



St. Mary's University
Department of Computer Science
Security Enhancement for IP Network
Integration with Mobile IP Based
Communication

By
Tigist Eshetu

A thesis Submitted to School of Graduate studies of St. Mary's University
in Partial Fulfillment for the requirement for the Degree of
Master of Science in Computer Science

January 2023
Addis Ababa, Ethiopia

St. Mary's University
Department of Computer Science
Security Enhancement for IP Network
Integration with Mobile IP based
Communication

By
Tigist Eshetu

Advisor
Asrat Mulatu (PhD)

January 2023

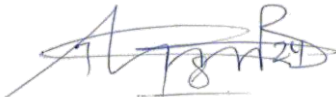
St. Mary's University
Department of Computer Science
Security Enhancement for IP Network
Integration with Mobile IP Based
Communication

Tigist Eshetu

The thesis entitled, "Security Enhancement for IP Network Integration with Mobile IP base Communication" has been read and approved as meeting the requirement of Master of Science in Computer Science, St. Marry University, Addis Ababa, Ethiopia.

Approval Sheet


Advisor: Asrat Mulatu (PhD)

Date and Sign: 

Internal Examiner

Date and Sign: _____

External Examiner: Dr. Yihenew

Date and Sign: 23/02/2023 

Dean, Faculty of Informatics _____

Declaration of Authorship

I declare that this thesis entitled “SECURITY ENHANCEMENT FOR IP NETWORK INTEGRATION WITH MOBILE IP BASE COMMUNICATION” has not been submitted for any other ward and that it is all my own work. I also confirm that this work fully acknowledges opinions, ideas and contributions from the work of others. The work was done under the supervision of Asrat Mulatu (PhD).

Name: Tigist Eshetu

Signature: _____

Place: Addis Ababa

Date of submission: January 04, 2023

This thesis has been submitted for examination with my approval as a university advisor

Advisors Name: Asrat Mulatu (PhD)

Signature: _____

Acknowledgments

First, I gave thanks to the almighty God as, without his help one can finish nothing. Then I would like to take this opportunity to my supervisor Asrat Mulatu (PhD) for his support and follow up, and advice that he gave me throughout my thesis work. I am also very thankful for my colleagues who gave me materials and helpful ideas.

I am very pleased to thank my husband who has been helping and encouraging me, throughout the course of this work.

Abstract

Mobile IP communication mostly exist in wireless networks where users need to carry their devices across several networks within different IP address. Mobile IP is enabled and supported by mobile devices like Cellular phones, Personal Digital Assistances, Global Positioning Systems, and handheld devices which have been developed rapidly and their communication capabilities are enhanced effectively. These devices allow users freedom of movement and to access internet services in any location. Now days, enterprises are deploying Mobile IP services to enable their usersto access the enterprise services while the user is in mobile mode. The challenge in such scenario, deploying Mobile IP for accessing enterprise services with mobility, security of intermittent connection is the first challenge to be addressed. In this study, alternative methods for securing and enhancing the connectivity of mobile nodes that uses Mobile IP for communication and accessing enterprise services in mobility mode. When the mobile nodes with Mobile IP needs to access the enterprise services in mobility mode, the persistence connectivity to the home networkwhere the enterprise services are provided is the backbone for secured service access. To create secure and persistence connectivity, the role of routing algorithms and mobility models are assessed in two different scenarios. The first scenario is integration of mobile node that uses Mobile IP when it gets away from the home network. The second scenario is integration of Mobile Ad hoc networks that implement Mobile IP to access enterprise services using the enterprise IP network. The evaluation result of the efficiency of the routing algorithm and the mobility models are assessed in terms of the network throughput in the communication. The results shows that routing algorithms and mobility models has great impact on the integration of Mobile IP networks and regular IP network communication.

Keywords: Mobile IP, Mobile Ad hoc Networks, Integration, Connectivity, Routing, Mobility Models

Table of Contents

Declaration of Authorship.....	III
Acknowledgments.....	IV
Abstract.....	V
List of Figures.....	IX
List of Tables.....	X
List of Abbreviations and Acronyms.....	XI
Chapter One.....	1
Introduction.....	1
1.1 Background.....	1
1.2 Problem Statement.....	3
1.3 Objectives.....	5
1.4 Research Design /Methodology/.....	5
1.5 Data Collection and Sampling.....	8
1.6 Programming and Development Tools.....	9
1.7 Significance of the Research.....	9
1.8 Scope and Limitation of the Research.....	9
1.9 Organization of the Thesis Report.....	10
Chapter Two.....	11
Literature Reviews and Related Works.....	11
2.1 Introduction.....	11
2.2 Mobile IP.....	11
2.3 Mobile Ad Hoc Networks (MANETs).....	14
2.4 Simulation Tools and Mobility Modeling Tools.....	15

2.5	Security Mechanism for Mobile IP	16
2.6	Integration of MANETs into IP-Based Access Networks.....	18
2.7	Related Works and Gap Analysis.....	20
2.8	Conclusion.....	22
Chapter Three.....		25
Proposed Solution		25
3.1	Introduction	25
3.2	Proposed Design.....	26
3.3	Operations of Mobile IP and IP Based Communication Integration.....	31
Chapter Four		34
Experimentation and Evaluation.....		34
4.1	Introduction	34
4.2	Experimentation Setup.....	34
4.2.1	Network Simulation	35
4.2.2	Mobility Simulation	36
4.3	Simulation Environment Configuration	36
4.4	Simulation Test Case Scenarios	37
4.5	Result Evaluation	39
4.5.1	Simulation Results for IP Network Communication with Nodes with Mobile IP	39
4.5.2	Simulation Results for Mobile IP communication within Home Networks supported by IP Networks	42
Chapter Five.....		45
Conclusions and Future Works.....		45
5.1	Conclusions	45

5.2	Contributions.....	46
5.3	Future Works.....	47
	Appendices.....	48
A.	Mobile IP Network Topology.....	48
B.	MANET Network Topology.....	49
C.	Sample Codes.....	50
	References.....	51

List of Figures

Figure 1 Research Development Process.....	6
Figure 2 Generic Architecture for Mobile IP and IP networks communication.....	26
Figure 3 Proposed architecture	28
Figure 4 Simplified Architecture	29
Figure 5 Random Walk Point Mobility Simulation Result.....	40
Figure 6 BonnMotion Mobility Simulation Result.....	41
Figure 7 Random Walk Point Mobility Model in MANET.....	43
Figure 8 BonnMotion Mobility Model in MANET.....	44
Figure 9 Mobile IP with two Gateways	48
Figure 10 Manet with 1 Gateway.....	49
Figure 11 OLSR Configuration.....	50

List of Tables

Table 1 Gap Analysis.....	24
Table 2 Network Simulation Environment Setup.....	36
Table 3 Simulation Test Bed Configuration	37
Table 4 Node Configurations for Mobile IP communication	38
Table 5 Node configuration for MANETs communication.....	38

List of Abbreviations and Acronyms

A

Ad hoc On Demand Distance Vector
(AODV) · 28

C

Care of Address
(CO) · 14
Communication Host
(CH) · 15
Constant Bit Rate
(CBR) · 28

D

DelayTolerant Networks
(DTN) · 27
Design Science Research Methodology
(DSRM) · 17
Destination Sequenced Distance Vector
(DSDV) · 28
Differentiate Service
(DiffServ) · 16
Dynamic Host Configuration Protocol
(DHCPv6) · 25
Dynamic Source Routing
(DSR) · 28

F

Foreign Agent
(FA) · 14

G

General Packet Radio Service
(GPRS) · 25
Global Positioning System
(GPS) · 13

H

Home Address
(HA) · 14
Home Agent
(HA) · 15

I

Internet Engineering Task Force
(IETF) · 13
Internet Protocol Security
(IPSec) · 14
Internet Protocol Version 4
(IPv4) · 25
Internet Protocol Version 6
(IPv6) · 25
IP
(Internet Protocol) · 13

M

Mobile Ad hock Network
(MANET) · 16
Mobile Host
(MH) · 15
Mobile IPv6
(MIPv6) · 25

P

Personal digital assistant
(PDAs) · 13

Q

Quality of Service
(QoS) · 16

R

Resource Reservation Protocol
(RSVP) · 16

S

secure mobile IP
(SecMIP) · 14

Simulation of Urban Mobility
(SUMO) · 28

V

Vehicular Network Simulation tool
(VanetMobiSim) · 28

Chapter One

Introduction

1.1 Background

Mobile IP is a standard protocol established by the Internet Engineering Task Force “IETF”, to provide an efficient and scalable mechanism for mobile nodes within the internet [1]. Mobile IP environments mostly exist in wireless networks where the users need to carry their devices across several networks within different IP address. Cellular phones, PDAs, GPS, and handheld devices are example of wireless device which have been developed rapidly [2]. These devices allow users freedom of movement and to access internet services in any location.

Many laptops, PDAs, handhelds, and other portable computing devices now include wireless connectivity as a standard feature, and more people are carrying computers when they travel to access the Internet anytime, anywhere [3]. Mobile IP technology allows users to keep one IP address from the home network and stay connected with the internet while the mobile nodes are moving over networks. The Internet Engineering Task Force’s mobile Internet protocol is a widely accepted standard that uses mobile agents to support seamless handoffs, making it possible for mobile hosts to roam from subnet to subnet without changing IP addresses [4].

In Mobile IP, the mobile node can change its existing location by maintaining the same IP address and keep connected to the internet on the other locations. This method solves the issue of terminating the communication when the mobile node moves to different locations. This approach is scalable to the internet as it is based on the regular IP structure [5]. Mobile IP is built on the standard IP protocol stuck for internet infrastructures to enable IP mobility. As Mobile IP is a layer 3 solution for IP mobility, it has suffered from security problems in the same way as a standard IP protocol as such issue of securing Mobile IP and it has become the significant point with increasing demand of Mobile IP with large set of mobility devices. Generally, Mobile IP is an open standard that allows users to keep the same IP address and keep connected, maintain ongoing application and other services while the move between different IP networks [6]– [8].

In Mobile IP, a mobile node will have two IP addresses that are named as Home Address (HA) and Care of Address (CO). The home address of the Mobile IP allows the mobile node to be identified with its home address irrespective of the IP network it is connected to. Any communication that is going to be made between the mobile node and any other nodes will identify the mobile node with its home address. When the mobile node is away from its home network, it assigns a representative in the home network that will receive packets destined to it. So, any packet whose destination address is the home address of the mobile node will be intercepted by representative and the representative will send it to the mobile node [9], [10].

There are security challenges in Mobile IP network communications other than the security challenges in the standard IP network communications. Mobile IP security challenges include protocols which support mobility of IP-address, mobility models that support mobility of different IP-nodes and efficiently of designed solution for integrating Mobile IP networks with the standard IP network communication [11]– [13].

Mobile IP provided solution for mobility from one home network to foreign network (visited network by mobile node). Mobile IP and its extension have provided many mobility solutions with minimum handover latency but still integration security remains an issue. While moving from one network to another various security problems can arise and can be experienced by mobile user [14].

On the other hand, Mobile IP can be integrated with IPSec to establish a solution called secure mobile IP (SecMIP) that protects Mobile IP devices and users from any security threats while they are accessing their organizations firewall through a virtual private network. This methodology will enhance the information security implemented by the network of the organization, but play minimum role on the integration security of the mobile nodes and the standard IP networks [15]– [17].

Integrating the Mobile IP network communication technology to the standard IP network communication will facilitate the current trend of user's mobility to an all-IP wireless environment. Many solutions have been proposed to integrate mobile nodes with Mobile IP networks to the Internet that uses standard IP communication. Some solutions use the Foreign Agent (FA) of Mobile IP as an Internet Gateway. One of the many ways of combining mobile nodes with the

Internet by maintaining the same IP address as in the Home IP, is the use of Mobile Internet Protocol (Mobile IP) alongside routing protocols, to route packets between the Internet and the mobile node, via Gateway agents. In this study, enhancing the integration security of mobile nodes with Mobile IP communication to the standard IP network communication based on using mobility models, routing protocols and VPN gateways are studied [15], [18]–[21].

1.2 Problem Statement

Securing Mobile IP has become the most significant point with increasing demand on mobile IP due to the rapid growth of IP enabled mobile device. The integration of a mobile nodes with Mobile IP to the Internet provides mobile users with Internet access and hence increases the scope of the internet application. In addition, the Internet can benefit from this integration by an extension of the network coverage area. However, the integration of heterogeneous networks raises many issues and challenge as Mobile IP grows rapidly. These issues, challenged and research solutions that put significant contributions in the state of the art are discussed as follow.

The “Triangular routing” Problem: The communication Host (CH) must send packets to the Mobile Host (MH) via the Home Agent (HA), while the MH sends packets directly to the CH. As the communication in the two directions follows different routes, the problem of” triangular routing” arises, which leads to low efficiency especially when the MH is far away from the HA and the CH is near to the MH. Solution for such problem is designed in [22]–[24]. But these solutions didn’t achieve stable integration solutions to the integration security problem.

The Handoff Problem: Handoff problem means that the HA sends the IP packets of the MH to the original foreign network via the tunnel because it doesn’t know the latest Care of address (CoA) of the MH during the period starting when the MH leaves the original foreign network and ending when the HA receives the new registration address of the MH. As a result, these dropped IP packets have an influence on the communication between the MH and the CH especially when handoff occurs frequently, or the MH is far away from the HA. Solutions for such problem is designed in [25]–[31]. These solutions are efficient in solving handoff problems and play important roles on integrations of Mobile IP and IP networks. But these solutions are limited on enhancing the handoff problems.

Problems of Intra-Domain Movement: The frequent intra-domain movements of the MH within a small area will lead to frequent handoff. Consequently, a great number of registered messages are generated in the network and the network performance is greatly affected. For the Intra-Domain micro-movements, improved protocols such as Cellular IP, HAWAII and TeleMIP can be adopted to solve the problem of frequent handoffs, and reduce handoff delay, packet loss ratio and registration information to the HA [3], [5], [7], [21], [30].

At last, QoS Problem: In the mobile environment, it is hard to provide QoS over Mobile IP due to dynamically varying wireless network topologies, limited network resources, unpredictable effective bandwidth, and high error rate. Lastly, Solutions to QoS problem: Resource reservation Protocol (RSVP) and Differentiate Service (DiffServ) have their respective strength and weaknesses in providing QoS over Mobile IP. But they can combine to solve the end-to-end QoS problems [7], [16], [17].

