Inter-domain Routing for Tactical Mobile Ad-hoc Networks

by

Izegbuwa Okundaye

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs

in partial fulfillment of the requirements for the degree of
Master of Applied Science in Electrical and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering
(OCIECE)

Department of Systems and Computer Engineering

Carleton University

Ottawa, Ontario, Canada, K1S 5B6

January 2013

Your file Votre référence
ISBN: 978-0-494-94262-8

Our file Notre référence
ISBN: 978-0-494-94262-8

The undersigned recommend to
the Faculty of Graduate and Postdoctoral Affairs
acceptance of the thesis

Inter-domain Routing for Tactical Mobile Ad-hoc Networks

submitted by

Izegbuwa Okundaye

in partial fulfillment of the requirements for

the degree of Master of Applied Science in Electrical and Computer Engineering

_____

Chair, Howard Schwartz, Department of Systems and Computer Engineering

_____

Thesis Supervisor, Thomas Kunz

Carleton University
January 2013

Abstract

The purpose of this thesis is to provide a routing solution for a large scale tactical inter-domain network containing multiple Mobile Ad-hoc Networks (MANETs) and fixed networks. The solution proposed in this thesis involved using Open Shortest Path First – MANET Designated Router (OSPF-MDR) and OSPFv3 in the fixed networks. A border gateway routing protocol which actualizes wireless mobility features and routing abilities similar to the Border Gateway Protocol (BGP), named BGP – MANET Routing (BGP-MR), was also proposed. BGP-MR introduces the dynamic election of gateways and recursive purging of routes from the BGP table as BGP peers are lost due to mobility.

The proposed solution is tested to show OSPF's ability to provide convergence in large scale networks. Our results showed that after 20 minutes, networks running OSPF converged. The results demonstrate BGP-MR's ability to provide seamless routing and reduced overhead in interconnecting MANETs, regardless of their partitioning and merging characteristics.

Acknowledgements

It is a pleasure to thank the many people who made this thesis possible.

It is difficult to overstate my gratitude to my Masters supervisor, Prof. Thomas Kunz. With his enthusiasm, his inspiration, and his great efforts to guide me throughout my research and indeed thesis-writing period, he provided, sound advice, needed criticism and lots of good ideas, I would have been lost without him.

I am thankful to Communications Research Centre Canada (CRC) for funding this research and particularly Semra Gulder, Philip Hugg and Jiangxin Hu, for their advice and patience when I had numerous questions, and most especially for providing the resources that made this thesis possible.

I am indebted to my many student colleagues for providing a stimulating environment in which to learn and grow, I am especially grateful to David Fadairo for his time, being my biggest supporter, giving me an ear to bounce ideas off even though a lot of times he was lost to what my exact problem was, I wish to thank my family for providing a loving environment for me, my brother and my sister, who were particularly supportive with encouraging words.

Lastly, and most importantly, I wish to thank my parents, Louie E. Okundaye and Comfort O. Okundaye, they bore me, raised me, supported me, taught me, and loved me. To them I dedicate this thesis.

Table of Contents

List of Tables

List of Figures

List of Acronyms

AN: Airborne Network

AODV: Adhoc On-demand Distance Vector

AS: Autonomous System

BF: Bloom Filter

BGP: Border Gateway Protocol

BGP-MR: Border Gateway Protocol- MANET Routing

BGP-MX Border Gateway Protocol with Mobility eXtensions

BMDR: Backup MANET Designated Router

TCP: Transmission Control Protocol

BR: Border Router

CDS: Connected Dominating Set

CLI: Cross Layer Integration

CORE: Common Open Research Emulator

CR: Composite Routing

CRC: Communications Research Centre

DD: Database Description

DPBS: Distributed Peering Broker Service

DR: Designated Router

EBGP: External Border Gateway Protocol

EGP: Exterior Gateway Protocol

FSM: Finite State Machine

GIG: Global Information Grid

GPL: General Public License

GPS: Global Positioning System

GTNetS: Georgia Tech Network Simulator

GUI: Graphical User Interface

IBGP: Internal Border Gateway Protocol

ICMP: Internet Control Messaging Protocol

IETF: Internet Task Engineering Force

IGP: Interior Gateway Protocol

IMUNE: Integrated Multiprotocol Network Emulator/Simulator

InterMR: Inter-MANET Routing

MANET: Mobile Adhoc Network

MBR: MANET Border Router

NDR: Network Designated Router

OLSR: Optimized Link State Routing

OSPF: Open Shortest Path First

OSPF-MDR: Open Shortest Path First-MANET Designated Router

PDR: Packet Delivery Ratio

RFC: Request For Comments

RIP: Routing Information protocol

LSA: Link State Advertisement

SPF: Shortest Path First

TCL: Tool Command Language

TK: ToolKit

1: Introduction

1.1 Problem Statement

The research discussed here aims to provide a routing solution that will be efficient in a setup where more than one type of network is present:

- Fixed Networks
- Mobile Ad-hoc Networks (MANETs)

Each type of network can be seen as an individual domain, so an inter-domain routing protocol would be required to provide seamless communication between both networks.

The routing solution has to take into consideration:

1) The size of the inter-domain network in terms of a scalable routing protocol that converges.

2) The mobility present in the MANETs that will produce partitioning and merging of networks and might introduce packet losses across the topology.

3) Interconnecting more than one MANETs.

1.2 Motivation

This thesis is motivated by a joint project with Communications Research Centre Canada (CRC) as a way to provide a solution to a real life inter-domain routing problem for tactical networks.

The tactical network introduced by CRC contains fixed and mobile networks and some mobile networks may split or merge overtime.

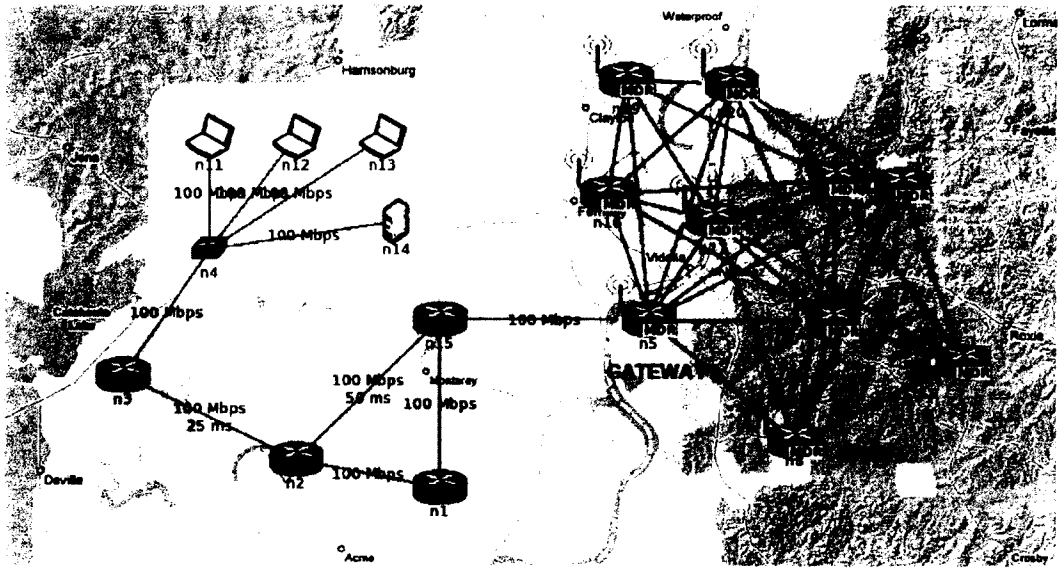

Figure 1.1 Sample Tactical Scenario

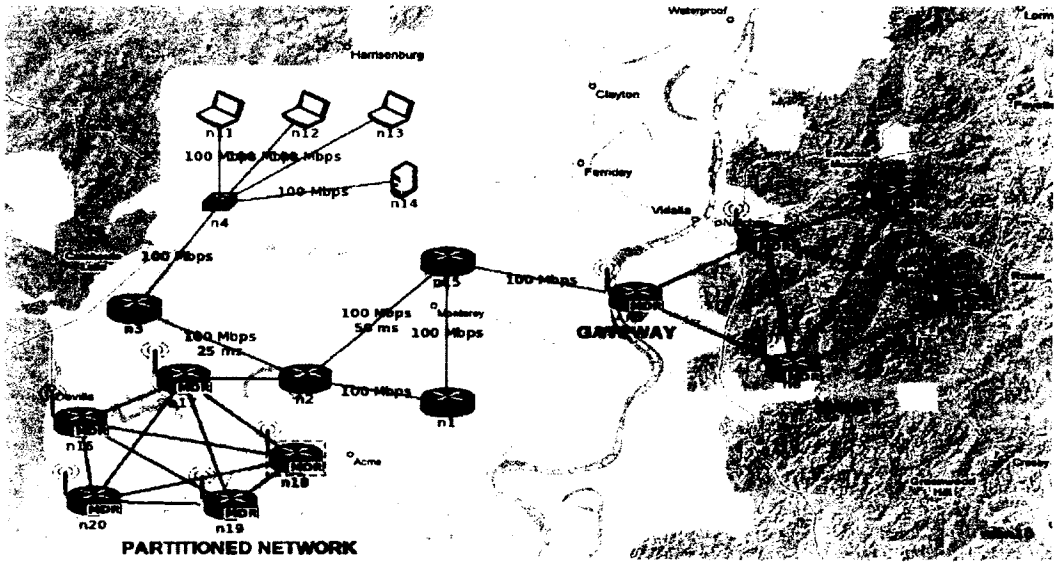

Figure 1.2 Scenario showing Partitioned MANET

Figure 1.1 shows an example of a tactical network with fixed and mobile networks present, while Figure 1.2 depicts how a MANET is capable of partitioning into two or more MANETs. When MANETs split in large networks, the Interior Gateway Protocol (IGP) running with the MANET network does not have valid routes to the partitioned network and hence all the other routers in the network lose connectivity to the partitioned routers causing sub-optimal routing.

The proposed solution should be one that provides optimal connectivity via quick convergence from link breakage and high packet delivery ratio (PDR) between all domains with the least amount of overhead.

CRC have also specified some simulation parameters that have led to the basis of this research. One such parameter is the number of routers available in their tactical network being 200, and hence the simulations used for testing in this thesis will work around using a scenario of 200 routers to represent a large tactical network.

1.3 Contributions

1) We provide evidence to show that OSPF-MDR will converge when used in large tactical MANETs. Hence it is a good solution to inter-domain routing in large networks, since it has variants that can work in both fixed networks and MANETs.

2) We introduce dynamic gateways that handle the partitioning of MANETs caused by the mobility scenarios. Our protocol is a variant of the Border Gateway Protocol (BGP) that has been modified to include characteristics that extend it into a mobile environment.

Our solution to proposing an inter-domain protocol that works seamlessly between a MANET and fixed network is to utilize the Open Shortest Path First (OSPF) routing protocol, implementing OSPF in the fixed network and Open Shortest Path First - MANET Designated Router (OSPF-MDR), a variant that handles mobile networks, in the MANET environment. Dynamic gateways are introduced to monitor the change in the topology caused by router mobility and partitions using a protocol that runs between potential Border Routers (BR) in the MANET. This is based on the idea in [1], which introduces a protocol called Inter-Manet Routing (InterMR) which utilizes sub-protocols *i*-InterMR and *e*-InterMR. These sub-protocols support change detection within a single MANET, by which gateways maintain soft state of the MANET topology via periodic beacons. Failure to receive a beacon indicates a partition. Our idea is to implement this same technique by introducing a gateway protocol into the MANET that handles the detection of partitions within and outside a MANET. We propose modifying BGP which is a well-understood and widely deployed gateway protocol. This provides a strong basis of experience and skills from which to work, hence a protocol that is known to work can be extended, rather than developing a new protocol that must then be completely troubleshot, tested, and modified over a number of years. Working with a well-known protocol allows development effort to be placed in a narrowly focused area, rather than rebuilding from scratch many things that are already known to work.

1.4 Thesis Overview

Chapter 2 will discuss the relevant literature that has been reviewed during the course of this thesis; it contains work done by other researchers as it relates to this project and explains why we decided to take a different route to our solution. Chapter 3 summarizes the thesis background, a description of the key technologies utilized in this thesis; we will provide a detailed summary on each as it relates to this project.

Chapter 4 covers the initial testing and simulations to show OSPF as a suitable routing protocol for large scale tactical networks and Chapter 5 will cover the second phase of the testing to trace packet flow as MANETs move and partition and the need to introduce a gateway.

Chapter 6 introduces our proposed solution and gives a detailed description on how it is designed, while Chapter 7 covers the implementation and testing of the design solution. Finally, Chapter 8 contains conclusion on the implementation of this thesis and provides suggestions for future work.

2: Related Work

2.1 Literature Review

A lot of work has been done on proposing solutions to the underlying issues generated when integrating MANETs with fixed networks. Some of the proposed solutions have involved using an extension of the OSPF routing protocol used in fixed networks and modifying some key properties to enable it to function in MANETs, others have taken the path of combining the already existing MANET routing protocols with OSPF with techniques that accomplish the goal of inter-domain routing.

The design goals that need to be met when integrating MANET and fixed networks are:

1) Low Cost Routing i.e. Finding optimal paths from source to destination, by utilizing routes that take the minimum cost path from a source outside the MANET to a destination in the MANET or the minimum cost path to traverse a transit MANET.

2) Minimizing the amount of link state information originated within the MANET due to frequent link changes that is flooded into the larger network while maintaining accurate and efficient paths into the MANET.

3) Seamless routing when a physical partition occurs in the MANET by ensuring quick optimal route formation for packet delivery to a router in a partitioned network that does not adversely affect the overall overhead.

In [2], the paper takes the route of using the OSPF hierarchy by redistributing between OSPF Autonomous Systems (AS) to limit the MANET impact on the fixed network, and also introduces tunneling between MANET Border Routers to enable

summarization of the MANET prefixes. This approach assigns the MANET and fixed networks to different OSPF Autonomous Systems and this allows the different region to be summarized by border routers. The routes advertised are called redistributed routes; the OSPF Border Routers are configured to advertise fixed metrics on redistributed routes. Here, fixed costs mean that all routes from other regions are advertised as being the same cost from the border routers. Also Tunnels (Virtual Links) are created between all Border Routers in the regions to handle the issue of partitioning, this allows each MANET Border Router (MBR) to summarize the MANET prefixes and advertise them to the fixed network because a packet that reaches any MBR can be tunneled to another if needed. An MBR partitioned from a MANET router survives the partition by tunneling across the non-MANET links to another MBR that has connectivity to the router. Boeing's Common Overlay and Routing Environment (CORE) was utilized, a variant of the IMUNES [21] emulator to quantitatively evaluate the technique to reduce the effect of rapidly changing MANET topologies on the fixed network. CORE allows interconnection of (real) Cisco and (virtual) Quagga routers in a real time emulated network. The authors compared results for a baseline scenario in which a single OSPF area contains the larger network and the MANET, and when redistribution between OSPF Autonomous Systems is used to limit the MANET impact on the backbone, and thirdly when redistribution with tunneling is used between MBRs to enable summarization of the MANET prefixes and the latter was seen to be most effective.

Advantages of this technique:

1) The topology changes occurring in the MANET are completely transparent to the fixed network so one of the design goals is met.

2) The tunneling method also enables packets to enter the MANET from the MBR with the lowest cost route to the destination. An MBR that does not have the lowest cost route to the destination forwards packets to the lowest cost MBR.

3) It addresses the issue of MANET partitions by introducing tunnels between border routers.

Disadvantages of this technique:

1) Tunneling introduces an overhead in establishing and maintaining it, and there is an additional delay and bandwidth usage over the tunnel.

2) There may be suboptimal path selection into the MANET, because visibility into the MANET from the larger network is blocked.

In [3], to support internetworking between fixed networks and MANETs, a gateway, which operates on OSPFv3 is proposed as an interface whereas for the MANET, the Ad-hoc On-demand Distance Vector (AODV) routing protocol is employed, which is categorized as a reactive routing protocol. To overcome the issue of flooding the fixed network with topology changing LSAs, AODV was proposed for the MANET. AODV gets a route on demand and does not need to preserve routes to end devices which are silent during the communication; hence there is no need to constantly flood the fixed network with routes since the routes are created only when needed. The OPNET Simulator was used to analyze this technique using different scenarios and techniques. The results showed a satisfactory decreased ratio of packet loss during transmission and reception for low, medium and high traffic scenarios of varying pause times and speeds.

Advantages of this technique:

It meets the design goal of eliminating the overhead in the fixed network that will be caused by OSPF LSA's.

Disadvantages of this technique:

1) The routing performance suffers at high router speeds because a response received from a destination at speeds higher than 30 m/sec is rapid but this appears to be decaying after some time due to traffic load and congestion in the network.

2) Only 20 routers were considered in the simulations, so it is not shown how this will function on a larger scale. The issue of partition of the MANET was not considered, nor its effect on the AODV protocol.

[4] proposes a Cross Layering technique where OSPF is implemented on top of a layer-2 protocol that implements MANET Routing. The OSPF MANET extension is extended to include a cross layer integration interface (CLI). CLI allows the routing protocol to be more adaptive to the dynamically changing wireless channel using information gathered from lower layers. In such an approach, the system can be designed, and the protocol layers coordinated, such that the layer-2 protocol handles the mobile routing events, and works to produce the appearance of a completely-bridged network to layer-3 (i.e., in the simplest case all routers at layer-3 appear to be one-hop away from one another, while in reality they may be multiple layer-2 hops away from one another). Such an arrangement, if coordinated correctly between the protocol layer, can allow the

layer-3 topology (advertised to the rest of the OSPF network) to change less frequently even though the underlying layer-2 topology may undergo more rapid change.

This technique was analyzed using a Linux test bed and also emulated with a small operational test bed in the Integrated Multiprotocol Network Emulator/Simulator (IMUNES) and a Georgia Tech Network Simulator (GTNetS) platform to handle large number of routers, various traffic loading, and mobility settings. The simulations show satisfactory performance of AODV over OSPFv3 for a network of 20 routers with a transmission range of 100 meters, varying mobility levels and pause times using random waypoint mobility model.

Advantages of this technique:

1) Changes due to mobility are completely hidden from layer-3; hence there will be no Link State Advertisements (LSAs) created to flood the fixed network.

2) The approach can greatly improve the performance in terms of delivery ratio, end-to-end latency, and responsiveness of the OSPF routing protocol to topology changes compared to running AODV alone.

Disadvantages of this technique:

1) It does not consider a scenario where partitioning can occur due to mobility which is one of the requirements earlier stated

2) It might be unrealistic for a larger network; this technique proposes a complete layer 2 approach. This should work well for relatively stable and small topologies such as a community mesh network, especially when there are no network partitions and joins.

3) Although it has the potential to provide superior performance, CLI mechanism is not available for all radio technologies due to interlayer dependencies.

[5] proposes a technique known as Composite Routing. This is a combination of OSPF and a MANET-specific routing protocol which was in this case OLSR. This allows the proposal to achieve MANET routing performance without losing the main advantage offered by OSPF which is routing over existing heterogeneous interface types.

