Aalto University
School of Electrical
Engineering

AALTO UNIVERSITY
School of Electrical Engineering
Department of Communications and Networking

Supreeth Herle

Topology Management for Wireless Mesh Self-Organizing Mobile Backhauls

Master's Thesis submitted in partial fulfillment of the degree of Master of Science in Technology

Espoo, March, 2015
Supervisor: Prof. Jukka Manner, Aalto University, Finland
Instructor: M. Sc. Pekka Wainio, Nokia Networks, Finland

AALTO UNIVERSITY **ABSTRACT OF THE MASTER'S THESIS**

Author:	Supreeth Herle	
Title of the Thesis:	Topology Management for Wireless Mesh Self-Organizing Mobile Backhauls	
Date:	03.03.2015	Number of pages: 14 + 97
Department:	Department of Communications and Networking	
Major:	Radio Communications	
Supervisor:	Prof. Jukka Manner, Aalto University, Finland	
Instructor:	M. Sc. Pekka Wainio, Nokia Networks, Finland	

The mobile data consumption is increasing exponentially, creating demand for more capacity from the network. Cell densification with small cells, also known as Heterogeneous networks, is seen as a solution for the capacity problem. On the downside, this creates a problem for providing a cost-effective backhaul connection to these small cells.

The Self-optimizing Wireless Mesh Network (SWMN) backhaul has been proposed as a backhaul solution for small cells. In SWMN, the nodes form a partial mesh topology, where routing and data transmission is based on pre-computed prioritized set of routes and link-schedules. Hence, an entity that handles topology management functionalities is required, which enables automatic network configuration, network monitoring, optimization and management.

The main aim of this thesis is to verify the topology management functionalities. The work involved development of a simulator for creating test topology scenarios. Additionally, the task involved verifying the feasibility of functionalities in the proof-of-concept system.

Keywords: *Topology Management, SON, Mobile backhaul,Wireless Mesh Network.*

Language: *English*

ACKNOWLEDGEMENTS

I wish to thank my thesis instructor M.Sc. (Tech.) Pekka Wainio and my thesis supervisor Professor Jukka Manner for the guidance and feedback throughout the course of thesis. I would also like to thank individually everyone from Nokia Networks and Technical Research Centre of Finland who contributed to the Self-optimizing Wireless Mesh Network backhaul concept and its implementation.

My sincere gratitude goes to David, Tapio and Jori for all the support during the validation of concepts. I am also grateful to Pradeep and Siddharth for reviewing the text.

Finally, I thank all the people in my life, friends and especially family for all the support and motivation!

Espoo, March 2015

Supreeth Herle

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

2G	Second Generation Mobile Network
3G	Third Generation Mobile Network
3GPP	Third Generation Partnership Project
4G	Fourth Generation Mobile Network
AAA	Authentication, Authorization and Accounting
AC	Attachment Circuit
ADAS	Advanced Driver Assistance Systems
ASIC	Application Specific Integrated Circuit
BM	Beam Forming
BS	Base Station
Capex	Capital expenditures
CDMA	Code Division Multiple Access
CN	Core Network
E2E	End-to-End
ECM	Energy saving Control Module
EDGE	Enhanced Data rates for GSM Evolution
eNodeB	Evolved Node B
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Network Gateway
EPS	Evolved Packet System
E-UTRAN	Evolved UTRAN
FCC	Federal Communications Commission
FDD	Frequency Division Duplexing
FDMA	Frequency Division Multiple Access
FLRR	Fast Local Re-Routing
FM	Frequency Modulation
GAN	Generic Access Network
GbE	Gigabit Ethernet

GGSN	Gateway GPRS Support Node
GN	Generic Node
GNID	Generic Node ID
GNSS	Global Navigational Satellite System
GPIO	General Purpose Input/ Output
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
GW	Gateway Node
HetNets	Heterogeneous Networks
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HSUPA	High Speed Uplink Packet Access
HWID	Hardware ID
IMLB	Inverse Multiplexed Load Balancing
IMS	IP Multimedia Service
IoT	Internet of Things
ITU	International Telecommunication Union
LOS	Line-of-Sight
LSTR	Local Spanning Tree Repair
LSU	Link Status Update
LTE	Long Term Evolution
LTE-A	LTE-Advanced
M2M	Machine-to-Machine
MAC	Media Access Control
MIMO	Multiple Input Multiple Output
mmWave	Millimeter wave
MPS	Multimedia Priority Service
MS	Mobile Station
MU-MIMO	Multi-User MIMO

NGMN	Next Generation Mobile Networks
NLOS	Non-Line-of-Sight
NMT	Nordic Mobile Telephones
NSM	Network Status Monitors
NTT	Nippon Telephone and Telegraph
OFDMA	Orthogonal Frequency Division Multiple Access
Opex	Operational expenditures
PCP	Priority code point
PCRF	Policy and Charging Control Function
PDH	Plesiochronous Digital Hierarchy
PDN	Packet Data Network
PE	Protocol Engine
P-GW	Packet Data Network Gateway
PoC	Proof-of-Concept
PTP	Precision Time Protocol
QAM	Quadrature Amplitude Modulation
QCI	Quality Class Indicators
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
SAE	System Architecture Evolution
SCF	Small Cell Forum
SC-FDMA	Single Carrier FDMA
SDH	Synchronous Digital Hierarchy
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SM	Spatial Multiplexing
SMS	Short Messaging Services
SON	Self-Organizing Network
SRVCC	Single Radio Voice Call Continuity

ST	Spanning Tree
SWMN	Self-optimizing Wireless Mesh Network
TACS	Total Access Communication System
TCP	Transmission Control Protocol
TCR	Topology Change Report
TDD	Time Division Duplexing
TDMA	Time Division Multiple Access
TMM	Topology Manager Module
TOM	Topology Optimizer Module
UMTS	Universal Mobile Terrestrial System
USB	Universal Serial Bus
UTRAN	UMTS Terrestrial Radio Network
VC	Virtual Connection
VLANID	Virtual Local Area Network ID
VoIP	Voice over IP
WCC	Wireless Mesh Network Centralized Controller
WCM	WMN Configurator Module
WFQ	Weighted Fair Queuing
WiMAX	Wireless Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WRR	Weighted Round Robin

1 INTRODUCTION

Mobile data consumption has been increasing exponentially over the last few years and this trend is set to continue for years to come. This would result in huge stress on the mobile networks to provide more capacity. Densification of the network by deploying small cells in a much greater magnitude than the existing macrocells tends to solve the capacity problem. But these base stations would have to be deployed across diverse locations with lack of existing backhaul infrastructure. Also, employing a wired backhaul requires cabling between cell sites. This results in increased installation costs and time taken for each small cell deployment. Hence, connecting these small cells with a scalable and cost-effective wireless backhaul transport becomes a major challenge. Additionally, increased number of base stations increases the network complexity. This in turn increases the difficulty of planning, controlling and optimizing the network operations for an operator in a cost-effective manner.

Self-Organizing Network (SON) is viewed as a viable technology by operators to minimize the operating cost and effort by automating the network design, build and operate phases. Therefore, there arises a need to study the topology management mechanisms which are responsible for automating the network deployment, network configuration, optimization and network operation.

Self-optimizing Wireless Mesh Network (SWMN) backhaul solution is being jointly developed by Nokia Networks and Valtion Tieteellinen Tutkimuskeskus (VTT) Technical Research Centre of Finland Ltd. In SWMN concept, computationally intense network topology optimizations are performed in a centralized entity, called as Wireless Mesh Network Controller. The main scope of this master's thesis is to build a simulator and proof-of-concept system to study, validate and develop the Wireless Mesh Network Controller.

1.1 Problem statement

The mobile broadband usage is increasing at very rapid pace, creating a capacity crisis for the operators (Cisco, Feb 2014) [**1**]. Densification of the mobile network by deploying more cells in a coverage area is the solution to increase capacity and offer better service. Traditionally, more macro cells were deployed to satisfy the capacity demand. But, this approach results in huge capital and operating costs. Therefore, Heterogeneous networks are used. These networks consists of a mix of cells types and radio technologies working together seamlessly in a given cell area [**2**].

Since the number of small cells required is in an order of magnitude greater than current number of macro cells, there arises a challenge for providing a high capacity, cost effective, scalable and easy to deploy backhaul solution. The typical wired backhaul solution such as optical fiber is not always feasible due to unconventional installation location of small cells. Therefore, wireless backhaul solutions such as point-to-point microwave and millimeter wave radios, which offer the deployment, cost and high capacity advantage, are generally used. Since the availability of line-of-sight in dense urban areas is scarce, a direct connection to a gateway is not always possible. This calls for a topology where the cell sites are connected in the form of mesh architecture with few hops to the gateway. The large scale deployment of small cells results in increased network complexity and requires a high degree of automated mechanisms to handle the topology configuration, optimization, operation, management and maintenance. In other words, the backhaul solution must implement self-organizing functionality to reduce the efforts and costs required for managing the topology.

A Self-optimizing Wireless Mesh Network (SWMN) with millimeter wave radios is a backhaul solution studied and developed jointly by Nokia Network and VTT. According to this concept, the architecture consists of networked wireless nodes that may be located in base stations, which are connected in a partial mesh using pencil beam millimeter wave links with built in self-healing, self-configuration and self-optimization mechanisms. These wireless nodes in the topology are managed by the Wireless Mesh Network Controller (WCC), which is mainly responsible for network monitoring, optimizing the network topology, calculating the route, link-schedule information, creating the network configuration and energy saving mechanisms. The WCC was developed alongside this thesis. Along with the development of WCC, thorough testing and verification of the topology management concepts were required.

1.2 Authors contribution and test result overview

The main aim of this master's thesis is to validate the topology management functions implemented in the WCC of the SWMN system mentioned in the previous section. The validation process involved development of a simulator with a graphical user interface, which provided the network scenarios to WCC. Additionally, thesis also includes planning and execution of validation scenarios to verify the topology management functions, demonstrate the concept and automation of some of testing processes.

The test scenarios covered the route computation, schedule computation, topology optimization, topology management, WMN configuration and virtual connection provisioning features implemented in the WCC. These scenarios included testing the autonomous network build, by node/link addition, by node/link removal and domain splitting and merging. In addition to these, the scalability of WCC was also tested. The execution of these scenarios also involved testing in the proof-of-concept demonstrator system with live traffic injected into network.

During the testing and verification, ample errors and inconsistencies were found in WCC and Wireless Mesh Network node algorithms. These findings and suggestions provided for improvements were used for enhancing and expanding the SWMN concept and its implementation towards a working product. Also, the simulator and the demonstrator platform performed satisfactorily during the validation process. However, the emulation platform had minor bugs in the initial stages of validation which required noticeable work during the debugging process, but the system was functional as soon as the bugs were resolved.

1.3 Structure

This master's thesis consists of five main chapters. Chapter 2 describes the growth trend in mobile traffic and the reasons behind such a tremendous growth. The way in which mobile networks have evolved over the years, to cater for this growth, is presented.

Chapter 3 introduces to the mobile backhaul and the need for more backhaul capacity. Traditional backhauling techniques used in mobile network are also described. Furthermore, the concept of small cells is introduced and the requirements for a small cell backhaul are presented. Then, commonly used small cell backhauling methods are discussed.

Chapter 4 presents an overview about the SWMN concepts, key functionalities and the key elements. Additionally, a detailed description of the topology management functions performed by the WMN controller (WCC) and its modules is presented.

In Chapter 5, detailed description and objectives of the validation scenarios along with the topology are presented. Also, the validation setups used while testing are discussed.

Chapter 6 explains the results of the validation and provides a brief reasoning on the obtained results. Additionally, a short discussion on the concept and future work is provided.

Finally, Chapter 7 provides a summary and conclusion to this master’s thesis.

2 MOBILE TRAFFIC AND NETWORK EVOLUTION

Access to internet has become a prerequisite for the current generation smart mobile devices. Availability of affordable smart mobile devices has led to the drastic rise in mobile traffic [**3**]. This in turn calls for a change in the mobile networks to handle the increasing mobile traffic and to provide better services. This chapter discusses about the changes undergone by the mobile traffic and also about the evolution of mobile networks. Section 2.1 presents a study about the current and future mobile traffic trends and how it has evolved over the years and also reasons behind such an evolution. Section 2.2 presents the earlier generation and present generation of mobile networks and also gives an insight on what is expected of the future mobile networks.

2.1 Mobile traffic evolution

Voice traffic has been part of mobile traffic since the advent of telecommunication system. But during the evolution of Second Generation of mobile networks (2G) systems, access to internet was also added. This gave rise to mobile data traffic [**3**]. Introduction of data services led to the widespread usage of mobile phones and demand for data and higher data speeds started growing. Higher data rates were offered in 3G (third generation of mobile networks) systems. This enabled high quality audio and video streaming along with the better quality of experience in accessing internet [**3**].

In December 2009, mobile data traffic overtook voice traffic [**4**]. And, by the end of 2013, the mobile data consumption per month reached 1.5 exabytes (1 exabyte = 10^{18} bytes) from 820 petabytes (1 petabyte = 10^{15} bytes) in the end of 2012, accounting for a total of 81% traffic growth in 2013 [**1**]. According to the forecast made by Ericsson, mobile data traffic will grow 10-fold from 1.1 exabytes per month in 2013 to 12 exabytes per month in 2019 [**5**]. Some of the major trends contributing to the growth of mobile data traffic are the increasing number of smart phones, tablets that have access to mobile networks, content being accessed over the internet and higher network speeds at an affordable price [**5**].

Mobile data traffic is transitioning from a simple web browsing data, emails and file sharing to a more composite data consisting of video, audio and social networking content.

Among these data types video is more dominating and this is due to the higher bit rates of video content than other data content types [**1**]. According to Cisco, video traffic is expected to increase 14-fold between 2013 and 2018 which would result in video being 69% of the mobile data traffic [**1**]. Figure 2.1 illustrates the growth of mobile traffic content from 2013 to 2019 [**5**].

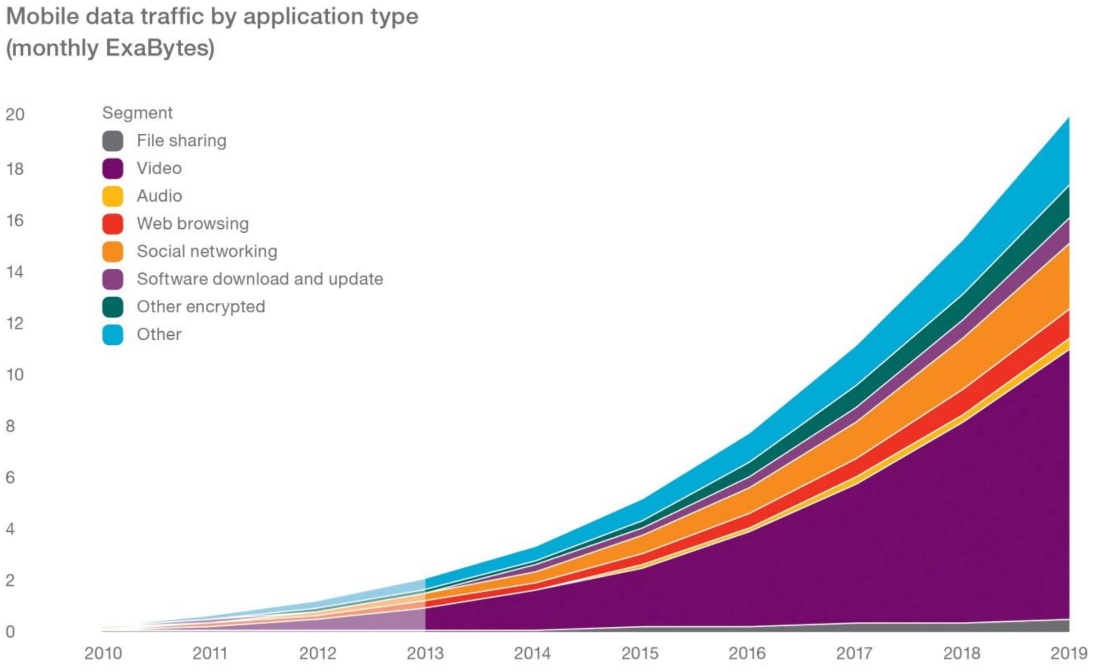


Figure 2.1: Forecast for different mobile data content by Ericsson [5**].**

One of the reasons behind this video dominance is due to the popularity of the cloud based applications and services such as YouTube, Spotify, Netflix, and Pandora. These applications contain unprecedented collection of high quality video/audio content enabling a mobile broadband user to access them anytime on their mobile device. Cloud based social applications such as Facebook, twitter and LinkedIn are major contributors for traffic generated through social networking. Social networking based traffic accounts for more than 10% of mobile traffic in 2013 and is the second largest traffic volume among the mobile data [**5**]. But this is only part of the story. Increase in the number of smart mobile devices such as Smart Phones, Tablets, Laptops and Machine-to-Machine (M2M) devices also play a crucial role in mobile traffic growth [**5**].

