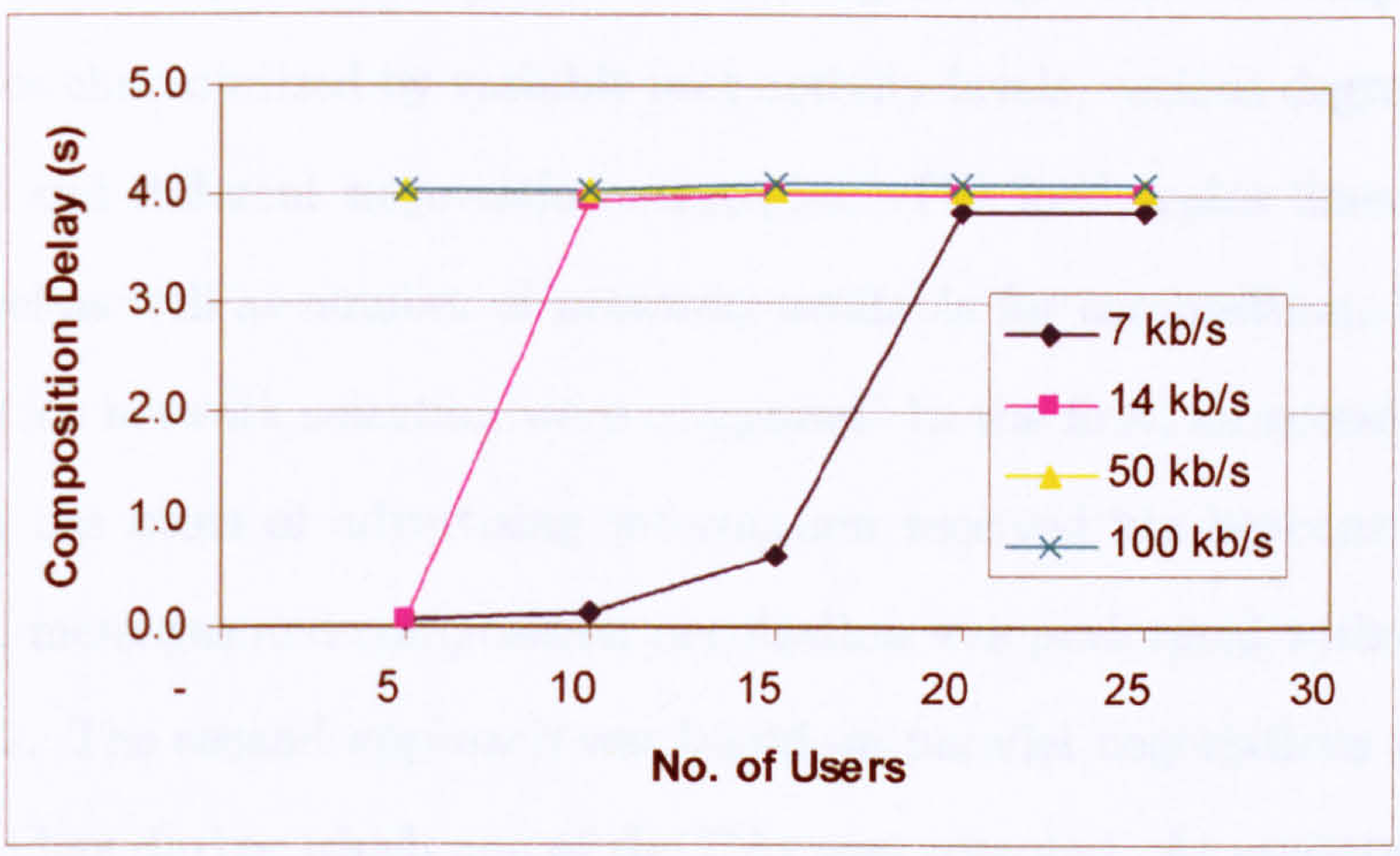


Figure 6.16: Composition latency

6.7 Discussion

The objective of the signalling load and delay analysis was to investigate the cost of composition in common usage scenarios. The benefits of network composition were highlighted in Section 6.4 with the help of some use cases. One of them is the creation of a more flexible and open regime for inter-network cooperation. With respect to an end user, this translates into more choice in selection of access providers, based on specific application and service requirements. From the point of access providers, composition allows tailored service offerings to users and also the possibility of dynamic relationships with them instead of the static subscription-based model prevalent today. These benefits have to be seen in the context of the costs incurred in executing composition processes.

