Scalable and extensible architecture for IEEE 802.11s wireless mesh networks.

Isabwe, Ghislain Maurice Norbert

Scalable and Extensible Architecture for IEEE 802.11s Wireless Mesh Networks

Ghislain Maurice Norbert ISABWE, BEng, MSc.

Submitted to Swansea University in fulfilment
Of the requirements for the degree of
Master of Philosophy

Swansea University
Prifysgol Abertawe

School of Engineering

SWANSEA UNIVERSITY

May 2011

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

Abstract

This thesis presents the results of an investigation into the issue of interworking with Ethernet local area networks (LANs) through multiple portals in a wireless LAN (WLAN) mesh, which has been being standardized by IEEE 802.11s.

A detailed description of WLAN mesh networks which run layer-2 path selection and forwarding protocols is given along with their challenges in scalability and extensibility.

Interworking with multiple mesh portals is necessary not only for network scalability but also reliability. However, if a WLAN mesh is connected to one external Ethernet segment through multiple mesh portals, broadcast loops may occur and the IEEE 802.1D bridging protocol may cause the Ethernet ports of mesh portals to be blocked, which results in interworking with the LAN through only one mesh portal. To address this issue, we propose a new interworking framework enabling multiple portals by deactivation of port blocking function of IEEE 802.1D bridge at Ethernet ports of mesh portals; thus allowing bridge protocol data units to be transparently forwarded inside the mesh network.

In order to avoid broadcast loops, a frame filtering algorithm was designed for mesh portals using newly introduced fields in the portal announcement information element and mesh header so that no frame can be transmitted from a mesh portal to another portal more than once, when both mesh portals are connected to the same LAN segment.

There was also provision of procedures for network topology/LAN segment identification and interportal communications to support the proposed interworking framework.

Performance evaluation by simulation was carried out where a wireless LAN mesh network was emulated based on existing models of mobile ad hoc network with a reactive path selection and forwarding protocol. Simulation results have shown a great improvement in end-to-end delay, packet delivery ratio and WLAN medium access delay in case multiple portals are enabled.

DECLARATION

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed:

Date: 13/05/2011

STATEMENT 1

This thesis is the result of my own investigations, except where otherwise stated.

Where correction services have been used, the extent and nature of the correction is clearly marked in a footnote(s).

Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed:

Date: 13/05/2011

STATEMENT 2

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed:

Date: 13/05/2011

TABLE OF CONTENTS

Acknowledgements

Thanks and Praises be to the Almighty God.

I also wish to express my sincere appreciation and great thanks to:

- my supervisor, Dr Kyeong Soo (Joseph) Kim, for his invaluable guidance, consistent encouragement and assistance
- Mrs Choudhuri Anjana who helped me in every way to make this research work possible
- my co-supervisor, Dr Jian Hua He for his guidance
- my dear wife and great friend, Gipenzi, for her love, patience and support while I carried out this work
- my lovely children and parents for their moral support
- my colleagues at the Institute of Advanced Telecommunications (IAT) and the Welsh Video Network (WVN) who helped in many different ways.

This research work was partly funded by the European Regional Development Fund (ERDF) Objective 1 (Grant code: ATR 502 522)

List of tables

List of illustrations

List of abbreviations

AIFSN	Arbitration Inter Frame Spacing
AODV	Ad hoc on demand distance vector routing protocol
AP	Access point
API	Application Programming Interface
BPDU	Bridge protocol data unit
BSS	Basic service set
CSMA/CA	Carrier sense multiple access with collision avoidance
CTS	Clear to send
CWmax	Maximum contention window
CWmin	Minimum contention window
DA	Destination address
DCF	Distributed coordination function
DHCP	Dynamic host configuration
DP	Designated portal
DPANN	Designated portal announcement
DS	Distribution service
EDCA	Enhanced Distributed Channel Access
ESS	Extended service set
FSM	Finite State Machine
FTP	File transfer protocol
HCF	Hybrid coordination function
HTTP	Hyper text transfer protocol
HWMP	Hybrid Wireless Mesh Protocol
IBSS	Independent basic service set
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol

IPC	Interportal communications
LAN	Local area network
MAC	Medium access control
MANET	Mobile ad hoc network
MAP	Mesh access point
MDA	Mesh deterministic access
MP	Mesh point
MPP	Mesh portal
MPR	Multipoint relay
OFDM	Orthogonal frequency division multiplexing
OLSR	Optimized link state routing
OPNET	Optimized Network Engineering
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PANN	Portal announcement
PCF	Point coordination function
PDF	Probability density function
PHY	Physical layer
PREP	Path reply
PREQ	Path request
QoS	Quality of service
RA	Receiver address
RANN	Route announcement
RA-OLSR	Radio Aware OLSR
RERR	Route error
RREP	Route reply
RREP-ACK	Route reply acknowledge

RREQ	Route request
RTP	Real time transport protocol
RTS	Request to send
SA	Source address
STA	Station
STP	Spanning tree protocol
TA	Transmitter address
TG	Task group
TTL	Time to live
TXOP	Transmit opportunity
UDP	User datagram protocol
VoIP	Voice over Internet Protocol
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless local area network
WMN	Wireless mesh network

Chapter I

Introduction

1 Introduction

1.1 On the networks research

Great advances and developments are being realised in network communications technologies over wireless media as well as wired media. However, wireless communications are gaining more and more popularity as they present many advantages in terms of mobility, easier deployment in hard to reach areas, and low cost.

The ***scope*** of this research work is Scalable Path Selection, Forwarding and Interworking protocols for the mesh extension of *Wireless Local Area Network* (WLAN) as defined in IEEE802.11s [10].

It is noted that, while studying WLAN Mesh, considerable work was done on Interworking in heterogeneous wireless mesh networks and coexistence with existing wireless infrastructures and wired infrastructures as well. However, apart from the WLAN Mesh, there will not be any proposals or innovations to make changes to the existing network architectures and protocols, either wired or wireless.

Wireless mesh networks (WMNs) are an emerging technology which can provide affordable and reliable wireless connectivity [16]. WMNs are self-organized and self-configured wireless networks which can automatically establish an ad hoc network and dynamically adapt to network topology changes. There exist different types of WMN based on physical layer, link layer and network layer protocols that are implemented.

WLAN Mesh is one of the latest WMN to be developed, with multihop path selection and forwarding capabilities, self-healing and interworking with external local area networks. Although WLAN Mesh has a lot of promises, it still has many unresolved issues, such as the number of supported network nodes and routing tables' size among others.

The ***aim*** of this research work is to study and propose a novel architecture to address the scalability and extensibility problems in WLAN Mesh networks.

The ***objectives*** of this research work are defined as follows:

1. To carry out a study of existing developments and contributions in the Wireless LAN Mesh Networking field
2. To investigate technological challenges in existing protocols with regards to Interworking and Scalable path selection and forwarding
3. To develop algorithms/protocols for addressing the above mentioned challenges
4. To carry out algorithms/protocols analysis through scenario case studies and experimentation
5. To disseminate research results through conferences, workshops and scientific publications

1.2 Overview of Wireless Mesh Networks

Over the years, wireless networking has registered tremendous technological advances in terms of bandwidth, availability, power consumption, mobility support and security amongst others.

Wireless Mesh Networking is one of the hottest areas of research with many promises on one hand but also with huge challenges on the other. WMNs are basically made of network nodes which can work as hosts but also perform routing functions along with or without "*Mesh clients*" which don't participate in routing.

The first type of nodes, also commonly referred to as "*Mesh routers*", play an important role of path selection and forwarding not only for themselves

but also for those nodes which are not in direct wireless reach of destination nodes, thus effectively enabling wireless multihop routing.

It is noted that Mesh routers will be acting as proxies on behalf of directly connected mesh clients for the purpose of routing, and they – mesh routers – are also capable of creating a fully connected mesh network among themselves as an ad hoc network.

WMNs have attracted a good level of attention due to their capability to self-organize, self-configure and self-heal in case of network connection disruptions. Mesh connectivity can be established either by a proactive or reactive (on-demand) path selection protocols. Furthermore, in [10] a hybrid routing protocol was proposed to take advantages of the flexibility of on-demand route discovery and the efficiency of proactive routing.

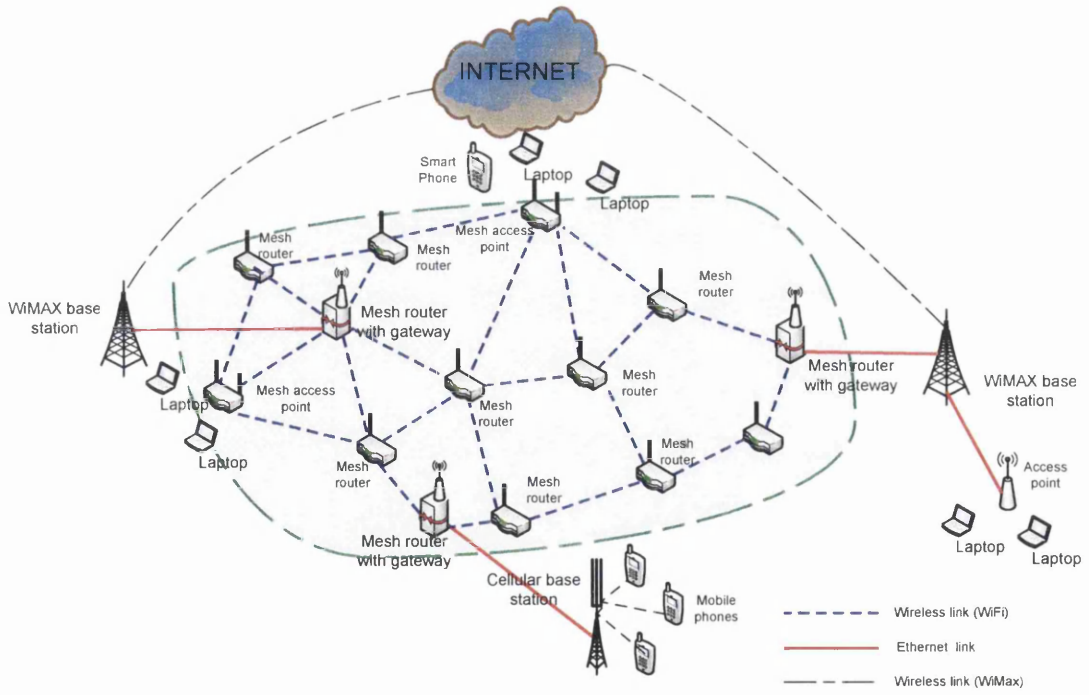

Figure 1: Wireless Mesh Network

Figure 1 shows an example of a WMN comprising of mesh routers, client nodes and other network nodes which are not part of the mesh network.

Later in this text, mesh routers will be referred to as "mesh points" with reference to IEEE802.11s.

WMNs are intended to support most of wireless technologies already deployed on PDAs, personal computers, mobile telephones and other handheld devices in such a way that those devices could directly connect to mesh routers in order to access network services. Furthermore, some mesh routers (mesh portals) have gateway capability to interwork with other network technologies such as Ethernet so that the mesh network can form part of a larger network which doesn't necessarily support mesh networking. A good example, as shown in figure 1, is provision of internet services to mesh clients with WiMAX backbone network. The same figure also illustrates network services provision to a cellular network through multihop relaying of WMNs.

Akyildiz et al. [8] have discussed the main advantages of WMNs including but not limited to self-organization, easy deployment particularly in hard-to-reach areas, minimum initial upfront cost, reduced operational and maintenance costs as well as their viability as access network, for instance broadband Internet access. Furthermore, WMNs can also be integrated with multiple wireless networks and can greatly improve the reliability of ad hoc mobile networks. However, they have also explored quite a number of pending issues which should be addressed for WMNs to meet user expectations. There is a scalability problem which gets more complex as the network size increases and also constraints on the number of possible hops. Each mesh router has a limitation as to how many non-mesh nodes it can support as a proxy for path selection and forwarding purposes, and also the network performance degrades as the number of hops increases due to the existing distributed random access MAC protocols such as carrier sense

multiple access with collision avoidance (CSMA/CA) which was not initially designed for multihop operation.

1.3 WLAN Mesh networks

The IEEE 802.11 Working Group, formed a Task Group (TG) "S" in 2003 to develop a Wireless Mesh Network (WMN) amendment [13].

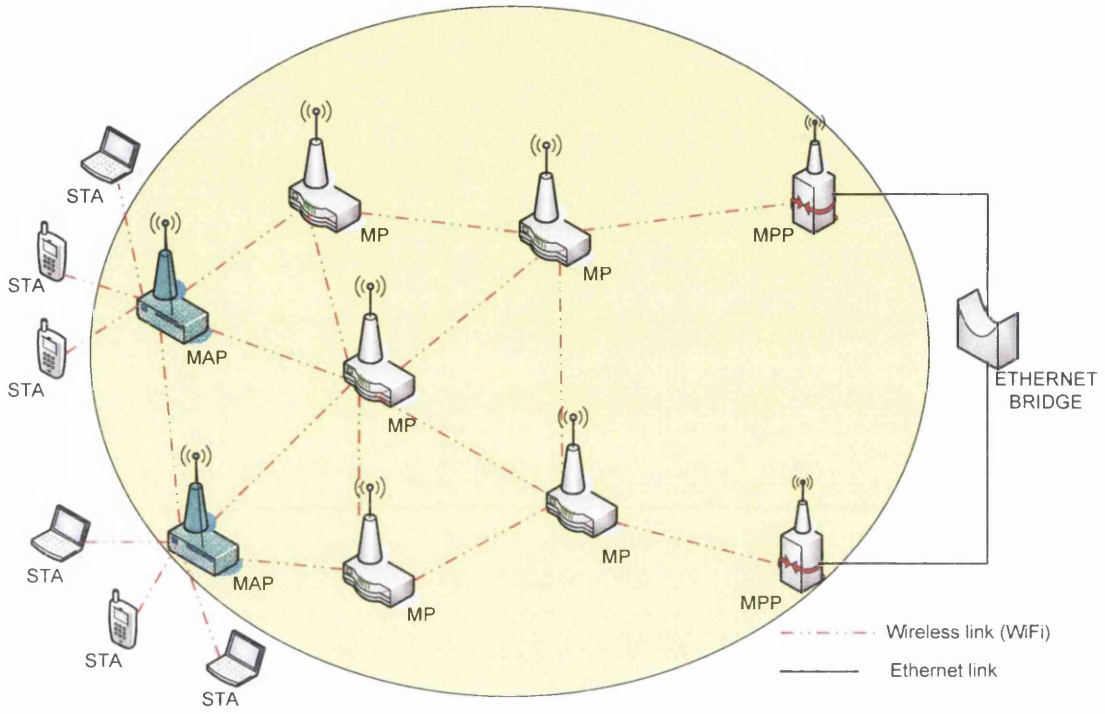

Figure 2: Example WLAN Mesh Network[1]

According to IEEE 802.11s WLAN mesh standard (work in progress), a WLAN mesh generally consists of the following components:

- Mesh point (MP): An IEEE 802.11 quality of service (QoS) station (STA) that supports mesh services[2]. A STA itself is defined as any device that contains an IEEE 802.11-conformant medium access control (MAC) and physical layer (PHY) interface to the wireless

[1] The Ethernet bridge is not part of a WLAN Mesh Network
[2] A QoS STA is a STA that implements the QoS facility.

medium (WM). Although a STA is the base of all mesh nodes, it is not explicitly part of the mesh network.

- Mesh access point (MAP): A mesh point that is collocated with one or more access point(s).
- Mesh portal (MPP): A mesh point that is collocated with one or more portal(s).

An MPP is a gateway point at which a WLAN mesh sends or receives frames to or from non-mesh networks, for instance a wired Ethernet LAN (IEEE 802.3). An MPP must be able to handle different frame formats from both types of network.

In a traditional WLAN, a STA needs to associate with an Access Point (AP) to be connected to the network, and a STA can not directly be connected to another (similar) STA, thus it will always depend on an AP.

Besides the 802.11 WLAN basic service sets (BSSs) which are connected to an Ethernet LAN via AP(s), ad hoc networking has been defined within independent basic service sets (IBSSs) mode where STAs can connect to each other without any central node such as an AP. However, the ad hoc networking was meant for connecting stations among themselves without any connection to a distribution system (DS), thus unable it to support infrastructure mode. Ad hoc networking is being explored within the IETF Mobile Ad Hoc Network (MANET) Working Group [6].

On the other hand, an MP will be able to provide mesh services, in order to participate in interoperable formation and operation of the mesh network. By "mesh services provision" it is meant the provision of wireless link paths between multiple nodes in a multihop fashion. MPs relay frames

between each other. Figure 2 gives an example snapshot of a WLAN Mesh network and Figure 3 shows a traditional, infrastructure-mode WLAN.