Smart phones and tablets usage is changing the internet access habits at a tremendous pace. These habits are so addictive that the smart phones are accessed almost constantly throughout the day. Due to this reason and availability of smart phones in lower price ranges, there has been a sharp rise in mobile device connections [**5**] [**1**]. Smart phones arrive in various form factors and increased capabilities every year. These factors also affect the data traffic generated per subscriber. For example, it is seen that smart phone user with bigger screen size spend more time streaming videos and playing games and thus consuming more data [**1**]. M2M subscriptions which are the key parts of Internet of Things (IoT) are expected to grow from 341 million to 2 billion in 2018 [**1**]. These devices collect data, process it and communicate with each other to stay connected. Similar to end-user mobile devices, M2M connections also have access to mobile broadband and are contributors to the mobile traffic growth.

The user base for Fourth generation of mobile networks (4G) subscriptions will reach 2.6 billion accounting for 30% of total mobile subscriptions by 2019 [**5**]. This transition emphasizes the demand for higher network speeds and better services from the operators. Thus the operators rely on the mobile networks to cater these needs of the customer.

Mobile networks play a key role in enabling all these technologies and to provide high quality user experience, as well as improved services. This calls for the mobile networks to evolve constantly according to the changing needs and demands. The details about previous and current generation mobile networks, followed by the overview of the next generation mobile networks are explained in following sections.

2.2 Mobile network evolution

Mobile network is a communication system that enables transfer of both data and voice by employing a radio network distributed over land areas called cells. Each of these cells is served by at least one fixed-location transceiver, known as cell site or Base Station (BS). When joined together these cells provide radio coverage over wide geographical area [**3**]. This enables a large number of portable transceivers, known as Mobile Stations (MS) to communicate with each other and fixed landline telephones anywhere in the network via base stations [**6**]. In addition to this global connectivity, mobile networks are also characterized by ubiquitous mobility, global roaming, trustworthy authentication, secure connection and global standards. Ubiquitous mobility refers to the ability to offer smooth continuity in communication when the user moves from one cell to another. This ability is enabled by handoff mechanism in mobile networks. Additionally, mobile networks provide secure connection through its authentication service [**6**].

The increase in mobile subscribers has resulted in need for more user capacity from mobile networks. One of the solutions to this growing demand is to reduce the cell sizes. Thus, the traditional macro cells which covered the entire geographical area with radius ranging from 1 to 20 km is also occupied by microcells and picocells, which have coverage areas from 400 m to 2 km and 4 to 200 m respectively. Femtocells, which have a range of 10 m, are used to improve the cellular performance within the buildings [**6**]. Figure 2.2 depicts the high level system architecture of mobile networks. Radio Access Network (RAN) handles all the radio related functionalities by providing a connection between the mobile station and the core network. Radio traffic to and from the mobile station is handled by the base stations.

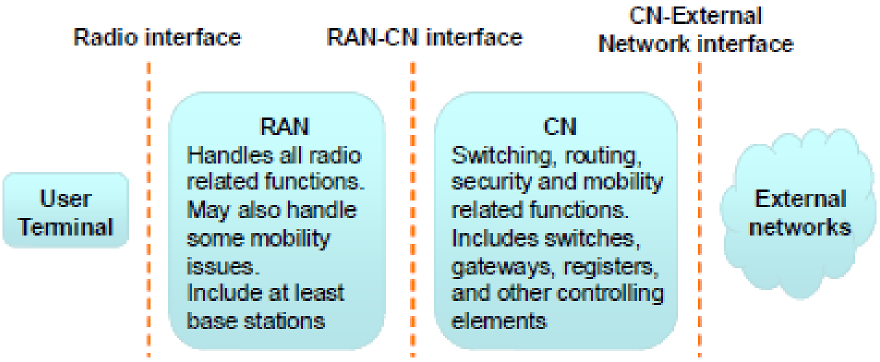

Radio interface
RAN-CN interface
CN-External Network interface
User Terminal
RAN
Handles all radio related functions. May also handle some mobility issues. Include at least base stations
CN
Switching, routing, security and mobility related functions. Includes switches, gateways, registers, and other controlling elements
External networks

Figure 2.2: General high level system architecture of mobile networks [7]

Core network (CN) is responsible for switching, routing calls, authentication, charging, operations and maintenance and data connections to external networks. The interfaces between RAN and CN constitute the backhaul in a mobile network [**8**].

First Generation Networks

Nippon Telephone and Telegraph (NTT), Nordic Mobile Telephones (NMT) and Total Access Communication Systems (TACS) are the most popular first generation mobile systems (1G) introduced in 1980. Analog Frequency Modulated (FM) wireless access using narrowband Frequency Division Multiple Access (FDMA) was the technology used in these mobile systems [**9**] [**10**]. These systems were allocated a 40 MHz bandwidth within the 800 to 900 MHz frequency range by the Federal Communications Commission (FCC) and had a channel spacing of 25-30 kHz [**9**]. Only a limited number of calls could be made at any given time due to the channel separation which resulted in inefficient utilization of the radio spectrum. Risks of eavesdropping and unencrypted communication are other drawbacks of first generation networks. These disadvantages formed the baseline for development of Second Generation mobile networks (2G) [**10**].

Second Generation Networks

The main characteristics of 2G mobile systems are digitization, encryption and compression of speech. These resulted in higher spectral efficiency and better services when compared to 1G mobile network systems [**10**] [**11**]. Second generation mobile networks uses digital multiple access technologies such as Time Division Multiple Access (TDMA) in Global System for Mobile Communication (GSM) and Code Division Multiple Access (CDMA) in IS-95 CDMA One [**10**] [**12**]. CDMA was deployed in United States, and the GSM technology was deployed as 2G standards in Europe, which led to a unified standard across Europe, thereby enabling seamless services such as international roaming. CDMA technology had greater network capacity than the GSM and TDMA based systems of 2G mobile systems and also provided superior voice quality with less background noise, enhanced security, fewer call drops and greater reliability [**13**] [**14**].

Initial GSM systems were capable of handling data rate up to 9.6 kbps generated from fax and Short Messaging Services (SMS) [**12**]. But this data rate was not sufficient for web browsing which led to the evolution of the GSM system to support packet data service in addition to traditional voice service leading to 2.5G mobile systems.

2.5G began with the introduction of General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE) that allowed sending of data over packet switched data networks via a separate connection from voice network. Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN) are the core network elements that facilitate packet switching in the GSM network. GPRS provides a theoretical maximum data rate of up to 171.2 kbps if all the 8 timeslots are used, this throughput was much higher than that of circuit switched data services on GSM [**13**] [**14**]. With the enhancements in the physical layer by adopting more sophisticated coding methods, the EDGE technology achieves speeds of up to 384 kbps [**12**].

2.2.1 Third generation networks

The three main reasons for the development of 3G systems are multimedia, higher link capacity and global standards. The data rate provided in 2G was far too low to experience the rich internet information. Hence there was a need for wide data-rate range from kbps to a couple of megabits per second. Next, with the rapid growth in the mobile communication, the issue of link capacity must also be addressed. Finally, establishing a global standard in a world where more and more people travel around is becoming very important, therefore International Telecommunication Union (ITU) defined International Mobile Telecommunications (IMT-2000) standard for 3G mobile networks [**9**]. 3GPP (3rd Generation Partnership Project) organization defined a mobile system called Universal Mobile Terrestrial System (UMTS) in Europe based on IMT-2000 standard. UMTS uses Wideband CDMA as the wireless access technology and employs a wider band than CDMA with a carrier bandwidth of 5 Mhz. Advantages of WCDMA are higher transfer speeds up to 2 Mbps, increased system capacity and communication quality by statistical multiplexing [**14**]. The standards released by 3GPP are grouped into releases, the first UMTS network with CDMA air-interface was specified in Release 99 [**15**]. Figure 2.3 shows the 3G architecture of UMTS mobile system.

The architecture of UMTS can be seen as an extension to GSM and GPRS. The main changes are in the radio access network part of the architecture. The access network in UMTS is called UMTS Terrestrial Radio Network (UTRAN). It consists of Node Bs and Radio Network Controllers (RNC). RNC is connected to multiple Node Bs, where each Node B is similar to BTS in the GSM network. RNC is equivalent to the BSC, but it also performs some of the functions of MSC such as management of radio resources. This is possible due to the connection between RNCs via Iur interface. As a result all the handover procedures are confined within UTRAN and unlike in 2G where handovers between BSC required intervention of core network. Another important design improvement in UMTS is that the core network and access network are separate and independent. This allows any RAN to connect to any UMTS core network via the Iu interface [**16**].

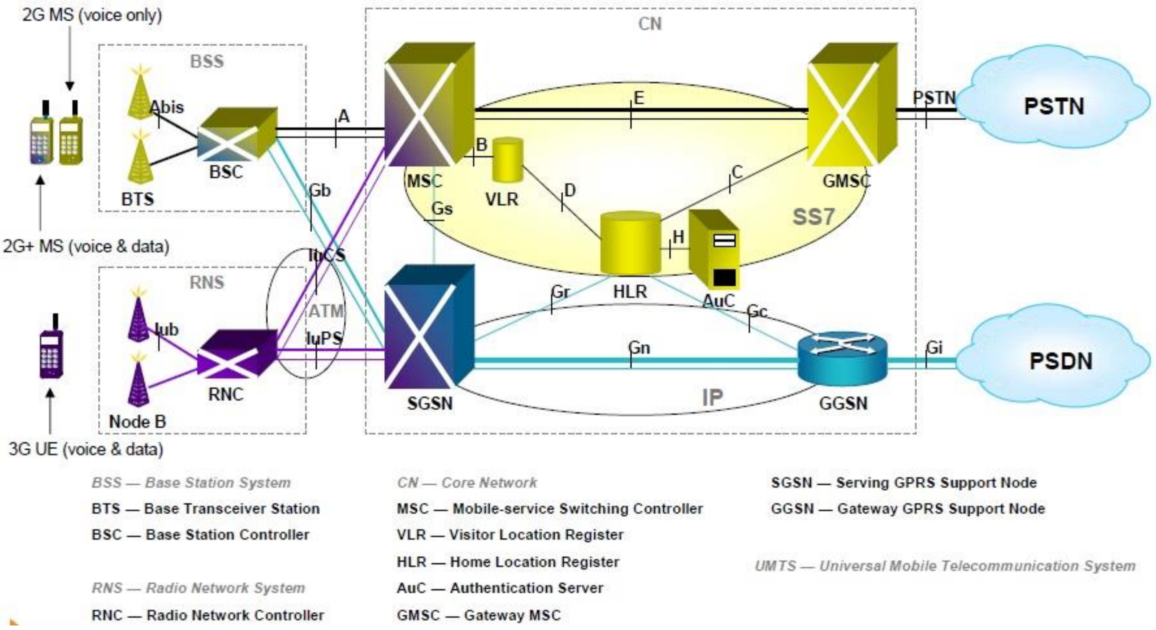

2G MS (voice only)
BSS
Abis
BTS
BSC
2G+ MS (voice & data)
RNS
Iub
Node B
RNC
3G UE (voice & data)
A
Gb
IuCS
ATM
IuPS
CN
MSC
B
VLR
D
Gs
E
C
GMSC
SS7
H
HLR
AuC
Gr
Gc
Gn
SGSN
IP
GGSN
PSTN
PSTN
Gi
PSDN
BSS — Base Station System
BTS — Base Transceiver Station
BSC — Base Station Controller
RNS — Radio Network System
RNC — Radio Network Controller
CN — Core Network
MSC — Mobile-service Switching Controller
VLR — Visitor Location Register
HLR — Home Location Register
AuC — Authentication Server
GMSC — Gateway MSC
SGSN — Serving GPRS Support Node
GGSN — Gateway GPRS Support Node
UMTS — Universal Mobile Telecommunication System

Figure 2.3: 3G architecture of UMTS (Release 99)

The 3GPP Release 99 helped in transitioning from the traditional 2G system to 3G systems by introducing new 3G radios. Meanwhile, features such as all-IP core network, virtualization of circuit switched network and packet switched voice service e.g. Voice over IP (VoIP) are the main highlights of the next release i.e. Release 4. Following this standard 3GPP Release 5 was defined. The features of this release are IP Multimedia Service (IMS) and HSDPA (High Speed Downlink Packet Access). The Release 6 added features such as High Speed Uplink Packet Access (HSUPA), Generic Access Network (GAN), integration of UMTS to wireless LAN networks and enhancements to IMS. High Speed Packet Access (HSPA), which is a combination of both HSDPA and HSUPA, provides data rates up to 14.4 Mbps in downlink and 5.8 in uplink [**10**] [**12**]. Finally in Release 7, 64 Quadrature Amplitude Modulation (QAM) and Multiple Input Multiple Output (MIMO) antennas were used in enhancement to HSPA, i.e. HSPA+. Other significant enhancements include continued packet connectivity to conserve MS battery, 16QAM for faster uplink in HSUPA and Quality of Service (QoS) improvements for VoIP applications. With each of the subsequent 3GPP releases there has been an improvement in terms of cell edge performance, system efficiencies, higher peak data rates and above all improved user experience. Release 8 defined the usage of dual-carrier HSDPA (2x10 MHz) with 64QAM or 64QAM with 2x2 MIMO and the Release 9 combined usage of the features in previous release, i.e. dual-carrier HSDPA plus the 64QAM and 2x2 MIMO for increased throughput up to 84 Mbps in downlink. Support for dual-carrier HSUPA was also added in Release 9. Throughputs were doubled in Release 10 with the usage of multi carrier (2x20 MHz) rather than dual-carrier defined in the previous release. With the continued improvements for HSPA+ in Release 11, the possible downlink throughput rates have once more doubled to 336 Mbps by employing 8 carrier HSDPA, 4x4 MIMO and 64QAM [**16**] [**17**].