The analysis presented considered a very specific use case involving one or more end users and multiple service providers. The signalling load was computed for various scenarios characterised by variable user activity levels, various degrees of network availability and different negotiation strategies. The load scales linearly with user activity level as well as number of networks available for composition. Two different approaches for network selection were compared. In the first, an access network was selected on the basis of advertising information received via beacons and network attachment messages and composition negotiation was performed with only the chosen network. The second approach was based on parallel negotiations with multiple access providers during which one of the CAs was accepted. As expected, it resulted in higher load compared to the first approach but the potential advantage is that the 'quality' and 'quantity' of information available will be higher resulting in the selection of an access provider that best matches service requirements. This is backed up by the results for different degrees of user's willingness to negotiate which indicate that it is preferable to negotiate 'more' with 'few' networks instead of short negotiations with many networks. Although signalling load appears to be quite low even for scenarios with very high user activity levels and many networks, it is important to put it in the context of application data flowing between the access network and end users. Using a simple traffic model, it was shown that signalling load is very small compared to user data exchanged even though the calculation assumed only one application session. Users take part in many application sessions while connected to the access network which implies that the relative signalling will be even lower.

Signalling load is not the only parameter of interest in the scenario being considered. The latency introduced by composition also needs to be considered because it impacts handover performance when the user is mobile and composing/decomposing with different access providers frequently. Therefore, a simulation study was performed to investigate the composition delay under different network load conditions. Results show that delay is very small, of the order of milliseconds when the network is lightly-loaded but goes up rapidly as the number of users increases, reaching a saturation limit when the network becomes overloaded. The results indicate that special measures may be required to expedite composition signalling in order to keep the delay small. This can take the form of having dedicated channel(s) for such signalling or perhaps, these messages could be assigned higher priority.

In summary, the findings of signalling analysis indicate that additional load from composition is relatively small and can be reduced further by using sophisticated negotiation strategies. Composition latency has strong dependence on network load and more consideration needs to be given to reducing the delay, especially when user mobility is high.

Chapter 7

Conclusions and Future Work

7.1 Summary

This thesis is devoted to the study of different yet related aspects of heterogeneous wireless networking. There are three main focus areas of the research presented in the previous chapters: routing for mobile ad hoc networks, capacity analysis for backbone wireless mesh networks and composition-based dynamic interworking between wireless networks. In the following, a summary of the main contributions and findings of the research are presented, followed by a discussion on its implication and the outlook for future work.

7.1.1 Routing in Mobile Ad hoc Networks

The first half of this work looks at routing in ad hoc networks. The RDMAR protocol, originally proposed by Aggelou and Tafazolli [3] [28], forms the basis of this investigation. The guiding principle in RDMAR design was minimisation of signalling overhead. A query localisation mechanism based on relative distance estimation was the key feature of native RDMAR. The RDE algorithm is instrumental in lowering control overhead arising out of route discovery procedures. In this work, a set of extensions have been proposed for RDMAR to improve its overall performance.

The first extension proposed here for RDMAR was position-assisted routing. In particular, the distance estimation algorithm was altered to work with both physical and relative distances. The query localisation mechanism now uses physical distance estimation to predict the hop-wise distance between source-destination node pairs whenever node location data is available and falls back on relative distance estimation otherwise. Furthermore, directed route discovery was introduced to prevent control messages from being forwarded to nodes that are not in the path between a given source-destination pair. The effectiveness of query localisation shows improvement as a result of this modification. This is reflected in 15 to 20 per cent reduction in control overhead for various node speeds ranging from 0 to 10 m/s. The impact of these changes on route acquisition delay is insignificant because the delay in discovering a route between a pair of nodes is mainly a function of the actual distance between them.

The second add-on to RDMAR is multipath routing. In the original protocol, the route with shortest hop count was used for forwarding application data. Modifications have been proposed to the route discovery process such that multiple parallel routes can be established between source-destination node pairs. Furthermore, routing data structures were also modified to store multiple routes. Given the sensitivity of certain types of traffic to packet inter-arrival times, a data forwarding algorithm that takes into account traffic type was proposed to make the most out of the multipath routing extension. TCP traffic was routed over the shortest path only and remaining paths,whenever available, provided redundancy in the face of path failures. All

UDP traffic was routed over multiple paths. However, in order to avoid using paths of varying lengths, only those with the same hop count were used at a given time. This is aimed at reducing jitter for packets traversing different paths. Simulation results presented here show that the packet delivery ratio is significantly improved when multipath routing is used. Furthermore, control overhead is also reduced, especially in scenarios with high mobility and high network load. This is mainly because the availability of many routes helps the network cope better with route disruptions caused by node mobility and link breaks due to collisions induced by high network load.