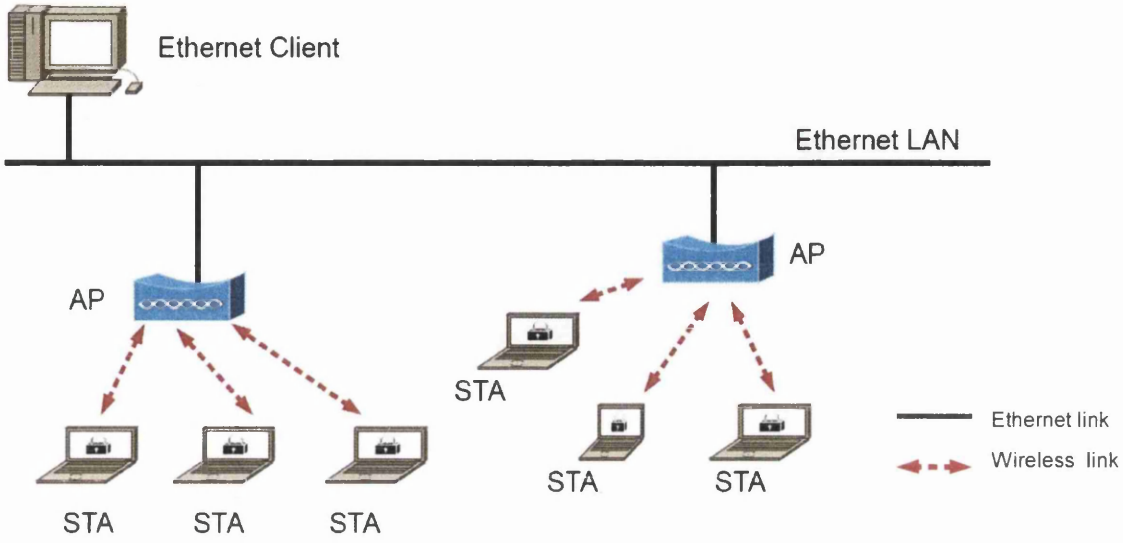

Figure 3: IEEE 802.11 WLAN

WLAN mesh integrates both IBSS mode and infrastructure mode with a possibility of serving as a backbone to different network technologies. WLAN mesh supports an Extended Service Set (ESS) by connecting MAPs wirelessly.

The following figure illustrates a simplified WLAN mesh protocol stack.

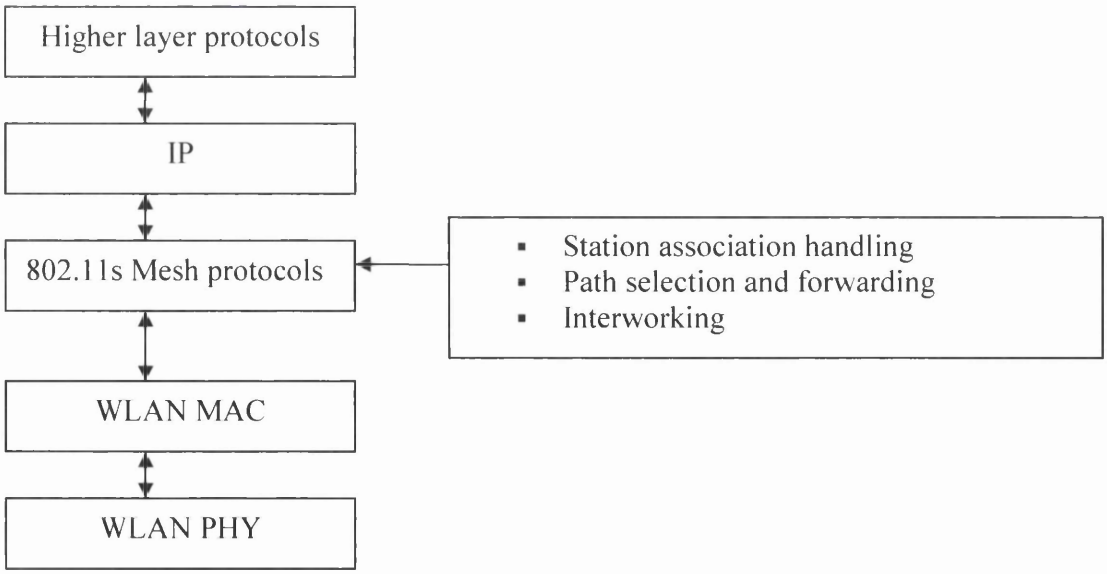

Figure 4: Simplified WLAN Mesh Protocol Stack

Figure 5 represents high level architecture of an MPP from a protocol point of view.

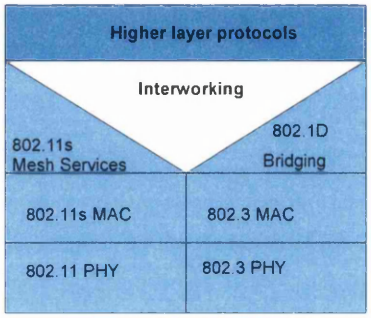

Figure 5: MPP Protocol layers

Besides the MPP, other mesh nodes can be designed in the same way but with only IEEE 802.11 protocol stack with additional mesh services (for an MP) and access point functionality (for an MAP). Figure 6 illustrates the three types of mesh nodes:

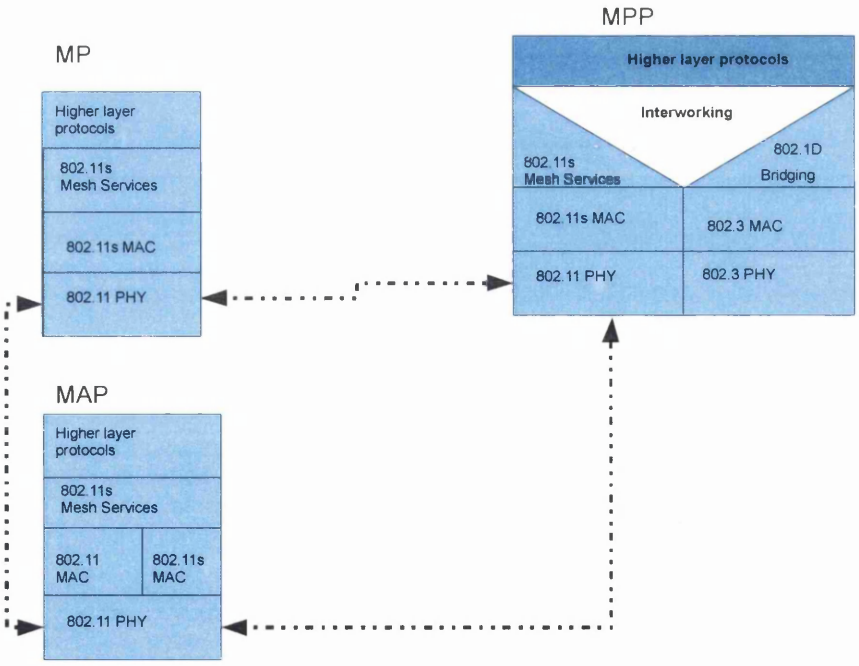

Figure 6: WLAN Mesh Protocol Stack

802.11s MAC (Medium Access Control) is a modification of 802.11 MAC in terms of beaconing and synchronization, multichannel operation, mesh

deterministic access (MDA), intra-mesh congestion control and power management[5].

1.4 Challenges in WLAN Mesh networks

WLAN Mesh networks have inherited PHY and MAC challenges from the IEEE802.11 base standard [12] plus additional requirements to support mesh services.

Major challenges in IEEE802.11s are summarised below [28]:

- Topology formation for multi-rate operation and physical rate control
- Link quality measurement and routing metrics
- Routing protocol: both the default protocol (HWMP) and optional protocol (RA-OLSR) are not yet fully optimized to meet cross-layer design requirements in order to work with other MAC functionalities. Their scalability remains an issue and multihop forwarding using MAC addresses requires additional addressing besides the end destination and source pair. Furthermore, interworking with Ethernet segment with spanning tree protocol (bridging) can lead to broadcast storms in certain network configurations.
- Congestion control: It is not possible to control intra-mesh congestion if there is no effective way to perform congestion monitoring. 802.11s doesn't provide a scheme for traffic load information sharing "among one-hop and multihop neighbours". When congestion happens, there is need for the traffic rate to be adjusted according to the measured congestion. Without an appropriate measure, the time window may be arbitrarily defined, and thus affect network performance.
- Multi-channel operation
- Mesh deterministic access (MDA): This mechanism is expected to reduce contention in mesh networks. However, the network should be

able to support other nodes which don't support MDA. MDA nodes are not able to prevent non-MDA nodes from accessing the medium during MDA opportunity (MDAOP) period.

- QoS: End-to-end QoS is not catered for in 802.11s as the available mechanism is based on traffic classes and it doesn't work in case different nodes have the same traffic class. There should be a reservation scheme.
- Security: Even though the mesh security association (MSA) services are defined in 802.11s, multihop mesh architecture requires appropriate mechanisms to ensure secure paths among MP.
- Mobility and fast handoff: MAP and MPs can be mobile in certain scenarios, thus handoff delay must be very small to allow real time services on non-mesh nodes supported through MAP.
- Multiple MPPs: Current standard provides only for one MPP per LAN segment, but multiple portals are needed for scalability, extensibility and improved reliability

1.5 Research Methodology outline

This research work follows an approach to study a particular type of network, for instance WLAN Mesh networks.

A *background study* on WLAN was carried out. Then, having identified scalability and extensibility of WLAN Mesh network as an area of special interest, a *literature review* was conducted in order to make an assessment of current status and advances made. Then a theory was developed along with an algorithm that can be implemented to improve scalability and extensibility. The next step was to carry out experimental work in order to validate the above mentioned theory, through development of a simulation model and data collection using statistical methods. Subsequent to data

collection, simulation results were presented together with their analytical interpretation. The figure below illustrates the adopted research methodology:

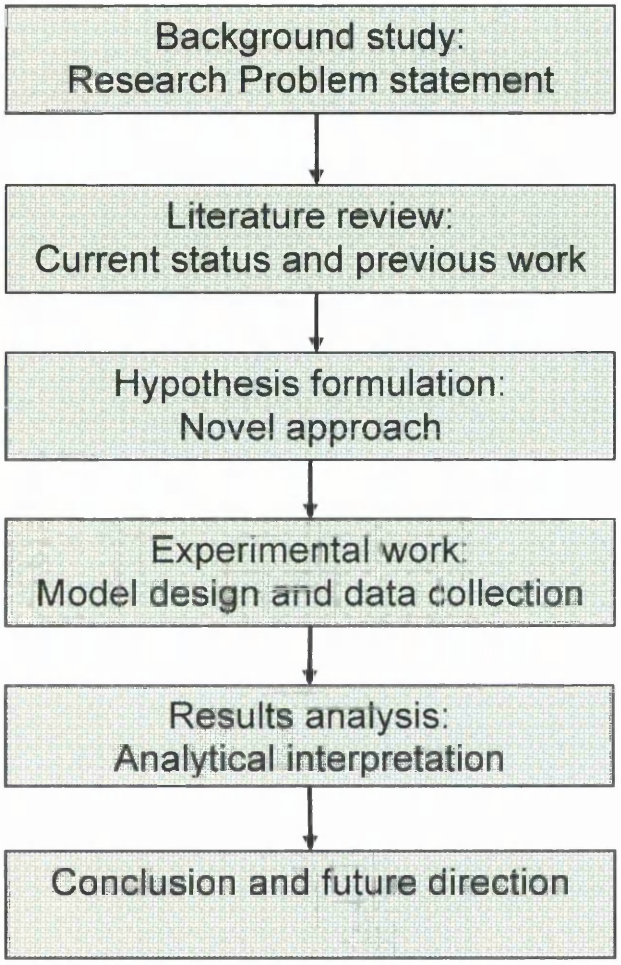

Figure 7: Research Methodology outline

1.6 Thesis organisation

The rest of this thesis is organised as follows:

Chapter 2 discusses path selection and forwarding protocols that are deployed in WLAN mesh. This research explored the working details of two popular protocols found in multihop wireless networks and gave an insight of a newer protocol proposed for the WLAN Mesh networks.

Chapter 3 deals with scalable interworking in WLAN Mesh networks. It provides the interworking problem statement followed by existing approaches to this issue. Following a critical analysis of the proposed mechanisms to address the interworking problem, this work proposes a novel approach to WLAN Mesh interworking with multiple mesh portals. This new approach is explained in detail including how it can work within various network topologies.

Chapter 4 is dedicated for experiments. Starting with a presentation of network modeling tools, it gives an experimental setup for the study of a WLAN Mesh network. Subsequently, network performance parameters were collected and presented. Based on the collected results, an in-depth network performance analysis is carried out by comparing scenarios with multiple operational portals versus a single operational portal.

Chapter 5 concludes with a summary of the work presented in this dissertation and gives a direction for further work in this area.

Chapter II

WLAN Mesh path selection and forwarding

2 WLAN Mesh path selection and forwarding

2.1 Introduction

Path selection and forwarding (commonly known as "routing") protocols are an integral part of network functions and play a key role in network performance.

It is noted that the term "*path selection and forwarding*" instead of "*routing*" has been used throughout the IEEE802.11s draft standard to avoid confusion between MANETs and WLAN Mesh, but the two terms technically mean the same.

Depending on network type and/or operational environment, some protocols perform well, whereas others are not fit for actual deployment due to their poor performance. In fact, first generation routing protocols such as RIP, OSPF and IS-IS, to mention a few, were developed with only wired networks in mind. Later on, wireless networks became more and more widely available and not only providing more opportunities in terms of availability but also with new areas of applications. Some of the hottest applications are for natural disaster management and the military, where wireless ad hoc networks often need to be put in place and operational without prior arrangements or setup beforehand. In such an environment there is a need for the network to get connected without central management and a capability to adapt to changing conditions in terms of mobility, increase/decrease of network nodes or operating conditions which may lead to closure of certain network links. It is in this regard that WMN networks were developed with appropriate routing protocols to meet those requirements.

There are mainly two types of routing protocols that are deployed separately or both combined to make a hybrid protocol:

- Proactive routing protocols: routing tables are populated as network nodes join the network regardless of a need to transmit data from any source-destination pairs. In proactive protocols, nodes keep constantly updating routing information from their neighbours as changes in network topology take place. Proactive protocols are efficient in wireless networks in such a way that once network convergence is achieved there won't be need for route establishments for data transmission between source and destination pairs. However, these protocols may not be scalable given the amount of information needed to keep global routing information.
- On-demand (reactive) routing protocols: these are protocols which determine path as a need arise to transmit data from a source to a given destination. There are no predefined paths, and these protocols are very flexible to easily adapt to changes in network topology. They also offer better scalability [15] when the network is more dynamic, but a rather huge initial delay due to their reactive path setup makes it difficult to be used for delay-sensitive applications such as VoIP.

The next sub-section presents three routing protocols, the first one being a purely proactive path selection and forwarding protocol, and the second protocol, a reactive path selection and forwarding protocol which forms a basis for the third path selection and forwarding protocol that has been proposed for WLAN Mesh networks, the Hybrid Wireless Mesh Protocol (HWMP). It is noted that besides HWMP, there have also been proposals [10] to use Radio Aware Optimized Link State Routing (RA OLSR) which is a variant of Optimized Link State Routing (OLSR) that uses radio aware metrics in forwarding path and multipoint relay (MPR) set calculation.

2.2 Proactive path selection and forwarding: Fast Optimized Link State Routing (Fast-OLSR)

Fast OLSR was designed to integrate fast mobility in the OLSR protocol, which is itself an optimization of the Link State Routing (LSR) protocol to support the requirements of mobile wireless LAN [26].

OLSR is a proactive routing protocol for mobile ad hoc networks. The main concept in OLSR is the use of MPRs, which are selected nodes to forward broadcast messages during the flooding process as shown in Figure 8.

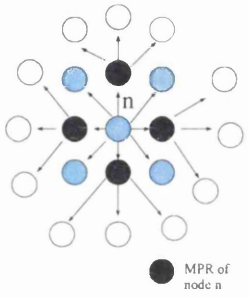

Figure 8: Multipoint relays

When MPRs are used, only a few selected nodes retransmit message when they receive the first copy of the message, thus substantially reducing the message overhead compared to a classical flooding mechanism where every node retransmits the messages. MPRs enable the minimization of flooding in the network and reduction of control packet size.

In OLSR, each node performs "Neighbour discovery" by broadcasting periodically *HELLO* messages containing the information about its neighbours and their link status. Upon reception of HELLO message, each node makes a table of nodes selected as its MPRs.

The topology dissemination is achieved by means of Topology Control (TC) messages which are forwarded in the same way as broadcast messages in the whole network.

Although OLSR has proven to be more efficient than classical LSR, it does not perform well with fast moving nodes as the links with neighbours are valid only during a short time interval [21]. Hence, another extension of OLSR, the "Fast-OLSR", was designed to cater for fast moving nodes in routing with a minimum routing overhead.

The study of Fast OLSR in this report is based on previous work by Benzaid et al [22].

Fast-OLSR has 2 objectives:

- Induced control traffic is tuned to mobility (to track a fast moving node): control traffic increases with mobility
- Bandwidth consumed by control traffic remains reasonable

The "neighbour discovery" should support switching to *Fast-Moving/Default* mode, establishing *Fast-Links,* refreshing *Fast-Links* and detecting new/broken links: an MPR of node *m* must receive a *Fast-Hello* within "*3xFast-hello-interval",* otherwise the link is considered broken and that has to be advertised in topology control messages.

Evaluation of Fast OLSR

The effect of the overlapping fraction α to the loss rate was tested and simulation results were compared with analysis results [22]. The analysis of the effects of overlapping in Fast-OLSR ad-hoc routing and performance evaluation by simulation has shown that zero packet loss can be guaranteed by using soft-handoffs with data buffering for a time period

directly proportional to *3xFast-hello-interval* with an additional consideration for the overlapping ratio, mobility (velocity) & cell size.