2.2.2 Fourth generation networks

With the persistent increase in the capacity demand and the intensification of competition in mobile broadband market the ITU issued requirements for 4G mobile networks in IMT-Advanced standard [**13**]. The requirements are: operation in up-to 40 MHz radio channel with very high spectral efficiency of 15 bps/Hz, peak data rate of 1 Gbps for downlink and 500 Mbps for uplink, reduced latency, support vehicular speed mobility, backward compatibility and interoperability with legacy systems [**10**] [**12**]. 3GPP Release 8 defines the first system to meet the IMT-Advanced requirements for 4G, called Long Term Evolution (LTE). LTE redesigned the mobile network architecture by introducing the Evolved Packet System (EPS), consisting of new flat-IP core network called the Evolved Packet Core (EPC)/ System Architecture Evolution (SAE) coupled with the new air-interface. Advantages of the EPS include easy transition from 2G and 3G systems, integration of WLAN and WAN, wide range of QoS capabilities, advanced security and flexible roaming. Orthogonal Frequency Division Multiple Access (OFDMA) technique is used for downlink in LTE as it can achieve high data rates in high spectrum bandwidth. This in contrast to 3G systems with WCDMA required highly complex terminals in order to achieve 100 Mbps over higher bandwidth channels. OFDMA also allows LTE systems to support carrier bandwidths ranging from 1.4 MHz to 20 MHz. In uplink, LTE uses Single Carrier FDMA (SC-FDMA) to improve battery life of the handsets. New MIMO capabilities for LTE were also specified in Release 8 such as

Spatial Multiplexing (SM), Multi-User MIMO (MU-MIMO) and Beam Forming (BM). Other enhancements include voice call continuity between LTE-HSPA VoIP and CS domain called the Single Radio Voice Call Continuity (SRVCC), Common IMS and Multimedia Priority Service (MPS). Comprising of these enhancements, LTE is capable of peak data rates of 326 Mbps in downlink and 86.4 Mbps in uplink at 20 MHz bandwidth, supports both Frequency Division Duplexing (FDD) and Time Division Duplexing (TDD) and reduced round trip latency time up to 10 ms for data and less than 100 ms for signaling between the MS and base station [**10**] [**18**] [**19**].

Figure 2.4 illustrates the overall architecture of the LTE. LTE consists of two main networks namely E-UTRAN and EPC. EPC is a simplified and flat all-IP core network designed to provide lower latency, higher data–rates and for increased network scalability and efficiency. Although EPC shares some similarities with UMTS packet core network, EPC is a significant departure from the core networks of previous generation mobile systems.

The key components of EPC are Mobility Management Entity (MME), Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), Home Subscriber Server (HSS), Policy and Charging Control Function (PCRF) and Evolved Packet Data Network Gateway (ePDG). MME is a nodal element in LTE and performs signaling and control functions to manage connections between UE and network, terminal to network session handling, mobility management and controls radio access network elements. The primary functions of the S-GW are to manage user-plane mobility and act as demarcation point between the access network and the EPC. Similar to S-GW, P-GW is the termination point of the packet data interface towards the external Packet Data Network (PDN). P-GW also supports packet filtering, policy enforcement features and charging. HSS is the central database which holds the user subscription information and performs authentication, mobility management, session and call establishing functions. PCRF is a policy-based QoS control network element that supports service data flow detection, policy enforcement and flow based-charging. The ePDG is used for interworking with non-3GPP IP access networks [**10**] [**20**] [**21**].

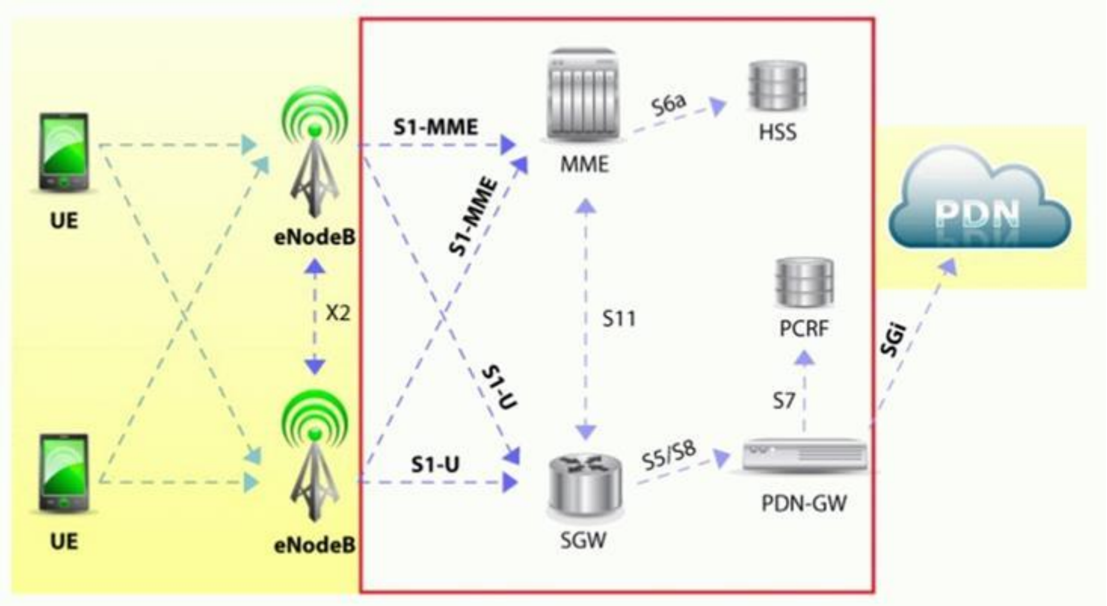


Figure 2.4: LTE network architecture

The access network of LTE known as Evolved UTRAN (E-UTRAN) consists of a network of enhanced base stations called the Evolved Node B (eNodeB). These eNodeBs are capable of communicating with each other via X2 interface, thus reducing burden on the core network. The eNodeB is responsible for radio resource management, IP header compression, data encryption and handover management between eNodeBs [**10**] [**18**].

Standard developments for LTE continued with Release 9, this includes introduction of LTE femtocell as home eNodeB to improve indoor coverage, Self-Organizing Network (SON) features e.g. optimizing the random access channel, evolved multimedia broadcast and multicast service and location services. The Release 10 focuses on the next generation of LTE called LTE-Advanced (LTE-A). The most significant features of Release 10 are data-rates of downlink up to 3 Gbps and 1.5 Gbps in uplink, carrier aggregation of up to 5 carriers to support 100 MHz bandwidth, 8X8 MIMO in downlink, 4X4 MIMO in uplink, relay nodes to support Heterogeneous Networks (HetNets) and enhanced inter-cell coordination to improve cell-edge performance. Further 3GPP releases mainly consist of enhancements to already existing capabilities and aim towards features to improve support for HetNets [**10**] [**22**].

2.2.3 Fifth generation networks

The industry has started laying the foundation for 5G with the world-wide deployment of 4G networks. 5G is associated with the enhancements to IMT-Advanced, initial requirements and standards for which are underway in the ITU. Some of the other standardizing bodies for 5G include the European Union's 5G PPP (5G Infrastructure Public-Private-Partnership), the Mobile and wireless communications Enablers for the Twenty-twenty Information Society Consortium (METIS) and Next Generation Mobile Networks (NGMN). The requirements that constitute 5G have not yet been defined but the capabilities and concepts expected from 5G systems are being discussed by the standardizing bodies.

Like 3G and 4G systems, 5G also focuses on system capacity increase and higher data rates. Additionally in 5G systems, wireless access must also be extended to any entity or machine that benefit from being connected. IoT is the term used for any object/machine that benefit from Internet access. The communication between these entities is referred as M2M [**23**]. The applications of IoT include smart cities, Advanced Driver Assistance Systems (ADAS) and autonomous vehicles in automobiles, telemedicine in the field of healthcare and also applications in the field of entertainment. These wide ranges of applications increase the number of connected devices that are predicted to reach 50 billion by 2020 [**24**]. As a result, the network must have high scalability and flexibility to handle all these devices. In addition to the tremendous increase in number of devices, media content such as 3D video, ultra-high-definition videos, gaming and augmented reality are becoming more popular [**1**] [**5**]. This type of multimedia services requires the network to provide higher bandwidth and reduced latency to have good user experience.

The above mentioned use cases and the demands are the guidelines for defining the requirements for 5G mobile systems. The guidelines include data rates of 10 Gbps or greater, latency less than 1 ms, use of higher frequencies (above 5 GHz up to the use of millimeter wave (mmWave) frequencies), usage of wider bandwidth of 1-2 GHz or greater, support for heterogeneous deployments and energy efficiency. This ensures good user-experience, real-time control of systems, ubiquitous connectivity, system scalability and uniform user experience across the coverage area [**23**] [**25**] [**26**].

The potential technologies to meet the demands and the requirements for 5G include massive MIMO, RAN transmission at centimeter and millimeter wave frequencies, multi Radio Access Technology (RAT) integration and management, ultra-dense networks, device-to-device communication, context aware networking and integration of wireless backhaul to access. The spectral efficiency can be greatly improved by using massive MIMO technique. This antenna technique enhances the multi-user MIMO technology by increasing the number of antennas on the base station to a value much greater than the number of users serviced at any given point of time and frequency. Radio transmissions in centimeter wavelength band (3 to 30 GHz) and millimeter wavelength band (30 to 300 GHz) benefit from the large amount of spectrum and large continuous spectrum chunks. The latter enables several Gigabits per seconds (Gbps) of data rates through wider transmission bandwidth. The path loss at higher frequencies can be reduced with use of smart beam-forming and reduced size of basic antenna elements. Integrating multi-RAT enables support for multiple radio access technologies in a geographical area. This also improves the user experience by switching between RATs in a seamless way. Densification of the macro network with small cell networks increases the system capacity, coverage and energy efficiency in the coverage area of macro base station. With the increased interest in small cell networks, wireless backhauls are being used where wired backhaul is not feasible. The solution of wireless backhauls operating in the spectrum above 6 GHz, including the millimeter wavelength band allows Gbps of transport capacity. Additionally, to have a unified wireless access solution, the backhaul and access (BS-UE) link are integrated and same set of radio access technologies can be used on both links. This configuration allows efficient use of technology, spectrum and improve overall quality and performance in end-to-end links [**23**] [**25**] [**26**] [**27**].

2.3 Summary

This section describes the rise in mobile traffic, especially mobile data. The reasons for such as exponential growth include the availability of smart phones, tablets and mobile broadband at an affordable price. Mobile networks have also undergone a series of evolution to meet the growth demand. The first generation of mobile networks introduced analog based communication, but, lacked system capacity. This led to second generation of mobile networks, which transitioned from analog to digital communication and had higher spectral efficiency than its previous generation networks. Also, mobile data was first supported in evolution of 2G (2.5G) networks by means of circuit switching, but the data rate was not sufficient. Therefore, in the third generation of mobile networks (3G), prominence was given to packet data and focus was to provide greater mobile data rate of several megabits per second. The 3G mobile networks were the first to introduce all-IP code network along with packet switched voice. With the advent of fourth generation of mobile networks (4G), the focus was not only to increase the mobile data rate but, also to provide Quality of Service to mobile subscribers. The mobile network architecture underwent a significant change during 4G with the introduction of flat all-IP network architecture, which provided higher data-rates, reduced the latency and increased the network scalability. Additionally, the concept of Heterogeneous networks was presented as a solution in 4G for the capacity problem, which involved densification of macro cell area with smaller cells. With the mass rollout of 4G networks, the industry is looking forward to lay down the foundation for the next generation of mobile networks. In addition to the increased data rates, the future networks will also focus on providing connectivity to any object that benefit from internet i.e. Internet of Things.

3 MOBILE BACKHAUL

The connections between radio access network and core network in a mobile network are called the mobile backhaul. It plays a crucial role in network performance and overall mobile network operation. Therefore, evolution of mobile backhaul becomes critical to cope with rapid growth in mobile data usage.

In this chapter, Section 3.1 provides a brief introduction to mobile backhaul and its role in a mobile network. Section 3.2 describes the legacy backhauling techniques and transition to packet-based backhauling techniques to achieve cost-effectiveness and higher data rates. Section 3.3 discusses about backhaul requirements to support small cell networks and the challenges involved in designing such a backhaul. Additionally, this section also describes the currently existing wireless small cell backhauling solutions. Finally, Section 3.4 describes the backhaul solution that is used as a baseline for this thesis.

3.1 Mobile backhaul overview

Radio access networks are evolving rapidly to keep up with traffic growth and needs of customers. These advanced radio access networks have resulted in significant increase in data rates over the air interface. The fixed core network has also undergone many improvements. However, mobile backhaul that serves as a transport medium between the mobile access network and the regional mobile controller site (BSC/RNC) or mobile packet core (MME/SGW/PGW) needs to catch up with all these enhancements on the rest of the network. Additionally, the need to support for legacy and next-generation technologies increases the design complexity and management costs of the network. Meanwhile, mobile operators look forward to increase average revenue per user while reducing the Capital and operational expenditures (Capex/Opex) by implementing a flexible architecture. Designing a backhaul network taking into account all these requirements has proven to be challenging. Figure 3.1 depicts a basic architecture of mobile backhaul in a mobile network. A typical backhaul network is usually divided into 3 domains: Access, Aggregation and Core. The domains are defined based on the network topology and technology used at the center and periphery of the backhaul network [**28**] [**29**] [**30**] [**31**].

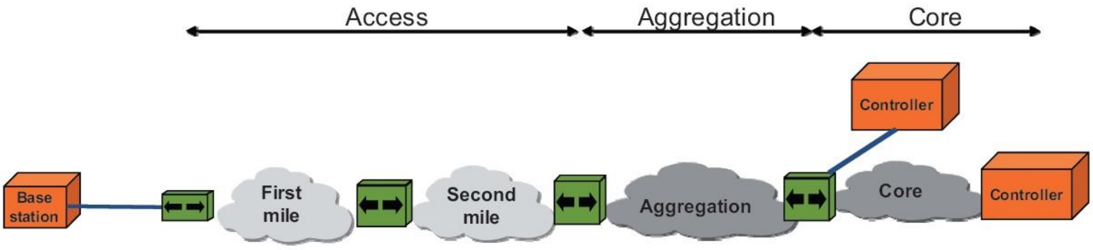


Figure 3.1: Basic architecture of mobile backhaul [31**].**

The backhaul access network provides connectivity between the base stations and the aggregation point. Considering the entire backhaul network, access network has very large number of links (number of BSs) with relatively low link capacities. This represents 70-80% of backhaul network costs and will tend to increase as the cell sizes reduce [**30**]. The type of physical topology used in backhaul access network is either tree or chain. Also, the connecting infrastructure can be microwave wireless links, optic fiber and copper cables. Selection of topology and the connecting infrastructure is based on the geographical location of cell site and bandwidth requirement. The aggregation network aggregates the traffic from the several access networks. This network terminates at the controller sites consisting of RNC or BSC and typically uses optical fibers connected in ring or meshes topologies. The cost and number of links of aggregation network is in between that of access and core network. The core network further connects aggregation network to other controller sites and the packet core network (EPC). This connection typically uses IP/MPLS routed network. The reason behind having ring or mesh topologies in layers above the access network is to support network resiliency feature in the events of failure. The number of links is the least in the core network but the links have very high capacities carrying traffic from both fixed and mobile networks. Since large volumes of traffic can be transferred over lesser infrastructure (links and nodes), the cost of core network is the least in the total backhaul costs [**30**] [**31**].

3.2 General Backhauling techniques

Many of the existing backhaul networks are hierarchical and implemented with legacy technologies that are incapable of supporting higher speeds and service requirements. These backhaul networks rely mainly on copper cables, optical fibers and microwave links as their physical medium for transmission. The wired backhaul solution such as copper cables and optical fibers are deployed in heavy traffic sites such as urban and sub-urban areas. But, microwave and satellite links are used in locations where wired infrastructure deployment is not possible [**32**]. Traditional mobile backhaul were based on T1/E1 circuit switching. This is due to the fact that 2G and 2.5G technologies were primarily designed for voice services and required guaranteed QoS, low latency, low jitter, timing and synchronization. Backhauls in these generations were based on TDM technology (Plesiochronous Digital Hierarchy (PDH) and Synchronous Digital Hierarchy (SDH)), with PDH offering very low capacity. In order to achieve greater capacity more T1 carriers needed to be used. But, the increase in number of T1 carriers is directly proportional to rice in backhaul cost. Additionally, the backhaul is not scalable due to the lack of support for bandwidth reuse and combining links. The problem of scalability was improved in 3G by using ATM or IP technology on top of SDH/PDH between the base station and the controller sites instead of TDM. In ATM, T3/E3 can be used in densely populated areas to handle more capacity while T1/E1 is used in less dense area. The ATM allowed reusing of bandwidth to achieve bit rates of 34 or 45, and 155 and 620 Mbps but added an additional network layer resulting in increased operational cost [**30**].