7.1.2 Capacity of Wireless Mesh Networks

An analytical framework was developed to estimate the capacity of infrastructure or backbone wireless mesh networks. Such networks are characterised by the presence of static wireless routers and access points. Client terminals are assumed to access the global Internet via the access points and traffic is routed to and from them using multihop wireless paths traversing one or more wireless routers. The capacity analysis is based on identification of collision domains which yields upper bounds on traffic throughput. A number of WMN scenarios were synthesised using different routing and channel assignment schemes and the maximum available capacity estimated for each scenario. Grid-based multi-radio, multi-channel WMNs were considered for this analysis. Results included here indicate that when the gateway node (which connects the WMN to the core network) is far from the access points (which act as traffic aggregators), capacity is rather low. This is because routes between APs and the gateway traverse a number of network hops, thereby causing interference over a relatively larger part of the mesh network. Results also show that use of multiple radio channels improves radio capacity but the gains are limited by the number of radios per node. Furthermore, a simple greedy channel assignment scheme provides capacity gain which indicates that further capacity improvements are possible with more sophisticated schemes for assigning channels.

7.1.3 Dynamic Interworking using Network Composition

The last part of this thesis deals with the concept of network composition, developed in the IST Ambient Networks project. Composition provides a framework for flexible and dynamic interworking between heterogeneous wireless networks. This is achieved using a combination of advertisements about services and resources and negotiation regarding terms of their usage over a period of time. In order to put the benefits of composition in the proper context, the associated overheads in terms of signalling load and latency were analysed for one specific composition use case involving an end user negotiating for network access with multiple service providers. Results show that the signaling load scales linearly with user activity level and number of negotiating partners. In order to avail the full benefits of composition, a user should be willing to negotiate with multiple providers to get the best 'deal'. However, the analysis indicates that, with respect to signalling load, it is preferable to negotiate "more" with "few" partners, instead of the other way round. A simulation-based study of delay shows that for a WLAN environment, composition delay is very small when the network is lightly loaded but it rises sharply as the load increases.

7.2 Implications of the Research

The research presented in this thesis has some interesting implications:

- Position-assisted routing results in improved performance in terms of signalling overhead but it is dependent on the availability of reliable and accurate information about node position. With recent advancements in node positioning technology and reduction in the cost of GPS receivers, using position information for routing is increasingly becoming a feasible option, from both technical and economical perspectives. Therefore, it makes sense to incorporate such mechanisms into routing protocols currently being standardized in the MANET working group in the IETF.

- Using multiple routes for packet forwarding results in higher throughput and lower signalling overhead. Although, multipath routing did not receive much attention in wireline networking, the broadcast nature of wireless channels make them ideally suited for exploiting multiple routes for increased scalability, flexibility and resilience.

- Wireless mesh networks are being touted as the next big thing in the area of wireless networking but careful attention needs to be paid to the different, often contradictory, factors that influence the performance of these networks. In particular, capacity gains are possible by deploying multi-radio systems in order to make the best use of available radio channels. Furthermore, integrating routing and channel assignment algorithms can help spread the load more evenly in the network, thereby improving the overall performance in terms of spectral efficiency, throughput and delay.

- Network composition provides a flexible and dynamic framework for interworking between heterogeneous networks. The scalability of the composition process is crucial in ensuring that its benefits do not come at a high price. The analysis of overheads introduced by the composition process shows that although the signalling load is relatively small, more attention needs to be paid to the delay introduced by composition. A more rigorous feasibility analysis for a wider variety of usage scenarios is required to understand the full implications of compositions.

7.3 Future Work

The work presented here tries to answer some questions but opens other avenues for research, as mentioned below:

- The position-assisted routing scheme assumed availability of node position information without actually modeling any specific positioning algorithm. A number of such mechanisms have been proposed in literature and it is worth including them in the simulation model in order to investigate how realistic node positioning models will impact the protocol performance.

- The multipath routing extension to RDMAR used a coarse approach for selecting routing strategy for data forwarding by dividing traffic into two categories depending on the transport protocol used. However, not all the applications that use UDP have the same forwarding requirements. Therefore, more fine-grained approaches need to be investigated to make better use of multipath routing for different types of applications.

- The multipath routing extension collects all discovered routes and discriminates between them only on the basis of hop count. More sophisticated approaches based on other metrics for route quality should be explored. In literature, many proposals have considered route disjointness as a criterion for comparing and shortlisting routes. Other criteria such as route stability, available QoS etc. should also be taken into account.