Though the growth of Mobile IP it was slow compered to Wireless LAN, the need of Mobile IP is increasing rapidly. While the introduction of Mobile IP Protocol, there have been several research's done in different area. The first area of research aims on making Mobile IP communication system efficient. This area of research planned improvements on mobile IP for improving the performance of Mobile IP. The research includes methods for Securing Mobile IP Based Communication using IPsec and analysis the security issue in mobile IP, finally propose solution to secure the system.

To overcome the incompatibilities between different architectures, gateways are used. In this study to integrate Mobile IP networks and standard IP network communications efficiently, mobility models, MANET protocols and VPN gateways are implemented. The mobility models used to manage nodes mobility and the selected protocols will enhance the nodes communication and the VPN gateway will secure the communications. Generally, this study at the end answers the following research questions:

1. How best a traffic pattern mobility models can be designed for the integration of Mobile IP and IP network communications?
2. How best routing protocols enhances the integration of Mobile IP and IP network communications?

1.3 Objectives

General Objective

The objective of this study is to design and develop integration security enhancement on Mobile IP network communication to standard IP network communication for mobile users.

Specific Objectives

Throughout the research process, this research will achieve the following specific objectives to deliver the overall research goal.

- To analyze traffic patterns used to enhance integration security in Mobile IP and IP networks
- To analyze routing protocols used to enhance integration security in Mobile IP and IP networks
- To analysis the integration security issues in Mobile IP and IP networks
- To design components that used to enhance the secure integration of Mobile IP and IP network communication
- To demonstrate the proposed design on simulation environment

1.4 Research Design /Methodology/

Research Approach /Development/

In this study, to enhance the security for integrating IP Networks with Mobile IP communication, Design Science Research Methodology (DSRM) is applied. The stated research problem is systematically structured and arranged based on the principles of design science research to produce the required blueprints, measurements, analysis and development of the proposed comfort service model [32].

To produce the desired solution, which is the artifact, DSRM involves rigorous process to solve stated problem, to design the model, to evaluate the designs, and to communicate the results and

make research contributions. The approach plays an important role in construction of the model components through systematic demonstration.

Research Process

To design the security enhancement model for integration IP networks with Mobile IP, first the characteristics and requirements of IP Networks and Mobile Networks must be identified, thus the design requires data to be gathered from multiple sources, including literature, journals, and surveys, therefore the design is started by identifying the problem. Among the entry points for research in design science, since the modelling research is objective oriented, the entry point for this study is in the second step of design science research by setting out objectives of the solution. The overall research process model of this research is shown in following figure which is adopted from and the details are discussed as follow. The figure to show the design science research implementation methodology is adopted from [32].

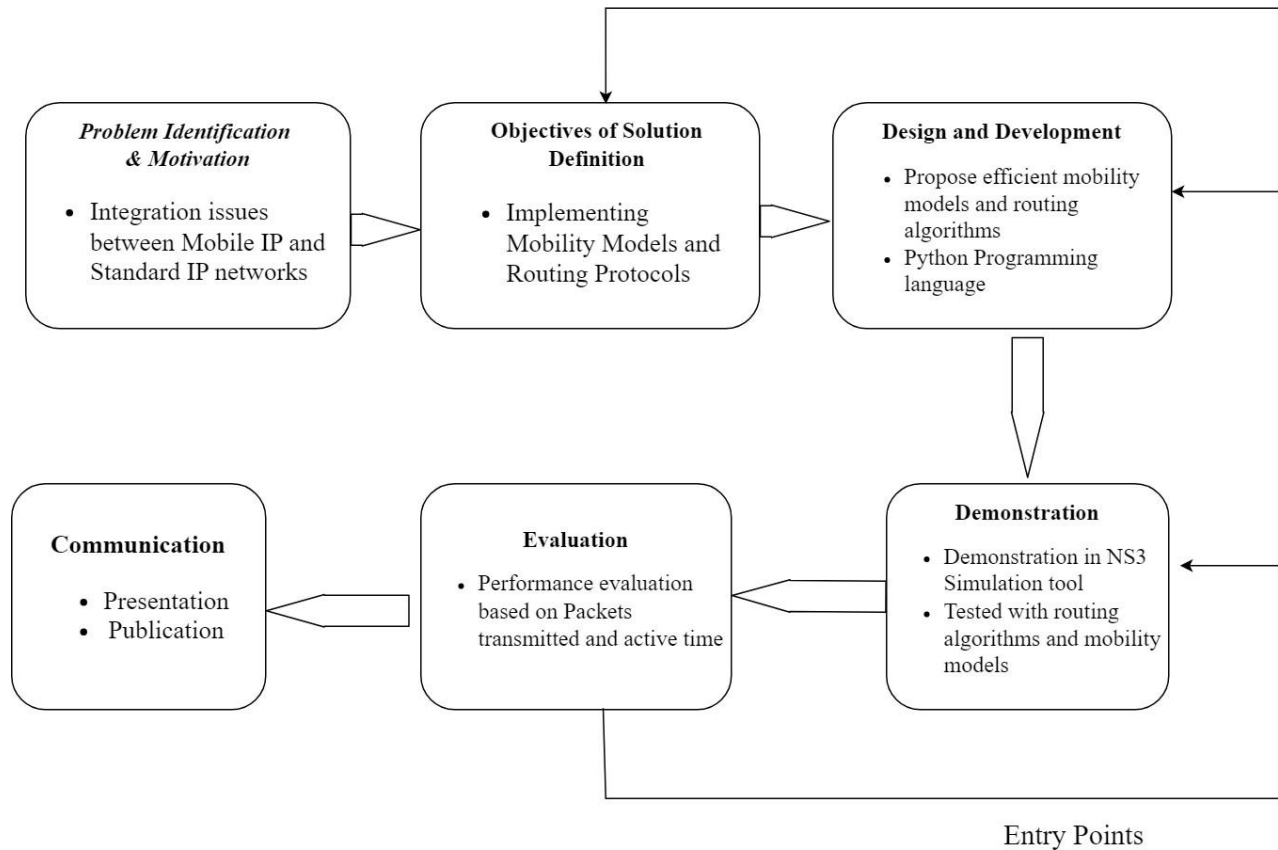


Figure 1 Research Development Process

1. Problem Identification & Motivation

Mobile IP has been widely accepted as a standard to support IP mobility in a wireless Internet environment to keep a session connected when a mobile host roams from subnet to subnet. Another emerging wireless network architecture that is gaining more and more popularity is the mobile ad hoc network (MANET), which can be flexibly deployed in almost any environment without the need of infrastructure base stations. In order to move to an all-IP environment, there seems to be a growing demand to integrate these two architectures together. Typically, mobile hosts are served by access points that can connect to them directly (in one hop).

By enhancing the required security measures for integrating IP network and Mobile IP based communication, it's possible to allow users to roam outside of their home networks, while still retaining network connectivity. Security is always important in any network communication, especially when integrating IP network communications with mobile IP networks, because mobile devices are using wireless communication that is less secure than a wired network.

2. Objectives of Solution Definition

The objective solution of this study is to identify the characteristics and types of IP network and Mobile IP communications and enhancing the security measures that could be implemented during integration of these IP network communication and Mobile IP communications for secure communication. These enables users to maintain their communication experience both on IP networks and Mobile IP communications.

3. Design and Development

In the design phase of this research, the security enhancement method for integrating IP network communication and Mobile IP communications modelled and implemented by considering the communication characteristics of both IP networks and mobile ad hoc networks that implement mobile IP for communication. At this phase, the theoretical framework is discussed and conceptual model is designed to achieve the objective of the solution. Generally, the modelling process is based on construct theoretical frameworks, requirement specifications, develop model

Architecture and Implementation – which is basically based on standard software development lifecycle.

4. Demonstration

In the demonstration phase, the integration of internet with mobile ad-hoc network, using routing protocol for two performance matrices Packet Delivery Ratio and End to End Delay, will be implemented using Network Simulator-3 network simulation tool. To provide the connectivity between wired and wireless network, basic scenarios will be demonstrated that can provide large Packet Delivery Ratio and less average End to End delay.

5. Evaluation

Then after the designed artifact is evaluated in a simulation environment for performance evaluation based on performance metrics. The performance of the model is evaluated based on the successful packet delivery and end to end delay as integration security measure for the integration of IP network and Mobile IP network communication.

6. Communication

Finally, this research is communicated through a presentation for final evaluation and after the final evaluation by the expertise, it is published by reviewing the publishing standards of the respective journal site.

1.5 Data Collection and Sampling

Data Population

The research population of the study:

- Wired Domain (fixed network)
- Wireless Domain (MANET)

1.6 Programming and Development Tools

Implementation is the process of translating the detailed design into code. Source codes for the designed model is developed using python programming language. Python, a general-purpose programming language, effectively used to build almost any kind of program that does not need direct access to the computer's hardware and good enough to implement machine learning concepts.

Additionally, different libraries are used from Python programming tool for data processing and plotting. It's a relatively simple programming language that is easy to learn and there are freely available libraries that interface to Python and provide useful extended functionality.

1.7 Significance of the Research

This study has different significance in a different context. The significance of the research can be generalized as follow:

- This research will generalize research theories formulated to solve problems associated with integration of IP Network and Mobile IP communications
- Provides new insight into the design, development, and deployment of a new application service in Mobile IP communications
- Enhance users experience and business productivity over network communication

1.8 Scope and Limitation of the Research

VSN is a recent research area and has a number of open issues and challenges to be addressed in the field of study. This study aims to enhancing the security of mobile IP communication integrated with mobile IP based communication. In this study, the security enhancement for integration of the IP network and Mobile IP communication demonstrated only in a simulation environment due to the associated cost and lack of infrastructure required to implement and test in real-world environment.

1.9 Organization of the Thesis Report

This thesis report is organized in five chapters with sections and subsections in each chapter. The contents of each chapter and the respective objectives are described as follow to show the roadmap of the report at glance.

The first chapter of this report is the introduction section which provides conceptual backgrounds about Mobile IP and standard IP based communication. Additionally, the chapter contains the problems and proposed solutions that this thesis aims to solve including objectives and solution approaches.

The second chapter of this thesis report contains the reviews of literatures and related works in the field of Mobile IP communication and integration of the Mobile IP technologies to the standard IP based communications in wired networks. This section contains the state of the art in the Mobile IP communications and the gaps in the literatures that needs to be solved.

The third chapter of this thesis report is about the proposed solution design that can be employed to solve the problem stated earlier in this thesis, chapter one – problem statement section. This section also describes the proposed solution components and how they are supposed to solve the stated problems.

The fourth chapter of this thesis report is about evaluation of the proposed solution for performance and efficiency in simulation tools. This section describes the evaluation metrics and evaluation environment to test and demonstrate the proposed solution. Again, this section contains the evaluation results and their interpretations.

Finally, chapter five of this thesis report is about conclusions for this thesis work, findings of this study and future works that needs further investigations in the field of Mobile IP and standard IP based communications.

Chapter Two

Literature Reviews and Related Works

2.1 Introduction

In this section, the corresponding previous researches that have been done in the field of integrating the Mobile IP and standard IP communications networks are explored and these studies are categorized into different main groups for systematic review. On the-state-of-the-art, most researches focus in the integration techniques and mechanism to integrate the Mobile IP and IP network communications. In this section, the researches in the-state-of-the-art are categorized into different sections and reviewed.

The research papers reviewed in the first categories of the research focus on the concept and applications of Mobile IP technologies. The second section of the research categories focus on possible integration architectures of Mobile IP and standard IP networks. Researches reviewed in the third section focus on possible environments where the integration can take place such as Manets. Additionally, Mobility models are reviewed in this section which can enhance the integration of Mobile IP and IP network communications. Finally, there is a summary on the reviewed papers which sums up the existing state-of-the-art in the integration of Mobile IP and standard IP networks.

2.2 Mobile IP

The Mobile IP is defined by IETF to support IP mobility in mobile environments. Mobile IP is a key technology for managing mobility in wireless networks. Mobile IP is designed to support host mobility on the Internet for secure communication. When a mobile node moves across different connection points, in Mobile IP technology, the mobile node can maintain connectivity with other nodes on the Internet, by maintaining the same address. It is the improvised version of Internetworking Protocol (IP) that boosts mobile communication [2], [5].

Mobile IP implies that a user is connected to one or more applications and network services across the Internet, that the user's point of attachment changes dynamically and frequently, and that all connections are automatically maintained despite the change in location of the mobile node. When the Mobile Node moves its attachment point to another network, it is considered a foreign network for the host network of the mobile node.

There are two versions of Mobile IP which are defined depending on IP version used in the network: MIPv4 for IPv4 networks and MIPv6 for IPv6 networks. Mobile IPv4 (MIPv4), like IPv4, assumes an end-to-end networking model where addresses are unique and directly reachable (i.e., there are no firewalls or private addresses, for instance), and provides mobility for IPv4 nodes in such ideal network conditions. MIPv4 is a long-term effort in the Internet Engineering Task Force (IETF); the base specification has been stable for a long time – the first MIPv4 base specifications. Mobile IPv6 is an enhancement for IPv6, which enables IPv6 node to move from one IPv6 subnet to another without changing its IPv6 address. It is built based on the same principles of Mobile IPv4 and using the feature of IPv6. In Mobile IPv6, MN uses IPv6 Neighbor Discovery to acquire a new CoA using IPv6 stateless address auto-configuration or state full address auto-configuration such as DHCPv6 or PPPv6 [5], [33], [34].

Mobile IP agents are being deployed in enterprise networks to enable mobility across wired and wireless LANs while roaming inside the enterprise Intranet. With the growing deployment of access points ("hot spots") in public places such as hotels, airports, and convention centers, and with wireless WAN data networks such as General Packet Radio Service (GPRS), the need is increasing for enabling mobile users to maintain their transport connections and constant reachability while connecting back to their target "home" networks protected by Virtual Private Network (VPN) technology [5], [34].

Mobile IP has become very important for scientific, humanitarian, military purposes and businesses by providing mobility based on IP addresses using several applications, which keep the communication between devices continue unbroken as the user or node moves from one link to another. The Mobile IP technology has allowed mobile users to roam freely between wireless connections, known as hotspots, for network communication. This method of Internet access has several advantages such as communication portability and security and service mobility [35], [36].

In a Mobile IP environment, a mobile host can change its point of attachment from subnet to subnet on network communication. If a mobile host is away from its home network, when the corresponding Internet host sends an IP datagram for delivery to the mobile node on the host's home network, the datagram will be tunneled to the host's current foreign network. The home agent will encapsulate the datagram with an IP header carrying either the foreign agent's IP address or the mobile host's collocated care-of address. In the operation of Mobile IP, there are four basic components, namely: Home Agent, Foreign Agent, Mobile Node and Correspondent or Communication Node [1], [2], [4], [7], [19], [34], [37].