The introduction of 4G began the use of entirely IP based RAN architecture with IP packets carried over Ethernet. The main factors driving toward packet based backhaul network is the increasing cost of the backhaul, requirement for QoS based traffic priority, support for native packet traffic, requirement for lower network latency and simple or flat network architecture. Unlike traditional backhauling technologies, packet based backhaul solutions employ packet routers and switches for forwarding IP packets. These routers and switches are directly connected by physical layer connections such as optic fiber or microwave links. The technology and interface improvements in packet based connections allow higher cost efficiency and handling higher volumes of traffic in addition to simplified network architecture. Widespread usage of packet based backhaul networks was not possible due to the huge number of existing legacy backhauls servicing 2G and 3G users. But at present, new connections to base stations are predominantly deployed with packet-based technology over Ethernet [**28**] [**30**].

Microwave radio links are an alternate choice for wired backhaul and are deployed in geographically challenging areas where wired solutions are not economically or physically feasible. These wireless links are often used in access and aggregation tiers of backhaul and are operated in frequencies 6-38 GHz license bands and 2.5 and 5.8 GHz unlicensed bands.

Data rates that can be achieved by microwave links are in the range 4-32 Mbps in access tier and 140 Mbps in aggregation tier when operated in licensed bands [**30**]. Deploying microwave backhaul results in a high Capex due to equipment and spectrum licensing costs but these are compensated over time by lower operating expense when compared to T1/E1 copper links. The underlying transmission technique can be based on PDH, SDH or Ethernet when used along microwave radio links. Millimeter wave radio links are seen as potential backhaul solution to provide capacity ranging from 1 to 10 Gbps [**32**].

3.3 Small cell backhaul

Densification of the coverage area of existing macrocell base stations with small cells reduces the capacity bottleneck and improves radio coverage in access network. A small cell is a radio access network deployed and managed by the operators with coverage area less than the macrocell. The small cells are mainly characterized by small form factor base stations with low equipment and installation costs. The use cases include deployments to offload traffic from macrocells, enhance overall user experience, to provide connectivity to remote rural places and to improve the indoor coverage in shopping malls and apartments [**33**]. Figure 3.2 illustrates a typical scenario of small cell deployed to complement macrocells, thereby forming a heterogeneous network. Due to less coverage area of small cells, the number of small cells must be much greater than the number of macro cells. Increase in the number of small cells creates a challenge for providing a backhaul connection of sufficient capacity and QoS. In addition, small cells need to be deployed closer to users they serve which require base stations to be placed below the rooftops and on street lamps and other utility poles where conventional wired backhaul solutions are usually not feasible. In order to address all these challenges a wide range of backhaul solutions are being proposed and considered [**2**] [**33**]. However, the backhaul solution that would be employed differs for each of the deployment use cases.

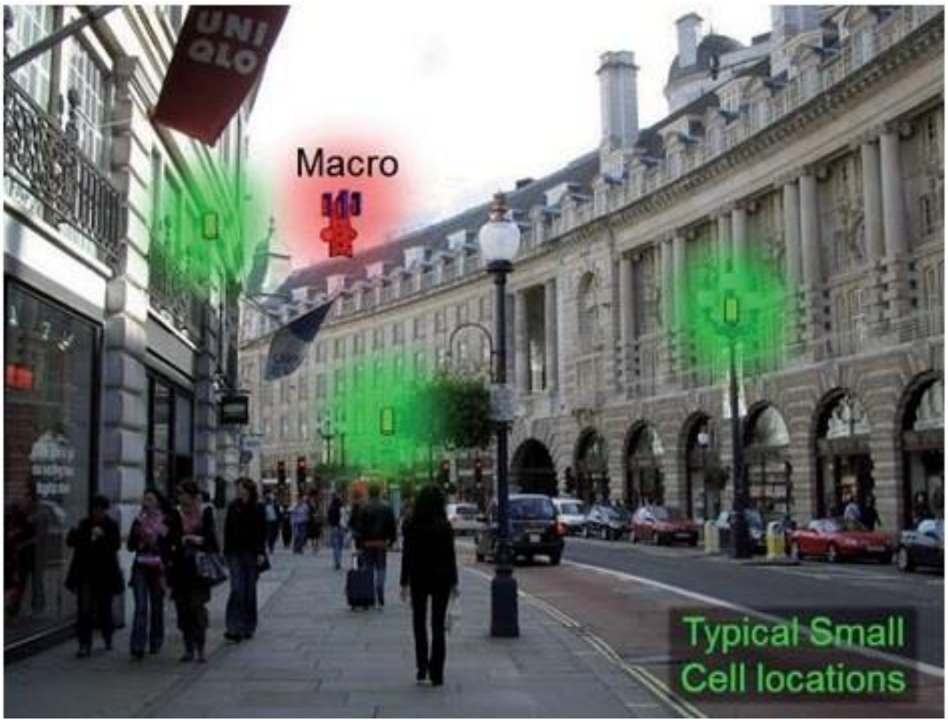


Figure 3.2: Small Cell deployment scenario [2].

3.3.1 Requirements and challenges

This section defines the requirements for a LTE small cell backhaul that are formulated by Next Generation Mobile Networks Alliance (NGMN) and Small Cell Forum (SCF). But the requirements for 5G small cells would be more stringent than that of LTE small cells. These requirements must be satisfied by a backhaul solution to be used to connect small cell networks to the core sites.

Backhaul coverage and connectivity

In the context of small cell backhaul access, backhaul coverage refers to the ability of the backhaul to provide connectivity to the deployed small cells and core network. These small cells are usually deployed outdoors 3-6 m above the street level, spaced 50-300 m apart from each other and must be within few meters (~10 m) of high demand or servicing location when used as hot-spot on demand. The challenge of coverage lies in the difficulty in connecting the street level small cells to the rooftop macrosites. In the case of wired backhaul solution, the backhaul needs to be below ground or within buildings resulting in high installation costs. On the other hand, for wireless backhauls, there is a high chance of non-availability of line of sight in dense urban areas due to obstruction caused by building or vehicles. This requires the wireless backhaul to implement multi-hop solutions to improve coverage [**2**] [**33**].

Throughput and capacity

An estimate of throughput requirement for small cell was given by NGMN by extending the simulation carried out to measure the variation in backhaul traffic from LTE base station to small cells [**34**]. The simulation considers user plane traffic generated during the quiet and busy times from a single LTE small cell site. Figure 3.3 shows the simulation results of backhaul traffic per small cell site.

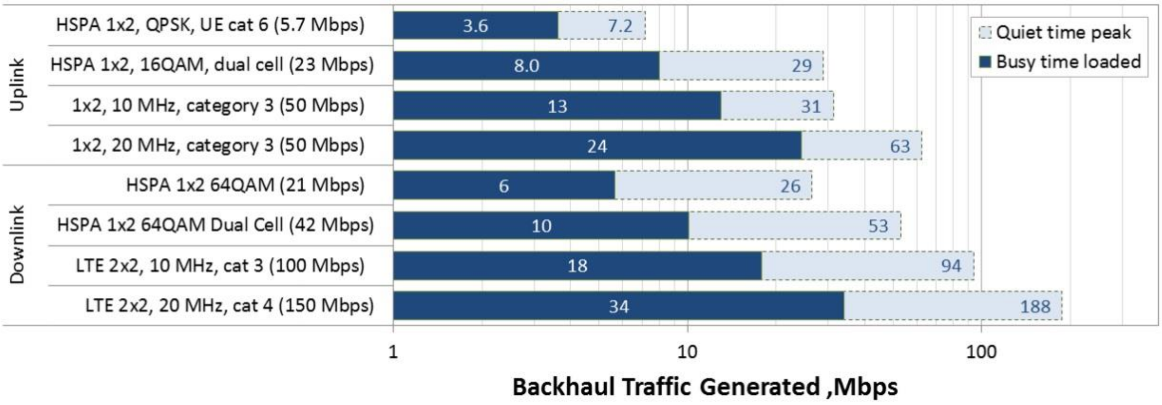


Figure 3.3: Backhaul traffic generated by HSPA and LTE small cell [2].

It can be observed from the simulation results that peak throughput rates from a single cell site are generated during quiet times i.e. when the base station is serving a single user with low cell interference and best signal conditions rather than fully loaded or busy times [**2**] [**33**]. The former case is more predominant in the case of small cells where the base stations are closer to users when compared to macrocells. But providing hundreds of Mbps capacity is not possible in all of the proposed backhaul solutions resulting in constrained backhaul approach. This approach reduces the achievable peak data but there is minimum impact on the user's Quality of Experience (QOE) since the user experiences data rates much higher than the rates during busy times. Further reduction in backhaul capacity would render addition of small cells useless [**35**]. Therefore, the backhaul must be designed based on the average traffic at busy times with a small margin for traffic variations [**33**].

Delay or latency

Latency plays a crucial role in QoE of users who have subscribed various services, and also limits the achievable throughput by the UE. With technologies beyond 4G focusing more on users QoE, 3GPP has recommended minimum acceptable one-way packet delays between UE and PGW for various services represented by Quality Class Indicators (QCIs) to label traffic priorities. The service with most aggressive delay requirement is gaming with 50ms and other real-time service such as voice and IMS signaling with 100 ms delay requirement [**36**]. However, these values are upper bounds to be considered in the delay budget and operators would try to keep the delay well within the specified limits. Delay budget calculation by SCF specifies 10 ms small cell backhaul delay in order to achieve 50 ms round trip delay [**33**]. This backhaul delay is so less that there is an excess 60 ms delay even if gaming service round trip delay requirement is considered. Hence, a small cell backhaul delay of 1-10ms can easily meet the stringent delay requirement for service and is tolerable up to 60ms above which QoE starts to degrade in delay sensitive services [**33**].

Availability, outage and resiliency

Availability of a cell site is the percentage of time the backhaul is in fully working condition and is represented in terms of number of ‘nines’ of percentage e.g. 99.999% (5). In general, packet transport networks are required to meet availability value of 5 nines (99.999%) in order to provide the same performance as SDH/SONET networks. But availability varies from one segment to other in an end-to-end connection and is typically lower at the last mile backhaul and RAN and highest at the core network [**33**]. When small cells are deployed in existing macrocell network the availability can be relaxed to 99-99.9% since macrocell is able to provide the radio coverage with an availability of 99.9-99.99% in case of small cell outage. But in the absence of macrocell network, small cells need to meet availability criteria of 99.9-99.99% [**2**].

System failures or outages caused by equipment failures, power failures or obstruction to wireless links impact the availability. Hence resiliency is required to be implemented in the last mile for the connection to recover from outage or to avoid them. One of the ways to introduce resiliency is by using mesh topologies which offer multiple routing options between the source and destination [**33**] [**2**].

QoS/ Classes of Service (CoS) support

To ensure good user experience, transport networks must facilitate QoS prioritization of the traffic i.e. important traffic such as signaling, voice and synchronization must be able to take precedence over best-effort traffic during congestion. This is achieved by tagging the packets with QoS priority class e.g. Differentiated Services Code Point (DSCP) identifier in IP packets and Priority Code Point (PCP) in Ethernet frames. So, when the packets are received these priority bits are read and the corresponding packets are placed into appropriate 'class of service' queues [**33**].

Synchronization

Synchronization is very important aspect in RF systems since it helps in maintaining the correct operation of system along with satisfying the spectrum licensing conditions. Systems based on FDD require frequency synchronization, whereas TDD systems must be phase synchronized in addition to frequency [**33**]. The requirements for LTE small cell backhaul synchronization are defined in 3GPP specification 3GPP 36.104. Synchronization can be achieved with a reference source clock at the base stations like Global Navigational Satellite System (GNSS) or sending clock references to the base stations. However, GNSS will be rendered useless when used indoors due to signal loss caused by building or jammers [**2**]. Several techniques are developed to provide synchronization for packet based backhaul but not all techniques provide phase synchronization needed for TDD systems. These techniques include Network Timing Protocol (NTP), synchronized Ethernet and IEEE 1588 v2 [**2**] [**33**].

Operation, management and traffic engineering

Small cells are usually deployed in very large numbers and are placed in busy areas where it is difficult to revisit site location to make changes. This deployment scenario calls for a high degree of self-configuration facility with configuration files being received from a centralized location [**2**]. Additionally, the backhaul solution must also provide provisions to monitor the operation and update the network configuration remotely. These features reduce the installation and operational expenses of an operator [**33**]. Finally, it is beneficial from the point of supporting end-to-end QoS to provide means to change the conditions of backhaul dynamically based on demand or link status. This feature requires active network monitoring for delays, jitter and packet loss over the backhaul [**2**].

3.3.2 Small cell wireless backhauling techniques

Different types of wired and wireless backhauling solution have been proposed for small cells. Wired backhaul solutions are used in scenarios where high capacity and reliability is required. But from the ease of deployment perspective of small cells, the wireless backhaul solution has an advantage of not needing to run cabling between cell sites, resulting in reduced installation costs and faster deployment [**2**]. These wireless solutions can be broadly categorized based on carrier frequency (~600 MHz to 80 GHz), line-of-sight (LOS) and non-line-of-sight (NLOS) propagation, spectrum licensing arrangement, dynamic spectrum licensing and topology [**33**]. The following section discusses about the wireless backhaul solutions which fall under these categories and its challenges.

Sub-6 GHz licensed and unlicensed bands

Deployment of small cell backhaul in sub-6 GHz has number of benefits for applications requiring point-to-point or point-to-multipoint link, line-of-sight and non-line-of-sight link. But there are different challenges associated with licensing type of carrier frequency because these backhauls operate in both licensed and unlicensed bands (2.4 and 5 GHz). The license bands vary from one country to another [**2**]. The advantages of using licensed bands are: ability to provide guaranteed QoS and scalability by avoiding interference. Whereas, the operation in unlicensed band eliminates the cost incurred in securing the spectrum but creates a major challenge to eliminate the adjacent and co-channel interference. This interference is due to sharing of unlicensed spectrum with Wi-Fi, Bluetooth and other applications. In case of licensed band backhaul solution, capacity is limited by spectrum allocated and the channel bandwidth generally ranges from 5-20 MHz.

Techniques such as Latency aware QoS scheduling are used to ensure QoS and to lower the latency. Depending on the deployment type and frequency, the coverage area ranges over few kilometers. On the contrary, in unlicensed bands, achievable coverage area is few hundreds of meters due to the interference. Unlicensed band backhaul solutions operate on 40 MHz channel bandwidth using contention-based protocols to access the unlicensed spectrum simultaneously along with the existing radio technologies. From the capacity to cost ratio point of view, backhaul solution in sub-6 GHz unlicensed bands holds an edge over licensed bands counterparts by providing huge capacity in several hundreds of Mbps at a very low cost.

The non-line-of-sight feature of sub-6 GHz backhaul makes it suitable for rapid deployment of small cells under a macrocell network. Installation times can be further reduced by using self-aligning antennas. Unlicensed backhaul solutions are typically used for Wi-Fi access points at remote locations, whereas the licensed band solutions are used to provide capacity and coverage [**33**].