- The analysis of network composition has focussed on one specific scenario and the results, to some extent, have to be seen in that particular context. The analysis assumed a more or less pre-defined Composition Agreement. Therefore, additional composition use cases should be investigated to get a better idea of how the process scales in different scenarios. Furthermore, more sophisticated advertising and negotiation strategies need to be studied.

Bibliography

[1] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," January 1999, rFC 2501.

[2] "Mobile Ad-hoc Networks (MANET)," IETF Working Group, http://www.ietf.org/html.charters/manet-charter.html.

[3] G. Aggelou and R. Tafazolli, "RDMAR: A Bandwidth-Efficient Routing Protocol for Mobile Ad hoc Networks," in *Proceedings of ACM Internation Workshop on Wireless Mobile Multimedia (WoWMoM)*, August 1999, pp. 26–33.

[4] I. F. Akyilidz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," in *Elsevier Computer Networks Journal*, vol. 47, March 2005, pp. 445–487.

[5] N. Niebert, A. Schieder, H. Abramowicz, C. Prehofer, and H. Karl, "Ambient Networks: An Architecture for Communication Networks Beyond 3G," in *IEEE Wireless Communications Magazine*, April 2004, vol. 11 no. 2, pp. 14–22.

[6] "Network Composition Feasibility Study (Release 8)," March 2007, 3GPP TR 22.980 (version 8.0.0).

[7] N. Abramson, "The ALOHA System - Another Alternative for Computer Communications," in *Proceedings of the 1970 Fall Joint Computer Conference*, vol. 37, 1970, pp. 281–285.

[8] R. E. Kahn, "The Organization of Computer Resources into a Packet Radio Network," in *IEEE Trans. on Communications*, vol. COM-25 no. 1, January 1977, pp. 169–178.

[9] G. S. Lauer, "Packet-radio Routing," in *Routing in Communications Networks*, M. E. SteenStrup, Ed. Prentice-Hall, 1995, ch. 11, pp. 55–76.

[10] C. E. Perkins, Ed., *Ad Hoc Networking.* Addison-Wesley Professional, December 2000.

[11] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovi, *Ad Hoc Mobile Wireless Networks: Protocols and Systems.* Prentice Hall, December 2001.

[12] C. Hedrick, "Routing Information Protocol," June 1998, RFC 1058.

[13] J. Moy, "OSPF Version 2," April 1998, RFC 2328.

[14] Y. Rekhter and Y. Li, "A Border Gateway Protocol 4 (BGP-4)," March 1995, RFC 1771.

[15] D. Oran, "OSI IS-IS Intra-domain Routing Protocol," February 1990, RFC 1142.

[16] C. L. H. Rutgers, *An Introduction to IGRP*, August, http://www.cisco.com/warp/public/103/5.html.

[17] R. Ogier, F. Templin, and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," February 2004, RFC 3684.

[18] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in *Proceedings of ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications 1994*, September 1994, pp. 234–244.

[19] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," in *Mobile Networks and Applications*, vol. 1 no. 2, November 1996, pp. 183–197.

[20] G. Pei, M. Gerla, and T.-W. Chen, "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks," in *Proceedings of IEEE International Conference on Communications (ICC 2000)*, vol. 1, June 2000, pp. 70–74.

[21] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," July 2003, RFC 3561.

[22] D. Johnson and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," February 2007, RFC 4728.

[23] V. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," in *Proceedings of IEEE INFOCOM '97*, April 1997, pp. 1405–1413.

[24] Z. J. Haas, "A New Routing Protocol for the Reconfigurable Wireless Networks," in *Proceedings of the 6th IEEE International Conference on Universal Personal Communications (ICUPC '97)*, vol. 2, October 1997, pp. 562–566.

[25] Y.-B. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in Mobile Ad hoc Networks," in *Wireless Networks*, vol. 6 no. 4, 2000, pp. 307–321.

[26] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," October 2003, RFC 3626.

[27] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing," March 2007, draft-ietf-manet-dymo-08.

[28] G. Aggelou and R. Tafazolli, "Determining the Optimal Configuration for the Relative Distance Microdiscovery Ad hoc Routing Protocol," in *IEEE Transaction on Vehicular Technology*, vol. 51 no. 2, March 2002, pp. 354–370.

[29] P. Enge and P. Misra, "Special Issue on GPS: The Global Positioning System," in *Proceedings of IEEE*, vol. 87 no. 1, January 1999, pp. 3–172.

[30] T. Rappaport, J. Reed, and B. D. Woerner, "Position Location Using Wireless Communications on Highways of the Future," in *IEEE Communications Magazine*, October 1996, pp. 31–41.

