Traffic Engineering Multi-Layer Optimization for Wireless Mesh Network Transmission - A Campus Network Routing Protocol Transmission Performance Enhancement

A Thesis Submitted for the Degree of Doctor of Philosophy

By

Okechukwu Emmanuel Muogilim - 0621938

School of Engineering and Design

Wireless Networks and Communication Centre

Brunel University, Uxbridge

Supervisors – Prof John Cosmas

Dr Jonathan Loo

May 2011

TABLE OF CONTENTS

LIST OF FIGURES

Figures ***Page***

LIST OF TABLES

Tables ***Page***

ABBREVIATIONS

ACK – Acknowledgement

AODV- Ad hoc on demand distant vector

ATOM – Any Transport Over MPLS

CS/ CSMA- Collision sense multiple access; collision avoidance

DiffServ – Differentiated Services architecture

DSDV- Dynamic sequenced distant vector

DSR- dynamic state routing

HSR- hierarchal state routing

IEEE- Institute of electrical and electronic engineering

IETF- Internet Engineering Task force

IPSEC-Internet protocol security

ISIS- intermediate system, intermediate systems protocol

LSP – Label Switched Path

LSR – Label Switched Router

MAC-medium access control

MANET-Mobile ad hoc network

MR-multi radio

MPLS-Multi-protocol label switching

MIRA – Minimum Interference Routing Algorithm

OLSR-Optimized link state routing

OSI-Open system international

OSPF-Open shortest path first

PHB – Per Hop Behaviour

SA – Simulated Annealing

SLA – Service Level Agreement

STP- Spanning tree protocol

TE-Traffic Engineering

TORA- temporary ordered routing algorithm

VPN-Virtual private network

WLAN-Wireless local access networks

WMN-Wireless mesh networks

ZRP-Zone routing protocol

ABSTRACT

The wireless mesh network is a potential network for the future due to its excellent inherent characteristic for dynamic self-healing, self-configuration and self-organization. It also has the advantage of easy interoperability networking and the ability to form multi-linked ad-hoc networks. It has a decentralized topology, is cheap and highly scalable. Furthermore, its ease in deployment and easy maintenance are other inherent networking qualities. These aforementioned qualities of the wireless mesh network bring advantages to transmission capability of heterogeneous networks.

However, transmissions in wireless mesh network create comparative performance based challenges such as congestion, load-balancing, scalability over increasing networks and coverage capacity. Consequently, these challenges and problems in the routing and switching of packets in the wireless mesh network routing protocols led to a proposal on the resolution of these failures with a combination algorithm and a management based security for the network and its transmitted packets. There are equally contentious services like reliability of the network and quality of service for real-time multimedia traffic flows with other challenges such as path computation and selection in the wireless mesh network.

This thesis is therefore a cumulative proposal to the resolution of the outlined challenges and open research areas posed by using wireless mesh network routing protocol. It advances the resolution of these challenges in the mesh environment using a hybrid optimization – traffic engineering, to increase the effectiveness and the reliability of the network.

It also proffers a cumulative resolution of the diverse contributions on wireless mesh network routing protocol and transmission. Adaptation and optimization are carried out on the wireless mesh network designed network using traffic engineering mechanism and technique.

The research examines the patterns of mesh packet transmission and evaluates the challenges and failures in the mesh network packet transmission. It develops a solution based algorithm for resolutions and proposes the traffic engineering based solution.. These resultant performances and analysis are usually tested and compared over wireless mesh IEEE802.11n or other older proposed documented solution.

This thesis used a carefully designed campus mesh network to show a comparative evaluation of an optimal performance of the mesh nodes and routers over a normal IEE802.11n based wireless domain network to show differentiation by optimization using the created algorithms. Furthermore, the indexes of performance being the metric are used to measure the utility and the reliability, including capacity and throughput at the destination during traffic engineered transmission. In addition, the security of these transmitted data and packets are optimized under a traffic engineered technique.

Finally, this thesis offers an understanding to the security contribution using traffic engineering resolution to create a management algorithm for processing and computation of the wireless mesh networks security needs.

The results of this thesis confirmed, completed and extended the existing predictions with real measurement.

ACKNOWLEDGEMENTS

First and foremost, I thank God for giving me this opportunity and blessing of life and good health to the end of this project. I also extend special gratitude to my project supervisors - Professor John Cosmas and especially Dr Jonathan Loo for accepting me, treating me with great respect and professionalism, showing me the ropes and different types of projects and opportunities and finally, always offering to assist me even when he has left the university. He facilitated my discovery of the professional side of my studies and career. He was like an elder brother, tolerant of my numerous problems. He also facilitated my achievement of this project, giving me his time, advice and resources. He gave me the confidence I needed; I commend his patience for my challenges. I also wish to thank Prof Al Raweshidy who guided me and showed me the initial ropes in my studies and research.

My parents were my backbone financially, with other help coming from my brothers Chike, Nnamdi and Chuma. This gave me the needed impetus and time to concentrate on my work. My family was like my fortress during this period - in prayers and in constant support - I thank you all. Special gratitude to my mother, who gave me a substantial part of her pension for my tuition and other numerous sacrifices, I thank you all from my heart. I am grateful for the support of my family during the period.

To my colleagues and staffs of WNCC and School of Engineering and Design I want to use this medium to say I am grateful for the support and contributions you made helping me achieve on my PhD; without all of you it would have been hard and boring.

I have special thanks for Idia and my son - Chidera for their patience and understanding throughout the period, for the times I was away to concentrate on my studies. I would like to dedicate this thesis to everyone I mentioned above and all those who prayed for me throughout my research and have been supporting me.

Author's Declaration

I certify that all material in this thesis which is not my own work has been identified and that no material has previously been submitted and approved for the award of a degree by this or any other University.

Signature …….....

CHAPTER 1

Introduction

1.1. Motivation

Emerging wireless mesh network IEEE802.11n [1] has numerous advantages over the traditional MANET [2] and ad hoc networks. The inherent advantages are due to its architectural design differences comparative to the traditional ad-hoc ones. Its routers and gateways routers are semi-mobile and they form the backbone of the infrastructure coupled with the access points (AP). The wireless mesh clients are often linking and co-operating with other networking nodes and devices. They are dynamic, mobile and are easily forming mesh of networks. They are usually located at the peripherals of the mesh infrastructure.

The WMN [3] due to these unique characteristics and structure has inherent qualities such as self-healing, self-configuration and organization. In addition, it is cheap and easy to maintain and quick in deployment. These adaptive qualities give wireless mesh a commercial potential advantage for broadband [4] access, for multimedia and real-time traffic transmission and high demanding communication and finally for high coverage capacity and a comparative higher scalability in increasing networks.

High demanding and contentious communication in digital network usually means introduction of interference, low scalability and poor load balance in the mesh network. It also infers the unreliability of fairness and quality of service (QoS) of the transmission. Mostly, multimedia network transmission and priority routing over wireless mesh creates a bottleneck of arrays of contentious signals over a limited bandwidth such as shown in figure 1.1. These raise diverse challenges and problems for WMN. The transmission over WMN can be re-modelled to improve efficiency, to enhance the quality of service and reliability of the network in communication.

The transmission in network uses routing and switching of data bound packets for end-to-end transmission in WMN. In the WMN, this routing of

network bound traffic is in layer 3 of the ISO/OSI layer standard. The routing protocol determines the routing type that the network transmission employs. It is the underlying protocol that runs the routing, the network and packet transmission in the mesh. The WMN is different from the old traditional ad hoc networks due to the mobility of the mesh router and the dynamic high mobility of the mesh clients. Optimizing [5] the routing protocol is carried out using a TE [6] technique. TE is the controlling of traffic from source to destination to achieve a higher throughput and to ensure a faster transmission. It is the mapping of the source node to the destination node using matrices of the traffic transmission and using delay-bound constraints as metrics. [7]

We explored optimization using TE [8] of the routing protocol of the WMN. Networking in a wireless network share a common medium; there are many challenges which determine the channel capacity. Simultaneous traffic of signal transmitted from the source node to the destination such as shown in figure 1.1 consist of high definition video signal, voice signal and many other multimedia signal as shown in figure 1.1 with high bandwidth demand of the already limited bandwidth in the mesh network. This simultaneous flow of signal causes contention in access networks like WMN and packets are lost and dropped during the process and on transmission to the destination node. The QOS and reliability of the packets and data integrity are all affected by this interference on the transmission medium. These aforementioned, affect the overall channel capacity of the network.

There are two ways of transmission as shown in figure 1.1 in an access based medium: contention and contention free. The contention based approach uses Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). The IEEE 802.11 standard [1] which defines specifications for Wireless Local Area Networks (WLANs) is one example in which the 802.11 compliant wireless stations compete for channel occupancy. However, the contention free approach commonly uses Time Division Multiple Access (TDMA) in which one or more fixed or variable size time slots are assigned to a device. The method by which a networking device gets access to the wireless medium is crucial in determining the techniques to be used to efficiently utilize the medium as well

as the transmission flow from the source node to the destination nodes in WMN.

The transmission of these variable signal specified standards are engineered using traffic engineering technique to optimize the following:

- The throughput at the destination node
- The packet data integrity during transmission – security of the packets
- To improve the reliability of the communication
- To improve the basic data rate of the packet data while in transmission
- To reduce contention over the wireless mesh transmission domain
- Coverage capacity
- Scalability
- Load balance
- Security
- Faster speed of transmission over the WMN

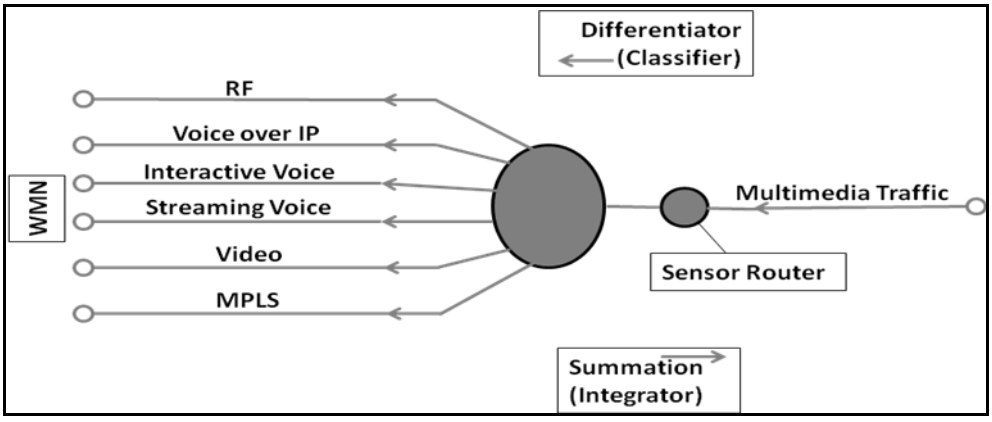


Figure 1.1: Multimedia traffic in a transmission in WMN

1.2. Aim of Research

The research presented in this thesis is in multiples of diverse contributions to resolving and showing optimization of WMN routing protocol using TE techniques. These contributions are the following:

1. A proposal for multi-protocol optimization using a design resolution to these challenges including: congestion, delay and interference with its resultant high overhead in a multi-radio and multi-channel WMN. We implement TE technique over WMN-routing protocol (RP) to formulate higher coverage capacity protocol with fast-forward, linearly-sequenced and deterministic algorithm to solving the scalability, load balance and low-path computation challenges in the WMN-RP. We propose an adaptive link-state traffic engineered-routing protocol algorithm with least cost (ALSTE-RP) for WMN. ALSTE-RP is compared to a normal WMN packet transmission to show performance based optimization.

2. An investigation of TE management model approach to resolving WMN security threats and addressing the security challenges in the WMN routing and transmission operation. The proposed TE model minimizes the effect of bandwidth depletion, traffic flooding attacks and distributed denial of service (DDoS) in WMN. It offers a new security resolution model for the dynamic and distributed-sequenced WMN through traffic engineering management approach.

3. Finally, we analyzed the performances of the metric used and its advantages, while the open research issues were raised and discussed too. We conclude and proffer ideas for the future using the enumerated and proposed designs.

1.3. Overview of the Wireless Network – Traffic Engineering

Wireless mesh networks traffic engineering (WMN-TE) optimization is a co-operative and hybrid technique of the wireless mesh infrastructure network where the functionalities of the mesh environment transmission is enhanced by low-computational IP traffic engineered configuration. The IP nodes of the WMN and the router gateways access of the backbone infrastructure networks are configured to act as matrices of set source data-packet and destinations in delay-based constrained routing to achieve WMN-TE.

The WMN is self-healing, self-configuring and has inherent fault tolerance against other networks core qualities. These aforementioned are adaptable internetwork characteristics qualities which prompted international standardization organizations to specify the mesh networking modes: IEEE802.11, IEEE802.15, IEEE802.16 and IEEE802.20. .These standardized modes are specification of extensions for the ad hoc network. In addition, an optimal design criterion means that a WMN has different set of deployment objectives from application point for changes in requirements such as topology changes or inefficiency of the protocols or failure of the functioning parts.

WMN can function as a complementary and access network to the wireless networks or broadband networks. The node mobility and the topological differences are the two areas that WMN differ from ad hoc networks. The topological diversity in these networks contributes to the difference in performance in routing. WMN is a network for the future and it has promising commercial potential. Its primary advantages are its inherent fault tolerance against network failures and its ability to form multiple networks and more, especially its broadband capability. WMN are characterised by static wireless networks relay nodes providing distributed infrastructure for mobile client nodes over a mesh topology.

In order to improve the throughput capacity in WMN, it has an added functionality of multi-radio state (WMN-MR). This is essential to supporting the diverse traffic demands during multimedia transmissions. These multi-radio specifications in WMN networks are better than single radio communication and they give varied data rate speed of channel transmission. The routing protocol of the WMN depends on the network infrastructure. It also depends on the topology and the different designs of the wireless mesh routing protocol. The design of the metric, the route reliability, the overhead and path computation, the load balance and finally the route failure recovery are the deterministic properties of the qualities of the routing protocol in a wireless mesh scenario. In addition, to the protocol design challenges, a WMN sometimes employ system-level solutions and designs. Some examples of

these are the cross-layer optimization system design, design for security and trust in the network, the network management designs and network lows and survivability challenges designs.

The most popular traffic application in networks is the gateway via internet transmissions. WMN act as an access network to the internetworks and broadband networks. In a campus wide area network, it serves the community with broadband internet access for their businesses and home usage. In this situation, voice and data packets are transmitted over WMN infrastructure such as in VOIP and Skype application services. It therefore became necessary to provide support and infrastructure to real–time and best effort delivery services over the WMN. The layer heterogeneity is another challenge in the WMN as data may pass through different networks before being delivered to the WMN. The experiences and analysis drawn from its deployment and the study of the WMN created the key challenges with respect to the scalability, extensibility, reliability and cognition. These further led to critical thinking of enhancing packet transmission in WMN communication using TE.

1.3.1. The routing protocol design challenges

Unlike the routing protocol for ad hoc networks, the routing protocol for WMN varies in many factors: the topology of the network, the network scenario and the different design issues such as the routing metric, the load balance, overheads and the node mobility. Other factors like the reliability of the network, the route adaptability and the support infrastructure also play major roles in deciding the routing protocol. However, one of the most important criteria for effective routing protocol is the throughput capacity and minimal overheads whilst transmitting data packets.

The design of the routing protocol is therefore an important aspect in designing a WMN-MR which in turn depends on the design of the WMN architecture. It may be dependent on deployment factors too or the network applicability. However the routing protocol design of a WMN can be classified into different categories such as:

- The routing topology

- The routing backbone
- The routing information

The routing protocol can be flat, hierarchal or hybrid based on the topology of the routing protocol. In hierarchal routing topology such as in figure 1.2, a routing hierarchal level is built in the mesh client and router nodes in the mesh networks in such a manner that the path selection nodes from the lower level progressively use the higher level nodes information to obtain a path AND information such as shown in fig 1.2. Flat state routing protocol on the other hand does not have higher level of hierarchies. Each node in the structure finds its own path to the destination. In addition, tree design based routing protocol also exist. This is a situation where the backbone routing is designed to forms a topological tree-network. An example of such is the spanning tree protocol (STP) IP routing technique in the backbone network. The designed routing protocol implemented at the WMN layer could be backbone or backboneless. In backbone routing protocol in WMN, the mesh can be optimized for throughput, quality of service and network scalability. Some other routing protocols use a mixture of both or rather segments of the network using different routing protocols are called hybrid routing protocol.

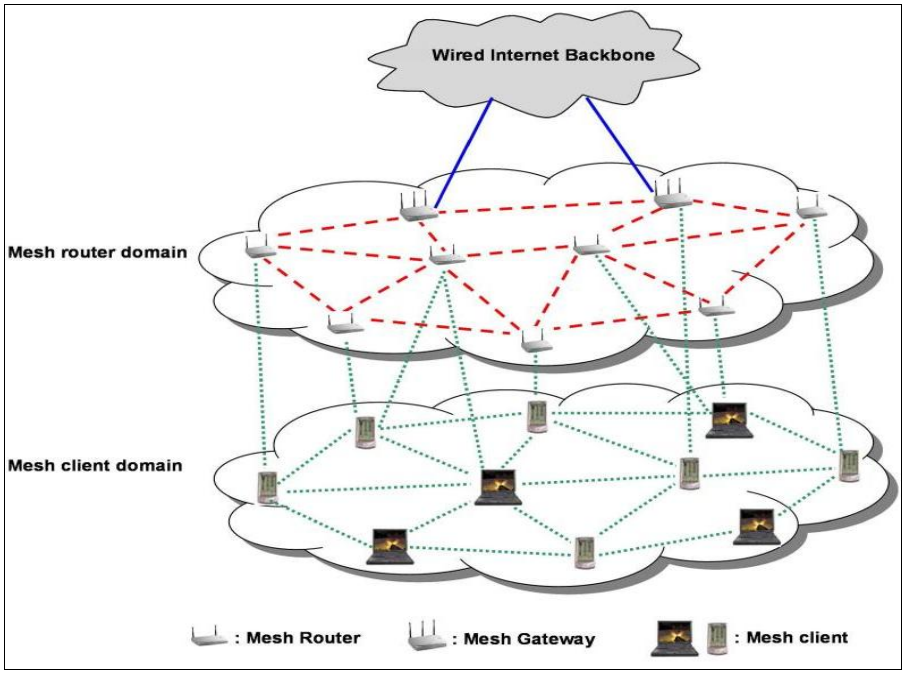


Figure 1.2: Hierarchal wireless mesh network scenario

Routing protocols are either proactive or reactive and get their names by the mechanism of information updating as shown in figure 1.3. The proactive routing protocols for example periodically update the routing table with information of the mesh network nodes and routers without prompting from a communicating node while in the reactive routing protocol; information update is carried out as a resultant to the node in the network trying to communicate with another node by prompting or routing transmission. Examples of the reactive routing protocol are the Ad hoc on demand distant vector routing protocol (AODV) and the Dynamic source routing protocol (DSR), while the Destination sequenced distant vector routing protocol (DSDV) and the optimized link state routing protocol (OLSR) are the proactive types as shown in the figure 1.3. The hybrid takes the advantages of both qualities of the table-driven and the on demand approach qualities in routing packet data. An example of the hybrid routing protocol is the zone routing protocol (ZRP).

In multi-radio, multi-hop and heterogeneous communication, the metric for the routing protocol is an important design factor. It determines the level of key performance index acceptance and rating in wireless mesh transmissions. A routing metric is the routing weight, parameter or value that is closely associated to its links and paths. Hop counts represent the simplest routing metric in WMN computation.

1.3.2. Mesh routing and forwarding

The WMN routing has been an open research topic. The packet frames are routed over wireless mesh infrastructure through the backbone networks or nodes to the gateway routers. The path selection and the mesh forwarding are used to define the process of selecting a single-hop or multi hop paths and later forwarding through these paths to destination nodes. WLAN mesh routing protocol adapts the earlier work done by the IETF-MANET work group as well as the wireless STP. Data packets use the IEEE 802.11 standard four-address format with 802.11e extensions for 802.1Q tag transfer and some additional mesh specific information. Mesh path selection is the process baseline management messages for neighbour discovery, link state

measurements and maintenance and the location of active path selection protocol. IEEE802.11s draft standard allows the WLAN mesh to be implemented with any path selection metric.

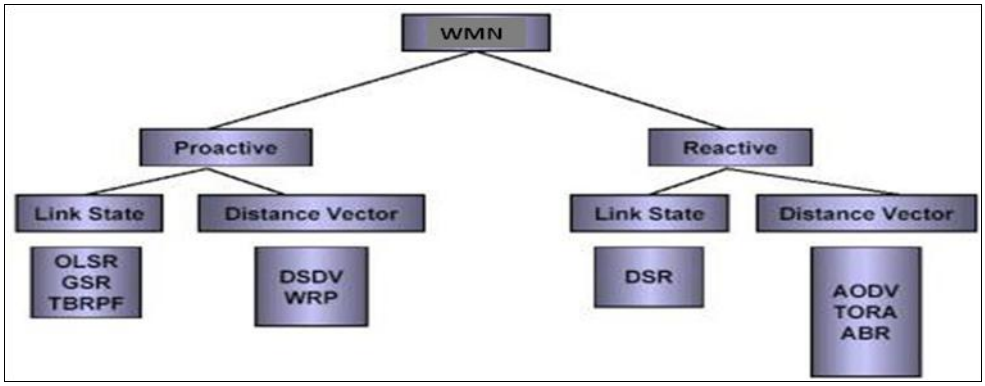


Figure 1.3: WMN routing protocols

1.4. Aim and objectives of the thesis

The aim of this thesis is to investigate and develop a novel routing protocol using the TE technique for WMN and security for campus sized wide area network. It also shows demonstrable strength as access transmission technique for broadband networks. This technique will improve scalability in increasing WAN deployments and can be used in fast forwarding secure transmission over WMNs. In view of the WMN having challenges in the routing protocol for multi-layer internetwork heterogeneous usage. This resulted to lower output data rate and overall low throughput capacity in the routing protocol.

In addition, it addresses the topological challenges and enhances backbone design for effective data packet routing/switching from source client node to destination node. The TE-WMN routing protocol and security management was experimented and the performance of the analysis made through tested measurements indicated validation of effectiveness in usage. These tested analyses include the effects of the reliability, throughput, routing overhead, end-to-end delay, delivery ratio, traffic mobility, and scalability. These were modelled using OPNET 16.0. The simulation results were computed over

WMN environment and readings taken; the routing metric is applied to the statistical readings for relationship with the algorithm.

The following was considered to achieve the objectives:

- A planned modelled framework and infrastructural architectural design of a WMN environment with import of traffic engineering from VPN, MPLS and VOIP voice-traffics over mesh scenario.

- A developed algorithm for security based management approach for WMN.

- Validating the optimized gain through simulated performance gain in analysis.

- Completing and extending the prediction and hypothesis with a real-time measurement results.

- Validating the effectiveness of the approach and techniques in modelling and simulating traffic engineering –MPLS over mesh networks.

- Observing and identifying the critical technical differences between the WMN design scenario and the initial state before optimization.

1.5. Main research contributions

1. A measurement based technical survey analysis of WMN routing protocols with a proposed views on TE over mesh routing protocol. Classification and open research challenge analysis.

2. A planned design of a campus based WMN with imported traffic of VOIP, whiteboard, VPN MPLS and a TE configuration to adapt the MPLS for transmission from source node at the backbone infrastructure via the getaway router to destination node.

3. Secured TE data packet transmission. A management based TE security approach for WMN.

4. Multiprotocol optimization of traffic transmission over WMN-routing protocol using MPLS VPN TE coded transmission over mesh campus environment to show performance in scalability, reliability and higher output throughput.

1.6. Research Methodology

The research methodology followed a three stage strategy in achieving the aims and objectives of the contributions made which were as follows:

- The initial literature review;
- The mathematical formulation and analysis; and
- The importation of wireless traffic modules in OPNET design modeller and its TE over mesh for verification of results/performance and coding.

In the initial stage, the literature review, including relevant research articles, research papers which included conference proceedings, published papers, journal papers and also IEEE802.11n standardization, proposals, seminars and white papers on WMN-routing protocols were researched and studied. The research proposal of the journals with the overall guiding research intentions and its applications were studied and read. Further, critical analysis of the results and age of the research papers were comparatively analysed. The important challenges and open research issues were isolated and incremental work on the topic were also studied. A survey paper was used to articulate all the important open research areas and to create a problem formulation for the intended research path.

The aim of the research was evaluated as the research proceeded with a project timeline. After the literature review, there was a need to develop a baseline to act as a yardstick to compare the investigations and observations

outcomes of the proposed approaches through simulations. A mathematical analysis of different parameters was carried out to decide on the best path selection computation for the TE WMN.

To validate the outcome of proposed ideas, we carried out a feasibility study of two network simulation software. The NS-2 and the OPNET 16.0 were studied and tried. However, OPNET 16.0 proved easier in operating and better in modelling and simulating a WMN environment to capturing a TE optimization through importation of MPLS-TE traffics. C++ / C- programming was used in coding of the program functions

1.7. Thesis Organisation

The thesis is arranged as follows:

- Chapter 2 is a critical survey which gives an insight into the challenges in the routing protocol of WMN. In addition, it proposes views on TE as optimization for enhanced routing and data transmissions.

- Chapter 3 explains the comparative performance of TE as an optimization technique using MPLS VPN traffic imported over WMN, creating an algorithm and derivation mathematical computation to solve the path-selection equation.
- Chapter 4 extends the qualities of TE over WMN routing protocol optimization by redefining a new proposed management approach to security of the WMN. It validates the improvement in secured transmission and on infrastructural capacity to secure the WMN.

- Finally chapter 5 is the final analysis and summation of the previous chapters and the future proposal of the TE optimization of WMN routing protocol transmission.

CHAPTER 2

A Review of the Routing Protocols in Wireless Mesh Network: with Views on Traffic Engineering

2. 1. Introduction

Wireless Mesh Network [9, 10] as shown in Figure 2.1 consists of the quasi-static wireless mesh routers, nodes-access points and nodes-clients. The WMN routers acts as backbone to the wireless mesh architecture. These wireless mesh backbone routers can be interior or exterior gateway access to the internet protocol wireless cloud. The advent of WMN [11, 12] created a novel, low-cost network, easily scalable over large networks. WMN is also a self-configuring, fast deployable and interoperable wireless network. Presently, using the different forms of the general architecture and structure, there exist infrastructure, non-infrastructure and hybrid types of WMN. The non-infrastructure WMN has no central hub, and so has the disadvantage of lower data traffic rates over multi-hop and heterogeneous WMN. Nevertheless, its natural ease of self-configuration, self-healing and self-organization uses the decentralized architecture efficiently for interfacing and communicating with existing network protocol. WMN are infrastructure mobile networks. The network can either be connectionless or connect-oriented in operation during route discovery or in route establishment stages. The mesh clients run on batteries and have limited radio transmission ranges and traffic transmission to the next mobile nodes traverses the multi-hops node links through the Access-Points (AP) to the backbone router infrastructure. Therefore, most wide area mesh architecture is hierarchal in topology. In WMN transmission operation, packets are forwarded to the upper layer AP the backbone gateways or bridge to the wireless cloud. These wireless mesh access techniques give the mesh networking added ease in integration through the inter-network interface connectivity with other wired networks and wireless standards like wireless local area network (WLAN), WIMAX (IEEE 802.16) and WIFI (IEEE 802.11n).

The unique structure of the WMN architecture, as shown in Figure 2.1 includes: its robustness, low cost, low battery power, reliability and ease of maintenance. WMN therefore can serve as access networks for wireless broadband, internet and other multimedia wireless networks. WMN is currently undergoing research development and standardization by the Internet Engineering Task Force (IETF) [1, 13]. The technical developments are in research areas of increasing large network scalability, node mobility, security, QoS, path diversity, transport and routing protocol. The WMN has other areas of improvement caused by the need for integration with other existing wireless or wired network standards. WMN will be a potential cheap access to community wireless broadband internet (IEEE 802.20).

The QoS and reliability over large networks are currently undergoing development and while the wireless meshes routing protocol standardization is still ongoing too. Various metrics and routing costs [14-18], network design adaptations and modifications [19-23] have been proposed to adapt regressive throughput as the network deployment increases [1, 24-30]. Most of these metrics reflect a measure of performance evaluation and cost of the routing protocol. These design adaptations and modifications are mostly algorithm, embedded and infrastructural network changes to the traditional wireless network routing protocol.

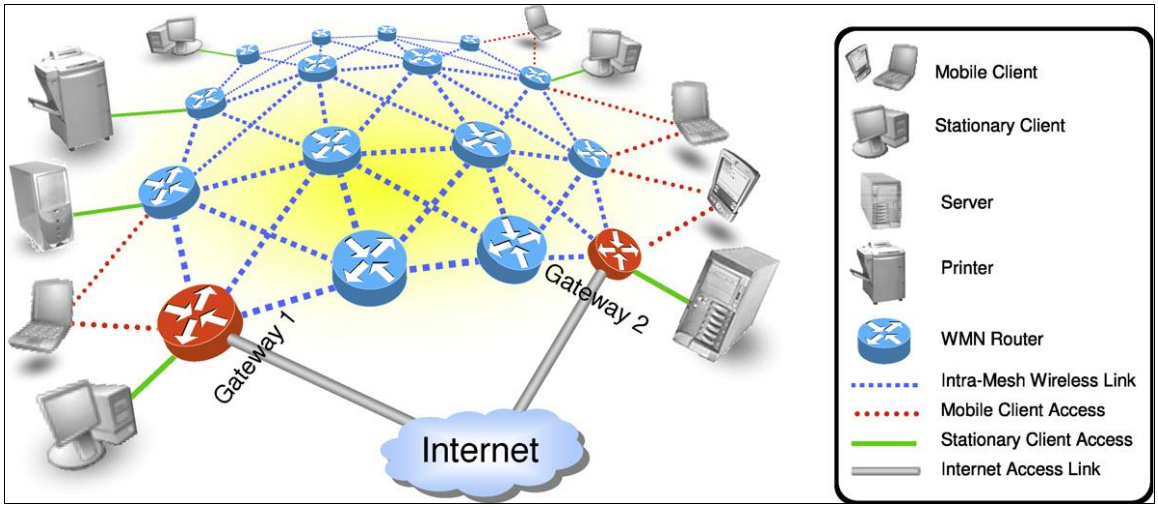


Figure 2.1: A WMN scenario with connected mobile nodes and routers [2]

WMN will be a potential cheap access to community wireless broadband internet (IEEE 802.20) as in Figure 2.2. The WMN architectural structure and characteristics are multi-hop in node mobility, the position of wireless AP, mesh routers distribution and routing mechanism as depicted in Figure 2.2. The WMN routing protocols are a carry-over from the traditional wireless ad hoc networks [31-35].

Mobile ad hoc network (MANET) [36-39] was later developed to solve the challenges of high mobile routers and node-clients mobility in wireless ad hoc environment. The architectural differences in WMN compared to other wireless network created new research opportunities and design challenges in mesh routing mechanism, end-to-end transmission and the metric of the WMN. Performance evaluation of these protocols differs on node mobility, size of the networks and the traffic over the WMN. The architecture creates chains of multiple-ad hoc networks in a hierarchal structure. The traffic transmission creates an asymmetric traffic of communication with most of the traffic packets going towards the exterior gateway router via interior gateway routers to the wireless cloud as shown in Figure 2.2. The engineering of these traffics are also used in developing efficient algorithms to enhance connectivity and multi-path access in the routing updates and data transmissions.

The comparative difference in the configuration of the ad hoc, mobile ad hoc network (MANET) routing protocols compared to the WMN routing protocols [40-52] are usually design adaptations with respect to the WMN, low power and minimal router mobility. The mobility of the wireless mesh router is quasi-static or stationary compared to MANET routers which are highly mobile. The wireless ad hoc network routers are also static like WMN. These differences in network infrastructure and network router mobility created research challenges in the migration from MANET to WMN. The challenges in the evolving WMNs are usually in areas of scalability, robustness and efficient structure-backbone with adaptive multiple metric. The planning and setting-up of the access points and other design consideration has also been proven to have an effect on the overall reliability and throughput of the WMN.

The environment topologies and settings like urban and rural environments can also influence deployments and performance. The ease of the WMN in deployment and linking nodes directed this review to path diversity solutions [53-64] and congestion control mechanism [65-67] and load-balancing solution [68, 69] in WMN. We also evaluated the route selection and maintenance in WMN, analyzed the scalability challenges and solutions in an increasing sized WMN. Finally, performance of the traffic scenarios in multimedia scenario and packet data traffics over wireless mesh networks was examined.

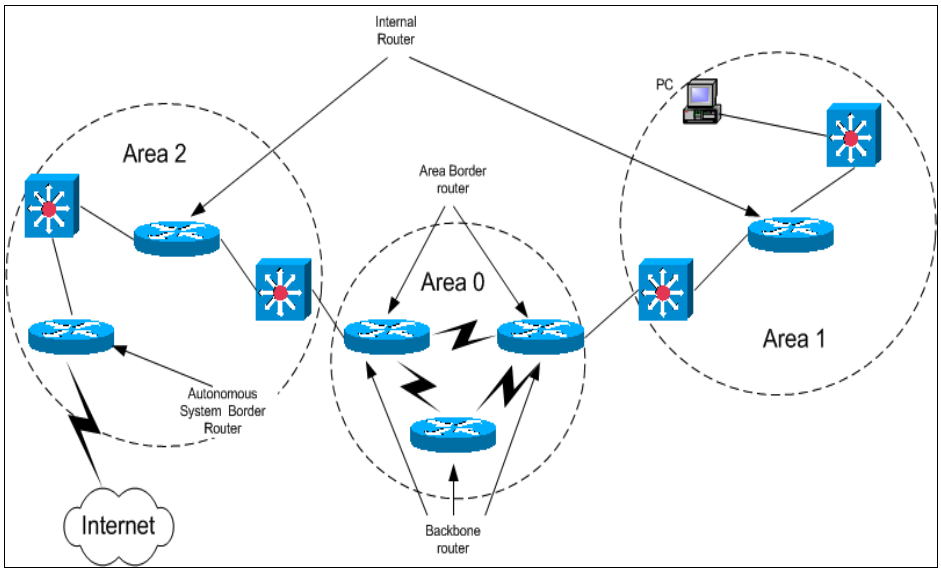


Figure 2.2: Source node to gateways packet transmissions in WMN [104]

We performed a review of the WMN routing protocols. Study and observation of these adaptations and modifications in the design was carried out using references from published research papers and journals. These design solutions were evaluated in terms of the comparative efficiency and reliability of the routing protocol algorithm [70-73]. In view that the standard routing protocol is expected to be reliable, efficient and adaptive for diverse wireless standards running on WMN, potential research opportunities and open areas for research inputs were explored. In this study, migration from ad hoc to MANET and WMN with respect to the routing protocols designs was compared and evaluated. Recent research advances in the routing protocols with respect to algorithm designs and solution mechanism in the network

routing protocol were also examined. In our study of the traffic and the end-to-end transmission of data, voice and video packets in the routing protocol, focus was on the routing challenges, limitations and advantages of the existing routing protocols.