OLSR routes packets within the MANET and also exports the MANET topology to OSPF and abstracts the MANET as a connected mesh. OSPF provides global IP routing and determines the best entry and exit points to/from the MANET. Composite Routing eliminates some properties of OSPF-MDR like the hello protocol and also the flooding of router LSAs because there is no need to discover 2-hop neighborhood relationship as the topology of the MANET is already retrieved from OLSR. Also there is an introduction of a new router, the Network Designated Router (NDR) which generates LSAs for a cluster of MANET routers, thereby hiding the frequent changes from fixed networks.

This proposal was evaluated using a test bed consisting of lightweight Linux routers and performance results were collected to compare OSPF-MDR, OLSR and Composite Routing (CR) under different scenarios and by varying router mobility and network size. Overall CR was seen to perform better.

Advantages of this technique:

The elimination of hello protocol and flooding of LSA's greatly reduces overhead. MDR generates a network LSA that can hide frequent MANET topology changes from the fixed network.

Disadvantages of this technique:

It does not take the possibility of physical partitioning of the MANET into consideration.

[6] presents a new approach for exterior gateway routing called Border Gateway Protocol with Mobility Extensions (BGP-MX). The BGP-MX approach relies on extending the Border Gateway Protocol (BGP) with mechanisms that enable BGP to function correctly and efficiently in mobile networks that are part of the Airborne Network (AN) environment while interoperating with an unmodified BGP infrastructure within the Global Information Grid (GIG). BGP is an exterior gateway routing protocol on the Internet, it is however inadequate for mobile environments mainly because it requires manual configuration to establish connections between BGP peers and it is slow to adapt to topology changes.

Hence the introduction of the BGP-MX software enables BGP to automate the process of discovering peers in adjacent ASes and the process of establishing connections between them, and enhances BGP routing mechanisms with new techniques that enable BGP to adapt quickly to link disconnections due to topology changes within the AN environment. The proposal also utilizes a Distributed Peering Broker Service (DPBS) which uses a geographic overlay to select BGP-MX-capable gateway routers for dynamic BGP peering, responding to their queries for peering instructions and commanding them to re-peer as necessary based on movement of routers within the grid. The BGP-MX routers have GPS (Global Positioning System) capabilities and they will periodically report their attributes, such as position and mobility status to the DPBS. The DPBS will use the information that it receives from the BGP-MX routers to intelligently determine

peering connections between BGP-MX routers that reside in different ASes. The DPBS could be configured with different policies for establishing connections between ASes. A prototype implementation was performed in a laboratory test bed setting to highlight the major capabilities of BGP-MX routing software extensions and confirm its feasibility. It was concluded that BGP-MX would successfully work in a MANET.

Advantages of this technique:

1) Dynamic discovery mechanism and policy-based peering.

2) Detection of path instability because of mobility and selection of the most stable path that is available in the network compared to Legacy BGP.

Disadvantages of this technique:

The issue of handling the partitioning and merging of networks has not been explored at all.

[7] is very similar to the proposed solution in [6], it also utilizes BGP and proposes an extension to the original routing protocol. It enables to dynamically select peers and also introduces the notion of Connected Dominating Sets (CDS) just like in OSPF-MDR to create a backbone network that sends periodic LSAs and thereby reducing overhead; this proposal is named BGP-MDR.

To evaluate this technique, a network emulation test bed composed of tens of Linux-based workstations was used to compare it with OSPF and OSPF-MDR with respect to its generated protocol overhead, its ability to develop valid routes to destinations (e.g., reachability), and its influence on network's outage events. It was realized that a network running OSPF or OSPF-MDR generally has more outage events that is, the network convergence is not stable, than if the network runs BGP (or BGP-

MDR). It is claimed that the OSPF protocol variations generally converge more quickly, leading to shorter average outage events, whereas the BGP protocol variations react more slowly, and tend to combine multiple network outage events together into fewer, but longer, outage events. Also it is seen that the amount of BGP overhead can be several times higher than the MANET routing protocol OSPF-MDR. Similarly, BGP also produced more overhead than OSPF (i.e.,1700 kbits/sec versus 500 kbits/sec). Note also that BGP-MDR did notably decrease the amount of BGP overhead (i.e., 1700 kbits/sec down to 950 kbits/sec) indicating that the overhead reduction benefit of a connected dominating set (CDS) does extend to path vector routing protocols such as BGP. In conclusion, BGP-MDR is a big improvement from legacy BGP and by applying future overhead reducing techniques will make it more attractive for use.

Advantages of this technique:

The proposal utilizes a lot of the OSPF-MDR techniques like the CDS implementation, hence reducing overhead when compared to legacy BGP.

Disadvantages of this technique:

1) BGP has the ability to cause wide-scale network disruptions due to the protocol's configuration complexity and its security weaknesses.

2) BGP can become unstable (i.e., oscillate) based on certain configurations of its routing polices.

3) A limitation was put on the network partitioning when the proposal was evaluated. The authors specified 5% partitioning range for routers from the initial point of movement which means that routers can only partition to a distance of 5% of the entire network size.

2.2 Conclusion

The recent work done on integrating MANET and fixed networks has been surveyed and summarized; the advantages and disadvantages of various proposals have also been listed. While some proposals are preferable to others, none of them completely meet the design goals stated earlier. A common technique deployed by all proposals is to isolate the MANET from the fixed network to enable an overhead reduction. Many proposals have had major issues with adequately resolving issues arising from routers partitioning from a MANET or the splitting of MANETs into two or more MANETs. After reviewing the techniques used, we can conclude that the best way to produce seamless inter-domain communication will be to use one protocol across all the domains.

Deciding to use one protocol for all three domains would make the architecture much simpler, one way to go about it is to introduce the MANET extension of OSPF. This MANET extension works in almost the same way as the Open Shortest Path First (OSPF) routing protocol for fixed IP networks. The MANET extension for OSPF is compatible with Open Shortest Path First version 3 (OSPFv3) for fixed networks, so that solves the issue of integration.

There are 3 types of proposed OSPF extensions [8]:

- OSPF-MDR (MANET Designated Router), defined in RFC 5614 [9], uses MDRs, Differential Hellos, and Connected Dominating Set (CDS) flooding
- OSPF Cisco's Extension, defined in RFC 5820 [10], uses Smart Peering, Incremental Hellos, and Overlapping relays
- OSPF MPR (Multi-Point Relaying), defined in RFC 5449 [11], makes use of MPR selector sets and MPR flooding.

Both Cisco's Extension and OSPF-MPR borrow ideas from Optimized Link State Routing (OLSR), while OSPF-MDR extends OSPF's Designated Router (DR) adjacency reduction technique. These extensions are all Internet Engineering Task Force (IETF) proposals and a de facto standard has not yet been selected. However, Cisco is able to deploy its extension in real routers today, and Boeing has created a deployable version of OSPF-MDR that exists in the Quagga routing suite.

For the purpose of this thesis we will be deploying OSPF-MDR because the CDS provides a means for overhead control within the network, which is one of our major concerns since this is a large-scale network.

BGP will also be utilized in the gateways of each domain network. Unlike [6] and [7], which used BGP as an the underlying interior gateway protocol, this thesis proposes to modify BGP to enable dynamic gateway selection, and thus employ BGP on only gateway routers that are in use, reducing the overhead instability issues experienced in [6].

3: Thesis Background

3.1 Open Shortest Path First (OSPF)

OSPF is a one of the most popular Interior Gateway Protocols (IGP), this means that it routes packets between routers belonging to the same Autonomous Systems (AS). These packets are routed using a method based on Dijkstra's algorithm- the Shortest Path First (SPF) for calculating the shortest path to any destination known by the router that is running OSPF.

It is classified as a link state routing protocol, hence the router running OSPF maintains a database describing the state of the AS's topology, this database is referred to as the link-state database. All routers running OSPF in the network contain similar databases, and the databases are shared and exchanged across the network by a system of flooding using Link State Advertisements (LSA).

OSPF uses different packet types to acquire and maintain neighbor relationships and also to maintain the link state database and all packets types contain a similar 20 byte header.

Packet name	Protocol Function
Hello	Discover/maintain neighbors
Database Description	Summarize database contents
Link State request	Database download
Link State Update	Database update
Link State Ack	Flooding acknowledgment

Table 3.1 OSPF Packet Types

The hello protocol uses hello packets to discover and maintain neighbor relationships with bi-directional neighbors. Hello packets are sent out periodically from all the routers interfaces, the default time interval is 10 seconds.

3.1.1 Neighbor States and Synchronization of Databases.

When an adjacency is formed between OSPF neighbors, the routers go through different neighbor states to reach full adjacency with each other; these states are defined in RFC 2328 [12].

Neighbor States	Description
Down	Initial state of neighbor Conversation, no recent information has been received from the neighbor
Init-Way	A hello packet has been seen from the neighbor but the router does not appear in the neighbors hello packet
2-Way	Communication between neighbors is bi-directional. Neighbors appear in each other's hello packet
Exstart	First step in creating adjacency between neighboring routers, master-slave relationship is established.
Exchange	Router sends Database Description (DD) packets to its neighbor
Loading	Link state request packets are sent to the neighbor asking for more recent LSAs that have been discovered in the Exchange state
Full	The neighbors are fully adjacent

Table 3.2 OSPF Neighbor States

Every OSPF network has a Designated Router (DR) that is elected by the hello protocol. A router's hello packet contains its router priority which is configurable on a per interface basis, hence when a router's interface becomes functional, it checks if there is an existing DR for the network. If there is, it accepts it as its DR. If not, it elects itself as DR if it has the highest router priority in the network; there is a baseline for determining DR election that is defined in RFC 2328 [12].

The main function of a DR is to generate a network-LSA on behalf of the network that lists all routers connected to the network and to become adjacent to all other routers on the network since link state databases are synchronized across adjacencies. There is

also a Backup Designated Router (BDR) that is elected by the hello protocol, it maintains adjacencies with all routers on the network and becomes the DR if the DR fails.

3.1.2 Differences between OSPFv2 and OSPFv3

There are presently two versions on OSPF, OSPFv2 which is described in RFC 2328 [12] and OSPFv3, described in RFC 5340 [13]. OSPFv3 is essentially equivalent to OSPFv2 with support for IPv6 addressing. There are however some notable differences, most relevant to this thesis are:

- OSPFv3 packets and most of the LSAs (described later) do not carry addressing semantics. All OSPFv3 routers are identified by their router ID, leaving a network protocol-independent core.
- Two routers can become neighbors regardless of their associated network prefix, this follows from the fact that link-local addresses are used for all inter-router communication.
- Multiple OSPF protocol instances can be run per link, so it is possible to run IPv4 addresses on OSPFv3.

3.1.3 OSPF-MDR: Supporting Mobile Ad-hoc Networks (MANETs) using Connected Dominating Sets (CDS)

RFC 5614 [9] defines an extension to OSPFv3 to support MANETs. The MANET Designated Router (MDR) approach aims at generalizing the DR mechanism: instead of electing only one DR and BDR in a network to act on behalf of other routers, this approach elects several MDRs such that they form a CDS. The MDRs and Backup MDRs

(BMDR) form a bi-connected CDS for robustness, so that all non-MDR and non-BMDR routers have at least one MDR router as a neighbor.

This CDS is used in two ways:

- To reduce flooding overhead, only MDRs and BMDRs flood new LSAs back out the receiving interfaces.
- Adjacencies are formed only between MDRs, BMDRs and a subset of their neighbors, allowing for much better scaling in dense networks.

Another important feature of OSPF-MDR is the optimized hello protocol, a differential hello that reports only changes in neighbor states, thereby reducing overheads.

3.2 BGP (Border Gateway Protocol)

BGP, defined in RFC 4271 [14], is one of the few existing Exterior Gateway Protocols (EGP). It is the most common protocol for interconnecting networks over the Internet, and provides a means of communicating between different Autonomous Systems (AS). The primary function of BGP is to exchange network reachability information with other BGP routers. This information contains a list of ASes these reachability information transverse, hence a graph can be constructed of AS connectivity to be used for packet forwarding and routing loops pruning.

Routing information exchanged via BGP supports only the destination-based forwarding paradigm, hence a router forwards packets based solely on the destination address carried in the IP header of the packet. BGP neighbors, called peers, are established by manual configuration between routers. Peers within an AS are called

Internal BGP (IBGP) peers, when BGP runs between peers in separate autonomous systems it is called External BGP (EBGP).

3.2.1 Messaging Structure

BGP uses an incremental update strategy to conserve bandwidth and processing power, hence after the initial exchange of complete routing information, a pair of BGP peers exchange only changes to that information. This requires a reliable transport between the peers in order to function correctly, consequently BGP uses Transmission Control Protocol (TCP) for reliable transport. BGP listens on TCP port 179; a BGP speaker will periodically send a 19-byte keep-alive message to maintain the connection.

BGP has 4 different messaging types, indicated by the 1-byte unsigned integer contained in the message header showing the type code.

Message Type	Description
1- OPEN	After a TCP connection is established, the first message sent by each peer is an OPEN message.
2- UPDATE	Used to transfer routing information between BGP peers, the information contained in the UPDATE message can be used to construct a graph that describes relationships of the various ASes.
3- NOTIFICATION	Sent immediately an error condition is detected, the BGP connection is closed immediately after it is sent.
4- KEEPALIVE	Exchanged between peers often enough not to cause the hold timer to expire.

Table 3.3 BGP Message Types

3.2.2 BGP Finite State Machine (FSM)

The BGP Finite State Machine (FSM), as described by RFC 4274 [15], is a set of rules that is applied to BGP peers relationship. The FSM must be initiated and maintained for each new incoming and outgoing peer connection.

The BGP FSM has the following states associated with each peer:

States	Description
IDLE	State when BGP peer refuses any incoming connections.
CONNECT	State in which BGP peer is waiting for its TCP connection to be completed.
ACTIVE	State in which BGP peer is trying to acquire a peer by listening and accepting TCP connections.
OPENSENT	BGP peer is waiting for OPEN message from its peer.
OPENCONFIRM	BGP peer is waiting for KEEPALIVE or NOTIFICATION message from its peer.
ESTABLISHED	BGP peer connection is establishes and exchanges UPDATE, NOTIFICATION, and KEEPALIVE messages with its peer.

Table 3.4 BGP Finite States

3.3 Common Open Research Emulator (CORE) and the Quagga Routing Software Suite

Selecting a tool to analyze the feasibility and effectiveness of the proposed network routing solution is another important step. The proposed solution to providing an inter-domain routing protocol that efficiently carries out routing between a MANET and a fixed network is to use OSPF MDR (Open Shortest Path First-MANET Designated Router) - which is an extension of the OSPFv3 that operates on MANETs - and includes a gateway protocol that extends OSPF-MDR to handle the partitions and unpredictable mobility of ad-hoc networks effectively.

Common Open Research Emulator (CORE) [16] was found to be one of the few simulators/emulators that implements OSPF-MDR and provides a means via Quagga of modifying or adding to the original source code to implement the extensions proposed.

3.3.1 Introduction to CORE

CORE [16] is an emulator not a simulator, it is a representation of a real computer network in real time, and it can also be connected to real networks and routers as a means of expanding the network. It provides an environment for running real applications and protocols, taking advantage of virtualization provided by the FreeBSD or Linux operating systems. CORE is efficient and scalable, it runs applications and protocols without modifications and it has a very user-friendly Graphical User Interface (GUI) which is customizable.

CORE is typically used for network research, studying protocols, demonstrations, application and platform testing, evaluating networking scenarios, security studies, and

growing the size of networks. The CORE GUI utilizes the Tool Command Language (Tcl) programming language and the Toolkit (Tk) graphical user interface toolkit also known as tcl/tk programming language. It is initialized using a command line interface. The CORE Services manage the virtual routers and networks.

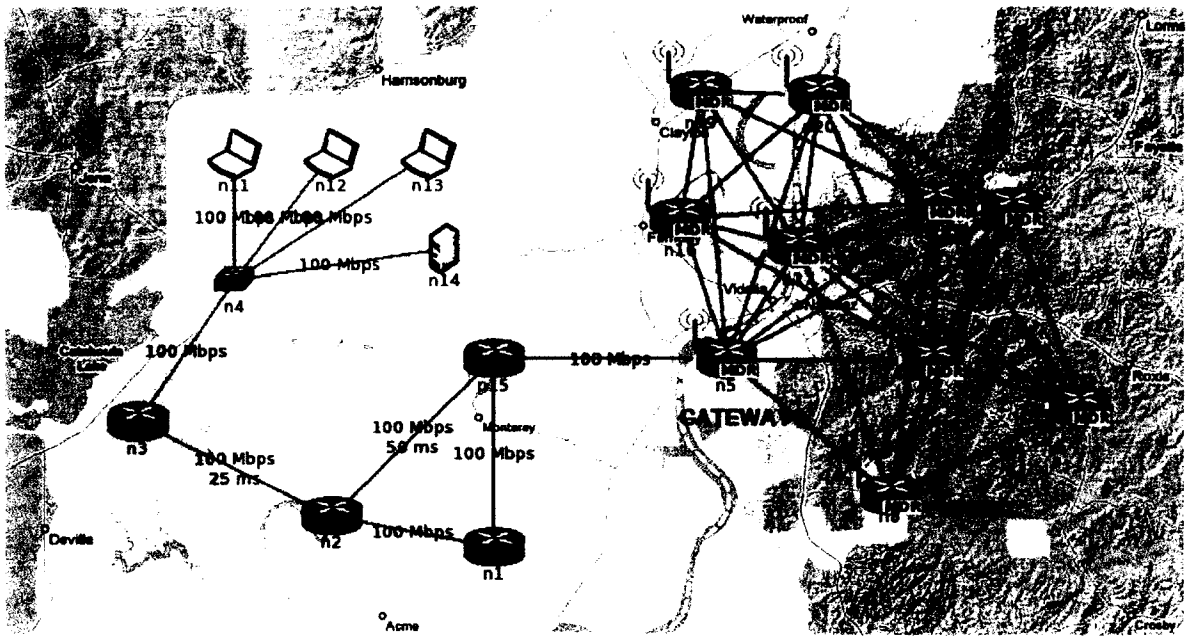

Figure 3.1 Sample Topology in the CORE GUI comprising of Mobile and Fixed Routers

3.3.2 Introduction to the Quagga Routing Suite

The wireless extensions to OSPFv3 described in this thesis were implemented by Richard Ogier and Boeing Phantom Works by modifying the OSPFv3 implementation provided by the Quagga routing software [17] to implement RFC 5614 [9]. Quagga is a General Public License (GPL) licensed routing software suite providing implementations of routing protocols including Border Gateway Protocol (BGP), RIP, and OSPFv3 amongst others. It is actually a fork of the GNU Zebra routing software [18], focusing on building a more active development community than the centralized model of GNU Zebra.

Presently Quagga is the only routing protocol suite that provides an implementation of OSPFv3 for MANETS. When deciding whether to use Quagga or GNU Zebra as a basis for our implementation, Quagga was chosen because of its active development community. There seems to have been very little activity around GNU Zebra for the last couple of years - the latest release was at the end of 2003. Quagga, on the other hand, provides bug-fixes and general implementation updates on a regular basis.

3.3.3 Software Architecture of Quagga

While traditional routing software is designed so that one process manages the entire routing functionality, Quagga separates the routing daemons into different processes. This way, if a routing daemon fails, others will not be affected. As a result, increased reliability and modularity are achieved.