Microwave: 6-50 GHz

Microwave frequencies for mobile backhaul have been in use for decades and it accounted for about 55% of the global wireless backhaul at the end of 2011 [**30**]. In a wireless backhaul, link capacity is directly dependent on channel bandwidth and spectral efficiency. Multiple Gbps of throughput in a microwave backhaul is possible by utilizing multiple single carriers. On the other hand link capacity can also be increased by increasing the spectral efficiency by means of using higher modulation (1024QAM), 2X2 MIMO on a line of sight link and cross polar interference cancellation [**37**]. Also, higher spectral efficiency and wider channel bandwidth results in lower RTT latency over single hop (< 1 ms). In terms of coverage, there is a tradeoff between the availability, capacity and operating frequency. For small cell application, huge capacity at a high availability of 99.999% can be obtained with a point-to-point backhaul at 30-42 GHz frequency. This results in coverage range of 2-4 km, the coverage is further reduced when used in point-to-multipoint link due to low gains of wide sector antenna [**37**]. But wider coverage area is obtained at lower operating frequency and availability. Rapid deployment of small cells with microwave backhaul offers microwave hub site to be connected to the small cells in point-to-multipoint configuration. Thus, only the small cell antenna needs to be aligned when the hub site is operational, thereby reducing installation times. Microwave backhauls are generally deployed in scenarios where high capacity is in demand and the provision for line-of-sight is available between the hub site and small cell. Propagation at microwave frequencies is vulnerable to signal fading during heavy rainfall. Resiliency against this fading is supported in microwave backhaul systems by implementing link adaptation techniques [**33**].

Millimeter Wave: 50-300 GHz

The motivation behind operating in millimeter frequencies (50-300 GHz) for small cell use case is the generous availability of wideband RF-channels and Gbps of capacity using simple single channel configuration. Moreover, the small cells are expected to be as little as 50 m apart, making it ideal to use millimeter frequencies which provide high capacity with short-range links. The typically used frequencies are V-band (60 GHz) and E-band (70-80 GHz) are contiguous bandwidth of license exempted 9 GHz (57-66 GHz) and two lightly licensed 5 GHz bandwidths (71-76 GHz, 81-86 GHz) respectively [**2**]. This enables accommodation of large scale of small cells with wider channel allocation (50 MHz up to 1000 MHz) in a given area when compared to deployments and channel allocation at frequencies lower than millimeter wave frequency. Furthermore, operating at millimeter frequency has an implicit advantage of reduced antenna diameter of few centimeters resulting in smaller equipment size. High frequency of microwave enables high gain directional antennas to be used in long range links. But on the downside, high frequency results in narrow beamwidth which requires antennas alignment during installation [**2**]. The coverage range at 60 GHz and 70-80 GHz are up to 1 km and 3 km respectively which makes it ideal to use the low cost equipment operating at 60 GHz for street-to-street, street-to-rooftop connections and radios operating at 70-80 GHz for roof-to-roof connectivity. In this way, cells with E-band backhaul are seen as aggregation points for the traffic from cells with 60 GHz backhaul.

The drawbacks of operating at millimeter wave frequency are attenuation caused by the oxygen present in the atmosphere for 60GHz frequency range and due to water molecules for 70-80 GHz frequencies. Moreover, transmission at these frequencies relies on line-of-sight communication through narrow beamwidth antennas with absence of reflection from or penetration through obstacles. As a result, there is very low risk of interference but multiple hops are required to reach a destination to go around obstacles in the propagation path. Another disadvantage associated with millimeter wave radio is the loss of link alignment by the pole sway in extreme weather conditions. The advantages such as scalable capacity and lower latency of millimeter wave technologies far outweigh the disadvantages. This makes millimeter wave technology well suited for small cell backhaul in dense urban deployments [**33**] [**2**].

3.4 Optimal backhaul solution for small cells

Based on the requirements and the proposed solutions discussed earlier in this chapter, this section discusses about the technology choice to design an optimal backhaul solution for small cells. These include:

- From the capacity and connectivity perspective of small cells access, wired backhaul solution offers higher capacity and reliability than the wireless solutions. But if we consider the large scale deployments of small cells, there arises the issue of cabling between the cells or to aggregation points. Also, the solution must be aimed at minimizing the installation time and cost. This makes wireless backhaul solution in millimeter wave in general as the most viable choice to satisfy the capacity needs of small cells.
- High availability offered by present access backhaul network is also expected from small cell backhaul since small cells play a crucial role in providing connectivity in less coverage areas or used to offload the macro cell traffic. This requirement in turn requires the backhaul to implement a certain degree of resiliency because small cells backhaul links can be easily obstructed (e.g. trees, vehicles). Resiliency is improved by using mesh topology, wherein nodes in the network form multiple redundant links. This way traffic can be redirected via alternate paths in events of link outage and network load.
- Small cell access backhaul must ensure QoS by supporting traffic prioritization based on priority class. This makes sure that certain class of traffic is given higher preference than other during congestion scenarios or based on delay requirement of traffic class.
- Small cell backhaul require synchronization in frequency or phase domain based on the technology employed. Accurate synchronization over packet switched backhaul is more challenging than with legacy circuit switched (e.g. E1 or STM-1) backhaul. However, techniques such as IEEE 1588v2 (PTP) and Synchronous Ethernet are defined to allow base stations to extract synchronization from a remote clock

reference. Among these techniques, PTP provides accurate frequency and phase synchronization.

- Large scale deployments of small cells, often located in unconventional locations and small form-factor of small cell base stations complicates the on-site operations and maintenance. This problem can be alleviated by introducing a high degree of self-configuration in the small cells. Also, management tools to enable network-wide over the air-configuration and updates will help in minimizing installation and operational costs and simplify handling of several radio access technologies.

The backhaul solution that satisfies above mentioned points is a wireless mesh network formed using millimeter wave radios with comprehensive routing and scheduling schemes along with provisions for Quality of Service and security. A lot of research has been conducted on the feasibility of wireless mesh networks on various applications. The most popular among them are IEEE 802.11 Wireless Local Area Network (WLAN) mesh, IEEE 802.15.5 Wireless Personal Area Network (WPAN) mesh and IEEE 802.16 Wireless Interoperability for Microwave Access (WiMAX) mesh. But most of these proposed solutions offer a complete mesh solution and address only few problem area of mesh networking (e.g. Media Access Control (MAC), scheduling, protection, QoS). Therefore, the proposed solutions cannot be directly applied to fulfill the small cell backhaul requirements without extensive modifications [**38**].

The self-organizing wireless mesh network backhaul presented in the Chapter 4 satisfies the above listed small cell backhaul requirements. The term self-organizing network (SON) refers to automation of network operations, and is categorized along key OAM areas of configuration, optimization and troubleshooting. They are self-configuration, self-optimization and self-healing. Self-configuration is a process to reduce the human operator intervention when a new network element is brought into service. This process is carried out in three phases namely auto-connectivity setup, auto-commissioning and dynamic radio configuration. Self-optimization involves optimization of the network parameters during its operation. Some of the features under self-optimization are load balancing, traffic steering, energy saving and capacity optimization. Finally, self-healing is an attempt to reduce the troubleshooting effort in case of cell degradation or outage [**39**]. Detailed implementation of these self-organizing features in the proposed backhaul solution is discussed in Chapter 4.

3.5 Summary

A mobile backhaul is a connecting transport medium between the mobile access network and the mobile core network. The backhaul network is divided in to 3 domains: access, aggregation and core, presented in the decreasing order of cost and number of links in each tier. Typically, a backhaul connection is provided by using copper cables, optical fiber and microwave radios. In order to keep up with the growth of radio access and core network, the backhaul network technology has also evolved from low capacity TDM based technology to ATM and entirely packet based i.e. IP backhaul transport. The advantage of IP based backhaul is the provision for employing QoS scheme, support for native packet data, lower network latency and flat network architecture. However, with the introduction of small cells in 4G, the wired backhaul solution is not always feasible due to the unconventional deployment location of small cells. Therefore, an entirely new wireless backhaul solution, which provides high capacity cost-effective backhaul, must be designed.

The requirements for a backhaul for small cells include high throughput, coverage area of few hundred meters, lower latency, high availability, resiliency, support for QoS and traffic engineering capabilities.

Some of wireless backhaul technologies used in small cells are based on usage of microwave radios. However, an optimum wireless backhaul solution for small cells can utilize the millimeter wave radios, which offers high data rates. High availability and resiliency can be achieved by connecting the small cells in the form of a mesh network. Additionally, to facilitate large scale deployment of small cells in a cost effective manner, implementation of self-organizing functionalities such as self-configuration, self-optimization and self-healing along with the network-wide management tools makes such a backhaul solution ideal for small cell deployment.

4 TOPOLOGY MANAGEMENT FOR WIRELESS MESH SELF-ORGANIZING NETWORK BACKHAUL

This chapter discusses about a mobile backhauling concept jointly developed by Nokia Networks and VTT with inherent self-configuration, self-optimizing and self-healing capabilities targeted for small cell deployments [**40**] [**41**].

Section 4.1 gives an overview description of concepts of proposed wireless mesh solution and its key features and elements. Section 4.2 introduces to the topology manager entity of the centralized controller (WCC) and its role in enabling self-organizing functionality in Self-optimizing Wireless Mesh Network (SWMN) system.

4.1 Overview of wireless mesh self-organizing network concept

The Self-optimizing WMN (SWMN) backhaul concept is designed to provide very high capacity first mile access backhaul to small cell mobile base stations. According to this concept, in a heterogeneous network of macro, micro, and pico base stations, the base stations are connected in the form of a partial mesh using point-to-point wireless backhaul. The network elements are connected to each other mainly with pencil beam point-to-point directional millimeter wave radio links. These radios can be electronically steered to point in any direction, thereby allowing the establishment of wireless links between base stations in all directions. However, the base stations can also be connected via wired medium such as fiber [**38**] [**42**] [**40**] [**41**].

SWMN system employs an extensive set of self-organizing features resulting in autonomous network management and network configuration. This leads to a reduced or zero OAM intervention. These self-organizing features are implemented in the following ways self-configuration in the form of automated mechanism from link alignment of the millimeter wave radio, neighbor discovery, authentication till the connection establishment between the end points (e.g. a set of base stations and an aggregation transport network gateway). Self-healing feature is implemented through automated resiliency schemes which reduce the effects of link or equipment outage. And, self-optimization is employed by offering flexible

QoS scheme, comprehensive set of traffic engineering mechanisms such as load balancing and congestion control mechanism. These mechanisms allow autonomous deployment of cell sites with reduced installation times, provision for QoS based traffic engineering and flexibility in handling the traffic inside the mesh network. Thus enabling efficient use of backhaul transport capacity [**38**] [**42**] [**40**] [**41**].

Typically, a Self-optimizing WMN (SWMN) network consists of 20-200 backhaul nodes connected in partial mesh topology. These backhaul nodes are grouped into local sub-networks. The sub-networks can overlap over each other to provide coverage to larger area. Within these sub-networks, the nodes are linked with each other through point-to-point wireless or wired connections. The partial mesh topology assumes a certain level of redundant links to enable the link protection and other resiliency features of SWMN [**40**] [**41**].

There are two types of backhaul nodes, a SWMN generic node (GN) and a SWMN gateway node (GW). A SWMN generic node provides local transport connectivity to one or more base stations to connect to the SWMN sub-network. The SWMN generic nodes can also act as relay points in the absence of client base stations. The gateway nodes connect the SWMN nodes to the external transport network. Thus, the gateway nodes handle all the incoming and outgoing traffic to and from its SWMN sub-network. A large SWMN sub-network can have more than one gateway node to provide multiple points of traffic entry and exit to the external transport network. This also ensures that connectivity with the external network is maintained in the events of non-redundant gateway node failure. Figure 4.1 illustrates a typical wireless mesh network. A gateway node is usually present in the macro base station or in a small cell site having reliable access medium to other transport network, and the generic backhaul nodes are present at small cell sites [**42**] [**40**] [**41**].

The intelligence in the gateway and generic SWMN nodes is called Protocol Engine (PE). Additionally, SWMN concept also introduces a centralized intelligence called WMN Centralized Controller (WCC). The WCC is responsible for implementing automated topology management functionalities such as network configuration, network optimization and among other functionalities. Thus, it maintains an optimum topology and connectivity in a SWMN sub-network, also known as domain. A WCC can handle multiple domains, which collectively constitutes a SWMN area. The centralized controller can be deployed either in SWMN gateways or in the core network cloud. But the latter option is more beneficial since a single WCC present in the cloud can have access to entire network [**42**] [**38**] [**40**].

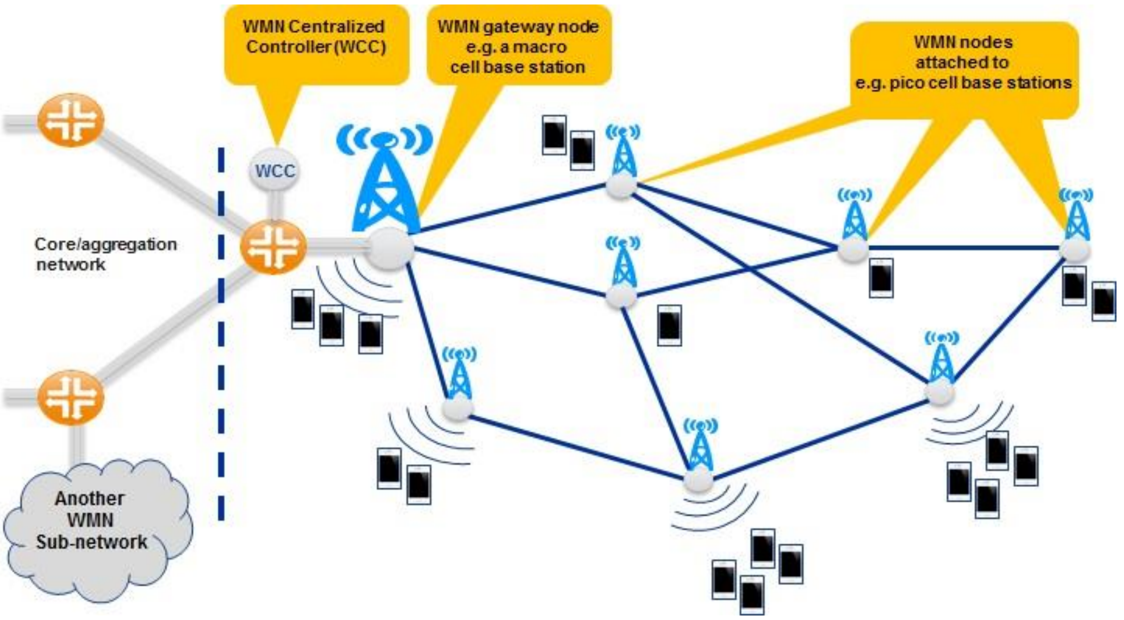

WMN Centralized Controller (WCC)
WMN gateway node e.g. a macro cell base station
WMN nodes attached to e.g. pico cell base stations
WCC
Core/aggregation network
Another WMN Sub-network

Figure 4.1: Wireless Mesh Network [38**].**

4.1.1 Transport Service, routing and forwarding

SWMN offers Ethernet transport service. The layer 2 solution was chosen as a baseline to develop the Proof-of-Concept (PoC) system, but can be extended to support layer 3 or IP transport service as well. The connectivity between the backhaul nodes is mainly wireless pencil beam point-to-point millimeter wave radio links. The channel access scheme can be either Frequency Division Duplexing (FDD) or Time Division Duplexing (TDD) [**43**] [**42**] [**40**] [**41**].

The routing in SWMN is based on pre-computed routing paths and forwarding information from the centralized controller. Each SWMN node computes the local forwarding table upon receiving pre-computed prioritized list of alternative routing paths sent by the WCC. A forwarding table consists of routing path information, node identification number and an output interface. The forwarding tables at each node are used to forward the traffic dynamically based on path/route availability, max vs. available (link/path) capacity, path congestion status and traffic priority [**42**] [**43**].

The use of pre-computed routing scheme makes it possible to switch to alternate paths within few microseconds in cases of failure or load balancing situations with no data loss or no retransmissions (“hitless switching”). The use of pre-computed routing requires the number of nodes in a domain to be within a certain range. This leaves the decision of node count in a domain to the WCC, which is responsible for network optimization [**43**].