The Home Agent component is a home network and it is the network of the home operator or business entity where the mobile node has its subscription. It is the IP network to which the mobile node originally belongs as per its assigned IP address that is related to the IP topology and IP routing of the organization. Home Agent is a router in home network to which the mobile node was originally connected. It is a router on the home network serving as a gateway for communication with the Mobile Nodes using their home IP address over a foreign network. A home agent on the mobile host's home network serves as a binding cache and forwarding agent for the mobile host. Extensions for optimized routing allow these forwarding capabilities to also exist at the correspondent hosts themselves.

Foreign Network is the current network to where the mobile node is located away from its home network. Foreign Agent is a router in a foreign network to which the mobile node is currently connected for communication using its assigned home IP address. The packets from the home agent are sent to the foreign agent which delivers them to the mobile node. This is typically a router on a mobile node's visited network that collaborates with the Home Agent to complete the delivery of datagrams to the mobile node while it is away from its home network. Generally, it's a router on a mobile node's foreign network that cooperates with the mobile node's home agent to finish registration and packet delivery. Foreign agents are responsible for managing mobile host registrations, maintain a list of all currently registered mobile hosts that are visiting the network served by the foreign agent on the foreign network, a network where the mobile node currently resides.

Mobile node in Mobile IP is a host or router that changes its point of attachment from one network or subnetwork to another, without changing its primary IP address assigned in its home network address. A mobile node can continue to communicate with other Internet nodes at any location using its (constant) IP address.

Correspondent or communication node is any IP host or router that communicates with a mobile node. A correspondent node may be either mobile or stationary. A correspondent node, itself, may be either mobile or stationary. To send a packet to a mobile node, a correspondent node transmits the packet to the mobile node's home address, which causes the packet to be routed toward the mobile node's home network. There, the packet is intercepted by the mobile node's home agent. The home agent then tunnels the packet to the mobile node's current foreign agent, using the care-of address as the tunnel destination. The foreign agent decapsulates the packet and delivers it locally to the mobile node. If a mobile node sends a packet to a correspondent node, it simply sends it in the same way as if it were at home, but uses its foreign agent as the default router for delivering the packet. The foreign agent, simply acting as a router, then forwards the packet directly to the correspondent node.

Mobile IP can be used and deployed in different networks architectures designed to provide solutions for enterprises or for general public. Most common network types that Mobile IP can be deployed includes Mobile Ad Hoc Networks (MANET), Vehicular Networks (VANET) and Delay Tolerant Networks (DTN). The Mobile IP can be deployed in these networks and their associated extension networks to provide its services by integrating with the standard IP networks.

2.3 Mobile Ad Hoc Networks (MANETs)

A MANET is a network consisting of a set of mobile hosts which may communicate with one another and roam around at their will. A routing path may consist of a sequence of wireless links without passing base stations (i.e., in a multi-hop manner). This requires each mobile host to serve as a router. Applications of MANETs occur in situations like battlefields, outdoor assemblies, and emergency rescues, where base stations or fixed network infrastructures are not available, but networks need to be deployed immediately [7], [21], [38].

Extensive efforts have been devoted to the routing issues on MANET. Routing protocols can be classified as proactive and reactive. A proactive protocol (such as the DSDV protocol) constantly updates routing information so as to maintain a (close to) global view on the network topology. On the contrary, a reactive protocol searches for a path in an on-demand manner. This may be less costly than a proactive protocol when host mobility is high. Representative reactive protocols include DSR, ZRP, CBR, and AODV [20], [39]–[42].

Additionally, the reactive routing protocols in MANET can be categorized as unicast routing protocols and Multicast routing protocols. Most of the applications in MANET are based on unicast routing. A review of unicast routing protocols for MANET is in. Multicast routing is not widely used in MANET, but it is useful in multimedia communications. In multicast routing a source node sends the same packet to multiple nodes. Multicast is studied in. Broadcasting issues are studied in [20], [39], [41], [42].

2.4 Simulation Tools and Mobility Modeling Tools

To test the proposed solutions of problems by researchers in the field of the study, simulation tools play an important role by representing vehicular traffic mobility models with corresponding scenarios and reproducing realistic mobility models. The Performance of opportunistic networks vary based on the way mobile nodes move, population density and the distance between source and destination. Simulation tools are used for analyzing such factors on the performance of routing and application protocols, and the behavior of applications.

There are different synthetic mobility traces generated using real world road scenarios, such as SUMO (Simulation of Urban Mobility) and VanetMobiSim (Vehicular Network Simulation tool). On the other hand, real-world traces have been recorded by logging the position of mobile nodes including vehicles during their mobility, such as the mobility trace of Seattle, and reproduces the mobility of users within specified period of time [3], [6], [21], [43]–[45].

To study mobility patterns, traffic congestion or communication protocols, users' mobility behavior, vehicular traffic simulator and scenario is needed to evaluate the new proposed solution in a realistic environment. Different simulation tools, which can represent mobility, are available and choices for simulation tools depend on the size and type of simulation required. To evaluate

the integration of Mobile IP and standard IP network for effective communication, for instance, wireless and static IP with MANET simulators are recommended. There are simulation tools which focus on routing choices of the agents to simulate single mobile nodes, which are called multi-agent traffic simulation tool such as MATSim [46].

On the other hand, there are open-source tools for generating user mobility models to represent mobility of mobile users in a particular place for simulation. These tools include IMPORTANT, BONMOTION and GEMM. IMPORTANT, the mobility generator tool, implements random mobility models including Manhattan model and Car Following Model. The GEMM tool introduces Attraction Point, Activity and Role concepts in mobility models to implement destination interest of people or mobile devices. Another simulation tool, STRAW, is a realistic mobility model that implements intersection traffic management using traffic lights and traffic signs [3], [38], [45]–[47].

2.5 Security Mechanism for Mobile IP

Access to internet has stretched a long expanse, from mere luxury to a necessity. Users expect access to the information openly offered on the internet irrespective of their current status i.e., stationary or mobile. Mobility support has become a stipulation to cater the needs of mobile internet users. Tagging mobility support to current internet infrastructure opens up a whole new set of concerns, privacy, data security, and performance to name a few. Delivering the data to the mobile user's current location without conceding the privacy is one of the biggest trials faced by the amenity benefactors. As it has been ascertained in several of earlier research efforts, security and performance together do not work well. Performance is affected negatively if an effort is made to secure the provided connection. Many researchers have tried to reach equilibrium amid security and performance while not compromising on the privacy of the mobile users. Most of such efforts revolve about using public key cryptography and pre-registration of the mobile clients. Adjacent to security, movement between different networks also affects the performance of mobile clients [11], [12].

When a mobile client moves from one network to another, the underlying infrastructure needs to move all the corresponding connections (connections established by the mobile client to the

internet) to the new-fangled location. Current internet infrastructure does not support this kind of transfer inherently. This calls for patches, like Mobile IP, that are developed to support user mobility within TCP/IP protocol stack. Mobile IP defines mobility support agents like Home Agent (HA) and Foreign Agent (FA) that are located in the home network and foreign network correspondingly. The HA is accountable for protecting the privacy of the mobile client. The HA intercepts all communication towards the mobile client (when mobile client is away) and securely forwards it to the mobile client's new location. The FA (of a specific network) is responsible for providing internet access to the mobile client when the remnants are visiting a foreign network. Working with HA and FA, the mobile IP protocol ensures that the current location of the mobile client is mystified from rest of the internet [7], [21], [34], [48].

When the mobile client moves from one network to another, it has to go through a registration route. This ensures that the HA is aware of the current location of the mobile client and also allows the HA to build a secure connection between itself and the mobile client's current location. One of the significant issues with the current approaches is the registration process. Most of the current proposed solutions suggest the mobile client to initiate the registration process after it has detected that it is in the range of a new foreign network. Depending upon the number of extensions (like security, QoS requirements etc.), the time required to complete the registration process will also boost. This will adversely affect the performance of the mobile clients when they are roaming [49], [50].

An alternative foremost issue is security. Most of the current proposals require the authority of a third caucus device to distribute the security keys [51]. This yet again delays the process and leaves room for security breaches. With Traditional Security mechanisms such as IPSec, there will be an increase in the delay and reduction in the throughput. Also, the key negotiation and generation as required by IKE imposes a significant penalty to the throughput. One of the workarounds to address such issues is the use of key exchange servers at the home network and foreign network. Exchange of keys with mobile node as well as foreign agent and home agent is allowed by the use of servers. With this solution, there is a fall in the delay but the throughput does not depreciate visibly [52]. Also, few security concerns ascend as the key exchange server is sometimes compromised and would lead to a single point of failure. Another proposal, based on the public key cryptography [5], tries to address some of these disquiets. In this scheme, the mobility agents

exchange their public keys to increase security. This reduces the security risks, but the throughput alarms still remain. Also, the delay in the key exchange process adds to the registration delay, further affecting the performance [11], [13], [49], [52].

2.6 Integration of MANETs into IP-Based Access Networks

The ubiquitous computing paradigm requires that mobile devices to be connected to the Internet anywhere and anytime. As Internet connection may be demanded in hostile environments where the existing infrastructure does not guarantee access to the Internet, the ad hoc networks provide a feasible solution to extend the coverage area of telecommunication networks due to their multi-hop capability. In turn, the use of ad hoc networks could lead to economic advantages as a result of the reduced infrastructure required. In spite of the advantages associated to their use, the integration of mobile ad hoc networks into IP-based access networks involves challenging aspects that must be solved [37], [53].

In the integration of Mobile IP and standard IP network communications, among other functionalities, the Internet Gateway is responsible for delivering several address configuration parameters through multiple hops and also provides the ad hoc routing functionalities commonly absent in conventional Access Routers. Possible implementations of the Internet Gateway consider the inclusion of extra functionalities in the final telecommunication network Access Router, which becomes an Access Gateway. Additionally, there are extra element connected to the Access Router (through a wireless or wired connection) to enable gateway functionalities on integrating mobile IP and standard IP networks [10], [15].

Furthermore, some approaches suggest that the seamless integration of a mobile ad hoc network into an IP-based access network should be based on the opportunistic configuration of some MANET devices that act as the Internet Gateway on behalf of the rest of the ad hoc devices[54], [26]. In particular, the configuration mechanisms are receiving significant attention as these networks have some specific characteristics that must be taken into account. As summarized in the draft, conventional auto-configuration mechanisms should overcome the drawbacks commonly

present in the current networking technologies. These includes lack of multi-hop support, lack of dynamic topology support, lack of merging support and lack of partitioning support [6], [34], [38], [48]. All these issues are discussed as follow.

Lack of Multi-Hop Support: Common Technologies in the Internet such as NDP (Neighbor Discovery Protocol), Stateless Address Auto-Configuration, or DHCP (Dynamic Host Configuration Protocol) were specifically designed for one-hop networks and, therefore, cannot work fully in conventional MANET contexts where mobile devices may be several hops away from the Gateway[21], [55].

Lack of Dynamic Topology Support: Some configuration supports establish a hierarchical scheme in order to distribute the configuration parameters (for instance, the Prefix Delegation procedures follow this approach). However, the mobile devices change their positions unpredictably, so static and fixed neighboring structures are not common in MANET. Therefore, the ad hoc configuration supports should establish the mechanisms necessary to cope with this dynamic topology. Additionally, these technologies should also operate even in the case of abrupt disconnections of mobile nodes, which are expected to be more frequent in wireless networks [45], [46].

Lack of Merging Support: IP communications are mainly supported by the fact that ad hoc nodes are univocally identified by an IP address. In conventional networks where a static topology is assumed, the uniqueness is achieved in a straightforward way. However, ensuring this condition in mobile ad hoc networks is not a trivial issue as the mobility of nodes may cause some nodes with duplicate addresses to coexist in the same scope. Furthermore, the node movements may lead to the invalidation of some previous suitable IP addresses. These events commonly occur in the merging of independent ad hoc networks. The configuration mechanisms in ad hoc networks should incorporate the procedures to detect and solve these problems which arise as a consequence of the merging [21], [38], [56].

Lack of Partitioning Support: The arbitrary movements of nodes in ad hoc networks may lead to new and different situations which are not common in conventional networks, especially the partitioning or the split of ad hoc networks. These events may lead to scenarios where some devices cannot reach the previously employed configuration servers. The configuration mechanisms in MANET should adapt themselves to these new conditions [7], [21], [38], [56].

2.7 Related Works and Gap Analysis

Currently, the use of portable computing devices has rapidly increased. Along with this network and computing changes organizations are rapidly implementing the same network model and protocols as used on the internet, the IP suite protocol. The IP protocol suite has been designed with the assumption that computers rarely change their point of network attachments, and routers never change their point of network attachments.

In Mobile IP changing the IP address of a node when it moves is not possible while keeping existing transport level connections open. This change requires the termination of all current network activities and users making several configuration changes. Wireless data links are more vulnerable to eavesdropping, traffic analysis and Denial-of-service attacks; wired data links are less vulnerable but not safe. Therefore, secure integration of Mobile IP and standard IP network communication will solve such types of security problems.

Classical Virtual Private Network (VPN) connections establish secure connections between a remote user and a home network by encrypting packets sent though the Internet rather than building a true private network. These VPN connections however, are best suited for stationary devices which, unlike mobile devices tend to have a stable network connection. Most mobile devices are susceptible to intermittent connection loss while switching from one network to another or experiencing a gap in coverage. For example, a cellular phone might switch between WiFi and 4G, or between one WiFi and another. Such connection losses or connection changes can cause the VPN connection to break causing the mobile applications utilizing the VPN to either timeout or crash. Mobile VPN bridges the gap between what users and applications expect from a wired network and the realities of mobile computing [17], [57].

For successful integration of Mobile IP and standard IP networks for effective communication, the general characteristics of mobile IP can be summarized as transparency of user mobility to the transport and application layer protocols, interoperability with stationary hosts running conventional IPs, scalability across the Internet, security by preventing an attacker from impersonating a mobile host and macro mobility by ensuring long-term connection while away from HA [34], [35], [38].

Integration of Mobile IP networks to the fixed infrastructure IP access network has many usage scenarios, and it provides many advantages for both Infrastructure and MANETs, which implement Mobile IPs, networks together. Integration of MANETs with the fixed infrastructure IP access network based on IP mobility protocols enables MANET nodes movement between different MANETs without losing the connection [11]. It can provide mobility support between different non-overlapping and overlapping MANETs with multiple gateways. Node mobility is realized without propagating host-specific routes throughout the Internet. Using mobile IP, a mobile device will have two addresses, that is, a primary or permanent home address and a secondary or temporary care of address, which is associated with the network that the mobile node is visiting [21], [46], [47].