The different routing protocols are handled by routing daemons. For example, the OSPFv3 daemon (referred to as ospf6d) handles the OSPFv3 routing protocol which includes OSPF-MDR. A dedicated daemon is responsible for changing the kernel routing table, and distributing routing information between the routing daemons. This is the Zebra daemon, which acts as a routing manager. Figure 3.2 depicts the Quagga system architecture. It illustrates the module-based approach of Quagga.

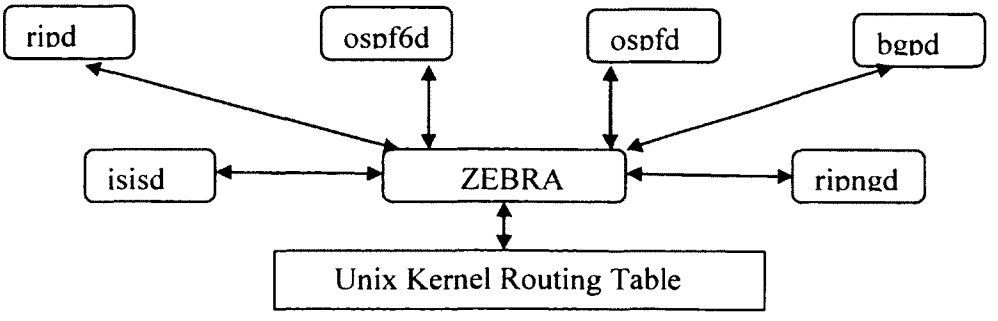

Figure 3.2 The Quagga Software Architecture

As shown in the figure above, the routing daemons are really just modules in the Quagga system. Not only does this make the system more robust (since upgrading and modification can be done separately), but adding a new routing protocol to the system does not require changing any of the existing software.

Quagga utilizes a strict layered architecture; this complements the module-based approach of Quagga; as the routing protocols are only concerned with interaction with Zebra. For example, adding a routing protocol will only require knowledge about the communication interface between the Routing Protocol layer and Zebra.

3.4 Inter-MR

In [1], a novel routing protocol is described that supports interoperability among MANETs, the main function of this protocol is to:

1) Develop an attribute-based address scheme that is transparent to split/merge operations of MANETs and at the same time does not require a separate name server.

2) Provide an algorithm that dynamically elects active gateways so that we can maximize the inter-MANET connectivity when the network topology changes due to router mobility.

3.4.1 Introduction to Inter-MR

InterMR can be seen as a gateway protocol for mobile networks, unlike BGP, whose prefix-based address scheme is not viable to properly aggregate IP addresses in a MANET that can be partitioned and merged. InterMR proposes an attribute-based

address scheme that adaptively defines the address of a MANET from all the attributes (e.g., symbolic names, properties, services, etc.) in the MANET, and the address is transparent to MANET split/merge [1].

In InterMR, the address of a MANET is defined to be the Bloom Filter (BF) [19] of all the attributes pertaining to the MANET, most prominently (but not exclusively) the symbolic host names. The Bloom Filter is the OR of the hashes of the attributes based on a universally known function. An attribute is said to be in the Filter if the Filter matches all the "ones" of the attribute hash. This address choice guarantees the uniqueness of the address since attributes are different from MANET to MANET. Moreover, the BF functions as Name Server for the interconnected MANET system. If a gateway has the full set of MANET addresses (i.e. the corresponding BFs), it finds which MANET a given destination is in by matching its attribute hash across BFs routers. In InterMR, the BF is computed by each active gateway in a MANET as it monitors MANET membership. It will be noted that the MANET address changes dynamically as the MANET splits/merges and as it acquires/loses members of the MANET.

The dynamic election mechanism provides a means by which potential gateways in each partition can determine whether they should become active gateways or not to maximize inter-MANET connectivity while satisfying the constraints on the number of active gateways after the topology has been changed. There are three major steps in the election mechanism: collecting of connectivity information, detecting intra-MANET topology changes, and making local decision whether or not to become active gateways.

We should also note that, in this research we are employing some of the characteristics of InterMR in the gateway routers between MANETs. The gateway protocol used will utilize the dynamic gateway selection procedure specified in Inter-MR.

3.4.2 Inter-MR Design

There are two types of topology changes. First, routers belonging to a single MANET can become partitioned into multiple sub-MANETs due to router mobility. Such a topology change must be detected by gateways in each sub-MANET. To support change detection within a single MANET, a sub-protocol was defined called i-InterMR, by which gateways maintain soft state of MANET topology via periodic beacons. Failure to receive a beacon indicates a partition. Secondly, as MANETs dynamically move, gateways in each MANET are required to detect new neighboring MANETs and start exchanging routing information with them and retire old inter-MANET routing entries. To handle this, another sub-protocol called e-InterMR is used to maintain and discover inter-MANET topology changes via inter-MANET beacons and propagation of inter-MANET routing information (e.g., routing entries of destinations in other MANETs). This requires gateways to maintain direct connectivity with adjacent gateways of other MANETs.

4: Analysis of OSPF as a Suitable Routing Protocol for Large Scale Tactical Networks.

4.1 Overview

According to information received by CRC on data accumulated by their researchers, OSPF-MDR has been challenged as a suitable routing protocol for MANETs. Previous experiments and simulations by researchers have shown a lack of convergence of OSPF when a large number of routers are used for any given network.

The reported simulation result showed that the routers in the network did not obtain complete next hop information about how to reach all other routers in their routing tables. Hence OSPF was allegedly seen to not have converged fully. If this result is true then different variants of OSPF (OSPFv2, OSPF-MDR) will not be a good solution to the problem of designing a routing protocol for a tactical inter-domain network.

OSPF-MDR is the MANET extension of OSPF. It is based on the selection of a subset of MANET routers consisting of MANET designated routers (MDRs) and Backup MDRs that form a connected dominating set (CDS). The CDS is used to reduce flooding overhead, as only the MDRs and Backup MDRs flood new link state advertisements (LSAs) out the receiving interface to their neighbors. In addition, adjacencies are formed only between MDRs and a subset of their neighbors which provides proper scaling in large scale networks.

Fast convergence to topology changes has emerged as a critical requirement for today's routing infrastructures. However, limiting the processing/bandwidth overhead of the routing protocol continues to be as important as before. OSPF, being a distributed protocol, requires timely execution of certain operations, e.g., generation and processing of hello packets, by the participating routers. This process might be causing the alleged

lack of convergence of OSPF. On the other hand in [20] an experiment of 200 routers was executed using Georgia Tech Network simulator (GTNetS), and OSPF-MDR was reported to have converged with a packet delivery ratio of 95.1%.

The ultimate goal of our experiment is to determine the validity of using OSPF as a routing protocol for an inter-domain network of 200 routers. The research problem produced by CRC introduces a scenario of 200 routers in a tactical network and hence in this thesis, we used 200 as a benchmark for a large tactical network. As an intermediate step, we study the convergence of legacy OSPF, also known as OSPFv2 and also the convergence of OSPF-MDR in a static network and a network with mobility respectively.

4.2 Experiment for Analysis

In this section, we explore two different network scenarios to evaluate scalability

- OSPFv2 in static networks
- OSPF-MDR in a MANET without mobility

These experiments will be carried out using Quagga 0.99.20mr2.1 running on CORE version 4.3, on a network of 200 routers having the following characteristics:

- 36 routers form a Headquarter Network (HQ) connected with 10Mbps links
- The remaining routers have been divided into smaller networks, connected with 64 kbps links
- The smaller networks each have a designated router (DR) which form a CDS with other DRs and are connected to the HQ network

- The simulation is run for a period of 5 and 20 minutes, with relevant statistics collected at the end of these time periods. We also run experiments for 30 and 40 minutes to study the stability of our converged results.
- Results gotten from all test beds are from individual runs since repeating simulations always yields the same result.

NOTE: It should be noted that the bandwidth of each link is dedicated.

In a first experiment, we configured the routers with OSPFv2, as the experiments progress, we will configure the routers with OSPF-MDR. The main statistic logged is the routing table of each router in the network

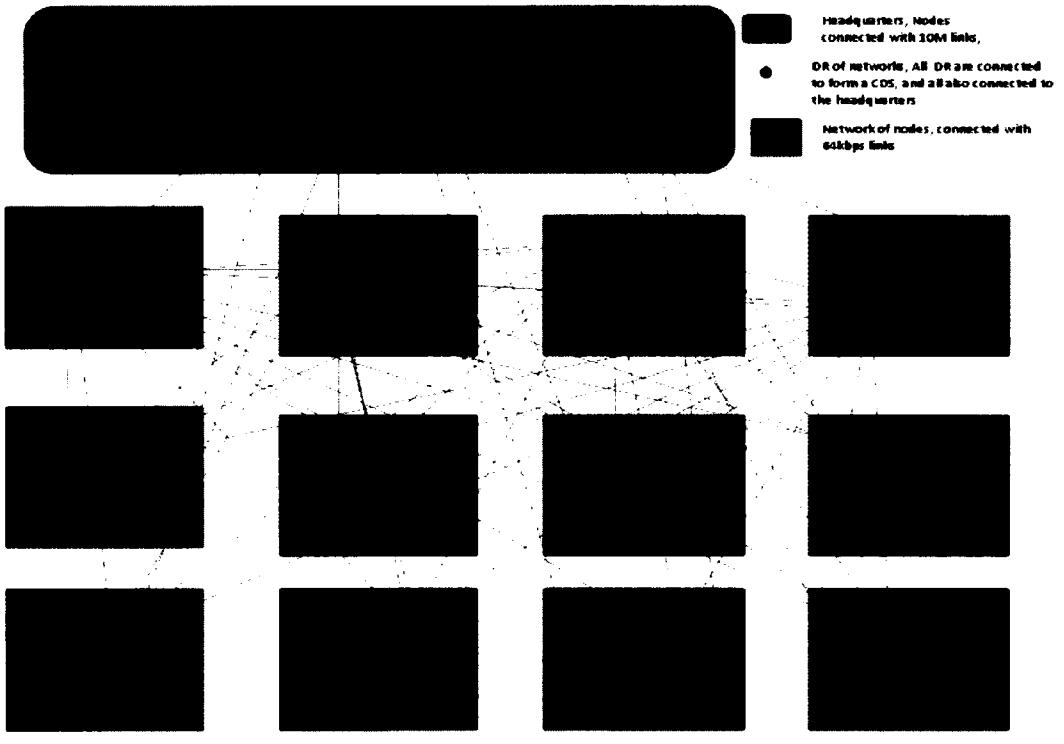

Figure 4.1 Overview of Routers in Tactical Network

The individual routing tables have been further analyzed using the following metrics

- **Convergence of the Network**: Number of routing entries that contain next hop routes to all network addresses in the network. As time progresses, each router should have a known route to every other router's interface in the network. Note that this implies that not all routers have a routing table of the same size – more central routers with more connectivity will have smaller routing tables, as they will not have entries to their interfaces/networks that are directly connected.
- **Percentage of Valid Routes**: Percentage of routes found in the routing table that are valid, i.e., the next hop address actually leads to the destination address
- **Stretch Factor of Shortest Path Routes**: The stretch factor is the variance that exists between the optimal shortest path length and the average path length of valid routes retrieved from the routing tables. To determine this, Dijkstra's Shortest Path First (SPF) algorithm is applied on the map of the topology that is created using the directly connected routes of each router. Dijkstra's SPF algorithm calculates the shortest routes between each router. To determine that the shortest routes have been found, a stretch factor of almost 1 is expected.

4.3 Test-Bed Results 1: OSPFv2 in a Static Network

The network has 200 routers, 448 links, and 87912 routes. 36 routers exist in the Headquarters, while the remaining 164 routers are split between 17 MANETs.

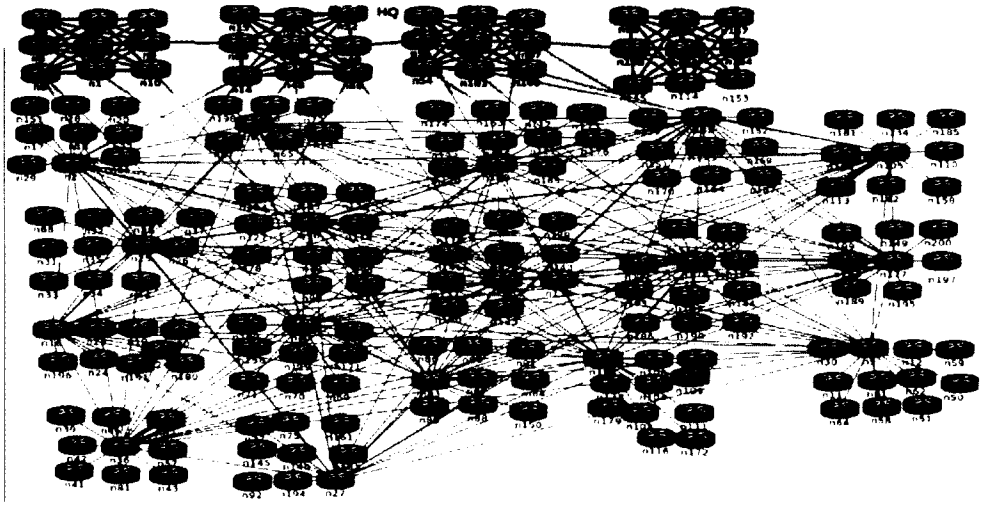

Figure 4.2 OSPF in a Static Network of 200 Routers

OSPF Parameters

Hello Interval	2s
Dead Interval	6s
Flood Delay	100s
Txmt Delay	1s
Rxmt Interval	7s
Interface Type	Ethernet
Network Type	Broadcast

Table 4.1 OSPFv2 Parameters

Link Parameters

Delay	80000us
Bandwidth for HQ Networks (Dedicated)	10Mbps
Bandwidth for smaller Networks (Dedicated)	64 kbps

Table 4.2 Link Parameters

Our results are shown below:

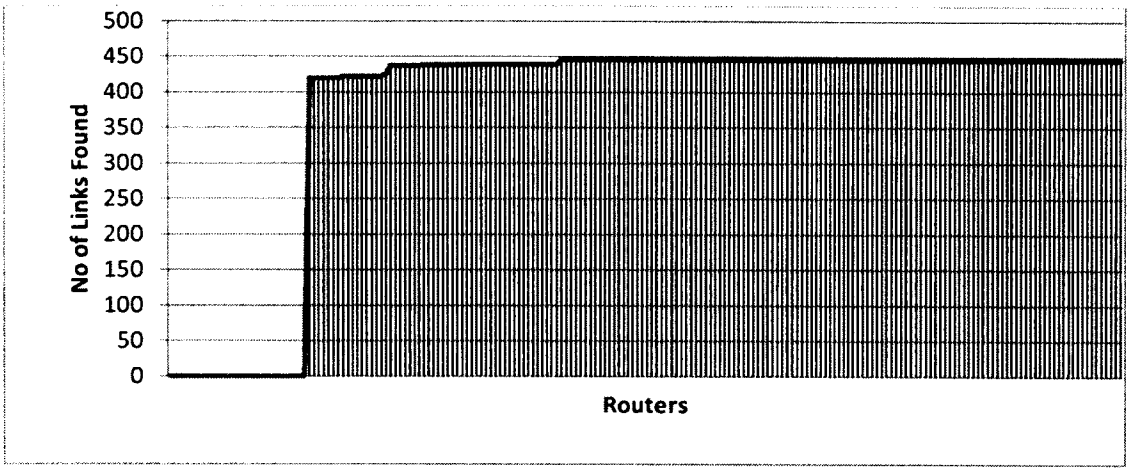

Figure 4.3 Ordered Size of Routing Tables, OSPFv2, after 5 Minutes

As seen in the above graph, after 5 minutes of simulation time using OSPFv2 in a static network, 29 routers out of 200 still have not found any routes.

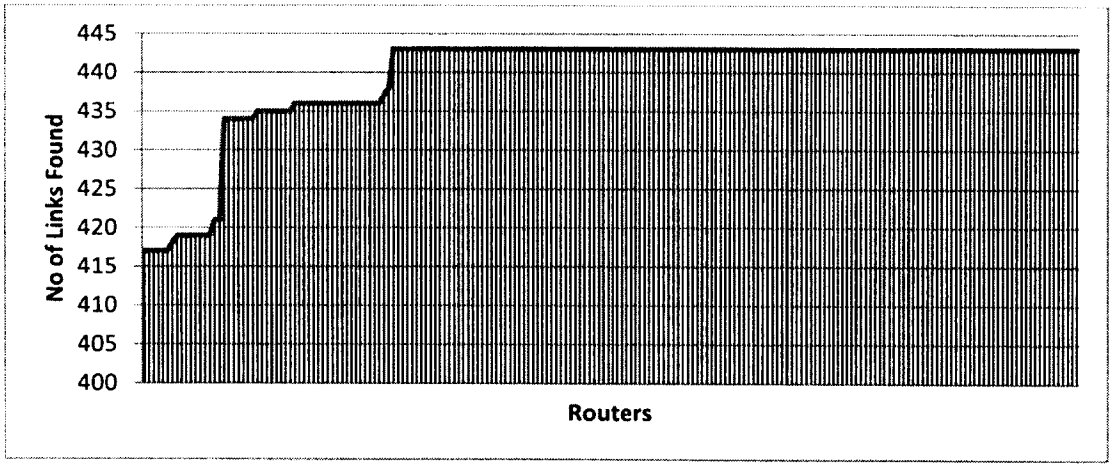

Figure 4.4 Ordered Size of Routing Tables, OSPFv2, after 20 Minutes

As seen in the above graph, after 20 minutes of simulation time using OSPFv2 in a static network, the entire network is converged; all routers have found routes to every other network address except the addresses of its own router.

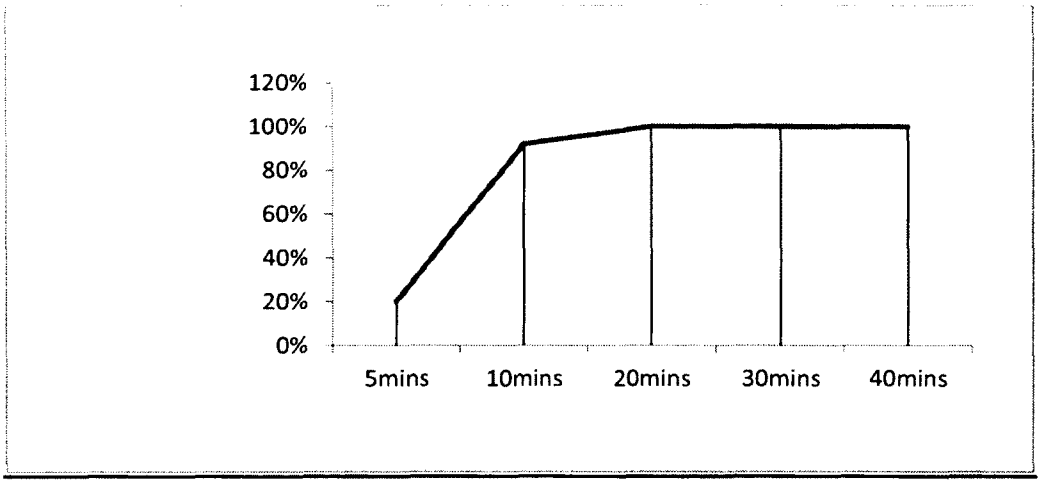

Figure 4.5 Percentage of Valid Routes for OSPFv2

The percentage of valid routes found after 5 minutes of simulation time is seen to be about 20%, and increases to 92% after 10 minutes. After 20 minutes of simulation time, when the network is seen to be converged, the percentage of valid routes rises to 100% and remains at that level.