4.1.2 Shared resources and scheduling

Scheduling is a process of allocating time slots to links during which a node can transmit or receive. Since in SWMN wireless communication is based on the concept of shared resources, where a shared resource can be, for example, a wireless transceiver or antenna, scheduling for data transmission becomes a challenge. In the simplest implementation of shared resources, a SWMN node can communicate with its neighbors only one at a time. This creates a restriction on resource access. However, with the use of shared hardware resource and smart beam steering algorithm a node can connect to several neighboring nodes without any manual intervention, thereby reducing the capital and operational expenses. To enable all these and to provide resource access to the nodes on a shared basis, a network wide scheduling scheme is required. Network level scheduling has an implicit advantage of reducing the interference caused due to simultaneous transmissions [**42**] [**43**] [**44**].

4.1.3 Network self-configuration

The term self-configuration refers to mechanisms which facilitates ‘Plug-and-Play”, for example, automatic connection setup and auto commissioning [**39**]. Such a feature is enabled in SWMN by the WCC through highly automated process from the power on phase of system till the connection setup to the mesh network. The operations involved in the self-configuration phase are radio link alignment, neighbor discovery, authentication and distribution of configuration messages [**44**].

The self-configuration mechanism can be briefly explained by the steps followed in autonomous deployment of SWMN nodes the first step involves deploying new node at the installation site and powering on the new node by the installing person. The only pre-configuration required for the node is its Hardware ID (HW ID), authentication parameters and some radio related parameters. Moreover, skilled workforce is not needed for the node installation since the link alignment of the antennas and the manual configuration is avoided by the electrical beam steering and self-configuration functionality. This way deployment of nodes is made quick, easy and economical [**44**].

In the next step, the new node starts neighbor discovery procedure. This procedure involves scanning periodically for new nodes by the nodes already existing in the network using a beacon message. The scanning process is facilitated by the beam steering mechanism and beam sweeping within RF antenna range. The new node receives and acknowledges the beacon message once its antenna gets aligned to the existing node. Then, the beam directions for both ends of the link are fixed and a notification about the newly added node is sent to WCC. Finally, the node is authenticated by WCC for its hardware and software validity and to prevent security attacks [**44**].

Once the node is authenticated, the new topology is fed to the topology optimizer which decides whether computation of routes and link schedule information is required or not. The new configuration is distributed to the entire network including the new node. The switch over to the new configuration occurs synchronously in all SWMN nodes so that ongoing traffic in the network is minimally affected [**44**].

After receiving the new configuration message, the new node is able to connect to the network and start forwarding traffic, including traffic from its local client. A similar process occurs when a new link is introduced between two existing SWMN nodes. The self-configuration is called upon by WCC whenever there is any persistent change to the existing topology e.g. caused by node or link failure [**44**].

4.1.4 Resiliency, fault management and self-healing

The SWMN system employs a comprehensive and automated resiliency mechanism to minimize the impact of node and link failures in the mesh network. The need for resiliency arises due to faults in the system during its operation. These faults are effectively managed in the SWMN by detecting the faults and re-routing the traffic to alternate pre-computed routing paths. The fault detection mechanism is event-based i.e. as soon as the fault is detected (e.g. weak received signal strength of the radio link) a Link Status Update (LSU) message is broadcasted along the routing paths that traverse the affected link. This informs the nodes about the faulty links or nodes. Fast fault detection combined with per-packet link quality monitoring results in a near-hitless protection scheme. Upon detection of fault, the hierarchical fault recovery scheme built into SWMN concept is triggered as described in [**44**]. Depending on the failure situation one of the recovery mechanisms is applied. The time scale taken by various mechanisms varies from few microseconds to tens of seconds. The fastest method involves re-direction of the traffic that is to be transmitted along the broken link along alternate pre-computed routing path. If the path failure is persistent, local correction to the routing paths can be made. Finally, if the failure situation lasts a long time (i.e. considered permanent), the WCC re-computes all the routing paths and re-configures the entire network [**45**] [**42**] [**44**].

4.1.5 Quality of Service

The SWMN system employs nine priority classes ranging from highest priority to lowest priority: HP1, HP2, HP3, HP4, HP5, LP1, LP2, LP3 and LP4. The HP1 priority class is mainly used for transmitting internal control messages and for carrying time synchronization messages. The remaining higher and lower priorities are used for traffic. The HP1 and HP2 frames are scheduled in Strict Priority Queuing (SP) while the other high and low priority classes are scheduled using Weighted Fair Queuing (WFQ). The strict priority classes are scheduled first and are optimal for carrying delay sensitive traffic, whereas the remaining effective capacity of the link is scheduled in WFQ manner for other traffic priority classes. The priority classes are mapped to the Priority code point (PCP) in the Ethernet frame (IEEE 802.1Q) header of the client traffic. The weights of WFQ and the queue sizes for the different priority classes can be configured as per the needs [**42**] [**45**] [**44**].

4.1.6 Load, congestion management

The SWMN system includes load and congestion management mechanism which ensures efficient backhaul capacity utilization by selecting the best routing path (usually the path with large available capacity) for each traffic flow or alternatively for an individual data packet [**44**] [**42**]. The system is based on the monitoring of link capacity and link quality. The monitored load management parameters are available link capacity, link quality, output queue length and frame drop rates. These parameters are measured and maintained for each traffic priority at each of the nodes. Congestion status is determined based on queue lengths and drop rates. A SWMN node originating the traffic measures the usability of the routing paths based on the flow’s intensity and congestion status in the path. If the node finds the routing path to be congested it may move the traffic away from the congested link to an alternate path with more available capacity. Any change in the link or load status triggers a LSU indicating the available capacity in that link and the congestion status [**42**] [**45**].

4.1.7 Synchronization

Accurate time synchronization is very essential in the SWMN nodes in order to follow network-wide link scheduling. The SWMN system employs IEEE 1588-2008 Precision Time Protocol (PTP) based time synchronization technique. According to this technique, the synchronization is distributed in a SWMN system via a synchronization tree. Either one of gateway node acts as grandmaster clock or an external grand master clock forms the root of the synchronization tree. New SWMN nodes form the branches to the synchronization tree and act as PTP boundary clocks offering bridged synchronization transport for timing messages. This way neighbors to gateway node or master clock reference act as slaves to grandmaster and the next tier act as slaves to first tier and so on. The grandmaster clock that can be used in the SWMN system is chosen by relying on PTP’s best master clock algorithm [**46**] [**42**].

4.1.8 Elements of WMN

The SWMN system consists of SWMN nodes and a centralized controller (WCC) [**44**].

Node elements

As mentioned earlier, there are two types of nodes namely: SWMN generic nodes (GN) and SWMN gateway nodes (GW). The SWMN nodes have Ethernet interfaces to the client system e.g. base stations and wireless network interface to interact with the neighboring SWMN nodes. The generic nodes send and receive topology change messages and configuration messages to and from centralized controller through the gateway nodes. A gateway node is very similar to a generic node except that it has an Ethernet interface to the external transport network and is logically connected to the centralized controller. The main functions of the gateway node are to provide access to aggregation networks and to relay control/configuration messages between the centralized controller and generic nodes. Additionally, the gateway node may act as a grand master clock to provide time synchronization in the SWMN [**44**].

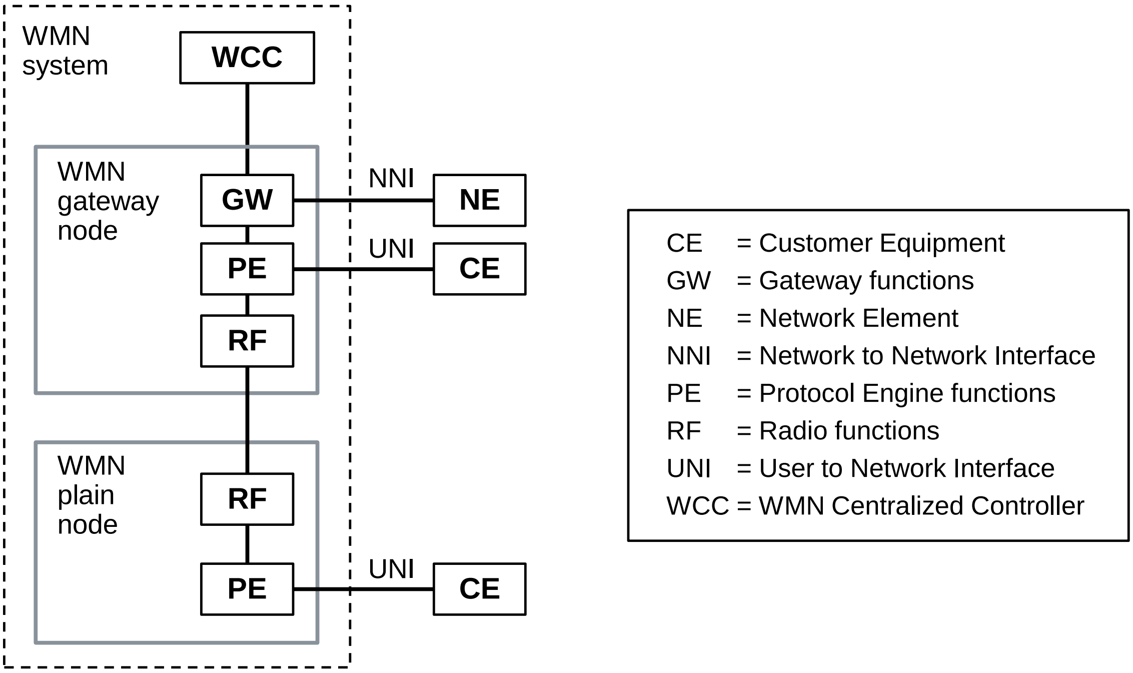


Figure 4.2: High level architecture of basic SWMN system [44**].**

Node SW components

The SWMN functionality and intelligence in a SWMN node is called the Protocol Engine (PE). The PE architecture consists of two parts namely: the control plane and the data plane. The data plane part of the PE handles all routing of user traffic in the mesh and also sending control messages to control plane, queuing and de-queuing of packets, low-level link state monitoring, load balancing and fast local re-routing. The control plane is mainly responsible for establishing a connection to WCC in case of gateway node, handling LSUs and TCRs, neighbor discovery, synchronization and monitoring congestion [**44**].

WMN centralized controller (WCC)

The architecture of the centralized controller is depicted in Figure 4.3.

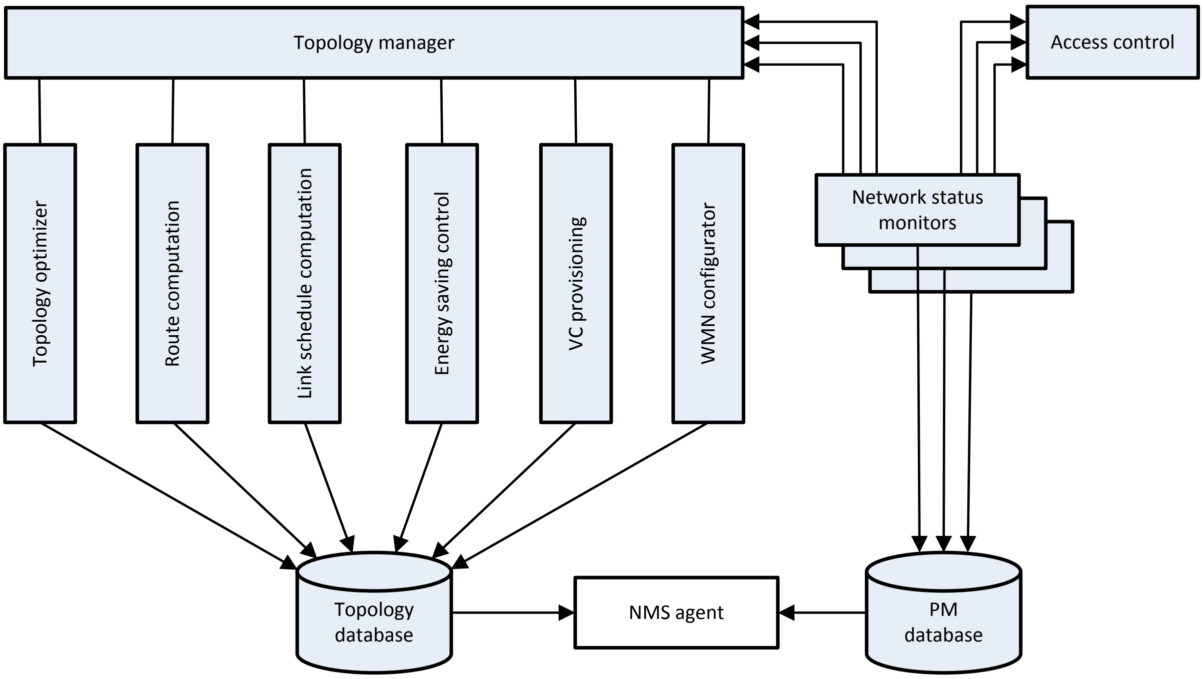


Figure 4.3: Functional architecture of WCC

The main functions performed by the WCC can be briefly overviewed by mentioning the tasks of the various blocks in WCC architecture. The topology manager is the vital part of the WCC as it controls all the functions of the WCC and is responsible for all the re-computation and re-configuration decisions. It also maintains information about physical topology extracted from SWMN nodes. The topology optimizer deals with network optimizing decisions such as number of nodes or links in a SWMN domain and decisions regarding node or link inclusion into the network. The tasks of route and schedule computation blocks include computation of prioritized set of alternative routing paths and link-schedule information. These computations are performed whenever the physical topology changes as initiated by the topology manager. Once the computations are completed, the topology, routing and schedule information is composed in SWMN configuration messages by the configurator. The energy efficiency and authentication procedures are handled by the energy saving control and access control elements respectively. The Virtual Connection (VC) provisioning handles all the virtual connections that are defined to transmit data between the end points of the date paths. Finally, the network status monitors are responsible for performance and status monitoring of the network based on the messages received from SWMN nodes and decisions on forwarding this network state information [**47**] [**44**].

4.2 Topology management function by centralized controller

The autonomous functions performed by the WCC to configure, optimize, monitor and maintain a topology are collectively called as topology management. As an example this refers to network optimization in terms of end-to-end (E2E) latency, reliability and energy efficiency. These functions handle any changes in the network and optimize the physical topology by dynamically including or excluding links or nodes. This way the WCC ensures that route and schedule re-computation triggered due to topology change results in highly delay optimized routing paths and link schedule. The topology management functions of WCC also include monitoring the network performance, resource utilization, and to provide simple OAM functionality [**44**].

The main functions performed by the SWMN topology management are deciding the optimum SWMN domains within a SWMN area, determining the active network topology within a SWMN domain, shutting down nodes and links as part of energy saving control, routing and link schedule computation, monitoring the performance of SWMN domains and control the update of network configuration [**44**].

The Topology Manager Module (TMM) is responsible to carry out the topology management functionalities and the operations within WCC. To track down the changes in the network, topology manager gathers SWMN-area wide status information through Network Status Monitors (NSM). Based on this information, the topology manager triggers appropriate WCC modules and procedures if topology reconfiguration or optimization is necessary. For example, if topology change has been detected TMM initiates Topology Optimizer Module (TOM) and passes the current physical topology along with the topology changes as its input. The TOM decides which links and nodes to be included into the active topology and which to exclude. TMM then triggers the route and link-schedule computation units upon the active topology computed by the TOM. If the computation of optimal routing path and link-schedule computation turns out to be infeasible, then the cycle repeats from the topology optimization process. Upon obtaining an optimum route and schedule, WMN configurator is initiated to form the configuration message. This message is then distributed to the SWMN nodes. The TMM also exercises energy saving functionalities by triggering the energy saving control module [**47**] [**44**].