The characteristics of the ad hoc networks, particularly MANETs that implement Mobile IP, and its routing protocols differ substantially from fixed Internet and IP mobility protocols. Numerous integration solutions for integrating MANET with the Internet using IP Mobility protocols have been developed as the trend of moving to an all-IP environment. Integration solutions for routing can also be classified into two categories: tunneling-based-integration routing solutions and non-tunneling-based-integration routing solutions [38].

Tunneling-based-integration routing solutions approach, when the mobile node wants to send packet to destination, it first looks for the destination (using route discovery procedure as in AODV or searching in routing table as in DSDV or based on address network ID). If the destination address is located inside the MANET, it simply forwards packets using ad hoc routing protocol. If the destination address is not found in the MANET, it encapsulates packets and routes them to the FA (gateway). Then the FA decapsulates packets and sends them to destination using standard IP forwarding [13], [58].

Non-tunneling-based-integration routing solutions: In this approach, if the destination address is not located inside the MANET, the mobile node sends packets to default route, which is the route to the FA (gateway). Every node should be able to distinguish external address from internal address and has a default route to the gateway node, or every node should establish route to gateway node during route discovery. Packets are transmitted inside MANET to destination in the

Internet using standard IP forwarding. The gateway forwards data packets using standard IP forwarding [59], [60].

According to Mobile IP (MIPv4) MIPv4 uses protocol tunneling to hide an MNs home address from intruding routers. The tunnel terminates at MNs COA. At the COA, the original packet is removed from the tunnel and delivered to MN. In case of IPv4 Route Optimized Mobile IP (ROMIPv4) extends the operation of the MIPv4 protocol allowing optimization of packet routing from a CN to an MN. The protocol extension of ROMIPv4 provide a means for CNs to catch the binding of an MN and tunnel their own packets for the MN directly to its COA. MIPv6 uses IP version 6, in MIPv6 complies with the security architecture and packets that include a binding update or acknowledgement option must include IPv6 authentication header [13].

The authors also describe vital security requirements for mobile IP which are Authentication and integrity, authorization, Nonrepudiation, and key managements. Then evaluates the current Mobile IP deficiencies of MIPv4, ROMIPv4 and MIPv6. Based on the paper we can conclude that MIPv4 and ROMIPv4 provide support for mobile and portable end nodes in small IP based networks. and the network size directly impacts the effort to support manual key distribution process in MIPv4. Since no packet route optimization is supported in MIPv4, the network administrator will see an increase of network traffic. Authentication has been improved ROMIPv4 over that found in MIPv4. but authorization is still not sufficiently addressed. The most important requirement of Mobile IP is to permit a mobile node to communicate using only its home address while varying its point of connectivity to the Internet. Additionally, a mobile node must convey solid authentication when it updates its home agent of its current location [12], [13], [17], [61].

2.8 Conclusion

The papers revied in this section, specifically, in Related Works and Gap Analysis section, is summarized as follow to show the main concept of this thesis, which is not covered by all these studies.

Title	Concept	Gap
A multi-gateway-based architecture for integrating ad hoc networks with the internet using multiple foreign agents	Propose an architecture for integrating MANETs and the internet using multiple Mobile Gateways (MGs) and FAs.	The impact of mobility models and routing algorithms are not assessed.
802.11 WLANs and IP networking: security, QoS, and mobility	Discusses the standards to deploy WLANs by implementing Mobile IP. More over the paper discusses the importance of mobility management on the implementation of Mobile IP.	The role of mobility models for QoS is presented, but not supported by evaluation.
The Security Aspects of Mobile IP	The study mainly focuses on the security threats associated with IP networks and mobile IP.	Connectivity as a security is not discussed
Integrating mobile ad hoc networks and the internet: Challenges and a review of strategies	Discusses the challenges of connecting mobile ad hoc networks to the Internet and reviews the characteristics of ten proposed solutions with their relative merits and de-merits in the light of a few specific parameters.	Among the reviewed proposed solution, no study tries to enhance the connectivity of MIP and IP communication with Mobility models and routing algorithms.
An efficient integrated routing protocol for interconnecting Mobile ad hoc Networks and the Internet	An extended DSDV protocol, named as Efficient DSDV (Eff-DSDV) protocol is used to provide bidirectional connectivity between ad hoc nodes and the hosts in the infrastructure-based networks like Internet.	The study focuses on the routing algorithm and misses to consider mobility models
A Survey on Mobile IP	Describes and summarizes the characteristics of Mobile IP network communications and associated design issues.	According to this study, mobility models and routing algorithms efficiency has a great impact on the implementation of Mobile IP and these two design inputs are not assessed and the results are not numerically presented.
Mobile IP: Issues, Challenges and Solutions	Assesses and explains the challenges faced by Mobile IP and solutions from different perspective such as <i>Security Issues and solutions, reliability issues and solutions and triangulation problems and issues.</i>	The role of mobility models and routing algorithms to create reliable integration of mobile IP and IP network communication is assessed.

Mobility models for mobility management	Assesses the role of mobility models that are being used in performance evaluation of relevant mobility management procedures, such as handover and location update.	This concept is not adopted to enhance the connectivity of MIP and IP network communication
A Survey of Mobility Models in Wireless Ad hoc Networks	Presents the state of the art of mobile ad hoc networking, specifically the networking paradigms.	The paper provides good insight for the implementation of MIP with routing protocols and mobility models.
Internet Connectivity for Ad hoc Mobile Networks	Presents a method for enabling the cooperation of Mobile IP and the Ad hoc On-Demand Distance Vector (AODV) routing protocol, such that mobile nodes that are not within direct transmission range of a foreign agent can still obtain Internet connectivity.	The approach presented in this study is good enough on assessing the impact of the routing algorithms on the integration of MIP and IP network communication. However, the approach didn't correlate their proposed solution with mobility models to enhance efficient integration.
Implementation and Analyses of the Mobile-IP Protocol	The researcher tries to address implementation of MIP routing protocol that can be used in MIP environment	The designed protocol is don't consider the effects of mobility models on the integration of MIP and IP network communication
Integrating Mobile Ad Hoc Networks with the Internet Based on OLSR	Proposes a lightweight integration scheme for a MANET and the wider Internet, based on the optimized link state routing (OLSR)	The study only assesses a single routing algorithm and doesn't assess the role of mobility models

Table 1 Gap Analysis

Chapter Three

Proposed Solution

3.1 Introduction

Nowadays, networks have grown in both size and importance. In particular, TCP/IP networks have become the main means to exchange data and carry out transactions. Mobile IP allows mobile users to change their network attachment frequently without losing their connection, which gives many advantages to users. Mobile IP enables network mobility to provide a scalable, transparent, and secure solution. It is scalable because only the participating components need to be Mobile IP aware – the Mobile Node and the endpoints of the tunnel.

However, the mobility of communication devices and characteristics of the wireless channel introduce many security issues, particularly persistence connectivity issue which is studied in this research. On the other hand, the fast extension of inexpensive computer networks also has increased the problem of unauthorized access and tampering with data. It is also one of the most challenging tasks in mobile IP network.

As a response to increased connectivity threats in Mobile IP and its integration to IP based communications, several important security implications for Mobile IP are researched in the field of study. VPN and firewall are two of the most widely used security technologies nowadays used to integrate Mobile IP networks and the regular IP based communications. Since these technologies are not designed for mobile terminals, careful considerations are needed to be effective even for mobile terminals.

In this section, Mobile IP with VPN gateways is considered to provide enhanced integration security solutions for mobile IP and regular IP network communications. Mobile IP agents are being deployed in enterprise networks to enable mobility across wired and wireless networks while roaming inside the enterprise intranet. The growing deployment of access points in public places such as hotels, airports, and convention centers, and wireless WAN data networks such as GPRS,

enables mobile users to maintain their transport connections and constant reachability while connecting back to their home networks. This implies that Mobile IP and VPN technologies have to coexist and work together in order to provide mobility and security to the enterprise mobile users.

3.2 Proposed Design

The regular IP stack does not provide a support for mobility for mobile devices. To support regular IP network connectivity and Mobile IP communication, mobility services and tunnel managements play an important role. The emerging of mobile IP technologies made it possible to access mobile internet that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without the user's sessions or connections being dropped.

Mobile IP agents are being deployed in enterprise networks to enable mobility across wired and wireless networks while roaming inside the enterprise intranet. The “hot spots” in public places such as hotels, airports, and convention centers, and wireless WAN data networks such as GPRS and LTE, enables mobile users to maintain their transport connections and constant reachability while connecting back to their home networks protected by Virtual Private Network (VPN) technology. This implies that Mobile IP and VPN technologies have to coexist and work together in order to provide mobility and security to the enterprise mobile users. The following generic architecture shows the Mobile IP network integration to the regular IP network communication, which is a baseline for the proposed architecture. The architecture is adopted from [10].

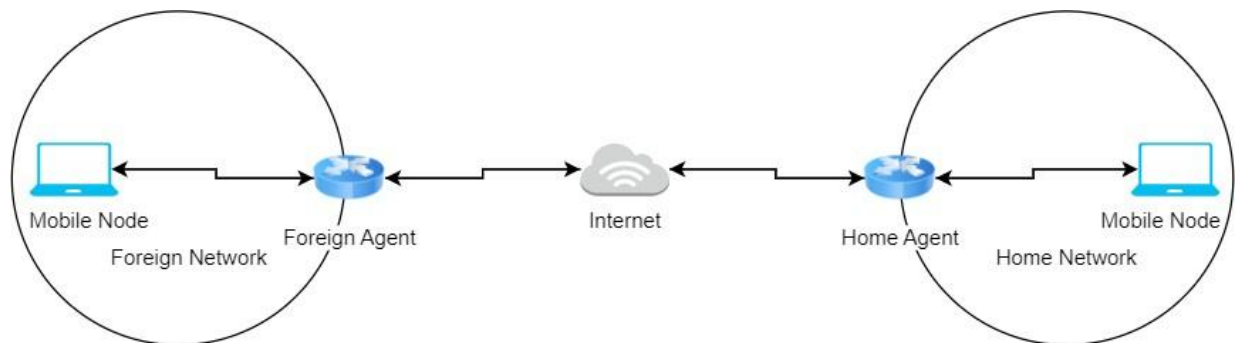


Figure 2 Generic Architecture for Mobile IP and IP networks communication

Mobile Node is any hand-held communication device that the user carries for communication over the internet such as smart phones, smart watches and tablets. Mobile IP allows such mobile nodes to be always reachable using the one or similar IP address when the mobile node moves between different IP networks. The IP address assigned for these mobile nodes is called the Home IP Address, an address assigned from the address space of the home network. Home Address is the permanent IP address assigned to the mobile node within its home network.

Home network is the network of the home operator or business entity where the mobile node has its subscription. It is the IP network to which the mobile node originally belongs as per its assigned IP address that is related to the IP topology and IP routing of the organization. Home Agent is a router in home network to which the mobile node was originally connected. It is a router on the home network serving as a gateway for communication with the Mobile Nodes using their home IP address over a foreign network.

Foreign Network is the current network to where the mobile node is located away from its home network. Foreign Agent is a router in a foreign network to which the mobile node is currently connected for communication using its assigned home IP address. The packets from the home agent are sent to the foreign agent which delivers them to the mobile node. This is typically a router on a mobile node's visited network that collaborates with the Home Agent to complete the delivery of datagrams to the mobile node while it is away from its home network.

In this study, based on the generic architecture of integrating mobile IP networks with regular IP network communications, a two-layered approach is implemented for the integration of Mobile IP with IP based communication model is proposed as a solution for the Enhancement for IP Network Integration with Mobile IP base Communication. The proposed model formulates the integration of Mobile IP and IP network communication problem in the mobile environments as a connectivity issue for the integration. To secure the integration of these communication models for enhanced communication, the proposed design describes the basic components as follow.

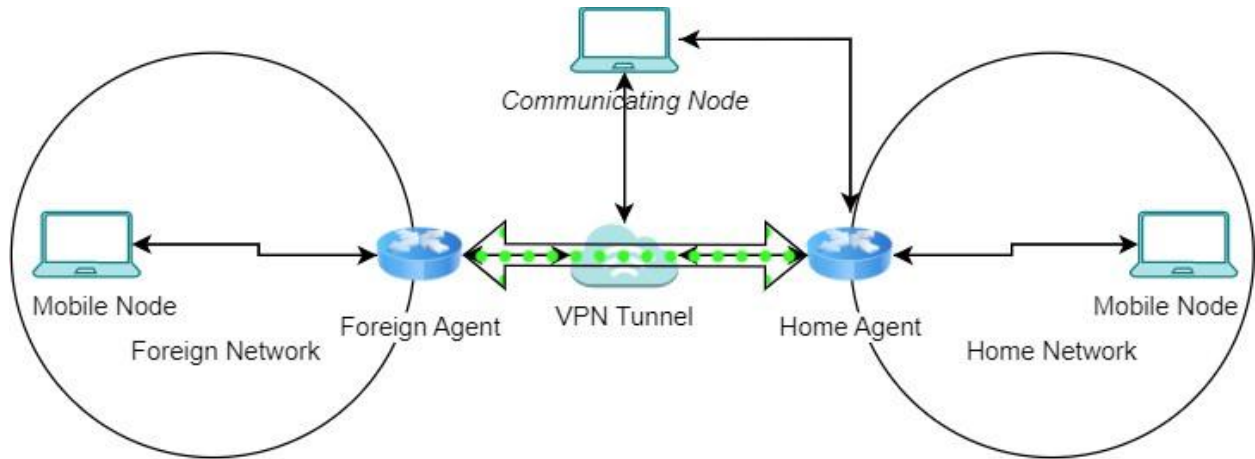


Figure 3 Proposed architecture

Mobile Nodes

Mobile node is always addressable with its home address which is allocated from its home network. The basic idea of IP mobility support is to maintain the address pair consisting of home and care-of address to update the current location of mobile nodes to minimize the handover latency and reduce the service disruption without needs of additional protocol overhead of adjacent layers. The care-of address changes for every movement of the mobile node due to the mobility nature of the device. Thus, it is hard to maintain the pre-configured Security Association between the mobile node, and home agent or security entities such as VPN gateway or firewall.