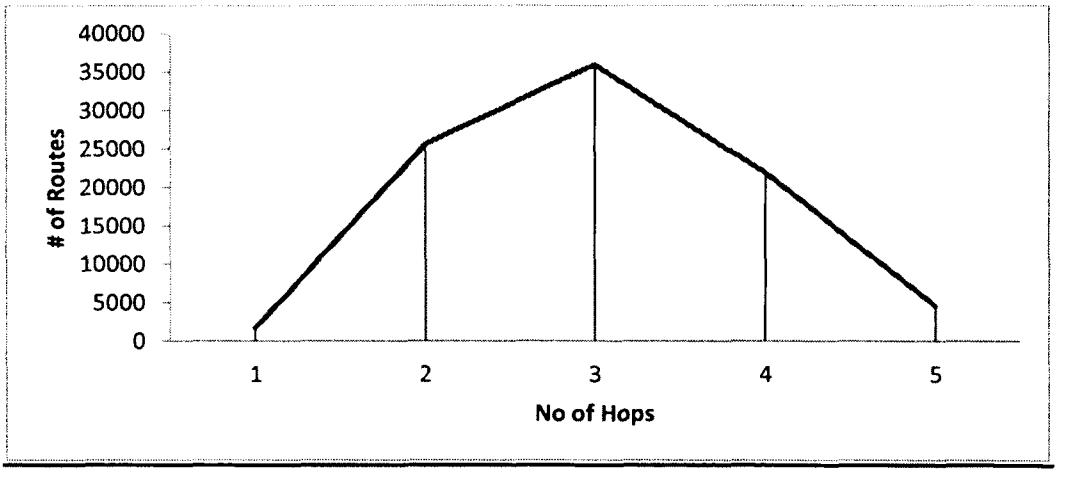

Figure 4.6 Optimal Path Length Distribution

The average number of hops for optimal routes, as determined by Dijkstra's SPF algorithm, is the Total number of hops/ Total number of routes = 3.023, this number can be compared with the average path length at any time. The averages will be compared to

note the difference, which captures in a single metric how well the protocol works, looking for optimal routes.

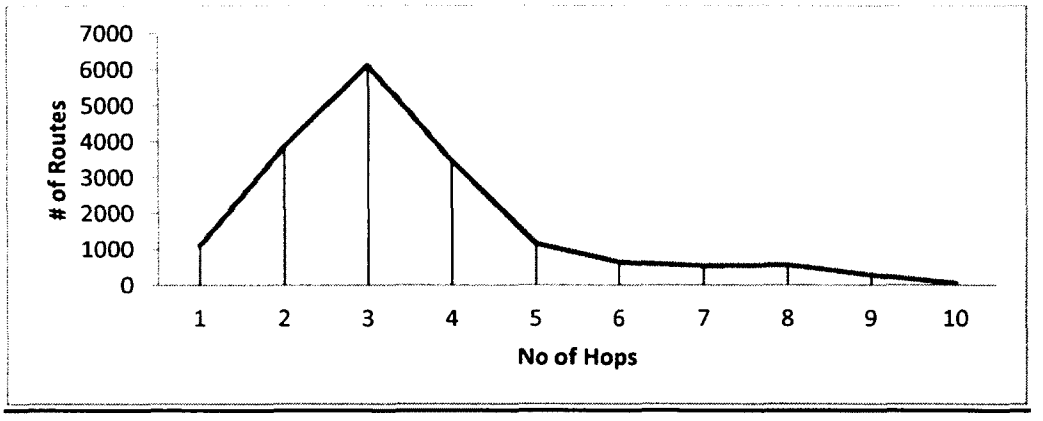

Figure 4.7 Path Length Distribution after 5 Minutes of OSPFv2

After 5 minutes, some routers use up to 10 hops to reach their destination, most routers use 3 hops, the average path length is 3.496 and comparing that to the average path length of the optimal (shortest) path, which was 3.023, we see that it is a stretch factor of 1.16 or routes are on average 16% longer than the shortest routes.

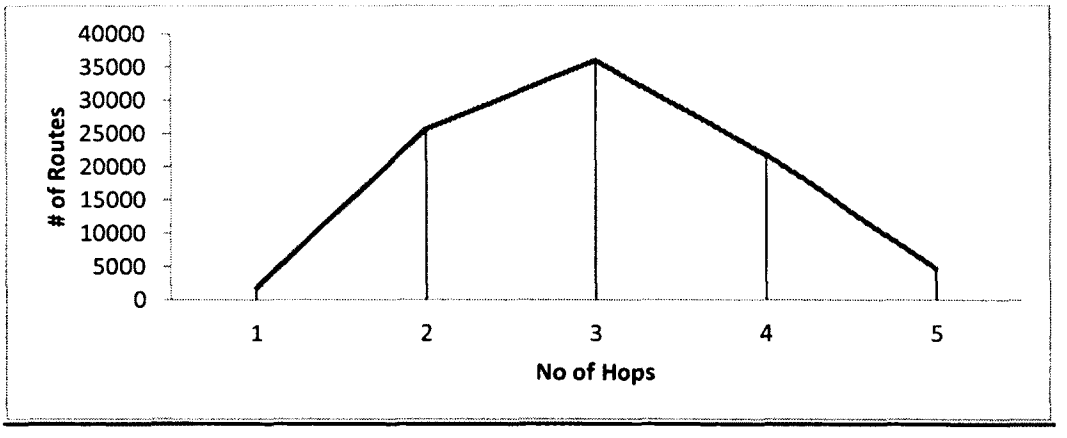

Figure 4.8 Path Length Distribution after 20 minutes of OSPFv2

After 20 minutes when the network is converged, we see that the highest number of hops is now 5, and most routers take up to 3 hops to reach their destination, the average path length is 3.024, and comparing that to the average path length of the optimal

(shortest) path, which was 3.023, we see that it is a stretch factor of 1.0003, we can say that the shortest paths have been found.

4.4 Test-Bed Results 2: OSPF-MDR in a MANET without Mobility

This network has 200 routers and 223 links, and 39800 routes. 36 routers exist in the Headquarters, while the remaining 164 routers are split between 18 MANETs.

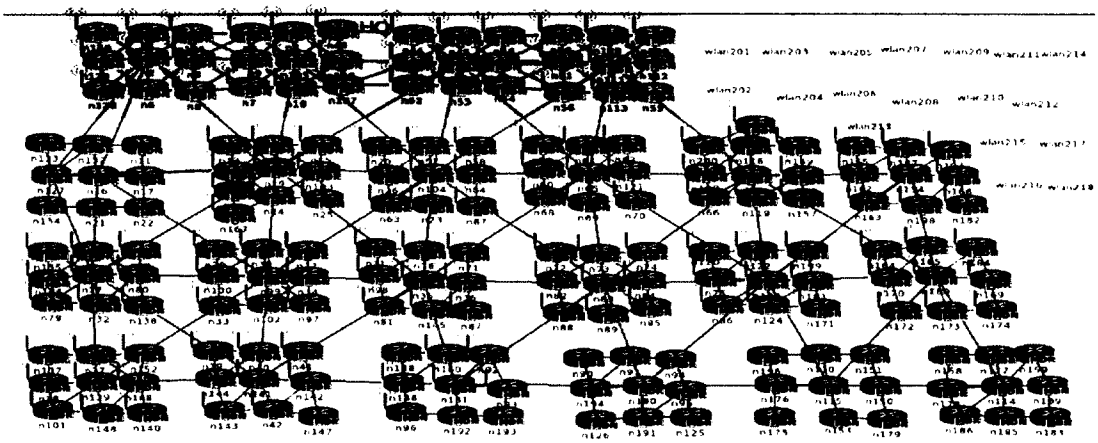

Figure 4.9 OSPF-MDR in a Static Network of 200 Routers

Hello Interval	2s
Dead Interval	6s
Rxmt Interval	5s
Transmit Delay	1s
Two Hop refresh	3
Ack Interval	1s
Hello Repeat Count	3
LSA Fullness	MinCostLSA (0)
Adjacency Connectivity	UniConnected(1)
MDR Constraint	3
Backup wait Interval	0.5s
Flood Delay	100s

Table 4.3 OSPF-MDR Parameters

Wireless Range for HQ	126.345m
Wireless Range for Smaller Networks	99.41m
Bandwidth for HQ	10Mbps
Bandwidth for Smaller Networks	64 kbps
Delay	20000us
Interface Type	Ethernet

Table 4.4 WLAN Parameters

Our results are shown below:

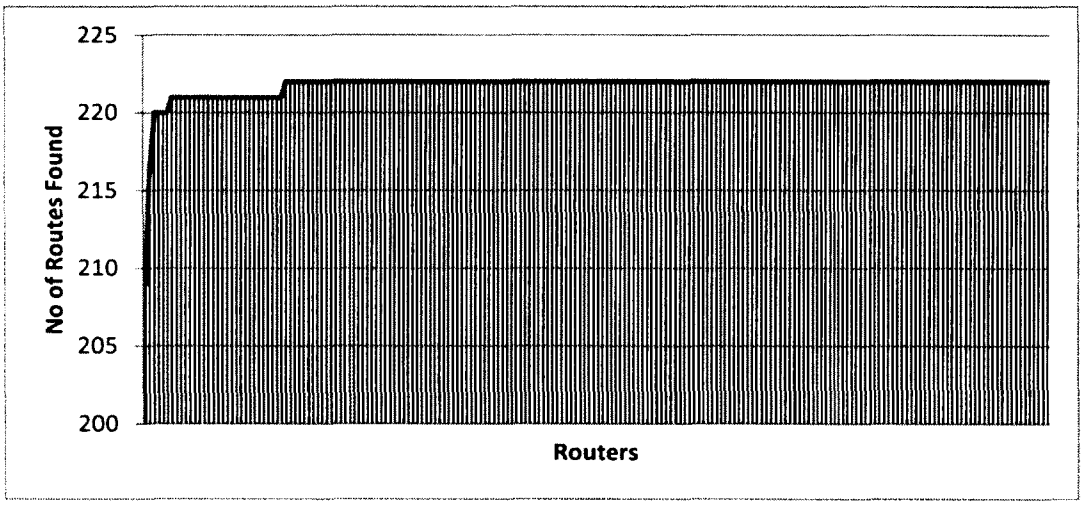

Figure 4.10 Ordered Size of Routing Tables, OSPF-MDR, after 5 Minutes

After 5 minutes there we see that all routers have found a considerable amount of routes unlike in OSPFv2.

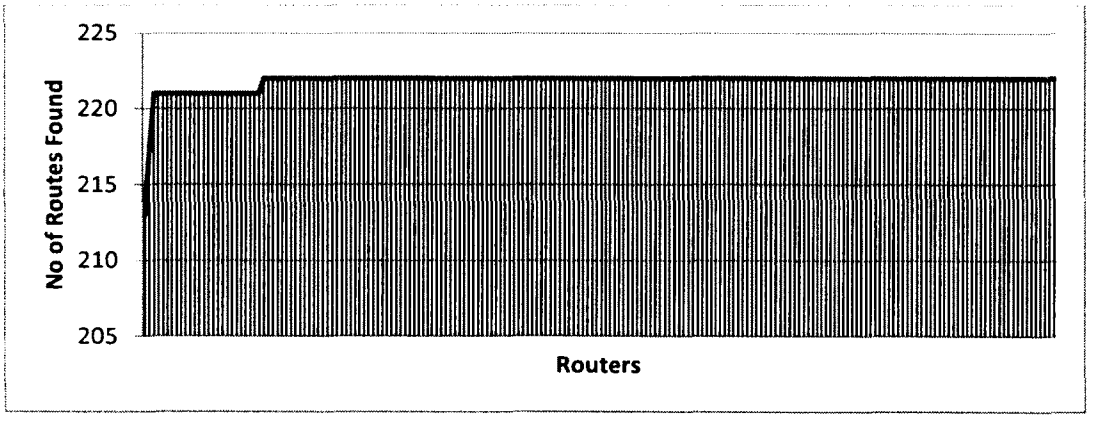

Figure 4.11 Ordered Size of Routing Tables, OSPF-MDR, after 20 Minutes

As seen in the above graph, after 20 minutes of simulation time using OSPF-MDR in a static network, the entire network is converged; all routers have found routes to every other network address except the addresses of its own router.

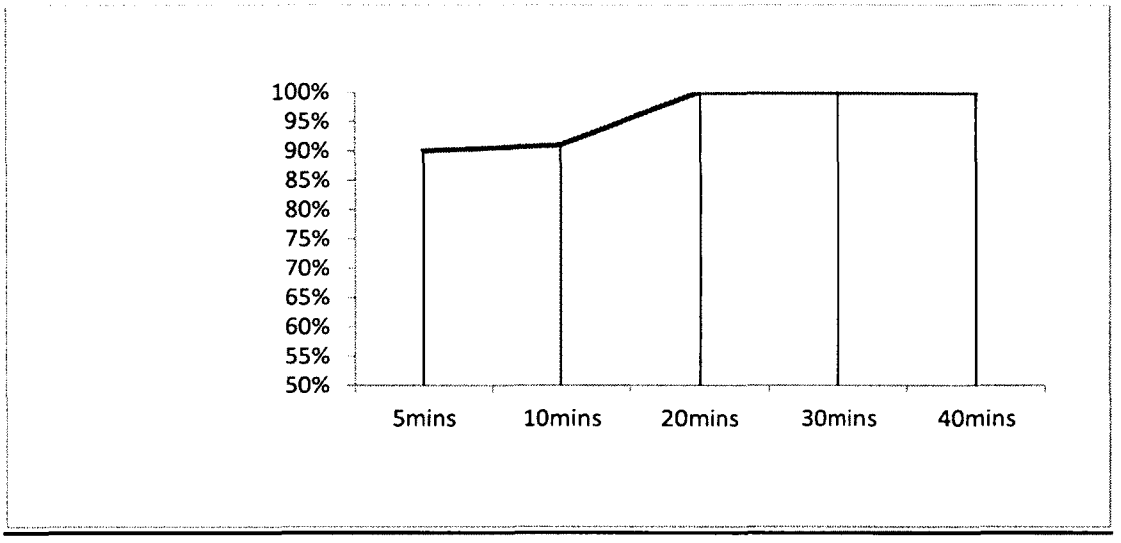

Figure 4.12 Percentage of Valid Routes for OSPF-MDR

The percentage of valid routes found after 5 and 10 minutes of simulation time are about 91%, but after 20 minutes of simulation time, when the network is seen to be converged, the percentage of valid routes rises to 100% and stays at that level.

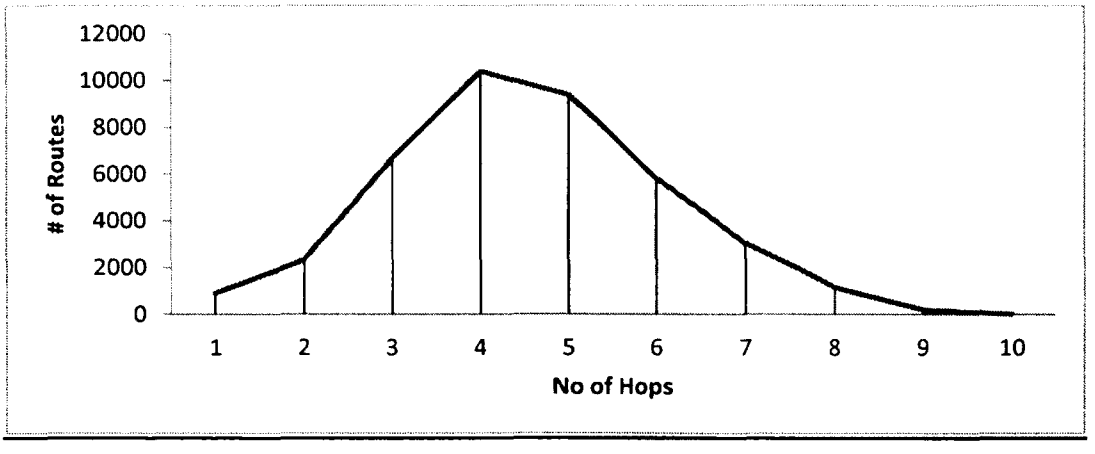

Figure 4.13 Optimal Path Length Distribution for OSPF-MDR

The average number of hops for the optimal, i.e., shortest hop, routes, is calculated as the Total number of hops/ Total number of routes = 4.544. This number can be compared with the average path length at any time. The averages will be compared to note the difference, which captures in a single metric how well the protocol works, looking for optimal routes.

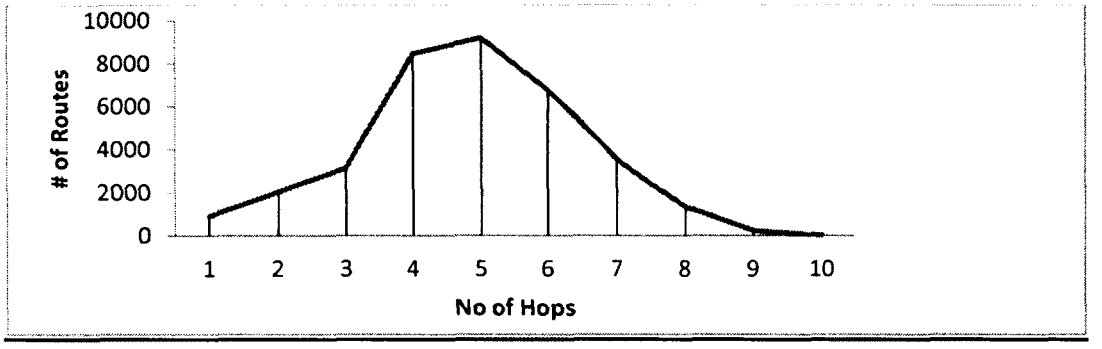

Figure 4.14 Path Length Distribution after 5 minutes of OSPF-MDR

After 5 minutes, some routers use up to 11 hops to reach their destination; most paths are 4 to 5 hops in length and the average path length is 4.84. Comparing this value to the average path length of the optimal (shortest) path, which was 4.544, , we see that it is a stretch factor of 1.065, so the routes are close to, but not quite identical to the shortest routes.

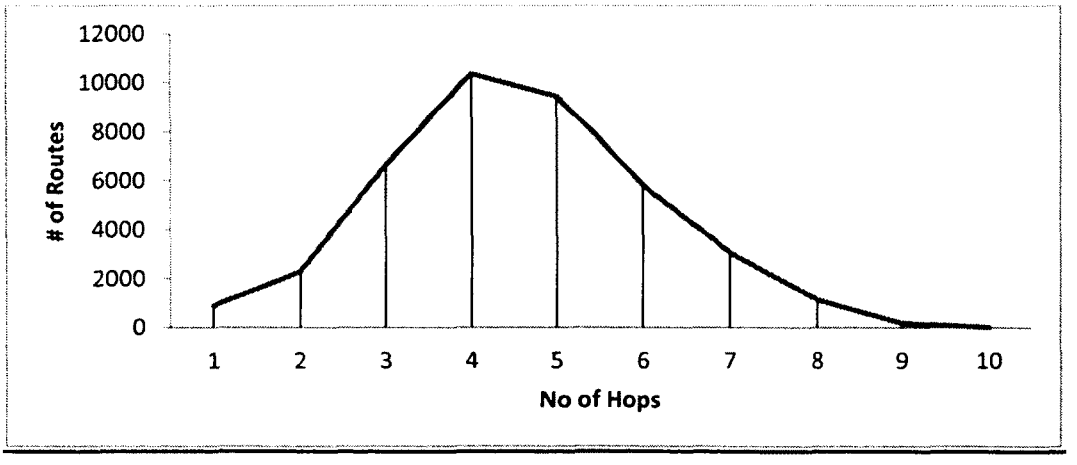

Figure 4.15 Path Length Distribution after 20 minutes of OSPF-MDR

After 20 minutes when the network is converged, the average path length is 4.548, which varies from the optimal path of 4.544 by a stretch factor of 1.0009. We can say that the shortest paths have been found.