2.3 Reactive (on demand) path selection and forwarding: Ad Hoc On Demand Distance Vector Routing Protocol (AODV)

AODV is a distance vector routing protocol designed for mobile nodes in ad hoc networks [4]. It easily adapts to changing link conditions and has the ability to notify nodes of link breakages. AODV has the main advantages of low processing, low network utilisation and is loop-free: it avoids looping problems such as "counting to infinity".

AODV makes use of a destination sequence number for best route selection and utilizes management messages for route discovery:

- Route Requests (RREQs)
- Route Replies (RREPs)
- Route Errors (RERRs)
- Route Reply Acknowledgement (RREP-ACK)

In AODV, a route table contains the following entries:

- Destination IP address, Destination Sequence number, Status and Routing Flags, Hop Count, Next Hop, Lifetime and List of Precursors.

When a route to destination is needed, an RREQ is generated and disseminated. A new route may be required when the destination was not previously known or a when a previous valid route expires or becomes invalid.

To avoid looping, an RREQ contains a last "destination sequence number" known for this destination and the destination sequence number is updated whenever a node receives new information about the sequence number related to the destination concerned. This is achieved by comparing the

currently stored sequence number and that from incoming message to ensure that the information is fresh enough.

Besides the destination sequence numbers, an RREQ ID and originator IP address are buffered to avoid reprocessing and reforwarding from neighbours.

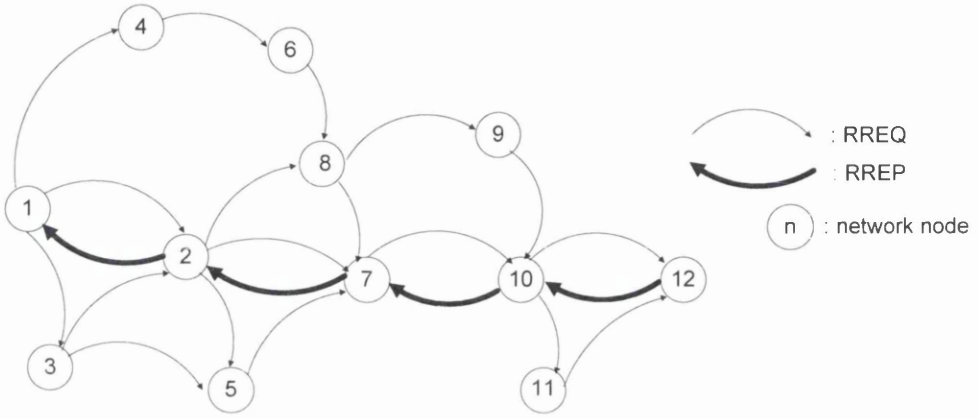

Figure 9: AODV route discovery

Figure 9 illustrates a route discovery session using RREQ and RREP management messages. Given node 1 as the traffic source, and node 12 for destination, a RREQ message is flooded throughout the network. Once the RREQ is received at node 12, a RREP message is generated and sent back (unicast) to node 1. It is assumed that other management messages, such as local connectivity messages, were successfully exchanged between neighbours.

AODV route discovery process can also be represented by a finite state machine (FSM) to show the states of the protocol. The FSM shown in Figure 10 gives an overview of state transitions for the establishment of a route from source to destination including route rediscovery in the event of

a link failure. It is noted that this FSM diagram contains some elements based on the work done by Ye and Li[3].

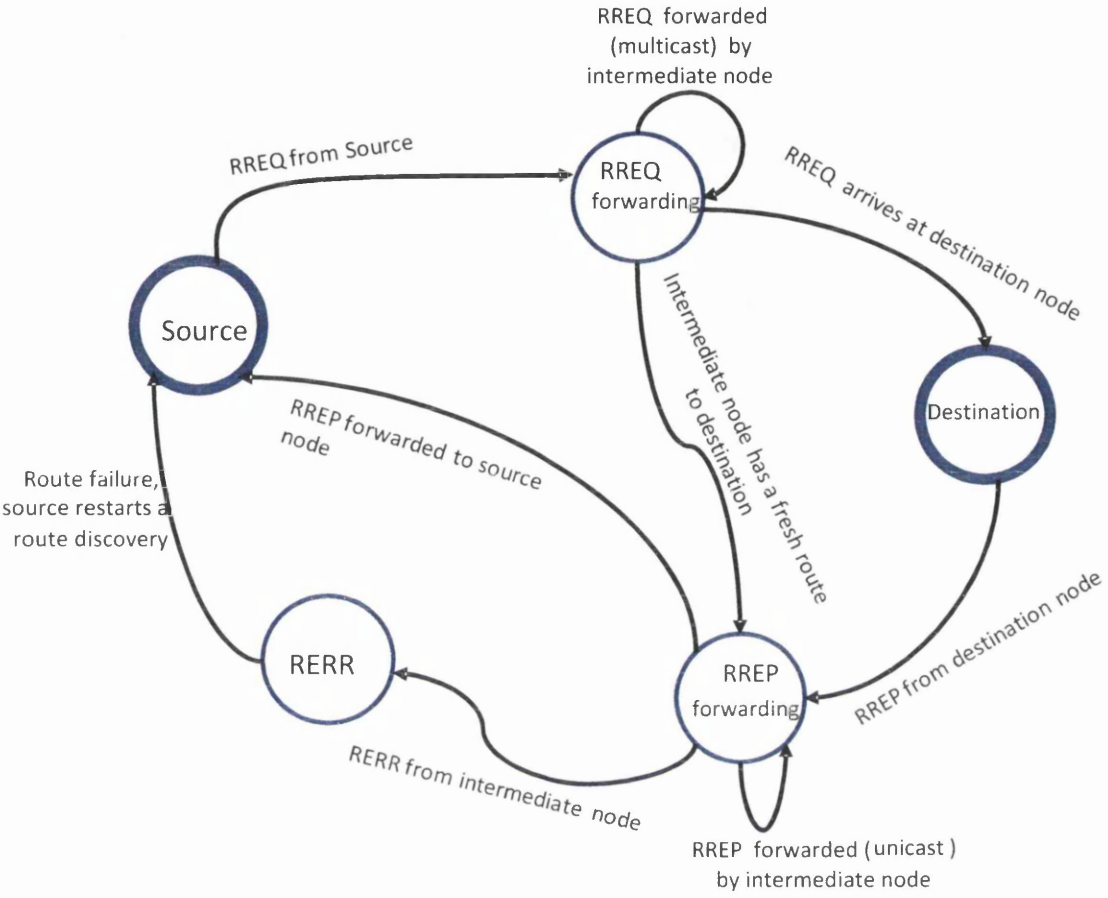

Figure 10: A FSM for AODV route discovery

AODV operation is summarised below:

- RREQ attempts are made up to the max TTL value given in IP header
- When an RREQ is broadcast for the first time, the source waits NET_TRAVERSAL_TIME ms before another RREQ is sent, in case no RREP was received

[3] Xia Yi and Junshan Li. "An FSM-based Automatic Detection in AODV for Ad Hoc Network". In proceedings of International Symposium on Computer Network and Multimedia Technology, CNMT 2009.

- To avoid congestion, Repeated RREQ attempts uses the Exponential backoff algorithm
- If no route is found after RREQ_RETRIES time, data packets are dropped and "Destination Unreachable Message" is sent to the originator
- The *Expanding ring search technique* is used to avoid unnecessary network-wide dissemination of RREQs:
    1. TTL=TTL_START
    2. TTL=TTL_START+TTL_INCREMENT until TTL=TTL_TRESHOLD
    3. TTL=NET_DIAMETER.
    4. Timeout for receiving a reply is RING_TRAVERSAL_TIME
- TTL in RREQ IP header is initially set to Hop Count+ TTL_INCREMENT in case a new route to the same destination is needed in future
- At reception of an RREQ a node:
    - Creates or Updates the sequence number of previous hop
    - Checks if it had not already received a RREQ from the same source within PATH_DISCOVERY_TIME: if yes, the new RREQ is discarded
    - Increments the hop count value by 1
    - Searches for a reverse route to the originator (longest prefix matching)
    - Sequence number is updated and set to "valid" status
    - Next hop in routing table is updated to the value from which the RREQ was received
- RREP is generated either when:
    - A node is itself the destination

- A node has active route to destination: sequence number is equal or greater than the value in RREQ

Case1 (sequence number is equal to the value in RREQ):

- RREP is forwarded back to source node
- Hop count is set to 0
- Sequence number is incremented by 1
- Destination node copies MY_ROUTE_TIMEOUT value into the Lifetime field of RREP

Case2 (sequence number is greater than the value in RREQ):

- Node Sequence number is copied to the RREP' destination sequence number
- The route table is updated: node originating RREQ, next hop towards destination is kept in precursor list, lifetime is calculated
- RREP is forwarded back to source node
- Gratuitous RREP is forwarded to destination node

- Route Error Messages:
  - A Node can issue an RERR on:
    - Detection of a link break or unsuccessful link repair
    - Reception of a packet for which it has no active route
    - Reception of an RERR from a neighbour for one or more active routes
- An RERR is received by nodes in precursor list of the unreachable destination. Generally RERR are broadcast to 255.255.255.255

- Before RERR is transmitted, routing table entries are updated: destination sequence number, route entry status and lifetime.
- Local repairs:
  - When a link breaks and destination is not farther than MAX_REPAIR_TTL hops away
  - Destination sequence number is incremented and RREQ broadcasted to the destination
  - In case an RREP is obtained with higher hop count than the failed link, an RERR is issued.
- System reboot:
  - Each node on reboot has to wait for messages from neighbouring nodes to get appropriate sequence number information
- AODV and Aggregated networks:
  - In case mobile nodes share a common subnet prefix (making a subnet), a single node can act as a subnet router
  - The subnet router advertises reachability for all other nodes in the subnet
- AODV with other networks:
  - An Infrastructure router is used to access external network.
  - A destination sequence number is kept for external subnet.
- Security considerations:
  - AODV does not provide security mechanisms: possibility of impersonation and denial of service
  - Performance of proposed authentication mechanisms is not appraised
- Internet Protocol versions issues: AODV works similarly for IPv4 and IPv6 except the message length

2.4 Hybrid path selection and forwarding protocol: *Hybrid Wireless Mesh Protocol (HWMP)*

HWMP is a path selection and forwarding protocol adopted by the current IEEE 802.11s [10] draft standard. Every standard compliant device will be able to support this protocol for interoperability among devices from different vendors [3].

HWMP is a hybrid protocol which combines the flexibility of on demand protocols in a changing environment and the efficiency of proactive protocols in a fixed environment [19]. That makes HWMP suitable for mesh implementation as a mesh network may consists of both fixed nodes and mobile nodes (infrastructure and non-infrastructure mode).

HWMP is based on common set of protocol primitives, generation and processing rules founded on Ad Hoc On Demand Distance Vector (AODV) protocol [4] with an adaptation to use the MAC address in path selection and link metric consideration.

In HWMP two modes of operation can be supported depending on configuration:

- On demand mode: in this mode, there is no root node and MPs can communicate through peer-to-peer paths. However, this mode can also be used even if there is a root node provided the on-demand mode can provide a better path.
- Proactive tree building mode: this mode functions with a root node in the mesh network so that paths from each node to the root node can be predefined either using Path Requests (PREQ) or Root Announcements (RANN) process.

The two modes above can be used concurrently in a mesh network where communication can start with proactive mode while the on-demand mode tries to find the best path, and then switch to the latter one once the best path is found.

HWMP uses the following information elements in path discovery:

- Path Request (PREQ),
- Path Reply (PREP),
- Path Error (PERR) and
- Root Announcement (RANN).

A link cost metric will be used to select HWMP paths, and this metric information is propagated between Mesh Points (MPs) by PREQ, PREP and RANN elements. It is noted that the current standard considers an "Airtime Link Metric" as a default mandatory path selection metric.

The airtime link metric (*airtime cost*) is calculated as given below:

$$c_a = \left[o + \frac{B_t}{r} \right] \frac{1}{1 - e_f} ,$$

where o is the channel access overhead, which includes frame headers, training sequences, access protocol frames etc. This value varies depending on PHY.

B_t – the number of bits in test frame

r – data rate in Mb/s

e_f - frame error rate for the test frame size B_t

The data rate r means the rate at which the MP would transmit a frame of size B_t with frame error rate e_f based on current conditions of radio environment.

Looping is avoided in HWMP by means of sequence number mechanisms in such a way that each MP keeps its own sequence number which is communicated to other MPs. Although HWMP is the default routing

protocol as per the IEEE802.11s standard, it still has a number of shortcomings [28] in terms of scalability, interaction with other MAC functionality, multiple metrics integration and supporting of legacy nodes just to mention a few.

2.5 Summary

Chapter 2 discussed WLAN mesh path selection and forwarding, technically meaning the same as routing in MANET. It was explained that a new routing protocols for WMN were developed in order to meet the requirements of such networks which rely on wireless media, support node mobility, support ad hoc topologies and may lack central management among other key characteristics.

Three path selection and forwarding protocols were presented, the first two being based on different functional principles while the third is hybrid protocol based on main principles of those two.

i. Fast Optimized Link State Routing (Fast-OLSR) is a proactive routing protocol designed to integrate mobility in the OLSR protocol for ad hoc mobile networks. Fast-OLSR is based on the same principles as OLSR regarding the minimization of broadcast messages by using MPRs. Additionally, Fast-OLSR can tune control traffic to track a fast moving node but always keeping the control overhead reasonable.

ii. Ad Hoc On Demand Distance Vector (AODV) is a reactive distance vector routing protocol which can easily adapt to changing link conditions by notifying nodes about link breakages. AODV requires low processing, low network utilisation and is loop free.

iii. Hybrid Wireless Mesh Protocol (HWMP): this is a path selection and forwarding protocol adopted by IEEE802.11s. It is a hybrid of reactive and proactive protocols, combining the flexibility of the former in changing environments and the efficiency of the latter in fixed environments. Although this protocol is the default protocol for WLAN Mesh networks, it still presents some challenges including but not limited to scalability, multiple metrics integration and support for legacy nodes.

Chapter III

Scalable interworking in WLAN Mesh networks

3 Scalable interworking in WLAN Mesh networks

3.1 Introduction

WLAN Mesh networks should be able to interwork with non-mesh networks for data transmission unless they are deployed in isolated environments. An obvious example is a wireless node being part of the mesh network which may need to access services available on the Internet. Understandably, this will involve at least one gateway node to connect the mesh network to the Internet. There is a possibility that several mesh nodes could need connections to the Internet at the same time (simultaneous connections), thus generating a considerable traffic load between the mesh network (perceived as a single network segment) and the Internet. As the number of mesh nodes increases, scalability becomes an issue given that MPs act as proxies for associated STAs. Lim et al. [2] have discussed scalable station association information handling in order to address the problem of huge proxy tables for MAP. The authors proposed a scheme for Local Association Base (LAB) and Global Association Base (GAB) management to deal with the increasing numbers of STAs associated with each MAP. Besides limitations in terms of proxy table size, mesh network scalability is challenged with the possible number of active MPPs in the mesh network. In fact, if only a single MPP is operational, it will be a proxy for all other nodes and becomes a bottleneck between the mesh network and non-mesh network. The remaining part of this chapter discusses the selection of single-hop or multihop paths and forwarding of data frames across these paths between MPs at the link layer (i.e., layer 2) of OSI protocol reference model, followed by a detailed presentation of WLAN Mesh interworking.

3.2 Layer-2 path selection and forwarding

Traditionally routing protocols have been implemented at OSI Layer 3 (e.g. IP), making the use of layer-3 addresses. This approach works well in wired networks, infrastructure WLAN and has also been deployed in mobile ad hoc networks (MANET). MANETs and WMNs work on the same major principles of multihop wireless routing but they are different in such a way that MANETs are mostly being deployed with mobility and ad hoc capabilities as the key characteristics. WMNs are widely deployed in static environments with the main concerns being extensibility, scalability, reliability and how practical they can be in terms of deployment.

Given the fundamental differences between the two closely related types of network, the proposed path selection and forwarding protocols for WLAN Mesh networks are generally derived from MANET routing protocols with additional extensions to support routing at layer 2. The protocol uses MAC addresses, radio aware routing metric and provides mesh unicast, multicast as well as broadcast data delivery [3].

Although there are several advantages of layer-2 path selection and forwarding, interoperability is the most obvious reason. Wang et al [28] have suggested that IEEE802.11s could be the first standard to specify routing in the MAC layer. Given that there were many proprietary protocols that needed to be interoperable in 802.11 mesh networks, an extensible framework that is supported by all of them had to be put in place.

With path selection and forwarding mechanisms in the MAC layer, only MAC addresses are used for packet forwarding to/from MPs, MPPs, MAPs and associated STAs. This requires at least four MAC addresses in each frame header comprising of original source and destination MAC addresses given in IEEE802.11 [12] and an additional 2 addresses to support multihop forwarding. Furthermore, a 6-address scheme [20] was introduced because

the 4-address scheme could not efficiently support all scenarios in mesh networks in case frames sent from STAs are delivered through multiple MPs, with a possibility to include MPPs as well. The new (optional) addresses will be part of a mesh header as shown in the figure below, where

- RA: Frame Receiver Address
- DA: Destination address
- SA: Source Address
- TA: Frame Transmitter address.