[31] J.-H. Yap, X. Yang, S. Ghaheri-Niri, and R. Tafazolli, "Position Assisted Relaying and Handover in Hybrid Ad hoc WCDMA Cellular System," in *Proceedings of 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2002)*, September 2002, pp. 2194–2198.

[32] Z. Xiang, S. Song, J. Chen, H. Wang, J. Huang, and X. Gao, "A Wireless LAN-based Indoor Positioning Technology," in *IBM Journal of Research and Development*, September-November 2004, pp. 617–626.

[33] I. Cubic, D. Begusic, and T. Mandic, "Client Based Wireless LAN Indoor Positioning," in *Proceedings of 8th International Conference on Telecommunications (ConTEL 2005)*, June 2005, pp. 335–339.

[34] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS)," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM 2001)*, vol. 5, November 2001, pp. 2926–2931.

[35] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A Library for Parallel Simulation of Large-scale Wireless Networks," in *Proceedings of the 12th Workshop on Parallel and Distributed Simulations - PADS '98*, May 1998, pp. 154–161.

[36] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," in *Mobile Computing and Networking*, October 1998, pp. 85–97.

[37] S. R. Das, C. E. Perkins, and E. E. Royer, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks," in *Proceedings of IEEE INFOCOM 2000*, vol. 1, March 2000, pp. 3–12.

[38] J. Cain, S. Adams, M. Noakes, and E. Althouse, "A Near-Optimum Multiple Path Routing Algorithm for Space-Based SDI Networks," in *Proceedings of IEEE MILCOM '87*, October 1987, pp. 29.3.1–29.3.7.

[39] W. Zaumen and J. Garcia-Luna-Aceves, "Loop-free Multipath Routing Using Generalized Diffusing Computations," in *Proceedings of IEEE INFOCOM 98*, March 1998, pp. 1408–1417.

[40] S. Lee and M. Gerla, "AODV-BR: Backup Routing in Ad hoc Networks," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC 2000)*, vol. 3, September 2000, pp. 1311–1316.

[41] A. Nasipuri and S. Das, "On-Demand Multipath Routing for Mobile Ad Hoc Networks," in *Proceedings of IEEE International Conference on Computer Communication and Networks (ICCCN'99)*, October 1999, pp. 64–70.

[42] H. W. Gunyoung Koh, Duyoung Oh, "A Graph-Based Approach to Compute Multiple Paths in Mobile Ad Hoc Networks," in *Lecture Notes in Computer Science: Web and Communication Technologies and Internet-Related Social Issues HSI 2003*, August 2003, vol. 2713/2003, pp. 323–3311.

[43] S. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad hoc Networks," in *Proceedings of IEEE International Conference on Communications (ICC 2001)*, vol. 10, June 2001, pp. 3201–3205.

[44] M. Pearlman, Z. Haas, P. Scholander, and S. Tabrizi, "On the Impact of Alternate Path Routing for Load Balancing in Mobile Ad Hoc Networks," in *Proceedings of ACM International Symposium on Mobile Ad hoc Networking & Computing (MobiHOC 2000)*, August 2000, pp. 3–10.

[45] H. Lim, K. Xu, and M. Gerla, "TCP Performance over Multipath Routing in Mobile Ad Hoc Networks," in *Proceedings of IEEE International Conference on Communications (ICC'03)*, vol. 2, May 2003, pp. 1064–1068.

[46] L. Wang, L. Zhang, Y. Shu, and M. Dong, "Multipath Source Routing in Wireless Ad hoc Networks," in *Proceedings of Canadian Conference on Electrical and Computer Engineering*, vol. 1, October 2000.

[47] TROPOS networks Inc., "Metro-Scale Mesh Networking with Tropos MetroMesh Architecture," www.tropos.com/pdf/tropos_metro-scale.pdf, February 2005.

[48] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," in *IEEE Trans. Information Theory*, March 2000, vol. 46 no. 2, pp. 388–404.

[49] J. Li, C. Blake, D. S. J. D. Couto, H. I. Lee, and R. Morris, "Capacity of Ad Hoc Wireless Networks," in *Proceeding of 7th ACM International Conference on Mobile Computing and Networking*, July 2001, pp. 61–69.

[50] M. Grossglauser and D. Tse, "Mobility Increases the Capacity of Ad Hoc Wireless Networks," in *IEEE/ACM Trans. Networking*, August 2002, vol. 10 no. 4, pp. 477–486.

[51] M. Gastpar and M. Vetterli, "On the Capacity of Wireless Networks: The Relay Case," in *Proceeding of IEEE INFOCOM 2002*, vol. 3, June 2002, pp. 1577–1586.