2.2. Related Works on Routing Protocols

Various routing protocols of the WMN are designed to perform improved path selection, fast routing updates and network convergence. The path selection traffic and the routing update notifications are usually single path and unidirectional transmission. The routing protocols are usually adapted to the network topology, geographical settings, network architecture and the mobility of the routers and node-clients [74-82]. These form underlying solutions to constraints in the limitation of the above-listed variations of routing protocols in the WMN.

There are technically two types of routing protocols in the WMN: proactive and the reactive (on-demand) routing protocols. They are so defined according to their mechanism of updating and maintaining the states of the routing protocol. Conventionally, in the wired network environment, we have the distant vectors and the link-state routing protocols. However, in the wireless environment, the on-demand routing protocol maintains the routing state by updating the route information on the routing table or cache, as reaction to topological changes and demands. On the other hand, proactive routing protocol is constantly updating and maintaining routing states dynamically, without prompting or changes in the nodes or network. These updates are usually route request (RReq) packet messages and its accompanying route reply (RReply) packets notifications. There are also route error/route failure (RErr) and other route maintenance acknowledgements and alerts.

In WMN routing protocol, the route selection and path determination are dynamic routing mechanisms controlled by the routing protocol; however these are constrained by lack of path diversity and congestion. The

mechanism adopted by the routing protocol depends on the design classification adopted in the wireless network. The traditional wireless ad hoc networks, routing protocols uses either proactive or reactive mechanism routing protocol in wireless mesh networks are carry-overs of the older ad hoc routing protocols in wireless network.

The traditional routing protocols are predominantly ad hoc on demand routing protocol (AODV) [83-88], direct source routing (DSR) [89-91], destination sequenced distance vector routing protocol (DSDV) [92-94] and optimized link state routing protocol (OLSR) [95,96].These traditional routing protocols are either reactive/on-demand or proactive routing protocols and the hybrid [97] types which are usually a combination of the qualities of the reactive and proactive routing protocols. There are adaptations of location, geographical, topology and power solutions in achieving a routing protocol mechanism.

For ease of study, performance comparison and analysis in our review, we adopted four traditional routing protocols; two reactive routing protocols -DSR and AODV and two proactive protocols -OLSR and DSDV. Further analysis and comparison will be evaluated in Table 2.1 and 2.2. In routing protocol algorithm designs, we concentrated our review on research concepts using the three major mechanism of the routing protocol as illustrated in Figure 2.3.

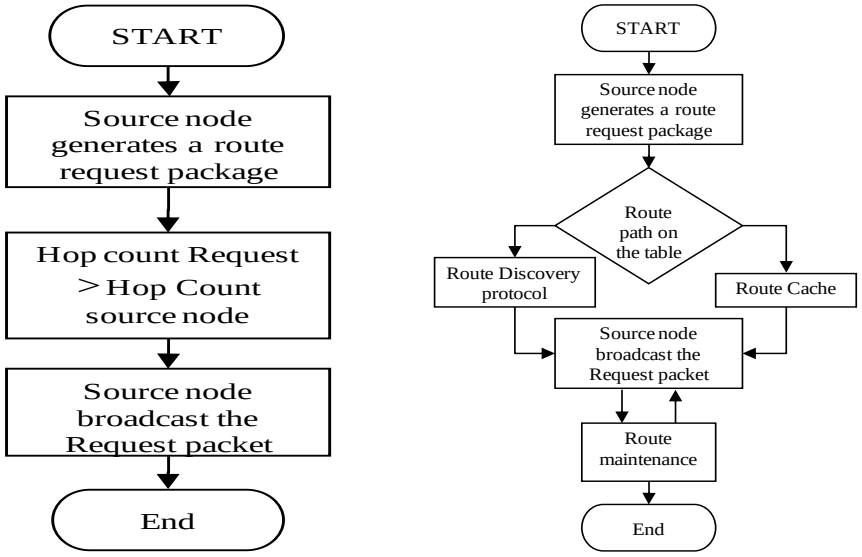


Figure 2.3: (a) Router route request process, (b) Route discovery and maintenance process.

The wireless routing protocol's process of maintaining the routing table involves periodic updates of the link state and mobile nodes in the WMN. These periodic updates can be link state protocol description unit (LSP) or 'hello' messages packets. The speed of network information convergence is a deterministic factor for efficiency of the routing protocol. The faster the speed the more effective the routing protocol in updating the routing table, selecting an optimal route and transmitting. Furthermore, end-to-end packet delivery from source-node to destination-node in the network is a logical decision based on the routing protocol algorithm functions. The routing protocol algorithm is the management software running the routing protocol of the WMN. In real-time traffic, especially in streaming multimedia transmissions i.e. video traffic, voice over internet protocol (VOIP) and multi-protocol Label Switching (MPLS), drop packets, path loss and interference distorts the final image and quality of service. The hybrid nature of the WMN is a major characteristic that enables addition of new links and integration with other networks. However, this feature makes the WMN susceptible to interference, route failures, high overhead and latency which causes congestion and network connectivity failures.

Currently, the routing techniques employed in WMN are mostly derivatives or adaptations from the traditional wireless routing protocols. There are numerous IETF and IEEE standard drafts and studies on routing protocol for WMN [98-103]. However, there are no established standard routing protocols for WMN (IEEE 802.11s). In the development of the WMN routing protocol, a lot of research studies have been undertaken on virtually every technical aspect of the routing protocol. These research works are in form of test-beds, theoretical and practical proposed solutions for improved routing algorithm for WMN routing protocol. The improvement on the algorithms can be either adaptive mechanism or design modification. The topological solutions use the location management selection approach.

Furthermore, there are different research methods in resolving the challenges in WMN routing protocols such as: derivative, adaptive, cognitive,

geographical solution approach and multi-metric solution. The improved variant methodology approach consequently led to the traffic pattern analysis which mostly proposes best effort routing protocol for wireless mesh environment rather than the optimal route determination method with less control overhead. Nevertheless, in TE resolution [104-108], best path determination and optimal route selection are mostly considered using TE designs and adaptations.

In the study of WMN, active research works are ongoing to enhance new research opportunities in multi-metric, multi-path, multi-radio and multi-channel designs in routing protocol. While the multi-metric explores combinations of different metrics to achieve a standard metric for route cost, the multi-path uses the underlying physical resources to create path diversity from source-node to destination-node in every WMN transmission. Furthermore, cross-layer optimizations solutions have been proposed for both upper layer and higher applications WMN routing protocol. In our study, adaptive designs of different routing protocol's algorithms for these resolutions were reviewed as shown in Table 2.1. Equally, observation shows that research study and evaluation on the performance of an effective multiple metrics for the WMN routing protocol is in progress. The robustness of the overall WMN has created research design openings and optimal adaptation for the resolution of link failures/recovery and network load balancing defects. In this study, focus was more on the algorithm research developments and also the many routing protocol design-adaptations.

While the emerging standards are being considered and tested, other modifications in the routing protocol have been proposed as improved-variants and adaptations of the traditional WMN routing protocols. In this context we reviewed the routing protocols based on multi-hop connectivity issues with reference to open research challenge resolutions. The next section of this review further compares diverse resolutions of the WMN routing protocol.

2.3 Wireless Mesh Networks Routing Protocols

The current routing protocols emerging in the wireless mesh network can broadly be classified into three types:

- The Proactive WMN Routing Protocols
- The Reactive WMN Routing Protocols
- The Hybrid WMN Routing Protocols.

2. 3.1. Proactive Routing Protocols

The proactive routing protocols as shown in Table 2.1, maintain the state of the routing table by periodic updates of the mobile node (clients) in the WMN. In the proactive mechanism, routing and links information are updated without a topological variation in the WMN. It has different update mechanisms and diverse types of information can be stored in the routing tables. Proactive routing protocols include: destination sequenced distant vector routing protocol (DSDV), optimized link state routing protocol (OLSR), fisheye routing protocol (FRP) [42], Distance routing effect algorithm for mobility (DREAM) [43], hierarchal state routing protocol (HSR) [44], source-tree adaptive routing (STAR) [44], topological broadcast reverse path forwarding (TBRPF) [99], cluster gateway switch routing (CGSR) [45] and multimedia support in mobile wireless networks (MMWN) [46] as observed in Table 2.1.

DREAM is an example of a proactive routing protocol which uses both geo-positional sensors (GPS) and a location inter-node exchange mechanism. The geographical coordinates are stored in the location table and these exchanges information periodically. It has less overhead because of the GPS location aiders. The frequency of periodic update is matched with the node mobility changes. The mechanism of exchange, gives the routing protocol an advantage by using less bandwidth in operation. This mechanism of location updating offers complete link state or distance vector update. The DREAM routing protocol is very scalable. However, the disadvantage in this routing protocol is that stationery nodes do not send updates messages and this can increase interference and slow convergence in the routing information update. Therefore, a complete state of the routing information may be missed.

Nonetheless, DREAM offers better matching of mobile nodes with updates than fisheye state routing.

The fisheye state routing (FSR) is a proactive routing protocol. It is a developed version of the global state routing (GSR) [47], but it reduces the updates of the GSR using a fisheye scope method whereby it updates nearby nodes using a higher frequency period than for the remote nodes. In doing this, it reduces the size of the routing update messages. The scalability is moderate as the disjointed frequency updates of routing information especially at the remote nodes which causes inaccuracies when the mobility of the remote nodes increases in the WMN.

The STAR protocol introduces another mechanism of updating based on a link state algorithm. The router maintains a source-tree which has information on links from source to best route destinations. It has a reduced overhead as a result of using the least overhead routing algorithm (LORA). It also uses optimum routing approach when required. The periodic link state updates are replaced with a better mechanism for conditional update dissemination. This results to reduced bandwidth overhead and latency. The STAR protocol however has a high processing overhead as each of the nodes maintain a graph of the network and for highly mobile nodes it consumes more memory and has a high processing time. There is always a potential of mobile nodes reporting different topological graphs to the source-tree and complicating information updates.

Hierarchal state routing protocol (HSR) is a link state based algorithm routing protocol. It is based on hierarchal route addressing and topology. Each node has a hierarchal identity number (HID) which are used in number matching in sending packets from source to destination in the networks. The logical nodes, behaving like the cluster algorithm, are assigned subnet addresses from the highest node at the top of the cluster to the lowest. These nodes are connected through ‘tunnelling’ logically and dynamically. The information update is done by flooding from the top of the hierarchy to the lowest nodes. The lowest level nodes have the physical layer topologies of the network. The advantages of hierarchy level routing are mostly in the separation of levels on

node mobility management using home agents. It also has lesser degree of control overhead compared to FSR and other proactive routing protocols. However, it exhibits the same disadvantages as CGSR in cluster maintenance and management.

The multimedia support in mobile wireless networks (MMWN) is also a hierarchal routing protocol. The routing state of the network is updated using a clustered hierarchal approach. The cluster has two different types of mobile nodes: the cluster endpoint mobile nodes and the mobile switch nodes. In each cluster group we have the location manager whose duty is in principle to perform location management for the cluster group. The MMWN store its routing information in a dynamically distributed database. Its advantages are the mechanism of location updating and location selection which reduces the processing overhead compared to other proactive routing protocols like DSDV and HSR. It is an adaptation of cluster-hierarchal based routing and also bears the same disadvantages as HSR. In addition, its cluster processing and complex management leaves a higher latency.

The optimized link state routing protocol (OLSR) is a proactive and link state algorithm based. In multi-hop wireless mesh protocol it is a point-to-point routing protocol which maintains the topology of the network by periodic advertisement and exchanging link state messages. OLSR minimizes the size of each node control messages and uses multi-point relaying (MPR) mechanism whereby some set of nodes are selected by each mobile nodes in the network to retransmit its packets. Mobile nodes which are not in the set of the retransmitting nodes can view, access and process each packet but cannot retransmit.

The cluster-head gateway switch routing protocol (CGSR) is a developed cluster-based hierarchal routing protocol. It addresses the mobile nodes in cluster groups. These cluster groups are usually assigned to a cluster head which is a mobile node. The head node controls and manages the inter-cluster and cluster domain transmissions. This is turn connect to the access-point which transmits to the next level routers that could act as gateways to the internet cloud. The advantage of this routing protocol is that each mobile

node only maintains the routes to its cluster-head thereby reducing intra-node overhead. Nevertheless, the cluster hierarchal method produces a bottleneck when there is congestion in the network. The failure of the head node of the cluster causes congestion and high end-to-end delays.

The OLSR adapts the hello message for broadcast to the next hop neighbour node which decides the optimal path by using the hello information. These individual nodes select a subset of one hop neighbour which is central between its two opposite paths. Table 1 illustrates a comparative assessment of proactive routing protocols. The proactive nature of this routing protocol informs the network of the best path before transmission of packets.

There are other proactive protocols and adaptations or new research modification of the algorithms. The proactive routing protocols basically follow the same principle of initiating best path and destination route before source node transmission of data packets. The hierarchal topology proactive routing protocols perform better than the flat topology ones. The DREAM routing protocol was very scalable and has less control overhead due to its faster exchange of routing information and the use of its location manager and selectors. The OLSR performs best comparatively. The hierarchical routing protocols have upper layer control and management which enables a better control. It however has the disadvantage of high processing overheads and latency. The increasing scalability and connectivity of the WMN is done by an effective route maintenance and control of retransmission or re-broadcasting. The cluster routing protocol has the disadvantage of a predicted bottleneck in connectivity of the WMN on failure of a cluster head.

2.3. 2. *Reactive Routing Protocols*

Reactive routing protocols are algorithms designed to react on-demand and only when prompted by routing needs. Table 2.2 illustrate reactive protocol table of comparison, strength and disadvantages. The on-demand routing protocols unlike the proactive routing protocol has initial design considerations of reducing overhead caused by updating the routing table, maintaining the routing tables and caching routes. Furthermore, they reduce route maintenance by being reactive to only active routes. Therefore, on-demand

routing protocol has a different route discovery and route maintenance mechanisms. In reactive protocols, route discovery process unlike the proactive uses flooding request packet through the network. The nodes at the destination reply those requests with route reply and error reply as the case may be. Reactive routing protocol can be multi-hopping or source routing. The packets are forwarded to their destinations as indicated by the headers and IP addresses. The multi-hopping goes through nodes and intermediate nodes on 'hop-by-hop' basis, exchanging information and transferring the route tables unlike in the source routing mechanism where the intermediate nodes play no role in the establishment of routes.

There are many types of reactive routing protocols including: ad hoc on demand routing protocol (AODV), dynamic source routing (DSR), routing on-demand acyclic multi-path (ROAM) [48], temporally ordered routing algorithm (TORA) [49], location-aided routing (LAR) [50], cluster-based routing (CBRP), associated-based routing (ABR) [51] and ant-colony-based routing algorithm (ARA) [52] and many others. We analyzed and reviewed some of the reactive routing protocols comparing their adapted characteristics, strengths and weakness as presented in Table 2.2.

The AODV routing protocol has comparable technical characteristics of dynamic source routing (DSR) and high destination sequenced distance vector routing (DSDV) protocols. However, it has an improved control overhead than the DSR in route discovery mechanism because the packets are routed with only destination address information rather than the full routing state information as in DSR. The sequenced numbering process of the DSDV routing protocol is also used by AODV in beaconing and periodic packet sequence numbering. The AODV route replies contain the IP destination addresses of the destination nodes and the sequence numbers unlike the DSR which carries every node address along the route path. These advantages make the AODV routing protocol very adaptable to highly dynamic networks like MANET and WMN, nonetheless it is disadvantaged during route selection as nodes may experience huge delays. In addition, link

failure recovery may initiate another route discovery process which introduces extra delays and consumes more bandwidth as network scalability increases.

Dynamic source routing protocol (DSR) nodes have the ability for checking best routes to a destination before initiating the route discovery process. This is possible because DSR stores multiple route addresses in its cache. The process of route discovery and maintenance does not require periodic beaconing or hello adverts update. It means bandwidth can be conserved in the wireless mesh networks and node power or battery can be conserved when not in active mode. Nevertheless, in high mobile networks like MANET and WMN, the DSR has its disadvantages. The route discovery and maintenance mechanism requires each packet to carry the full addresses from the source node to destination node for every hop in the network. This inadvertently means high control overhead, high processing overhead and high bandwidth over increasing network size (low scalability). This classifies DSR as effective over small to mid-sized networks.

Temporally Ordered Routing Protocol (TORA) is an improved version of the light-weight mobile routing protocol (LMR). It uses the process of route reversal and route repair. The LMR uses flooding technique to determine multiple routes to destinations but route selection is done by next hop basis. The nodes select the next available route without route discovery. Although this creates less control overhead, it produces many invalid routes and the optimal route is not always selected; TORA on the other hand uses DAG instead of routes request/reply. In TORA, control messages sent to the next neighbour nodes are reduced. It helps in removing storage mechanism and overhead. TORA supports multicasting in wireless networks but has to be enabled. It can be used as LMR with adaptive multicasting (LAM). It however has disadvantages similar to LMR with regards to invalid routes.

The location aided routing protocol (LAR) uses flooding algorithm process just like DSR but it reduces control overhead by using location information. The algorithm uses location node sensors like GPS. The LAR can maintain routing states by either using boundary coordinates stored in the route destination through route request and reply acknowledgements. The shortest distance to

relative destination is selected. It can also use zone request to exceed boundary limits where packets can travel to reach the destination nodes. The two approaches conserve bandwidth and limit control overhead in the wireless networks. The disadvantage is that each node is meant to have a GPS sensor for location update. In addition, over increasing network size, the control

Table 2.1: Comparison of Proactive Routing Protocols

Protocols	RS	No of tables	Freq. of updates	HM	Critical nodes	Characteristic	Advantages	Disadvantages
DSDV	F	2	Periodic dynamic	Yes	No	Loop free	Sequenced and loop free	High control overhead
FSR	F	3 and a list	periodic and local	No	No	Control freq. of updates	reduced overhead	high memory overhead & inaccurate network information
DREAM	F	1	nodes mobility based	No	No	use mobility & updates 2 control updates	Low control overhead/ memory overhead	Utilizes GPS for location activities.
MMWM	H	1 database	conditional	No	yes & LM	use LORA & reduces Control overhead	low control overhead	cluster formation & maintenance
OLSR	F	3 (routing, topology, neighbour)	periodic	Yes	Yes & Cluster head	Use MPR to reduce Control overhead	reduced control overhead	2 hops neighbour information needed for routing
HSR	H	2 (link state & location management)	subnet based periodic	No	yes, cluster head	hierarchy structure &Number ID	Low Control overhead	high processing time

CGSR	H	2	No	No	yes & cluster head	Cluster head exchange updates	reduced control overhead	High processing & potential cluster-head failure congestion
STAR	H	1&5 lists	No	No	No	use ORA / LORA	low control overhead	high memory &processing overhead

H – Hierarchal architecture routing structure, F- Flat architecture routing structure, LM- Location manager, LORA- Least overhead routing approach, ORA- Optimum overhead approach, RS- Routing structure

overhead increases because each packet is required to carry the full address information over routed hops.

Associativity-based routing (ABR) uses route request/reply method for route selection. It also uses periodic beaconing in connectivity-linking (associativity). It is a source based generated routing protocol. Each node's associativity maintains ticks which are selected with preferences given to the node with higher associativity compared to lower associativity tick. This means lesser route reconstruction is demanded. The route selection is based on the stability of the routes and not necessarily on shortest path to destination. It uses a localized service discovery protocol in resolving link failures. The advantages of using ABR are that it saves bandwidth and the route paths last longer because of the stability. The disadvantage on the other hand is that ABR does not have multiple routes or route caches. The ABR's periodic beaconing requires high energy and node battery consumption because the nodes have to be active.

Routing on-demand acyclic multi-path routing protocol (ROAM) is another example of reactive protocol algorithms. To eliminate search to count-to-infinity problems, it uses internodes coordination along directed acyclic paths to form sub-graphs, computed from routers distance to the destination nodes by a process called 'diffusion computation', by which multiple flooding on reactive routing protocol is eliminated. The protocol updates every time the distance from the router to the destination changes. In addition, ROAM protocol reduces the amount of storage space and bandwidth by maintaining update information in a router table, where the router acts as a destination node or intermediate node.

Ant-colony based routing (ARA) is a reactive routing protocol which adopts the ant behavioural characteristics of its food hunting to model its paths and connectivity to routes. ARA like AODV and DSR has route discovery and maintenance process phases. In route discovery, the forward ant (FANT) is similar to route request propagated over the entire wireless network. The pheromone which is a scent of trail for food is measured and given a value depending on the number of hops to the destination. Backward ant (BANT) is

Table 2.2: Comparison for Reactive Routing Protocols

Protocols	RS	Route diversity	Beacons	Metric mechanism	Route maintenance	Reconfiguration strategy	Advantages	Disadvantages	Characteristics & Strategy
AODV	F	NO	YES	new route & SP	RT	RT	adaptive to high dynamic topologies	Scalability problems in large networks and overheads in hellos message packets	Remove route then SN and local route repair
DSR	F	YES	NO	SP & next hop	RC	RC	route diversity and ease of connectivity	Flooding overheads and scalability over large networks due to source routing.	Remove route the SN
LAR	F	YES	NO	SP	RC	RC	Localized route discovery.	flooding problems and source routing overheads	Remove the route & the SN
ARA	F	YES	NO	SP	RT	RT	lo w overhead, low packet size processing	flooding route discovery process overheads & delays	use alternate route and by backtracking to the new next route
TORA	F	YES	NO	SP & next available route	RT	RT	multiple routes	temporary routing loop	Link reversal and route repairs
ABR	F	NO	YES	Stable associatively & SP	RT	RT	route stability & TTL duration	scalability problems	Use localized broadcast query
ROAM	F	YES	NO	SP	RT	RT	processing removes the search to infinity problems	high control overheads in mobile networks	Remove route & search next route by diffusion computation.
CBRP	H	NO	NO	next available route	RT @ cluster	RT & cluster head	low cluster head exchange routing	cluster head failure bottlenecks &	Remove the node & the SN and local

							information	maintenance problems & loops issues	route repair

RC-route cache, F-flat, H-hierarchy, SP-shortest path, SN-source node

returned to the source through the same path. The path is determined through the transmission of updates and network traffic. The route maintenance is resolved by increment of inter-node value of the pheromone as the data transmission occurs. The backward tracking to the source from the point of node link failure is a link failure recovery mechanism. In a situation whereby the link failure is not found, route discovery is used to determine a new alternate route. It has the advantage of reduced control overhead packets of BANTS and FANTS but it also has low scalability problems of increasing nodes and traffic because of the flooding mechanism of route discovery.

Cluster-based routing protocol (CBRP), as in the proactive routing protocol, is hierarchal in architecture and just like the proactive cluster protocol, each cluster group controls and determines what happens in the cluster. The clusters have cluster heads and exchange of routing information and data traffics are coordinated by these cluster-heads. The control overhead is reduced as only the cluster-heads transmit and receive data. However, the hierarchal structure can form connectivity bottle necks and high processing. This also causes propagation delays and looping.

In the study of the different types of reactive routing protocols, we used comparative tables as shown in Table 2.2 to highlight differences, challenges and development in the on-demand routing protocols. It is worthy to note that there are several reactive routing protocols; however, our analysis in this study is focused on these selected ones.

This is a combination of the reactive routing properties and proactive mechanisms. It is designed in zones of activities to reduce control overheads and processing times. In the hybrid routing protocols, zones are usually assigned to different routing processes in determining route and path selection. The proactive routing can be used in the peripheral nodes while the flooding and route discovery is used in central nodes. The strategy is to utilize the qualities that are derived from both the advantages of proactive and reactive routing processes to create an improved routing scheme – hybrid.

The deterministic factors for best performance among the above listed routing protocols are usually based on traffic load, node density and size of the network. We also analyzed the performance of routing protocols using other factors as a base for comparison. In WMN, the mobility of the nodes is an important design shift from ad hoc and MANET routing protocols. Mobility and randomness of the traffic at client-nodes, is directly proportional to the traffic load and the load balancing. The traffic of the data can be multimedia, bidirectional or single way network traffics. In addition, it can be burst traffic, busy traffic, periodic traffic or very slow. The variation of the traffic has a limiting or sublime effect on the overall performance metric. The multimedia traffic and IP traffic may be time sensitive data packets transmissions. In such delay-sensitive end-to-end packet delivery, the best performance is always a factor of the traffic over WMN. In real-time video transmission and surveillance scenarios, efficiency of the routing protocol is reflective on the display quality exhibited which is a resultant effect of the traffic transmission network.

The node density distribution affects inter-node exchanges and connectivity in the network. The node represents the mobile mesh clients which are trans-receivers in action. The mesh client's concentration in the WMN means more contention for channel allocation and link access. Connectivity will be higher, resulting in more packet drops, increased interference and end-to-end delay aggregation. Also, the data traffic packets will be short links and disjointed. Retransmission of data packets and acknowledgement of route requests may be prone to "looping" or counting to infinity challenges. On a positive side, there will be faster convergence and short link-state route protocol information updates. The node battery will be better managed with high power efficiency. Cluster based routing protocols perform best in high density mesh client WMN environments. Hierarchal state routing and distance vector based routing protocols suffer higher latency in comparison to a relatively less dense mesh client WMN. In hierarchal routing protocol scenario, the peripheral node-clients suffers more overhead and " Fairness" disadvantages in access to

lower layer available contentious channel for the transmission of data packets to Access Points (AP).

In WMN analysis, the third factor - the size of the network, is a well documented and researched issue. Scalability over large network has been a major research challenge for WMN. Scalable mesh network solution contributions have been proposed. Naturally, smaller WMN networks have less delay, less interference and lower latency challenges compared to metropolitan and large area networks. Research has shown that WMN will be most exploited in a community enterprise as a result of its ease of deployment and cheap cost. Many algorithms have been developed as scalable routing protocol algorithm for WMN. Multi-radios and multi-path solutions have also been proposed as a remedy for scalability issues. Further adaptations on multi-path using multi-gateways as a solution for scalability and connectivity have also been proposed. Recently, a cognitive solution for scalability was proposed by Akyildiz and Chowdhury [30].

The scalability of large WAN wireless mesh networks has shown increasingly low speed of convergence and network aggregation. It exhibits high delays in transmission, more drop-calls and interference. The multimedia traffic transmissions experience delay and distortion of images and video in real time environments. The delays and interferences cause bottleneck congestion in the gateway of a hierarchal routing protocol. In other words, scalability affects other factors in a large WMN traffic transmission especially in increasing node sizes and nodes number extensions in WMNs. The resolutions of these faults are usually applied in the routing layer of the network. The more effective the routing protocol in transmission from source to destination, the easier it is for the network to extend its peripherals.

In the “Collective Analysis in the Study of Routing Protocols for Wireless Mesh Networks”, A. Zakrzewska et al [93] carried out a study and evaluation of the performance of the four traditional wirelesses mesh routing protocols: AODV, DSDV, OLSR and DSR. In Table 2.3, traditional routing protocols were analyzed and differentiated. The major indexes for comparison were network

size, nodes mobility and network traffic load. The NS-2 network simulation tool was used to implement a WLAN extended WMN in IEEE 802.11s. The mobility scenario was enabled with a random waypoint model. The node starts its random movement with a speed (V) uniformly distributed. The scalability of the network was investigated for different network sizes and dimension using mesh node clients and routers in simple incremental proportions. Different network architecture with random moving nodes (clients) was used in order to study the protocol capabilities.

A ready-to-send (RTS) and a clear-to-send (CTS) were used before packets were sent over the network. Various network dimensions and designs were used as stated below on NS-2 simulation tool over a traffic speed of 10m/s:

- 30 nodes, 900 m * 300m, 10 mesh routers
- 50 nodes, 1500m * 300m, 16 mesh routers
- 100 nodes, 1500m * 700m, 32 mesh routers
- 150 nodes, 1500m * 1100m, 48 mesh routers
- 200 nodes, 1500m * 1500m, 64 mesh routers.

AODV is a reactive sequenced routing protocol designed for MANET. It uses route request/reply for route discovery and sequenced numbers when exchanging information. It keeps only next hop addresses and is very scalable over large WMN. Furthermore, it uses flooding based route discovery and can lead to high packet delays. However, OLSR is a proactive routing protocol which uses a link state shortest path algorithm. It works on the principle of multi-point relays (MPR) concept. The broadcast and information messages are exchanged between the MPR because the route discovery process is optimized with total control numbers transmitted. DSR is also a reactive routing protocol with a different mode of route selection and updating mechanism. It discovers routing state only when it is needed. DSR uses route request and replies just like AODV but unlike AODV it keeps the whole network routing information in a cache. DSDV is one the earliest routing protocol for ad hoc networks. It uses sequenced numbers for accurate data processing which helps in preventing looping. DSDV is a table driven protocol

which consumes the network resources when the network is stable. These are comparatively evaluated over three critical factors namely Network size, Node speed/mobility, and Traffic load. Four comparative and deterministic metrics were developed and employed.

- Packet delivery ratio: defined as total packets delivered at the destination node compared to total packets sent from the source node.
- Average end to end delay: defined as average time needed for a data packet to be delivered over the network from source nodes to destination nodes.
- Aggregate throughput: the sum of the data delivered to all nodes in the networks in a given time unit (seconds).
- Normalized routing: the ratio of all the routing packets sent to the successfully received data packets.

Evaluation and results in Table 2.3 shows that AODV routing protocol exhibited more strength than the other routing protocols and over increasing network size and it showed the least end-to-end delay. Its overhead is directly proportional to the increase in network size. This is due to its flooding mechanism in route discovery process. However, it has the worst network load because of higher overhead controls sent over the WMN. Its performance over increasing nodes mobility from 0 m/s to 10m/s is considerably good, but OLSR has a better performance compared to all the other routing protocols. DSR on the other hand exhibited the worst performance because of its routing cache and the time it takes to update from the cache. In the network load, the DSDV and OLSR performed very well due to the constant proactive periodic updates which are relatively stable. DSR sends acknowledgement notifications to all the routes in the networks and it is not scalable in WMN.

Topology changes causes the on-demand routing protocols to frequently send more control packets to balance the effects. In the final test, increasing

network traffic load as shown in the network by data transmission, AODV and DSR showed 80% packet delivery over uniform network while the proactive routing protocols did not perform as well. High traffic load causes congestion and high drop calls. This impairs the networks throughput and packet delivery ratio. We can therefore conclude that reactive protocols perform fairly better than proactive protocols in increasing nodes mobility and traffic loads.

There is no best routing protocol as demonstrated by this simulation, but what we have are different topologies and metrics for diverse routing considerations. Scalability was also observed as a recurring challenge with all the routing protocols but AODV fared best in the test for network size and increasing nodes mobility as seen in increasing high scalable WMNs. DSDV showed a low requirement for processing overheads. OLSR on the other hand performed better than the other routing protocols in end-to-end delays and data delivery ratio. DSR performed worst in most of the testing and even worse in low mobility and small networks as the source routing overhead and caching creates a high control overhead. AODV performed best comparatively but showed deficiencies in end-to-end delay and low control overhead over increasing network sizes. Its processing overheads can be reduced by carefully eliminating the amount of route request and replies combined with its flooding mechanism for route discovery. We therefore focused on AODV routing protocol. We factor different modifications and variants. We check comparative performance over the three tests routine as done above for the traditional ad hoc routing protocols.

Table 2.3: An Initial Comparison of Traditional Topology Routing Protocol

Protocols	Metrics	Message overhead	Convergence	Protocol type	Summary
DSR	Shortest path	High	Medium	Source routing	Route Discovery-cache
AODV	Shortest path	High	Medium	Distance vector	Route discovery Update
DSDV	Shortest path	High	Fast	Distance Vector	Route Table Exchange
TORA	Shortest path	Moderate	Medium	Link reversal	Update packets
GRP	Directional path	Low	Fast	geographical	Directional route discovery
HRP	Link Quality	High	Medium	hierarchal	Route discovery with Cluster level

We therefore conclude in the above study that AODV and OLSR performed best using the three test parameters. DSDV performed relatively better than DSR in the packet delivery but DSR did very well in small networks but scale poorly in most other parameters of comparative analysis. In conclusion, all the traditional routing protocols had deficiencies in scalability over large networks, multi-path access, and bandwidth constraint over high demanding traffic like multimedia and video traffics as shown in the scenario Figure 2.4.