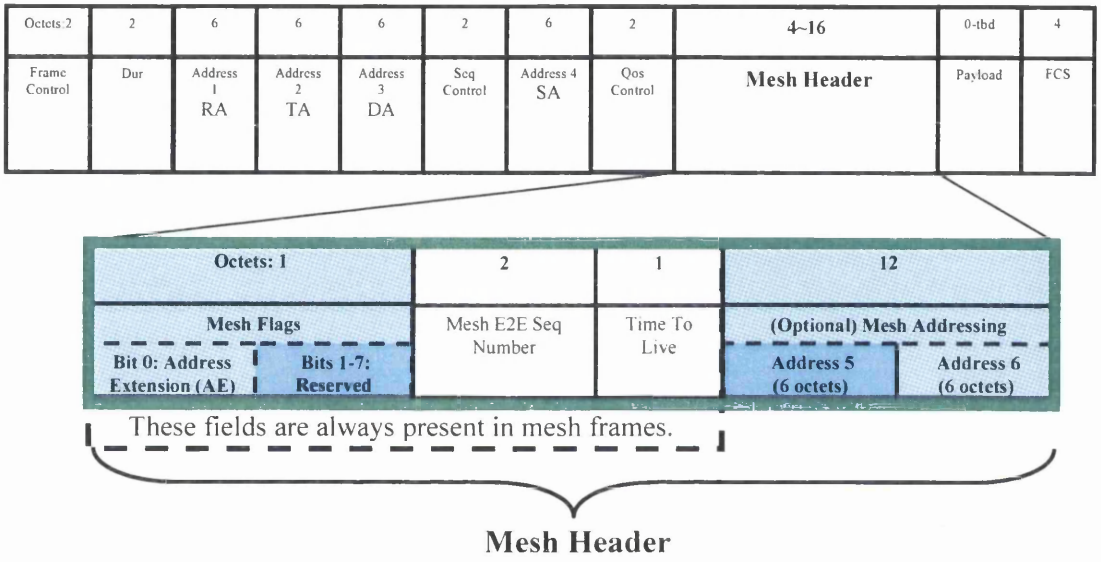

Figure 11: 6-Address Scheme [20]

3.3 WLAN Mesh interworking

The MPP being a gateway point as mentioned in Section 1.3, it should be able to handle different frame formats and forward the information to intended destinations with layer-2 path selection and forwarding protocols inside the mesh network.

One of the major issues is to provide a practical solution to interworking with bridged LANs, where the spanning tree protocol (STP) is being used. In fact, a traditional bridge as defined in IEEE 802.1D standard [11] will consider a WLAN mesh as a single network segment; thus allowing only one port to access this segment so that broadcast loops can be avoided. This would create a bottleneck at the bridge port as every communication between nodes inside the mesh and those outside will use only one port. Furthermore, the network reliability can not be assured, hence affecting the overall network performance.

The interworking section of the current IEEE802.11s standard is mostly devoted to the description of two major functions:

1. MPP announcement protocol and
2. Proxy protocol.

The MPP announcement protocol is based on the portal announcement (PANN) information element and allows MPs to select the appropriate MPP and build a path towards it. The proxy protocol, on the other hand, is used to inform a destination MP (including MPP) of the proxied addresses of the source MP. In interworking with external networks, this proxy protocol provides "proxy information" to MPPs, which will be transferred to the MAC relay entity as defined in IEEE 802.1D so that the bridge part of MPPs can learn the addresses of all the MPs and their associated STAs.

It is noted that the interworking specifications in the current IEEE 802.11s draft standard include some basic components – e.g., MPP announcement,

proxy protocols, and message formats – to support multiple portals, but they are not enough to actually implement it.

In order to address the above issues, there should be alternative path(s) not using the same port, or in other words, not the same MPP. With the use of multiple MPPs on the same LAN segment, the network load can be shared among various MPPs (i.e. load balancing) and the network reliability can be improved.

However, as multiple MPPs are connected to a single LAN segment, if MPPs are combined with a standard layer-2 bridge, the STP will leave only a port of one MPP open, while all others will be blocked as mentioned above. On the other hand, the path through a port which was left open may not be the best one for forwarding frames between some of the nodes in the mesh and the external network, thus resulting in unnecessary contention delays and forwarding overhead due to the increased number of hops between those nodes and the MPP.

The best solution would be to allow the use of multiple MPPs simultaneously and provide an algorithm for broadcast loops prevention.

It is in this regard that we propose a new interworking framework for IEEE 802.11s WLAN mesh, which consists of procedures for network topology/LAN segment identification, a frame filtering process at MPPs, inter-portal communication scheme and new information elements as well as a mesh header field to support this framework. The next section explores suggested solutions from the research community and we present our own approach later on.

3.3.1 Existing approaches to WLAN Mesh Interworking

In an attempt to solve the above mentioned problems, various research works have been carried out. To the best of our knowledge, however, none of them has proven to be effective for all possible interworking scenarios.

In [17], the use of "Extended Mesh Portals" has been proposed to enable multiple MPPs in interworking with a logical separation of WLAN Mesh. It proposes the assignation of a single MPP for each group of nodes such that an MPP can only forward frames to and from its member nodes. This proposal may raise scalability issues; as the number of nodes in the mesh network increases, so does the protocol overhead to determine which nodes belong to which MPP. Besides that, in case an MPP needs wireless connectivity with another MPP which is not on the same wired LAN segment, there should be no frame filtering and therefore the operation mode needs to be changed from an extended mode to a normal one. Switching from one mode to another (i.e., extended mode vs. normal mode) will also require some processing to determine whether concerned MPPs need wireless connectivity or not, which results in increased delays.

A further solution proposed by S. Rahman et al. [23] has put an emphasis on the portal roles, with one portal working as a default portal whereas the remaining work as backup portals. A default portal is a default forwarder for a given external LAN with a capacity to respond to 802.1D BPDUs. On the other hand, a backup portal which has a wired connection to a default portal does not forward or respond to 802.1D BPDUs. This proposal requires the identification of portal roles, and then the selection of one default portal per LAN segment. With a single portal in operation, there will be a potential bottleneck in case a large number of nodes needs to use that portal; that is why multiple forwarding portals are necessary on the same LAN segment.

Another approach based on multihop grouping was suggested, where a group consists of one MPP and one or more MPs. Kim et al. introduced the idea of dynamic frame filtering with conditional frame forwarding using frame filtering information in [18]. By grouping, MPs are assigned to MPPs

in such a way that each MP can communicate with outside nodes (located on LAN segments) by using only one selected active MPP. This solution does not cater for network topologies where multiple external networks are connected through a WLAN mesh.

In [25], Strutt and Kruys suggested that multiple MPPs can be used in interworking by subdividing a mesh network into several broadcast domains with a single MPP per broadcast domain, such that there is no mesh connection between the broadcast domains. This solution requires additional means for broadcast domains identification among all mesh nodes. It can also result in inefficient operation in case the frame source and destination reside in different broadcast domains. A different multi-portal approach was also given to configure and provide a protocol to select only one portal to be active at a time. This involves a portal arbitration protocol for connected portals, but there is no provision for load balancing as only one portal can be used at a time.

3.3.2 Novel approach to WLAN Mesh Interworking with Multiple Mesh Portals

WLAN mesh networks should be able to use multiple MPPs regardless of whether they are attached on the same wired LAN or not. Furthermore, multiple portals should be supported in all possible cases of source and destination nodes' locations, with any node being on either side of the mesh network. We consider various network topology scenarios, where the source and destination can be either inside or outside the mesh network with a possibility of both nodes being on separate wired LANs.

Regardless of network topology, when a communication from source to destination needs to use MPP(s), there are only two possible cases:

1. The correct MPP(s) is (are) known and then frames are delivered via unicast through the MPP(s).
2. The correct MPPs are not known and frames are broadcast to all MPPs, including those connected to the same wired LAN segment.

The latter case is more likely to cause broadcast loops as a frame from the mesh network via one MPP may come back to the mesh through another MPP and keep bouncing back and forth to the non-mesh network as shown by dotted lines in Figure 12

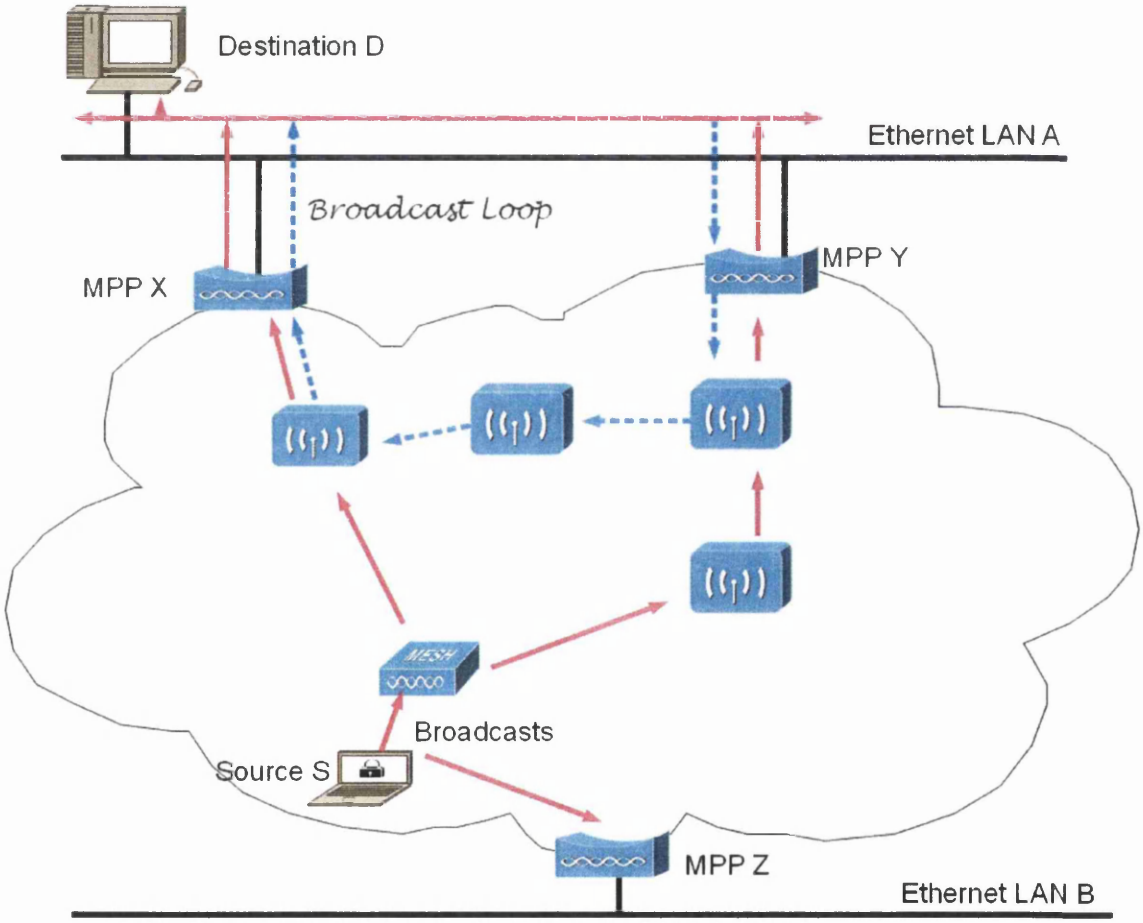

Figure 12: Broadcast loop formation in WLAN mesh network

Broadcast loops will be created if the MPP simply broadcasts all frames with unknown destination address without considering the frame contents

and without the blocking function as normally done through the STP (our new MPP architecture does not perform port blocking). On the other hand, an MPP can examine the frames it receives in order to determine whether the frame has already been broadcasted by another MPP or not.

That process, hereafter called "Frame Filtering", will allow the MPP to discard duplicate frames hence avoiding the formation of loops.

A mesh data frame – when transmitted between neighbour MPs – contains a "Mesh Header" field as shown in Figure 13, which is inspected during the frame filtering process.

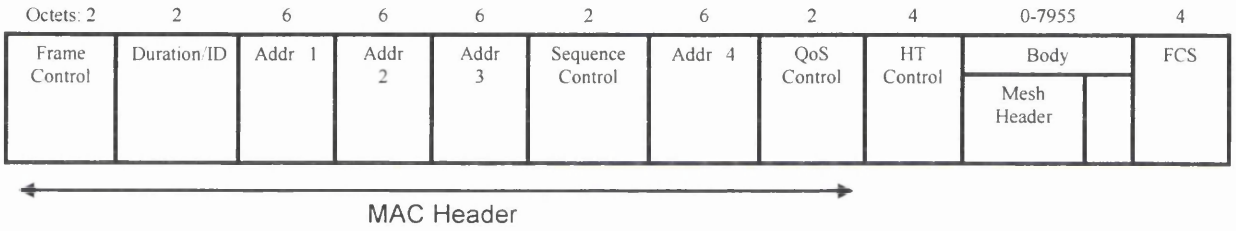

Figure 13: IEEE 802.11s MAC frame format

To prevent the formation of broadcast loops, the following additional information is needed during the frame filtering process:

1. Bridged LAN segments identifications (LAN_IDs)
2. Unique 5-bit MPP identification (MPP_ID) in every frame forwarded by an MPP to the mesh network.

When a frame is internally generated, the MPP_ID is set to all zero's, which is also the default value.

The first information (LAN_IDs) will be carried within the portal announcement (PANN) information element, which is used for announcing the presence of an MP in a mesh network that has a live connection to an external network.

The new PANN information element format is shown in Figure 14 with a 5-bit LAN_ID that we introduce. The 5 bits were taken from the flags field (so far reserved), with a maximum capacity of 31 LAN segments to be attached to the mesh network.

Octets: 1	1	1		1	6	4	4	4
Element ID	Length	Flags		Hopcount	Time to Live	Originator Address	Sequence Number	Metric
		Bits 0-4: LAN_ID	Bits 5-7: Reserved					

Figure 14: PANN Information Element

3.3.2.1 Network Topology/LAN Segments identification

The newly introduced information element field, the LAN_ID, must be provided before any frame filtering can take place. This information is derived from network topology identification procedures which assign a single LAN_ID to each and every wired LAN segment.

With reference to the work by S. Rahman et al [23], this research proposes the following steps for wired network topology identification:

1. When an MPP becomes live for the first time (turned ON), it will assign itself a 5-bit MPP_ID generated based on its MAC address and use the same value as the initial LAN_ID.
2. All MPPs in the mesh network broadcasts PANNs so that every MPP learns wireless MAC addresses of all other MPPs
3. Every MPP unicasts its wired MAC address to other MPPs so that each MPP can build a list of wired MAC addresses of every other MPP
4. Each MPP performs multiple unicasts by sending frames to individual wired MAC addresses it has learned in the previous step. In case a response to the sent frames is received, both MPPs will

know that they are on the same wired LAN segment. Otherwise, there is no common wired LAN segment.

5. MPPs on the same wired LAN segment compare the values of their LAN_IDs and the least of them is selected as the LAN_ID for this particular LAN segment.
6. All MPPs send updated PANN containing new values of LAN_ID

Wired LAN segment's information will be updated whenever the network topology changes.

As for MPP identification, the "Mesh header" field in the Mesh data frame is modified in order to include the portal identification of the MPP which forwards the concerned frame as shown in
Figure 15.

Octets:1			1	4	0,6,12,18
Mesh Flags			Mesh Time To Live (TTL)	Mesh Sequence Number	Mesh Address Extension (present in some configuration)
Bits 0-1: Address Extension(AE) Mode	Bit 2: Power Save Level	Bits 3-7: MPP_ID			

Figure 15: Mesh Header Field

3.3.2.2 Portal Announcement

Portal announcements allow the MPs to learn all MPPs and LAN segments to which they are attached, thus allowing each MP to choose an appropriate MPP and select a path towards it.

In case a mesh network is connected to several LAN segments with some MPPs being connected to the same LAN segment, every MP will be able to select the best unique MPP for communication with each LAN segment[4].

As sets of MPs will be allocated to particular MPPs, every MPP will have a reasonable number of MPs per LAN segment to serve as a proxy. This will

[4] The actual procedure for selecting the best unique MPP is specific to a path selection protocol in use in the mesh network.

make the load balancing possible especially when the link cost is related to the load and MPPs will be selected based on the link cost between them and MPs.

Every MP will build a table containing the following information:

- MPP_IDs of all MPPs for which it received PANNs
- Link cost to MPPs
- Corresponding LAN_ID for each MPP–LAN segment pair, i.e., the LAN segment which a particular MPP is connected to.

3.3.2.3 Frame filtering process

When a frame originating from an external LAN reaches an MPP, the MPP_ID will be copied into the "Mesh Header" field as shown in Figure 15 and then forwarded to the next hop MP inside the mesh network. There are two possible destinations:

- If the frame destination address is inside the mesh network, the MP will do the path selection and forwarding for the frame to reach the final destination.
- If the frame destination address is not known, the MP will forward the frame to all one hop nodes excluding MPPs which are attached to the same LAN segment as the one from which the frame originates. This can be achieved by comparing the LAN_ID of the source MPP with those of other MPPs.

The frame filtering process at MPPs for loop avoidance is described by the flowchart shown in Figure 16.