To maintain the preconfigured security association between the mobile nodes and the home agent, implementing mobility models for the mobile nodes can enhance the integration of the mobile IP with the regular IP network for communication. Mobility models have their own mobility patterns that will impact the protocol performance that can be used on the VPN tunnel that used to connect the home agent and the foreign agent gateways. Mobility management generally deals with automatic roaming, authentication, and intersystem handoff.

The random waypoint mobility model is simple and straightforward stochastic model. In this mobility model, the mobile node moves from its current position to a new location by randomly choosing its destination such as restaurants and public areas where there is a hotspot or using cellular networks. On reaching the destination, the node pauses for some time distributed according to some random variable and the process repeats itself. Once the pause time expires, the node

chooses a new destination, speed, and pause time. Destination points are uniformly randomly chosen in the system area.

The node assumes an initial location (x_0, y_0) , and $k = 1$

A destination location (x_k, y_k) is chosen within the (convex) network area, and a speed s_k is chosen uniformly from an interval $[v_{min}, v_{max}]$. Then the node moves along the line segment between the two locations toward (x_k, y_k) at a constant speed s_k .

If pausing is enabled, the node pauses for t_{kp} after reaching (x_k, y_k) , where pausing time t_{kp} is drawn from a general distribution with density function $f_p(t)$.

$k = k + 1$ and go to Step 2.

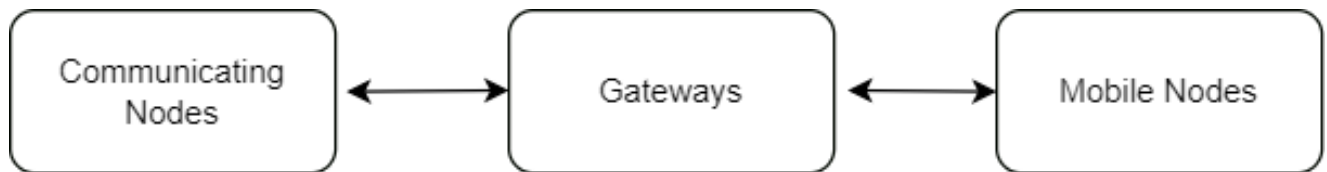


Figure 4 Simplified Architecture

Gateways (Agents)

A gateway IP refers to a device on a network which sends local network traffic to other networks. The gateway has a wide range of applications and advantages. The main features are explained and it's applied accordingly in the right place to achieve high efficacy. It usually works as a safety guard to the local networks and links the local network to the public network system.

The integration architecture has two main gateways that used to transfer packets from source to destination. These gateways are Home Agent and Foreign Agent gateways. The mobile node, who has a home IP address, is accessible through home agents. The home agent communicates to the foreign agent where the mobile node currently resides.

Home Agent is a router in home network to which the mobile node was originally connected. It is a router on the home network serving as the entry point for communication with the Mobile Node; it tunnels packets from a device on the Internet, called a communicating Node, to the Mobile Node

found on foreign network. A tunnel is established between the Home Agent and a reachable point for the Mobile Node in the foreign network for communication.

A Foreign Agent is a node in the Mobile IP network that empowers roaming IP clients to register on the foreign network. The Foreign Agent will communicate with the Home Agent to enable IP datagrams to be communicated between the home IP network and the roaming IP client on the foreign network. The foreign agent can offer a few types of assistance to the mobile node during its visit to the foreign network. Foreign agents can likewise give security administrations since they belong to the foreign network as opposed to the mobile node which is only visiting using Care of Address mechanism.

Care-of-Address (CoA) is a unicast routable address associated with a mobile node while visiting a foreign network. The Foreign Agent is the tunnel end-point and forwards packets to the mobile node. Many mobile nodes using the Foreign Agent can share this COA as a common COA.

Generally, these gateways can be implemented using VPN, firewall and other security features. In this study, these gateways, the Home Agent and the Foreign Agent, are implemented using Mobile VPN technologies for securing the integration of the mobile IP network and the regular IP network communications. A VPN gateway is a virtual network gateway used to send encrypted traffic between the mobile node home network and an on-premises location over the public Internet, which is the foreign network. The VPN gateway controls the flow of incoming and outgoing packets with pre-defined filtering rule. This becomes an obstacle to deploy the Mobile IP with coexisting VPN environment because CoAs of mobile nodes which are obtained outside VPN domain are usually unknown to VPN.

Most existing VPN solutions are intended for wired networks with high-speed, highly reliable connections. In a mobile environment, these network connections are less reliable. This affects traditional VPN performance resulting in frequent application failure, data loss and reduced productivity. Mobile VPN bridges the gap between what users and applications expect from a wired network and the realities of mobile computing.

3.3 Operations of Mobile IP and IP Based Communication Integration

This section explains how Mobile IP and the regular IP networks integrated for enhanced communication. The Mobile IP process has three main phases, which are discussed in the following sections. A Mobile Node discovers its Foreign and Home Agents during agent discovery - Agents Discovery. The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration - Registration. A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams - Tunneling.

Agent Discovery

During the agent discovery phase, the Home Agent and Foreign Agent advertise their services on the network by using the ICMP Router Discovery Protocol (IRDP). The Mobile Node listens to these advertisements to determine if it is connected to its home network or foreign network.

If a Mobile Node determines that it is connected to a foreign network, it acquires a care-of address. Two types of care-of addresses exist: Care-of address acquired from a Foreign Agent and co-located care-of address.

A Foreign Agent care-of address is an IP address of a Foreign Agent that has an interface on the foreign network being visited by a Mobile Node. A Mobile Node that acquires this type of care-of address can share the address with other Mobile Nodes. A co-located care-of address is an IP address temporarily assigned to the interface of the Mobile Node itself. A co-located care-of address represents the current position of the Mobile Node on the foreign network and can be used by only one Mobile Node at a time. When the Mobile Node hears a Foreign Agent advertisement and detects that it has moved outside of its home network, it begins registration.

Registration

The Mobile Node is configured with the IP address and mobility security association (which includes the shared key) of its Home Agent. In addition, the Mobile Node is configured with either its home IP address, or another user identifier, such as a Network Access Identifier.

The Mobile Node uses this information along with the information that it learns from the Foreign Agent advertisements to form a Mobile IP registration request. It adds the registration request to its pending list and sends the registration request to its Home Agent either through the Foreign Agent or directly if it is using a co-located care-of address and is not required to register through the Foreign Agent. If the registration request is sent through the Foreign Agent, the Foreign Agent checks the validity of the registration request, which includes checking that the requested lifetime does not exceed its limitations, the requested tunnel encapsulation is available, and that reverse tunnel is supported. If the registration request is valid, the Foreign Agent adds the visiting Mobile Node to its pending list before relaying the request to the Home Agent. If the registration request is not valid, the Foreign Agent sends a registration reply with appropriate error code to the Mobile Node.

Finally, the Mobile Node checks the validity of the registration reply, which includes ensuring an associated request is in its pending list as well as proper authentication of the Home Agent. If the registration reply is not valid, the Mobile Node discards the reply. If a valid registration reply specifies that the registration is accepted, the Mobile Node is confirmed that the mobility agents are aware of its roaming. In the co-located care-of address case, it adds a tunnel to the Home Agent. Subsequently, it sends all packets to the Foreign Agent.

Tunneling

The Mobile Node sends packets using its home IP address, effectively maintaining the appearance that it is always on its home network. Even while the Mobile Node is roaming on foreign networks, its movements are transparent to correspondent nodes. Data packets addressed to the Mobile Node are routed to its home network, where the Home Agent now intercepts and tunnels them to the care-of address toward the Mobile Node.

Tunneling has two primary functions: encapsulation of the data packet to reach the tunnel endpoint, and decapsulation when the packet is delivered at that endpoint. The default tunnel mode is IP Encapsulation within IP Encapsulation. Typically, the Mobile Node sends packets to the Foreign Agent, which routes them to their final destination, the communicating node.

Chapter Four

Experimentation and Evaluation

4.1 Introduction

It's better to test and evaluate the proposed model in real-world test-bed environment. But the proposed model is evaluated in simulation environment due to technological limitations, economical costs and environmental challenges in the real-world environment. Additionally, researches on MANET and related services rely on simulation as a tool for design and evaluation to feature the trade-off between the realism of results and the flexibility of the proposed solution as studied in [21], [28], [38], [40].

There are two types of datasets widely used in MANET simulations: synthetic mobility datasets generated by simulation tools and GPS traced mobility datasets collected from real-world traces. Synthetic mobility datasets are simulator-generated datasets and GPS traced mobility datasets are real traffic tracking datasets collected in real world environment [62]. In this study, synthetic mobility dataset generated by mobility generator tools is used in order to focus on the objective of the study and to obtain significant results for the proposed solution.

The proposed solution is implemented using python programming language and experimental environment setup is designed and configured in the NS3 simulation tool. The proposed solution is evaluated for performance and efficiency in terms of connecting the mobile users to the IP network of the mobile node home network based on location and long period of time without getting disconnected.

4.2 Experimentation Setup

The proposed solution provides an efficient integration approach for integration of Mobile IP and regular IP network communication while the mobile user left its home network. For the experimentation purpose, a synthetic mobility dataset is used for continuous simulation to test and

evaluate the proposed solution. The dataset is divided into training dataset and testing dataset for training and evaluating the proposed solution respectively. Both the training dataset and testing datasets are synthetic mobility traces generated by a simulation tool in simulation environment.

4.2.1 Network Simulation

Network simulation builds typologies between mobile nodes that uses Mobile IP and IP Network communication based on the given mobility models of the mobile nodes. Due to the cost associated to the deployment of such network architectures in the real-world environment, researches have shown simulation is useful to test and evaluate new models, algorithms and techniques [28], [40], [62]. Therefore, simulation is an alternative methodology prior to the actual implementation of MANETs and its intended applications such as VANETS.

In order to identify efficient interaction of mobile nodes in the network, after integration of the Mobile IP and the IP network architectures, the generated and exported format of network simulation is represented on a network simulation tool, NS3. The network simulation of node helps to identify efficient interactions of mobile nodes with the integration of IP networks with the help of the agents. The efficient integration of the Mobile IP network and the regular IP networks provides different mobility applications including service mobility that can be implemented and provided by enterprises. Due to the technology provided and supported regulars, NS3 is a recommended network simulation tool for MANETs in this research.

The network simulation configuration parameters used in this study are presented in the following table. These parameters are attributes that can be configured and used in the real-world environment for the deployment of the algorithm to enable efficient integration of Mobile IP and IP network communications.

Parameters	Values
Simulation Tool	NS-3
Radio Frequency	5.9 GHz
MAC Protocol	IEEE801.16P
Routing Algorithms	AODV & OLSR

Table 2 Network Simulation Environment Setup

4.2.2 Mobility Simulation

Mobility models have a broad range of applications in areas related to human movements, such as urban planning, transportation, and simulations of diseases spread. Recently, mobility models play important role for implementation of Mobile IP application at large scale including large organizations to provide mobility services. In the last decade, the extensive geolocated user trajectories collected from mobile devices allowed for more realistic mobility modelling, improving its accuracy.

Here in this study, Random Walk Point and BonnMotion mobility models are employed to models and design node mobility that communicate with nodes at different network, nodes at home network connected with regular IP network communication or nodes at another network. The mobile node implements Mobile IP for communication.

4.3 Simulation Environment Configuration

To produce accurate research results, test execution environment of this study consists the following hardware specification and enabling software environment. This test bed configuration determines the simulation and evaluation process of the proposed solution. This simulation test bed is a generalized summary of mobility modelling of the mobile nodes that uses Mobile IP and integrated to the IP network, and network simulation of this study – the integration of the Mobile IP communication and the IP network communication network. This test-bed is built on Linux which is the most mature open-source platform with regards to IP, IPsec and MIP different versions.

Parameters	Values
Mobility Model	BonnMotion & Random Way Point
Nodes	Mobile Devices – Phone/Laptop
Nodes Speed	10m/s
Simulation Time	120sec
Transmission Range	250m

Table 3 Simulation Test Bed Configuration

4.4 Simulation Test Case Scenarios

Integrating mobile IP with MANETs would realize the dream of broadband wireless Internet access. Based on the network architecture, the integration network architecture of Mobile IP and regular IP network communications in [chapter 3], several different communication scenarios may exist. In this section, the possible communications scenarios between the Mobile IP and the regular IP network communications are reviewed for the assessment of the proposed solution.

The simulation is done under NS3 network simulation tool. The basic configuration is that in a 10000m² area with variable number of mobile nodes. The maximum speed of the mobile nodes that use Mobile IP is 20m/sec and simulation period is 120 seconds. Transmission range is 250m and routing protocol is AODV.

The two possible communication simulation scenarios are in assessed in this study, to evaluate the proposed solution for designed integration performance. After creating the underlying network, MANET and the IP network, the proposed solution is evaluated for integration performance of Mobile IP and regular IP network communications. In the communication simulation scenarios, we have to domains – the fixed network domain which implements regular IP network communication and the wireless domain which implements Mobile IP network communications. In this study, these two domains are integrated for efficient communications.

The first integration of Mobile IP and regular IP network communication simulation scenario is intended to test the communication procedure when the mobile node that uses Mobile IP gets away from its home network and the data travels to the mobile node from the host network. In this case, Mobile IP will be involved to forward packets between the two network communication domains.

In the transmission from the node that wants to communicate the mobile node that uses Mobile IP to the mobile node with Mobile IP on the foreign network, packets will arrive at gateway by IP routing techniques of the IP network of the home network. These packets will be encapsulated and tunneled, by Mobile IP, to gateway, which will then forward to the mobile node.

Parameters	Values
No. of Mobile Nodes	10
No. of Wired Nodes	10
No. of Gateways	2
Data Rate	100kb/s

Table 4 Node Configurations for Mobile IP communication

To support such scenario, mobile nodes have to monitor any existing home or foreign agents. Registration and deregistration procedures in Mobile IP should be followed. The routing of these packets will be supported by AODV and OLSR routing protocols. The home agent should maintain the current locations of its mobile nodes that uses Mobile IP for communication. The foreign agent should maintain the visiting mobile node in their MANETs.

The second integration of Mobile IP and regular IP network communication simulation scenario is intended to test the communication procedure when the source and destination nodes are located on two different networks within the home network. Assume that each MANET is connected to the internet and being served by a MG. In this scenario, packets from MNs are transmitted to the MG and foreign agent using AODV and transmitted through the internet using the IP routing until it reaches the foreign agent. From the foreign agent, it will be forwarded to the MG serving the destination MANET, using MIP routing, and finally delivered to the required destination using AODV protocol.