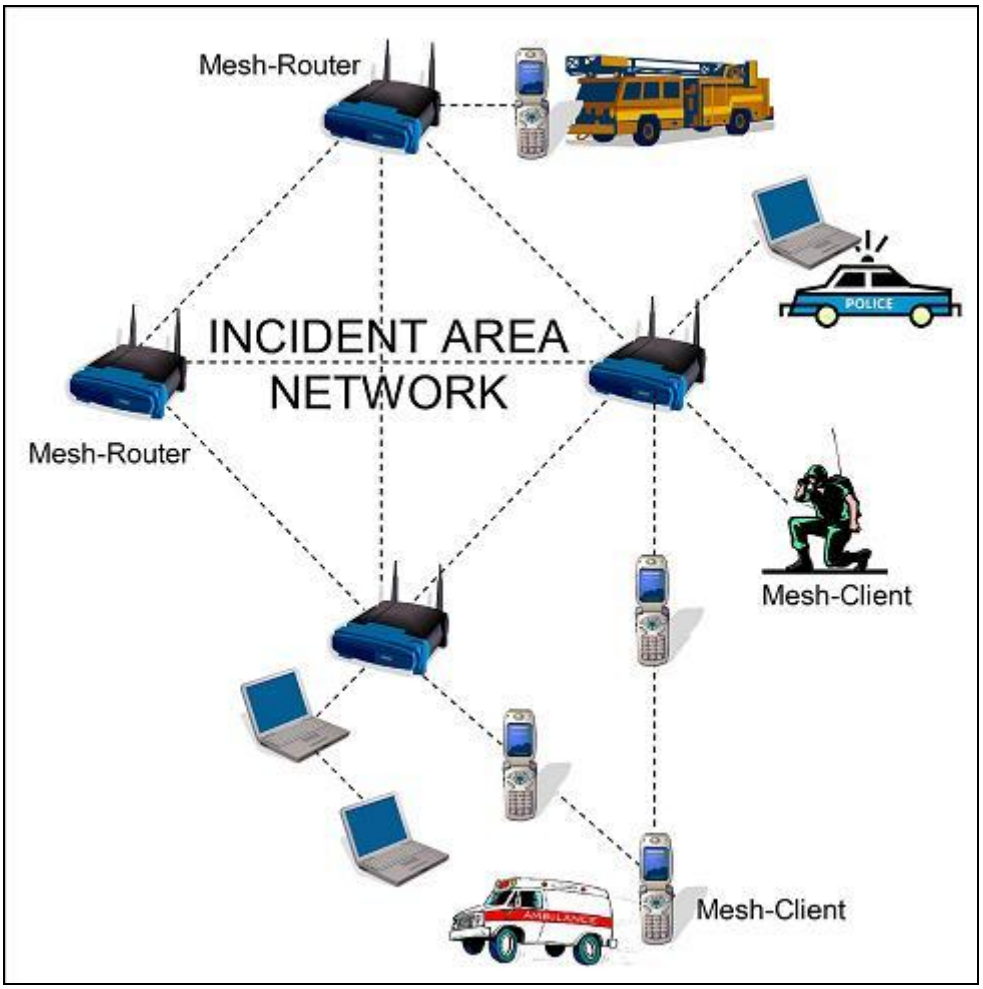


Figure 2.4: A multimedia Wireless Mesh Networks scenario for broadband networks [105].

The routing protocol showed many design deficiencies especially using traditional routing protocols over WMN and also in modern traffic demands i.e. video streaming, interactive videos and broadband networks.

Variants of these old traditional routing protocols were investigated in [46]. In the search for an effective routing protocol for WMNs, other research studies were evaluated and analyzed. Path diversity solutions were adapted and developed with multi-path algorithms and designs [52]. In readdressing the delays and throughput challenges, V. Loscri, 2007 [53] proposed a coordinated distributed scheme (CDS) mechanism with multi-path parallel routing over an IEEE 802.16. The simulation NS-2 tool was used in designing a mechanism to build multiple paths for a couple of source nodes and destination nodes. These paths are utilized in parallel types. The CDS was incorporated in the MAC layer and compared with a unidirectional AODV routing protocol. The router table and destination address are selected using a pointer to the list of multi-path.

In another study [63], a delay-bounded multi-channel routing was simulated over WMN using a token ring in the mesh for its characteristic ability to utilize multiple channels within neighbourhoods. It was implemented over IEEE 802.20 (mobile broadband) as shown in Figure 2.4. Delay rules in joining the rings and creating new rings in the token ring contention access. A multipoint to multipoint network like WMN where each access point acts as a relay device (router, bridge or repeaters) was used. The state machine was used to implement multi channel in WMN. Delay-bounded rules and logics are utilized in a distributed algorithm in the ring mesh to manage interference and collisions in the rings. It showed better performance in throughput and in end-to-delays, it however has high control overhead and possible delays from failures of state phases.

In resolving direction and location management in WMN, an orthogonal rendezvous routing protocol (ORRP) [55] was proposed in for WMN. Geographical routing using nodes ID, ID to location mapping and node localization techniques were utilized like in GPS. Embedded coordinate space is used to reduce the dynamism and complexity of the binding and states needed in location and node mapping of ID’s. ORRP performs well in sparse area networks and achieves high probability connectivity. It avoids flooding and updates disseminations which reduce the overheads. It can be compared

with free-space optical, smart and directional antennas. However, ORRP suffers heavily from high mobility scenario in WMN and also has the challenge of looping. It needs a better error correction mechanism.

Simple opportunistic adaptive routing protocol (SOAR) [56] provides another routing protocol solution. Routing protocol which transmits notifications over pre-determined paths has not always been efficient in WMN. SOAR addresses the resource consumption and duplication by carefully selecting nodes and using priority based timers which maximize the progress with low coordination in packet forwarding. It supports effective local recovery and performs very well over multiple flows of traffic in WMN. However, SOAR has a major disadvantage; it was likened to the shortest path link algorithms which do not necessary select the optimal paths.

A hybrid approach for routing protocol solution was demonstrated in proposed hybrid routing algorithm. The algorithm is modified dynamically based on high and low mobile nodes and static routers. A combination of a reactive (DSR) and a proactive routing protocol was employed. Distributed Bellman-Ford algorithm (DBF) was used for computational efficiency and also due to its characteristic use of less storage. However, DBF has challenges of short and long looping problems and low inter-node coordination resulting from fast topological variations. The scheme uses DSR for highly mobile nodes and DSDV for low mobile nodes. It reduces the information traffic in the network by discarding route reply message when the targeted node has already been seen. Periodic updates are controlled but with high overheads and the route discovery process introduces looping problems to the network.

The solution for slow convergence problems in WMN was addressed in the journal article “Fast-converging distance vector routing protocol for WMN” [57]. It addresses latency challenges which cause most increases in control overheads in WMN. The four traditional routing protocols were used for the test over NS-2 simulation software. Bellman-Ford routing algorithm was applied. Distance vector routing protocol was used because of its characteristic slow convergence. The article highlighted the effects of network

traffic updates, exchanges and the impact on networks using performance comparisons. By increasing the frequency of exchange of information in the network, the control overhead increases thereby controlling route updates by reducing the update interval was forgone for additive and increment multiplicative decrease (AIMD). Fine-tuning of updates intervals approach was considered. The node neighbour sensing scheme was used for updates, exchanges and incremental change in state was applied. A fast converging distance vector routing protocol algorithm was proposed as a solution because it reduces bandwidth, control overhead and congestion in WMN. The throughput rate was also increased as a resultant. Looping in WMN was improved by marking nodes number sequentially, thereby distinguishes dead routes from new routes in the WMN.

Other research studies adopted diverse approaches and techniques in creating solutions for control overheads and processing WMN routing protocols. Directional AODV routing protocol [58] was proposed using on-demand routing protocol challenges while discovering routes. Flooding causes high message control overhead and more processing time. Directional-AODV (D-AODV) algorithm was applied on the WMN to reduce re-broadcasting of routes request and replies. This was done by using restricted directional flooding mechanism. The number of routing packets (flooding) was decreased by directionally forwarding these packets towards the gateway nodes and routers in WMN. Consequently, the redundancy of retransmission or re-broadcasting which has high demands on bandwidth and effective transmission is reduced. This approach is based on the cognitive route knowledge towards the gateway nodes. The learnt routes are cached, enabling recent data packet forwarding in transmission to have better knowledge of routes than the nodes. It uses the hop-to-hop count metric and are compared over throughput, relative control overhead, average path length and end-to-end delay of data packets. It showed 47% improved performance for random topology and 15% on grid topology. However, assumptions of directional flow of data traffics from source nodes to destination gateway router are assumed as normal route path in the WMN.

Other more recent studies, employed intelligent and cognitive techniques like the intelligent mesh based multicast routing algorithm using particle swarm optimization on demand multicast algorithm (PSO-ODMRP) [59]. The particle swarm technique method utilizes the random mobility of network nodes as defined by the particle swarms in the paper. It uses the proactive routing mechanism to maintain states and reactive routing mechanism to reduce the impact of high topological changes by acquiring routes on-demand. There are two types of multicast routing protocols based on behavioural characteristics. The first type maintains routing states and the second, organizes protocol into their global data structure prior to forward multicast packets in transmission. On demand multicast routing protocol (ODMRP) is mesh based and demand driven. Mesh is formed by a set of forwarding nodes responsible for forwarding data packets periodically from source to destination. Multicast trees are built by the source by flooding control packets and by query join messages and appropriate node ID's are received and used in reverse transmission. PSO uses natural flow of traffic like weather, terrain or battery power to indicate fitness form of a function. It also uses optimal search solutions rather than suboptimal solutions. Particle velocity dimension are modelled for best route using NS-2 over a radio and IEEE 802.11 MAC layer model. PSO-ODMRP model algorithm optimization show good performance on low mobility speed but does not find optimal solution in high speed mobility environments.

A major solution to most challenges in WMNs routing protocol has been path diversity. There have been different techniques using multi-path solutions for problems of scalability over increasing large networks, connectivity, high bandwidth, congestion and looping in routing protocols. Another study explored the use of hybrid routing scheme in a secured-multi-path WMN [60]. This approach considered WMN as a hybrid network. The basic idea of using hybrid routing protocols is the simultaneous use of the proactive routing protocol in some areas and the reactive routing protocol schemes in other areas in the same WMN.

Cryptographic method is used to secure the transmissions from source node to destination node. It employs the Ford Fulkerson algorithm [112] for performing maximum flow and calculates all the possible disjointed nodes. Computationally, it is more complex and more secure. The architecture was segmented into zones of operation for the different routing protocol. The proactive routing protocol is active in the router backbone for high link backbone communicating paths while the route maintenance are done using the reactive routing protocol because of its mechanism of response to topological variations. It has the advantage of less delay in route determination. It enables route discovery process for path determination and route maintenance, operating a simple authentication mechanism designed to provide reliability. Secure multi-path routing protocols are more resilient to intrusion attacks than normal routing protocols. The public key assures the authenticity and integrity of a new node in the network and the messages are encrypted by a private key of the router node. The client node and the router node encrypt the messages by their private keys before transmissions. It has a better performance in alternate route, security and throughput but it also has a relatively higher overhead compared to other multi-path techniques.

The connectivity challenges and traffic transmission issues like congestion, drop calls, scheduling, prioritizing and scalability are being studied and research is on going for solutions in WMN. These problems affect the outputs in terms of throughput, deliverable data rate, end-to-end delay, bandwidth, control overhead and latency in routing protocol of WMN. As shown above, different studies and research have shown partial solutions to these challenges in routing protocol of WMN. The most effective and all encompassing solution has been the integration of some of the prescribed solution mechanism and inter-layer/cross layer protocol optimization. Path diversity has also shown efficiency in performance against these routing protocol weaknesses.

Performance improvements provided by route path diversity in a multi-hop WMN environment, highlighted different techniques and mechanisms enabled in exploiting path diversity. The potentials and gains shown by cooperative

diversity (channel and path) are active research areas for routing protocol in WMN. Multi-path routing are also enabled in buildings and it exploits the wireless resource redundancy in the underlying networks like fault tolerance, load balancing, bandwidth aggregation and improved QOS metric to providing a more effective routing.

In traffic transmission, selection of a route over available alternate routes demands effective strategy and optimal selection algorithm. A multi-path route algorithm may select a route over others for traffic forwarding by using other routes discovered paths as back up or the paths can be used simultaneously. Optimal path demands best QOS determination and best metric efforts. The use of paths concurrently can be done using prioritization and splitting of traffics to satisfy best QOS in transmission. Coding schemes can be used to reduce redundancies and bandwidth allocation for this path splitting and traffics transmission.

A different multi-path solution has however been proposed for ad hoc wireless networks and MANET. The routing protocols ROAM, multi-path routing protocol (MP-DSR) [61], ad hoc on demand multi-path destination sequence vector AOMDV [62] and split multi-path routing protocol (SMR) [68] all uses different multi-path techniques to show performance improvements in ad hoc wireless networks. In WMN however, the design architecture of static mesh router and highly mobile mesh client's nodes make it imperative that low battery and infrastructure WMN approach is adopted in designing the algorithm. Links and hierarchical layer structure of WMN should also be taken into consideration.

2.4. Traffic Engineering Open Research Opportunity

Having analyzed the weakness and challenges in most of the routing protocol algorithms and mechanisms, we can effectively deduce from all these analysis, an observation of partial resolutions and modifications. Further observations revealed that most of the solutions were usually embedded, infrastructural design algorithms and variants-improvement schemes in

resolutions for a novel routing protocol. The challenges in WMN routing protocol especially in traditional routing protocols: AODV, DSR, OLSR and DSDV, have created research opportunity for the resolution of scalability, link failures/recovery, path-diversity, bandwidth aggregation and network load-balancing defects. In previous sections of this chapter, we concentrated on the developments in algorithm research and the different routing protocol design-adaptations [113-115]. Furthermore, evaluation was conducted on the resolutions using the infrastructural solutions and designs. The comparative analysis of using adaptation techniques and the challenges of partial solution shows the need for a comprehensive approach to the problems in WMN routing Protocol.

The significant areas of research challenges such as load-balancing, path-diversity, data transmission security, connectivity, congestion control and bandwidth aggregation as prevalent weakness in the routing protocol of WMN were highlighted. These weaknesses have resultant effects on route processing time, path determination and selection with the attendant processing overheads.

In view of the issues highlighted, we introduce Traffic Engineering (TE) [116-118] as an open research opportunity. It offers, unlike the older methods, Internet Protocol multi-addressing and comprehensive solution in achieving the resolutions of these challenges and imperfections in WMN routing protocol. Furthermore, it enables a traffic design approach for transmission mechanism in router to router and intermediate nodes with connectivity resolution which are avoided by the switched Labelled paths in the routing layer of the network.

Using analysis of the asymmetric flow communication in the WMN routing protocol, we observe that the Internet Protocol cloud is usually the end destination of most data traffic. Internet Protocol addressing is a more effective mode of capturing the network topology and connectivity access [115]. The route discovery and maintenance mechanism requires each packet to carry the full addresses from the source node to the destination node for

every hop in the network. This inadvertently means high control and processing overheads and high bandwidth over increasing network size (low scalability). The use of IP traffic engineering addressing and configuration lower the processing time and uses low overhead. IP addressing and quick capture algorithm converges faster than the older versions.

Most mobile nodes act as transceiver stations, their IP addressing are usually the best form for the resolution of link failures. Internet protocol MPLS virtual path network (VPN) creates a secure transmission path for notifications and acknowledgement of routing protocol traffic. It further directs the traffic data to the destination with reduced interference [116]. It also improves congestion control through connectivity using secured multi-path solution for traffic and data transmission in the Networks.

Routing layer research challenges such as scalability, connectivity, interference and congestion issues are better resolved using traffic engineering mechanism. Traffic engineering using MPLS technique creates additional multi-path route-redundancy for improved congestion control and link failure recovery [116]. It also improves the scalability of the networks by creating a high-connectivity environment. Alternate paths can be configured as access links in broadband and ISP for aggregation of multiple bandwidths in WMN routing protocol. This concept will be a technical departure from the typically adopted mechanism prevalent in most studies. Efficient designs of Traffic management techniques and algorithm are used as solution to achieve improved scalability with better load balancing, path-diversity and route-connectivity solutions. Cooperative hybrid multi-path routing designs [117] such as the use of the MPLS layer 2.5 switching over routing on WMN routing Protocol are facilitating much needed solutions in WMN routing protocol.

The use of MPLS traffic Engineering (MPLS-TE) [118] have shown remarkable improvements on bandwidth aggregation and load balancing mechanism in the routing layer of the WMN. The Multi-Protocol LAN Switching (MPLS) creates a path balance of packets transmission and flow of data. It further creates a pathway for message retransmission and failure

notifications while transmitting acknowledgement in the routing protocol. The internet protocol addressing and design configuration of this tunnelling with respect to WMN delivers a high QOS in WMN [117]. The adapted improvement in computation of the configuration improves scalability, bandwidth aggregation, load balancing and reduced congestion delays. It also increases fault tolerance and stability of routes in WMN multimedia traffic transmission compared to other variants and traditional routing protocols as previously discussed.

In WMN routing protocol, the architecture and operation from our study shows that there exists an asymmetric traffic transmission starting from the peripheral node to the access point (AP) then further down to the routing protocol backbone/ Interior gateway to the wireless cloud. These traffic flows in the wireless mesh network routing protocol creates a traffic re-engineering solution which is a departure from the usual network infrastructure hardware resolution. It is analogical to solving traffic road congestion either by building new access paths to lessen traffic flow or putting in place traffic regulatory access lights to control traffic density and road usage. They are both good concepts depending on the traffic design and its mechanism of operation.

Wireless mesh network traffic engineering (TE) is the mechanism of achieving efficiency by traffic manipulation to fit the network resources. It can be configured by IP addressing, IP routing and configuration. In addition, traffic engineering can be achieved by changing the interface IP metrics in large wireless mesh networks; however, this may create huge overheads in a large network. Multi protocol LAN switching (MPLS) between the layers 2.5 to layer 3 of the OSI layer model can resolve these issues by intelligent mapping of two or more divergent architectures, routing protocols, address spaces, signalling protocols, resource allocation and even enhanced bandwidth access.

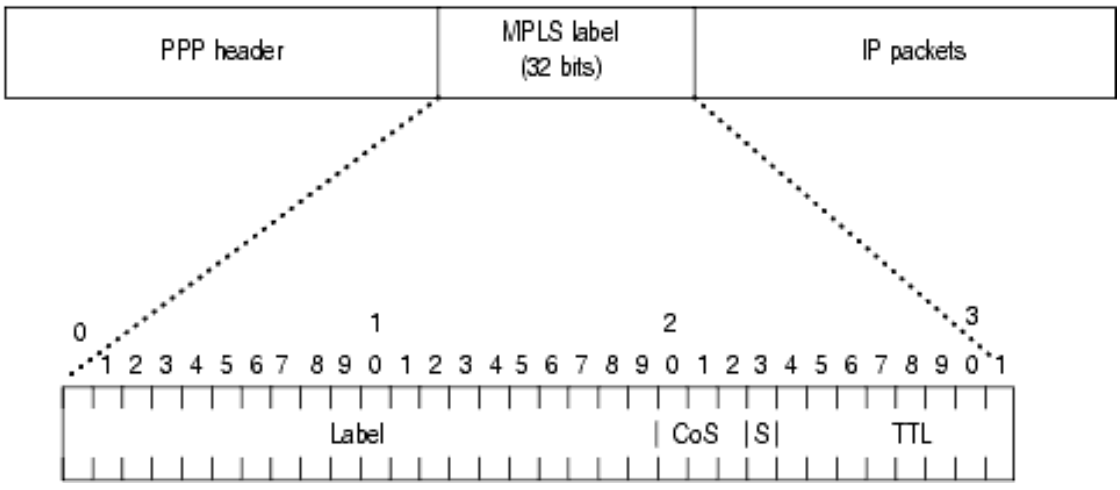
2.5. MPLS Traffic Engineering and IP Tunnelling

Multi-protocol Label Switching (MPLS) enables the mechanism for traffic engineering in wireless mesh network traffic patterns that is independent of routing tables. MPLS is also independent of any routing protocol, resulting in less processing time and overhead. In the network, it can act as independent or combine with existing switching circuits' mechanism to provide routing services and gateway function sometimes when needed. This technique differentiates the bandwidth priority and access therefore improves the processing time and lowers overhead and latency.

As shown in the Figure 2.5, it works on the principle of assigning short label tags to network packets (data packets); this label tags are 20 bits unsigned integer, carrying detailed information on the mechanism of achieving end-to-end transmission of data through the network. Traffic engineering techniques involve creating label switched-paths (LSP) among the mesh routers in the wireless mesh network. These switched paths are connect-oriented and provide an alternate path from source to destination packet traffic without going through the next node or sets of nodes hops transmission. The purpose of traffic engineering in a network layer is to deliver priority based and time-sensitive traffic over the network in a shorter time. Furthermore, the encapsulation of these Label switched path in traffic engineering enables secure pathway for data transmission. Geo-position location like in DREAM proactive routing protocol can be tracked using IP addresses and the MAC address of the mobile stationery nodes in the WMNs. In the routing layer operation, the data packet transmit from one router to the next, an independent forwarding logical decision is made at each hop. The IP network layer header is checked, and the next-hop is chosen based on the metric and on the information on the routing table. In an MPLS operation, the analysis of the packet header is performed just once, when a packet enters the MPLS cloud [111]. This ensures less overhead and speed of convergence from source to destination in the WMN. The MPLS enabled wireless mesh network is highly scalable. In MPLS operation, the packet is assigned / tagged to a traffic stream identified by a label, which is a short (20-bit), fixed-length value

at the front of the packet. These labels are mapped to the label forwarding table. This table stores information on traffic forwarding and the labels like class of service are used in packet prioritizing before transmission i.e. VOIP, Skype and MPLS.

In this research, we came to the summation that most challenges and problems with the routing protocol of the WMNs are transmission faults and the ineffectiveness of the algorithms/mechanisms. In some existing routing protocols, partial solutions for the weakness generate other challenges and weaknesses. In resolving these problems, evaluation of the solutions and their mechanisms was done on the existing routing protocols. Therefore, path diversity in packet transmissions will provide an effective solution in the WMN routing protocol. MPLS enables the multiple alternate transmissions and routing of the packets in WMNs. This mechanism, in operation within a wireless network, gives secure traffic transmission and path diversity in the network. In addition, it provides a secured path for data encapsulation and tunnelling for these packets, videos and voice traffics especially in IP VPN tunnelling. Furthermore, MPLS-TE gives good load-balancing and improved connectivity especially against drop calls in the routing layer of the WMN.



Label: Label value, 20bits

CoS: Class of service, 3bits (also known as experimental bits)

S: Bottom of stack, 1bit

TTL: Time to live, 8bits

Figure 2.5: Label Allocation in MPLS Routers.

2.6. Advantages of Traffic Engineering

In multimedia and real-time type traffic environment, divergent multiple traffic streams with different service requirements as in Figure 2.4 contend for transmission access on a limited bandwidth; traffic engineering provides the class prioritization and efficient use of network resources. It provides administration and negotiated sharing and network bandwidth optimization.

In real-time network operations, high capacity utilization of service and fault resolution must be adopted for multiple link failure scenarios. Simultaneously, there must be mechanisms to efficiently and speedily re-route traffic through redundant link capacity. On recovering from the faults, optimization may be necessary to include the restored capacity of time-sensitive operations like traffic routing in multimedia video or online streaming television.

Traffic congestion and link-failures both occur when network resources are overwhelmed by the traffic transmission and when the transmission is experiencing interferences/network problems. It may be due to hierarchal bottlenecks on the border gateway protocol access (BGP). This suggests that the network design or parameters are inadequate to accommodate traffic-load. The design may be poor whereby traffic streams are not effectively mapped to available network resources resulting to the partial utilization of network resources. Congestion resolution can be improved using traffic engineering to effectively map network resources.

The challenges of intermediate nodes (router) in routing protocol are mostly with regards to the connectivity and processing time of routed traffics and packets. In addition, it addresses convergence, optimal routes selection in the route discovery stages and path determination in dynamic mesh routers. MPLS-TE provides direct alternate path to destination nodes bypassing

intermediate nodes. The location, selection and determination of a route in the routing protocol and the eventual failure resolution of a link or node in WMN differs, depending on the metric, topology and architecture.

In previous sections, different research studies and mechanisms were reviewed. Further comparative discussions were analyzed on the strength and usage in WMN, while the disadvantages and weaknesses in the existing WMN routing protocols were highlighted. The migration in research resolution depicted by studies, research improvements and modifications done on WMN routing protocol were examined. Areas for further research and open opportunities were identified. Qualities of MPLS-TE as a possible future solution for improved, low processing and less overhead high data transmission as obtained in multimedia traffics in WMN was identified. In addition, metrics and different algorithms in routing protocol were evaluated. We will not be discussing the implementation of the mechanism in WMN and techniques of MPLS-TE in this paper. Observation has shown that cross-solution or comprehensive resolution of these challenges will provide the needed standard for routing protocol for WMN. A standard wireless standard will improve reliability, interoperability and integration with other wireless standards. It would provide standard platform for scalable meshing and multi-access in community broadband and enterprise wireless networks.

2.7. Lesson Learned

In the previous sections, we reviewed different IEEE 802.11 standard routing protocol algorithms and the alternative proposed algorithms stemmed from adaptations and modifications of the ad hoc network standard algorithms for both MANET and WMN. While the emerging IEEE 802.11s standard routing protocols are being considered and tested, more innovations are being proposed. There are also proposed improved-variants and hybrid WMN routing protocol versions. The routing protocols were reviewed based on packet transmission and connectivity issues with reference to open research

challenge resolutions. Here in this section, we further discussed what have been learned from our study.

The study showed that diverse types of routing protocols have different attributes, strengths and advantages. Nevertheless, these proposed routing protocols also bring disadvantages and flaws, when used in diverse routing applications or network topologies. The routing flaws and challenges such as count-to-infinity, spoofing, delay location and speed of updates or failure recovery perform variably in different operations namely proactive or reactive. There is also a structural factor: cluster-based, hierarchical or flat architecture of the network transmission and also the routing table update mechanism. We deduced that mobility and randomness of the traffic at client-nodes are directly proportional to the network's traffic load and the load balancing. The transmitting spectrum of traffic may be multimedia, bidirectional or single way network traffics such as they can be constant, burst or periodic. The variation of the traffic has a limiting or sublime effect on the overall performance metric. Some IP traffics may be time-sensitive in data packets transmissions and such will require prioritization in WMN.

The traffic engineering technique is introduced as an open research opportunity is a holistic and more comprehensive approach to achieving a routing operation which can work in different terrains and scenarios. MPLS being multi-layer path diversity and equally comprehensive solution is able to overcome most of the challenges and flaws analyzed in the preceding sections. It will open an area of research opportunity in resolving routing protocol challenges by configuring secure tunnels and traffic paths using IP routing commands and addressing.

Transmissions using traffic engineering techniques can create path diversity for failed packets retransmission and facilitate faster routing table updates. This can enhance efficient connectivity, throughput and bandwidth in WMN routing protocol. Furthermore, the retransmission of data packets and acknowledgement of route requests may resolve the "looping" or counting to infinity problems in WMN routing protocol. Consequently, there will be faster

routing protocol convergence and faster updates in short link-state route protocol information.

The traffic engineering label mapping tag technique reduces overhead and processing time. It also saves time in routing tables updating and speed of convergence. The IP configuration and addressing removes the instances of looping and count to infinity error challenges. The location management, GPS and directional based routing protocols all have high processing and overhead which increase latency, is resolved using IP addressing and intelligent configuration. IP addressing resolves mesh client node location. The comprehensive proposed research opportunity shows that even with the best metrics optimal routing is not only ensured but can be improved in a multi layer optimization using TE. Research emulation test beds and evaluations have not been explored as of the time this review paper is produced but a lot of works has been done on MPLS-TE routing protocol for WMNs.

2.8. Conclusion

In this chapter, analysis and study was carried out on the WMN, the design migration and developmental trends in wireless mesh network routing protocol was done. Our study focus was more on the routing protocol layer. We highlighted many and divergent techniques the routing protocols capture the challenges of the traditional older ad hoc network routing protocol and we further did a comparative analysis on the various design algorithms with specific evaluation on its adaptation to solutions properly investigated. Derivative solution based-routing protocol proposals were observed. The concept and mechanisms of the routing protocol algorithms were also studied as comparative strengths of resolution in the routing protocol. A review of the many variants/adapted solutions with respect to the inherent and open research opportunities and challenges were explored too. The relevance of the diverse routing protocol to wireless mesh network routing and switching challenges was also looked into.

Finally, an open research opportunity on traffic engineering mechanism in synergy with the WMN was explored. The resolutions of existing routing protocol challenges were studied too. The numerous design-creative and adapted solutions to routing protocol network traffics were compared and objectively discussed. Furthermore, formulating comprehensive solutions through multi-faceted IP approaches to these major challenges offering the network resolution through traffic engineering - MPLS transmission engineering mechanism.

The proposed mechanism could improve path diversity, scalability, load balancing and security of the routed packets in routing protocol of wireless mesh protocol. This MPLS-TE can equally improve efficiency in bandwidth aggregating and connectivity especially in broadband networks. The advances in traffic engineering techniques using low-computationally overhead and low processing IP configurations and commands will further encourage potential commercial usage and adoption for faster forward switching routing protocol and the combined mechanism of traffic engineering and routing will promote faster data packet transmission in WMN. Traffic engineering mechanism also creates a secured packet traffic transmission over wireless mesh network.

TE also gives the administrator an enhanced flexibility approach in QoS and real time prioritization which in turn increases the scalability and load balance in WMN. TE addressing and intelligent configuration command can also increase the resultant throughput during transmission. These open research potentials will also generate a multi-protocol holistic standard for WMN. All these raised issues and possibility are open to further scientific research test and analysis. This chapter has lead to further work on Wireless mesh network – a traffic engineering management security adaptation published as journal for networks Elsevier 2010 [113,114] by the same authors and new interested research respectively.

CHAPTER 3

Wireless Mesh Networks – Multimedia Traffic over Scalable Wireless Mesh Network

3. 1. Introduction

Traffic engineering (TE) in wireless mesh networks [8,117,119] augments the mesh networks ability to configure Internet Protocol (IP) nodes client and to use created list of traffic commands to regulate and control the optimal network efficiency in the WMN transmission. The high potential demand of multi-service technologies over wireless mesh network creates numerous traffic transmission challenges with its adverse decrement on the mesh network scalability. However, MPLS-TE [120-122] is an extensible internet protocol (IP) mechanism for packet transmission with excellent cross-domain adaptable qualities. In addition, TE has an inherent natural ability to route data transmission through special mapped assignment of tagged packets from source nodes to the destination in the wireless mesh network. The tagged label in MPLS-TE routing technique has a label stack where transmissions of information are resourced to enable tunnel linked repairs. It also includes reliable QoS mechanism, efficient packet/data security during packet transmission and effective bandwidth management, better congestion control mechanism [113] and higher throughput output compared to the traditional ad hoc networks. In WMN optimization using TE [123,124], nodes and router nodes can be configured using extended IP access list commands, label distributive protocol (LDP), virtual private network (VPN) or GRE-tunnelling in an optimized internet protocol configured routing command over the WMN's infrastructure.

TE concepts vary from the IP based TE to the MPLS-TE, offline and online TE mechanism and the unicast or the multicast variation schemes. In traffic optimization, we further classify TE into intra-domain and inter-domain TE optimizations. Using the routing enforcements mechanism for TE, we can

divide TE mechanism into the IP-based TE's and the MPLS-TE. Using the subject of availability for classification, we have offline traffic operations and online traffic operations. While finally, using the aspect of traffic types we have unicast traffic and multicast traffic. The MPLS-TE employs the use of intelligent setting up of dedicated LSP's for delivering encapsulated IP packets. It uses traffic splitting for forwarding and routing of packets through explicit paths for its optimization but can suffer large overheads over large WAN networks due to its many LSP. It also needs path protection mechanism as back up paths otherwise traffics cannot be delivered through alternate paths. The IP based TE employs weighted links of Interior gateway protocol (IGP). It uses fine grained path selection unlike MPLS-TE which employs dedicated explicit paths. Optimization therefore can be done by tweaking or tuning of the routing attributes intelligently. Though IP based TE lacks flexibility in path selection, it has better scalability and availability resilience than MPLS–TE. It also has reduced overhead due to non use of LSP.

On the other hand, WMN essentially is an IEEE802.11n standard technology, [1] which defines the operation of mesh transmission of traffic over ad hoc networks. WMN, being an evolving standard in ad hoc network communications, presents numerous open research opportunities and challenges as shown by Akydiliz 2005 [3] in a survey of WMN. The scalability in increasing sized mesh networks creates challenges [11] such as: lower coverage capacity of the WMN over increasing wide area network (WAN), poor reliability [21] of transmitted data, lesser load balance [125] and lower output data rate. WMN has attractive commercial selling qualities such as cheap installation, usage and interoperability with other network platforms for wireless high broadband access [126]. In addition, it is easily deployed due to its dynamic mesh nature and cheaper cost.

In an increasing number of nodes, campus mesh network model as shown in figure 3.1, observation indicates that TE enables a simultaneous, diverse packet transmission over WMN using both routing protocol and TE data packet switching within dynamic mesh operations.

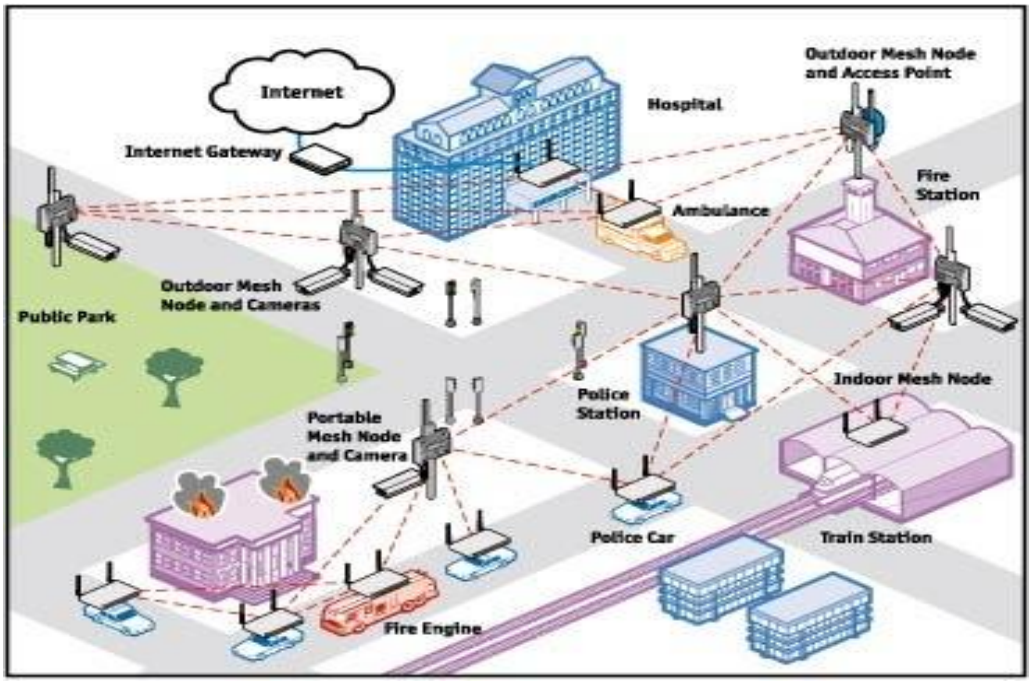


Figure 3.1: A Campus WMN deployment with traffic communication [17]

However, in TE, packet transmissions with multiple transmission delay-constraints are used to implement optimal and low-cost path selection that satisfies all sets of constraints [124] such as time-delay, end-to-end transmission, QOS and increased packet forward traffic in scalable WMN. In addition, TE mechanism can be enabled over WMN for higher throughput optimization of packets on high demand traffic scenarios in WMN. Furthermore, other resultant effects such as load balance in the WMN could be resolved using either path fast re-routing or by multi-path link state path balancing transmission.