[52] F. Cali, M. Conti, and E. Gregori, "IEEE 802.11 Wireless LAN: Capacity Analysis and Protocol Enhancement," in *Proceedings of IEEE INFOCOM 1998*, vol. 1, March 1998, pp. 142–149.

[53] J. Jangeun and M. L. Sichitiu, "The Nominal Capacity of Wireless Mesh Networks," in *IEEE Wireless Communications Magazine*, October 2003, vol. 10 no. 5, pp. 8–14.

[54] A. Raniwala, K. Gopalan, and T. cker Chiueh, "Centralized Channel Assignment and Routing Algorithms for Multi-channel Wireless Mesh Networks," in *ACM SIGMOBILE Mobile Computing and Communication Review*, April 2004, vol. 8 no. 2, pp. 50–65.

[55] A. Raniwala and T. cker Chiueh, "Architecture and Algorithms for an IEEE 802.11-based Multi-channel Wireless Mesh Network," in *Proceedings of INFOCOM 2005*, March 2005, vol. 3, pp. 2223–2234.

[56] R. Draves, J. Padhye, and B. Zill, "Routing in Multi-radio, Multi-hop Wireless Mesh Networks," in *Proceedings of ACM MobiCom 2004*, September 2004, pp. 114–128.

[57] J. Jun, P. Peddabachagari, and M. L. Sichitiu, "Theoretical Maximum Throughput of IEEE 802.11 and Its Applications," in *Proceedings of 2nd IEEE International Symposium on Network Computing and Applications*, April 2003, pp. 259–256.

[58] "3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)," September 2005, 3GPP TS 23.234 (version 6.6.0).

[59] M. J. (Ed.), "Ambient Network System Description," April 2007, ambient Networks Public Deliverable D07-A2.

[60] T. Rinta-aho, R. Campos, A. Mehes, U. Meyer, J. Sachs, and G. Selander, "Ambient Network Attachment," in *Proceedings of the 16th IST Mobile and Wireless Communications Summit*, July 2007.

[61] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," February 2007, internet Draft draft-ietf-hip-base-07, Informational.

[62] N. Akhtar, R. Campos, C. Kappler, P. Poyhonen, P. Paakkonen, and D. Zhou, "GANS: A Signalling Framework for Dynamic Interworking Between Heterogeneous Networks," in *Proceedings of IEEE Vehicular Technology Conference 2006 (VTC-2006 Fall)*, September 2006.

Appendix A

C-GSLP Message and Object Formats

The message and object formats of the protocol for composition negotiation, realization and deletion are presented below.

Common Header

All C-GSLP messages must contain the 32-bit header illustrated below:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Message Type |   Msg Subtype  |              Flags            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Message Type

The size of this field is 8 bits. The following message types are defined:

1 = CANEG

2 = CARLZ

3 = CADEL

Message Subtype

The size of this field is 8 bits.

CANEG: The subtypes for this message are as follows.

1 = CANEG_Negotiate

2 = CANEG_NegotiateAck

3 = CANEG_Validate

4 = CANEG_ValidateAck

5 = CANEG_Cancel

CARLZ: The subtypes for this message are as follows.

1 = CARLZ_Prepare

2 = CARLZ_Ready

3 = CARLZ_Commit

4 = CARLZ_Cancel

CADEL: The subtypes for this message are as follows.

1 = CADEL_Delete

2 = CADEL_DeleteAck

Flags

The size of this field is 16 bits. The flags are message specific and they will be processed differently for each type of message. Any bit that is not defined for a specific message must be set to zero and must be ignored upon reception.

Object Formats

C-GSLP objects follow the Type-Length-Value (TLV) format. Each object consists of a 32-bit common header and a variable-length data field. The common header indicates the type and length as shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|r|r|r|r|       Type            |r|r|r|r|       Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//                             Value                           //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Length is expressed in terms of 32-bit words and indicates the length of 'Value'. If there is no Value, Length=0. Value is a whole number of 32 bit words. If there is any padding required, the length and location must be defined by the object-specific format information; objects which contain variable length (e.g. string) types may need to include additional length subfields to do so. The bits labeled 'r' are reserved. C-GSLP currently defines the following object types: Composition Agreement Identifier, Composition Agreement Data, and Error Data.