Parameters	Values
No. of Mobile Node	10
No. of Gateways	1
Data Rate	100kb/s

Table 5 Node configuration for MANETs communication

4.5 Result Evaluation

The enterprise network service is composed of Internet, intranet and DMZ. The rationale of Mobile IP is to provide the mobile access transparency without regarding to the type of services or network topology. However, the announced Mobile IP specification does not deal with such a service from outside to inside the intranet smoothly. In this section, the proposed solution is evaluated and the numerical result obtained from Python data analysis tool and NS3 simulation environment is presented. The evaluation result is described in terms of the load, throughput, delay, media access delay, tunneled traffic sent and received (bits/sec) based on selected routing algorithms and mobility models.

4.5.1 Simulation Results for IP Network Communication with Nodes with Mobile IP

The first simulation experiment design enables integration of Mobile IP with the regular IP networks that allows communication of mobile nodes with wired node attached on the home network while the mobile node that uses the mobile IP gets away from its home network and the data travels to the mobile node from the host network. Data transmission from the mobile node that uses Mobile IP and attached to the foreign network to the wired node attached to the home network packets will arrive at gateway by IP routing techniques of the IP network of the home network. These packets will be encapsulated and tunneled, by Mobile IP, to gateway, which will then forward to the mobile node.

In this simulation, the OLSR and AODV routing algorithms are selected for routing data from mobile node that use Mobile IP from foreign network to wired node attached to home network. these routing algorithms are recommended to be used in such scenarios according to [39], [43], [63]. The mobility of the node that communicate in such scenario are designed based on Random Way Point mobility model and BonnMotion mobility model. These mobility models are generic mobility models used to designed simulate node mobility in mobile environment such as MANETs and VANETs [3], [45] – [47], [62].

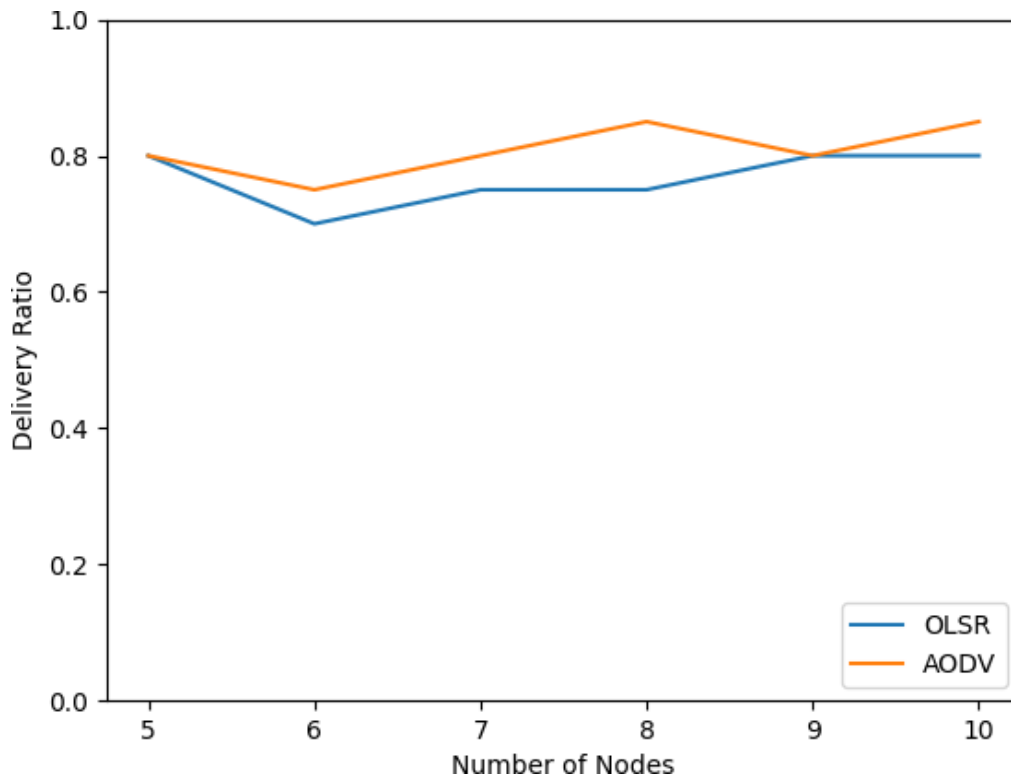


Figure 5 Random Walk Point Mobility Simulation Result

The simulation result for the Mobile node at the foreign network that uses Mobile IP for communication with the wired nodes at the home network that uses regular IP network is presented in figure 5 - Random Walk Point Mobility Simulation Result. The simulation is done using on NS-3 simulation tools with ADOV and OLSR routing algorithms with Random Walk Point mobility model. According to the result graph, with the default mobility model implemented in NS-3 network simulation tool, AODV routing algorithm has a better overall network throughput on implementing Mobile IP communication with wired communication. The overall network throughput performance for AODV routing algorithm is calculated to 81% (rounded up) and the overall network throughput performance for OLSR routing algorithm is calculated to 77% (rounded up). Therefore, for enhanced Mobile IP communication in default mobility models with the regular IP network communications, AODV routing algorithms are efficient. But these network throughput results need an enhancement for better communication efficiency.

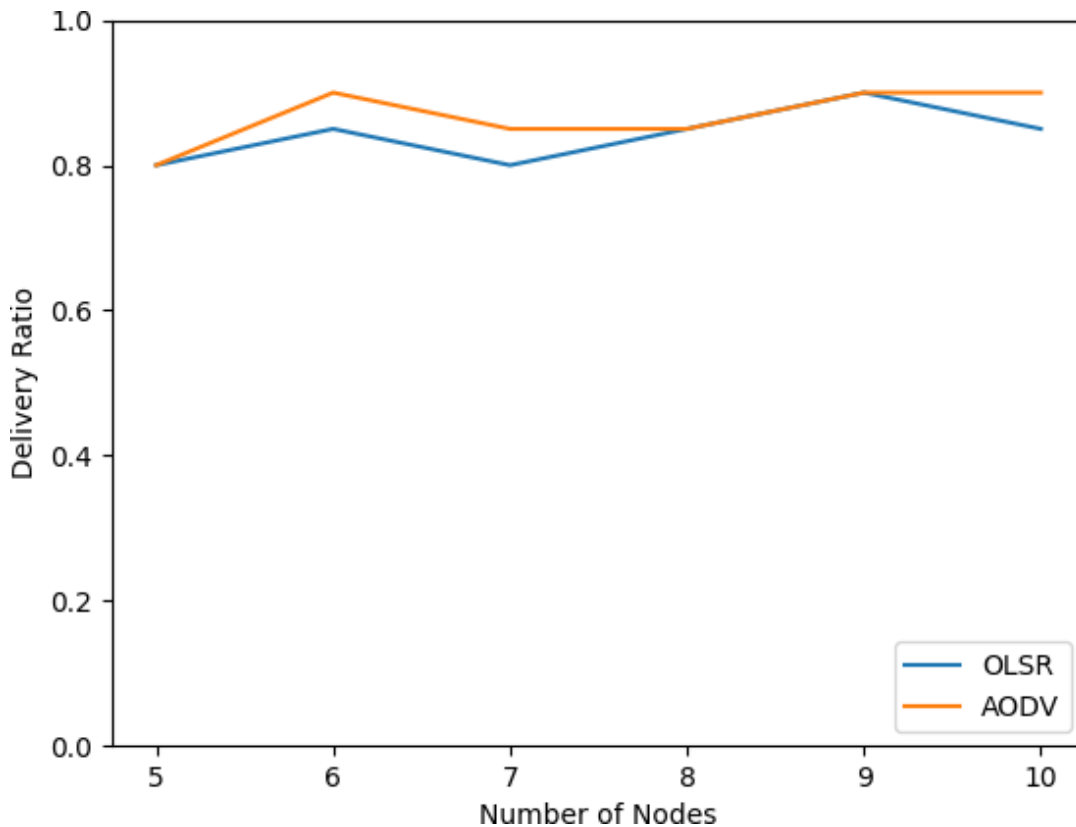


Figure 6 BonnMotion Mobility Simulation Result

The simulation result for the Mobile node at the foreign network that uses Mobile IP for communication with the wired nodes at the home network that uses regular IP network is presented in figure 6 - BonnMotion Mobility Simulation Result. The simulation is done using on NS-3 simulation tools with ADOV and OLSR routing algorithms with BonnMotion mobility model. According to the result graph, with the default mobility model implemented in NS-3 network simulation tool, AODV routing algorithm has a better overall network throughput on implementing Mobile IP communication with wired communications that implements regular IP networks. The overall network throughput performance for AODV routing algorithm is calculated to 87% (rounded up) and the overall network throughput performance for OLSR routing algorithm is calculated to 84% (rounded down). Therefore, for enhanced and secured Mobile IP communication in terms of efficient communication in BonnMotion mobility models with the regular IP network communications, AODV routing algorithms are efficient.

To achieve secured IP network communication with the regular IP networks in terms of efficient communication, implementing efficient mobility model with efficient routing algorithm is the best methodology. However, to select the best routing algorithms and mobility models that can be used in such types of network communications, testing and evaluating MANET routing algorithms and mobility models are recommended. In the following section, MANET routing algorithms and mobility models are tested and evaluated as follow.

4.5.2 Simulation Results for Mobile IP communication within Home Networks supported by IP Networks

The second simulation experiment design enables integration of Mobile IP with the regular IP networks that allows communication of mobile nodes that uses Mobile IP for communication within different MANETs inside the home network with the support of regular IP networks. Data transmission between mobile nodes that uses Mobile IP between different MANETs inside the organization will arrive at local gateway by IP routing techniques of the IP network. These packets will forward to the mobile node through mobile gateways that can be used by the MANETs – which enables integration of MANETs and the regular IP networks.

In this simulation, the OLSR and AODV routing algorithms are selected for route data between mobile node that use Mobile IP for communication between MANETs within the home network. These routing algorithms are recommended to be used in such scenarios according to studies in [20], [39]. The mobility of the node that communicate in such scenario are designed based on Random Way Point mobility model and BonnMotion mobility model. These mobility models are generic mobility models used to design simulate node mobilities in mobile environment such as MANETS and VANETS. The simulation results of these routing algorithms and mobility models in MANET are presented in the following figures.

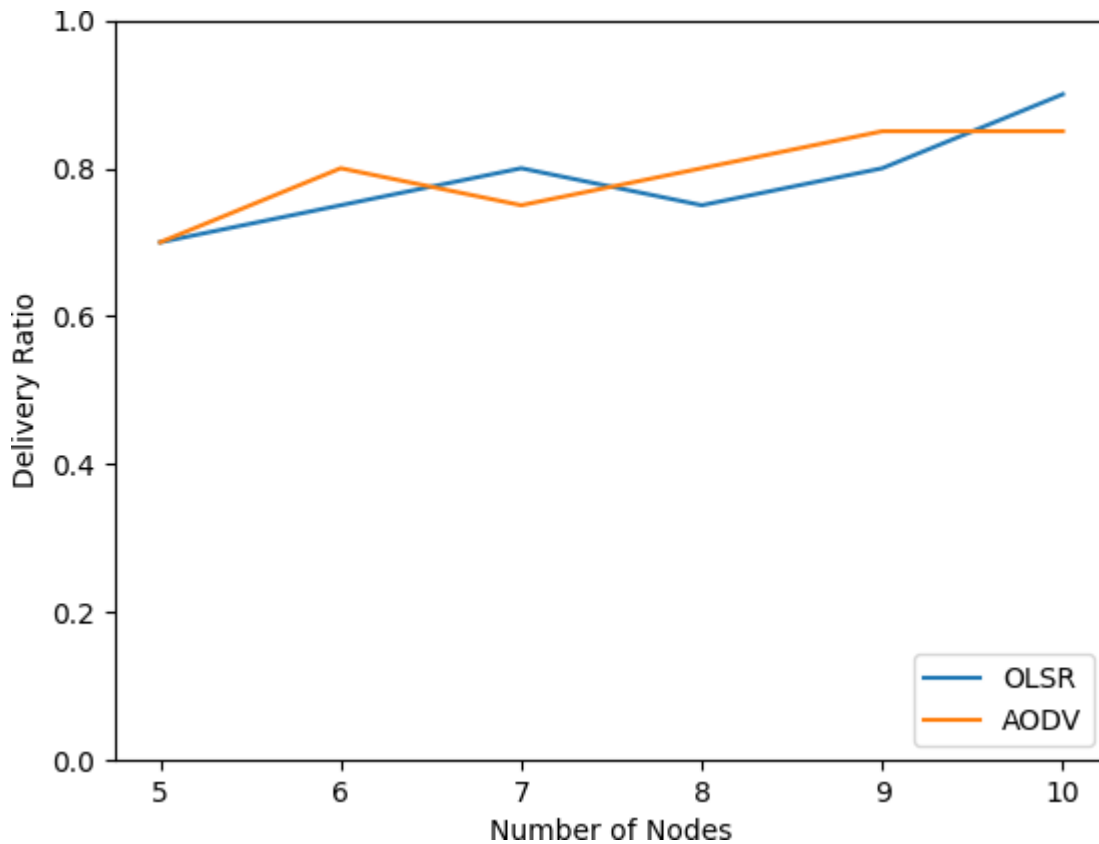


Figure 7 Random Walk Point Mobility Model in MANET

The simulation result for the MANET communications that implements Mobile IP for communication within the home network that uses a single home agent for integration with regular IP is presented in figure 7 - Random Walk Point Mobility for MANET. The simulation is done using NS-3 simulation tools with AODV and OLSR routing algorithms with Random Walk Point mobility model. According to the result graph, with the default mobility model implemented in NS-3 network simulation tool, AODV routing algorithm has a better overall network throughput on implementing Mobile IP communication. The overall network throughput performance for AODV routing algorithm is calculated to 79% (rounded down) and the overall network throughput performance for OLSR routing algorithm is calculated to 78% (rounded down). Therefore, for enhanced Mobile IP communication in default mobility models for MANET communication, AODV routing algorithms are efficient. But these network throughput results need an enhancement for better communication efficiency with implementing better mobility models.