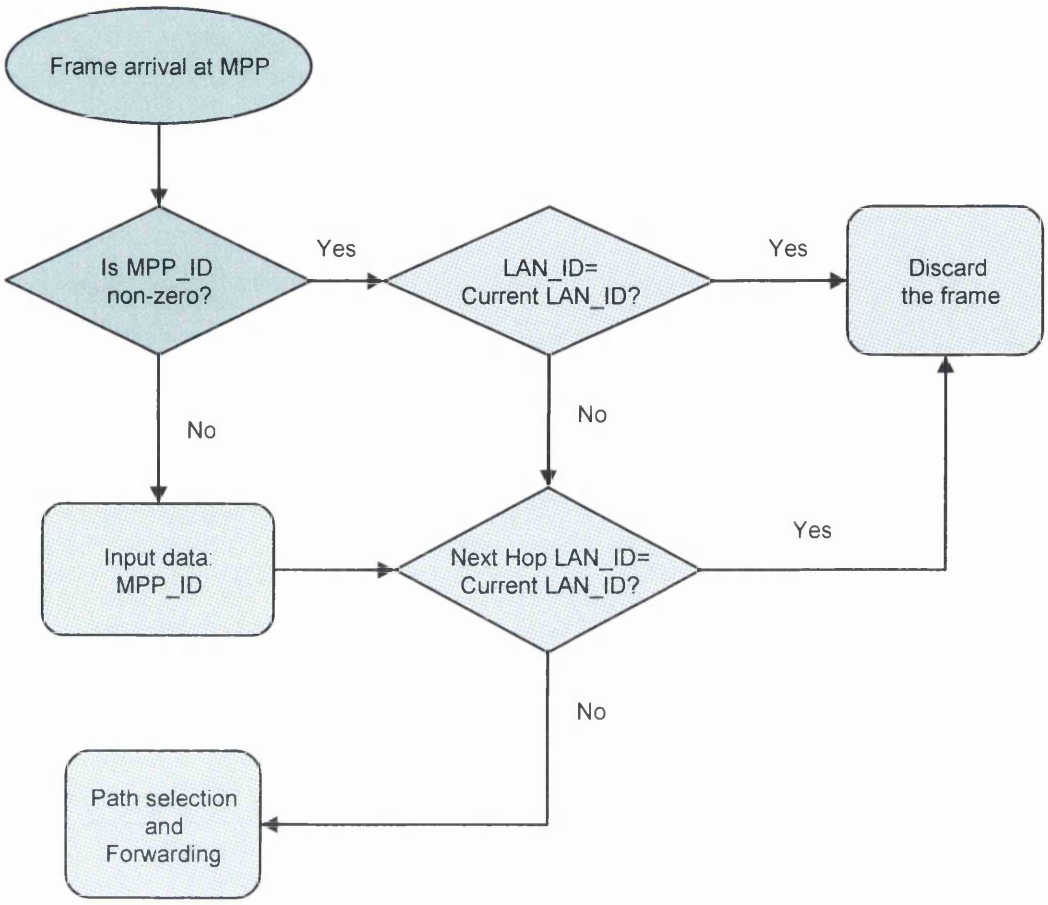

Figure 16: Frame filtering at MPPs for broadcast loop avoidance

3.3.2.4 Inter-Portal Communication Procedures

Besides the portal announcements, there is also a need for MPPs to communicate and share the path selection related information. These processes are termed as "Inter-Portal Communication (IPC) Procedures".

The IPC procedures are triggered by an MPP after receiving a new unicast data frame from either MP or MPP, which informs other MPPs on the same LAN segment of the selection made by a particular MP or MPP of the triggering MPP as its Designated Portal (DP). This allows the informed MPPs to avoid subsequent frame duplications.

Given that IPC procedures are done by MPPs on the same wired LAN segment, all information exchanges will be carried through the wired medium in order to avoid unnecessary communications overloads on the

limited wireless resources. On the other hand, there could be cases where more than two MPPs are connected to the same wired LAN segment, thus requiring the IPC procedures to happen between all those MPPs. This will involve the sending of the same frame to multiple destinations.

In sending that information, there are two possible approaches:

1. Multiple unicasts (i.e., using individual MPP addresses)
2. Multicasting (i.e., optional use of group addresses)

Note that the latter case could reduce a communication overhead, but involves further procedures to assign a group address to MPPs on the same LAN segment.

For the information to be delivered through the IPC procedures, this research introduces a new information element, known as "Designated Portal Announcement" henceforth noted as DPANN.

Once the best unique MPP is selected for a source-destination pair, the DP will send a DPANN to MPPs on the same LAN segment. DPANN information element is shown in
Figure **17**, with the following fields:

- ID : This is an identification used to mention that DPANN is a management information element. DPANN is assigned to the value of 17 as this value was so far reserved in the IEEE 802.11 standard [12].
- Length: The length is set to 5+(M*2*6).
- Sequence number: This field is assigned the sequence number of the DPANN and it will be used for avoiding DPANN duplication.
- No. of Proxied Nodes (M): It is set to the number of source-destination pairs for which the MPP was chosen as a DP.

- Destination MAC Address 1: This is the MAC address of the first destination node to use the concerned MPP as its DP.
- Source MAC Address 1: This is the MAC address of the first source node to use the concerned MPP as its DP.

Octets:1	1	1	1	1	6	6	...	6	6
ID	Length	Sequence Number	Designated Portal: MPP_ID	No. of Proxied Nodes(M)	Destination MAC Address1	Source MAC Address1	...	Destination MAC Address M	Source MAC Address M

Figure 17: DPANN Information Element

As the new destination-source pairs choose a given MPP as their DP, their MAC addresses are appended to the DPANN (from Address 1 to M, where M is a variable integer).

Whenever the IPC procedures are triggered as mentioned above, the DPANNs are sent to all concerned MPPs for them to update their databases of DPs per source-destination pairs. It is mentioned that each MPP will dynamically keep updating its own information base as the network topology changes.

The IPC procedures are likely to increase the overall network latency, however; given that the DPANNs are sent through the wired medium only, their impact on the mesh network is not expected to significantly affect the network performance.

Furthermore, it is noted that the use of the wired medium for communications between MPPs was previously suggested in [23] for other purposes such as the LAN segment identification. We suggest using the same approach because the wired networks offer far more resources compared to the wireless networks. Still, there is another challenge arising from the use of wired medium for communications between wireless nodes (for instance, the sources and destinations of DPANNs are in fact on the

wireless interfaces of MPPs.). There will be necessary DPANN frame handling procedures on the wired LANs, which are not detailed in this report.

3.3.2.5 Interworking examples

In this section we illustrate how the proposed frame filtering process with the new fields enables multiple MPPs in interworking with external LANs through several examples for various network topologies.

We assume the following for the examples considered in this section:

- The frame filtering process prevents frame forwarding to/from MPPs on the same LAN segment. This does not apply for the IPC frames, which are control frames.
- IPC procedures are triggered by an MPP when receiving a new unicast data frame from either MP or MPP. These procedures inform all MPPs of the known paths to external nodes and the selection made by MP or MPP (as its proxy) with regard to those nodes in order to avoid subsequent frame duplications.
- In case a destination node is outside the mesh network, its address has been learned by all MPPs connected to the same LAN segment through the learning process of bridging functionality.

3.3.2.5.1 External source and internal destination

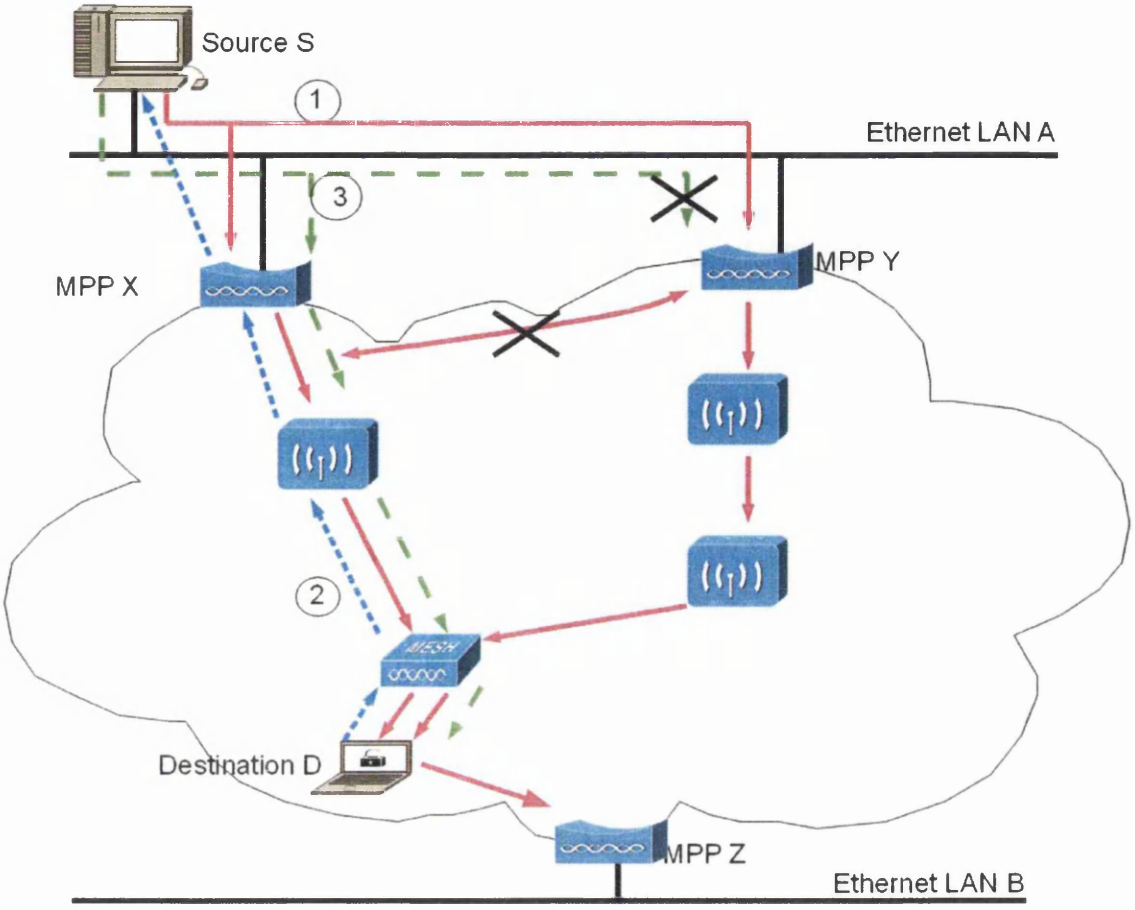

Figure 18: External source and Internal destination

In an interworking scenario involving an external source node and an internal destination node as shown in Figure 18, the information exchange is done as follows:

1. The source S sends frames with destination address D to both MPPs X and Y which then broadcast to the mesh network path requests (PREQs) on behalf of S. Then through multihop forwarding, the PREQs reach destination D. It is noted that the destination D will receive multiple PREQs with the same source and destination address.

2. The destination D selects one portal, to which it can send (unicast) a path reply (PREP). Let us assume that MPP X in this case is chosen. This triggers IPC procedures, which informs all MPPs (including MPP Y) that MPP X is selected as a proxy for S with regard to D. MPP X will be able to forward subsequent packets to S by means of the bridging functionality.
3. After the path has been set up, the source S unicasts data frames to the destination D via both MPP X and MPP Y, but MPP Y discards the frames (as it has learned from the IPC procedures that only MPP X is a proxy for S). Finally, MPP X unicasts the data frames to the destination D.

3.3.2.5.2 Internal source and external destination

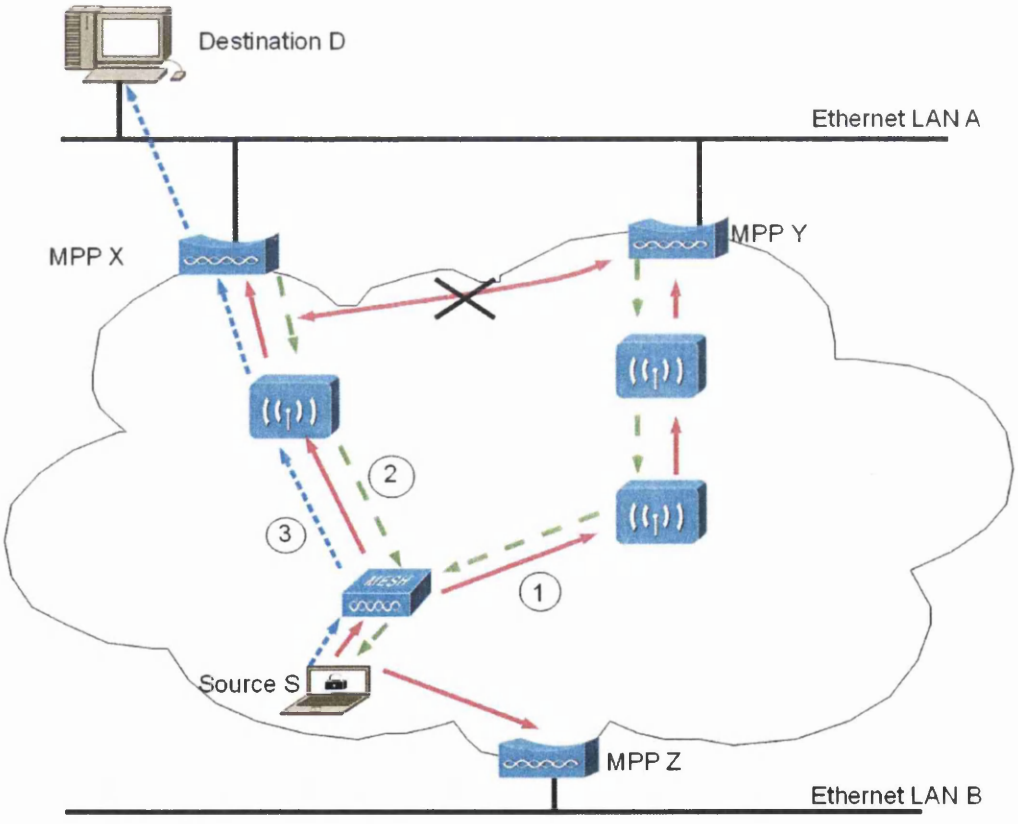

Figure 19: Internal source and External destination

In this scenario a source node inside the mesh network communicates with a destination outside the mesh network, as shown in Figure 19. The following steps take place in this case:

1. Source S broadcasts PREQs with destination address D to all MPPs.
2. The MPPs connected to the LAN segment where the destination D is attached (MPPs X and Y in this example) send unicast PREPs to the source S on behalf of the destination D. Multiple PREP frames will be received at source S.
3. The source S selects one portal, say MPP X in this case, and unicasts data frames to the destination D through MPP X. This triggers interportal communications, which informs all MPPs (including MPP Y) that MPP X is selected as a proxy for S with regard to D. After this, there will be only unicasts between S and D through MPP X.

3.3.2.5.3 External source and external destination

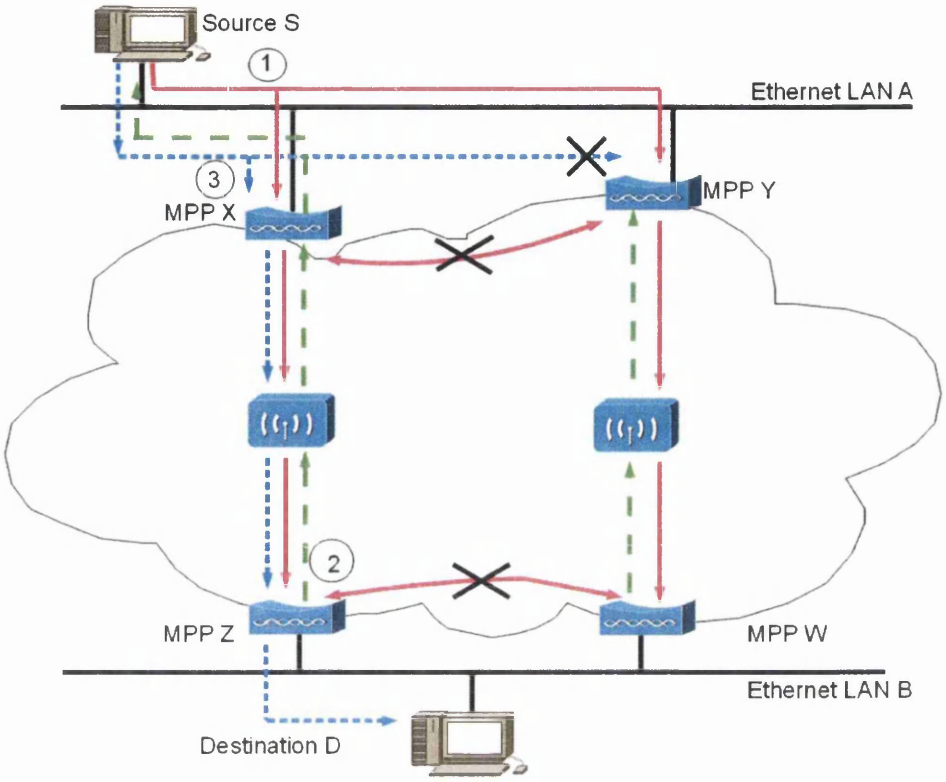

Figure 20: External source and External destination

In this scenario, both the source and destination are connected to wired networks, but they communicate via the wireless mesh network. Figure 20 shows such a scenario involving multiple portals on each wired LAN segment. To establish communication between the source S and destination D, the following steps are taken:

1. The source S sends frames with destination address D to both MPPs X and Y which then broadcast to the mesh network PREQs on behalf of S. Through multihop forwarding, the PREQs reach MPPs Z and W, which are connected to the LAN segment where the destination D is attached. It is noted that Z and W will receive PREQs with the same source and destination address from both X and Y.