4.2.1 Topology optimizer

The process of topology optimization starts with status information regarding the current topology sent by the topology manager. With this information as an input, the topology optimizer groups the nodes in the SWMN area into domains and decides upon the active and dormant links of the topology. The topology optimizer makes the decision of active links by comparing the results of the optimization algorithm and the given physical topology. The important links are retained and the redundant links are selectively removed based on topological constraints until each node has number of links equal or less than number of links allowed for a node. The end-result obtained from the topology optimizer module is the active topology which is given as an input for route and link-schedule computation [**47**] [**44**].

4.2.2 Route computation

Based on active topology information, Route Computation Module calculates a prioritized set of alternative routing paths from any node to any node for the given topology. Since the traffic flows in the mesh network are primarily between generic nodes and their primary gateways, the route computation is optimized for those paths. However, the traffic between the generic nodes is also supported to provide e.g. fast X2 connectivity. The route computation can be influenced by traffic engineering parameters such as link capacities, traffic along certain links and path delay constraints. However, the most important optimization parameter is the bi-directional end-to-end delay between the nodes. The route computation is performed only when the topology changes i.e. after addition or deletion of node, after permanent link failures or link removal [**42**] [**44**].

4.2.3 Link-schedule computation

Similar to route computation, the scheduling information is also pre-computed by the WCC for the given topology. The computation of scheduling information involves dividing the given topology into activity sets. An activity set is a collection of links that can be active simultaneously. An optimized subset of activity sets is calculated based on end-to-end delay and optionally using similar traffic engineering parameters as where used in route calculation. The resulting optimized activity set will be repeated cyclically providing a schedule to the nodes which they can transmit or receive [**42**] [**44**].

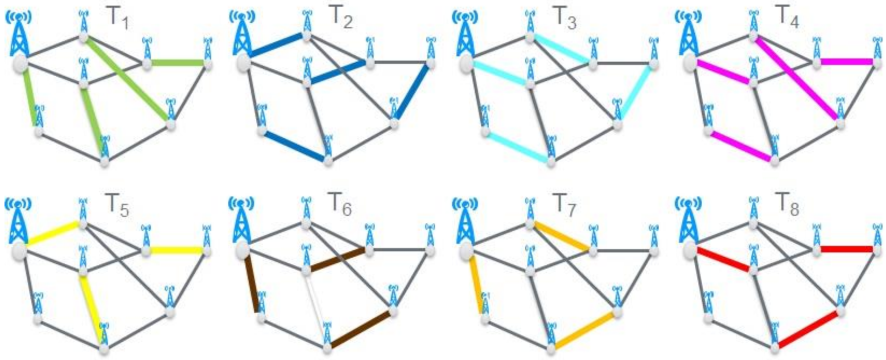


Figure 4.4: Example of schedule computation. The colors represent the active links during a certain transmission opportunity.

4.2.4 WMN configurator

The main task of WMN Configurator Module (WCM) is to distribute the new configuration to all the nodes in the SWMN network. It forms the configuration messages consisting of new active topology, new routing path information and new link-schedule information. The configuration messages compiled by the WMN configurator are distributed among the SWMN nodes through the gateway nodes in each domain. In addition, WCM determines the required order of topology change actions i.e. domain splitting, merging and node handover between domains in order to reach the new optimized topology. The WMN configurator also determines the suitable time to switch to new configuration based on the network status. Furthermore, synchronization of nodes in the events of domain splitting and node handover between domains is carried out by the WCM [**47**].

4.2.5 Energy-saving control

The Energy –saving Control Module (ECM) handles all the energy saving processes at SWMN node level. These include for example determining nodes or links which have been inactive for a very long period. Upon detection of these nodes or links, re-configuration of SWMN network is triggered to shutdown or put to the nodes sleep to save energy [**47**].

4.2.6 Network status monitor

The Network Status Monitor (NSM) observes the network for topology changes and maintains an up-to-date status of the network. It is also responsible for collecting the link quality and load information delivered through LSUs to analyze the performance of the network and to identify when some topology change is permanent. Based on the state of the network, the NSM may decide upon the network status information (e.g. permanent topology change) and the time at which it needs to be forwarded to other parts of the network. Also, these monitors may be used as a countermeasure against denial-of-service attack on access control module by filtering out authentication attempts by blacklisted nodes [**47**] [**44**].

4.2.7 Virtual connection (VC) provisioning

The VC provisioning module manages all the virtual connections that overlay the SWMN network. The task of this module is to map Attachment Circuits (AC) to a VC, that is, establish connectivity between client ports in source and destination [**47**].

4.2.8 Access control

All the node authentication procedures are carried out in the Access Control module. Whenever a new node is added to the network, it is authenticated by this module through AAA infrastructure. Also, the access control has the ability to black-list un-authorized nodes [**47**] [**44**].

4.3 Summary

This section describes a novel concept for small cell deployments called the Self-optimizing Wireless Mesh Network (SWMN). According to this concept, the backhaul nodes that may be present in base stations are connected to the gateway in the form of a partial mesh network using point-to-point directional millimeter wave radio links. The routing and data transmission in the mesh network is based on prioritized list of alternate routes and active link-schedule times pre-calculated for a given topology respectively. The concept also implements self-organizing features to automate the neighbor discovery, link establishment, provide high resiliency, optimization based on flexible QoS scheme, load and congestion management. The key modules in this concept are SWMN gateway node, SWMN generic node and Wireless Mesh Network Centralized Controller (WCC). Among these elements, the WCC is responsible for executing the topology management functionalities in the network. The modules present in WCC are topology manager, topology optimizer, energy saving control, VC provisioning, route computation, link-schedule computation, network status monitor, access control and WMN configurator. These modules help in automating the network configuration, network optimization and network management. Also, the WCC maintains a network status through network monitoring mechanisms.

5 TOPOLOGY MANAGEMENT VALIDATION SYSTEM

The Chapter 4 explained the concepts of topology management in SWMN backhaul. This chapter provides the validation scenarios for topology management functions and also gives an overview about the proof-of-concept system used for validation. This chapter also talks about the author’s contribution to Self-optimizing WMN (SWMN) system. The main contributions by the author are:

- Defining the validation scenarios to test the topology management functions and autonomous network build-up features in the Lanner MR-730 environment and simulator environment.
- Development of python based simulator to test topology management functions of the WMN centralized controller (WCC).
- Testing and debugging of the SWMN PE and WCC Proof-Of-Concept software implementation in target environment i.e. in the Lanner MR-730 network processor and in a Linux machine, respectively.
- Detecting concept anomalies in the PE and WCC proof-of-concept systems and resolving them with the implementation team.
- Developing an interactive GUI based visualization and network management controls in the simulator.

Section 5.1 discusses about validation scenarios and the testing methodology for verifying different topology management functions. These scenarios include node addition, node deletion, domain formation, domain split and merge, etc. Section 5.2 provides a survey on potential systems that could be used for proof-of-concept validation. Finally, Section 5.3 provides details about emulator and simulator validation test setups.

5.1 Validation scenarios

The validation scenarios provided in the following sections will test the topology management functions and features of WMN centralized controller. These scenarios involve incremental addition or deletion of SWMN nodes or mesh links to trigger certain events which help in validating the topology management functionalities at a basic level. Since the SWMN system is unlike any other system that implements standardized set of protocols, the validation tests are created only for this system in particular [**42**]. The validation plan created in conjunction with the developed system provides an extensive set of test cases for each of the topology management functions. Therefore, a handful of test cases which provide an overview over the topology management function are chosen and explained in the validation scenarios. These scenarios test the validity of the WCC through various topology scenarios, which are created by addition or deletion of node or link to the SWMN network. This way, autonomous network build-up, an essential feature of SWMN, can also be verified. Furthermore, the scalability of the system is verified by adding a large number of SWMN nodes to the network.

5.1.1 Autonomous network build-up

Objective and background

One of the prime features supported by the topology management mechanism of WCC is the autonomous network build-up. This is enabled through autonomous neighbor discovery functionality in the SWMN nodes and optimizer, route computation, link-schedule computation, VC provisioning and WMN configurator modules in WCC. The verification of these topology management modules during a network build-up are carried out in this test scenario through incremental addition of SWMN nodes.

Method for testing autonomous network build-up

The basic test for autonomous network build-up starts by connecting the gateway node to the WMN centralized controller and subsequently adding new SWMN nodes and connections. The validity of this feature can be verified through a WCC visualization which shows the current topology of the network. The indications of new nodes can be inferred from the log messages in the WCC Linux terminal and the primary gateway node. Since the routing in the mesh network is based on prioritized list of alternative routes generated by the route computation module, the correctness of routing information can be verified by sending different priority traffic between SWMN nodes using the predefined VLANIDs. Meanwhile, the packets with undefined VLANIDs should be rejected.

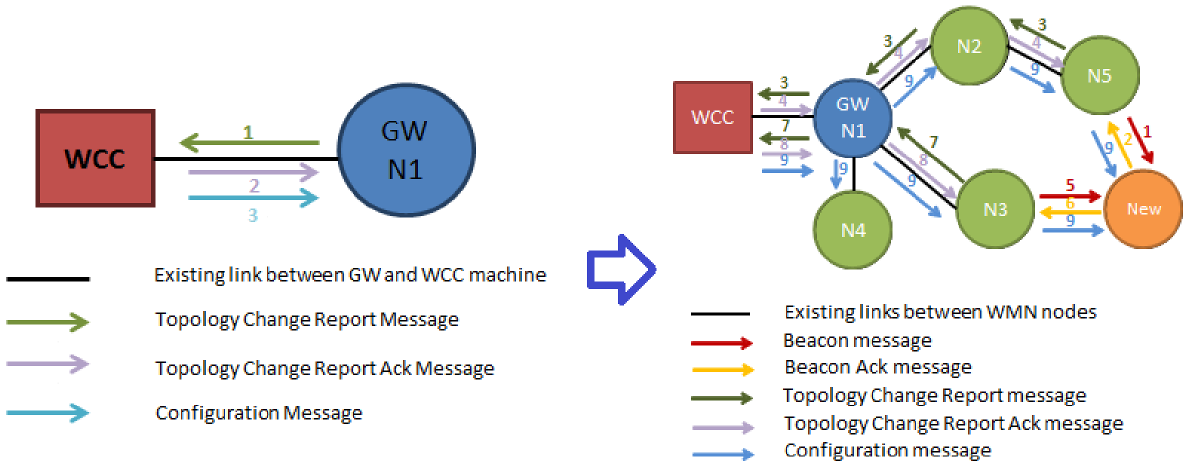

WCC
GW
N1
1
2
3
Existing link between GW and WCC machine
Topology Change Report Message
Topology Change Report Ack Message
Configuration Message
WCC
GW
N1
N2
N3
N4
N5
New
Existing links between WMN nodes
Beacon message
Beacon Ack message
Topology Change Report message
Topology Change Report Ack message
Configuration message

Figure 5.1: Gateway node and new node detection procedure in autonomous deployment scenario.

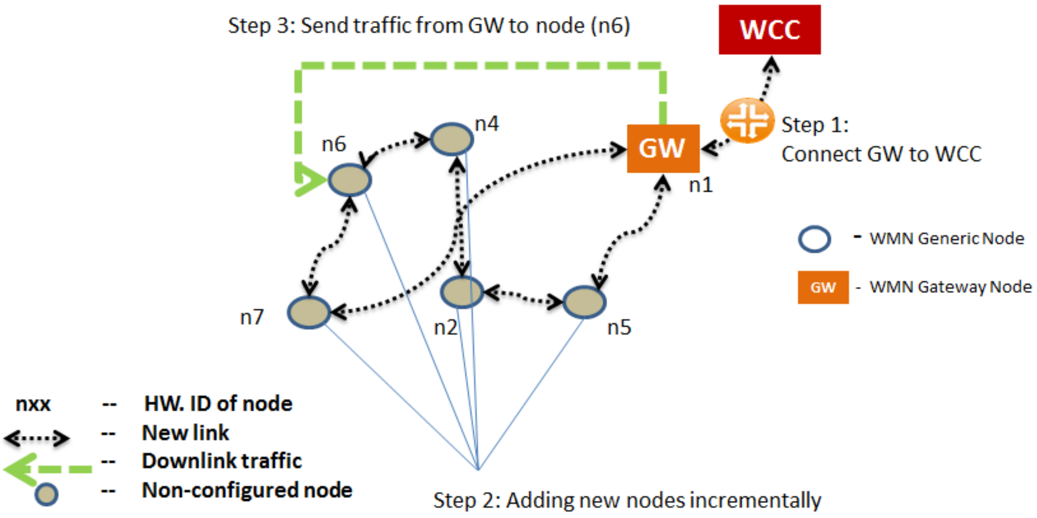


Figure 5.2: Topology for testing autonomous network build-up, routing and scheduling functionality.

Similarly, the network-wide schedule computed by the link-schedule computation module of WCC can be verified by sending traffic between nodes and observing the timing of the packets received at the receiving node. The timing of packets must be coherent with the configured transmission slot duration. Thorough test for schedule computation can be carried out by varying the configured transmission slot and observing the corresponding change in the packet timing. The tests for routing and schedule computation can be done using Spirent packet capture or a packet sniffer tool. Figure 5.1 shows the control message exchange performed during neighbor discovery. The topology used to verify the autonomous network build-up is depicted in Figure 5.2.

5.1.2 Node addition/deletion

Objective and background

The motive behind this test scenario is to verify one of the basic topology management functions, also known as a node insertion or removal from the active network topology. As explained earlier in Chapter 4, the topology manager initiates the route and link-schedule re-computation whenever the physical topology changes, i.e. addition of node or removal of node. Based on the type of SWMN nodes (GW or GN node), two different node addition and node deletion validation scenarios have been defined. These scenarios are also tested against live traffic situations in the SWMN network.

Method for testing node insertion/removal with ongoing traffic in mesh network

The objective of this scenario is to verify the topology management functions when multiple nodes are added/deleted at a time to/from the existing mesh network and also to portray that ongoing traffic in the mesh is unaffected by this network change. It is assumed initially that the network consists of few SWMN generic nodes and a SWMN gateway node connected to the WCC. Also, traffic is flowing between existing SWMN generic nodes and the gateway node. Ethernet traffic of specific data rate and packet length is sent using Spirent Test Center traffic generator, where the input client port of SWMN gateway node Lanner MR-730 unit and receiving client port of a SWMN node are connected to Spirent unit for traffic measurements. In the next step, a group of three SWMN nodes are added/ removed and the result is observed in WCC topology visualization. The newly added nodes appear in the visualization once the network is re-configured with the new routing and schedule information. Furthermore, dropped packet count and latency can be monitored in the Spirent Test Center application to verify that whether the node addition / removal have not affected the ongoing network traffic. Figure 5.3 represents a real-life network topology of Arlington Heights, a suburb of Chicago used as reference topology to test addition of new group of nodes. Similarly, Figure 5.4 depicts the topology used to test the node removal scenario.