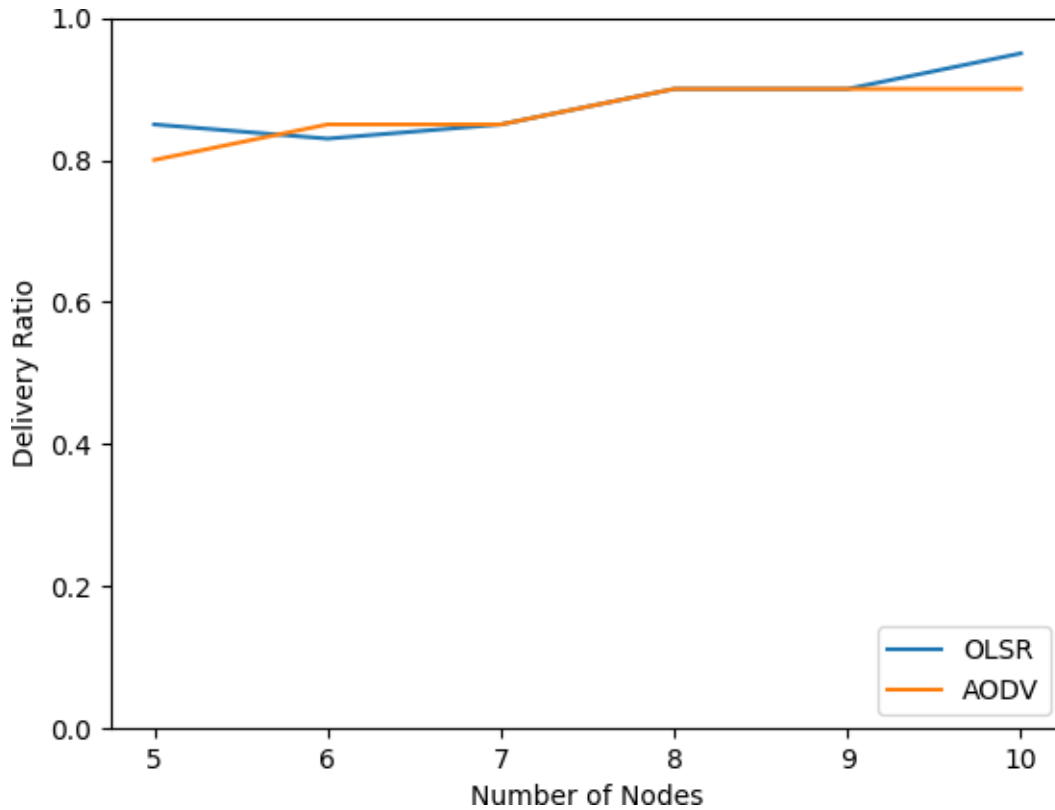


Figure 8 BonnMotion Mobility Model in MANET

The simulation result for the MANET communications that implements Mobile IP for communication within the home network that uses a single home agent for integration with regular IP is presented in figure 8 - BonnMotion Mobility for MANET. The simulation is done using NS-3 simulation tools with AODV and OLSR routing algorithms with BonnMotion mobility model. According to the result graph, with the default mobility model implemented in NS-3 network simulation tool, AODV routing algorithm has a better overall network throughput on implementing Mobile IP communication. The overall network throughput performance for AODV routing algorithm is calculated to 86% (rounded down) and the overall network throughput performance for OLSR routing algorithm is calculated to 85% (rounded down). Therefore, for enhanced Mobile IP communication in default mobility models for MANET communication, AODV routing algorithms are efficient.

Chapter Five

Conclusions and Future Works

5.1 Conclusions

Advance in technology enforces changes in the way humans culture react to their environment and affects humans' daily lives. One of the enduring trends in the computing industry over the years has been increasing portability. Mobility-enabled IP centric networks are becoming widely used to define networks that fulfill the users need to be able to establish and maintain a session between their computer and their network as they roam from one place to another. These networks use the established Internet Protocol (IP) addressing and routing mechanisms in concert with a new mobility protocol to deliver multimedia traffic to roaming users. Changes in the evolution of the IP network communications and advancements in networking paradigm yields new communication technologies, which is called Mobile IP communication.

On the underlying structure and infrastructure of regular IP network communications, Mobile IP communication enables a computer to roam freely on the Internet and on an organization's network while maintaining the same address assigned in the home network. Consequently, computing activities are not disrupted when the user changes the computer's point of attachment to the Internet or an organization's network. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. The packets addressed to a mobile node's home address are transparently routed to its care-of address.

Mobile IP is targeted to the users who are mobile and need to work in a flexible manner - in the office, on the road, at customer premises, or at home – any business that needs mobility. There are numerous applications that do not deal with well with regularly network changes – dynamic networks that frequently change their topology. In general, deploying a Mobile IP based solution ensures that such applications will work properly in a mobile environment. There are several

examples of applications where sudden changes in network and IP-address can cause problems. The most common ones are Remote Access VPNs, Database applications, Voice over IP and MANET related services including sensor networks.

In Mobile IP communication, a datagram moves from one point to another within the Mobile IP framework. This communication process can be summarized as follow. First the Internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process). If the mobile node is on its home network, the datagram is delivered through the normal IP process to the mobile node. Otherwise, the home agent picks up the datagram. If the mobile node is on a foreign network, the home agent forwards the datagram to the foreign agent. The foreign agent delivers the datagram to the mobile node. Datagrams from the mobile node to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The foreign agent forwards the datagram to the Internet host.

The communication process of mobile nodes that implement Mobile IP with wired nodes implemented with regular IP networks can be optimized for better performance. This communication enhancement can be considered as a communication security issue in this study. To enhance the communication efficiency of Mobile IP networks and regular IP networks two important communication aspects are explored and assessed in this study. These metrics are mobility models and routing algorithms. In this study, the role of mobility models and routing algorithms are experimentally assessed for their performance to enhance and secure the communication process.

5.2 Contributions

This study focuses on reviewing the state-of-art on trends and approaches in Mobile IP network communication with regular IP networks. Therefore, the Mobile IP communication framework to enable such communication is received for enhanced and secured communication. This study provides a solution by using mobility models and routing algorithms for the gaps demonstrated in problem section.

Generally, the contribution of this study can be summarized as:

- The proposed solution analyzes the mobility behaviors of mobile users (mobile nodes) that use Mobile IP for communication
- The proposed solution analyzes routing algorithms used by mobile users (mobile nodes) for communication that uses or implements Mobile IP framework for communication
- The results obtained from analysis of BonnMotion Mobility Models with AODV and OLSR routing protocols are presented with network throughput performance and the best result is discussed.
- The effect of the mobility models on the communication process of Mobile IP and regular IP networks are well explored and discussed in the result section.

5.3 Future Works

Despite substantial contributions of mobility models and routing algorithms in Mobile IP and regular IP network communications, there are a number of open research challenges that need to be addressed in order to further advance the area.

Mobile IP will be successful in the future as it has several notable features like no geographical limitation, no physical connectivity required, supports security, no modifications for the current IP address. Despite the fact that many solutions have been proposed, there are still many open research issues that need to be further investigated, such as the quality of service based on the MANET application priority when managing mobility handover, Performance Improvement in Mobile IP, Handover Protocols for Mobile IP, gateway advertisement control overheads, and investigating the feasibility of other MANET underlays such as OLSR and AODV to better meet the needs of an integrated network.

Appendices

A. Mobile IP Network Topology

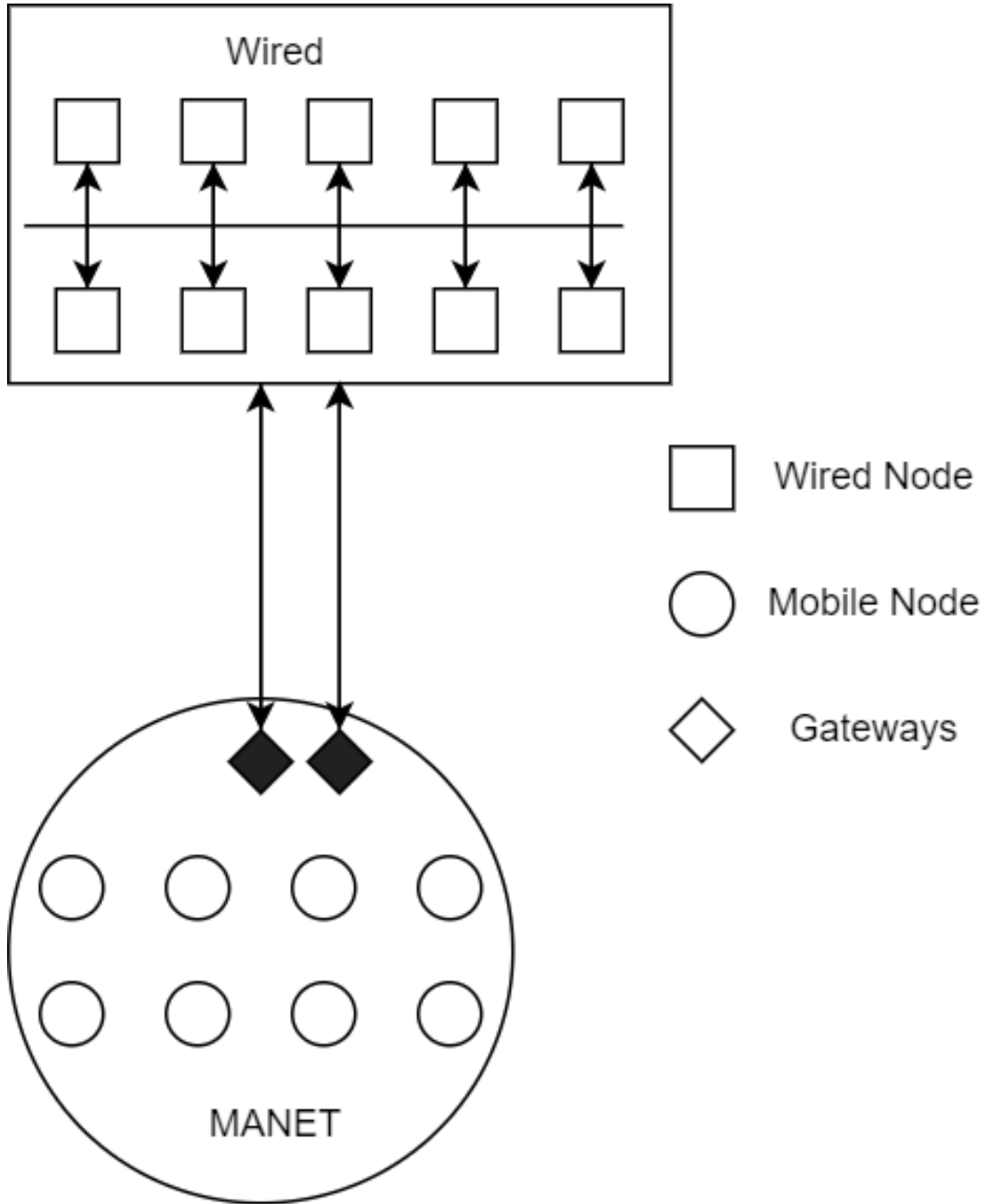


Figure 9 Mobile IP with two Gateways

B. MANET Network Topology

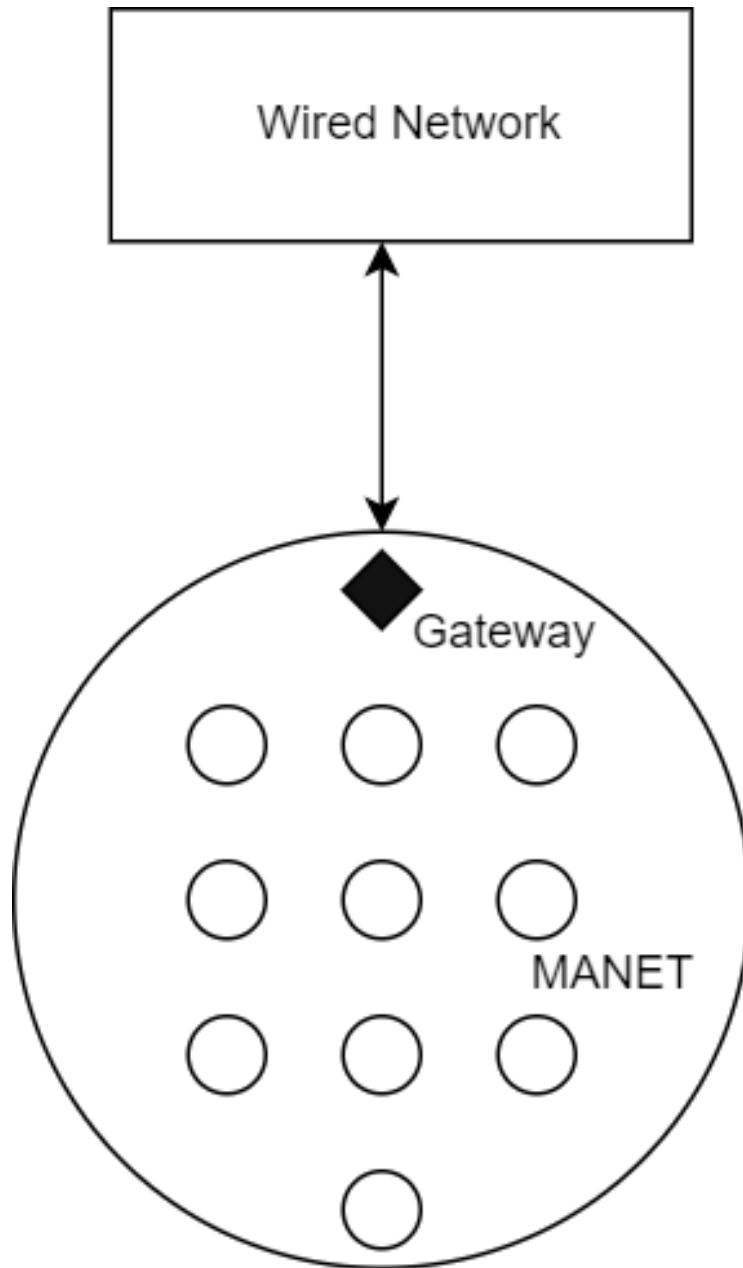


Figure 10 Manet with 1 Gateway

C. Sample Codes

```
# Create the backbone wifi net devices and install them into the nodes in
# our container
#
wifi = ns.wifi.WifiHelper()
mac = ns.wifi.WifiMacHelper()
mac.SetType("ns3::AdhocWifiMac")
wifi.SetRemoteStationManager("ns3::ConstantRateWifiManager",
                             "DataMode", ns.core.StringValue("OfdmRate54Mbps"))
wifiPhy = ns.wifi.YansWifiPhyHelper()
wifiPhy.SetPcapDataLinkType(wifiPhy.DLT_IEEE802_11_RADIO)
wifiChannel = ns.wifi.YansWifiChannelHelper.Default()
wifiPhy.SetChannel(wifiChannel.Create())
backboneDevices = wifi.Install(wifiPhy, mac, backbone)
#
# Add the IPv4 protocol stack to the nodes in our container
#
print ("Enabling OLSR routing on all backbone nodes")
internet = ns.internet.InternetStackHelper()
olsr = ns.olsr.OlsrHelper()
internet.SetRoutingHelper(olsr); # has effect on the next Install ()
internet.Install(backbone);
```