4.5 Conclusion

In this chapter we were able to show that OSPF will converge when used in large tactical MANETs and hence is a good solution to inter-domain routing in large scale networks, since it has variants that can work in both fixed networks and MANETs.

We tested OSPFv2 in a network of 200 fixed routers and we demonstrated that a network of that size converges after 20 minutes. We also ran OSPF-MDR on 200 wireless routers and demonstrated convergence at 20 minutes as well. In our inter-domain scenario we will have a combination of both wireless and fixed routers and OSPF will run in both domains.

5: **OSPF-MDR in a MANET with Mobility**

In this chapter we introduce mobility into OSPF-MDR to demonstrate the problem stated earlier, motivating our work to proposing a solution to inter-domain routing in MANET.

The following problem statements will be addressed:

1) The issue of packet loss as MANETs partition and move around the network

2) Interconnecting different MANET: When more than one MANET exists in a topology, connecting them has to be done through an exterior gateway protocol.

Currently we are introducing mobility into an OSPF-MDR Wireless LAN topology that has 12 routers. There are 3 MANET networks in this topology, each consisting of 4 routers. Each router in the MANET domain is connected to WLAN 13, which is shown in Figure 5.1. WLAN 13 acts as the Network address for all connections under that network and assigns one IP address to every router.

The mobility scenario is designed as such that

- Routers 1, 2, 3, and 4 belong to MANET 1
- Routers 5, 6, 7, and 8 belong to MANET 2
- Routers 9, 10, 11, and 12 belong to MANET 3

After the simulation is started and has run for 20 minutes to ensure convergence, mobility is introduced and TCPdump is used to collect packet flow information between routers for 600 seconds. The routers move at a speed defined by the mobility scenario created in core, which averaged at 22.5m/s.

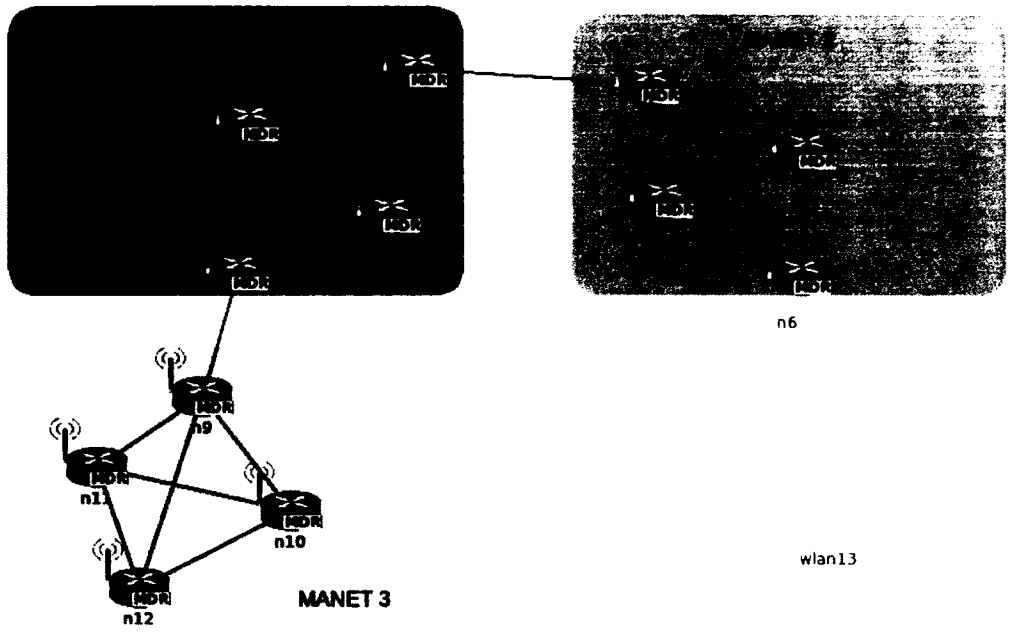

Figure 5.1 Topology at 0s of Mobility

Figure 5.1 represents the topology just before mobility is introduced into the MANETs

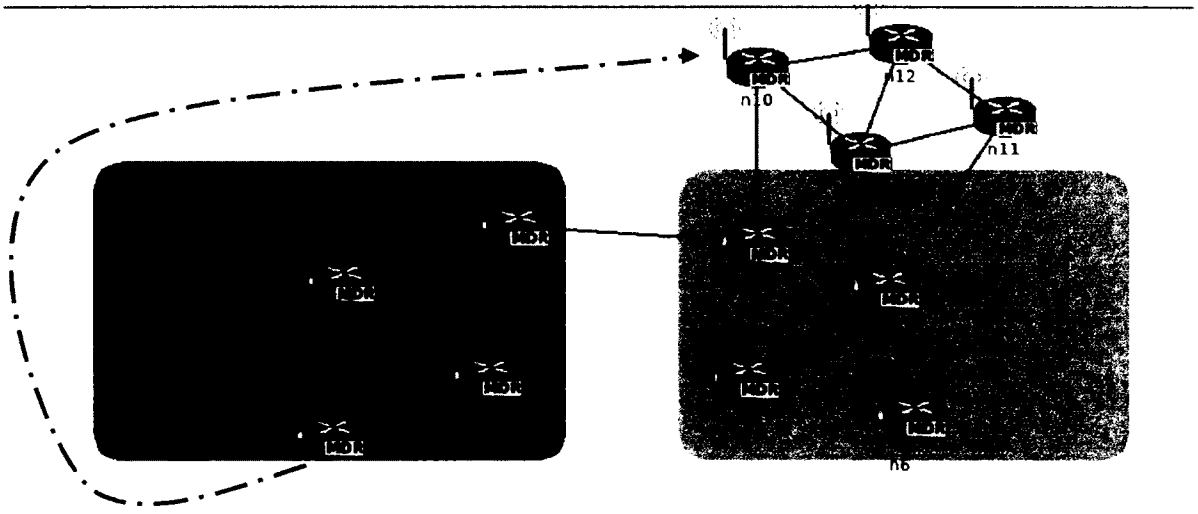

Figure 5.2 Topology at 120s of Mobility

At 120s MANET 3 moves and merges with MANET 2

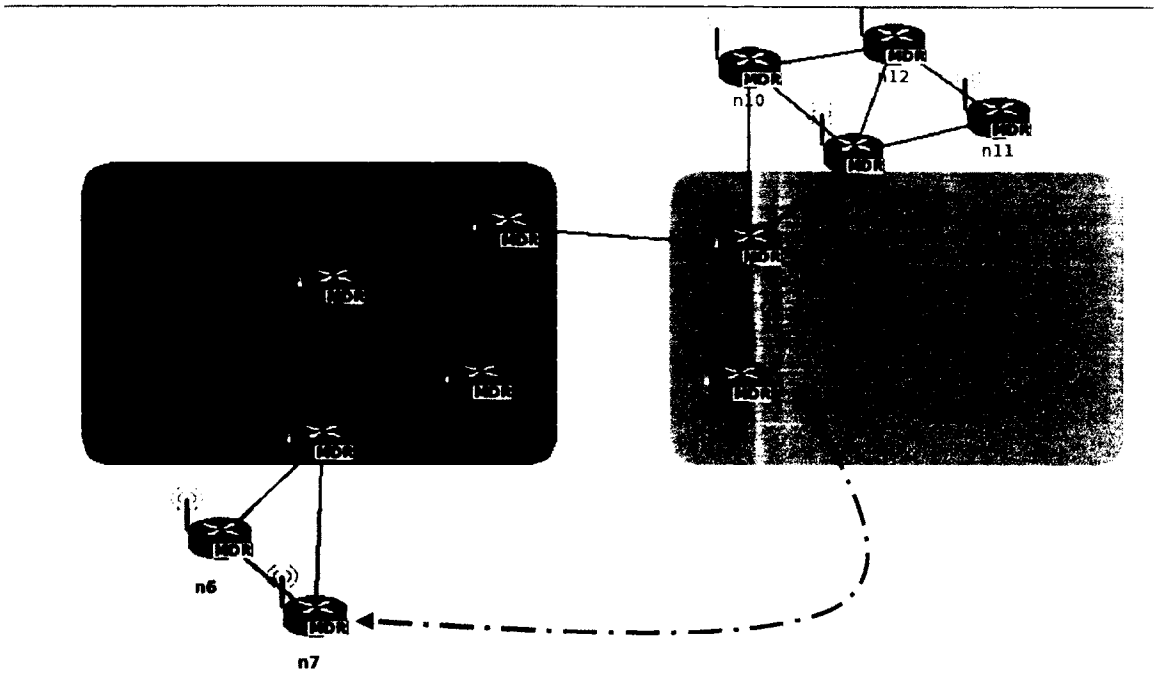

Figure 5.3 Topology at 240s of Mobility

At 240s MANET 2 splits, and routers 6 and 7 merge with MANET 1

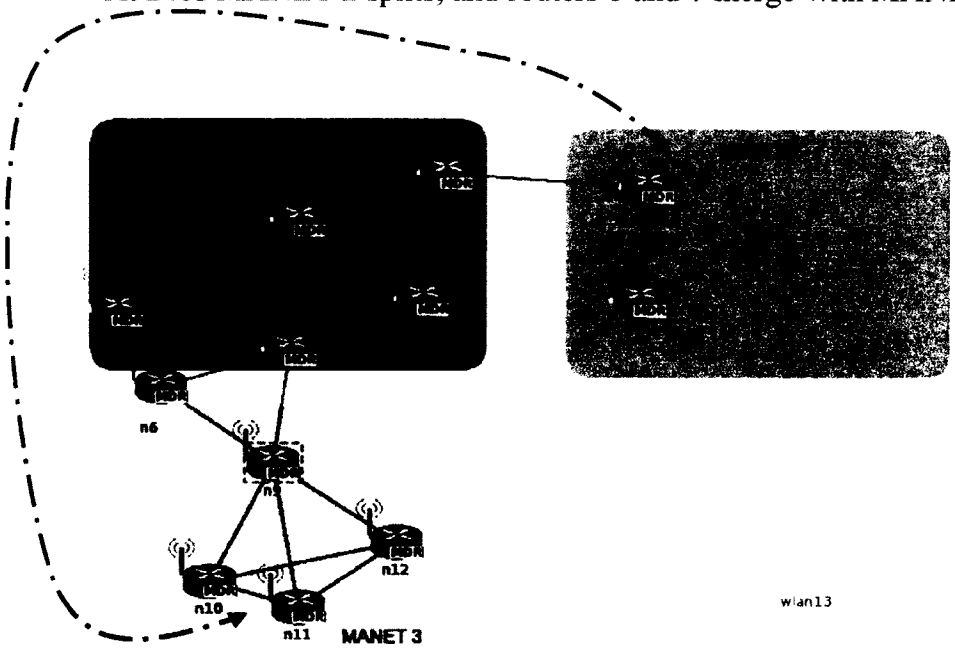

Figure 5.4 Topology at 360s of Mobility

At 360s MANET 3 moves and connects back to MANET 1

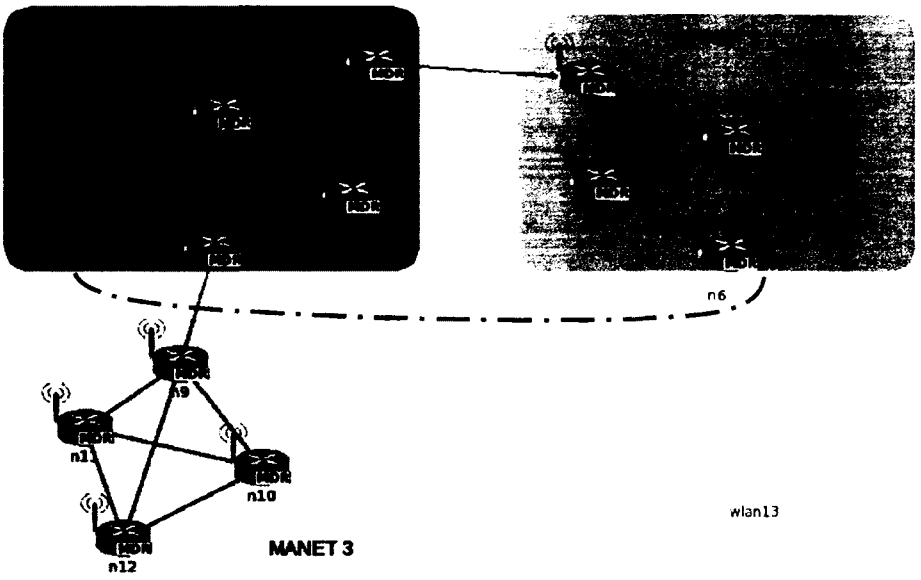

Figure 5.5 Topology at 480s of Mobility

At 480s, routers 6 and 7 merge back with MANET 2, and at 600s routers stop moving around and the simulation ends.

To analyze this network, we will be monitoring 4 ping (ICMP) Internet Control Message Protocol flows that are started when mobility is introduced in the network

1. From router 5 in MANET 2 to router 10 in MANET 3
2. From router 6 in MANET 2 to router 11 MANET 3
3. From router 1 in MANET 1 to router 12 in MANET 3
4. Within MANET 3 from router 7 to 8, since a split is occurring in that MANET

We will monitor the effects of mobility and the split and merge scenarios highlighted above on these flows. The flows are analyzed and plotted using wireshark, showing the number of packets delivered versus time. A continuous ping is sent between

the selected routers: 1 packet is sent every second; each ping packet contains 100 bytes of data.

5.1 Test-Bed Results 3: Demonstrate Need of Gateway Protocol

To reiterate how packets are dropped as routers moves within their MANET and also split and merge with other MANETs, at the start of the simulation selected routers are configured to send continuous ping packets to another router just before mobility is introduced.

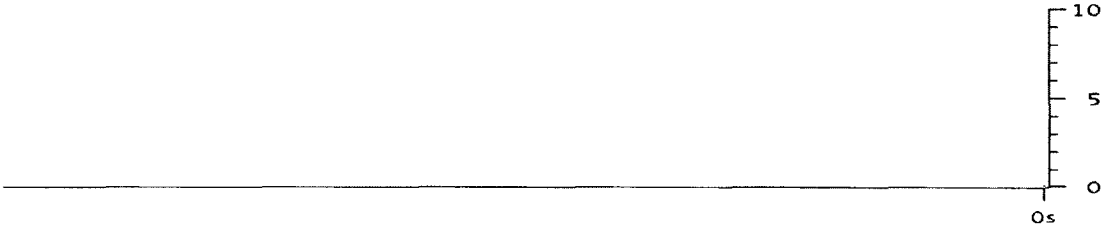

Figure 5.6 ICMP Packets between Routers in different MANETs

Figure 5.6 plots the number of ping packets delivered versus time on router 1 as pings are sent between MANETs. Because of the absence of gateways, pings between router 5 and router 10, router 6 and router 11, and router 1 and router 12 are never delivered during the entire simulation time.

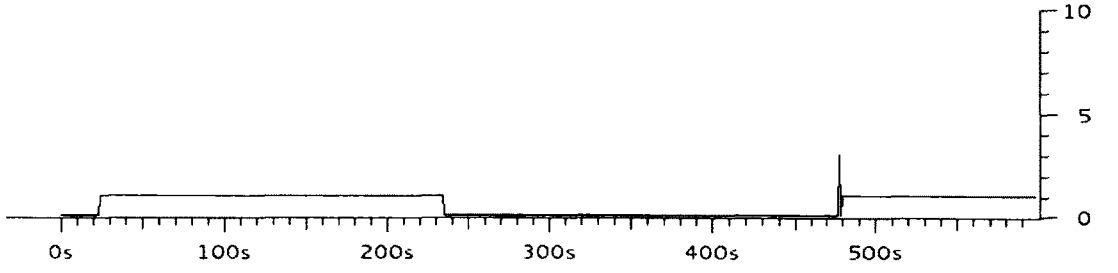

Figure 5.7 ICMP Packets between Router 7 and Router 8

Figure 5.7 plots the number of ping packets delivered versus time on router 8 as pings are sent from router 7 to router 8. We note that at the start of the simulation, pings

are delivered within MANET 2. At 240s, when MANET 2 splits, the number of ping packets delivered drops to 0. At 480s, when the routers in MANET 2 merge back together, pings are delivered again to their destination.

We can conclude from Figure 5.6 and Figure 5.7 that routes are only known within MANETs. Also, when MANET 2 splits, pings between routers 7 and 8 are not delivered. Pings between routers in different MANET are never delivered throughout the simulation time; hence routes are not shared between routers in separate MANETs because of the absence of gateways routers running a gateway protocol. In the next section we will introduce a gateway protocol and see if that solves this issue.

5.2 Test-Bed Results 4: Introducing BGP on all Routers

In this Test-Bed we configure all routers in the network with BGP. The concept of BGP as a gateway protocol has earlier been discussed in Chapter 3. The BGP keep-alive and hold-down timers are set to their default of 60s and 180s respectively. TCPdump is configured on all routers running BGP-MR; the packets collected are used to analyze packet delivery and the amount of BGP overhead using wireshark. Wireshark provides a summary of the average number of BGP control packets sent per second and the average size of each packet on each gateway router and an average is taken using all routers running BGP-MR to determine the BGP overhead.

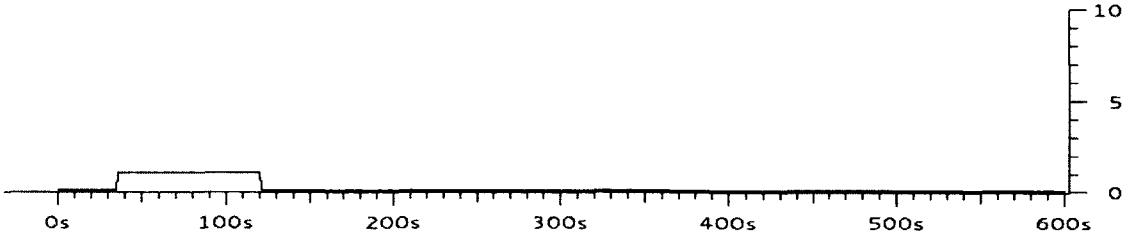

Figure 5.8 ICMP Packets between Routers in different MANETs

Figure 5.8 plots the number of ping packets delivered versus time between routers 5 and 10, routers 6 and 11, and routers 1 and 12. We see that after 120s when MANET 3 moves and merges with MANET 2, the pings are no longer delivered. Even though gateways exist between the MANETs, when BGP routers move, their BGP peers do not empty their table of that existing route entirely because they have other BGP peers still having the route in their BGP tables. Hence a new route is not established; instead the BGP table keeps the entries but changes the best next hop slot to point to a directly connected BGP peer. This causes a loop within MANETs and packets sent out never leave the MANET.