The Internet Engineering Task Force (IETF) [127] has developed standards for traffic engineering in IP-based networks; however there is a need for an adapted standard version for WMN. Virtual networks such as VPN, MPLS, GRE, IPSec and tunnelling techniques can be enabled as a mechanism to implement traffic engineering over WMN.

3.2. Related background

In the WMN operations, the backbone mesh routers also act as gateway nodes to the exterior internet cloud (internet) or interior gateways to other wireless network technologies. WMN can also function as packet trans-

receivers nodes/station, which essentially receive and route data-packets from decentralised source nodes to destinations.

The access-point (AP) uses multiple node channel interfaces for hosting and re-transmission packets traffic flowing from the wireless mesh client's nodes in the peripherals. It provides exchange and integration nodes between the mesh client and the mesh backbone routers infrastructure in WMN. Most times in a hierarchal network the AP forms the cluster heads for packet-data transmission. The WMN has commercial qualities of self-configuring, self-organizing and self-healing; these inherent characteristics make the WMN an excellent wireless access technology for scalable multimedia and community broadband [129]. WMN easily creates extensible IP networks forming larger chains of wireless networks and integrating with other wired network too. In WMN deployment, increasing network size and infrastructural scalability comes with nodes-interface mismatching issues, fail links, interference challenges, drop packets and high latency. Consequently, the resultant throughput decreases with increasing network size. In addition, the speed and time of convergence increases due to the end-to-end transmission distance and delays. These factors reduce the throughput and quality at the destination nodes, lowering the speed of convergence in the network. In extended multi-hop communication in heterogeneous networks, WMN suffers coverage decline too especially during extended node/network packet transmission.

3.3. Traffic engineering background

The importance of TE applications for WMN administration has been gradually increased due to its several advantages in ad hoc networking. Resolution of congestion and link failures become more challenging with increasing mesh node connectivity. Using effective mapping of packet data traffic to the network resources will improve overall reliability and efficiency of the mesh network. TE regulates these rules of mapping traffic flows over WMN's source to destination routing to maximize data transmission flow. The TE technique controls and differentiates diverse traffic scenarios such as in video and multimedia packet transmission streams. It also increases reliability in heterogeneous and multi hop gateway traffic forwarding. In WMN, QoS

differentiations mechanism are the summation of differential traffic priorities in the spectrum and drop packets probabilities allocated to diverse packet traffic, also impacting through access of various traffic trunks to network resources.

Routing of data-packets during transmission around the peripheral nodes are predominantly done using client's node adjacency [130] traffic exchanges. The routing protocol uses a deterministic-sequential distributed algorithm for node to destination packets transmission. The routing algorithm forms the underlying software commands running the entire routing protocol in the WMN architecture. In the multimedia networks, the wireless mesh IP nodes and routers could be configured and enabled in the model WMN using carefully designed internet protocol (IP) commands. This IP mesh node functions as transceivers stations and ultimately sends and receives data packets, to the predominantly wireless cloud destination bound. The inter-node distance and proximity of the wireless mesh client nodes and AP in the network also influence scalability [9] over increasing network size. The transmission speed during network convergence and in the neighbour route discovery mechanism, routing table updates and in-data transmission from source node to destination node provides a cost metric for many latency factors in the WMN.

WMN can operate as an underlying access network for broadband and multimedia networks and can also easily facilitate integration of mesh networks with other wireless and wired networks. WMN provides an excellent enterprise for potential commercial network access and emerging technologies for community broadband and multimedia networks. The broadband networks are increasingly popular due to the upsurge in internet and small office home office (SOHO) node stations and electronic commerce (e-commerce) web applications. The wireless broadband networks are a dependable access network and appropriate for many real-time communication operations and applications like voice, data and multimedia communication services. WMN access for broadband communication networks is both interoperable and easily complementary with other networks too.

Most of the transceiver-IP nodes in the WMN are mesh clients nodes and routers with gateway functions operating as IP web-access to the wireless cloud. While the mesh routers may act as IP gateway backbone, the mesh clients employs medium access control (MAC) addresses for frame transmission among neighbourhood mesh nodes. The IP addresses are enabled by configuration commands and are either dynamically or statically assigned in the network routing protocol layer of the WMN.

WMN has added ease of integration with other wireless systems and extending wired networks and is easily scalable over increasing network sizes, providing a low cost, easy to repair and low battery consumption in WMN. However, gradual losses occur with scalability and as coverage widens in WAN scenarios. The architecture and operation is shown in figure 3.2 and depicts a cluster-based, hierarchal structured-mesh transmission of packet traffics and network notification packets transmission through the peripheral (client) nodes through the AP nodes to the backbone wireless mesh router nodes via router gateways to the wireless clouds (internet). In hierarchal WMN, the mesh nodes are assigned different roles during transmission operations.

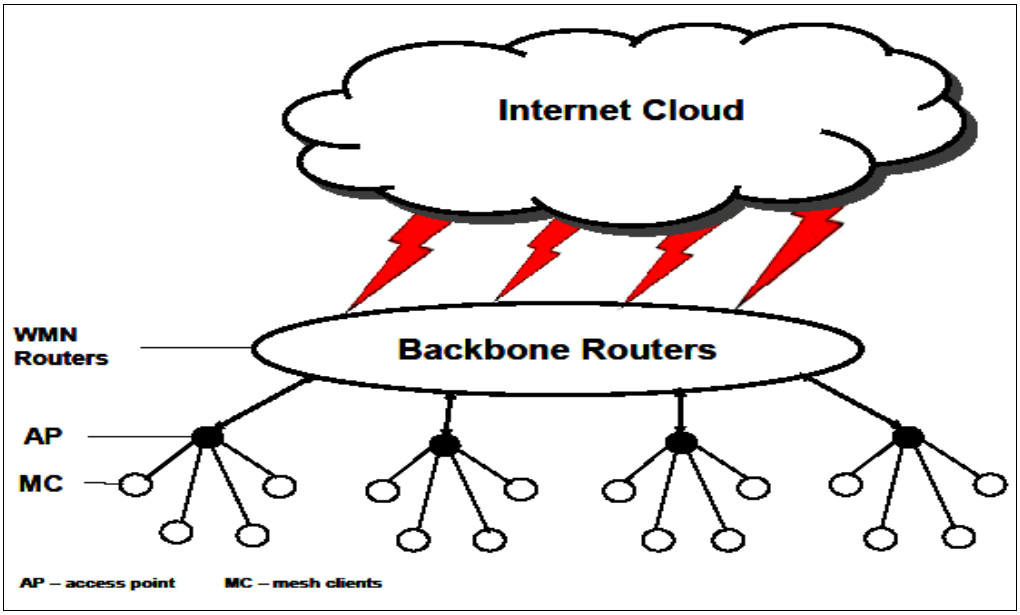


Figure 3.2: A three layer-level WMN transmission

In the hybrid model is a departure from the existing traffic of data packets over WMN architecture. Existing mechanism like the MPLS based technique or the proposed IP based TE mechanism is also applied over WMN architecture to create potential high QoS, cheaper access to community wireless broadband internet (IEEE 802.20) such as asymmetrical digital subscribers link (ADSL), with added low-congestion and enhanced scalability. This inevitably, results in higher throughput and data rate in the destination node sink.

The quality of service (QoS), congestion control and reliability over increasing network size/nodes are easily impaired factors in WMN communication due to the medium (wireless) and different high distributed overhead challenges such as interferences, jitters and distortions. Data communication in WMN undergoes other degradation factors as well such as routing protocol resolutions, optimal path and channel assignment overhead processes. These could consequently affect the speed and throughput, real-time operation and reliability of the network.

The TE techniques have the flexibility of usage in diverse applications during WMN routing protocol optimization. It further creates extensive traffic forwarding capabilities and varied multi-services applications in the TE using efficient algorithms and IP addressing command techniques in WMN optimization. The IP addressing, configuration and command ensures the ease of the routing and path mapping between different node sources to destination routing applications in the network. TE technique approach to the routing protocol design in WMN adapts configuration of IP mesh nodes. WMN-TE are implemented to optimize network performance by optimal tuning of the transmission traffic carrying data, therefore achieving a faster and more effective packet transmission on pre-determined and selected paths to accomplishing overall optimal routing in WMN communication. This technique, dynamically assigns network paths through a switched virtual circuit called label switched paths (LSP) based on the constraint of the existing traffic load

and available bandwidth. It also switches routed traffic through multi-secure transmission paths in the networks.

In the subsequent parts of the chapter, we discuss the TE background and analyze the existing technical challenges in routing protocols and scalability problems in WMN. The proposed ALSTE-RP proposed solution will be presented with the algorithm and discussed while the network simulation and analysis and comparative performances, showing different reactions to derived metrics will be discussed followed by the summary and reference.

3.4. Adaptive Link State Traffic Engineering Routing Protocol (ALSTE-RP)

The TE design for the scalable routing protocol in WMN architecture such as that shown in fig 3.3 is mostly dependant on the type of routing, transmission challenges and routing metrics. TE has high potential capabilities in optimizing a co-operative WMN. The routing protocol is enhanced because while packets transmission are in operation, TE creates a concurrent transmission in which packet data are mapped to destination node and transmitted through layer 2.5 switching. The main objective of TE is to provide an optimised WMN with faster-forward routed paths providing a high level scalable performance. TE mechanism is employed to achieve efficiency by configuring traffic to fit the network resources. However, in the ALSTE-RP, we explored a multi-layered objective protocol solution as a holistic approach to resolving these numerous routing protocol design challenges. Most challenges in various proposed routing protocols in the WMN are partial and are not fully comprehensive solutions for the multi-layered WMN in the distributed architecture. We therefore developed a algorithm for this multilayer –optimization of the WMN's routing protocol and also using TE technique for a faster forwarding (source node – destination node) switching matrix in the router and AP nodes of the campus network.

The ALSTE-RP is an adaptive TE technique providing scalable routing of packets in WMN communications and for intelligently allocating higher

bandwidth using IP configured mesh nodes and routers in a distributed and decentralised network environment. It is a WMN multi-protocol optimization technique using a sequenced distributed multi-protocol faster forwarding routing protocol algorithm. This design is achieved employing a faster-forward path computation algorithm design in a TE technique for the WMN. This guarantees reliable forward-based linearly deterministic routing scheme. This process will definitely create some selfish mesh nodes and poor fairness and bandwidth management since the routing protocol components determines the optimal path-forwarding metrics. Optimization criteria employed in TE over WMN most times causes severe unfairness in traffic distribution due to greedy mesh transmitting nodes.

The ALSTE-RP procedure also employs the specially designed TE-routing algorithms to achieve the improved performance. TE can equally be achieved in WMN by configuration commands in IPv6 addressing, IP routing with static configuration commands. In addition, TE can be achieved by configuring the interface- IP metrics in large wireless mesh networks; however, this may create huge overheads in a large network. Using an OPNET16.0 modelling software tools for enabling TE scenarios in WMN based environments, we optimize the label source-destination mapping mechanism. There are also, opportunities of maximizing the security transmission paths to the destination or minimizing the resource usage such as acknowledgements and constant updating mechanism in the routing protocol.

In this proposed design proposal, we adopt a decentralized linear-distributed, deterministic processing of the packet transmission in the architecture but we also use a hierarchal structured cluster-based mesh network design approach. The distributed scheme is implemented in various ways but we adopt the scheme where the egress-ingress node pair can both send traffic over the WMN architecture. In the hierarchal scenario, for the purpose of optimization, we allow the mesh client on the periphery to use node-adjacency for transmission while pre-determined paths, from the AP through the mesh routers through the gateway routers to the destination, are linearly determined

unlike the stochastic method, which has high computation and hence high processing overhead.

In Mesh clusters, node and points of switching and transmission systems like AP are linked to four client mesh nodes in a domain-hierarchal structure. We further optimize using least-computed path, linear-sequenced distributed optimization algorithm to determine the optimal path selection and transmission capacity rate. In order to increase network transmission capacity while reducing data-traffic congestion in the network, the proposed algorithm may need to regulate network traffic by adjusting various parameters that control the operation of mesh nodes. The WMN network administrator may identify topology information, which indicates a configuration of the nodes and links, and a traffic matrix, which indicates a relative traffic demand weighting for each source node-destination node pair. Optimization of the WMN routing protocol using TE captures the maximum utilization of the mesh network resources.

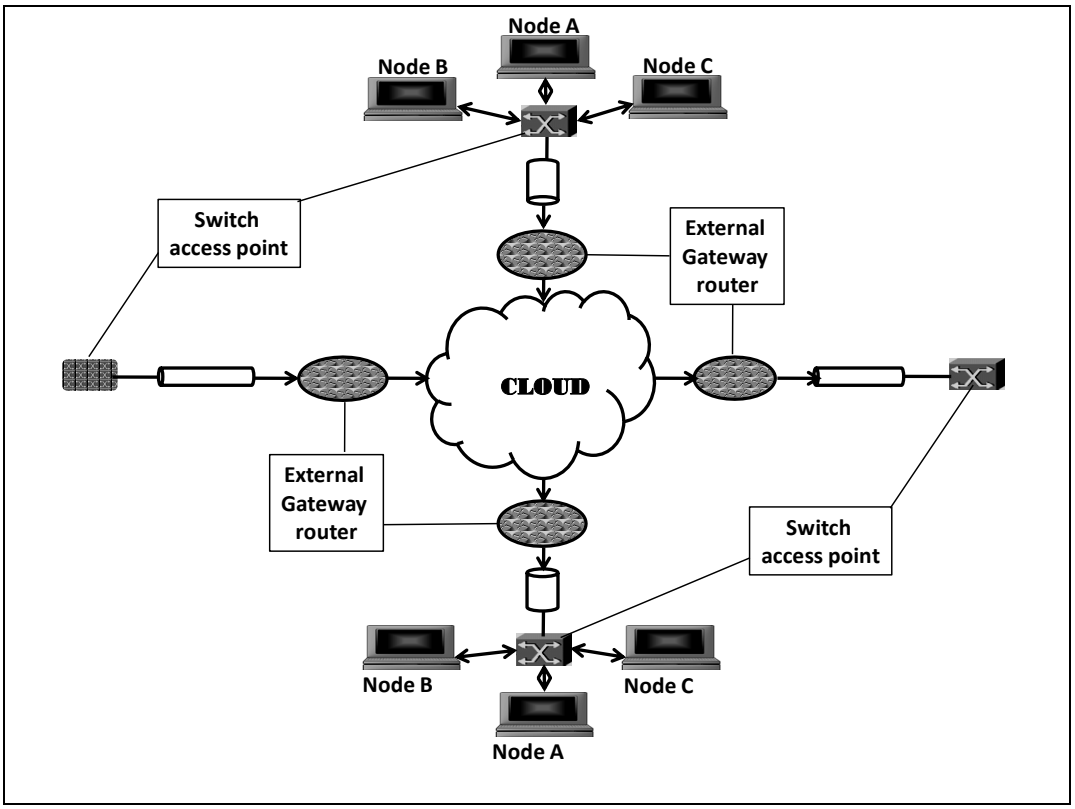


Figure 3.3: A traffic engineering packet transmission (ALSTE-RP).

In the model shown in figure 3.3, node A, B, C will be sending routing messages among themselves using node to node adjacency mechanism while a pre-determined path from AP through the backbone routers and gateways to the wireless cloud or internet is enhanced in the network using TE techniques. The combination of these two methods of transmitting packets and communication in the network depicts the new algorithm for the ALSTE-RP.

3.4.1. Various factors in optimization mechanisms

In most TE optimization techniques, we consider the effects of the controlled label switched path (C-LSP) and also adapting the most achievable objectives and using performance metrics on OPNET 16.0. Various TE algorithms have been proposed as low-computational metrics for resolving scalable routing protocol challenges in WMN. Path selection in the TE-optimization technique depends on mechanism, mapping the ingress- egress traffic pairs to nodes of the LSP or route final path determination of the routed traffic flows. We adapt various routing protocol optimization techniques in the WMN to match the TE technique. In the routing protocol's TE design and optimization, we input the sequential deterministic qualities of WMN packet processing to adapt the optimization techniques for ALSTE-RP. A scalable TE scenario was implemented in a real-time simulated environment using OPNET 16.0.The influencing factors in WMN optimization includes:

- **Traffic control and management**– this design promotes the control of data traffics based on identifying specific traffic patterns in the data cache or using pre-existing flow history and adapting novel specific traffic. Best suited for both point-to-point TE links and Link state connections. Learned traffic pattern is best suited for this control purposes.

- **Redundancy control of traffic** - eliminates the transfer of redundant data and updating of redundant links across the WAN by sending coded information updates instead of the actual lengthy packet. Eliminates repetitive traffics.

- **Traffic data compression** - data traffic patterns (transmission links) can be represented as coded signs that can be translated at the receiving mesh nodes, i.e. cryptography or encryption. This also reduces high overheads and data memory spaces and enables faster processing. It gives data packet security and needed encapsulation.

- **Routing protocol cache/proxy** – reduces high bandwidth utilization and helps in faster access of routing information in the routing protocol. In addition, improves the security of transmitted packets against attacks. i.e. DSR

- **Anti-spoofing** – protects the network from security challenge, a spoofing attack is a situation in which one mesh node or program successfully acts as another by falsifying data and thereby gaining an illegitimate advantage in the WMN.

- **Overhead reduction** – reduction of the latency and interference in the network transmission using a designed algorithm. Low computational path selection.

- **Higher processing design**- adapting a larger space and higher processing power mechanism.

- **Traffic management (scheduling)**– Planned transmission in divergent heterogeneous traffic requires employing priority based real-time timers or programmed send operations to routing and link usage on the WMN.

- **Connection limits** - Prevents access gridlock in routers and access points due to denial of service (DOS) or peer-to-peer on WAN links. It controls network access and connectivity in WMN.

- **Multi-adaptable data rate traffic**– balanced sharing of bandwidth and links from one user node to another transmitting node from getting more than a fixed amount of data at a given time.

The ALSTE-RP approach in WMN allows setting up explicitly routed TE-label switched paths (TE-LSP), where the links satisfy mapped-sets of TE identified metric-based constraints. TE mechanism combines explicit routing capabilities of the network with a constraint-based TE based routing concept based on dynamic mesh node neighbour resources discovery mechanism of router information updating. The proposed ALSTE also uses time-delay and throughput constrained path, low-computation, with distributed LSP signalling with resources reservation protocol (RSVP-TE) for the QOS of the wireless network. The adaptable options are modelled using network simulator OPNET 16.0 and enabled over a campus designed WMN for performance and analysis. The TE ensures that functions such as network resources usage, reliable QoS delivery at the mesh destination nodes, and faster link recovery are highly optimized. TE-LSP can be used to route traffic flows between network edge routers in the mesh network. Our computational approach increases the overall resource utilization using TE-based adaptive optimization of network components.

In ALSTE optimization, we studied different optimization procedures and adopted the technique using the multi-layered objective protocol formulation of the faster processing and low-overhead computation, TE technique in a linear function programming of the link's bandwidth usage. However, this process minimises routing overhead cost and has a drawback in terms of uneven distribution of traffic links on WMN. The irregular traffic distribution of transmission links creates under-utilization of mesh network resource and sometimes, over exploitation too. However, there are other proposed

optimization techniques, with different TE path computations, minimizing the resource usage and maximum link utilization of the network resources and achieving a finer traffic distribution and extended scalability but nevertheless, it comes with a high packet processing overhead.

In this research, we propose ALSTE-RP using a deterministically sequenced, low-computational, iterative optimal path search based algorithm to address interference based high overhead, increasing scalability overheads and to improving load balance on the WMN. We import node and link failure recovery mechanism to readdress the congestion and distribution challenges. Delay-based routing protocol constraints are used to optimize real-time delivery of multimedia traffics in a hierarchal designed WMN infrastructure.

There are existing proposed works on other various algorithms for TE-routing protocol resolution such as mixed integer programming optimization, piecewise linear function or game theory based approach and linear programming methods. In all these, the degree of path diversity depends on the choice of routes for the LSP's. The computation of these routed paths also adds to the capacity by over extending wider coverage areas.

3.4.2. Optimization algorithms in routing protocol for wireless mesh networks

The existing WMN is an adaptation of the ad hoc wireless network and therefore brings on board multi wireless packet traffics from diverse traffic applications with different quality of services requirements. The main requirements of these algorithms are to keep the computation low, reduced complexities and improve performance based on the constrained factors. In addition, TE ensures efficient traffic flow control and connectivity management. TE-low computed paths are achieved using constrained metrics such as time-delay, QoS, reliability, load balancing, coverage capacity per increasing nodes/scalability, data-rate throughput, packets drop in transmission. These factors are optimized using a transmitted packet deterministic sequence method, in a low-complexity computation.

Routing protocol in WMN transmits network transmission information and also updates the topological, link and mesh nodes states on the routing cache or database.

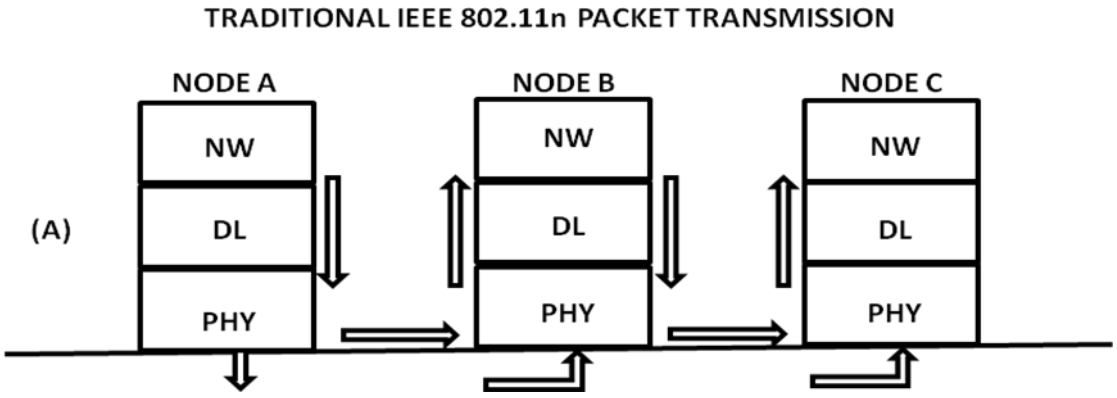


Figure 3.4a: A layered transmission without TE optimization

In the Wireless mesh transmission scenario, we use the schematic model representation as shown in figure 3.4a. We modelled using OPNET 16.0 and we expanded the network transmission direction and layer activities as shown in figure 3.4a. Optimization is a combined cross layer hybrid in layer 2 and layer 3 but the physical layer (PHY) transmission of packets which is also optimised is carried out employing node adjacency packet switching mechanism. These physical layer or layer 1 transmission of packets is done on the peripherals using nodes clients in the WMN environment. In this model a combinational sequential hierarchal algorithm is proposed for path computation. The combination of the node adjacency and the linear hierarchal sequentially distributed transmission using faster-forwarding, TE switching and maybe routing in layers 2 and 3 of the model. The hierarchy between the AP and the internet cloud is pre-determined with a path and are usually TE optimised. In figure 3.4b the two upper layers, the network and the data-link layer are optimized for the TE fast forward packet transmission either by routing or by fast switching. The fast forward switching and routing algorithm creates a more forward transmission of the data packets without the normally

received acknowledgements sent across the network. These measures ensure faster processing at the nodes and also the overall network. The cross layer effect of the optimization enables faster throughput at the destination nodes of the Campus mesh network.

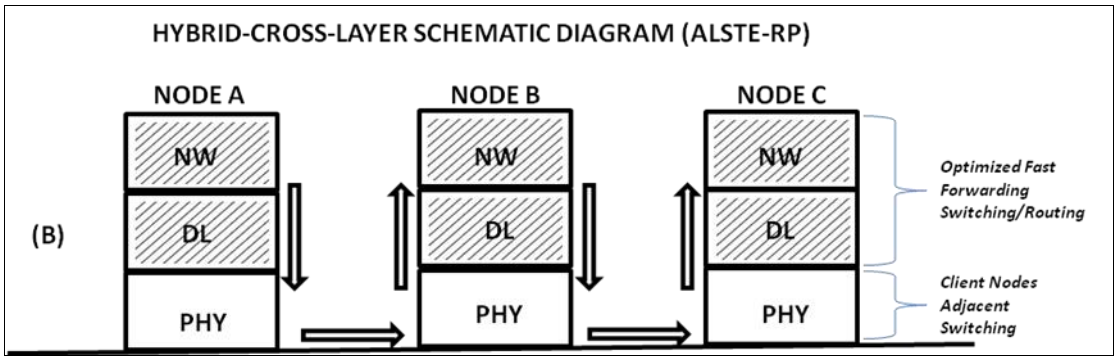


Figure 3.4b: Layered transmission showing TE- optimization

3.4.3. Algorithm development

Designing and modelling WMN as shown in figure 3.4a and 3.4b, we focussed more on the TE of the routed packets. In this aspect of transmission of the wireless mesh routed packets, we study the enhanced capacity utilization of a normal routing protocol given by the equation formulation ????. Djikstra's shortest path equation is employed for weighted path selection and calculation but since we are dealing with transceiver mesh node we also use IP addressing configuration for TE paths. These are deterministically-sequenced in an iterative search on a looped-pseudo code. A designed TE improves major factors in the networks traffic throughput and enhances low-path computational overhead with fast packet forward algorithm which was later coded using C++-programme language in the OPNet 16.0 model design of the WMN network traffic for real–time simulation and performance testing using already the identified metrics.

3.4.4. Controlled Path selection mathematical formulation -ALSTE-RP

We propose an optimal routing scheme for WMNs through inspiration from Djikstra's shortest path algorithm. In the initial phase, a packet makes ant-like

moves to its destination by randomly selecting a path. After a packet passes through a node, the node increases its pheromone value [23, 24]. Thus, we have applied a finite element method to assign a pheromone value to each node within a WMN. Let us consider a system model of with connected an undirected graph G= (V, L) Where V is the set of vertices (node) and L is the set of edge (link) with pheromone value as cost of link figure 3.5. Each node V contains set of multiple pheromones P (t) corresponding to the destination ID at time *t*. Djikstra's algorithm provides shortest path for any given vertex ***j*** to source vertex, which uses dynamic integrative process equation 1 and equation 2. We get the shortest path through back tracking the S (V_j) up to source vertex [1, 2].

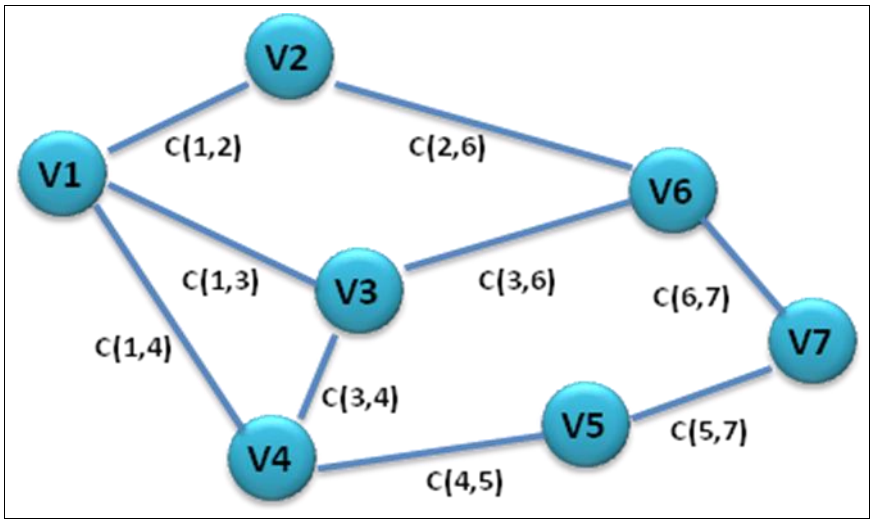


Figure 3.5: Undirected graph G= (V, L), (c is cost of link L)

$f(V_j) = \min\{f(V_j), C(k,\mathbf{j}) + f(\mathbf{V_k})\}$, ……(1)

V_j is neighbor of $V_{\mathbf{k}}$, V_{k0}= Source Vertex

$\{S(V_j) = k, f(V_j) < C(k,j) + f(V_{\mathbf{k}})\}$,…… (2)

Where S is optimal successor vertex for vertex j

Algorithm:

Input:

G= (V, L): Graph **G** with vertices **V** and L is an edge with **Cost**

VS: Source Vertex

VD: Destination Vertex

Output:

Path: set of vertices that on optimal path between **VS** and **VD**

Variable:

Cost2S: Array of distances from the source **VS** to each vertex **V** in **G**

Prev_Opt_Vertex: Array to store previous vertex on optimal path from source to each

U: Array to store Vertices

CV: current Vertex

Begin:

For each Vertex **V** in **G**

Cost2S [V] set **infinity**

Prev_Opt_vertex [**V**] set **NULL**

End

Cost2S [VS]:= 0

Push **VS** in **U**

While U is not empty

CV: = **U [**First**]**

For each neighbor vertex **nV** of **CV**

if [**Cost2S**[**CV**] + **Cost** (**nV**, **CV**)] < **Cost2S**[**nV**]

Cost2S [**nV**]:= Cost2S [**CV**] + **Cost** (**nV**, **CV**)

Prev_Opt_vertex [**nV**] := **CV**

End

End

U: = push all **nV**

Sort the **U** in increasing order based on Cost2S value

If U **[**First**]** vertex equal to Destination vertex VD

Temp: = **VD**

Push vertex **VD** into **Path**

While Prev_**Opt_vertex [temp]** is not equal to **VS**

Push vertex **Prev_Opt_vertex [temp]** into **Path**

Temp: = Prev_Opt_vertex [temp]

End

Push vertex **VS** into **Path**

Return Path

End

End

End

3.5 Modelling, simulation environments and factors.

Figure 3.6 shows the WMN model implemented in OPNET 16.0 Modeller for ALSTE-RP. The model is adapted from the IEEE 802.11b/g based ad hoc network and includes the mesh mobile clients and static backbone mesh routers. The hierarchal architecture of the WMN was implemented using administrative domain (AD) cluster design in a hierarchal structure. In the model, every IP router was dynamically assigned as AP for each of the four WLAN mesh nodes in the cluster -base Access Point pattern.

The modelled architecture with mesh nodes are enabled using random waypoint wireless model. In addition, the mesh routers with IP gateway functionalities were assigned as backbone routers. In the model, 18 traffics sources: MPLS, Acer, MPLS VPN and single sourced transmissions are assumed to have maximum mobile average speed of 5 m/s. 25 mesh IP gateway routers are placed in multiple AD of 100 nodes clients mesh. The analysis is done between the normal traffic packets transmissions and compared with the ALSTE-RP optimised traffics in the modelled simulation environment and later these results are evaluated and then compared with real-time scenarios.

The TE enabled IP configuration and dynamic assignment of node addresses in the network while the ALSTE-RP attributes are enabled in the advanced attributes of the OPNET 16.0 simulation modeller together with the IP routers gateway functionalities. These ALSTE-RP attributes are used to activate TE techniques and flows of transmissions. These wireless traffic scenario adaptations were enabled in the mesh client nodes of the WMN model. In addition, the IP gateway functionalities were enabled in the routing protocol advanced attributes, mesh routers, AP for backbone route transmission and the inter-domain communication.

The mobility scenario is based on the random waypoint model. Each node and mesh router starts its movement to a random destination with a random speed, V (uniformly distributed and not higher than Vmax where it is a subset of {0, 1, 2, 3}. We employ a pause time of 15 seconds for another traffic transmission. We employed a constant bit rate (CBR) source for the traffic scenario. The packets are 512 bytes in length and are generated at a rate of 4 packets per second.

In the simulation, we investigated the influence of the TE techniques on throughput, routing overhead, end-to-end delay, delivery ratio, traffic mobility, scalability and reliability. The metrics outlined in the next section are used to measure the performance the TE security techniques.

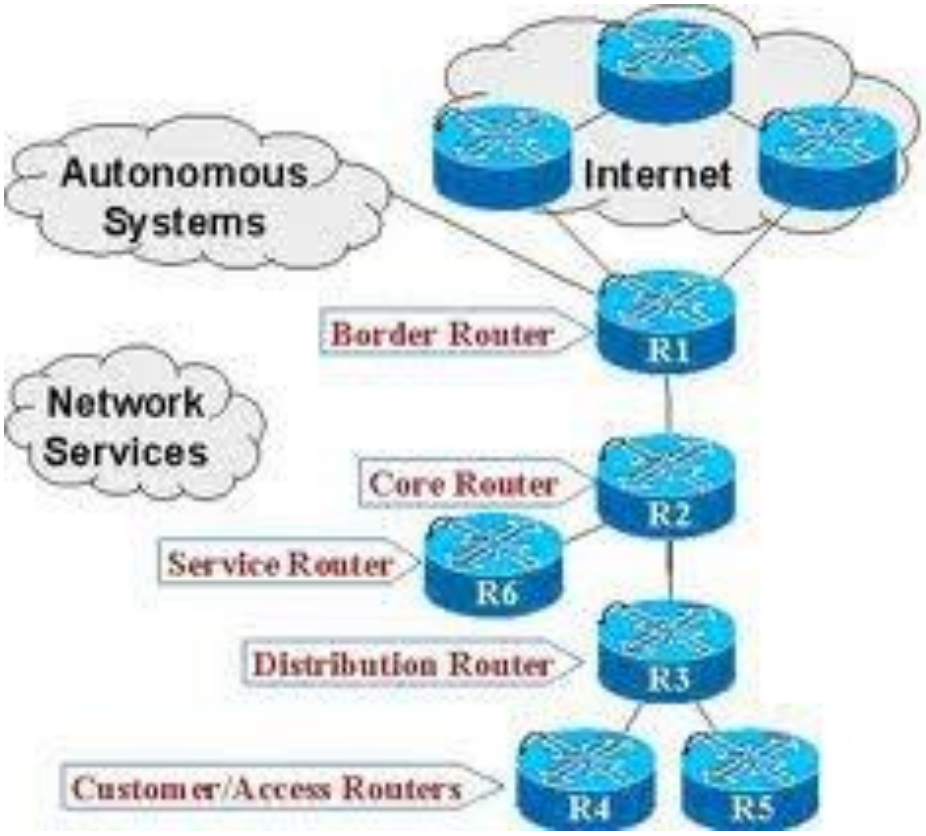


Figure 3.6: example of WMN-TE model architecture implemented in OPNET 16.0 Modeller for ALSTE-RP simulation.