Figure 11 OLSR Configuration

References

- [1] “Introduction to Mobile IP - Cisco.”
https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/mobile_ip/mobil_ip.html
(accessed Dec. 08, 2022).
- [2] C. E. Perkins, “Mobile IP,” *IEEE Communications Magazine*, vol. 35, no. 5, pp. 84–99, May 1997, doi: 10.1109/35.592101.
- [3] G. Solmaz and D. Turgut, “A Survey of Human Mobility Models,” *IEEE Access*, vol. 7, 2019. doi: 10.1109/ACCESS.2019.2939203.
- [4] A. Ashraf, “A Review on Mobile Internet Protocol (Mobile IP),” *IJSRD-International Journal for Scientific Research & Development*, vol. 7, 2019.
- [5] T. Y. Wu, C. Y. Huang, and H. C. Chao, “A survey of mobile IP in cellular and mobile ad-hoc network environments,” *Ad Hoc Networks*, vol. 3, no. 3, 2005, doi: 10.1016/j.adhoc.2003.09.011.
- [6] F. M. Abduljalil and S. K. Bodhe, “A survey of integrating ip mobility protocols and mobile ad hoc networks,” *IEEE Communications Surveys and Tutorials*, vol. 9, no. 1, 2007. doi: 10.1109/COMST.2007.358969.
- [7] S. Ding, “A survey on integrating MANETs with the Internet: Challenges and designs,” *Comput Commun*, vol. 31, no. 14, pp. 3537–3551, Sep. 2008, doi: 10.1016/j.comcom.2008.04.014.
- [8] C. Ahlund and A. Zaslavsky, “Integration of ad hoc network and IP network capabilities for mobile hosts,” in *10th International Conference on Telecommunications, ICT 2003*, 2003, vol. 1. doi: 10.1109/ICTEL.2003.1191288.
- [9] L. Lamont, M. Wang, L. Villasenor, T. Randhawa, R. Hardy, and P. McConnel, “An IPv6 and OLSR based architecture for integrating WLANs & MANETs to the Internet,” in *International Symposium on Wireless Personal Multimedia Communications, WPMC*, 2002, vol. 2. doi: 10.1109/WPMC.2002.1088290.
- [10] M. K. Denko and C. Wei, “A multi-gateway-based architecture for integrating ad hoc networks with the internet using multiple foreign agents,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 3, no. 2, 2008, doi: 10.1504/IJAHUC.2008.017003.
- [11] A. Prasad and N. Prasad, “802.11 WLANs and IP networking: security, QoS, and mobility,” *Communications*, 2005.

- [12] S. F., "The Security Aspects of Mobile IP," *Int J Appl Inf Syst*, vol. 9, no. 5, 2015, doi: 10.5120/ijais2015451417.
- [13] Y. Jung and M. Peradilla, "Tunnel gateway satisfying mobility and security requirements of mobile and IP-based networks," *Journal of Communications and Networks*, vol. 13, no. 6, 2011, doi: 10.1109/JCN.2011.6157474.
- [14] L. H. Yen and C. S. Jian, "Mobile IP extension to ad hoc wireless networks," *Journal of Internet Technology*, vol. 8, no. 1, 2007.
- [15] H. Ammari and H. El-Rewini, "Integration of mobile ad hoc networks and the internet using mobile gateways," in *Proceedings - International Parallel and Distributed Processing Symposium, IPDPS 2004 (Abstracts and CD-ROM)*, 2004, vol. 18. doi: 10.1109/ipdps.2004.1303253.
- [16] K. U. R. Khan, R. U. Zaman, and A. Venu Gopal Reddy, "Integrating mobile ad hoc networks and the internet: Challenges and a review of strategies," in *3rd IEEE/Create-Net International Conference on Communication System Software and Middleware, COMSWARE*, 2008. doi: 10.1109/COMSWA.2008.4554470.
- [17] A. Alshalan, S. Pisharody, and D. Huang, "A Survey of Mobile VPN Technologies," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, 2016, doi: 10.1109/COMST.2015.2496624.
- [18] Z. Ren, C. K. Tham, C. C. Foo, and C. C. Ko, "Integration of mobile IP and multi-protocol label switching," in *IEEE International Conference on Communications*, 2001, vol. 7. doi: 10.1109/icc.2001.937032.
- [19] Y. C. Tseng, C. C. Shen, and W. T. Chen, "Integrating mobile IP with ad hoc networks," *Computer (Long Beach Calif)*, vol. 36, no. 5, 2003, doi: 10.1109/MC.2003.1198236.
- [20] K. U. R. Khan, A. V. Reddy, and R. U. Zaman, "An efficient integrated routing protocol for interconnecting Mobile ad hoc Networks and the Internet," in *Proceedings of the International Conference on Advances in Computing, Communication and Control, ICAC3 '09*, 2009. doi: 10.1145/1523103.1523195.
- [21] M. al Mojamed, "Integrating IP Mobility Management Protocols and MANET: A Survey," *Future Internet*, vol. 12, no. 9, 2020, doi: 10.3390/FI12090150.
- [22] S. Kumar, A. Kumar, K. Nigam, and R. Kumar, "PERCEPTIVE APPROACH FOR ROUTE OPTIMIZATION IN MOBILE IP," / *Indian Journal of Computer Science and Engineering*, vol. 1, pp. 313–320.

- [23] “[PDF] Triangle Routing in Mobile IP (Final Report) | Semantic Scholar.”
[https://www.semanticscholar.org/paper/Triangle-Routing-in-Mobile-IP-\(-Final-Report-\)-Mahmood/dd50737f8850b3a3c3b17137cc5e9ebfeb215c9f](https://www.semanticscholar.org/paper/Triangle-Routing-in-Mobile-IP-(-Final-Report-)-Mahmood/dd50737f8850b3a3c3b17137cc5e9ebfeb215c9f) (accessed Dec. 08, 2022).
- [24] T. Ihara, H. Ohnishi, and Y. Takagi, “Mobile IP route optimization method for a carrier-scale IP network,” *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS*, 2000, doi: 10.1109/iceccs.2000.873934.
- [25] J. Park and Y. Mun, “The layer 2 handoff scheme for mobile IP over IEEE 802.11 wireless LAN 1,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3043, 2004, doi: 10.1007/978-3-540-24707-4_128.
- [26] I. W. Wu, W. S. Chen, H. E. Liao, and F. F. Young, “A seamless handoff approach of mobile IP protocol for mobile wireless data networks,” *IEEE Transactions on Consumer Electronics*, vol. 48, no. 2, 2002, doi: 10.1109/TCE.2002.1010140.
- [27] G. Yue, Z. Zeng, Q. Wu, and N. Zeng, “An efficient handoff scheme of mobile IP adapting initiative predictive neighbor,” *Jisuanji Gongcheng/Computer Engineering*, vol. 32, no. 13, 2006.
- [28] C. Blondia, N. van den Wijngaert, G. Willems, and O. Casals, “Performance analysis of optimized smooth handoff in Mobile IP,” in *Proceedings of the International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2002. doi: 10.1145/570758.570763.
- [29] S. Ding, “Mobile IP handoffs among multiple internet gateways in mobile ad hoc networks,” *IET Communications*, vol. 3, no. 5, 2009, doi: 10.1049/iet-com.2008.0275.
- [30] J. Sen, “Mobility and Handoff Management in Wireless Networks,” in *Trends in Telecommunications Technologies*, 2010. doi: 10.5772/8482.
- [31] C. E. Perkins and K. Y. Wang, “Optimized smooth handoffs in Mobile IP,” *IEEE Symposium on Computers and Communications - Proceedings*, 1999, doi: 10.1109/iscc.1999.780874.
- [32] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A design science research methodology for information systems research,” *Journal of Management Information Systems*, vol. 24, no. 3, 2007, doi: 10.2753/MIS0742-1222240302.
- [33] A. Elmangoush, A. Corici, A. Al-Hezmi, and T. Magedanz, “Mobility management for machine-to-machine (M2M) communications,” *Machine-to-machine (M2M)*

- Communications: Architecture, Performance and Applications*, pp. 187–206, Jan. 2015, doi: 10.1016/B978-1-78242-102-3.00011-3.
- [34] “A Survey on Mobile IP.” https://www.cse.wustl.edu/~jain/cis788-95/ftp/mobile_ip/index.html (accessed Dec. 08, 2022).
- [35] H. Ohnishi, Y. Takagi, and A. Kurokawa, “Mobile IP technology,” *NTT Technical Review*, vol. 2, no. 7, 2004.
- [36] K. Leung, D. Shell, W. D. Ivancic, D. H. Stewart, T. L. Bell, and B. A. Kachmar, “Application of mobile-IP to space and aeronautical networks,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 16, no. 12, 2001, doi: 10.1109/62.974834.
- [37] J. Chandrasekaran, “Mobile IP : Issues , Challenges and Solutions,” *Solutions*, 2018.
- [38] N. Swami and A. Bairwa, “A Literature Survey of MANET,” *International Research Journal of Engineering and Technology*, vol. 03, no. 02, 2016.
- [39] S. Munira, S. Humaira, S. Fahin, A. Siddik, and A. K. M. Fazlul Haque, “DSR and OLSR routing protocol based performance evaluation and integration on MIP with MANET,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, 2019, doi: 10.11591/ijeecs.v17.i3.pp1306-1312.
- [40] GEETHANJALI. N, BRINDHA. G, D. MOL.A, and SINDHU. M, “APPLICATION AND SIMULATION OF ROUTE OPTIMIZATION IN MOBILE IP,” *International Journal of Computer and Communication Technology*, 2016, doi: 10.47893/ijcct.2016.1358.
- [41] P. P. Rajesh Pal, “Route Optimization in Mobile IP,” *Motorola Whitepaper*, 2002.
- [42] C. Perkins and D. Johnson, “Route optimization for mobile IP,” *Cluster Comput*, vol. 1, 1998.
- [43] M. Benzaid, P. Minet, K. al Agha, C. Adjih, and G. Allard, “Integration of mobile-IP and OLSR for a universal mobility,” in *Wireless Networks*, 2004, vol. 10, no. 4. doi: 10.1023/B:WINE.0000028542.48770.01.
- [44] M. W. Xu, Q. Wu, G. L. Xie, and Y. J. Zhao, “The impact of mobility models on mobile IP multicast research,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 4, no. 3–4, 2009, doi: 10.1504/IJAHUC.2009.024522.
- [45] V. Casares-Giner, V. Pla, and P. Escalle-García, “Mobility models for mobility management,” *Lecture Notes in Computer Science (including subseries Lecture Notes in*

- Artificial Intelligence and Lecture Notes in Bioinformatics*), vol. 5233, 2011, doi: 10.1007/978-3-642-02742-0_30.
- [46] F. Bai and A. Helmy, “A Survey of Mobility Models in Wireless Adhoc Networks,” *Wireless Ad Hoc and Sensor Networks*, 2004.
- [47] T. Camp, J. Boleng, and V. Davies, “A survey of mobility models for ad hoc network research,” *Wirel Commun Mob Comput*, vol. 2, no. 5, 2002, doi: 10.1002/wcm.72.
- [48] R. Attia, R. Rizk, and H. A. Ali, “Internet connectivity for mobile ad hoc network: a survey based study,” *Wireless Networks*, vol. 21, no. 7, 2015, doi: 10.1007/s11276-015-0922-3.
- [49] C. Y. Yang and C. Y. Shiu, “A secure mobile IP registration protocol,” *International Journal of Network Security*, vol. 1, no. 1, 2005.
- [50] S. Rathi and K. Thanushkodi, “Performance analysis of mobile IP registration protocols,” *WSEAS Transactions on Computers*, vol. 8, no. 3, 2009.
- [51] K. M. Al-Adhal and Dr. S. S. Tyagi, “Security Mechanism for Mobile IP,” *International Journal of Engineering Research & Technology*, vol. 3, no. 5, May 2014, doi: 10.17577/IJERTV3IS051387.
- [52] “Key Mechanism in Mobile IP.” https://www.brainkart.com/article/Key-Mechanism-in-Mobile-IP_9884/ (accessed Dec. 09, 2022).
- [53] P. M. Ruiz, F. J. Ros, and A. Gomez-Skarmeta, “Internet connectivity for mobile ad hoc networks: Solutions and challenges,” *IEEE Communications Magazine*, vol. 43, no. 10, 2005, doi: 10.1109/MCOM.2005.1522134.
- [54] A. T. Cabrera, “Integration of Mobile Ad Hoc Networks into IP-Based Access Networks,” pp. 527–561, 2009, doi: 10.1007/978-1-84800-328-6_21.
- [55] C. Umana and S. Lorena, “IP Mobility Support in Multi-hop Vehicular Communications Networks,” *undefined*, 2012.
- [56] L. Lamont, M. Wang, L. Villasenor, T. Randhawa, and S. Hardy, “Integrating WLANs & MANETs to the IPv6 based Internet,” in *IEEE International Conference on Communications*, 2003, vol. 2. doi: 10.1109/icc.2003.1204528.
- [57] D. Ahmat, M. Barka, and D. Magoni, “Mobile VPN Schemes: Technical Analysis and Experiments,” in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics*

and Telecommunications Engineering, LNICST, 2018, vol. 208. doi: 10.1007/978-3-319-66742-3_9.

- [58] G. Montenegro, “Bi-directional Tunneling for Mobile IP,” *undefined*, 1996.
- [59] B. Al-Kasasbeh, R. E. Al-Qutaish, and K. Al-Sarayreh, “Indirect Routing of Mobile IP: A Non-Encapsulation Approach,” *undefined*, 2008.
- [60] S. Jin, “Implementation and Analyses of the Mobile-IP Protocol,” *undefined*, 2008.
- [61] R. A. Khan and A. H. Mir, “IPsec in Mobile IP : A Survey,” 2013.
- [62] K. Smolak, W. Rohm, K. Knop, and K. Siła-Nowicka, “Population mobility modelling for mobility data simulation,” *Comput Environ Urban Syst*, vol. 84, 2020, doi: 10.1016/j.compenvurbsys.2020.101526.
- [63] M. al Mojamed, “Integrating Mobile Ad Hoc Networks with the Internet Based on OLSR,” *Wirel Commun Mob Comput*, vol. 2020, 2020, doi: 10.1155/2020/8810761.