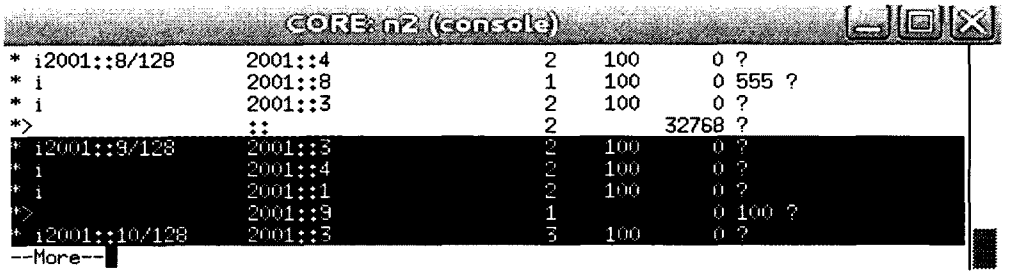

Figure 5.9 BGP Table of Router 2 at 30 Seconds

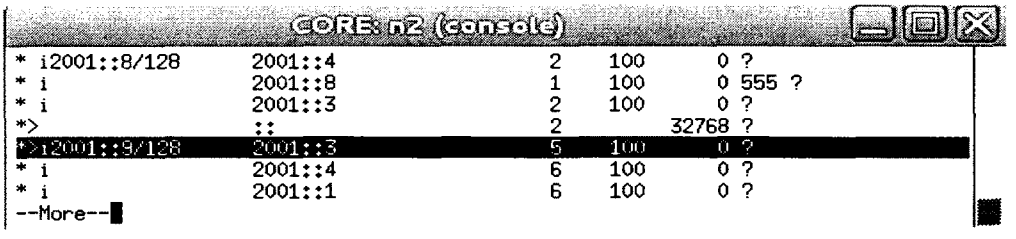

Figure 5.10 BGP Table of Router 2 at 140 Seconds

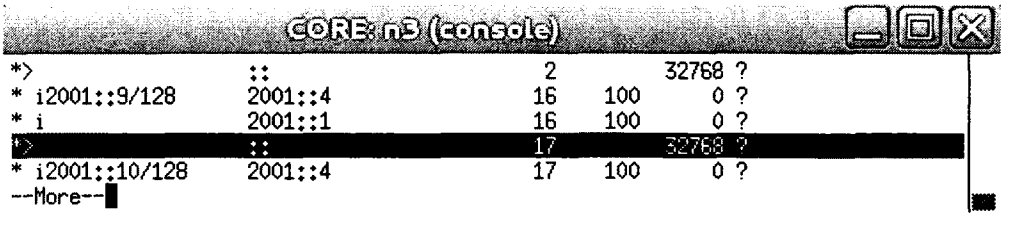

Figure 5.11 BGP Table of Router 3 at 150 Seconds

This looping behavior is explained further by showing screenshots of the BGP routing table of router 2 as MANET 3 moves and merges with MANET 2. At the beginning of the simulations, after the BGP tables have been populated, we see in Figure 5.9 that router 2 in MANET 1 shows router 9 with IP address 2001::9 as the best next hop router to router 9 which is in MANET 3, this is indicated by the ">" sign in the screenshot. After MANET 3 moves at 120 seconds, we see in Figure 5.10 that router 2 now has now chosen router 3 in MANET 2 as the best next hop router, in fact all its other options are also routers within its own MANET. We further checked the BGP table of router 3 in Figure 5.11, this shows the best next hop to router 9 as itself.

Hence when router 2 wants to send a packet to router 9, it sends it to router 3 and the packet never leaves that MANET. At the end of the simulation when the MANETs are properly re-established, the looping still persists because even though new next-hop routers are available, BGP does not change its best next hop router unless its current best-next hop router becomes unavailable.

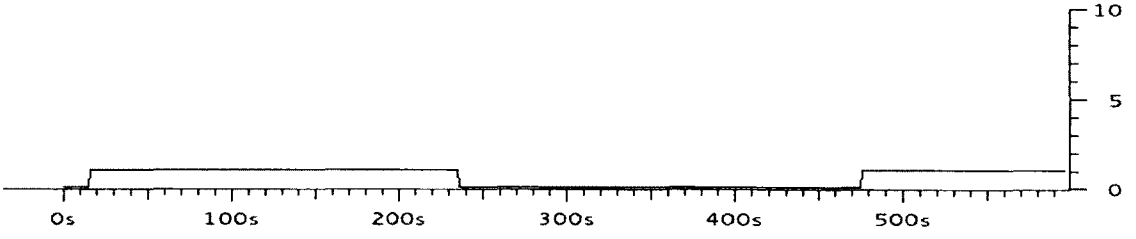

Figure 5.12 ICMP Packets between Router 7 and Router 8

Figure 5.12 plots the number of ping packets delivered versus time on router 8 as pings are sent from router 7 to router 8. We note that at the start of the simulation, pings are delivered within MANET 2. At 240s, when MANET 2 splits, as explained in Figure 5.8, the BGP tables of their BGP peers still show old routes and these routes cause the number of ping packets delivered drops to 0. At 480s, when the routers in MANET 2

merge back together, pings are delivered again to their destination because router 7 and 8 communicate with OSPF.

From Figure 5.8 and Figure 5.12, we can see that introducing gateways on all routers in the network shows improvements in packet delivery. But this is still not an effective solution as BGP is unable to handle the changing routes present in a mobile topology. The BGP overhead measured averaged 4.5 kbps when BGP was configured on all 12 routers, it should be stated that this average overhead only varies slightly from the overhead measured on individual routers.

5.3 Conclusion

In this experiment we see the effect of mobility on a network running OSPF-MDR. We plotted a TCPdump of ping packets between routers using four flows. With the absence of a gateway protocol we showed that ping packets between routers in a split MANET are not delivered as routes between sub-MANETs are not shared and ping packets between routers in separate MANET are never started.

A gateway protocol, BGP, was then introduced into the network and configured on all routers and we saw the problem of looping that might exist in a MANET environment, because routes are not totally purged from the BGP tables. BGP selects a new best next hop that introduces a loop within MANETs. The BGP overhead was also quantified and measured and seen to be at an average of 4.5 kbps. These routers are running on a bandwidth of 64 kbps, hence BGP uses approximately 7% of the bandwidth for its control packets. This number is expected to grow higher as the size of the topology increases.

A test-bed was set up configuring BGP on only selected routers that lead out of each MANET. We noticed that due to the looping caused by BGP, the ping packets delivery results are still the same as when BGP is configured on all routers in the network. However, a reduction was noticed however in the overhead to an average of 1.9 kbps which is about 3% of the available bandwidth and a significantly lower value than when enabling BGP on all routers. Introducing a gateway protocol that interconnects MANETs by dynamically enabling gateways when a MANET splits will allow sub-MANETs to exchange routes as long as a gateway is present in each separate part. This introduction of a dynamic gateway will reduce the percentage of overhead that the BGP control packets introduce into the network. The design, implementation and testing of this solution is documented in subsequent chapters.

6: BGP-MR: A Gateway Protocol for Tactical MANETs

6.1 Introduction

A border gateway routing protocol which actualizes wireless mobility features and routing abilities similar to BGP was developed from an existing C language implementation of BGP in the Quagga [17] routing suite and named Border Gateway Protocol – MANET Routing (BGP-MR). The research was aimed at creating a proof-of-concept protocol capable of handling border gateway routing tasks for continuously moving mobile routers. Taking the scenario of tactical inter-domain topology, which requires both heterogeneous and mobile features, the protocol design involved the ability to minimize routing overhead by dynamically disabling the protocol on a non-border BGP-MR router and activating the protocol for a border BGP-MR router while using OSPFv3 for routing in the fixed networks and OSPF-MDR within mobile ad-hoc network groups. The protocol was confirmed to enable several groups of mobile ad-hoc networks utilizing backbone OSPF to disconnect, connect / reconnect in reasonable time and move while doing so. In each case it was confirmed that only the minimal amount of routers necessary to establish connections between groups of ad-hoc networks were active. The protocol enabled the smart disabling and activating of BGP-MR when necessary, hence reducing routing packet overhead that might have occurred from the implementation of legacy BGP on such a network as shown in Chapter 5.

6.2 Border Gateway Protocol – MANET Routing (BGP-MR)

The protocol implementation was based on a modification of the C programming language BGP code in the Quagga [17] routing suite. The modification was aimed at adding several mobility features to the legacy BGP to allow it act as a gateway in MANETs. These features include:

i. Dynamic gateway passive election

ii. Dynamic gateway active election

iii. Gateway EBGP movement sensing

The concept behind dynamically electing gateways to become active or passive was inherited from the Inter-MR protocol [1]. Inter-MR describes a dynamic election process for gateway routers whereby potential gateways in each partition or MANET can determine whether they should become active gateways or not to maximize inter-MANET connectivity while satisfying the constraints on the number of active gateways after the topology has been changed.

Two parameters were added to BGP-MR responsible for controlling the dynamic election of BGP-MR routers, they are described in Table 6.1.

Parameters	Description
Post Interval	Minimum Interval for beacon exchange for EBGP neighbors, default is 10 seconds
Wait Count	Minimum number of beacons sent for a BGP peer to decide to become active or passive, after a topology change with a directly connected EBGP peer, default is 5

Table 6.1 BGP-MR Parameters

BGP HEADER
Beacon

BGP HEADER
Notification

Figure 6.1 BGP-MR Message Format

Figure 6.1 shows the structure of the 2 BGP-MR Messages sent between peers to maintain BGP relationships and to notify each other of a change in topology. These messages contain the fixed size legacy BGP header with the type slot set to 6 indicating that a BGP-MR packet is affixed. The 2-byte notification slot notifies an IBGP peer when a BGP-MR router turns active/passive while the beacon is also a 2 byte message sent between EBGP routers to maintain peer relationships.

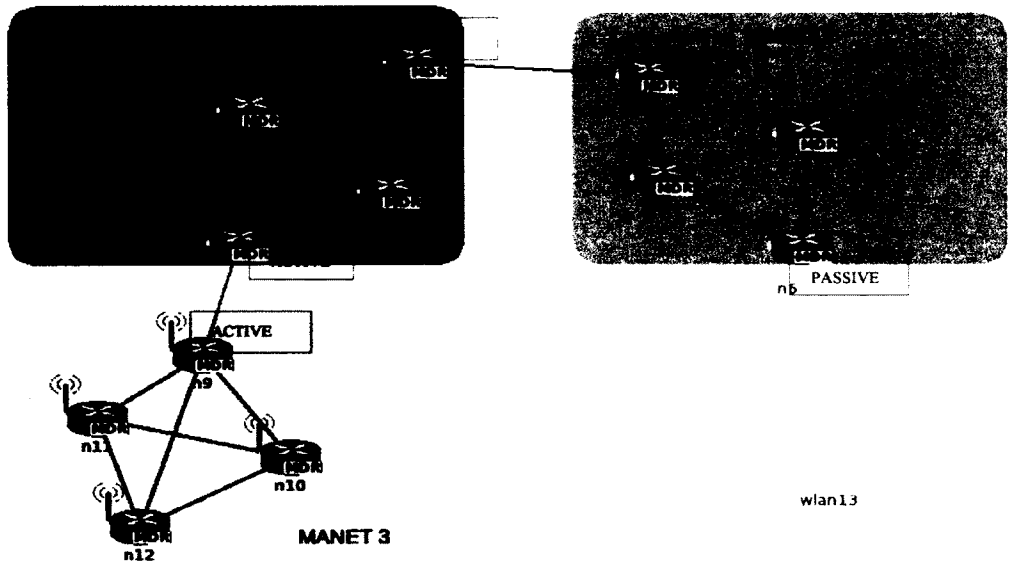

Figure 6.2 Dynamic Election of Gateways

The dynamic election is such that only routers that are directly connected to an EBGP peer become active as a BGP-MR router, this is best explained by Figure 6.2, which shows a scenario of 3 MANETs connected with gateways. Routers 2, 4, 5, 6 and 9 have been configured as BGP-MR gateways; MANET 1 and MANET 3 are connected by

the EBGP relationship of router 2 and router 9, hence both gateways are active, MANET 1 and MANET 2 are connected by the EBGP relationship of router 4 and router 5, hence both gateways are active. Router 6 is not connected to any EBGP peer so it elects itself as a BGP-MR passive router and just listens for BGP beacons in case any EBGP peer comes within its wireless range. Once an EBGP peering is lost and another EBGP router is not found, the current BGP-MR router waits the post interval time and then elects itself as a passive BGP-MR router.

A passive BGP-MR router still listens for beacons around its one hop external Autonomous System (AS) environment so that it can become active if another EGBP peer becomes available due to mobility. It should be noted that a passive BGP-MR router does not participate in the BGP routing process; hence this reduces the overhead within the network when it is passive.

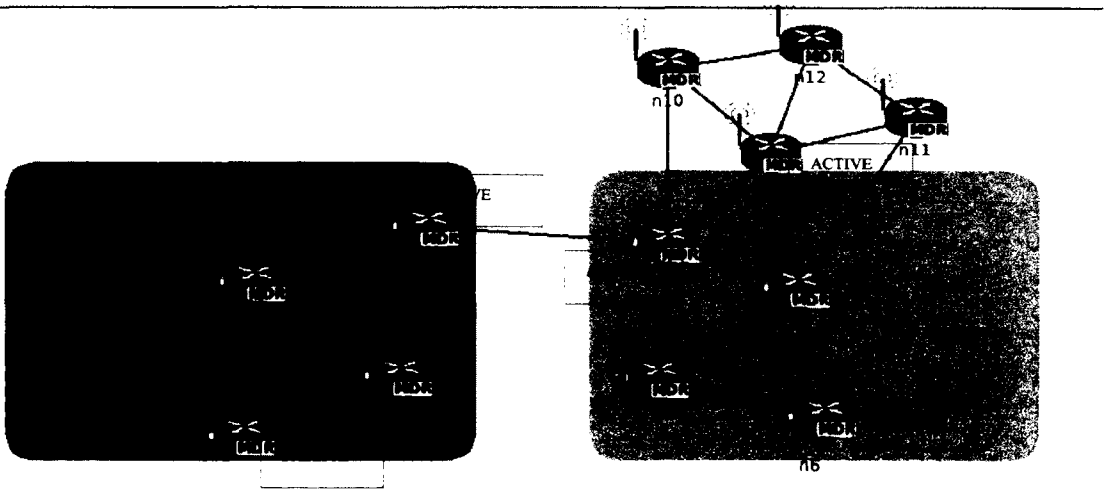

Figure 6.3 Dynamic Election of Gateways II

In Figure 6.3, MANET 3 merges with MANET 2; hence router 2 loses its EBGP neighbor and elects itself to turn into a passive router. When the connection to an EBGP

peer is lost, a router sends a recursive beacon to all its IBGP and EBGP peers to alert them of the loss of that route and instructing them to purge their BGP routing tables of all routes to that network address and repopulate the routing table. These peers in turn send the beacon to purge to their own BGP-MR peers, hence the idea of a recursive beacon. In Figure 6.3, router 2 will broadcast a recursive beacon through router 1 and router 4 instructing its neighbors to purge their tables of all routes to router 9. This process eliminates the problem of looping seen when running legacy BGP in a MANET environment, where a route to a router that has moved away is not totally purged, rather a best-next hop neighbor is selected.

At this point, the gateway selection process does not attempt to minimize the number of active routes. If router 7 had been originally configured as a BGP-MR router, in Figure 6.3 when MANET 2 merges with MANET 3, router 7 as well as router 5 will stay active, even though only one of the two is required to connect MANET 2 and MANET 3. Designing smart algorithms to reduce the number of active BGP-MR routers is left for future work, but is non-trivial. In the above example, the choice between router 5 and router 7 is not arbitrary: Router 5 also interconnects MANET 2 with MANET 1, so it would be a better choice than activating router 7 (which results in having to activate router 5 as well).

Selecting how many routers in a MANET should be configured as gateway will be a tradeoff between security policies and the designed scenario. The number should be such that all routers have a means of communicating with neighboring MANETs, but must also take into consideration the size of the topology to reduce the BGP-MR

overhead generated. Some new commands have also been introduced into BGP-MR to assist the MANET routing process:

Commands	Description
bgp MANET enable	Enables BGP-MR on a router, in router configuration mode
bgp MANET post-interval <10-60>	Sets the post interval time in router configuration mode
bgp MANET wait-count <5-15>	Sets the wait count in router configuration mode
show bgp MANET	Shows the MANET status of a BGP router, whether active or passive
show bgp MANET post-interval	Shows the configures post interval and wait count time
show bgp mactive/mpassive	Forces a BGP-MR router to become active/passive (used for debugging purposes)

Table 6.2 BGP-MR Commands

6.3 Methodology

Since the original implementation of the BGP routing protocol involves the use of a Finite State Machine (FSM), the modifications made were designed to integrate into the state machine requiring only slight modifications to objects used such as the peer and table systems. However, the mobile ad-hoc features will be required to be active irrespective of the passive or active status of the underlying FSM. Hence, using a parallel thread feature, a scanning procedure to perform mobile ad-hoc networking which includes scanning for IBGP and EBGP peer movement, the ability to dynamically turn a BGP-MR router passive or active and the sending of beacon notifications was developed.

The main BGP-MR process circulates around establishing and maintaining BGP-MR peer relationships using beacons, dynamic gateway elections and expired routes cleanup, this process is controlled by the BGP-MR manager which contains the counts and flags that handle the current status of all devices running BGP-MR; the flags and counts used in the main BGP-MR process are described below:

BGP MANET status flag	Shows the status of a configured BGP peer
Restart flag	Status is used to know when to restart thread
MANET open flag	Is set when a BGP-MR router turns automatically active
BGP peer last reset flag	Determines activation or deactivation of IBGP peer relationships
Peer status count	Number of peers that can be seen from the table
EBGP peer status count	Number of EBGP peers that can be seen from table
EBGP seen peer count	Number of EBGP peers that a router is directly connected to

Table 6.3 BGP Manager

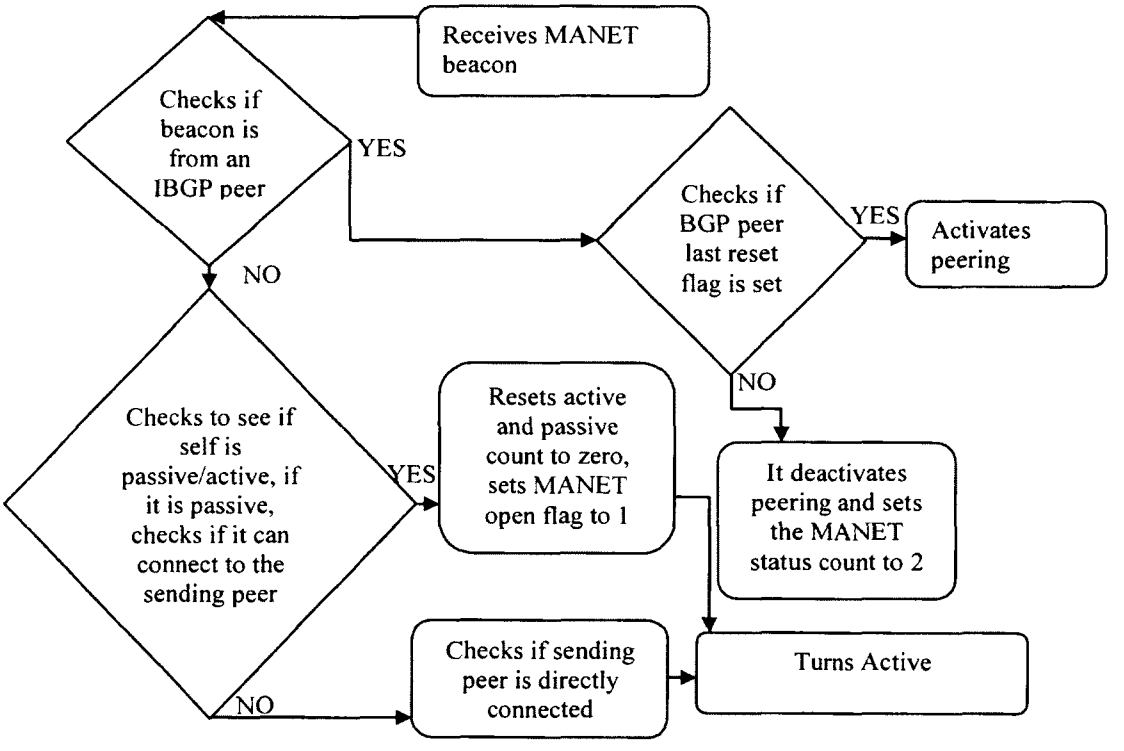

Figure 6.4 Beacon Handling Process

Figure 6.4 shows what happens when a BGP-MR router receives a beacon from a neighbor. The neighbor relationship established using beacons differs when the sending router is an EBGP or an IBGP neighbor, IBGP neighbors send beacons to notify each other when they are turning active or passive, while EBGP neighbors exchange beacons to maintain relationships and take decisions on whether to turn active or passive.