3.5.1. Performance metrics

To analyze the performance of ALSTE-RP in our experiment, we define the following performance metrics:

- **Packet delivery ratio**: The ratio of data packets successfully received at the destination to data packets sent at the source.

- **End-to-end packet delivery rate:** The throughput a data packet transmitting from the source mesh node to the destination is the successful end-to-end data transmissions within a simulation run.

- **Average end-to-end delay**: The transaction time of passing a data packet from the source to the destination, including time of all necessary processing, back off as well as transmission, and averaged over all successful end-to-end data transmissions within a simulation run.
- **Traffic reliability**: The total data packets successfully delivered over a given transmission time for both data packets and control packets.

- **Average Throughput:** defined as the sum of the data delivered to all the nodes in the network in a given time unit (seconds).

- **Average traffic load** – defined as the ratio of the data packets sent to the successfully received data packets.

- **Accepted bandwidth** – bandwidth utilized during packet-data transmission.

- **Scalability per increasing node –** transmission reliability and delivery during network transmission.

3.5.2. Simulation Evaluation and analysis

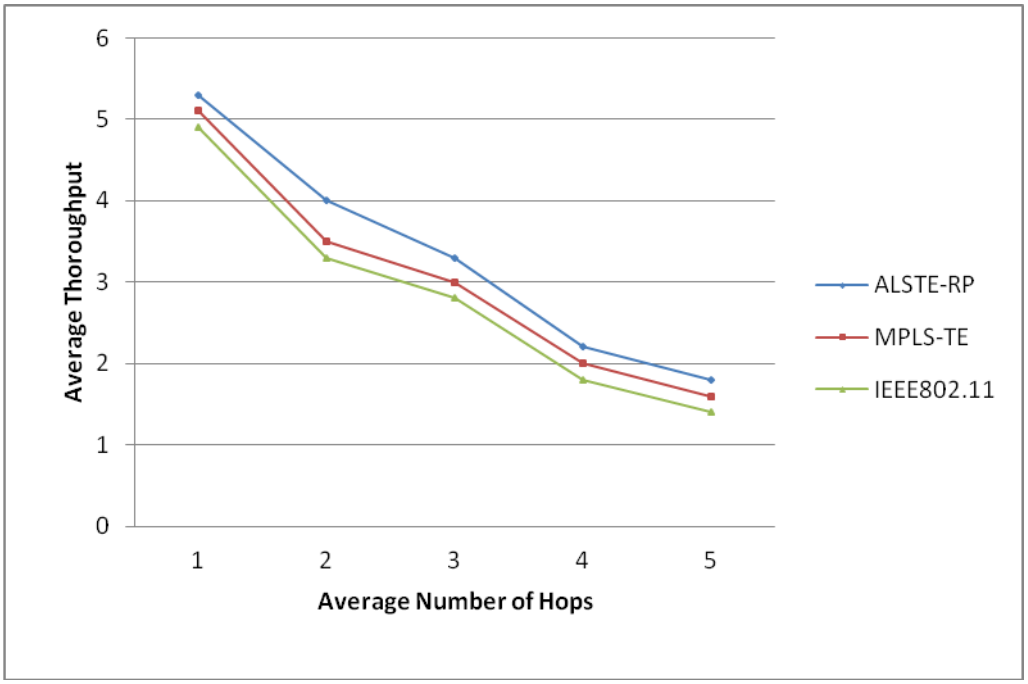


Figure 3.7: The influence of throughput in ALSTE-RP traffic over WMN multi hops network.

The influence of TE traffic packets over WMN multi-hops using average throughput as shown in figure 3.7 at the destination depicts clearly from the graph that ALSTE–RP has the highest gain in throughput over increasing node multi-hop. MPLS-TE performed fairly and has marginal advantages over the normal IEEE802.11. Average throughput compared against average number of hops in the networks shows a decrease in throughput over increasing number of hops in the network. ASLTE-RP using traffic splitting and dedicated IP channels showed more packets in the output because of these and many other traffic engineering tweaking and tuning of the traffic routing attributes in the networks.

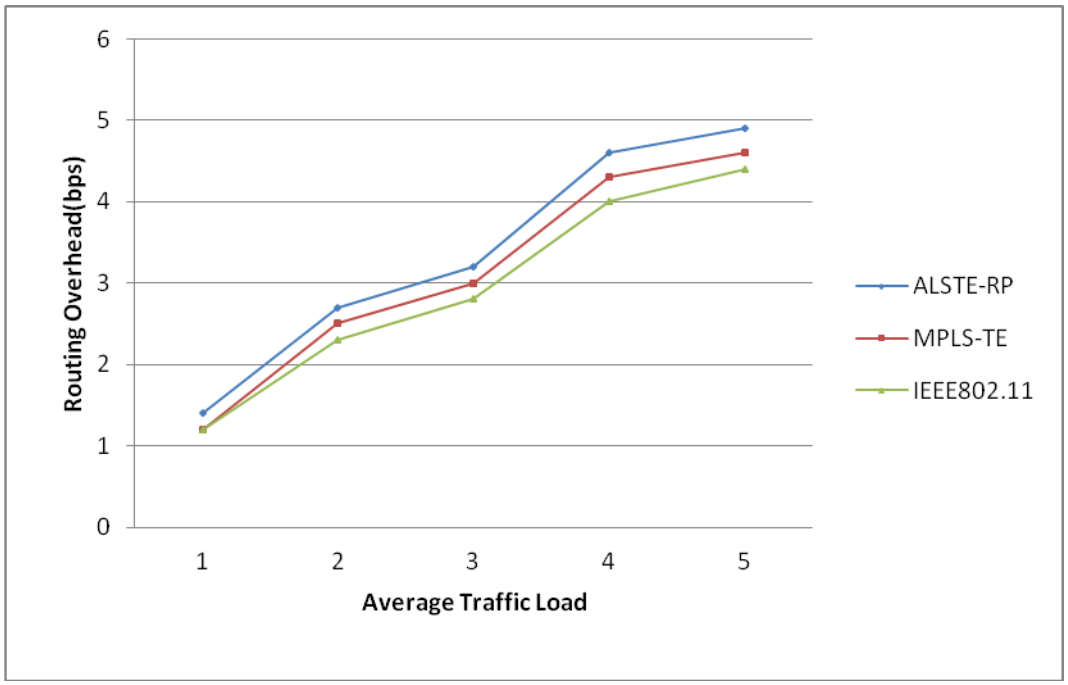


Figure 3.8: The influence multi-traffic packets overheads over average traffic load.

The increase in the average traffic load over WMN shows a corresponding increasing higher routing overhead in the WMN as shown in figure 3.8. ALSTE-RP made a fair gain in low computational routing overhead but like IEEE 802.11 and MPLS-TE traffic experiences low level routing computational overheads. In the MPLS-TE routing optimization, the presence of multiple LSP raises the level of overheads. Though the mechanism ensures dedicated alternative routes, its diversity and optimal performance is affected by the numerous LSP in large WAN mesh networks. IEEE802.11 performance can be attributed to the presence of numerous interference and hierarchal cluster bottlenecks. In summary, the routing optimization overheads are directly proportional to the traffic average traffic load.

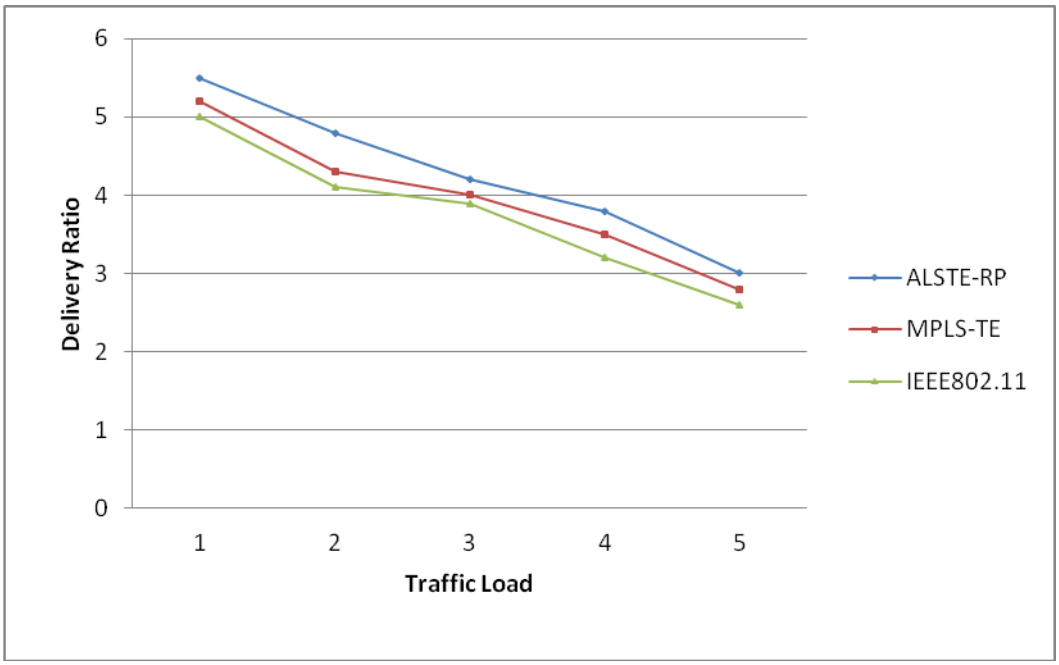


Figure 3.9: The ratio of packets delivery ratio over different routing optimization traffic loads

The source to destination of the packet delivery ratio is inversely proportional to the traffic load on the WMN network as shown from the simulated graph in figure 3.9. The delivery ratio of the various routing optimization traffic increases with decrease in the traffic load. In ALSTE-RP this can be attributed to the TE optimization techniques being used while the rest of the various comparing traffics have similar attitude but with lesser gain.

The delivery ratio is also inversely proportional to the number of hops in a WMN networks as shown in the simulated graph of figure 3.10. The more the number of hops in a large network, the more the scalability challenges and channel routing and limited bandwidth are contestable parameters too. These challenges gives rise to an increase in interference and lowers the delivery rate over average number of nodes in mesh networks. The resultant effects of intermediate nodes and fail nodes and bottlenecks in routing of packets can be overcome with routing optimization TE mechanism such as in ALSTE-RP. In summary, ASTE-RP showed higher performance in delivery ratio under traffic load and higher number of hops in a campus WAN mesh networks.

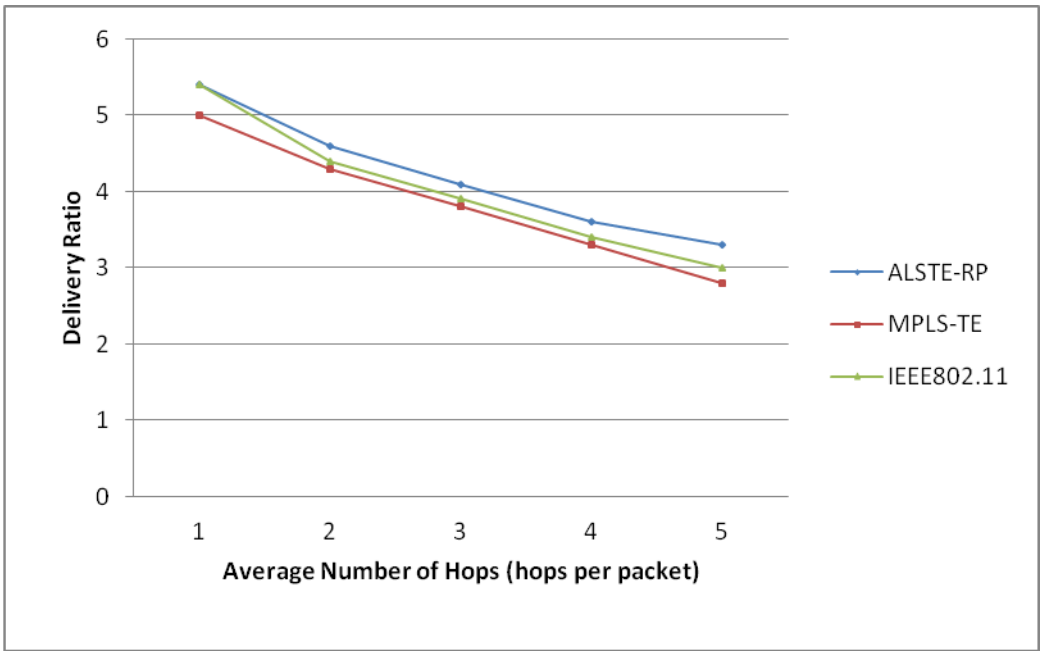


Figure 3.10: The ratio of the packet delivery ratio over average number of multi-hops

3.6. Conclusion

We considered routing optimization using traffic engineering techniques over mesh networks. We further implemented traffic engineering technique over WMN-routing protocol (RP) to formulate higher coverage capacity with lower computational cost, deterministic algorithm to solving the scalability, load balance and low-path computation challenges in the WMN-RP. We propose an adaptive link-state traffic engineered-routing protocol algorithm (ALSTE-RP) with least cost for WMN. ALSTE-RP is compared to a normal WMN packet transmission to show performance based optimization. The resultant performance and analysis shows marginal increased scalability, throughput and a low-computational overhead.

ALSTE-RP increased the throughput at the destination node of the WMN. The result from the simulation and reading indicates higher improvement in the quality of service and less routing overheads. The ALSTE-RP improved traffic control management and redundancy control though the processing gain was higher it showed better performance in mesh connectivity. The routing protocol optimization also showed improved factors in anti-looping and anti-spoofing in wireless mesh routing protocols.

The TE route aggregation and path diversity is also embedded in the core attributes of the ALSTE-RP therefore creating multi-path access and data packet connectivity. The data packet delivery and the end to end transmission showed improved performances using ALSTE-RP too. The scalability tested over an increasing campus network showed a fairly improved performance compared to the IEEE802.11 normal traffic.

In real-time network operations, high capacity utilization of service and link failure resolution is generally improved. Re-route traffic through redundant link capacity creates higher access to increased link capacity utilization. Optimization restores capacity of time-sensitive operations like traffic routing in multimedia video or online streaming television too. Therefore, traffic congestion and link-failures during transmission is highly mitigated and latency reduced.

In overall, ALSTE-RP optimization using the TE in WMN, generally increases efficiency with high throughput data rate and is highly scalable in multimedia traffic communication. It is recommended for broadband community access and mesh internetworking. ALSTE-RP also ensures data integrity and secured communication. In the routing layer of the WMN with optimization with ALSTE-RP algorithm ensures increased load distribution balance and fairness in the mesh network. In ALSTE-RP we may have challenges in high processing but nevertheless it has far more reaching optimization advantages comparatively.

CHAPTER 4

Wireless Mesh Network Security: A Traffic Engineering Management Approach

4. 1. Introduction

The WMN [3,9,10,132] as shown in figure 4.1 is comprised of the mesh routers, mesh clients and the mesh backbone infrastructure. The mesh clients are mobile and dynamic while the mesh router has static or minimal mobility. These mesh routers form the backbone infrastructure of the WMN, while the mesh clients form two level of nodes operation: at the peripherals and on the access-points (AP).

The WMN is similar in operation to the Mobile Ad hoc network (MANET) and it employs a multi-hop routing mechanism from source node to destination node. However, unlike the MANET, WMN uses multiple interfaces and multiple radio frequencies. Furthermore, it uses high speed back-haul network and gateways to optimize network performance and integration with other wireless networks. The mesh routers can also be gateway nodes to the exterior internet cloud or to other networking technologies. These mesh routers operate as bridging points in inter-network and integration with other wireless devices. The AP is a node interface for hosting and retransmission; it provides integration between the mesh client and the mesh backbone infrastructure in WMN. The WMN is self-configuring, self- organizing and self-healing. These qualities make the WMN an excellent wireless access technology for multimedia and community broadband (IEEE 802.16) [134].

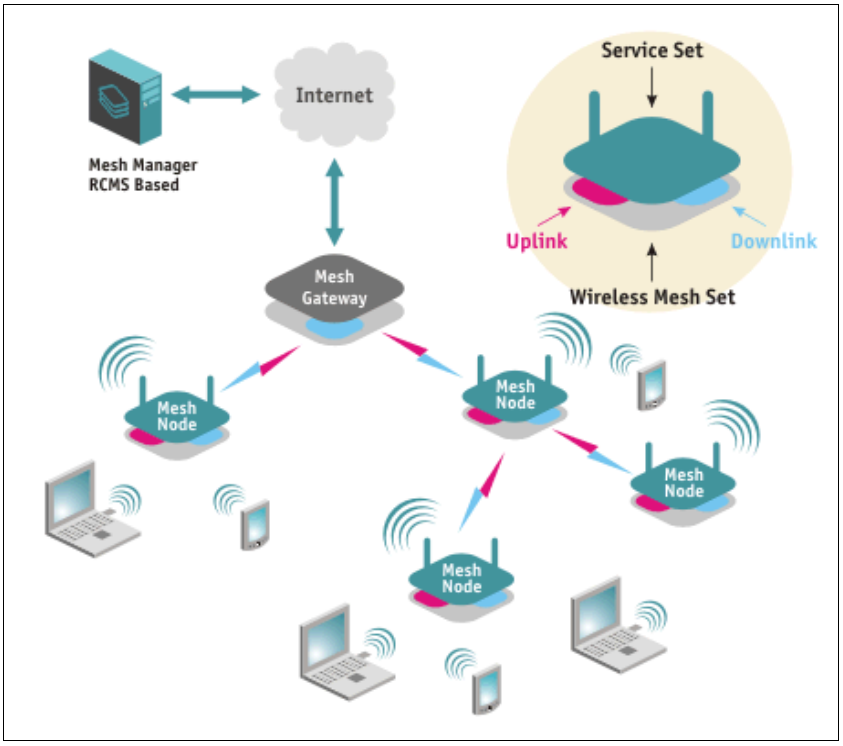


Figure 4.1: Wireless mesh network scenario with internet gateways. [133]

WMN is an IEEE 802.11s standard [135] with extensive work being done by workgroups on achieving a standard for its different challenges and protocols. The modifications and adaptations of the ad hoc networks are mostly on the security and routing protocol of WMN. This has led to the adoption of wireless local access network (WLAN, IEEE 802.11i) security and WIFI protected access (WPA) [136] for WMN. However, improvements by the standardization forums have seen enhancement in the authentication, encryption and integrity of WMN security.

Moreover, as most wireless network are now mostly seen as access-networks to internet or internet service providers(ISP), the Internet Protocol (IP) are easily configurable to achieving a better comprehensive security in the WMN architecture. The WMN unlike the ad hoc networks has commercial qualities, such as it is easily scalable, mobile and dynamic; but these characteristics also create security lapses in the WMN routing operations and MAC layer of the WMN protocol. In 2004, IEEE 802.11i formed a task group (TG) [137] to prepare and improve the standardization of the WMN.

TG was to ratify and prepare the standard amendment to meet the targeted requirement for WMN (IEEE 802.11s). The use of WMN as gateway access to community broadband internet has created an increasing requirement for secure wireless communication operations. In response to the high commercial demand for multimedia and broadband network operation, due to its low-cost and easy operation, high sensitive applications have created a necessity for an effective and comprehensive security mechanism in WMN.

WMN operate as access underlying network for broadband. The Broadband are dependable and appropriate for many important communication operation and application like voice, data and multimedia services. WMN access for broadband communication networks is both interoperable and easily complementary. Many wireless network applications utilize the broadband network for connection to the internet. WMN, similar to other network applications, make use of IP addressing and configuration. Most of the transceiver-IP nodes in the WMN are mesh clients and routers with gateway functions operating as access to the internet. Furthermore, the mesh routers act as backbone network, while the mesh clients use medium access control (MAC) addresses for frame transmission among neighbourhood network nodes. The IP addresses are enabled by configuration and are either dynamically or statically assigned in the network routing protocol layer. Other layers of the WMN like the transport and session layer protocols transmit routed packets after encapsulation of the data traffics in IP datagram - user datagram protocol (UDP) or transmission control protocol (TCP).

WMN provides a good potential commercial access for community broadband and multimedia networks. The broadband networks are increasingly popular due to the upsurge in internet applications and electronic commerce (e-commerce). WMN is easily scalable over increasing network sizes and provides a low cost and low battery consumption network. It also has an added ease of integration with other wireless and wired networks. The architecture and operation incorporate a hierarchal

transmission of traffic and network notification packets through the peripheral (client) nodes through the AP nodes to the backbone wireless mesh router nodes via router gateways to the wireless clouds (internet).

The routing operation of these data traffic over wireless mesh architecture network creates a vulnerable security system caused by the multi-hop traffic transmission and loose node-to-node data exchange during inter-node authentication mechanism, while routing neighbourhood nodes information and exchanging new nodes updates. In addition, the multi-hop behavioural characteristics of the WMN create challenges on the security of the traffic operations while in transmission through the gateway to the wireless cloud. The dynamic topology updates further exposes the whole network security to persistent and corruptible attacks. The reliability and authentication [138] of data traffic in WMN during neighbourhood nodes exchanges through link state and in routing operations is loose and very insecure. The ease in WMN integration with other wireless nodes and communication networks like in broadband and multimedia, has also established the necessity for an unyielding privacy protection and security mechanism [139-140].

The distributed-sequenced mechanism in the network's MAC channel frames also creates susceptibility to attacks while the mobile mesh client nodes and its consequent dynamic topology in the wireless mesh infrastructure also establish the need for more effective, resilient and comprehensive security system in WMN. The constraint in WMN security creates the challenge of possible attacks by invasive worms and viruses, when on attack through simple dynamism of mesh become distributed in the architecture. These attacks compromise the confidentiality, integrity and violate the privacy of the network users. Furthermore, the nodes can also be compromised by the operation of traffic transmission, unverified router information exchange traffic and network notification infiltration. Finally, there are other attacks on the WMN, from physical vandalism to external physical destruction of the hardware. All these consist of possible constraints on the security of the WMN. There is still a requirement for a comprehensive

security mechanism to prevent attacks and counter attacks in all the different protocol layers and usage of WMN.

The WLAN, which is a subset of WMN security mechanisms, employs the Wi-Fi protected access (WPA2/IEEE 802.11i) [142] to provide standard authentication, access-control and encryption between wireless nodes and AP in the WMN. There are several WMN architectures and their security varies with the variation in infrastructure. In addition, these existing security mechanisms may work perfectly in ad hoc networks, but in Mobile Ad hoc Networks (MANET) and WMN, which uses mobile node clients and either mobile or static mesh routers, there is requirement to develop a mesh-managed security mechanism to adapt the WMN transmission traffic operations and dynamic architecture. The Wi-Fi Protected Access (WPA) was supposed to be the solution to several weaknesses noticed in the previous wireless networks with wired equivalent privacy (WEP) [143]. WPA implements most of the IEEE 802.11i standard and was a transitional measure in place of WEP while the standard was being prepared. WPA works with all wireless network interface cards however, it is not compatible with first generation wireless access points. WPA2 implements the full standard and offers better security. WPA uses a less secure "pre-shared key" (PSK) [144] mode mechanism on IEEE 802.1X authentication servers, which distributes different keys to each user in the network

The routing protocol of the WMN carries out most of the routing and transmission of data. The mechanisms of routing are diverse and depend on the dynamic topology and traffic existing in the network. The IP enabled nodes and mesh routers in the WMN architecture are mostly internet gateway nodes. These IP nodes Mesh clients (IP nodes) connect to the wireless cloud through IP enabled addressing, configuration and logical TE through secured interface routing. In TE, the Multi-Protocol LAN Switching (MPLS) [145] uses the label switching mechanism technique to forward traffic data through the network from source to the destination using segregated best paths. It provides packet encapsulation which creates secure paths for data traffic transmission too. This mechanism also offers a secured and

reliable alternate path for routed packets in the network. The TE [146] mechanism is a concept using data traffic management rules (configuration and access-list) to address internet and gateway protocols data transmission and routing best path determination. This technique also addresses the security, route selection, best path and the consequent effect of bandwidth optimization through these processes.

In the remaining parts of this chapter, we will discuss the different security challenges and threats in the WMN while the existing security solution mechanism will be evaluated with a bias to traffic- engineering security resolutions in WMN. The different Multi-protocol TE techniques to resolve the different security challenges in WMN will be discussed in later in the chapter. Then, technical design, metric formulation and security scenario testing, evaluation and analysis using TE management technique model in WMN security will be discussed.

4.2 Types and analysis of security challenges in WMN

The characteristics of the architecture and structure of WMN just like the ad hoc and other wireless mobile communication networks are susceptible to security challenges. The distributed-sequenced network architecture and the vulnerability of the shared wireless medium in the channel-access and the neighbourhood clients‟ information exchanges, expose the WMN to these security attacks. The WMN is a dynamic multi-hop network and these frequent changes in the topology require security authentication for notification updates. Security attacks can occur in the routing layers, the nodes-clients updates and as notification message poisoning. In addition, there are the communication security lapses in routing operation and packet transmission Therefore; the IEEE 802.11s security is not yet fully standardized. Some of these attacks and security impairments [147] are:

- Signal Jamming
- Distributed Denial of Service (DDoS)
- Battery Exhaustion attacks
- Worm hole attack

- Black hole attack
- Location disclosure attacks
- False message attacks
- Rushing attack
- Spoofing of wireless infrastructure
- Theft of service attack
- Traffic Flooding attacks
- Route cache and table overflow attack
- Resource depletion attack
- Forging
- DNS spoofing
- Tampering
- Physical attack

These attacks create negative impairments, message corruption, network infiltrating and depreciate the network resources. In summary, these attacks damage and compromise network data-traffic. These attacks target network essential components like the AP, the battery life, the node mobility, the routing table and cache including also in the bandwidth of the WMN. Security challenges can be resolved by counter-attack mechanisms, intrusion detection concepts [148] and network resolution or diffusion of affected threats in the network. In multi-hop wireless network architecture, the security mechanism uses a comprehensive security mesh key and encryption. A secure MAC layer also ensures that traffic from mesh network is authorized and by doing this safeguards access into neighbourhood nodes. The listed security attacks as shown in Table 4.1, in the WMN security attacks can occur on a protocol layer or are multi-protocol in communication. Therefore, a multi-protocol mesh solution approach remains the best technique to resolving these security issues.

The IEEE 802.11s identified different conditions for contention based and connectionless access to the wireless channels. The contention based

mechanism in data traffic allows a back-off while keeping transmitting node connected to the wireless medium. The MAC layer in the second layer of the protocol stack ensures fairness in access and transmission in the radio channel. The IEEE 802.11s MAC [149] layers use the coordinate function (CF) to seamlessly provide contention and contention free access in the medium. The traffic flooding attacks on the MAC layer are resolved using enhanced distributed Channel Access (EDCA) which is a QOS aware coordinating function [150].

To resolve the attack, the standard defines a mesh deterministic access (MDA) [151], which is an improvement as it gives contention-aware, contention-free and contention based access. It further provides authentication based contention access resolving the problem of hidden nodes within the radio frequency range causing interference and creating multiple reception terminals due to the fact that many nodes are transmitting at the same time. Rogue stations usually use these hidden nodes to broadcast and to request for limited bandwidth preventing real stations from transmitting. This mechanism gives privileged access and exclusive permits for station to the radio channel.

Table 4.1: A WMN Protocol layer security threats and attacks

PROTOCOL LAYERS	SECURITY THREATS
Application	Resources depletion, application authentication
Transport	DNS spoofing, traffic attacks false message
Routing	Black-hole, Wormhole, Grey-hole, rushing attacks, Location disclosure, DOS
Data Link	Signal Jamming, flooding attacks
Physical	Tampering, Collision jamming, physical attacks, battery

The multi-hop nature of WMN packet data transmission to the gateways has important commercial potential; nevertheless, it contributes to some of its mesh security weakness. In wireless mesh communication the security attacks are mostly interception of links and packets, denial of service attacks (DoS) [152-153]. The denial of Service (DoS) is a major security attack that frequently occurs in the WMN. In distributed sequenced traffic processing Wireless network, it results to a worse scenario called distributed denial of service (DDoS). The security threat of DDoS occurs most times in the WMN when requesting nodes are not offered with requested services and updates in a maximum given time. The DoS attack network availability and reduce communication between network devices in data transmission and reception. It violates the access security and authentication of traffic in ubiquitous WMN in so doing prevent communication of transmission by stopping a sending/receiving device or maybe links too. The mesh routers which are mostly the backbone infrastructure in the WMN architecture are coordinate nodes in a hierarchal topology. Though different WMN can interconnect in gateways and routers through different administrative domains (AD), the DDoS attack on mesh routers can paralyze the entire transmission of data packets across the WMN. The DDoS threat can appear as wormhole, Black-hole and Grey-hole and Distributed flooding DDoS attacks in the routing layer of the OSI model as differentiated in Table 1.

A DDoS is always very difficult to manage in large WAN networks. They consume large network resources to the extent of rendering the WMN ineffective. DDoS are spread by natural distributed processing architecture of the network. It normally quickly floods the access point (AP) and backbone mesh routers using those hierarchal control points to congest the WMN traffic communication. The use of network programmed anti-Trojan or antivirus software to target these DDoS zombie threats are usually employed to neutralize the attacks and to destroy the DDoS zombies. The DDoS can also be Traffic flooding attack in the WMN, where the attack compromises the

large number of mesh clients in campus network. It overflows the network and causes flooding. It congests the network resource and use up available bandwidth.

The routing mechanism of the WMN in multi-hop transmission keeps changing from disjointed traffic, to slow and quiet traffic in the backbone and to active exchanges in the peripherals. The attackers can infiltrate the routing mechanism and its performance by altering, tampering or even forging of false messages or routers notification. The attacker can modify packet data messages using replicate nodes to carry out DDoS attacks. In spoofing of wireless infrastructure, the attacker uses a replicate or a silent "man in the middle" attack to execute information disclosure threat in an enterprise deployment such as WMN. These attacks can be alleviated using EAP [154] methods that allow authentication between clients and the WMN infrastructure.

Furthermore, in the routing layer protocol the wormhole and the Black-hole are security attacks that cause security weakness in the WMN architecture. The Black-hole is a security attack situation where on receiving the route request notification message, the attacker claims he has the link to the destination node even when this is false, consequently making the source node to continue sending messages to the attacker which are not forwarded to the destination node. However, in a wormhole security attack, the source node and destination nodes in a wireless network are maliciously connected by a wormlike, which is a low- latency link of transmission. Once the wormhole link is established, it can be used by the attacker to compromise the integrity of the WMN security. In wormhole the attacker uses DDoS techniques to threaten the WMN security.

In the Physical layer, tampering security threats involves the attacker modifying the data-traffic information on routed packets. The WMN works on the principle of mutual meshing and supportive hierarchal network. It is a web-like, interwoven and dynamic network; therefore while transmitting data, the attacker can distort the sequence numbering, the number of hops

or other frame data field. Consequently, this causes network resources to reroute, redirect and reconfigure routes, taking up bandwidth and processing time and consequently degrading the eventual performance of the entire WMN. It sometimes could result to looping problem, count to infinity in the routing protocol and high overheads in the network. Tampering generally occurs when routing information is lacking in reliability check and accuracy of data packets. On other hand the “pretend attack” is the inability to verify the joining node in a mesh network or the ability of the attacker to claim link or act as if it is a mesh router. This occurs in the WMN when source address of the data packet is not verified.

In addition, in physical layer of the WMN protocol, we also have the signal jamming. This is the security threat that occurs when an attacker jams the interface of a transmitting or routing node on the physical channel. They usually employ the frequency hopping on the communicating node or may even use the defence tactics of spread frequency spectrum matching over the communicating signal range. This security threat is very difficult to be prevent using detection intrusion because the attacker is blocking the sensing devices. In some level of the hierarchal model, the attack is flooding and frequency jamming attack in the physical layer. Spread frequency optimizers like direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) techniques are regularly employed in prevention and detection of these signal jamming, ultra wide band (UWB) and different frequency multiple access technologies are also used enhance prevention.

Another malicious security threat involves forging. In this scenario, the attacker forges network notification messages and broadcast wrong information to the network and other surrounding nodes. Wrong routing information like link availability and hop counts are usually forged by the attacker. The poor verification and authentication of the packet data contributes more to this threat in WMN. In addition, the other threats and attacks in the routing layer as shown in Table 4.1 are resource depletion attack and rushing attacks. These security threats on WMN attacks the radio

frequency bandwidth, the node header, routing table, cache and the battery of the nodes-routers. In the rushing and resource depletion attacks, the attacker continuously sends a lot of route request packets over the WMN in a short time creating a bottleneck and congestion for nodes in processing these network route notifications. These insidious attacks deplete or slow down the network resources. There are also topological attacks caused by the attacker obtaining the topological information variation in the routing layer of the WMN. The attackers usually impersonates a requesting node, learning the traffic flows especially in hierarchal routing protocol, obtaining the location control nodes and eventually controlling the information spreading in the network. The WMN is an enterprising wireless network and it comes with improved ubiquitous traffic and easy scalable mesh formation. These characteristics improve availability and confidentiality however; there is a clear need to improve the reliability of the network with a more secure system that will fit the dynamic mesh mechanism of the WMN. The design of WMN and mechanism of operation have shown proof of the need for a more effective secure mesh network. Furthermore, wireless network migration from ad hoc networks to MANET and lately WMN creates adaptive design consideration both on infrastructure and also on the security of the client node meshing access control and inter access-point meshing.