2. MPPs Z and W independently select MPPs X and Y as their proxies with regard to S, respectively, and unicast PREPs to them. This triggers IPC procedures, which, based on the fact that there are two possible mesh paths between S (i.e., LAN A) and D (i.e., LAN B), select the best path – the one between MPPs X and Z in this example – and inform all MPPs of this selection.
3. The source S starts sending unicast frames to the destination D, which are received by both MPPs X and Y, but MPP Y discards the frames as it has learned from the IPC that MPP X is a proxy for S. Similar procedures will take place when MPP W receives data frames from the destination D.

3.4 Summary

Chapter 3 has presented scalable interworking in WLAN mesh networks, starting with a discussion of layer-2 path selection and forwarding followed by an insight into WLAN mesh interworking with bridged LANs (which run the spanning tree protocol) problem. Previous related works that were discussed consisted of different approaches to allow multiple portals in WLAN mesh networks. These include multiple MPPs with a logical separation of WLAN mesh; a solution which emphasises on portal roles in such a way that all portals can't work simultaneously and other solutions based on mesh network subdivisions.

This research work has proposed and discussed a novel scheme for multiple portal support in IEEE 802.11s WLAN mesh interworking with external LANs, where problems of broadcast loops and load balancing exist. To overcome those problems, the research suggested a frame filtering process at MPPs which is based on new portal and LAN segment identifications introduced in the mesh header and the PANN element, respectively. This filtering process can detect and discard frames that have already been forwarded by an MPP on the same LAN segment, thus avoiding looping but ensuring the use of multiple MPPs on the same LAN segment. Through several interworking scenarios, it was shown that the frame filtering process, together with interportal communication procedures, can efficiently enable multiple MPPs in interworking with external LANs. This can improve the network reliability and overall performance.

Chapter IV

WLAN Mesh experimentation

4 WLAN Mesh experimentation

4.1 Experimental setup

For the study of WLAN Mesh networks, this research implemented a network simulation model consisting of MPs, MPPs, Ethernet switch and Ethernet stations using OPNET Modeler 15.0 [14].

A network simulation software (OPNET) was run on a standard Personal computer with the following specifications:

1. Operating system: Microsoft Windows XP Professional SP3 (Version 2002)
2. Compiler Environment: Microsoft Visual C++ 2008 Express Edition
3. Hardware: Samsung X22 laptop with
    1. Intel® Core™ 2 Duo CPU
    2. T8100 @2.10Ghz
    3. 795 Mhz, 2.00 GB of RAM

OPNET (Optimized Network Engineering Tools) Modeler is a modeling and simulation tool for communication networks and distributed systems. It provides a development environment of a full protocol stack from the Physical layer protocols through the application layer. The wireless module allows modeling of various aspects of wireless transmissions, such as the physical characteristics (modulation technology), data rates, transmit power, channel settings (bandwidth, min frequency) as well as specific protocols of wireless networks.

OPNET is based on a Discrete Event Simulation (DES) concept. A system model is described by a sequence of instantiated events which make changes in states of the system. This is characterized by finite state machines associated with a set of processes making the whole system. Events are managed in an event list in order to maintain the correct order of

their execution. The simulation environment takes the model through a succession of events for a period of time (simulation time) to replicate the behaviour of a real system.

Object orientation and flexibility for custom model development are some of the key features of OPNET. It also provides graphical specification, Application programming interface (API) and automatic generation of simulations.

OPNET has built-in network models which cover a wide range of communication protocols such as TCP/IP suite of protocols and protocols for specific types of networks. For instance, the OPNET Modeler v15.0 supports IEEE802.11a/b/g and the following MANET routing protocols:

- AODV
- Dynamic Source Routing (DSR)
- Optimized Link State Routing (OLSR)
- Temporarily Ordered Routing Algorithm(TORA)

Because the current version does not support IEEE 802.11s, however, this research carried out modifications on existing models to meet the requirements (Details will be given in section 4.1.1).

Custom models can be created using available editors such as the *Project editor, Node editor, Process editor, External system editor, Link model editor, Packet format editor, Interface Control Information editor* and a *Probability density function (PDF) editor.* Moreover, with OPNET support for C and C++ programming languages, more flexibility is given to make necessary changes in function blocks at the node model level.

Each network node has a set of attributes which are used to define its operation. The attribute parameters can be given individually to every node

or the same attributes could be used on a number of nodes in the model. Below, is an example of a WLAN attributes' set.

Attribute	Value
Wireless LAN	
Wireless LAN MAC Address (IF5 P0)	Auto Assigned
Wireless LAN Parameters (IF5 P0)	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	OFDM (802.11a)
Data Rate (bps)	54 Mbps
Channel Settings	(...)
Bandwidth (MHz)	Physical Technology Dependent
Min Frequency (MHz)	BSS Based
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000

Figure 21: Example WLAN attributes

As part of the node attributes, there is also a possibility to define the network traffic either through application definitions, packet generation settings or load demands. A set of predefined applications, such as FTP, HTTP, VoIP, can be given to a group of users (defined under a *Profile*) in order to carry out Performance evaluation of the model.

For the simulation purposes, raw packet generators were implemented across the network whereby traffic generation parameters and source–destination pairs were defined accordingly. Details of the simulation parameters are given in section 4.1.2 below.

Table 1 and Table 2 [5] provide a list of some of standard model library protocols and technologies across different layers of OSI (Open System Interconnection) model provided by OPNET.

Layer-1, -2 and Support	Layer-3 and Support	Layer-4	Application
ATM	ATM	TCP	FTP
Ethernet 10, 100, 1000	Frame Relay	UDP	E-Mail
ARP	IP	NCP	HTTP
Frame Relay	RSVP		Voice
FDDI	OSPF		Video
Token Ring 4, 16	RIP		Database
PPP	BGP4		Printing
SLIP	IGRP		Remote Login
SRP	EIGRP		Customized Multi-tier
Spanning Tree	IS-IS		General Background Traffic
ATM LANE	X.25		
X.25 (LAPB)			

Table 1: Standard model library protocols and technologies

[5] OPNET Modeler 15.0 Product Documentation

MPLS (Multi-Protocol Label Switching)
UMTS (Universal Mobile Telecom System)
DOCSIS (Data Over Cable System Interface Specification
PNNI (Private Network-Network Interface)
IP Multicasting
Circuit Switching
Advanced Servers
IP Version 6

Table 2: Specialized model Library Protocols and Technologies

OPNET Modeler provides an option for changing the predefined node models as well as the attributes. This is achieved by exploring through the node model as shown below:

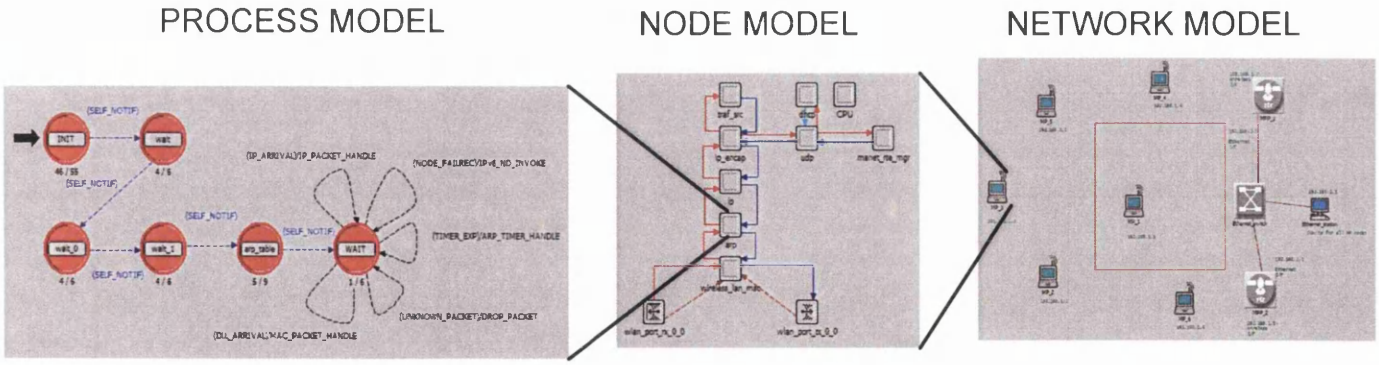

Figure 22: Inside a network model

At the process model level, a user can open the "Function block" in order to access the program code behind the operation of the process model. At this point, all necessary changes can be made in the source code. It is noted that

some of the required program files are not directly accessed in this way, but they are located in OPNET software folder. For example, header files are located under /models/std/include folder.

The following figure shows a snapshot of the code for data traffic generation in our simulation model:

```
static void
manet_rpg_generate_packet (void)
    {
    int             row_num;
    double          schedule_time;
    double          pksize;
    double          next_pkt_interarrival;
    Packet*         pkt_ptr;
    InetT_Address   src_address;
    InetT_Address*  src_addr_ptr;
    InetT_Address*  copy_address_ptr;
    double    tf_scaling_factor = 1;


    /** A packet needs to be generated for a particular flow    **/
    /** Generate the packet of an appropriate size and send it  **/
    /** to IP. Also schedule an event for the next packet       **/
    /** generation time for this flow.                          **/
    FIN (manet_rpg_generate_packet (void));

    /* Identify the right packet flow using the interrupt code  */
    row_num = op_intrpt_code ();

    /* If no destination was found, exit                        */
    if (manet_flow_info_array [row_num].dest_address_ptr == OPC_NIL)
        FOUT;

    /* Schedule a self interrupt for the next packet generation */
    /* time. The netx packet generation time will be the current*/
    /* time + the packet inter-arrival time. The interrupt code */
    /* will be the row number.                                  */
    tf_scaling_factor = Oms_Sim_Attr_Traffic_Scaling_Get ();
    next_pkt_interarrival = (oms_dist_nonnegative_outcome (manet_flow_info_array [row_num].pkt_interarrival_dist_ptr)) / (tf_scaling_factor);
    schedule_time = op_sim_time () + next_pkt_interarrival;

    /* Schedule the next inter-arrival if it is less than the   */
    /* stop time for the flow                                   */
    if ((manet_flow_info_array [row_num].stop_time == -1.0) ||
        (schedule_time < manet_flow_info_array [row_num].stop_time))
        {
        op_intrpt_schedule_self (op_sim_time () + next_pkt_interarrival, row_num);
        }

    /* Create an unformatted packet */
    pksize = (double) ceil (oms_dist_outcome (manet_flow_info_array [row_num].pkt_size_dist_ptr));

    /* Size of the packet must be a multiple of 8. The extra bits will not be modeled       */
    pksize = pksize - fmod (pksize, 8.0);

    pkt_ptr = op_pk_create (pksize);

    /* Update the packet sent statistics    */
    manet_rpg_sent_stats_update (pksize);
```

Figure 23: Extract from a node model function block

After the simulation model is completed, a simulation run has to be launched through a graphical user interface which provides control to the simulation set in terms of simulation duration, seed for statistical processes as well as the number of runs that needs to be done depending on input parameter variations. An example configuration of a DES is given in Figure 24.

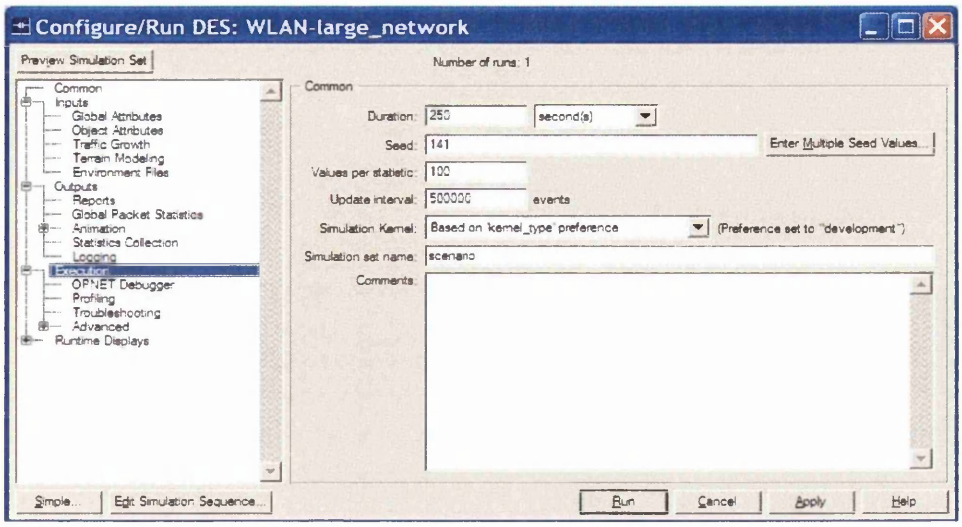

Figure 24: DES Configuration/ Run

With the WLAN Mesh model, steady-state conditions of the network were simulated with raw packet generators co-located with mesh points and Ethernet node. On the other hand, transient conditions of interest can be studied as well like shown in Figure 25.

In addition to doing multiple runs with different simulation inputs, this research have also simulated the network model using various scenarios, for instance with a single operational MPP in the network and other scenarios with two MPPs being operational at the same time. Furthermore, other scenarios were considered with the mesh nodes being kept at different locations. The following paragraph discusses how simulation results were collected in order to carry out objective analysis based on comparisons of obtained results in different scenarios and by varying input parameters.

The simulation platform offers two major types of statistics:

- Global Statistics and
- Node Statistics

The global statistics are those obtained by combining data collected from many nodes in a network model. Although the global statistics are based upon node statistics, some of the former can't be obtained in the latter case given that they involve multiple nodes. Besides standard network performance analysis data such as data dropped/buffer overflow, data dropped/retry threshold exceeded, end-to-end delay, traffic load, media access delay, retransmission attempts (packets), throughput (bits/sec), control traffic received and control traffic sent, there is also a possibility to create custom probes to collect particular statistical data.

Generally, a system performance is measured by collection of statistical data of interest — e.g., data dropped (bits/sec), Media Access delay (sec), Retransmission Attempts (packets), throughput (bits/sec) — either as scalars or vector values. Then, the output is presented as a graph, animation or a spreadsheet with details of collected data.

Figure 25 represents a plot of Data Traffic received at 3 different mesh nodes from this research's simulation network model.

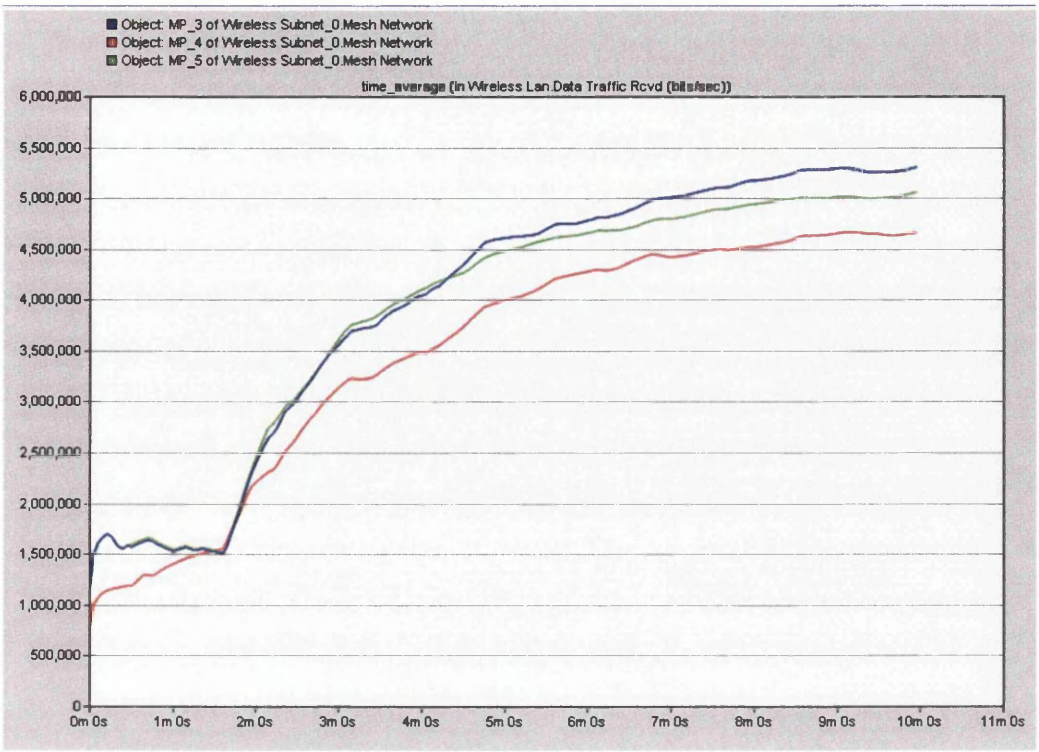

Figure 25: Data traffic received

In this research's simulations, standard statistics were collected and the corresponding graphs were plotted to express the network performance with regards to end-to-end delay, WLAN Media access delay, and data delivery ratio among others

Network performance analysis was carried out based on simulation traces obtained from scenarios with a single MPP in operation versus scenarios where two MPPs were connected to the same Ethernet segment. In order to increase the confidence of simulation results, multiple simulation runs were considered with various constant data bit rates for each source destination pair.