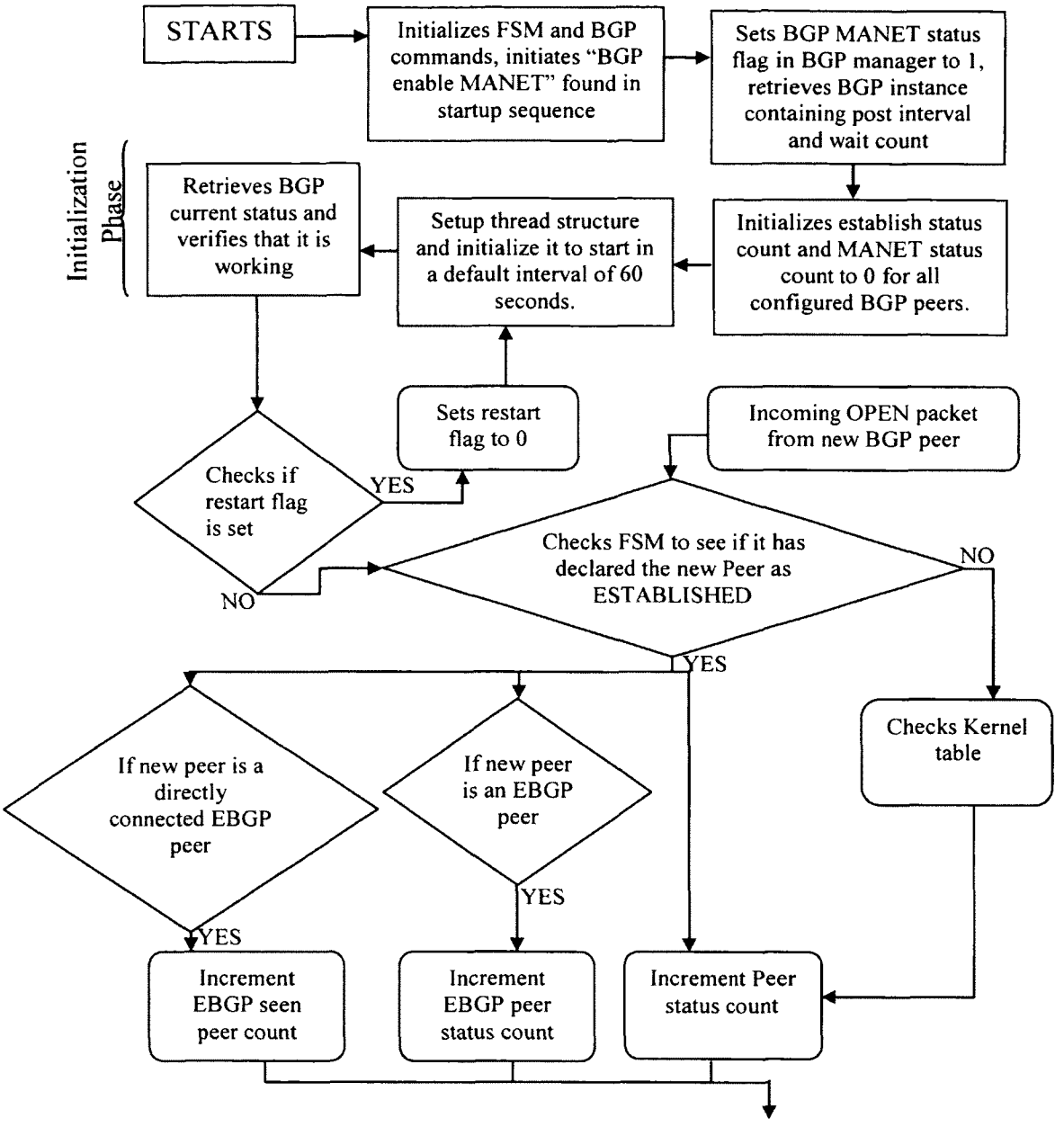

Figure 6.5 BGP Initialization phase

Figure 6.5 gives a high level description of what happens when the MANET process is started on a BGP-MR router; the BGP commands and parameters are initialized. It explains the conditions for incrementing the counts when an OPEN packet is received from a BGP peer; the counts are incremented when a known entry exists in either the BGP routing table or the zebra kernel table for that peer. The arrow continues into Figure 6.6.

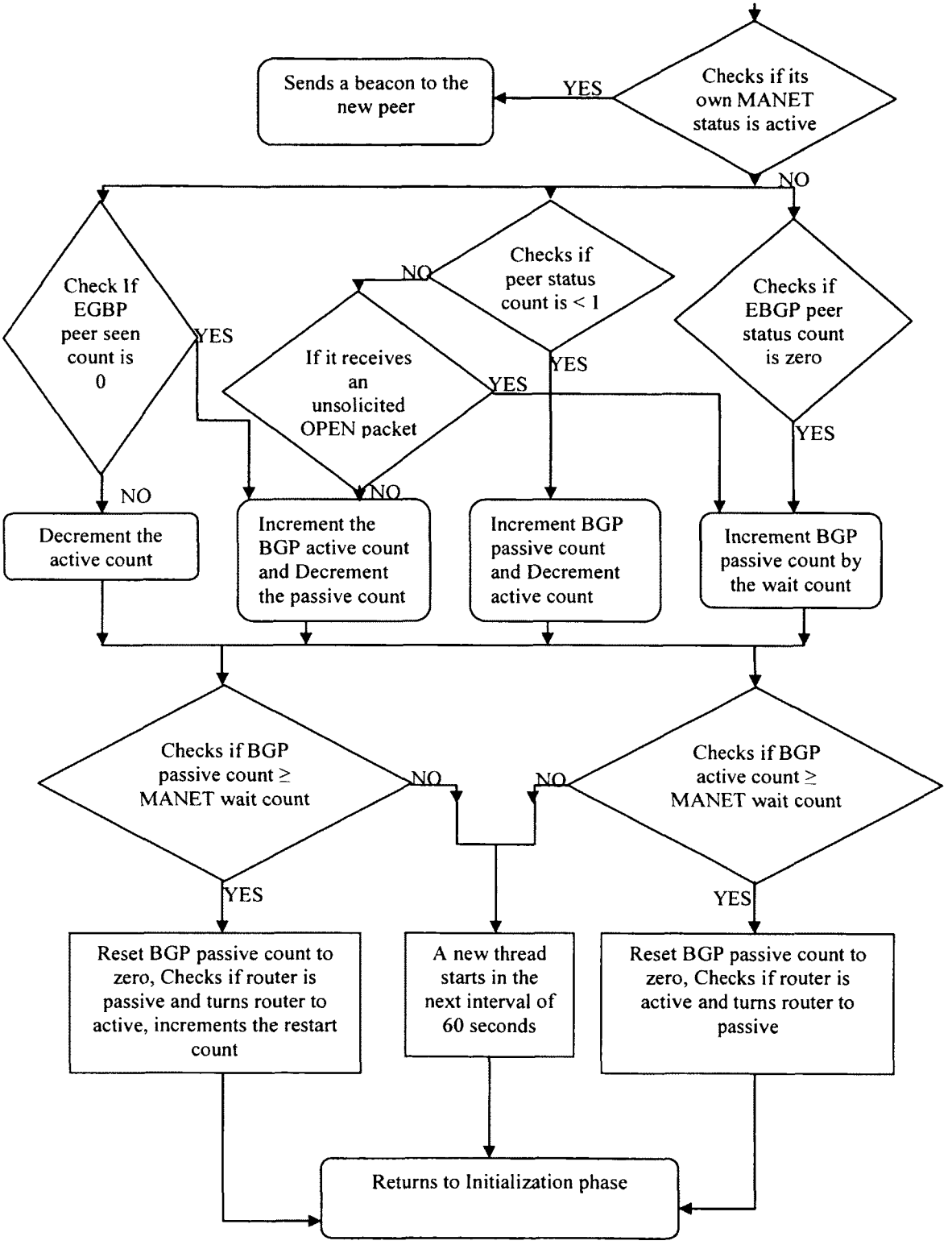

Figure 6.6 BGP-MR Dynamic Election Process

Figure 6.6 expatiates on the dynamic election process and the conditions that guide turning the BGP-MR instance active or passive on a selected router. A BGP-MR router turns active when the BGP passive count is greater than or equal to the wait count; the opposite is true for turning passive when the BGP active count is greater than or equal to the wait count, the active and passive count are incremented and decremented based on the value of the peer status count, the EBGP status peer count and the EBGP seen peer count described in Table 6.4, these three counts are incremented or reset based on respective peer relationships as described in Figure 6.5.

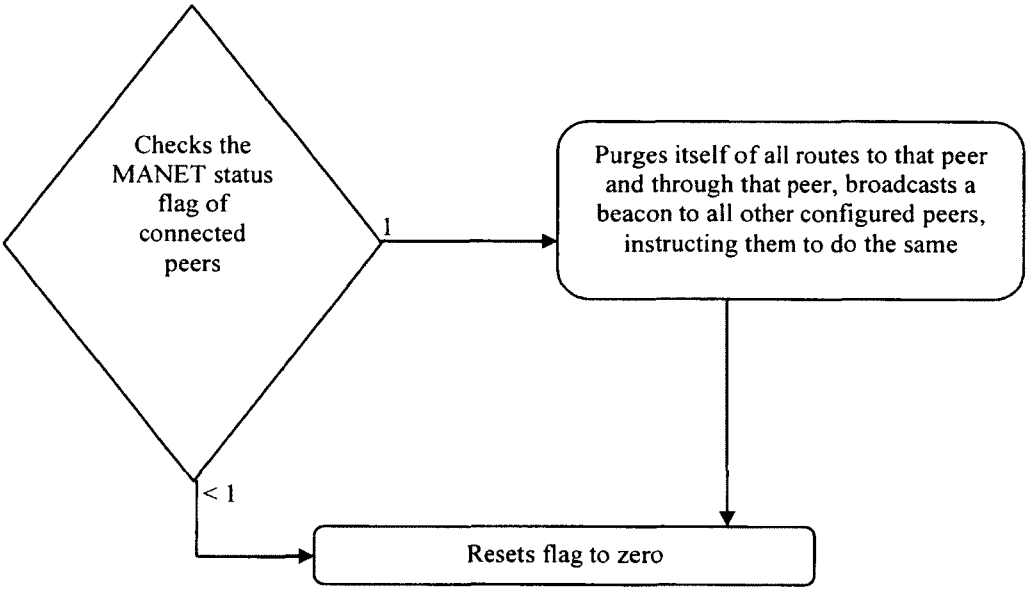

Figure 6.7 BGP Expired Routes Purging Process

Figure 6.7 explains how expired routes are purged from a BGP-MR routing table. Depending on the MANET status flag of connected peers, a router takes the decision to purge a route from its routing table. If the status flag is set to 1, all routes to and through that peer are purged from its routing table, and a recursive beacon is sent to all connected neighbors instructing them to do the same.

7: BGP-MR Test-Bed Results

The proposed gateway routing protocol BGP-MR is tested to see if it solves the problem statements and the issues highlighted in Chapter 5. First we introduce BGP-MR into the scenario of 12 routers earlier described and measure the number of packets delivered as ping packets are sent across selected routers and the percentage of bandwidth that the BGP-MR control packets utilize during the simulation time. Then we will introduce BGP-MR into a larger MANET scenario of 200 routers, comprising of a fixed network and multiple MANETs to see if we have provided an adequate inter-domain routing solution that provides seamless communication between both domains.

7.1 Test-Bed Results 5: Introducing BGP-MR on Gateway Routers

The scenario described in Test-Bed 3 is reintroduced for the testing of BGP-MR, all the earlier parameters and configurations specified for BGP and OSPF stay the same and "bgp MANET enable" is added to enable BGP-MR on the router, BGP-MR is configured on selected gateway routers 2, 4, 5, 6 and 9; new BGP-MR parameters have been added.

Post Interval	10 seconds
Wait Count	5

Figure 7.1 BGP-MR Parameters

The red vertical lines in the figures below indicate the start and end times where physical disconnection happens within the topology due to mobility, at this point it is impossible to deliver packets to disconnected routers. We should also point out that when routers reconnect after movement, BGP can take about 10 seconds to repopulate its routing tables this population is recursive, and routers farthest from the point of reconnection populate their routing tables last, just like when the routes are purged from

the tables. Also, if one of the BGP peers was inactive, it might take up to 40 seconds to reconnect.

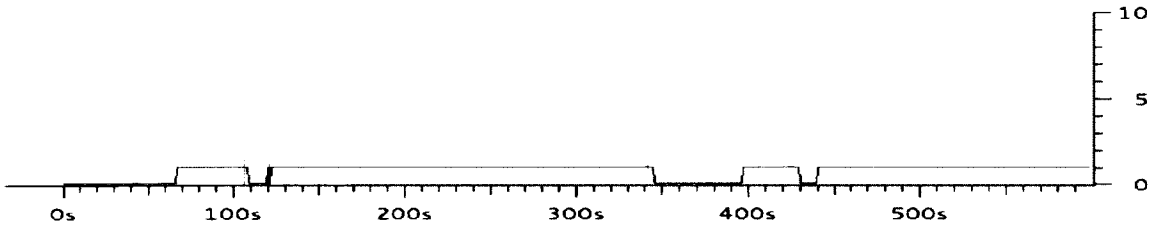

Figure 7.2 ICMP Packets between Router 5 and Router 10

Figure 7.2 shows number of ping packets delivered on router 10 as 1 ping packet is sent continuously between router 5 and router 10. We see a drop to 0 packets at 110s when MANET 3 moves and a rise back to 1 packet as MANET 3 merges with MANET 2 at 120s, this is repeated at 350s when MANET 3 starts to move back to its initial position.

The time it takes to recover at 370s is longer because BGP-MR has gone passive on router 2, when router 2 sees BGP packets from router 9 it becomes active and BGP-MR peering is done. At 430s we notice a short drop in the number of packets delivered even though the physical connectivity exists and a route has already been established between both routers, this could be due to the change in the network again when router 6 and 7 move at 420s, further analysis of this spurious connectivity problem can be analyzed in future works.

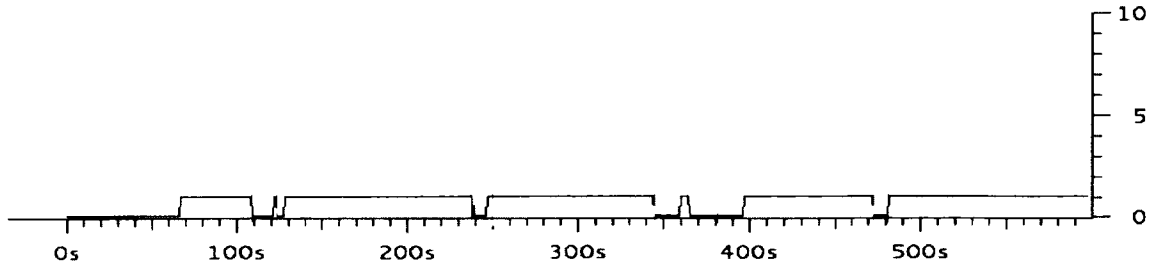

Figure 7.3 ICMP Packets between Router 6 and Router 11

Figure 7.3 shows the number of packets delivered on router 11 as 1 ping packet is sent continuously between router 6 and router 11. The number of packets drops down to 0 at 110s when MANET 3 moves and goes back up to 1 at 120s when MANET 3 merges with MANET 2, this happens again around 240s when router 6 and router 7 split from MANET 2, also at around 360s when MANET 3 returns to its initial position, and around 480s when router 6 and router 7 merge back with MANET 2. At 360s we notice a rise in the number of packets delivered as no physical connection actually exists. We speculate that this could be from routes that are cached in the kernel table, but further analysis of this phenomenon was not done.

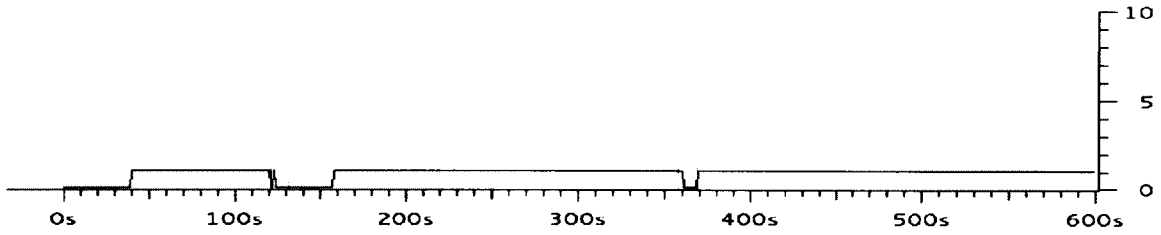

Figure 7.4 ICMP Packets between Router 1 and Router 12

Figure 7.4 shows the number of packets delivered on router 12 as 1 ping packet is sent continuously between router 1 and router 12. Again, a drop in packets delivered is noticed when MANET 3 moves to merge with MANET 2 at 120s. It takes a while for the route to come back up, as there are more hops between router 1 and router 12 than between most other routers. At 360 seconds we notice another drop as MANET 3 returns to the initial position, this is a much shorter down time because the number of hops between router 1 and 12 has significantly reduced.