Composition Agreement Identifier (CAI)

Type: 1 = Composition-Agreement-Identifier

Length: Fixed (128 bits)

Value: CA identifier is a cryptographically random identifier chosen by the C-FE that initiates CA Negotiation.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+              Composition Agreement Identifier                 +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Composition Agreement Data (CAD)

Type: 2 = Composition-Agreement-Data

Length: Variable

Value: Contents of the CA

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//                  Composition Agreement Data                 //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Composition Agreement Lifetime (CAL)

Type: 3 = Composition-Agreement-Lifetime

Length: Variable

Value: Lifetime of the CA

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//                Composition Agreement Lifetime              //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Error Data (ED)

Type: 4 = Error-Data

Length: 4 bytes

Value: Consists of a single byte Error_Class and 3 byte Error_Code

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Error_Class  |                  Error_Code                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Message Formats

CANEG =

Common-Header

Composition-Agreement-Identifier

[Composition-Agreement-Data]

[Composition-Agreement-Lifetime]

[Error-Data]

All CANEG messages must include the CAI object in addition to the common header. The CAD object is included in CANEG_Negotiate messages during composition negotiation. The CAL object is carried in CANEG_Negotiate message during the composition refresh procedure when the CA is about to expire. All CANEG_Cancel messages must contain the ED object.

CARLZ =

Common-Header

Composition-Agreement-Identifier

[Error-Data]

CADEL =

Common-Header

Composition-Agreement-Identifier

Appendix B

Composition Process Signalling Message Sizes

Details of the values for signalling bits exchanged in different phases of the composition procedure used in the analysis presented in Chapter 6 are provided below.

List of Information Elements

Network Attachment

1. **Ambient Network ID** (AN-ID)
   Unique identifier of an AN.
   Size - 128 bits

2. **Session Identifier**
   To uniquely identify different associations between ANs.
   Size 16 bits

3. **Routing Information**
   Node ID (NID) - 128 bits
   Locator Domain ID (LD-ID) - 128 bits (IPv6)
   NID router LD-ID 128 bits

4. **Flow Parameters**

   A flow is defined by its end nodes, so two Node IDs are needed

   Node ID (NID) - 128 bits

5. **Security Parameters**

   Signature and encryption algorithms for protection of user traffic once the attachment is done.

   Size is variable, here 64 bits are assumed.

6. **Encryption and Authentication Data**

   Diffie-Hellman value - 1536 bits

   Public Key - 1024 bits

   Puzzle challenge - 512 bits

   Puzzle response - 512 bits

   Signature - 512 bits

CA Template

The template used for composition negotiation between end user and access provider is shown below. The service in this case is "WLAN Access". The user AN has the customer role while the access AN has the provider role. The type of service is connectivity and deployment mode is 'usage'. Rest of the fields are self-explanatory.

The data sizes for the different fields are provided below.

1. CA Identifier: 256 bits

2. CA Lifetime: 32 bits

3. AN Identifiers: 256 bits (128 bits each)

4. Service name: 8 bits

CA Identifier
CA Lifetime
AN Identifiers
Service Name
Service Identifier
Roles
Service Type
Service Specification
Service Deployment Mode
Compensating Party
Compensated Party
Payment Method
Accounting Data Unit
Pricing Information

Table B.1: Composition Agreement Fields

5. Service id: 8 bits
6. Service type: 8 bits
7. Service deployment mode: 8 bits
8. Roles: 256 bits
9. Service specifications: 32 bits
10. Compensating party: 128 bits
11. Compensated party: 128 bits
12. Payment method: 8 bits
13. Accounting unit: 8 bits
14. Pricing information: 16 bits

GANS Signalling

Prior to the start of composition, a 3-way handshake takes place between the GTLP instances in the two ANs. In addition, each Composition-GSLP message used during the negotiation is encapsulated in a GTLP Data packet. The GTLP message sizes are:

1. GTLP Query: 665 bits
2. GTLP Response: 667 bits
3. GTLP Confirm: 615 bits
4. GTLP Data: 591 bits for the header + variable size payload

Note that the GTLP packet will be encapsulated in a TCP/UDP packet which in turn will from the payload of an IP datagram. The numbers mentioned here only refer to GTLP messages. The size of GTLP Data packet payload will depend on the particular GSLP message being transported using GTLP.