4.1.1 WLAN mesh nodes emulation

Considering the complex architecture of mesh nodes as proposed by the IEEE802.11s draft standard and their similarities with IETF MANET [6] nodes, necessary modifications were done on IETF MANET nodes to emulate WLAN mesh nodes.

It is in this regard that the IEEE802.11a MAC layer was reused to provide data link layer functionalities whereas path selection and forwarding in mesh network was achieved using AODV (Ad Hoc on Demand Distance Vector routing). It is noted that the default path selection and forwarding protocol for WLAN Mesh in the draft standard was inspired by AODV to provide reactive routing functions [10]. On the other hand, there would be a need for adaptation of AODV to handle MAC address-based path selection and link metric awareness - which is beyond the scope of this work – in order to be able to forward data to and from Ethernet segment. Thus, OSPF (Open Shortest Path First) [7] was adopted for non-Mesh side of MPPs.

With an ad hoc distance vector path selection and forwarding protocol running within the mesh network and a link state routing protocol over the Ethernet segment, two portals (gateway) were introduced to bridge both networks by providing routing table exchange functionalities and load balancing. Optimization of network resources is achieved by enabling the load balancing features which distribute traffic over multiple paths while transferring data to a destination. Packet based load balancing was used in our simulation model with the Mesh points sending successive datagrams over alternate paths following a round robin fashion. It is noted that with this load balancing in place, the user sessions/hosts are disregarded.

4.1.2 Simulation setup parameters

Figure 26 depicts a mesh network simulation model that was used. All MPs (MP_1 to MP_6) have similar configuration parameters and MPPs (MPP_1 & MPP_2) have another set of parameters to cater for both networks (wireless and Ethernet). Furthermore, we have configured an Ethernet station and a switch for the Ethernet segment.

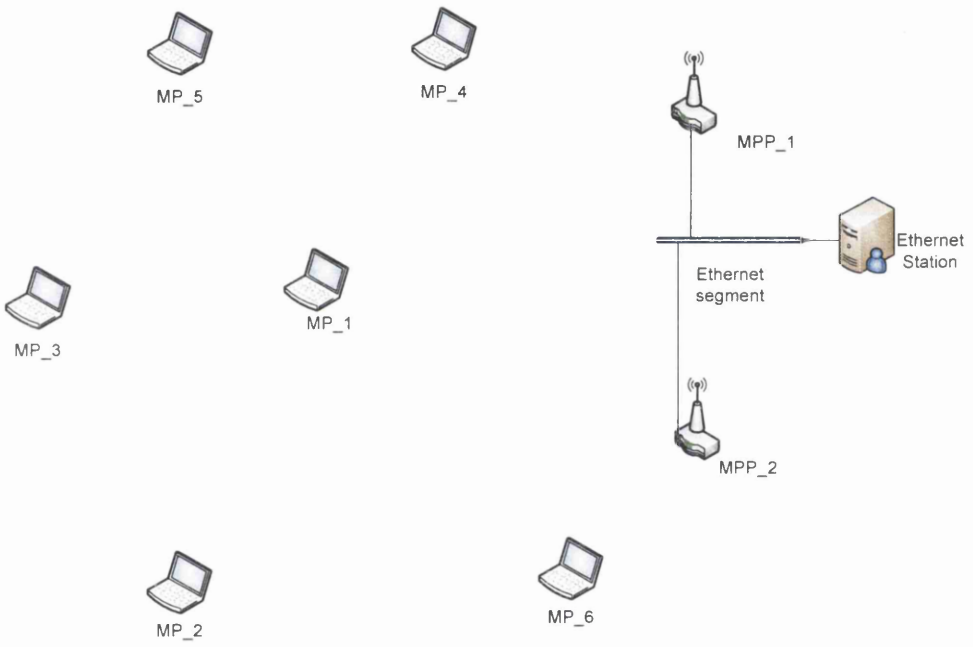

Figure 26: WLAN Mesh Network Simulation Model

4.1.3 MP node parameters

Every MP in this setting has three main parameter sets of interest:

- Path selection and forwarding parameters
- WLAN MAC settings
- Packet generation parameters

An MP node model in Figure 27 shows details of building processors necessary for packet generation and data transmission/ reception by this node. In this model, two building processors (dhcp and CPU) were not configured as their functions won't have any impact on the outcome of our simulation in this setting.

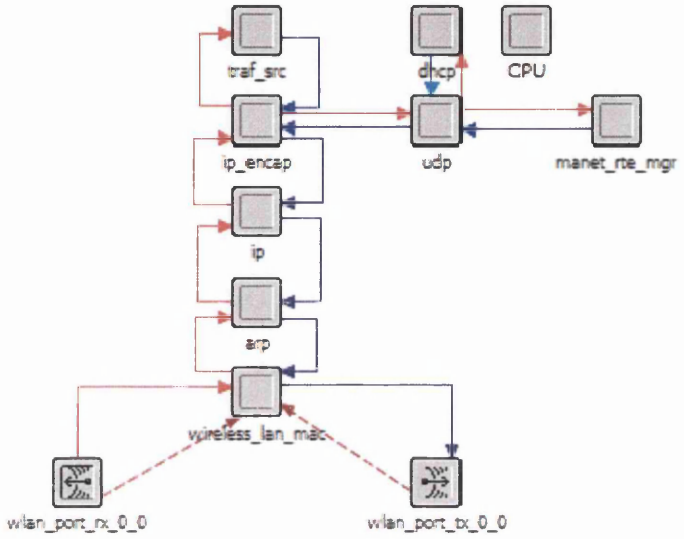

Figure 27: Mesh point node model[6]

- ***Path Selection and forwarding*** :

Attributes	**Value**
Path selection and forwarding protocol	AODV
Route request retries	5
Route request rate limit (pkts/sec)	10
Active route timeout (sec)	3
Hello interval (sec)	Uniform (1, 1.1)
Allowed Hello loss	2
Network diameter	35
Node traversal time (sec)	0.04
Route Error Rate Limit (pkts/sec)	10

[6] This is based on manet_station_adv node model from OPNET 15.0

Timeout Buffer	2
TTL Start	1
TTL Increment	2
TTL Threshold	7
Local Add TTL	2
Packet queue size (packets)	Infinity
Local Repair	Enabled
Addressing mode	IPv4

Table 3: Path selection and forwarding settings

- ***WLAN MAC settings:***

Attribute	**Value**
MAC address	Auto assigned
BSS Identifier	Auto assigned
Physical layer characteristics	OFDM (IEEE 802.11a)
Data rate	54Mbps
Transmit power (mW)	5
RTS Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short retry limit	7
Long retry limit	4
AP Beacon interval (sec)	0.02
Max ReceiveLifetime (sec)	0.5
Buffer size (bits)	56000000
Roaming Capability	Disabled
Large Packet processing	Drop
PCF Functionality	Disabled

HCF Parameters	EDCA Parameters	Access category parameters	Voice	CWmin	(PHY CWmin+1)/4 -1
				CWmax	(PHY CWmin+1)/2 -1
				AIFSN	2
				TXOP Limits	1504
			Video	CWmin	(PHY CWmin+1)/2 -1
				CWmax	PHY CWmin
				AIFSN	2
				TXOP Limits	3008
			Best effort	CWmin	PHY CWmin
				CWmax	PHY CWmax
				AIFSN	2
				TXOP Limits	One MSDU

Table 4 : WLAN MAC Parameters

- ***Packet generation parameters***

The network model shown in figure 24 comprises of 12 traffic sources. There is one packet generator in each MP and 6 packet generators in Ethernet_node in order to establish 6 source-destination pairs in both directions (ingress and egress).

All traffic sources generate 64 bytes long packets.

Simulations were carried out with data rates from 64 Kbps to 192 Kbps per traffic source with a step size of 32 Kbps. By studying the network behaviour with data rates of 64Kbps to 192Kbps we have managed to cover a wide range of user traffic observed on a public wireless LAN [1], in which the users' workload was classified as "medium session" with peak data rates between 60Kbps and 175Kbps

- Traffic generation parameters:
  - Constant bit rate traffic with:
    - Packet size: 64 bytes. The simulation program is designed in such a way that an unformatted packet of appropriate size (a multiple of 8) is generated and sent to IP layer which then encapsulates the packet and send it to data link layer. This being said, the payload of data link layer frame will be equal to multiples of 64 bytes plus network layer header size.
  - We have carried out 5 simulation runs with different interarrival times which follow a constant distribution as given below:

Run number	Inter-arrival time(sec)	Packet size (Bytes)	Data bit rate(Kbps) per mesh node
1	0.008	64	64
2	0.00534	64	96
3	0.004	64	128
4	0.00267	64	160
5	0.002	64	192

Table 5: Traffic generation parameters at MP

4.1.4 MPP node parameters

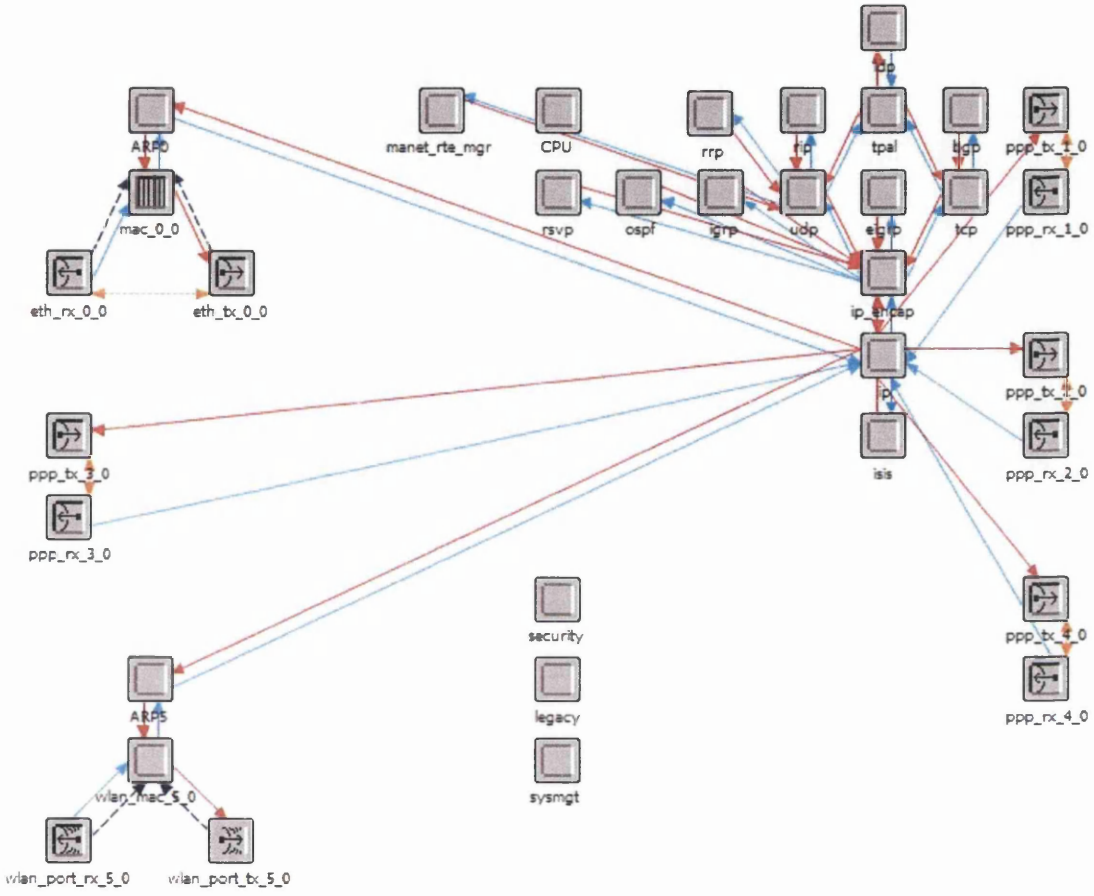

Figure 28: MPP[7]

Path selection and forwarding protocols:

- AODV: Same parameters as the wireless stations (MPs in this case). AODV is implemented at the wireless interface which is connected to the mesh network. MPs were set on the same IP network with the wireless interface of the MPP.

[7] This is based on manet_gateway_wlan_ethernet_slip4_adv node model from OPNET 15.0

- OSPF: This protocol is running on non-mesh interface of the MPP in order to allow reachability to non-mesh interfaces. Paths to the MPs are advertised to the non-mesh network by redistribution of routing table from AODV to the IP routing protocol (OSPF) of the non-mesh interface.

OSPF parameters:

S. no.	Parameter		Value
1	MTU (Maximum transfer unit)		Ethernet
2	Metric information	Bandwidth(Kbps)	Link bandwidth
		Delay	10microsec
		Reliability	255
		Load	255
3	Load balancing		Packet based
4	Administrative weight		110
5	SPF Calculation	Style	LSA Driven
		Delay(seconds)	5
		Hold time (seconds)	10

Table 6: MPP OSPF Parameters

Ethernet node:

The Ethernet node in our simulation model is a modification of legacy IEEE802.3 station which supports 10/100Mbps. This node has 6 traffic sources, each having for destination one of the MPs.

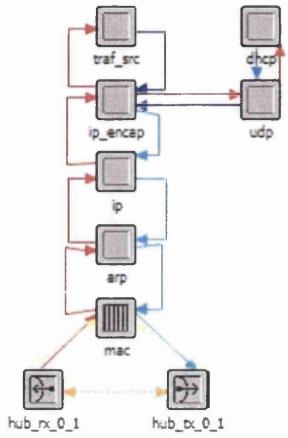

Figure 29: Ethernet node model[8]

4.1.5 Simulation scenarios

Two different scenarios were studied, 5 times each with varying data bit rate. With reference to figure 24, the first five runs were done with both MPP_1 and MPP_2 in operation. The remaining 5 runs were done with only one operational portal, MPP_1.

[8] This is based on ethernet_ip_station_adv node model from OPNET 15.0

4.2 Experimental results

4.2.1 End-to-end delay

The end-to-end delay in milliseconds given in Figure 30, shows the time elapsed from the generation of a packet (unformatted packet in this case) at the source node until destruction of the packet at destination node.

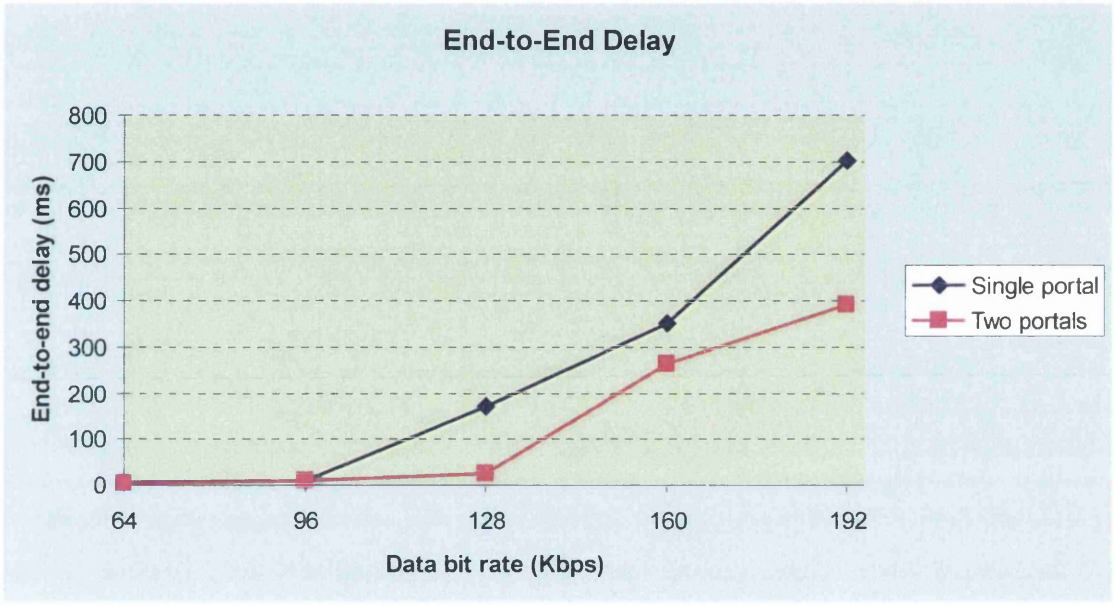

Figure 30 : End-to-end delay

The above graph is plotted from statistics collected at Wireless node (MP_2) as a destination and Ethernet station as the source node.

The average end-to-end delay increases with increase in data bit rate per node in both cases (single portal and two portals). This is due to the fact that there is a more buffering as the traffic load increases as a result of higher bit rates. From the figure, it is observed that at lower bit rates (64 Kbps and 96Kbps) there is not much difference in end-to-end delay whether two portals were used or not. In fact at this level of traffic load, packets can be sent in both scenarios without significant queuing delay. On the other

hand, as the traffic load increases, there will be more buffering and queuing if only one portal is in use, thus creating a bottleneck at the portal. With two portals in the network, the load balancing mechanisms share the load between the two, hence reducing queuing delays.