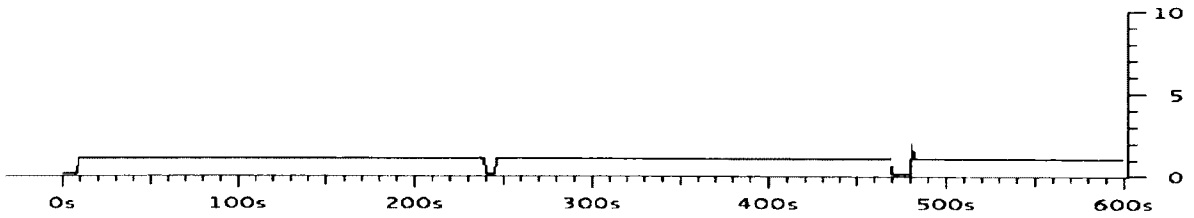

Figure 7.5 ICMP Packets between Router 7 and Router 8

Figure 7.5 shows the number of packets delivered on router 8 as 1 ping packet is sent continuously between router 7 and router 8. We notice a drop when router 6 and router 7 split from MANET 2 around 240s and another when they merge back around 480s. These drop times are unavoidable because they are due to physical disconnection.

The average bandwidth that BGP-MR control packets utilize was measured to be 0.45 kbps which is 0.7% of the total bandwidth, an improvement from the 7% we saw when running BGP. This average was taken over the 5 routers configured with BGP-MR, there is not a lot of variance between the individual overheads of each router and the average taken over all.

7.2 Test-Bed Results 6: Inter-domain Routing with BGP-MR

In this test-bed, BGP-MR is introduced in a topology of 200 routers, 60 of the routers form a headquarters fixed network running OSPFv3, while the other 140 running OSPF-MDR are split into 5 MANETs of 25 routers each and a 6^{th} having 15 routers. The scenario used for this topology as well as its mobility model was developed by CRC to emulate a real life tactical scenario, it covers an area of 7500X1500 meters and the WLAN is configured with a wireless range of 200 meters.

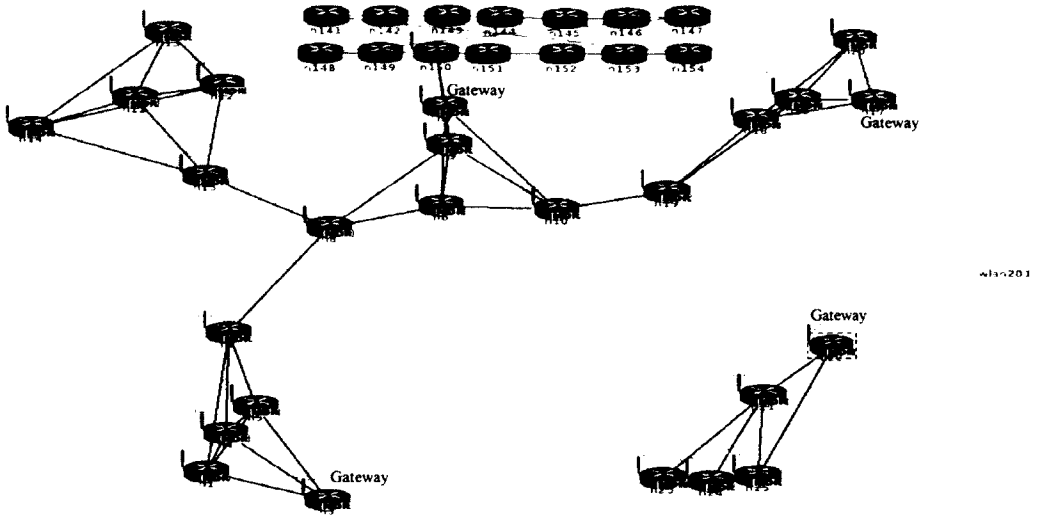

Figure 7.6 Cross-Section of 200 Router Inter-domain Topology

The fixed network has been configured with 4 gateway routers; each MANET has between 2 to 4 gateways depending on its position in the topology. There are a total of 26 gateways in the topology and 39,800 routes. Figure 7.6 is a cross section of the topology, showing a MANET of 25 routers connected to a section of the fixed network, the MANET shown has 4 gateways configured, one is currently connected to the fixed network, while the others connect some other MANETs not shown, and other MANETs are setup the exact same way. During the scenario, groups of 5 routers within a MANET partition and merge with a neighboring MANET, routers selected as gateways depend on the structure of the topology; this has been earlier discussed in Chapter 6.

The simulation is run for a total of 40 minutes and statistics are recorded from 20 minutes since it was earlier shown in Chapter 4 that OSPF converges after 20 minutes. All configurations for BGP-MR and OSPF are still the same as in previous test-beds. The statistics collected model those of Chapter 4 to show BGP-MR's performance when compared to BGP in a large scale inter-domain MANET scenario, the scenario includes

MANET partitions and merging and constant mobility; at the end of the simulation, the percentage of overhead will also be compared.

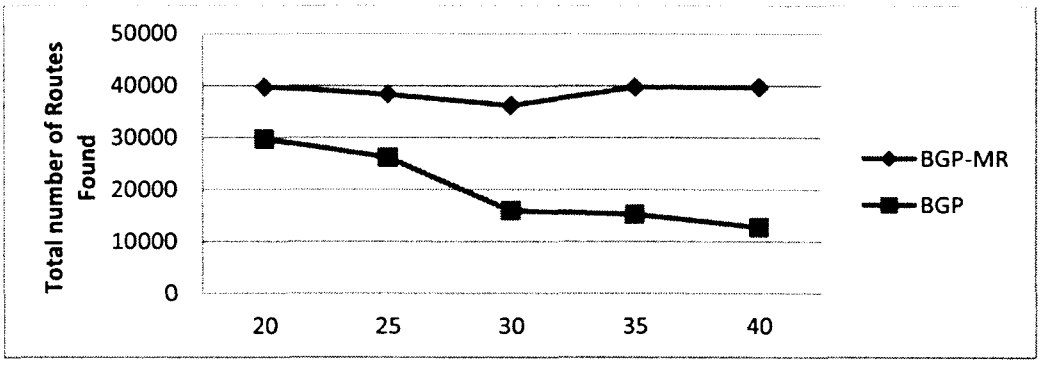

Figure 7.7 Total Number of Routes Found

Figure 7.7 shows the total number of routes found as time progresses in the simulation. We observe that neither BGP-MR nor BGP find the complete total of 39,800 routes, this can be attributed to the mobile nature of the topology as routes are constantly changing. However, BGP-MR finds close to the total number of routes as at 35 and 40 minutes, we see that the total number of routes found when BGP-MR is used is 39,720 and 39,687 respectively, this is over 99.7% of the total number of routes when the network is assumed to be fully connected. BGP, on the other hand, is steadily declining in the number of routes found, as at 40 minutes, just around 32% of routes are seen. This is because the BGP overhead was too much for the bandwidth provided of 64 kbps, hence some BGP packets stopped flowing and routes were not populated. The BGP control packets were measured to consume 55.68 kbps which is about 87% of the total bandwidth, compared to the average bandwidth that BGP-MR control packets utilize which was measured to be 8.9 kbps i.e. 14% of the total bandwidth.

This average overhead was collected using wireshark on each of the 26 routers running BGP-MR. Because of the ability of routers to go passive, there is some variance

between the average overhead and the individual overhead measured on some of the routers. Routers that are active for the most of the simulation have higher BGP-MR overhead than the ones that become passive at some points in the simulations because the passive routers are not sending BGP control packets while they are inactive. In this topology, even though routers that were active for most of the simulation measured as high as 20 kbps, it should be pointed out that most routers measured around the average range of 8.9 kbps.

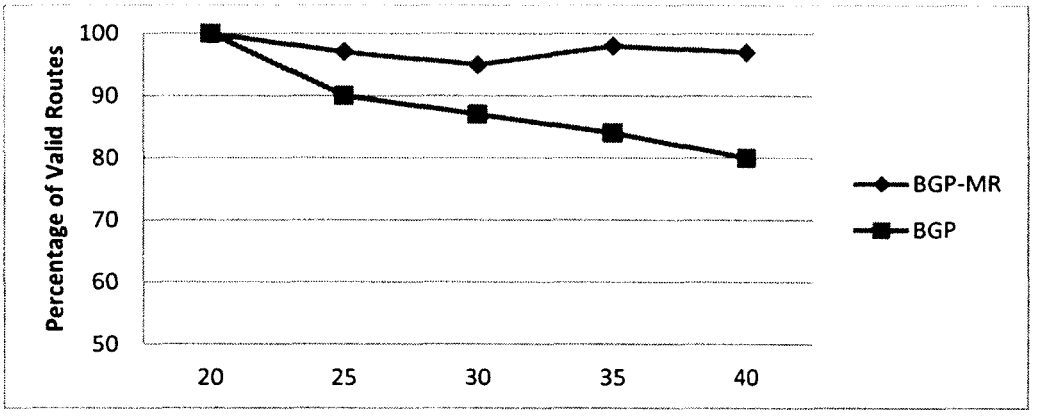

Figure 7.8 Percentage of Valid Routes Found

Figure 7.8 shows the percentage of valid routes found, we notice here that BGP-MR remains above the 95% percentile throughout the simulation while BGP declines as the simulation progresses. This can be attributed to the loops formed in BGP that renders some routes invalid as time advances and mobility continues.

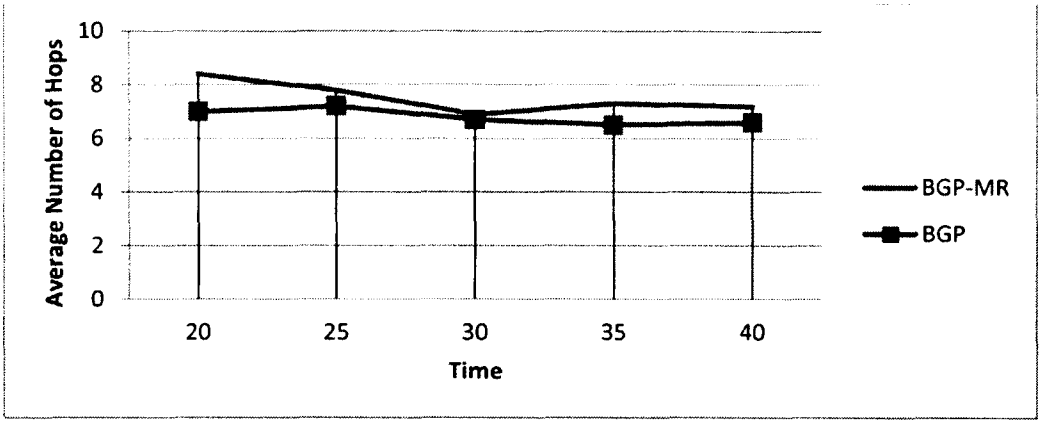

Figure 7.9 Average Number of Hops

Figure 7.9 shows the average number of hops as the simulation progresses, the average number of hops is around 7 hops. It should be noted that the average number is calculated with only the valid routes that exist at that particular time, for emphasis sake, the highest number of hops present in both topologies was 15 hops.

The optimal average path length when Dijkstra's algorithm has been applied on the starting topology is measured and compared with the average path length at 20 minutes, which is just before mobility begins to obtain the stretch factor. The optimal average path length was measured to be 6.1, while the average path length at 20 minutes when running BGP-MR is 8.4 hops, indicating a stretch factor of 1.37. The increase in average path length of about 37% shows that shorter routes between the nodes in the MANETs and the core network exist and might be achieved if different routers are selected as gateways, this concept can be analyzed further in future works.

7.3 Conclusion

In Test-Bed 5, we notice that the problem of looping has been solved because BGP-MR contains a feature that automatically causes the recursive purging of an IP address of a BGP-MR router that ends a peer relationship from the BGP routing table of its peers, so that a new route can be populated, thereby avoiding looping. We also observe that BGP-MR can take up to 40 seconds to reconnect when a node has to turn from passive to active; this is indicated by drops in the delivery of ping packets even after nodes are physically connected.

In Test-Bed 6 we introduce BGP-MR into a large inter-domain topology of 200 routers running OSPF; we compare the results with legacy BGP and demonstrate that BGP-MR finds more valid routes than BGP with less overhead of just 14% of available bandwidth, compared to BGP's overhead of 87% of available bandwidth.

8: Conclusion and Future Work

This chapter concludes the thesis; the first section provides some final conclusions on the results obtained in Chapter 7 with regards to solving the problem statements, while the second section outlines suggestions for future work with regards to implementation and testing.

8.1 Conclusion

Interest in inter-domain routing is starting to rise because of its application in military and vehicular networks. Mobile ad-hoc networks (MANETs) ensure that there is efficient and seamless communications in dynamic operation environments such as tactical military networks or emergency operations for disaster recovery. In these types of situations, networks in different administrative domains need to communicate and to achieve common goals while still maintaining their administrative policies that govern the separate networks.

The main objective of this thesis was to provide a routing solution for a large scale tactical inter-domain network containing multiple MANETs and fixed networks. The solution provided had to take into consideration the size of the inter-domain network in terms of a scalable routing protocol that converges; the mobility present in the MANETs that produce partitioning and merging of networks and might introduce packet losses across the topology and interconnecting more than one MANET.

We proposed a routing solution that utilizes OSPF as a scalable routing solution for an inter-domain network, since it has variants that can work in both the fixed and MANET environment. We tested OSPF-MDR, a variant of OSPFv3 for MANETs and

showed that after 20 minutes, the network of 200 routers running OSPF-MDR was seen to converge with all routers finding the shortest valid route to all other routers in the network. In this thesis, a proposal for a gateway protocol, BGP-MR, has been designed and implemented; it is a variant of BGP that supports dynamic election of gateways to enable BGP to function optimally in a mobile network. We introduced the concept of expired route purging to solve the looping problem in BGP, and then tested the solution using ICMP packet delivery. The results showed that BGP-MR overcame the problem of looping. To show that the problem statements have been solved, we implemented an inter-domain test-bed using OSPFv3 in the fixed network, OSPF-MDR in the MANETs and BGP-MR in the gateways connecting the different domains. We collected a number of performance metrics and compared the results with the one obtained from running legacy BGP. The results showed that the routing solution provided seamless communication despite the presence of mobility.

8.2 Future Work

One major improvement that can be made to this solution is to research further into BGP timers and how that can influence faster BGP neighbor peering, to reduce the down time noticed when new peers are formed. We were limited by the implementation of Quagga in CORE as not all timers have been integrated into Quagga's version of BGP. Quagga and CORE are both beta stage open source software that are being updated by researchers and volunteer workers; newer developments in Quagga might help improve the downtime and ensure faster convergence for both OSPF-MDR and BGP-MR. This thesis was developed and tested using Quagga 0.99.20mr2.1 running on CORE version

4.3, and as the thesis drew to an end those versions were updated with CORE 4.4 and Quagga 0.99.21mr2.2. It would be beneficial to test this routing solution using a test-bed of real routers to utilize proper processing speed and bandwidth limitations (sharing of the wireless media, for example) and to verify that the emulation results can also be obtained in a real test-bed. Selecting the optimal routers as gateways is another aspect of this solution that was not analyzed in detail, from the stretch factor of average path lengths earlier calculated, we see that shorter routes can exist if different routers are selected as gateway, depending on the policies guiding the inter-domain network and structure of the topology, this is a concept that can be further analyzed.

The scope of this thesis centered around finding a routing protocol for a large scale inter-domain network, simulations ran where limited to a 200 router network due to the case study provided by CRC, it should be noted that simulations were also ran on smaller networks of 50 and 100 routers with successful results. It is assumed that when the number of routers increase above 200, the proposed solution will still produce successful results, since each MANET exists within its own subnet and is independent of the total number of routers, problems may arise when two or more populated MANETs merge to form a very large MANET; this has not been analyzed in this thesis and will be an interesting concept for future works.

References

[1] C.K. Chau, J. Crowcroft, K.W. Lee, and S.H. Wong. "InterMR: Inter-MANET Routing in Heterogeneous MANETs," in Proceedings - IEEE International Conference on Mobile Ad-hoc and Sensor Systems MASS. September, 2010.

[2] P. Spagnolo, T. Henderson, "Connecting OSPF MANET to Larger Networks," in Proceedings - IEEE Military Communications Conference MILCOM. IEEE, October, 2007.

[3] S. ul-Arfeen, S. Musavi, M. Shah, N. Kanwal, "Cross Domain Contour of AODV over OSPFv3 in Heterogeneous Ubiquitous Networks Using Internet Gateway," Australian Journal of Basic and Applied Sciences 4(9), pp 4509-4521, 2010

[4] G. Pei, P. Spagnolo, S. Bae, T. Henderson, and J. Kim, "Performance Improvements of OSPF MANET Extensions: A Cross Layer Approach," in Proceedings - IEEE Military Communications Conference MILCOM. IEEE, October, 2007.

[5] J. Fang, T. Goff, and G. Pei, "Comparison Studies of OSPF-MDR, OLSR and Composite Routing," in Proceedings - IEEE Military Communications Conference MILCOM. IEEE, November, 2010.

[6] M. Kaddoura, B. Trent, R. Ramanujan and G. Hadynski, "BGP-MX: Border Gateway Protocol with Mobility Extensions" in Proceedings - IEEE Military Communications Conference MILCOM. IEEE, November, 2011.

[7] G. Carl, S. Arbiv and D. Ward, "Performance of BGP among Mobile Military Networks," in Proceedings - IEEE Military Communications Conference MILCOM. IEEE, November, 2011.

[8] T. Henderson, P. Spagnolo, and G. Pei, "Evaluation of OSPF MANET Extensions", Technical Report D950-10897-1, Boeing Phantom Works http://hipserver.mct.phantomworks.org/ietf/ospf, July 2005.

[9] R. Ogier and P. Spagnolo, "Mobile Ad-hoc network MANET Extension of OSPF using Connected Dominating Set CDS flooding," RFC 5614, August, 2009.

[10] A. Roy and M. Chandra, "Extensions to OSPF to Support Mobile Ad-Hoc Networking", RFC 5820, March 2010.

[11] E. Baccelli, P. Jacquet, D. Nguyen, and T. Clausen, "OSPF Multipoint Relay (MPR) Extension for Ad-Hoc Networks", RFC 5449, February 2009.

[12] J. Moy, "OSPF Version 2", STD 54, RFC 2328, April 1998.

[13] R. Coltun, D. Ferguson, J. Moy and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

[14] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[15] D. Meyer, and K. Patel, "BGP-4 Protocol Analysis", RFC 4274, January 2006.

[16] CORE (Common Open Research Emulator) Manual http://pf.itd.nrl.navy.mil/core/core-html/, last accessed 11/11/2012.

[17] Boeing Quagga Software http://hipserver.mct.phantomworks.org/ietf/ospf/releases/080602_release-1.01/ospf6d-boeing.pdf , last accessed 11/11/2012.

[18] The Zebra Routing Suite http://zebra.org, last accessed 11/11/2012.

[19] B. Bloom. "Space/time Trade-offs in Hash Coding with Allowable Errors," Communications of the ACM, vol. 13, pp 422–426. July, 1970

[20] M. Goyal, M. Soperi, E. Baccelli, G. Choudhury, A. Shaikh, H. Hosseini, K. Trivedi "Improving Convergence Speed and Scalability in OSPF: A Survey", published in IEEE Communications Surveys & Tutorials, vol. 99, pp. 1–21, December, 2011.

[21] Integrated Multiprotocol Network Emulator/Simulator (IMUNES) http://www.imunes.net/, last accessed 17/01/2013.