4.3 *Access-control Mechanism*

In WMN standard IEEE 802.11s, the mesh client access control mechanism contributes to the secure access control of the transmitting nodes in the network. It may vary from open wireless authentication to secured 3-way handshake verification as shown in figure 4.2 and it also provides access for non-mesh technologies.

Migration in wireless technology from ad hoc networks through MANET and presently to the existing mesh technology creates behavioural change in characteristics in wireless mesh clients, the routing mechanism and channel access in the security of the wireless networks. Furthermore, with

the access- control gateways to the wireless internet, IP configured access-list and other security are currently applied to IP nodes in mesh clients and AP. The routing protocols do not really have facilities for multi-hop routing security or traffic transmission packet reliability and integrity. In network deployment, the IEEE 802.11s does not secure un-trusted nodes as in the ad hoc networks. However, some ad hoc network security control concepts are carried over successfully and implemented in WMN such as the authentication of routing notifications using digital certificates, protection by symmetric cryptography using shared passwords and digital signatures (SAODV) [155], message detection and integrity protection using public keys in the shared keys security and hash chains encoding detection of tampering in routing information within the network (SEAD) [156]. This digital certificate acts as passes for mutual or shared authenticated key access. Security management mechanism can be applied in two areas of the WMN using adapted ad hoc techniques. The WMN in operation never applies encryption of data traffics. Furthermore, distributed sequenced data processing and transmission of routed packets equally circulates the failed secured points in the mesh network. The key major features of a secure WMN are the availability, integrity and confidentiality.

In addition, in the EEE802.11s, inter-mesh access point controls technology offers diverse traffic types which are liable to insecure communication mechanism in routing transmission. Wireless mesh access- points are transmission points in the hierarchal WMN to the routers-backbone. They receive data packets traffics from wireless mesh clients nodes and the peripheral nodes for onward transmission to the mesh routers or backbone networks. They also transmit routed packets to the nodes and peripheral nodes. Consequentially, they act as trans-receivers station nodes. The distribution mechanism is mostly sequential and incremental. The wireless distributive sequence system makes it easier to secure IEEE 802.11s by encrypting the security key with WEP. While on the WPA2-802.11s, the design develops into WDS encryption with WEP or AES and the mesh-clients

can be connected to the mesh AP using alternate security mechanism with or without encryption. The two techniques of inter-meshing the AP‟s communication in advanced 802.11s-WPA2 include:

- Configuring the static keys at the both ends of the WDS and employing encryption between the mesh nodes.
- WPA2-802.11s defines how key 4-way handshake mechanism works in WMN. Mesh traffic relays using WDS modes for inter-mesh AP traffic is secured by WPA2.

The WMN data routing operation and updating mechanism is a departure from the existing ad hoc networks security and the multi-hop and mobile node routers technique in the wireless infrastructure consequently impairs the data integrity and the overall network security. The intermesh exchanges can be governed by service levels of agreement (SLA) in the mesh router and AP hierarchal level and spot agreements in the clients' nodes/peripherals. Contention based access constraints in the WMN uses the CSMA/CA with RTS/CTS mechanism in prevention and resolving multiple and contentious access but suffers DoS attacks. The limitations of these conventional adopted techniques in effecting a secure transmission operation during WMN communication has necessitated a possible solution to these access control security challenges using traffic engineering.

4.4. Existing security measures in WMN

In WMN, the majority of the AP and mesh clients have to be enabled by a unique security key unless the AP nodes will not communicate with each other. The WMN currently uses the Ad hoc security standards and WMN being a further migration from ad hoc has its structural and architectural differences which necessitates the need for a security for multi-hop routing operation and secured inter- node peripherals exchanges and updates. The size of the network and the number of clients' neighbours help in determining the number of session keys. The different security measures in the WMN include:

- Authentication
- Cryptography
- Encryption
- Firewall
- WEP and WPA2
- Intrusion detection
- IP access-list filtering and control.
- IP virtual private networks traffic (VPN)
- Mesh security management.
- Web-mesh application managed security control
- Traffic engineering multi-protocol security mesh

4.4.1. Authentication

In a secured WMN communication, the integrity of the data packet from source-node to destination- node is checked and verified for unsuspecting mesh client access or infiltration and authorization to network resources is mostly in a privileged mode. The authentication of user nodes prior to access contributes to ensuring that the identity of the nodes and links in the network are preserved and forestalls infiltration of rogue nodes. In the WMN, some data and information are classified secret and need special password login access to be view or copied. Access to these areas of the network resources requires authentication of the user nodes. In multi-hop networks, there is no centralized authentication because of the dynamic traffic in the WMN. The authentication of the mesh neighbour nodes at the peripheral during network notification exchanges uses a mesh sequenced authentication technique. The WMN presents many security weaknesses especially because of it is a wireless system that features openness and non- infrastructure medium. Moreover, achieving a comprehensive authentication for multi-hop wireless node access has migrated from single hop ad hoc networks to MANET mobile traffic and finally to WMN multi-hop standards and adaptations.

Initially, in the ad hoc wireless networks, where we observed single-hop transmission, preventing malicious nodes or the attacker from gaining access into network resources requires an authentication technique as used by IEEE 802.1X standard which defines the port based network access. In this design, extensible authentication protocol (EAP) notification is transmitted between the client and (WLAN) port. The protocol for carrying authentication for network access (PANA) [157] was developed later for multi-hop traffic access. It offers authentication similar to IEEE 802.1X and it is independent of the underlying access technologies.

PANA is mostly applicable in IP layer's point-to-point links and multi-access traffic in WMN. A later evolutionary improvement was done on the EAP and PANA optimizing the qualities of both to adapt a design for multi-hop network. The new scheme uses EAP over transport layer security (TLS) in a PANA scenario. It works on the principle of authentication, authorization and accounting (AAA) and uses high-processing and high overhead asymmetric cryptography to establish authentication and manage shared public key infrastructure (PKI). However, it has high overhead in computation.

There are also other mechanisms like challenge handshake authentication protocol (CHAP) [158], as shown in figure 4.2 and message digest 5 (MD5) which are equally flexible with moderate overheads.

While the frame header encryption from the source node will assist in creating reinforced data integrity in the forwarded data packets, it will also address the jamming and flooding attacks as shown in Table 4.1, in the data link layers of the WMN protocol. However, secured node to node and hop-by-hop multi- paths encryption will resolve multi-hop security challenges using traffic engineering technique in the WMN. Generally, the MAC channel access control through Authorization, Accounting and Authentication (AAA) is applied on every node interface during exchange of notification and the topology architecture secures the network either through filtering, digital signatures or negotiated authentication (handshake).

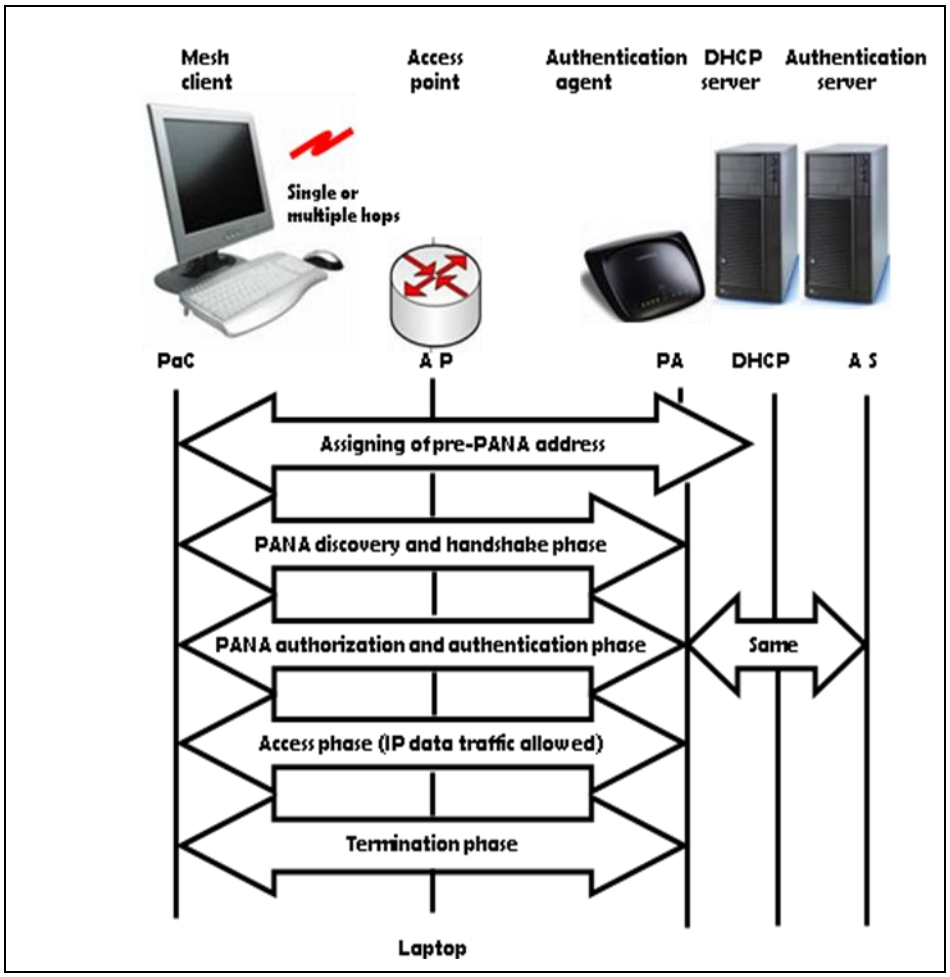


Figure 4.2: An authentication communication mechanism in WMN

WEP and WPA use 40-bits encryption and vector initialization and 256-bits respectively, for both client and AP security. While WEP shares a secret key which is static and enables attackers to analyze and hack into the network, the WPA on the other hand, provides a temporal key integrity protocol encryption and this enables distributive share key per packet. However it is vulnerable to DDoS attacks. These vulnerabilities in the existing security system provide research direction to the use of traffic engineering technique in solving security challenges in WMN.

4.4.2. Intrusion detection mechanism

The WMN security threat, prevention using intrusion detection system (IDS) [159] is perhaps the most effective method to checkmating intruder attacks and resolving security threats in the network. Nonetheless, the

decentralized network architecture and dynamic, random traffic make monitoring and management of the IDS more design demanding. The IDS for fixed wireless (ad hoc) networks and for WMN are completely different because of the topology and the aforementioned decentralized mesh architecture. Design considerations and techniques employed to develop a new comprehensive IDS mechanism to accommodate the characteristics offered by the WMN. The principal idea in formulating these techniques is to improve detection and prevention in the neighbourhood mobile nodes, in the mesh clients and to initiating a quicker response to the attackers' threat. IDS detects and responds to the presence of malicious nodes, links or activity in the WMN by sending out agent's notification and collating the mesh activity information from all the agents and the nodes. It then analyzes the information gathered to check for activities adverse to the security of the WMN. The set limits of the security rules, access limits and timing contributes to the security software dynamic administrator performance determination and security checks. In the security administrator, IDS generates an alarm alert when any malicious activity of an attack or threat to the WMN is determined. Consequently, IDS initiates a proper response to this "foreign" activity.

The IDS sensors are mostly deployed dynamically over scalable WAN to achieve peripheral nodes clients" coverage and response. It is mutually cooperative in gathering sensors notification for alert and response. The architecture and presumed threat determines the nature of the IDS to be installed. Hierarchal wireless networks and flat open wireless networks all differ in operation and these characteristics also determine the point of installing the IDS and the type of IDS to be installed. In the hierarchy, the cluster heads control the rest of the nodes in the cluster and provide functionality to the distributed system in message response and request. Mesh access points make available easy integration detection and preventive controls for wireless threats and attackers. The mesh clients in clusters, neighbourhood autonomous systems or domain may

use cooperative and mutually assistive mesh management monitoring and performance management system.

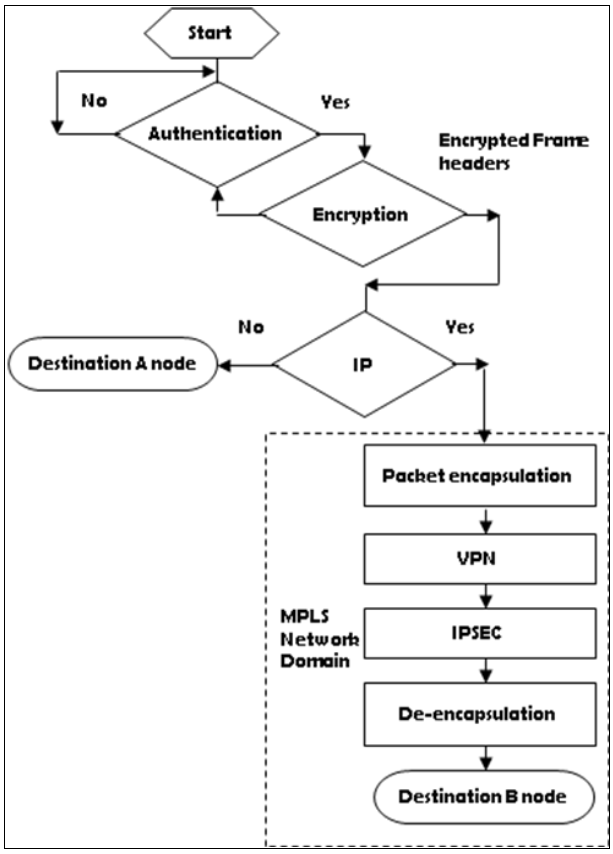


Figure 4.3: A flowchart illustrating a security design mechanism for traffic engineering

4.4.3. Traffic Engineering - Security management

In figure 4.3, TE security management model is proposed for WMN security. This security management model is a cumulative security technique in an incremental-sequenced co-coordinated function process. This management model security brings added qualities of the diverse security resolution mechanisms of MPLS, VPN and IPSec into the existing WMN security. It is made up of three different TE security techniques: MPLS, MPLS-VPN [161] and VPN-IPSec [162] all operating in an incremental-sequenced mechanism. These security attacks are best resolved by preventive methods but most difficult to predict. These clearly indicate that co-operative management security control systems as shown in figure 4.3 will provide the needed best overall practice access-control restrictions and

authentication while raising the levels of confidentiality, data integrity and privacy in the WMN. The idea is to achieve a multi-protocol and comprehensive security control solution in the WMN, having in mind some threats and attacks occur over different layers of the OSI layer modules simultaneously.

The limiting challenges in the MAC channel access-control, highlighted previously in this chapter and these security lapses in the routing protocol mechanism coupled with the open wireless, multi-hop security control and detection in the wireless mesh environment can be mitigated by the combination and integration of all the TE management security Model as shown in figure 4.3 and further linking them to web based-application security control like HTTPS. In IEEE 802.11s, the combination of multiple WLAN and ad hoc network systems in an easily increasing scalable and a heterogeneous multi-hop network forms the mesh architecture. The WMN security management can use a combination of trusted shared key and cryptography with intrusion detection to secure the network. The security design can apply firewall restrictions too, HTTPS especially for internet protocol and other inter-networking addressing while configuring wireless systems. In the IP controlled access security in WMN, access-list control, firewall, WEP and WPA has been used interchangeably and sometimes in combinations to secure wireless systems but we still observe security attacks and flaws in the routing and transmission of data packets. We also notice compromised data integrity and secured privacy invasion attacks in the WMN. We therefore analyze different securities threats and attacks using the proposed TE security management model shown in figure 4.3. The model mechanisms MPLS, MPLS-VPN and VPN-IPSec are implemented over WMN architecture using OPNET 14.5 Modeller in Section 4. We study the various levels of the security management model.

(A) MPLS-TE

Firstly, in figure 4.3 the multi-protocol security mechanism to various layer challenges in WMN is proposed as the comprehensive solution to WMN multiple layer security threats and multi-hops data traffic integrity and

availability. The MPLS mechanism, as shown in figure 4.4 offers one of the best TE security designs and technique for wireless mesh network in resolving security challenges. The MPLS is a switching technology which forward data packets through a network using label tagging attached to the headers of these forwarded packets through dedicated traffic paths. MPLS operates on layers 2 and 3 can sometimes traverse even the transport protocol layer. It is therefore a multi protocol switching data traffic technique.

The mechanism operates using labels attached or tagged, is analogous to a frame header encryption in other wireless transmission before the entry into the MPLS core network, modified as the packet traverses the network and these labelled tags are shed at the destination nodes of the network. The MPLS encapsulated data provides link authentication from infiltrating attacking nodes like in DoS attacks scenario and in security threats like wormhole, Grey-hole and Black-hole threats where network information access is compromised. DNS spoofing are also discouraged by the encapsulation of the IP header while in tag. Signal Jamming and message distortion of the data traffics blocked but unlike Frequency spread and block used in other wireless single-hop networks, the tunnel encapsulation provides authentication mechanism and protection for data in transmission. In the mesh network, the tags are removed as the packets exit the core network to the destination node. This equally provides inter-node updates verification and reliability.

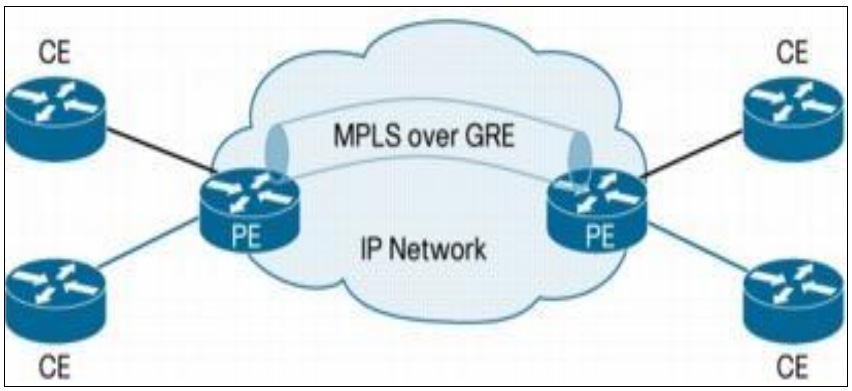


Figure 4.4: A simple MPLS mechanism in a wireless networks [160]

MPLS-TE software enabled an MPLS backbone operates over the mesh router backbone infrastructure to reproduce and increase the traffic engineering in campus WMN. On other hand, TE is an important security adaptation for internet provider and internet service provider (ISP) backbones. The infrastructure backbone's wireless mesh network must support multi-hop and dynamic traffic of high transmission capacity, and the networks must be very resilient to security threat, so that they can support WMN links or node failures in data traffic.

MPLS-TE equally provides an integrated security approach to traffic engineering especially in the routing operations of the WMN. TE optimizes the routing of IP traffic reliability and integrity, given the limitation imposed by backbone capacity and dynamic mesh network topology. MPLS-TE provides secured paths and encapsulated routed traffic flows over WMN based on the dynamic traffic flow and with the resources available in the network. MPLS also ensures priority traffic flows and efficient end- to-end transmission with high consideration given to bandwidth conservation which inadvertently controls bandwidth resource depletion attack threats through low bandwidth alerts. Route cache and table overflow attack and traffic flooding attacks threats which mostly deplete bandwidth availability can also be prevented by intrusion detection alerts and dynamic MPLS resolution control. MPLS-TE over WMN automatically adapts failed links and recovers dead nodes using the new routing limits and shortest path links updating.

WMN architecture connectivity is less expensive as access in Internet Service Provider (ISP) integrated infrastructure. MPLS-TE enables ISP‟s to route network traffic in a secured technique and provides effective and highly secured end-to-end transmission connectivity service to their users in low latency and less delay using throughput and delay as merit. In the TE technique, mesh routers see only a fully meshed virtual topology, making most destinations appear one-hop away. Therefore, authenticity of joining nodes and transmission links are verified by the use of the explicit Layer 2 transit layer gives you precise control over the ways in which traffic secures the available bandwidth. These provide counter security measures

to the threat for nodes and links infiltration based attacks like resource depletion, wormhole and Black-hole attacks.

With MPLS-TE, you do not have to manually configure the network devices to set up explicit routes. Instead, MPLS-TE mechanism relies on its coordinate functionality to enable the backbone topology and the automated signalling process. MPLS-TE accounts for link bandwidth and for the size of the traffic flow when determining explicit routes across the backbone. Furthermore, MPLS traffic engineering has a dynamic adaptation mechanism that provides a secure mechanism to TE in the WMN backbone. This mechanism enables the backbone routers to be more resilient to node and link failures during flooding attacks with faster recalculation of secure multi-paths. MPLS-TE provides a way to achieve the same TE benefits of secured multi-paths in the WMN architecture without having to run separate networks. The MPLS-TE mechanism does not encrypt data but relies on labelled tag on the IP data header which secures the integrity of the data packet while on transmission.

MPLS-TE automatically set up and maintains secure tunnel across the mesh router backbone infrastructure to the destination node. The traffic path used by the secure tunnel at any point in time is determined based on the tunnel resource requirements and network resources, such as bandwidth. WMN backbone resources are flooded via extensions to a secured link-state based Interior and (exterior) Gateways Protocol (IGP) but verified and authenticated for access control. The path tunnels provide encapsulation of traffic-data and secure path from interference. This filtering of data traffics and access control mitigate security threats like DNS spoofing, DDoS and Black-hole attacks. Unlike the distributed mesh security, the MPLS-TE generates its own paths for connectivity, authenticated access and verification in the WMN.

Tunnel paths are pre-determined and calculated at the tunnel head based on requirements between required and available resources and this eliminates the challenges of mismatch and packet sequence disorder. The

IGP automatically routes the traffic packets through these secured tunnels. Typically, a data packet from a WMN transmitting over the MPLS-TE backbone travels on a single tunnel which connects the ingress to the egress points of the MPLS. MPLS-TE operates on the principle of these IOS layer mechanisms: LSP tunnels are characterized by IOS tunnel interfaces, using configured destination, and are unidirectional paths.

- Link-state IGP for the global flooding of resource information, and extensions for the automatic routing of traffic onto TE LSP tunnels.
- The MPLS-TE path calculation mechanism that determines paths to use for LSP secures tunnels.
- MPLS-TE link management module that verifies and authenticates node link admission and accounting of the resource information to be flooded. (authentication of joining nodes in the wireless mesh infrastructure and accounting of the resources)
- Label switch path forwarding, which offers routers with a Layer 2-like ability to direct traffic across multiple hops wireless mesh networks as directed by the resource-based routing algorithm.

The routed paths are viewed as logical interfaces by the originating router and are mapped to the tunnel as secured paths. In the context of this document, these explicit routes are represented by LSP's and referred to as traffic engineering tunnels (TE-tunnels). The WMN are implemented and can install routes in the routing table that point to these TE-tunnels. In addition, these tunnels use explicit routes, and the path taken by a TE-tunnel is controlled by the router that is the head end of the tunnel. In the absence of faults, TE-tunnels are guaranteed not to loop, but routers must agree on how to implement the TE-tunnels or the traffic might loop through more than two tunnels.

The traffic engineering technique in IP multi-protocol routing provides a secure transmission of data- packets from source node to destination nodes in a WMN. The throughput and speed of convergence in TE has added

advantage compared to traditional routing protocol where a forward decision has to be made in every router or transceiver node and it is multi-protocol. Furthermore, security of the links and routed packets are more enhanced in TE mechanism due to the encapsulation of data packets as it traverses the links.

Moreover, MPLS-TE is easily interoperable in adapts to other network technologies and there is also the additional security option of virtual private network (VPN) core technique through the process of IP-TE segregation. Though recent findings have shown VPN security can be compromised by the security threats of integrity of the medium and confidentiality, the VPN-IPSec [34] in the MPLS domain technique gives an extra designed security which on properly configured, demonstrate a higher degree of protection.

The security threats in WMN-TE directed the research to other TE design solutions in WMN security. The security threats to TE based secured WMN as another traditional WLAN and ad hoc networks security has created new challenges as attackers develop more sophisticated techniques in breaching the integrity and protection of the WMN. In conventional IP enabled network routing, packets are routed through the best determined pathway to the destination node. The advertised routes and intermediate routers dynamically update and forward packets based on best route decision. However, in MPLS-TE technique, the MPLS network determines as to which route a packet go through to the destination nodes or routers therefore drop call, failed links and nodes can be avoided in the traffic transmission.

The packets are routed through the core MPLS network by the label edge router (LER). The packets on the same paths through an MPLS core network are called forward equivalence class (FEC). The best path determination decision of the MPLS on the forwarding packets is guided by the destination IP address, the port destination and destination interface. This is followed by the usual label tagging of the packet header between the IP header and the Ethernet frame header. The labels are mostly active

between two switching nodes and provide the best path to the destination through the MPLS core domain. The MPLS-TE allows traffic to be forwarded through the core to the destination node by simply labels look up and this represents a departure from the old traditional wireless routing mechanism of transmission of packets through the rigorous and high-processing routing table updates, best path determination and selection. High overheads security measures like encryption are not observed instead verification of joining nodes and traffic segregation with the VPN provides the access-control and privacy required in these WMN.

The potential security threats in MPLS-TE are analyzed and prevented by the mechanism. The threats are label information whereby the attacker can possibly use rogue path switching or rogue destination switching. In the rogue path switching, the attacker can maliciously use the label information to compromise the traffic engineering path by attaching rogue destination paths information before the label traffic switching. In the rogue destination switching, the attacker can maliciously use the label information to forward packets to a wrong destination and thereby compromise the integrity and reliability of the packets at the destination nodes. This circumvents the traffic segregation of the service provider to reach the server. In the acceptance of labelled packets from the outside MPLS core the attacker is able to enumerate the label and potentially threaten in two scenarios: either enumeration of label paths or enumeration of targets. The attacker can locate a targeted node like web server and using the port number to increment the target IP address number over significant time. In doing this the attacker uses forced label encoding and incremental forcing mechanism. In recording and updating the label paths, the attacker uses the knowledge of the targeted IP address and the labels for the LSP to reach its destination. A fixed IP address is used to send packets and the acknowledgement received. The main aim of the attacker is to get the replies information of either label path or targets.

Label information can be poisoned because they are not really authenticated and this means that an attacker can use the process of

MPLS accepting the LDP information from the outside core to manipulate the Label information base (LIB) of the MPLS devices. This technique can cause DoS and malicious collaborator security threats. In DoS, the attacker maliciously injects label paths into the networks to cause denial of service. While in the malicious collaborator, the attacker can poison the LIB of the MPLS domain. The attacker can change the LIB to have traffic forwarded to a specific device. This traffic can be captured and stored for later use. Finally, there is the threat of unauthorized access to the MPLS through the label edge routers (LER).

(B) MPLS-VPN

The second technique in the proposed security management model is the MPLS-VPN as shown in figure 4.3. It is widely acknowledged as the next generation traffic engineering and networking security technique. It combines the intelligence of multi-path routing with the layer 2 switching providing added advantage to the IP and other technologies. It is crucial for the establishment of scalable VPN delivering high end-to-end reliability and quality of service. The MPLS-VPN brings an added encrypting security technique lacking in MPLS and therefore complements the overall data packet integrity. The MPLS-VPN authentication and encrypting can be implemented in the peripherals and in mesh client nodes topological tables. The fast traffic reroutes and multi-path enhances and controls the bandwidth requirements in broadband and multimedia networks. It is potentially low-cost and interoperable. MPLS-VPN further offers a very high network security as a combined technique. It allows secured data and traffic paths to the peripherals and the mesh clients in the WMN. The MPLS- VPN uses its enterprise characteristics ability to perform route and traffic separation, route concealment and resistance to attacks. The VPN mechanism also uses the link and node encryption which MPLS lacks to complement a more effective security in WMN.

MPLS-VPN shares the same address space with other wireless networks without interfering network devices such as the MPLS core network and VPN. Furthermore, the data traffic from each VPN remains separate and

never accessing other VPN domain. VPN assigns and enable virtual routing and forwarding (VRF) commands and the edge router maintains a separate VRF for each VPN connection and this enhances security of the traffics and data consequently, there is no interference among the VPN's on the provide-edge router. It is also an important quality for remote access control and security in the network in a multi-hop enterprise environment. However, to enable routing separation across the core network in a MPLS-VPN scenario, to the providers edge router, VPN identifier are configured over multi-protocol border gateways (BGP) in the WMN domains. By offering this separation among addressing plans, routing and traffic, the MPLS-VPN creates a high security access-control of data packets to the MPLS core network as well as the VPN network. The mesh backbones VPN are resilient and it supports latency sensitive traffic too. This ensures lower drop calls and less packet drop in transmission. The reliability and integrity of the WMN communication is higher comparatively.

Another quality of this process is the concealment of the core network from outside potential attackers and this quality of the mechanism provides protection to the WMN. The MPLS network by its mechanism and configuration makes it difficult for a malicious attacker to send packets from outside to the core network such as in DDoS threats. It uses packet filtering mechanism and privacy protection of network information. Using a proper router configuration, the mechanism of signalling or by the attacker threatening edge routers can be blocked and secured. MPLS-VPN can prevent and resolve majority of the network layer attacks like spoofing and other attacks. MPLS-VPN can also adapt the IPSec security mechanism in the wireless multi-hop systems to provide a higher degree of security in critical networks. We used IPSec tunnelling in MPLS-VPN technique; the VPN brings an added encrypting security technique lacking in MPLS and therefore complements the overall data packet integrity. The VPN authentication and encrypting can be implemented in the peripherals and in mesh client nodes topological tables. This process entails high

overheads and IP configuration and addressing. The design method involves planned configuration of the IP address in the network.

(C) VPN-IPSec

The IPSec security mechanism in the figure 4.3, which is a resultant combination of VPN and IPSec in MPLS domain, provides a TE technique to managing authentication and data protection between multiple IP crypto mesh clients' node-peers engaging in secure data transfer. IPSec includes the Internet Security Association and Key Management Protocol (ISAKMP)/Oakley and two major sub-protocol of IPSec: Encapsulating Security Protocol (ESP) and Authentication Header (AH). VPN-IPSec uses symmetrical encryption algorithms for data protection. Symmetrical encryption algorithms are effective and easier to implement in hardware. Both algorithms offer a secure method of key exchange to ensure data protection and privacy using the Internet Key Exchange (IKE) ISAKMP/Oakley protocols. IKE uses a mathematical algorithm called a Diffie-Hellman exchange to create symmetrical session keys used by two crypto peers. IKE also controls the negotiation of the security limits for data traffic to be protected, the strength of the keys, the hash methods and traffic are protected from anti-replay.

VPN-IPSec proposed mechanism provides the required technique to securing voice packets from eavesdropping and modification. IPSec-VPN presents an option of configuration and indexes whereby the security levels can be raised or lowered the strength in different data protection. IPSec uses numerous Hash-Message Authentication Codes (HMAC) sets to select, for different levels of protection from attacks such as man-in-the-middle, packet replay (anti-replay), and data integrity attacks. An ISAKMP Security Agreement for two mesh clients to start a crypto is a single bi-directional secure negotiation channel used by both crypto peers to communicate important security parameters to each other, such as the security parameters for the IPSec Security Agreement (data tunnel). To implement a VPN technique with encryption, periodic changing of session encryption keys is necessary. Failure to change these keys makes the VPN

susceptible to brute force decryption attacks. IPSec solves the problem with the IKE protocol.

VPN-IPSec naturally offers a high degree of data privacy through establishment of trust points between communicating devices, and data encryption with the Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES) standard. IPSec are used to encrypt the WMN using WAN, IP VPN, or the Internet for connectivity. VPN-IPSec can be deployed across essentially any IP transport, including traditional WAN (such as FR, ATM), IP VPN, and Internet, integrated security services such as firewall can be applied in the WMN. Intrusion Prevention System (IPS) and DDoS prevention systems are resolved within the integrated VPN-IPSec design and it more frequent at the node peripherals. At IPSec headend locations, security functions have historically been distributed or dedicated devices. We deploy mesh routers and client nodes-acceleration for IPSec to minimize router- tables updates overhead, to support traffic with low-latency/jitter requirements, and for the best performance for overhead. Use digital certificates/PKI for scalable tunnel authentication. We can also set up QoS service policies, as appropriate, on head-end and branch router interfaces to help ensure performance of latency-sensitive applications. The in-built redundancy and failover with fast convergence with the fast source to destination convergence ensures high availability and resilience. Finally, IPSec-VPN ensures tunnelling without going through the gateway protocol.

4.5. Modelling, simulation environments and factors

Figure 4.5 shows the WMN model implemented in OPNET 14.5 Modeller for TE security. The model is adapted from the IEEE 802.11b/g based ad hoc network including the mesh mobile clients and static backbone mesh routers. The hierarchal architecture of the WMN was implemented using administrative domain (AD) cluster design. In the model, an IP router was

statically assigned as AP for each of the four WLAN nodes in the cluster while the rest of the nodes are enabled using random waypoint wireless model as mesh clients. In addition, the mesh routers with IP gateway functionalities were assigned as backbone routers. The ad hoc network security standard IEEE 802.11i was used for simulation due to the ongoing standardization of WMN security.

In the model, 18 traffics sources are assumed to have maximum mobile average speed of 3 m/s. 25 mesh IP gateway routers are placed in multiple AD of 60 nodes clients mesh. The IP nodes and routers exchange are secured by VPN encrypting technique while the backbone routers and AP are configured to use authentication for access-control. IPSec are also configured to secure the VPN tunnel and gateways router nodes. The TE security techniques namely IEEE 802.11i, MPLS, MPLS-VPN and VPN-IPSec, are modelled and simulated in the WMN model. MPLS-VPN is created in the traffic centre and configured in the mesh routers and clients of the WMN model.

The VPN is created in the IP configuration and dynamic assignment of node addresses in the network while the IPSec attributes are enabled in the advanced attributes and together with the IP routers gateway functionalities. The IPSec attributes are used to activate tunnelling in the VPN-IPSec models. These adaptations were enabled in the mesh client nodes of the WMN model. In addition, the IP gateway functionalities were enabled in the IPSec advanced attributes, mesh routers, AP for backbone route transmission and the inter domain communication.

The mobility scenario is based on the random waypoint model. Each node and mesh router starts its movement to a random destination with a random speed, V (uniformly distributed and not higher than Vmax where it is a subset of {0, 1, 2, 3}. We use a pause time of 15 seconds for another traffic transmission. We employed a constant bit rate (CBR) source for traffic scenario. The packets are 512 bytes length and are generated in 4 packets per second.