Furthermore, at 192Kbps, the performance difference between the two scenarios becomes more significant. Thus, in all cases, multiple portals should be used in order to keep the end-to-end delay at minimum.

4.2.2 Data packet delivery ratio

Data Packet delivery ratio: This is the ratio between the number of received and sent packets. It shows the percentage of packet delivered, which is a very good indication for network performance.

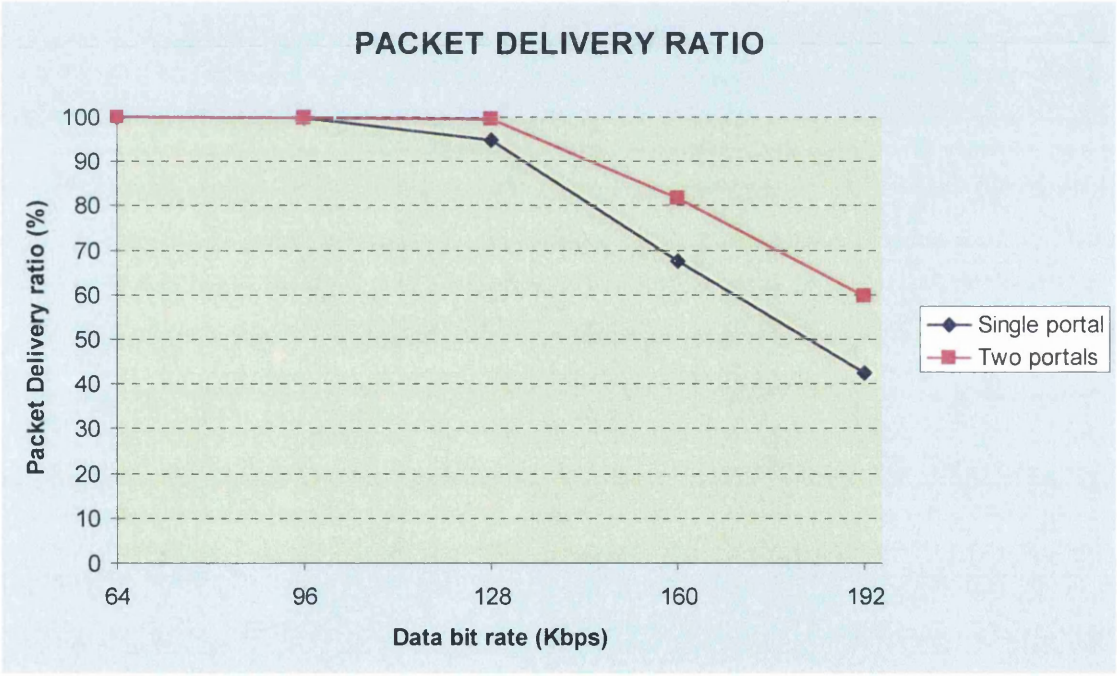

Figure 31: Data packet delivery ratio

Figure 31 shows a plot of the data packet delivery ratio versus data bit rate per node. It was observed that up to 128Kbps bit rates, in both the scenarios (single portal and two portals) the ratio is above 90%, which is good for most applications. However, above 128Kbps, the performance greatly

deteriorates with a single portal, and packet losses increase above 50% at 192 Kbps. If there was to be a transport layer protocol such as UDP, the network would be unusable. Having two portals provides an improvement of more than 10% at higher bit rates, starting with 160Kbps. The above graph clearly suggests that a network with a single portal would not be usable for real time applications that require higher data bit rates such as high definition videoconference. With videoconference, packet losses as little as 2% can visibly affect picture quality; thus with losses of up to 50% there can't be any effective communications.

4.2.3 Wireless LAN Media access delay

The Wireless local area network media access delay, called "delay" hereafter, is the total of queuing delay plus the contention delay of all frames transmitted by the WLAN MAC. This includes data frames, management frames, delayed Block-ACK and Block-ACK Request frames. Block ACK (block acknowledgement) mechanism improves channel efficiency in such a way that a several acknowledgements are aggregated into one frame [24].

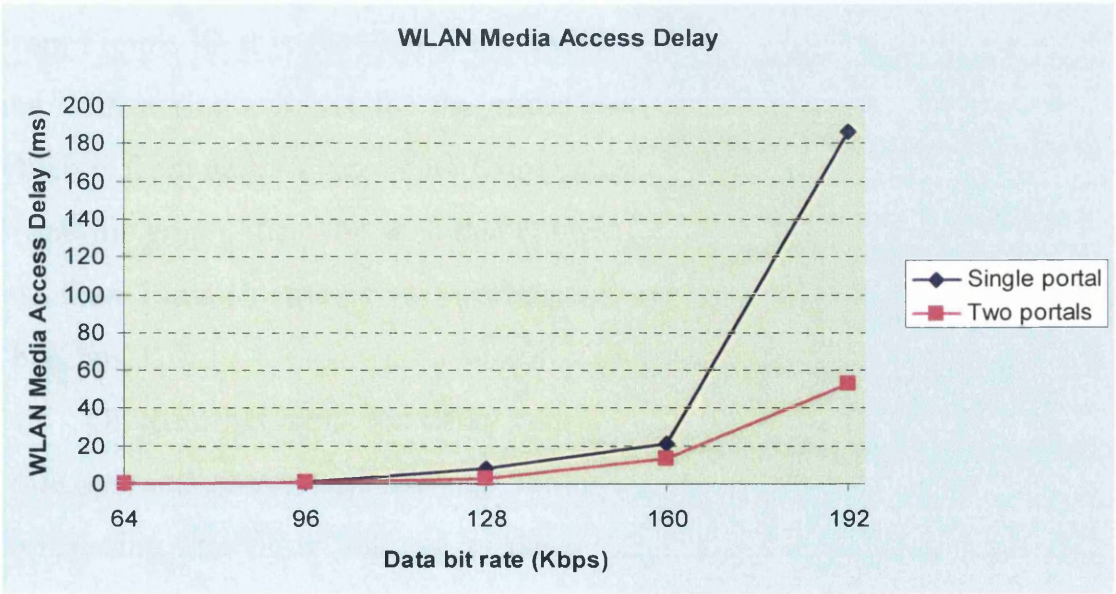

Figure 32: WLAN Media access delay

In this simulation environment, the delay for each frame is calculated based on the insertion time of the frame into the transmission queue and the time when the frame is sent to the physical layer for the first time. Given that there are different sources of frames, the insertion time is the arrival time for higher layer packets such as the generated raw packets whereas it is the creation time for other frames such as the Block acknowledgement frames. The delay will also include the elapsed time during RTS/CTS exchange that may take place before the frame transmission. It is noted that RTS/CTS (Request to send and clear to send) frames are control frames used in IEEE802.11 to reduce collisions. The mechanism consists of sending a RTS frame by the node wishing to start transmission and a CTS frame that is sent from the receiving node (recipient) when it is ready to accept transmission. If any other nodes receive either a RTS or CTS they should refrain from sending data for a period equal to the waiting time given in RTS/CTS frames before trying to have access to the medium.

The delay also takes consideration of *backoff* periods that may be triggered by collision(s) before initial frame transmission.

From Figure 30, it is shown that a network with two portals outperforms the one with a single portal for the entire range of data traffic in our study, which is from data bit rate of 64 Kbps up to 192 Kbps.

From this graph, it can be seen that contention and queuing at MAC layer is less than 15ms in case of two portals being in use for data bit rates up to 160Kbps.

On the other hand, the delay with single portal sharply increases from 160Kbps and above approaching 200ms delay. This value is very high considering that other sources of delay (at different protocol layers) will also contribute to the total end-to end delay, thus going well beyond the 150ms recommended maximum one-way delay for VoIP [27] which uses

Real time transport protocol(RTP). This figure proves the need for multiple portals for WLAN mesh interworking with non-mesh networks because most of such mentioned applications are likely to involve more than one type of network.

4.3 Summary

The aim of chapter 4 was to describe the experimental work and present the results along with corresponding interpretations. Using OPNET simulation tool, a WLAN mesh network model was designed and appropriate simulation setup parameters were chosen in order to carry out performance analysis studies.

This research work considered the following performance parameters:

1. End-to-end delay
2. Packet delivery ratio
3. Wireless LAN media access delay

The *end-to-end delay*, which is a time elapsed from packet generation at the source node until the packet destruction at the destination node (sink), was found to be increasing in relation to increments in data bit rates. The results graphs indicated a significant improvement of the end-to-end delay in scenarios with multiple portals when compared to scenarios with a single portal. On the other hand, the *data packet delivery ratio,* which is the ratio of the number of received packets at the sink to the number of sent packets from the source, was found to be decreasing as the data bit rate increases. Furthermore, this ratio decreases considerably at higher data bit rates in such a way that if only one portal was functional in the WLAN mesh network, the network would be impractical for sensitive applications such as real time communications. In addition to the first two performance parameters, this research has shown that the *Wireless LAN Media Access Delay* which represents the total of queuing delay together with the contention delay of all frames transmitted by the WLAN MAC, increases sharply from data bit rates of 160 Kbps and above in case of a single operational portal. This proves the necessity of multiple portals for WLAN mesh to efficiently interwork with non-mesh networks.

Chapter V

Conclusion

5 Conclusion

This research work has investigated a particular subset of wireless mesh networks which is the WLAN Mesh currently being studied under the IEEE802.11s Task group.

With the standardization of these networks being a work in progress, there is still more to be done to ensure compatibility among equipments from different vendors and for the network to be deployed on a large scale. Network scalability and extensibility remain a problem with existing path selection and forwarding protocols, given limitations on the number of STAs that can be supported in a WLAN Mesh network. There is a limited capacity for MAP, MP and MPP to support associated STAs in order to effectively perform intra-mesh frame forwarding and another problem arises for frame transfers between mesh nodes and external networks. The existing interworking framework allows only a single MPP to work as a proxy for mesh nodes.

A new framework to enable multiple portals in IEEE 802.11s WLAN mesh interworking with external LANs was proposed and discussed. The proposed interworking framework addresses the issues of broadcast loops and load balancing by a frame filtering process at MPPs which is based on new portal and LAN segment identifications introduced in the mesh header and the PANN information element, respectively.

The frame filtering process can detect those frames that have already been forwarded by an MPP on the same LAN segment and then discard them, thus avoiding the formation of broadcast loops while ensuring the use of multiple MPPs on the same LAN segment. There was also provision of procedures for network topology/LAN segment identification and inter-portal communication to complete the proposed interworking framework. Through several interworking scenarios, we have shown that the proposed

frame filtering process, together with IPC procedures, can efficiently enable multiple MPPs in interworking with external LANs while avoiding duplicate unicasting and broadcasting.

By using multiple MPPs, the mesh network load can be shared among those portals, thus improving the network performance and reliability.

A simulation model of a WLAN Mesh network was developed with OPNET based on existing MANET models in order to analyze network performance where simulations scenarios consisted of variations in data traffic generation and the number of operational mesh portals. Simulation results have shown that multiple portals are a requirement for real time protocols to be supported in mesh networks. Although light applications such as HTTP or FTP could be supported with a single portal at low data bit rate (up to 128Kbps), the amount of packet losses becomes critical as the bit rate increases.

Simulation scenarios with two portals have shown superior performance in terms of end-to-end delay, WLAN media access delay and data packet delivery ratio.

In order to disseminate and exploit the research findings, part of this work has been published in proceedings of the Second IEEE International Workshop on Enabling Technologies and Standards for Wireless Mesh Networking (MeshTech'08), Atlanta, USA. Other parts were submitted to ACM/Springer Mobile Networks and Applications (MONET) Special Issue on "Recent Advances in IEEE 802.11 WLANs". Furthermore, a patent application was submitted for this research's invention through the University of Wales Swansea (UWS) Ventures.

Future work will focus on development of a simulation model for WLAN mesh on a platform that runs HWMP path selection and forwarding at layer 2 along with the following IEEE802.11s functionalities:

- Multihop action that supports 6-address scheme
- Interworking with multiple portals involving more than one Ethernet segment

After network performance evaluation by simulation, mathematical analysis will be carried out for scheme validation.

References

References

[1] A. Balachandran, G. M. Voelker, P. Bahl and P.V. Rangan. *"Characterizing user behavior and network performance in a public wireless LAN"*, volume 30, pages 195 – 205. ACM SIGMETRICS Performance Evaluation Review, June 2002.

[2] A. O. Lim, Y. Kado, K.S. Kim, Y. Liu, M. Nozaki, K. Mase, H. Okada, M. Takai, X. Wang, B. Zhang. "*Scalable Station Association Information Handling*". doc: IEEE 802.11-07/0176r0, January 2007.

[3] M. Bahr. *"Proposed Routing for IEEE 802.11s WLAN Mesh Networks"*. In *"Proceedings of 2nd annual international workshop on Wireless Internet"*, Boston, Massachusetts, August 2006.

[4] E. Belding-Royer. C. Perkins, S. Das. *"Ad hoc On Demand Distance Vector (AODV) Routing Protocol"*. www.ietf.org/rfc/rfc3561.txt, July 2003.

[5] Kyeong-Soo Kim et al. *"Joint SEE-Mesh/Wi-Mesh Proposal to 802.11 TGs"*. doc.: IEEE 802.11-06/0328r0, February 2006.

[6] IETF Mobile Ad Hoc Work Group. http://www.ietf.org/html.charters/manet-charter.html, 2010.

[7] The Internet Society Network Working Group. "RFC 2328: OSPF2". http://www.ietf.org/rfc/rfc2328.txt, April 1998.

[8] I. F. Akyildiz, W. Wang, X. Wang. *"Wireless mesh networks: a survey"*. In *Computer Networks*, volume 47, page 445–487, 2007.

[9] IEEE 802.11 Working Group of the LAN/MAN Committee. *IEEE P802.11s™/D1.06, Draft Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer*

(PHY) specifications - Amendment: Mesh Networking. IEEE, July 2007.

[10] IEEE 802.11 Working Group of the LAN/MAN Committee. *IEEE P802.11s™/D2.0, Draft Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment: Mesh Networking*. IEEE, March 2008.

[11] IEEE Computer Society. *IEEE Std 802.1D™-2004, IEEE Standard for local and metropolitan area networks: Media access control (MAC) bridges*. IEEE, June 2004.

[12] IEEE Computer Society. IEEE standard for local and metropolitan area networks – specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, June 2007.

[13] IEEE Task Group TGs. *"Project Authorization Request (PAR) for IEEE 802.11s"*. Doc. no. IEEE 802.11-03/759r22, 2003.

[14] OPNET Technologies Inc. http://www.opnet.com/, 2009.

[15] J. Costa-Requena, T. Vadar, R. Kantola and N. Beijar. *"AODV-OLSR Scalable Ad hoc Routing Proposal"*. In Proceedings of the 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand, January 2006.

[16] K.S.(Joseph) Kim. *"Hybrid proactive On-demand Routing in Wireless Networks"*. ST Microelectronics, November 2006.

[17] M. S. Kim. *"Multiple mesh portal support in the WLAN mesh"*. Internal contribution to SEE-Mesh proposal for IEEE 802.11s, June 2005.

[18] Yonggyu Kim, Yeonkwon Jeong, and Joongsoo Ma. *"Interworking with multi portals in wireless mesh network"*. IEEE 802.11-06/1678r1, November 2006.

[19] J. Kruys. *"IEEE 802.11s Tutorial, Part 2: Security and Routing"*. http://ieee802.org/802_tutorials/nov06/802.11s_Tutorial_r5.pdf, Nov 2006.

[20] L. Chu, K. S. Kim, J. Kruys, S. Rahman, G. Vlantis. *"Extension to 6-address scheme for TGs mesh"*. IEEE 802.11-06/0841r5, Sept 2007.

[21] M. Benzaid, P. Minet, K. Al Agha. *"Integrating Fast Mobility in the OLSR routing Protocol"*. In *The 4th IEEE Conference on Mobile and Wireless Communications Networks(MWCN 2002)*, Stockholm, Sweden, September 2002.

[22] M. Benzaid, P. Minet, K. Al Agha. *"Analysis and simulation of fast-OLSR"*. In *Vehicular Technology Conference (VTC)*, volume 3, pp. 445–487, Apr 2003.

[23] J. Kruys, S. Rahman and M. S. Kim. *"Efficient interworking support in 802.11s mesh networks (version 2.0)"*. Internal contribution to SEE-Mesh proposal for IEEE 802.11s, Oct 2005.

[24] IEEE Computer Society. IEEE Std 802.11e™-2005 :IEEE standard for information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements: Part 11: Wireless LAN medium access control(MAC) and physical layer (PHY) specifications amendment 8: Medium access control (MAC) quality of service enhancements., September 2005.

[25] Guenael Strutt and Jan Kruys. *"Interworking considerations"*. IEEE 802.11-06/1091r0, June 2006.

[26] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot. *"Optimized Link State Routing"*. http://tools.ietf.org/html/draft-ietf-manet-olsr-07, December 2002.

[27] International Telecommunications Union. Transmission systems and media, digital systems and networks Recommendation G.114 : New Appendix II: Guidance on one-way delay for Voice over IP. http://www.itu.int/rec/T-REC-G.114-200309-P!Amd1, Sept 2003.

[28] X. Wang and A. O. Lim. *" IEEE 802.11s wireless mesh networks: Framework and challenges ". Ad Hoc Networks*, 6(6):970–984, 2008.