The sizes of C-GSLP messages used in the composition procedures include in the simulation and analysis models are:

1. **CANEG_Negotiate**
   Common Header: 32 bits
   CA Identifier: 32+128 (Object header + identifier)
   CA Data: 32 + X bits (Object header + Size of CA)
   Total size = (224 + X) bits

2. **CANEG_NegotiateAck**
   Common Header: 32 bits
   CA Identifier: 32+128 (Object header + identifier)
   Total size = 192 bits

3. **CANEG_Validate**

   Common Header: 32 bits

   CA Identifier: 32+128 (Object header + identifier)

   Total size = 192 bits

4. **CANEG_ValidateAck**

   Common Header: 32 bits

   CA Identifier: 32+128 (Object header + identifier)

   Total size = 192 bits

5. **CARLZ_RealizationPrepare**

   Common Header: 32 bits

   CA Identifier: 32+128 (Object header + identifier)

   Total size = 192 bits

6. **CARLZ_RealizationReady**

   Common Header: 32 bits

   CA Identifier: 32+128 (Object header + identifier)

   Total size = 192 bits

7. **CARLZ_RealizationCommit**

   Common Header: 32 bits

   CA Identifier: 32+128 (Object header + identifier)

   Total size = 192 bits

Appendix C

List of Publications

1. N. Akhtar, K. Moessner, "*On the Nominal Capacity of Wireless Mesh Networks*", submitted to Special Issue of Elsevier Computer Communications on Wireless Mesh Networks.

2. T. Rinta-aho, N. Akhtar, O. Queseth, J. Sachs, "*Ambient Network Advertisements*", in Proceedings of the 7th International Symposium on Communications and Information Technologies, October 2007.

3. N. Akhtar, J. Markendahl, K. Moessner, "*Analysis of Complexity and Transaction Costs for Co-operating Networks*", in Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, September 2007.

4. N. Akhtar , C. Kappler , P. Schefczik , L. Tionardi , D. Zhou, "*Network Composition: A Framework for Dynamic Interworking between Networks*", in Proceedings of the ChinaCom 2007 Conference, August 2007.

5. A. Bria, J. Markendahl , R. Rembarz , P. Poyhonen , C. Simon , M. Miozzo , N. Akhtar , R. Jennen, "*Validation of the Ambient Networks System Architecture*", in Proceedings of the ChinaCom 2007 Conference, August 2007.

6. J. Markendahl, N. Akhtar, P. Poyovnen, O. Strandberg, "*Analysis of Ambient*

Networks Mechanisms for Support of I-centric Communications", in Proceedings of the 18th WWRF meeting, June 2007.

7. N. Akhtar, J. Markendahl, O. Queseth , "*Analysis of Signaling Load and Negotiation Complexity using Network Composition in Multi-Provider Business Environments*", in Proceedings of the 6th Conference on Telecommunication Techno-Economics, June 2007.

8. N. Akhtar, J. Markendahl, O. Queseth, "*Impact of Dynamic Business Relations and Greedy User Behavior on Business Related Signaling Load in Multi-provider Networks with Ambient Network Technology*", in Proceedings of the Global Mobility Roundtable, May 2007.

9. C. Kappler, N. Akhtar, P. Mendes, "*GANS: Generic Ambient Network Signalling*", in Ambient Networks: Co-operative Mobile Networking for the Wireless World, N. Niebert et al, Ed., J. Wiley & Sons, April 2007.

10. R. Campos, N. Akhtar, C. Kappler, P. Poyhonen, P. Paakkonen, D. Zhou, "*On the Evaluation of the Extended Generic Internet Signalling Transport Protocol*", in Proceedings of the 15 IST Mobile and Wireless Communications Summit, June 2006.

11. N. Akhtar, R. Campos, C. Kappler, P. Poyhonen, P. Paakkonen, D. Zhou, "*GANS: A Signalling Framework for Dynamic Interworking between Heterogeneous Networks*", in Proceedings of the 64th IEEE Vehicular Technology Conference 2006 Fall, September 2006.

12. D. Zhou, P. Poyhonen, N. Akhtar, C. Pinho, "*Ambient Network Interfaces and Network Composition*", in Proceedings of the CIC/IEEE Global Mobile Congress '05, October 2005.

13. C. Kappler, N. Akhtar, R. Campos and P. Poyhonen, "*Network Composition using Existing and New Technologies*", in Proceedings of the 14th IST Mobile Summit, June 2005.

14. L. Fan, N. Akhtar, K. Chew, K. Moessner, R. Tafazolli, "*Network Composition: A Step Towards Pervasive Computing*", in Proceedings of the 3G 2004 Conference, October 2004.

15. R. Campos, N. Akhtar et al,"*Scenarios for Network Composition in Ambient Networks: A New Paradigm for Internetworking*", in Proceedings of the 11th WWRF Meeting, June 2004.

16. N. Akhtar, R. Tafazolli, "*Traffic-based Multipath Routing for Mobile Ad hoc Networks*", in Proceedings of the IEEE International Workshop on Wireless Ad-hoc Networks 2004, May 2004.

17. N. Akhtar, R. Tafazolli, "*Relative Distance Micro-discovery Ad hoc Routing*", in Proceedings of the 7th WWRF Meeting, December 2002.