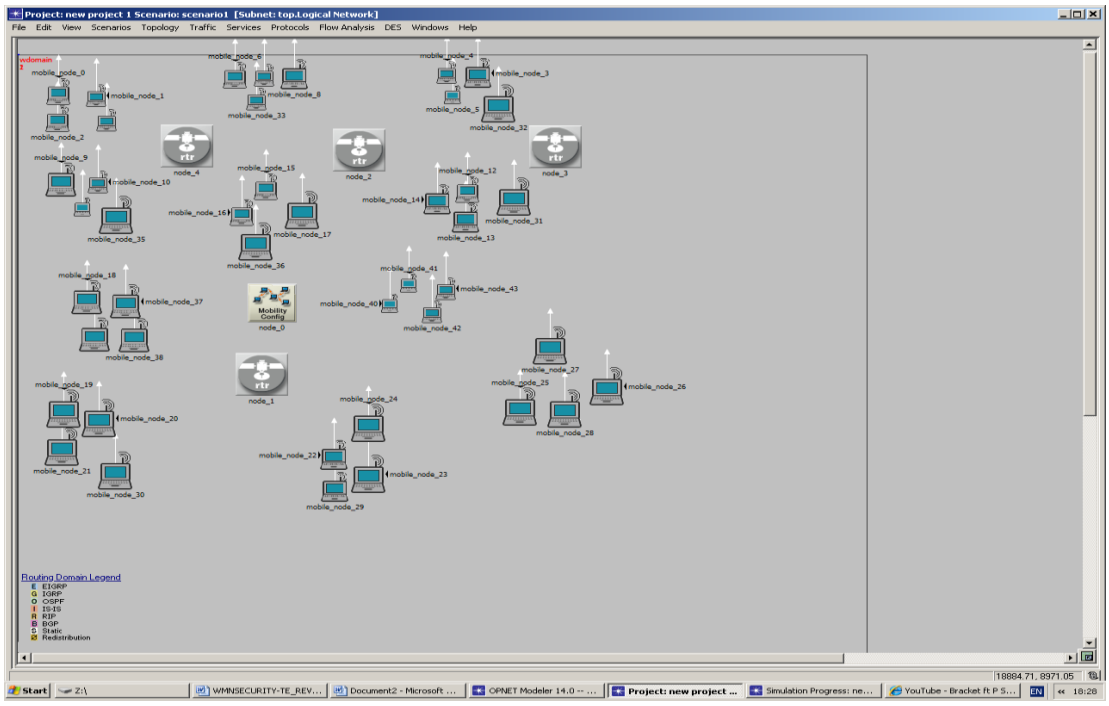


Figure 4.5: WMN model implemented in OPNET 14.5 Modeller for TE security simulation.

In the simulation, we investigated the influence of the TE security techniques on throughput, routing overhead, end to end delay, delivery ratio, traffic mobility, and traffic flooding attack (i.e. DDoS) by the rejection ratio, interference and failed nodes. The following metrics are used to measure the performance the TE security techniques:

- Packet delivery ratio (PDR) – defined as the ratio of the data packets received at the destination station compared to the total amount of data packets routed or transmitted by the source node.
- Average end-to-end delay – defined as the average time employed for a data packet to be delivered from the source node to the destination node
- Average throughput – defined as the sum of the data delivered to all the nodes in the network in a given time unit (seconds).

- Average traffic load – defined as the ratio of the data packets sent to the successfully received data packets.
- Average Hop-counts – defined as the overall hop-count for data packet from source node to destination node over a given unit time (seconds).
- Rejection ratio – This is quantity measures the ratio between the number of incoming bandwidth(in megabits) setup requests that are dropped (because a suitable tunnel could be found to route the request between an IE pair of nodes) and the total number of requests routed
- Topological density ratio – node density in an AD topological area.
- Interference – latency to transmission flow
- Accepted bandwidth – bandwidth utilized during transmission

4.51 *Simulation, evaluation and analysis*

In figure 4.6, the 802.11i performed worst and this can be attributed to the observed interference and drop packets in the wireless medium. The graph show a remarkable directly proportionality between the average throughput and the average number of hops in the WMN. The VPN-IPSec demonstrated higher packet traffics in the throughput compared to the MPLS and MPLS-VPN due to more effective cryptography, encryption and authentication of the tunnelled path in VPN the MPLS domain security of the packets and the separated and tunnelled-interference free route paths for the traffic packets. The graph depicts the higher number of hops as the throughput of a WMN increases. It shows an overall increase in packet traffic security in performance.

In figure 4.7, the data traffic routed per node is compared over an average traffic load in the WMN. The routing over head for VPN-IPSec is higher in IP configuration and computation. It draws considerably on network resources

and transmits lesser traffic load while the 802.11i shows a higher traffic load due to its simple security computation. It requires little or less overheads. The comparative TE security influence of interference and high processing mechanism lowers the traffic load in the WMN. The traffic load increased also result to slightly lower overhead in MPLS as an alternate secure path creates avenues for transmission in MPLS.

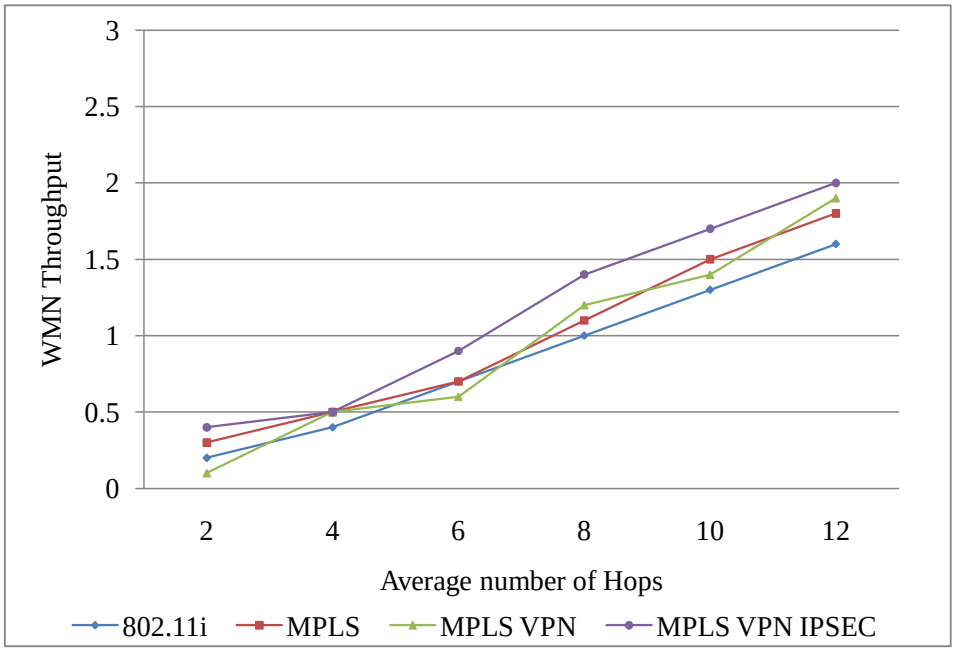


Figure 4.6: Influence of TE comparative security resolution in WMN throughput over multi-hop

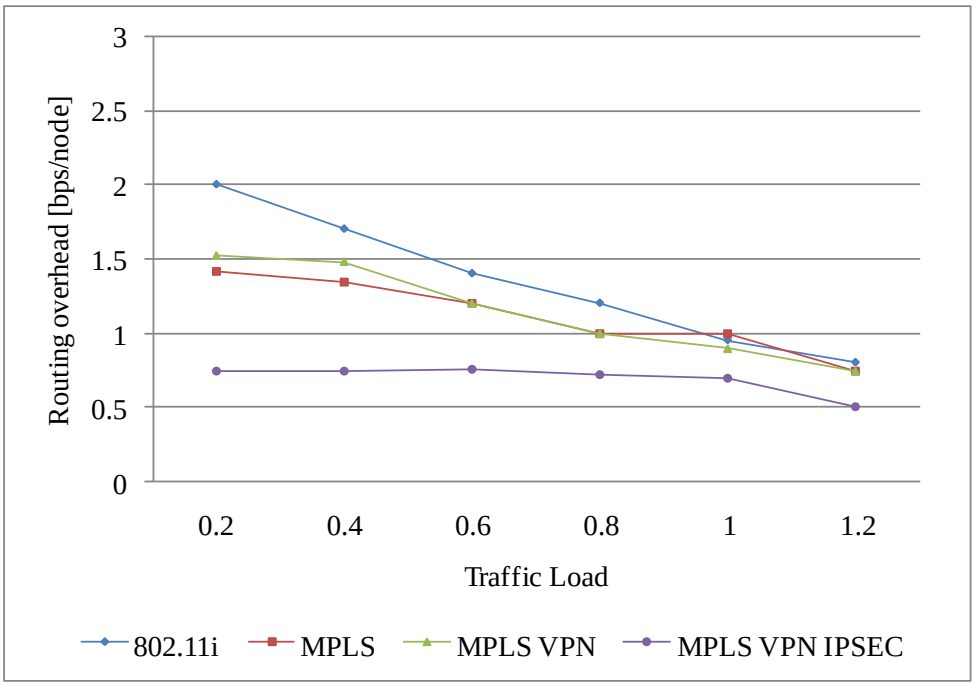


Figure 4.7: Influence of routing security overhead compared to the traffic load in the WMN

The end-to-end delay in the WMN was compared over traffic load as shown in figure 4.8, from the 18 traffic sources in the network. We observed, the higher the traffic load in the WMN, the lower the source to destination delay. These delays can be an attacker using a potential network slowing or deleting devices or mechanism. IP network spoofing, flooding and rush attacks in the routing layer of the WMN can influence these higher delays. The 802.11i experienced the worst delay as observed and have lower traffic load average compared to the other security mechanism. The high mobility of the routing nodes of the network creates a high demand for increase security measure to resolve the security threats.

In figure 4.9, the average delivery ratio was compared against the average hop count to observe the influence of the traffic transmission over multi-hop wireless mesh networks. The IPSec adapted MPLS- VPN security technique showed observed improvement on the security factor of multiple wireless nodes exchanging and traffic of packets data in a multi-hop environment. The delivery ratio increases with increase in the hops per packets in most of them but varies and showing a lesser extent in the

802.11i mechanism. This may be attributed to the absence of secure authentication and cryptography in the 802.11i mechanism unlike the rest. The VPN performed relatively closer giving an indication that encrypted authentication over WMN can influence positively on the lesser transmission delay. IPSec minimizes router-tables updates overhead, to support traffic with low-latency/jitter requirements, and for the highest performance for cost. This is reflected in figure 4.8.

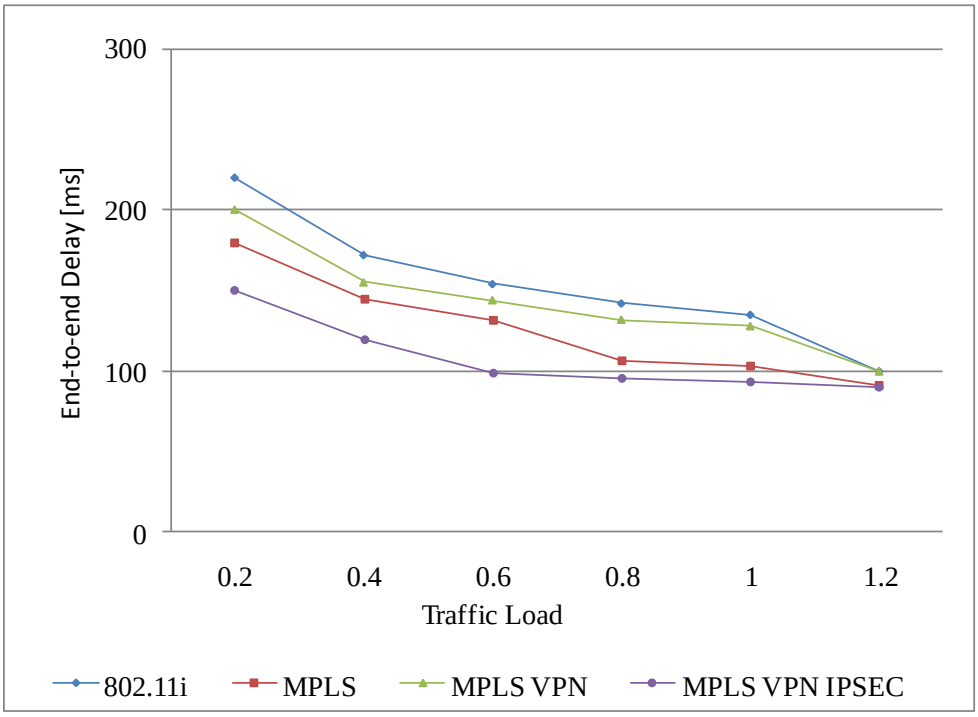


Figure 4.8: The influence of comparative TE security solution on end-to-end delay on traffic load.

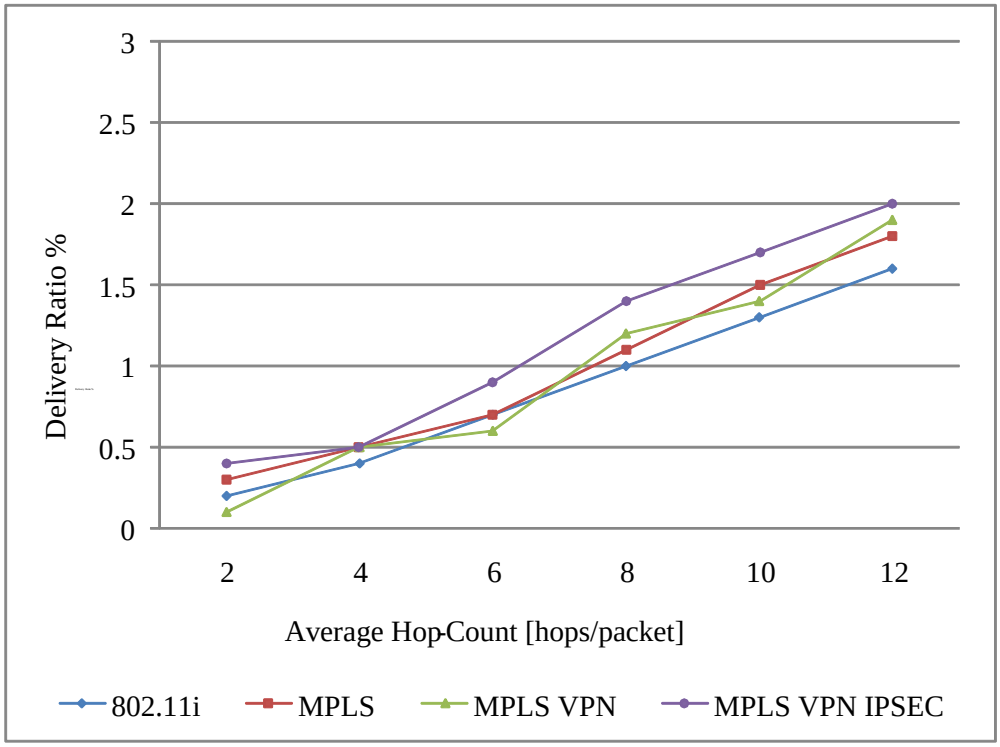


Figure 4.9: The comparative TE security resolution on the influence of the hop-count on the delivery ratio.

In figure 4.10, the traffic mobility increased with the average hop count. These accounts for the multi-hop and dynamic wireless mesh network architecture. The traffic mobility showed observed higher traffic mobility in a low-interference free medium such as VPN-IPSec. The MPLS and MPLS-VPN responded positively to the incremental rate of mobility in the WMN. The IDS system in the MPLS-VPN means that the technique did comparatively higher than the other two mechanisms. The mobility of a network and frequent topological changes makes security system very challenging.

In figure 4.11, the DDoS traffic engineering solutions are compared for effective resolution of traffic flooding attack effect on WMN bandwidth. As the reject ratio in the transmission increases, the bandwidth utilization of the WMN decreases. We look at the transmission in MPLS-TE as mostly the pathway between the ingress points to the egress point in the MPLS domain.

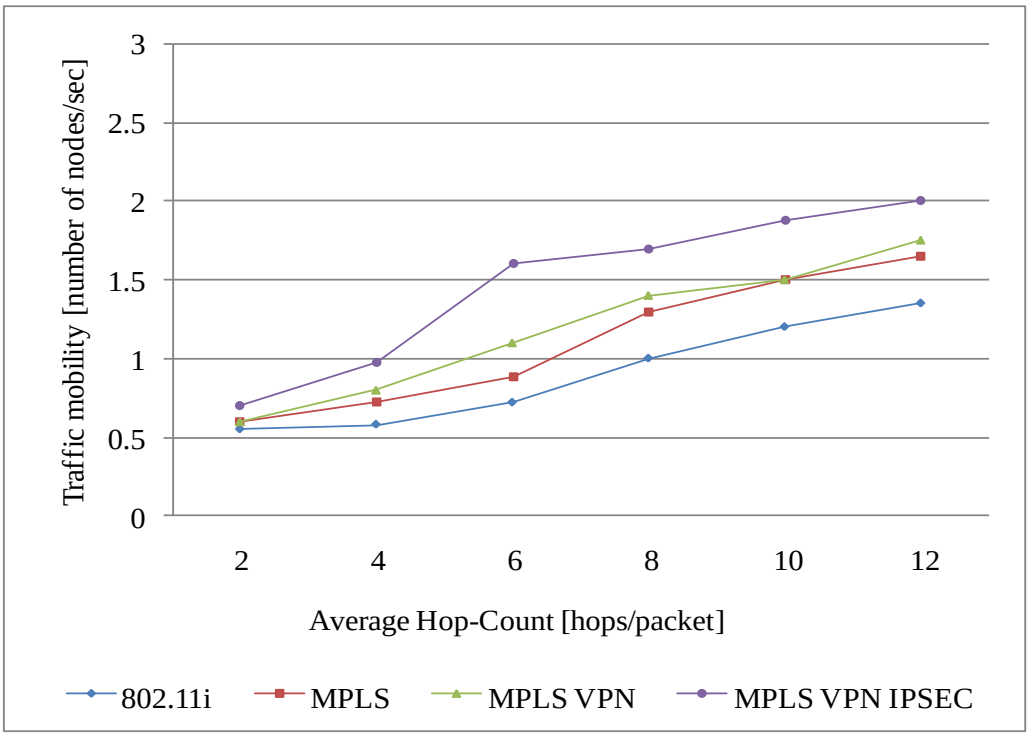


Figure 4.10: The comparatively TE security solution on influence of node mobility over multi-hop networks

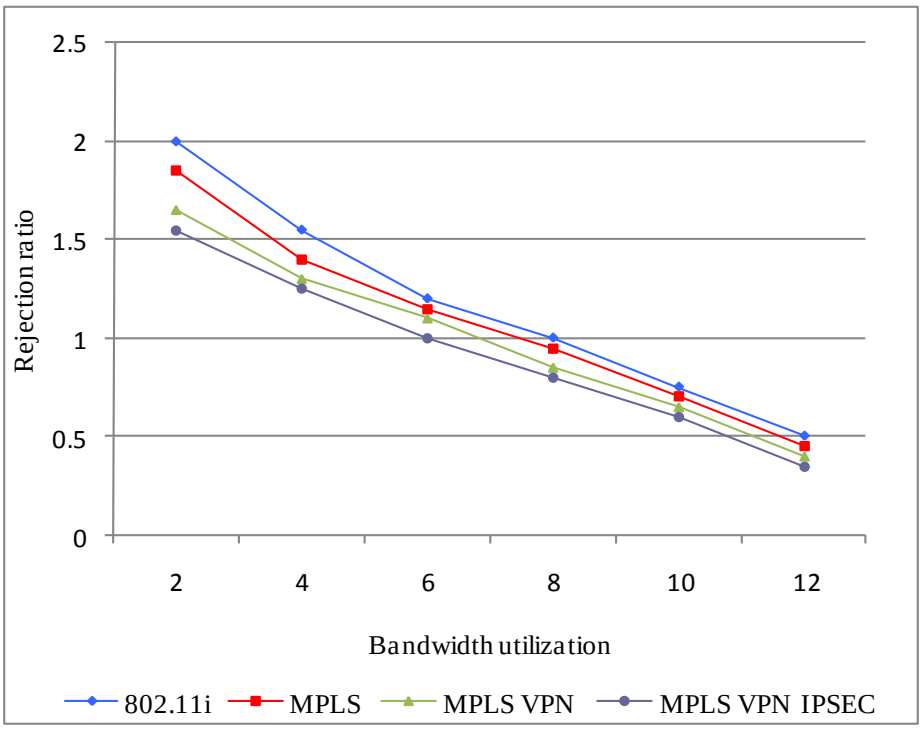


Figure 4.11: The influence of TE-security solution on traffic flooding attack (DDoS) on bandwidth.

The rejection ratio increase is directly proportional to the inverse of the bandwidth increase therefore, in IEEE802.11i which lacks encrypting technique on packet and node; it has the highest ratio in the four security techniques. The preventive mechanism of the protective authenticated path routes also contribute to this feature reflected in the graph. The MPL-VPN has the same encrypting technique in built in the VPN technology but it lacks the IPSec security adaptations and added flexibility of range in protecting the IP links and nodes (infrastructure). The MPLS security technique on its part offer authentication of access and provides a protected traffic path but lacks encrypting which we have noticed lowers effectively the DDoS. It completely lacks the IPSec cloud computing using IP gateway configuration command and access list and privilege login.

In figure 4.12, the comparative security techniques were applied in an interference traffic medium in the MPLS domain of the WMN. The performance of the security mechanism shows that the DDoS attack, using traffic flooding mechanism to depreciate the network availability and allowing the authenticated data traffic to flow from source to destination nodes, appreciates with comprehensive traffic engineering techniques like VPN-IPSec, unlike the MPLS-VPN which has similar mechanism but lacks the backbone IPSec secure transport mechanism or the loud computing ability of the IP gateway nodes which are primarily the backbone mesh networks in WMN. The rest performed averagely with interference decreasing the data traffic while in 802.11i, there is higher traffic processing.

In addition, the lack of encrypting with cryptography mechanism of the packet data and the Low mesh deterministic access due to contention lower the performance and affect the MPLS technique too in certain aspects. The intrusion prevention and DDoS security challenge is most comprehensively resolved by the protected paths of the MPLS mechanism and the encryption mechanism of the VPN.

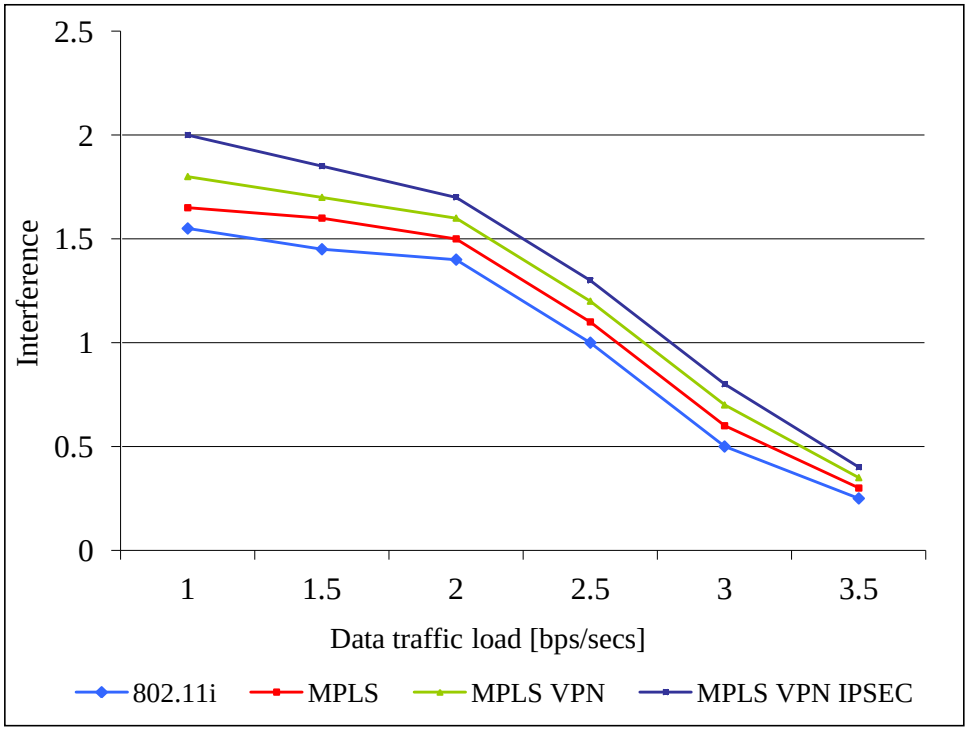


Figure 4.12: The influence of TE security on traffic flooding attack (DDoS) on interference

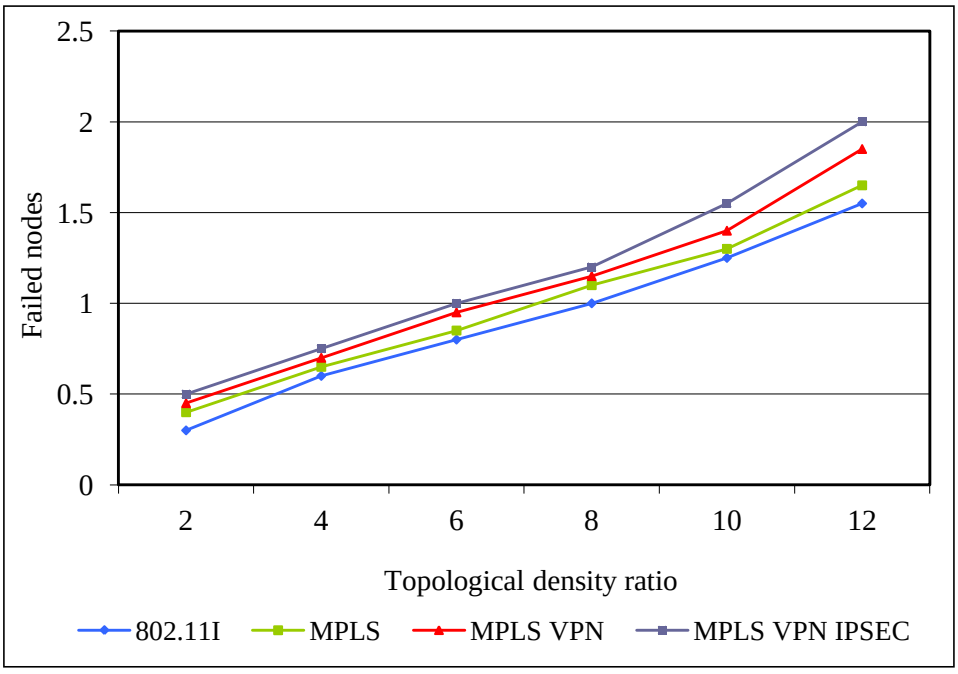


Figure 4.13: Influence of TE-security solution on multi-hop topological changes in traffic flooding attack

In figure 4.13, the failed nodes in the WMN increased with the rise in the scalability of the network resource availability. There is increasing number of nodes failures, in a topological dense location for the VPN-IPSec than the other security measures. We can explain this observation from the graph as due to the fact that we have more failures in the inter-node exchanges and peripheral transmission where the VPN-IPSec encryption is largely efficient but the other security measures acts more in the core areas and in the backbone routers and AP. The VPN-IPSec show more resilience and security in transmission of data packets. This security mechanism introduces the IP nodes and routers configuration and integration on MPLS and WMN. The flooding attack DDoS are mostly resolved using node authentication and encryption and sometimes cryptography of data packets to deny corruption or infiltration. The other techniques performed comparatively lower. This further strengthens the argument for a multiple security issues.

4.6. Conclusion

In the chapter we explored the security threats in WMN over a broadband network. Determination and investigation of the security solution using traffic engineering mechanism was explored. We tested the influence of security mechanisms over increased traffic loads and hop-count. Multi-layer comparative analysis with the traditional 802.11i was conducted a test for the observation of the influence of node mobility in a multi-hop scenario. Further evaluation was done on the network load influence, end-to-end traffic delays and delivery ratio in attack simulated scenarios. Observations of the technical advantages using a derived and adapted technique in traffic engineering were carried out. The proposed VPN-IPSec solution applied to the WMN security challenges and weakness showed enhanced overall performance. Severe security threats such as DDoS also showed comparatively more effective security resolution in WMN.

The proposed management model security technique demonstrated that a distributed security failure caused by traffic flooding, Grey-hole and Black-hole DDoS in WMN security can be prevented and resolved using VPN-IPSec. The security model showed efficient performance in intrusion detection and prevention mechanism too. Analysis of our investigation showed high performance in the different metrics used. In our analysis, we noticed that it will very hard to provide an effective security for multi-hopped wireless mesh network because of its inherent architectural weakness. However, we propose a mutual combination and use of cooperative IP communication security mechanisms in the prevention and defence of security threats and attacks in the WMN as shown by the IPSec and MPLS- VPN technique. The VPN-IPSec through authentication, encryption, cryptography and tunnelling and IP security configuration and operational mechanisms of the MPLS-TE lowers the overhead and processing of in the WMN. The improved VPN-IPSec integrates most the security measures needed to comprehensively secure both the data traffic and the infrastructure wireless mesh network.

CHAPTER 5

5.1 Conclusion

In this thesis, the aim of the contributions made is a measure of resolutions to some of the challenges of routing protocol in multi-hop wireless mesh networks and improvements to the scalability of increasing node campus meshed environment. In addition, more contributions were made in improving the security of wireless mesh transmission using traffic engineering management approach. The wireless mesh networks (WMN) is based on IEEE802.11 and 802.15 standards. The major research motivation for addressing these routing protocol and security challenges started from the literature review, which showed many open research challenges in the scalability, routing protocol and the security of WMN. These open research issues were properly evaluated and identification of improvement researches and works on these areas to further increase the performance and potentials of these factors were later carried out and explored. The traffic engineering technique over wireless mesh networks routing protocol was investigated and implemented using OPNET 16.0. The current study was reviewed and co-operative improvement using traffic engineering technique such as MPLS was applied for transmission optimization. Comparative performance analysis showed gain in multi path and scalability of using the mechanism in addition; employing our derived metrics TE optimization using enhanced djisktra's derived mathematical formulation showed enhanced performance compared to not using it.

This chapter is consist of two parts; a summary of research done in each chapter of the thesis and the possible future work in relation to the to the contributions in each chapter in order to make further extensions and hence create the possibilities of further performance improvements.

5.2 Summary of research

In summary, we surveyed and implemented a comprehensive, multi-protocol routing optimization using traffic engineered mechanism. This thesis is

organised as an organization of different contributions and journal in WMN routing protocol traffic engineering optimization.

Most future works on the this research will be focussed more on the implementation of hybrid TE techniques to enhance WMN routing protocol optimization especially with reference to challenging issues such as scalability over increasing large WAN, higher quality of service and packet delivery and more other cooperative mesh networking in IEEE802.11 technology engineering. We also expect more work on different TE routing optimization techniques and algorithms for further development of hybrid solutions. Adaptive routing metric are expected to be researched and developed for TE routing optimization. There are many open research areas in this work and there is expectation this research will open more constructive platform to developing solutions for these open research issues.

The proposed ALSTE-RP over wireless mesh network is expected to resolve many of the challenging issues in the WMN routing protocol such as scalability, interference, high overheads and processing gains. The inherent mapping in matrix characteristics of the TE technique improves the path diversity and connectivity of the WMN. The IP TE reduces the routing information messages and acknowledgements consequently improving the traffic load and overheads. The reliability of the transmitted packets are higher and more secured in TE techniques and analysis from the obtained results in the simulation test shows improvement in end to end delivery of data packet.

The proposed and developed ALSTE-RP will function effectively as access gateway routing and packet forwarding switching protocol in broadband community networks and in mesh healthcare network centres. It will bring a lot of advantages to real WAN networks and can be implemented over WMN in a cheap and simple adaptive method. The optimised algorithm through tested performance has shown improved performance in the routing protocol of WMN.

REFERENCES

[1] M. J. Lee, J. Zheng, Y.-B. Ko, and D. M. Shrestha, “Emerging Standards for Wireless Mesh Technology,” IEEE Wireless Communications, [see also IEEE Personal Communications], vol. 13, no. 2, pp. 56-63, 2006

[2] S Sesay**,** Z Yang**, “**A survey on mobile ad hoc wireless network” Information Technology Journal, 3 (2): 168-175, 2004 ISSN 1682-6027 © 2004.

[3] I.F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: A Survey,” Computer Networks, vol. 47, no. 4, pp. 445-487, March 2005.

[4] Bo Han, Weijia Jia and Lidong Lin “Performance evaluation of scheduling in IEEE 802.16 based wireless mesh networks”. Computer Communications Volume 30, Issue 4, 26 February 2007, Pages 782-792.

[5] Liang Dai, Yuan Xue, Bin Chang, Yanchuan Cao, Yi Cui (2008), Optimal Routing for Wireless Mesh Networks With Dynamic Traffic Demand *Mobile Networks and Applications* 13 (1-2) p. 97-116 http://www.springerlink.com/index/10.1007/s11036-008-0033-9

[6] S. Srivastava, A. Van de Liefvoort, and D. Medhi, “Traffic Engineering of MPLS Backbone Networks in the Presence of Heterogeneous Streams,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 53, no. 15, pp. 2688-2702, October 2009

[7] Aoun, Bassam, Boutaba, Raouf, Iraqi, Y, Kenward, G, “Gateway Placement Optimization in Wireless Mesh Networks With QoS Constraints”. IEEE Journal on Selected Areas in Communications vol 24 issue 11 pg 2127-2136 2006

[8] N. Wang, K. H. Ho, G. Pavlou, and M. Howarth, “An overview of routing optimization for internet traffic engineering,” *IEEE Commun. Surveys Tuts.*, vol. 10, no. 1, pp. 33–56, 2008

[9] J. Jun and M. L. Sichitiu, “MRP: Wireless Mesh Networks Routing Protocol,” Computer Communications, vol. 31, pp. 1413 – 1435, 2008.

[10] R. Bruno, M. Conti, and E. Gregori, “Mesh Networks: Commodity Multi-Hop Ad Hoc Networks,” IEEE Communications Magazine, vol. 43, no. 3, pp. 123-131, 2005.

[11] M. Bahr, J. Wang, and X. Jia, “Routing in Wireless Mesh Networks,” in Wireless Mesh Networking: Architectures, Protocols and Standards, Y. Zhang, J. Luo, and H. Hu, Eds.: Auerbach Publications, 2007.

[12] B. Li, Q. Zhang, J. Liu, C. Wang, X. Wang, and K. Farkas, “Advances in Wireless Mesh Networks,” ACM Journal on Mobile Networks and Applications, vol. 13, pp. 1-5, 2008.

[13] IEEE Standards, “IEEE 802.11TM Wireless Local Area Networks,” The Working Group for WLAN Standards, Ongoing.

[14] S. Roy, D. Koutsonikolas, S. Das, and Y. C. Hu, “High-Throughput Multicast Routing Metrics in Wireless Mesh Networks,” 26th IEEE International Conference on Distributed Computing Systems (ICDCS 2006), pp. 48- 48, 2006.

[15] A Baruch, H. David, and R. Herbert, “The Medium Time Metric: High Throughput Route Selection in Multi-Rate Ad Hoc Wireless Networks,” Mobile Networks and Applications, vol. 11, pp. 253-266, April 2006.

[16] C. E. Koksal and H. Balakrishnan, “Quality-Aware Routing Metrics for Time-Varying Wireless Mesh Networks,” IEEE Journal on Selected Areas in Communications, vol. 24, pp. 1984 - 1994, 2006.

[17] Q. Shen, X. Fang, and Y. Shan, “An Integrated Metrics Based Extended Dynamic Source Routing Protocol for Wireless Mesh Networks,” 2006 International Conference on Communications, Circuits and Systems Proceedings, vol. 3, pp. 1457-1461, 2006.

[18] D. Passos, D. Teixeira, D.C. Muchaluat-Saade, L.C. Schara Magalhes, and C. Albuquerque, “Mesh Network Performance Measurements,” In 5th International Information and Telecommunications Technologies Symposium, December 2006.

[19] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth, “On the Design and Implementation of Infrastructure Mesh Networks,” In Proceedings of the IEEE Workshop on Wireless Mesh Networks (WiMesh). IEEE Press, 2005.

[20] S. M. Faccin, C. Wijting, J. Kenckt, and A. Damle, “Mesh WLAN Networks: Concept and System Design,” IEEE Wireless Communications, [see also IEEE Personal Communications], vol. 13, no. 2, pp. 10-17, 2006.

[21] S. Waharte, R. Boutaba, Y. Iraqi, and B. Ishibashi, “Routing Protocols in Wireless Mesh Networks: Challenges and Design Considerations,” Multimedia Tools and Applications, vol. 29, pp. 285-303, 2006.

[22] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal, “Wireless Mesh Networks: Current Challenges and Future Directions of Web-In-The-Sky,” Wireless Communications, IEEE, vol. 14, pp. 79-89, 2007.

[23] Y. Chen, J. Chen, and Y. Yang, “Multi-hop delay performance in wireless mesh networks,” Mobile Networks and Applications vol. 13, pp. 160-168, April 2008.

[24] X. Wang and A. O. Lim, “IEEE 802.11s Wireless Mesh Networks: Framework and Challenges,” Ad Hoc Networks, vol. 6, no. 6, pp. 970-984, 2008.

[25] H. Li and M. Singhal, “A Scalable Routing Protocol for Ad Hoc Networks,” Proceedings of the 2005 IEEE 61st Vehicular Technology Conference (VTC 2005-Spring), vol. 4, pp. 2498-2503, May 2005.

[26] V. D. Park and M. S. Corson, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks,” Proceedings of the Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '97), vol. 3, pp. 1405-1413, April 1997.

[27] S.-J. Lee, W. Su, and M. Gerla, “On-Demand Multicast Routing Protocol in Multi-Hop Wireless Mobile Networks,” Mobile Networks and Applications, vol. 7, pp. 441-453, 2002.

[28] H. Jiang, W. Zhuang, X. Shen, A. Abdrabou, and P. Wang, “Differentiated Services For Wireless Mesh Backbone,” IEEE Communications Magazine, vol. 44, pp. 113-119, 2006.

[29] W-H. Tam and Y-C. Tseng, “Joint Multi-Channel Link Layer and Multi-Path Routing Design for Wireless Mesh Networks,” 26th IEEE International Conference on Computer Communications (INFOCOM 2007), pp. 2081-2089, May 2007.

[30] K. R. Chowdhury and I. F. Akyildiz, “Cognitive Wireless Mesh Networks with Dynamic Spectrum Access,” IEEE Journal on Selected Areas in Communications, vol. 26, pp. 168-181, January 2008.

[31] S. K. Das, B. S. B. S. Manoj, and C. S. R. Murthy, “A Dynamic Core Based Multicast Routing Protocol for Ad Hoc Wireless Networks,” in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking \&amp computing, Lausanne - Switzerland, 2002.

[32] T. B. Reddy, I. Karthigeyan, B.S. Manoj and C. S. R. Murthy, “Quality-of-Service Provisioning in Ad Hoc Wireless Networks: A Survey Of Issues And Solutions,” Journal of Ad Hoc Networks, vol. 4, no. 1, pp. 82–124, January 2006.

[33] C. E. Perkins and E. M. Royer, “Ad-Hoc On-Demand Distance Vector Routing,” Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 90-100, February 1999.

[34] T. Braun, M. Heissenbüttel, and T. Roth, “Performance of The Beacon-Less Routing Protocol In Realistic Scenarios,” Ad Hoc Networks, vol. 8, pp. 96-107, In Press.

[35] E. M. Belding-Royer and C. E. Perkins, “Evolution And Future Directions of The Ad Hoc On-Demand Distance-Vector Routing Protocol,” Ad Hoc Networks, vol. 1, pp. 125-150, 2003.

[36] H. A. Amri, M. Abolhasan, and T. Wysocki, “Scalability of MANET Routing Protocols for Heterogeneous And Homogenous Networks,” Computers & Electrical Engineering, In Press, Corrected Proof, January 2009.

[37] A. Boukerche, “Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks,” Mobile Networks and Applications, vol. 9, pp. 333-342, 2004.

[38] A. Divecha, A. Abraham, C. Grosan, and S. Sanyal, “Impact Of Node Mobility On MANET Routing Protocols Models,” Journal of Digital Information Management, February 2007.

[39] S. Corson and J. Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations: RFC Editor, 1999.

[40] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A Review Of Routing Protocols For Mobile Ad Hoc Networks,” Ad Hoc Networks, vol. 2, no. 1, pp. 1-22, January 2004.

[41] G. Pei, M. Gerla, and T.-W. Chen, “Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks,” 2000 IEEE International Conference in Communications, ICC 2000, vol. 1, pp. 70-74, 2000.

[42] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, “A Distance Routing Effect Algorithm for Mobility (DREAM),” in MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking. New York USA, ACM Press, pp. 76-84, 1998.

[43] G. Pei, M. Gerla, X. Hong, and C. Chiang, “A Wireless Hierarchical Routing Protocol With Group Mobility,” Wireless Communications and Networking Conference, 1999. WCNC 1999 IEEE, vol. 3, pp. 1538-1542, September 1999.

[44] J. J. Garcia-Luna-Aceves and M. Spohn, “Source-Tree Routing In Wireless Networks,” Proceedings of the Seventh International Conference on Network Protocols (ICNP '99), pp. 273-282, 1999.

[45] W. Liu, C. Chiang, H. Wu, and C. Gerla, “Routing In Clustered Multi-Hop Mobile Wireless Networks With Fading Channel,” in Proceedings of IEEE SICON'97, pp. 197-211, April 1997.

[46] I. Stojmenovic, “Location Updates for Efficient Routing in Ad Hoc Networks,” in Handbook of wireless networks and mobile computing: John Wiley & Sons, Inc., pp. 451-471, 2002.

[47] T-W. Chen and M. Gerla, “Global State Routing: A New Routing Scheme for Ad-Hoc Wireless Networks,” 1998 IEEE International Conference in Communications, ICC 98. Conference Record, vol. 1, pp. 171-175 vol.1, 1998.

[48] J. Raju and J. J. Garcia-Luna-Aceves, “A New Approach To On-Demand Loop-Free Multipath Routing,” Proceedings of the Eight International Conference on Computer Communications and Networks, pp. 522-527, 1999.

[49] V. Park and S. Corson, “Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification,” Internet-Draft, draft-ietf-manet-tora-spec-02.txt, October 1999.

[50] C.-K. Toh, “Associativity-Based Routing for Ad Hoc Mobile Networks,” Wireless Personal Communications, vol. 4, pp. 103-139, 1997.

[51] I. Bouazizi, “ARA - The Ant-Colony Based Routing Algorithm for MANETs,” in Proceedings of the 2002 International Conference on Parallel Processing Workshops: IEEE Computer Society, 2002.

[52] S. Bohacek, “Performance Improvements Provided by Route Diversity in Multi-Hop Wireless Networks,” IEEE Transactions on Mobile Computing, vol. 7, pp. 372-384, March 2008.

[53] V. Loscri, “A Routing Protocol for Wireless Mesh Networks,” Proceedings of the 2007 IEEE 66th Vehicular Technology Conference, (VTC-2007 fall), pp. 1523-1527, October 2007.

[54] D. Lin, T.-S. Moh, and M. Moh, “A Delay-Bounded Multi-Channel Routing Protocol For Wireless Mesh Networks Using Multiple Token Rings: Extended Summary,” Proceedings of the 2006 31st IEEE Conference on Local Computer Networks, pp. 845-847, November 2006.

[55] B -N. Cheng, M. Yuksel, and S. Kalyanaraman, “Orthogonal Rendezvous Routing Protocol For Wireless Mesh Networks,” IEEE/ACM Transactions on Networking (TON), vol. 17, pp.542-555, 2009.

[56] E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, “Simple Opportunistic Routing Protocol for Wireless Mesh Networks,” 2nd IEEE Workshop on Wireless Mesh Networks (WiMesh 2006), pp. 48-54, September 2008.

[57] Y. Huang and S. Bhatti, “Fast-Converging Distance Vector Routing for Wireless Mesh Networks,” in Proceedings of the 2008 the 28th International Conference on Distributed Computing Systems Workshops: IEEE Computer Society, pp. 279-284, 2008.

[58] A. N. Le, D.-W. Kum, S.-H. Lee, Y.-Z. Cho and I.-S. Lee, “Directional AODV Routing Protocol for Wireless Mesh Networks,” IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007 (PIMRC 2007), pp. 1-5, 2007.

[59] E. Baburaj and V. Vasudevan, “An Intelligent Mesh Based Multicast Routing Algorithm for MANETs using Particle Swarm Optimization,” International Journal of Computer Science and Network Security, vol. 8, pp. 214-218, May 2008.

[60] M. S. Siddiqui, S. O. Amin, J. H. Kim, and C. S. Hong, “MHRP: A Secure Multi-Path Hybrid Routing Protocol for Wireless Mesh Network,” Military Communications Conference (MILCOM 2007), IEEE, pp. 1-7, October 2007.

[61] R. Leung, J. Liu, E. Poon, A.-L. C. Chan, and B. Li, “MP-DSR: A QOS-Aware Multi-Path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks,” Proceedings of the 26th Annual IEEE Conference on Local Computer Networks (LCN 2001), pp. 132-141, 2001.

[62] M. K. Marina and S. R. Das, “On-Demand Multipath Distance Vector Routing In Ad Hoc Networks,” Ninth International Conference on Network Protocols, 2001, pp. 14-23, November 2001.

[63] S.-J. Lee and M. Gerla, “Split Multipath Routing With Maximally Disjoint Paths In Ad Hoc Networks,” IEEE International Conference on Communications, 2001 (ICC 2001), vol. 10, pp. 3201-3205, 2001.

[64] J. Tsai and T. Moors: “A Review of Multipath Routing Protocols: From Wireless Ad Hoc to Mesh Networks”, In Proceeding of ACoRN Early Career Researcher Workshop on Wireless Multi-Hop Networking, July 2006

[65] B. Hurley, C. Seidl, and W. Sewell, “A Survey of Dynamic Routing Methods for Circuit-Switched Traffic,” IEEE Communications Magazine, vol. 25, pp. 13-21, September 1987.

[66] B. Radunovic, C. Gkantsidis, P. Key, P. Rodriguez, and W. Hu, “An Optimization Framework For Practical Multipath Routing In Wireless Mesh Networks,” Microsoft Research, Technical Report, July 2007.

[67] M. R. Pearlman, Z. J. Haas, P. Sholander, and S. S. Tabrizi, “On The Impact Of Alternate Path Routing For Load Balancing in Mobile Ad Hoc Networks,” First Annual Workshop on Mobile and Ad Hoc Networking and Computing, 2000. (MobiHOC 2000), pp. 3-10, 2000.

[68] S. Ganguly, V. Navda, K. Kim, A. Kashyap, D. Niculescu, R. Izmailov, S. Hong, and S. R. Das, “Performance Optimizations for Deploying VoIP Services in Mesh Networks,” IEEE Journal on Selected Areas in Communications, vol. 24, pp. 2147-2158, 2006.

[69] P. Kyasanur and N. H. Vaidya, “Routing And Link-Layer Protocols For Multi-Channel Multi-Interface Ad Hoc Wireless Networks,” ACM SIGMOBILE Mobile Computing Communications Review, vol. 10, pp. 31-43, January 2006.

[70] D. Saha, S. Roy, S. Bandyopadhyay, B. Somprakash, T. Ueda, and S. Tanaka, “An Adaptive Framework for Multipath Routing via Maximally Zone-Disjoint Shortest Paths in Ad hoc Wireless Networks with Directional Antenna,” IEEE Global Telecommunications Conference, 2003.

[71] G. Li, L. Yang, W. S. Conner and B. Sadeghi, “Opportunities and Challenges in Mesh Networks Using Directional Antennas,” In Proceedings of WiMesh 2005, First IEEE Workshop on Wireless Mesh Networks, Santa Clara, CA, September 2005.

[72] D. Niculescu, S. Ganguly, K. Kim, and R. Izmailov, “Performance of VoIP in an 802.11 Wireless Mesh Network,” In Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM 2006), pp. 1-11, April 2006.

[73] A. Tsirigos and Z. J. Haas, “Multipath Routing In Mobile Ad Hoc Networks Or How To Route in The Presence Of Frequent Topology Changes,” Military Communications Conference, Communications for Network-Centric Operations: Creating the Information Force (MILCOM 2001), IEEE vol. 2, pp. 878-883, 2001.

[74] M. Oh, “An Adaptive Routing Algorithm for Wireless Mesh Networks,” in International Conference on Advanced Communication Technology (ICACT), pp. 2087-2091, 2008.

[75] J. Jaffe and F. Moss, “A Responsive Distributed Routing Algorithm for Computer Networks,” IEEE Transactions on Communications, vol. 30, pp. 1758-1762, 1982.

[76] V. D. Park and M. S. Corson, “A Highly Adaptive Distributed Routing Algorithm For Mobile Wireless Networks,” In Proceedings of the Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '97), vol. 3, pp. 1405-1413, April 1997.

[77] R. Draves, J. Padhye, and B. Zill, “Routing In Multi-Radio, Multi-Hop Wireless Mesh Networks,” in Proceedings of the 10th annual international conference on Mobile computing and networking Philadelphia, PA, USA: ACM, pp. 114-128, 2004.

[78] A. Raniwala and T. Chiueh, “Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network,” In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005), vol. 3, pp. 2223-2224, March 2005.

[79] T. Melodia, D. Pompili, and I. F. Akyildiz, “Optimal Local Topology Knowledge For Energy Efficient Geographical Routing In Sensor Networks,” Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004), vol. 3, pp. 1705-1716, March 2004.

[80] H. Frey, “Scalable Geographic Routing Algorithms for Wireless Ad Hoc Networks,” IEEE Network, vol. 18, pp. 18-22, 2004.

[81] D.S.J. De Couto and R. Morris, “Location Proxies and Intermediate Node Forwarding for Practical Geographic Forwarding,” Technical Report MIT-LCS-TR824, MIT Laboratory for Computer Science, June 2001.

[82] A. A. Pirzada, M. Portmann, and J. Indulska, “Performance Analysis Of Multi-Radio AODV In Hybrid Wireless Mesh Networks,” in Proceedings of the Eight International Conference on Computer Communications and Networks, 1999., vol. 31, pp. 885-895, March 2008.

[83] W. Al-Mandhari, K. Gyoda, and N. Nakajima, “Performance Evaluation Of Active Route Time-Out Parameter In Ad-Hoc On Demand Distance Vector (AODV),” in Proceedings of the 6th WSEAS International Conference on Applied Electromagnetic, Wireless and Optical Trondheim, Norway: World Scientific and Engineering Academy and Society (WSEAS), pp. 47-51, 2008.

[84] S.-J. Lee, E. M. Belding-Royer, and C. E. Perkins, “Scalability Study Of The Ad Hoc On-Demand Distance Vector Routing Protocol,” International Journal of Network Management, vol. 13, pp. 97-114, March 2003.

[85] M. Royer and C. E. Perkins, “An Implementation Study Of The AODV Routing Protocol,” in Proceedings of the IEEE Wireless Communications and Networking Conference, WCNC, pp. 1003-1008, 2000.

[86] C. Perkins, E. E. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) routing,” Internet RFCs, IETF RFC 3561, 2003.

[87] D. Chakeres and L. Klein-Berndt, “AODVjr, AODV simplified,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, pp. 100-101, July 2002.

[88] D.B. Johnson, D.A. Maltz, and J. Broch, “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks,”' Ad Hoc Networking, pp. 139–172, 2001.

[89] A. Mehdi and D. T. Mehdi, “Upgrading Performance of DSR Routing Protocol in Mobile Ad Hoc Networks,” in Proceedings of the World Academy of Science, Engineering and Technology, pp. 38-40, 2005.

[90] M. H. Lee and M. Sarahintu, “Performance Analysis of Dynamic Source Routing Protocol for Ad Hoc Networks Based on Taguchi’s Method,” Matematika, vol. 24, pp. 199-209, 2008.

[91] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” ACM SIGCOMM Computer Communication Review, vol. 24, pp. 234-244, October 1994.

[92] K. U. R. Khan, R. U. Zaman, A. V. Reddy, K. A. Reddy, and T. S. Harsha, “An Efficient DSDV Routing Protocol for Wireless Mobile Ad Hoc

Networks and its Performance Comparison," in Proceedings of the 2008 Second UKSIM European Symposium on Computer Modelling and Simulation: IEEE Computer Society, pp. 506-511, 2008.

[93] A. Zakrzewska, L. Koszalka, and I. Pozniak-Koszalka, "Performance Study of Routing Protocols for Wireless Mesh Networks," in 19th International Conference on Systems Engineering, 2008. (ICSENG '08), Las Vegas, NV, pp. 331-336, 2008.

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

[95] T. Clausen, "Optimized Link State Routing Protocol (OLSR) version 2," draft-clausen-manet-olsrv2-00, Internet draft, July 2005.

[96] M. Oh, "A Hybrid Routing Protocol For Wireless Mesh Networks," in 2008 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, pp. 1-5, 2008.

[97] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," IETF Internet Draft, RFC 4728, February 2007.

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

[99] J. Moy, "Open Shortest Path First Routing Protocol (OSPF Version 2)" IETF Internet Draft, RFC 2328, April 1998.

[100] G. Malkin, "The Routing Information Protocol (RIP version 2)" IETF Internet Draft, RFC 2453, November 1998.

[101] Z.J. Haas, M.R. Pearlman, “The Zone Routing Protocol for Ad Hoc Networks,” IETF Internet Draft, <draft-ietf-manet-zone-zrp-02.txt>, June 1999.

[102] IEEE 802.1 Standard Working Group, “IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control,” IEEE Standard 802.1X, November 2004.

[103] IEEE 802.1 Standard Working Group, “IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks,” IEEE Standard 802.1Q, December 2005.

[104] K. Murugan and S. Shanmugavel, “Traffic-Dependent and Energy-Based Time Delay Routing Algorithms for Improving Energy Efficiency in Mobile Ad Hoc Networks,” EURASIP Journal on Wireless Communications and Networking, vol. 5, no. 5, pp. 625-634, October 2005.

[105] I. Gojmerac, P. Reichl and L. Jansen, “Towards Low-Complexity Internet Traffic Engineering: The Adaptive Multi-Path Algorithm,” International Journal of Computer and Telecommunications Networking, vol.52, no. 15, pp. 2894-2907, October, 2008.

[106] K. N. Sridhar and L. Jacob, “Performance Evaluation and Enhancement of a Link Stability Based Routing Protocol for MANETs,” International Journal of High Performance Computing and Networking, vol.4, pp. 66-77, July 2006.

[107] G. Wang, Y. Ji, D. C. Marinescu and D. Turgut, “A Routing Protocol for Power Constrained Networks With Asymmetric Links,” In proceedings of the 1st ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, Venezia – Italy, October 2004.

[108] D. Li, X. Jia and H. Du, “QUOS - Topology Control for Non Homogenous Ad Hoc Wireless Networks,” EURASIP Journal on Wireless Communications and Networking, vol. 2006, no. 2, pp. 43, April 2006.

[109] S. Mudd, J. B. Garca, A. M. Fernandez, “Wireless Network Structure version 1.3”, 2002, http://www.wl0.org/~sjmudd/wireless/network-structure/english/article.pdf

[110] Wilibox (Wireless Linux in the Box) 2005–2009, http://www.wilibox.com/products/wili-mesh

[111] M. Burmester, T. V. Le, “Secure Multipath Communication in Mobile Ad hoc Networks,” International Conference on Information Technology: Coding and Computing (ITCC'04), Vol. 2, pp.405, 2004.

[112] M.S. Siddiqui, S.O. Amin, and C.S. Hong, “On a Low Security Overhead Mechanism for Secure Multi-path Routing Protocol in Wireless Mesh Network,” Proceedings of Asia-Pacific Network Operations and Management Symposium, pp. 466-475, 2007.

[113] J. He, M. Bresler, M. Chiang, and J. Rexford, “Towards Robust Multi-Layer Traffic Engineering: Optimization of Congestion Control and Routing,” IEEE Journal on Selected Areas in Communications, vol. 25, no. 5, pp. 868-880, June 2007.

[114] R. Boutaba, W. Szeto, and Y. Iraqi, “DORA: Efficient Routing for MPLS Traffic Engineering,” Journal of Network and Systems Management, vol. 10, no. 3, pp. 309-325, September 2002.

[115] C. T. Chou, “Traffic engineering for MPLS-based virtual private networks,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 44, no. 3, pp.319-333, February 2004.

[116] I. C.haieb, J-L. Le Roux, and B. Cousin, “A Routing Architecture for MPLS-TE Networks,” Proceedings of the fourth International Working Conference on Performance Modelling and Evaluation of Heterogeneous Networks (HET-NETs '06),
September 2006.

[117] O.E. Muogilim, K.K. Loo, R. Comley, “Wireless mesh network security: A traffic engineering management approach”, Elsevier Journal of Network and Computer Applications, 2010. (IN PRESS)

[118] D. Adami, R. G. Garroppo, S. Giordano, L. Tavanti, Multi-Constrained Path Computation Algorithms for Traffic Engineering over Wireless Mesh Networks, First IEEE WoWMoM Workshop on Hot Topics in Mesh Networking (HotMesh), Kos, 15-19 June 2009

[119] Hejiao Huang, Yun Peng (2008), Throughput Maximization with Traffic Profile in Wireless Mesh Network *Computing and Combinatorics* p. 531-540 2008

[120] S. Srivastava, A. Van de Liefvoort, and D. Medhi, “Traffic Engineering of MPLS Backbone Networks in the Presence of Heterogeneous Streams,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 53, no. 15, pp. 2688-2702, October 2009

[121] Weiyi Zhao, Jiang Xie (2010), Network Engineering and Traffic Forwarding (NETF): An Integrated Design for Inter-gateway QoS Handoffs in Infrastructure Wireless Mesh Networks *Communications Society.*

[122] Liang Dai, Yuan Xue, Bin Chang, Yanchuan Cao, Yi Cui (2008), Optimal Routing for Wireless Mesh Networks With Dynamic Traffic Demand *Mobile Networks and Applications* 13 (1-2) p. 97-116 http://www.springerlink.com/index/10.1007/s11036-008-0033-9

[123] R. Bhatia, M. Kodialam, and T.V. Lakshman,(2006) “Fast network re-optimization schemes for MPLS and optical networks,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 50, no. 2, pp. 317-331, February 2006

[124] Aoun, Bassam, Boutaba, Raouf, Iraqi, Y, Kenward, (2006) Gateway Placement Optimization in Wireless Mesh Networks with QoS Constraints. IEEE Journal on Selected Areas in Communications vol 24 issue 11 pg 2127-2136. 2006

[125] M.M. Sangsu, Jung, Dujeong, Lee, Kserawi, M, Rhee, J K K, Autonomous load balancing anycast routing protocol for wireless mesh networks, 2009 IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks Workshops pg 1-6.

[126] Bo Rong, Yi Qian, Kejie Lu, Rose Qingyang Hu, and Michel Kadoch, Multipath Routing over Wireless Mesh Networks for Multiple Description Video Transmission, *IEEE Journal on Selected Areas in Communications*, Vol.28, No.3, pp.321-331, April 2010.

[127] www.telecom-cloud.net/wp-content/uploads/2011

[128] www.IETF.org

[129] Community broadband (IEEE 802.16)

[130] Anand Prabhu Subramanian, Himanshu Gupta, Samir R. Das, and Jing Cao, “ Minimum Interference Channel Assignment in Multiradio Wireless Mesh Networks” IEEE Transactions on mobile Computing, VOL. 7, No. 11, November 2008

[131] I.F Akyildiz, X. Wang 2008, “Cross-layer design in wireless mesh networks” - IEEE Transactions on Vehicular Technology, 2008.

[132] K. Kar, M. Kodialam, and T.V. Lakshman, “Minimum Interference Routing of Bandwidth Guaranteed Tunnels with MPLS Traffic Engineering Applications,” IEEE J. Selected Areas in Comm., vol. 18, no. 12, pp. 2566-2579, Dec. 2000.

[133] S. Suri, M. Waldvogel, D. Bauer, and P.R. Warkhede, “Profile-Based Routing and Traffic Engineering,” Computer Comm., vol. 26, pp. 351-365, 2003.

[134] R. Boutaba, W. Szeto , Y. Iraqi, DORA: Efficient Routing for MPLS Traffic Engineering, Journal of Network and Systems Management, v.10 n.3, p.309-325, September 2002 [doi>10.1023/A:1019810526535].

[135] A. Vasilakos, M.P. Saltouros, A.F. Atlassis, and W. Pedrycz, “Optimizing QoS Routing in Hierarchical ATM Networks Using Computational Intelligence Techniques,” IEEE Trans. Systems, Man, and Cybernetics, Part C, vol. 33, no. 3, pp. 297-312, Aug. 2003.

[136] B. Wang, X. Su, and C.L.P. Chen, “A New Bandwidth Guaranteed Routing Algorithm for MPLS Traffic Engineering,” Proc. IEEE Int'l Conf. Comm. (ICC '02), pp. 1001-1005, 2002.

[137] R. Guerin, A. Orda, and D. Williams, “QoS Routing Mechanisms and OSPF Extensions,” Proc. Global Internet Miniconf., Nov. 1997.

[138] Z. Wang and J. Crowcroft, “Quality-of-Service Routing for Supporting Multimedia Applications,” IEEE J. Selected Areas in Comm., vol. 14, no. 7, pp. 1228-1234, Sept. 1996.

[139] B. John Oommen , Sudip Misra , Ole-Christoffer Granmo, Routing Bandwidth-Guaranteed Paths in MPLS Traffic Engineering: A Multiple Race Track Learning Approach, IEEE Transactions on Computers, v.56 n.7, p.959-976, July 2007 [doi>10.1109/TC.2007.1045]

[140] S. Jung et al., “Distributed potential field based routing and autonomous load balancing for wireless mesh networks,” IEEE Comm. Lett., Vol. 13(6), 2009, pp. 429-431.

[141] Pedro F. Felzenszwalb, Ramin Zabih, "Dynamic Programming and Graph Algorithms in Computer Vision," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 4, pp. 721-740, Apr. 2011, doi:10.1109/TPAMI.2010.135.

[142] Y. Chen, J. Chen, and Y. Yang, "Multi-Hop Delay Performance in Wireless Mesh Networks," Mobile Networks and Applications Vol. 13, April 2008, pp. 160-168.

[143] Wilibox (Wireless Linux in the Box) 2005 –2009, http://www.wilibox.com/products/wili-mesh

[144] D. Johnston, J. Walker, “Overview of IEEE 802.16 Security,” IEEE Security and Privacy, Vol. 2, No. 3, May 2004, pp. 40-48.

[145] G.R. Hiertz, S. Max, R. Zhao, D. Dee, L. Berlemann, “Principles of IEEE 802.11s”, in Proceedings of the 16th International Conference on Computer Communications and Networks (ICCCN), Honolulu, Hawaii, USA, Aug. 2007.

[146] M. Malekzadeh, A.A.A. Ghani, Z.A. Zulkarnain, Z. Muda, “Security Improvement for Management Frames in IEEE 802.11 Wireless Networks”, International Journal of Computer Science and Network Security, Vol. 7, No. 6, 2005, pp. 276-284.

[147] IEEE Standards, “IEEE 802.11i Standard”, IEEE Computer Society, July 2004

[148] K. Khan and M. Akbar, “Authentication in Multi- Hop Wireless Mesh Networks”, World Academy of Science and Technology, Vol. 22, 2006, pp. 100-105.

[149] X. Zheng, C. Chen C.-T. Huang, M. M. Matthews, N. Santhapuri, “A Dual Authentication Protocol for IEEE 802.11 Wireless LANs”, In Proceedings of the 2005 Second International Symposium of the Wireless Communications Systems, IEEE CS Press, 2005, pp. 565-569.

[150] N.B. Salem and J.P. Hubaux, “Securing Wireless Mesh Networks”, IEEE Wireless Communication, Vol. 13, No. 2, April 2006, pp. 50-55.

[151] N. Milanovic, M. Malek, A. Davidson and V. Milutinovic, “Routing and Security in Mobile Ad Hoc Networks”, Computer, IEEE Computer Magazine, 2004, Vol. 37, No. 2, February 2004, pp. 61-65.

[152] D. Kuhlman, R. Moriarty, T. Braskich, S. Emeott and M. Tripunitara, “A Proof of Security of a Mesh Security Architecture”, Technical Report 802.11-07/2436r0, IEEE Press, 2007.

[153] A.H. Lashkari, M.M.S. Danesh, B. Samadi, "A Survey on Wireless Security Protocols (WEP, WPA and WPA2/802.11i)," In Proceedings of the, 2009 Second IEEE International Conference on Computer Science and Information Technology (ICCSIT), August 2009, pp. 48-52.

[154] H.I. Bulbul, I. Batmaz and M. Ozel “Wireless Network Security: Comparison Of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols”, Wireless Communications and Mobile Computing Journal, Vol. 4, No. 8,20089, pp. 821-833.

[155] J. Sen, “A Survey on Wireless Sensor Network Security, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, August 2009, pp. 59-82.

[156] S. Suri, M. Waldvogel, D. Bauer, P.R. Warkhede, “Profile-Based Routing and Traffic Engineering”, Computer Communications, Vol. 26, No. 4, 2003, pp. 351-365.

[157] B. Wu, J. Chen, J. Wu and M. Cardei, “A Survey of Attacks and Countermeasures in Mobile Ad hoc Networks”, in Wireless Network Security, Y. Xiao, X. Shen, and D. Z Du, Springer, chapter 12, Network Theory and Applications, Vol. 17, 2006.

[158] M. Spainhower, J. Butts, D. Guernsey and S. Shenoi, Security Analysis of RSVP-TE Signalling in MPLS Networks", International Journal of Critical Infrastructure Protection, Vol. 1, December 2008, pp.68-74

[159] Y. Zhang, W. Lee and Y, Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", In ACM Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[160] R. Zhu and Y. Yang, "Model-Based Admission Control for IEEE 802.11e Enhanced Distributed Channel Access", AEU - International Journal of Electronics and Communications, Vol. 61, No. 6, June 2007, pp. 388-397.

[161] R. Rivest, "The MD 5 Message Digest Algorithm", IETFRFC 1321, April 1992.

[162] D.R. Raymond and S.F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defences," IEEE Security and Privacy, 2008, pp. 74-81.

[163] F. Xing and W. Wang, "Understanding Dynamic Denial of Service Attack in Mobile Ad Hoc Networks," IEEE Military Communication Conference (MILCOM), 2006

[164] K.M. Ali and T.J. Owens, "Selection of an EAP Authentication Method for a WLAN", International Journal of Information and Computer Security, Vol. 1, No. 1/2, 2007, pp. 210-233.

[165] A. Mishra and K. M. Nadkarni, "Security in Wireless Ad Hoc Networks", The Handbook Of Ad Hoc Wireless Networks, CRC Press, FL, 2003

[166] S. Capkun, J.P. Hubaux, and L. Buttyan, "Mobility Helps Peer-To-Peer Security" IEEE Transactions on Mobile Computing, Vol. 5, No. 1,

January 2006, pp. 43-51

[167] M. Parthasarathy: “Protocol For Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements”, IETF RFC 4016, March 2005.

[168] W.Liang and W. Wang “On Performance Analysis of Challenge / Response based Authentication in Wireless Networks", the International Journal of Computer and Telecommunications Networking, Vol. 48, No. 2, June 2005, pp. 267-288

[169] Y. Zhang, W. Lee and Y-A. Haung, “Intrusion Detection Techniques for Mobile Wireless Networks”, Wireless Network (ACM WINET), Vol. 9, No. 5, September 2003, pp. 545-556.

[170] Cisco, “Product support on 7600 and 6500 hardware series”, http://www.cisco.com.

[171] M. Naraghi-Pour and V. Desai, “Loop-Free Traffic Engineering with Path Protection in MPLS VPNs”, Computer Networks, Vol. 22, No. 12, August 2008, pp. 2360-2372.

[172] F. Palmieri, “VPN Scalability Over High Performance Backbones Evaluating MPLS VPN Against Traditional Approaches”, In Proceedings of the Eighth IEEE International Symposium on Computers and Communications (ISCC), Vol. 2, June-July 2003, pp. 975-981.