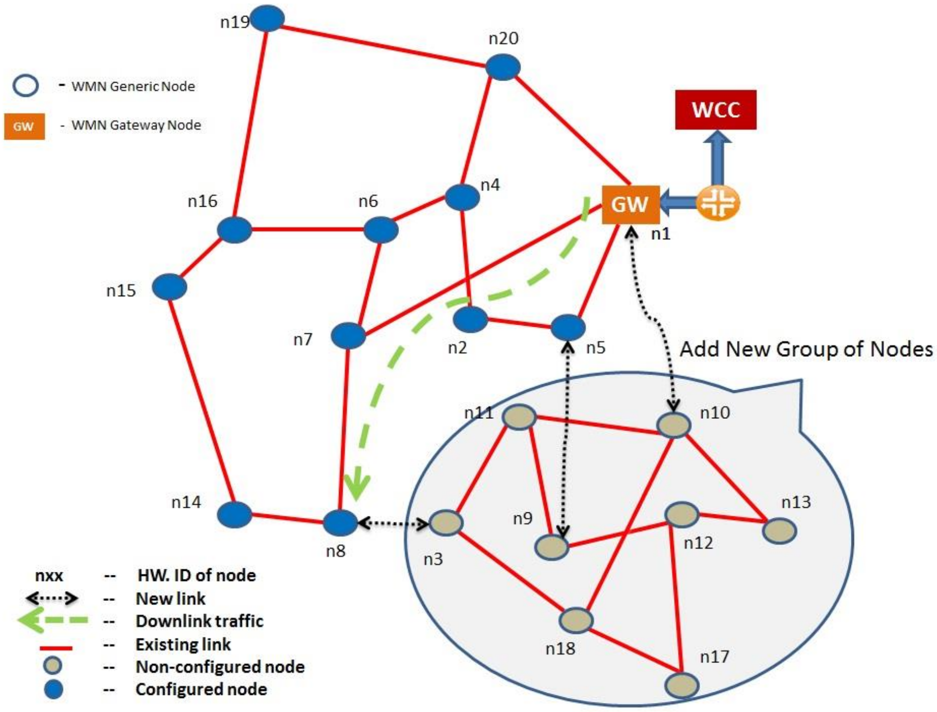


Figure 5.3: Arlington Heights, a suburb of Chicago topology for multiple nodes addition to network.

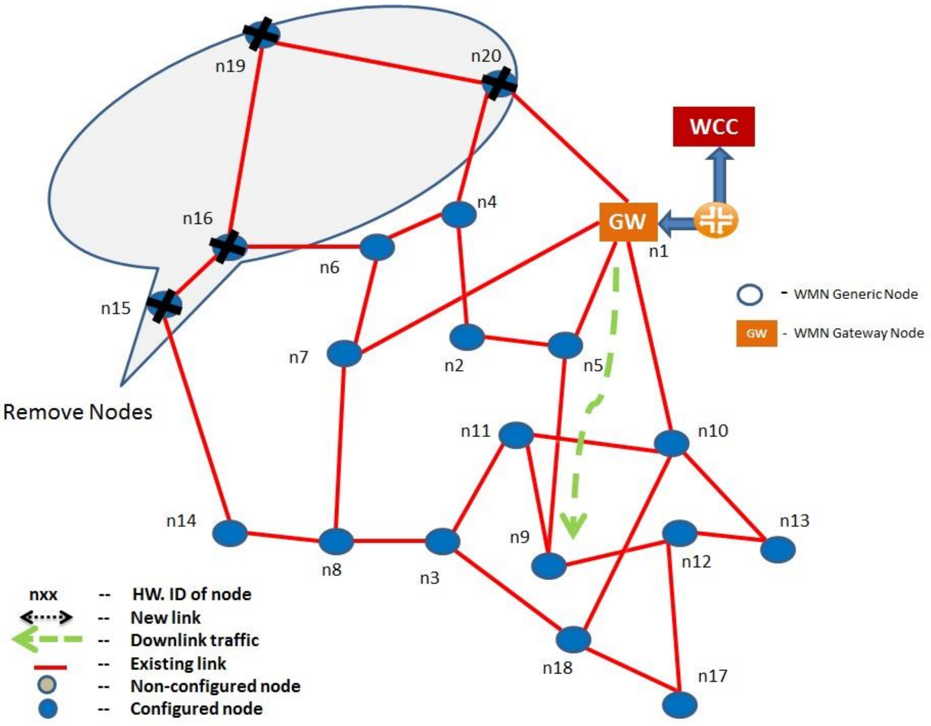


Figure 5.4: Arlington Heights, a suburb of Chicago topology for multiple nodes deletion from network.

Method for testing gateway node insertion/ removal

This test scenario verifies the topology manager operations when a gateway node is inserted or removed. This requires complete network re-configuration forcing the topology manager to re-compute the routing and schedule information taking the inserted/removed gateway node into consideration. The WCC visualization verifies the added or removed GW node in the topology. Also, the change in the hop count between the SWMN nodes due to the re-computed routing paths and schedule information can be examined from the visualization. The initial state of the network consists of few configured SWMN generic nodes and a single gateway connected to WCC. Figure 5.5 and Figure 5.6 depicts the topologies used to test new gateway node addition and primary gateway node removal scenario respectively.

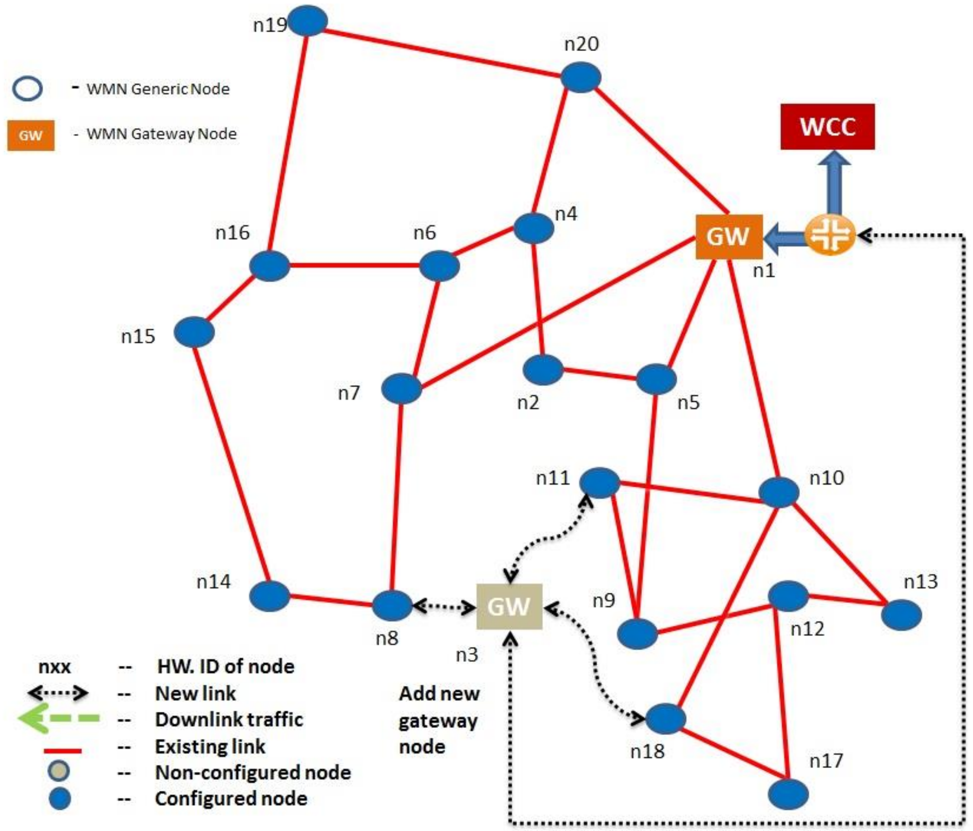


Figure 5.5: Test topology for inserting new gateway node.

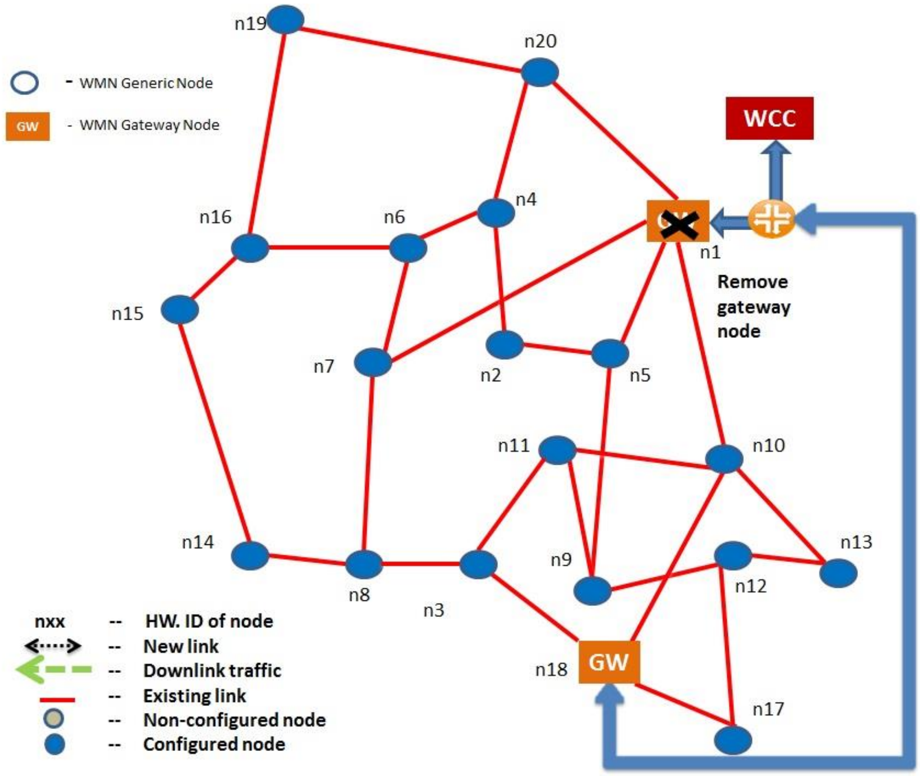


Figure 5.6: Test topology to make use of alternate gateway by removing a gateway node.

5.1.3 Link addition/deletion

Objective and background

The objective of the test cases discussed in this section is to verify the topology optimizer functionality when a link is added or removed between existing SWMN nodes. The verification of topology optimizer includes testing the decision making ability to allow or deny a new link from being added to the active network topology. The scenarios used for this purpose are: inserting a new link between SWMN nodes and removing link between nodes to depict permanent link damage situation in the presence of ongoing traffic.

Method for testing inclusion of a link into active topology when discovering a new link

In this test case, a new link is added between a SWMN generic node and the gateway node, where the number of outgoing links to the gateway node and generic node is less than or equal to maximum allowed links per node. This way the topology optimizer is able to allow the new link to be added to the active topology. The inclusion of newly added link can be verified from the thick black line representing a scheduled link in the WCC topology visualization. Additionally, this link is also included in the new route configuration and is scheduled for transmission which must be depicted in the spanning tree and link-schedule generated by the WCC. This test case is also applicable for link addition between two SWMN generic nodes and between gateway nodes as well, given that they satisfy the above mentioned criteria. The topology used in this scenario is shown in Figure 5.7, where new link is added between node 1 and node 7.

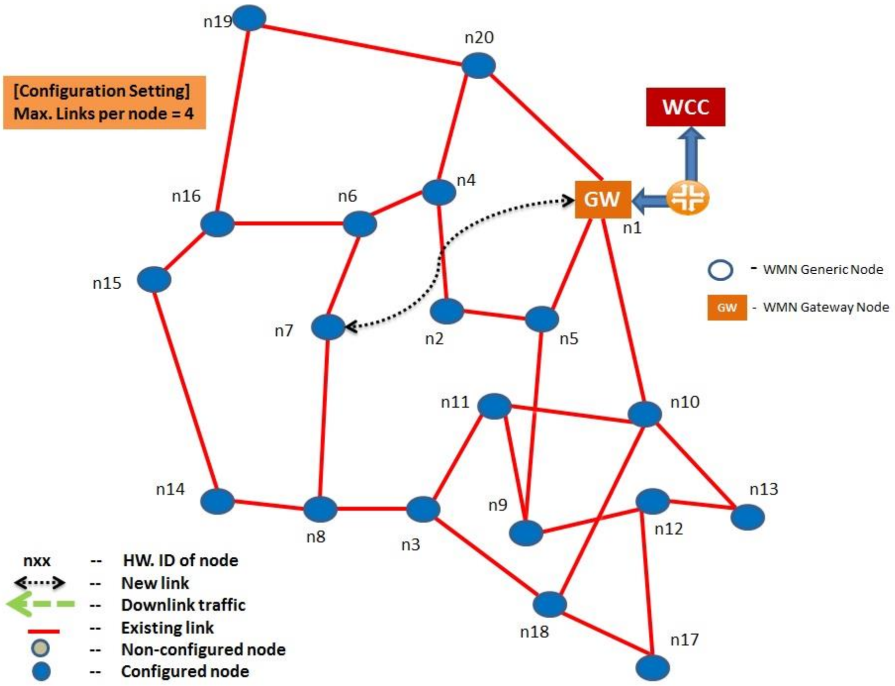


Figure 5.7: Test topology for new link addition between node (n7) and gateway node.

Method for testing exclusion of a link from active topology when discovering a new link

This test case involves adding a new link between two SWMN nodes existing in the mesh network. But these nodes should have the number of outgoing links greater than the value of maximum allowed links per node. Therefore, the topology manager detects the newly added link but the topology optimizer module takes only the maximum number allowed links per node into consideration for each SWMN node while determining the optimum active topology. This can be verified in the simulator visualization which represents the topology with active and dormant links. Furthermore, it can be verified from WCC visualization that certain link is absent in the active topology diagram but present in the physical topology.

Figure 5.8 depicts the topology used to verify the exclusion of link from active topology when a new link is added between node 2 and node 11.

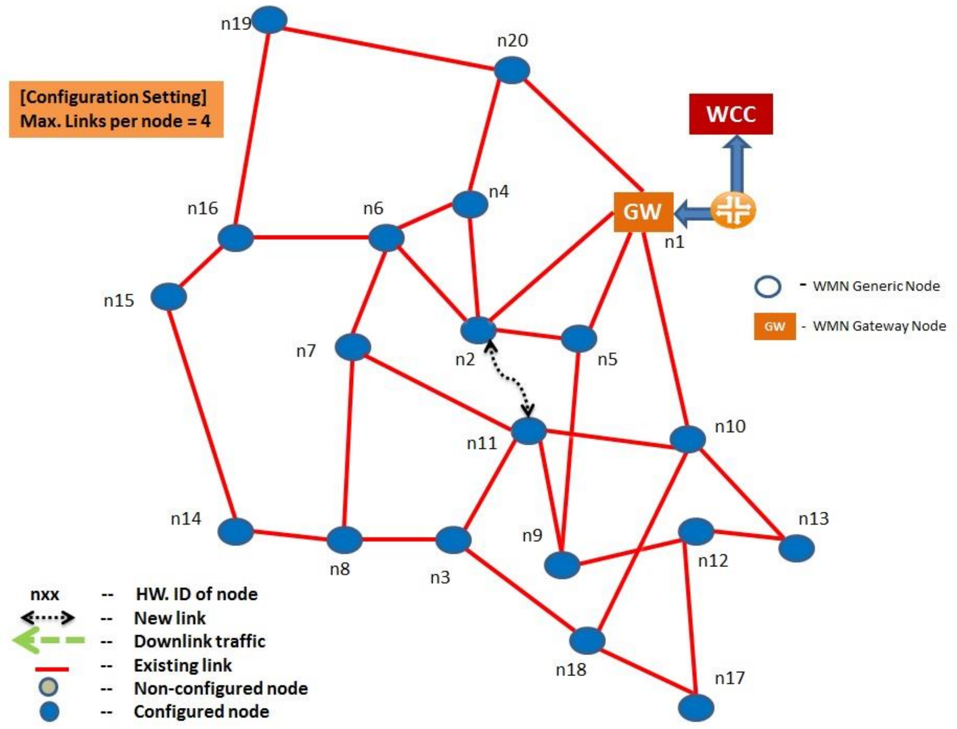


Figure 5.8: Test topology for new link addition between node (n2) and node (n11).

Method for testing the link removal between nodes with ongoing traffic in the link

As stated earlier in SWMN concept description, the system employs an extensive resiliency scheme which routes the traffic via pre-calculated secondary path to the destination in the events of link failure. But a prolonged link failure requires the topology manager to intervene and re-calculate the routing and schedule information by not considering the faulty link. This test case targets the above mentioned situation of link removal or permanent link failure. The test setup for this test case consists of few SWMN nodes with traffic flowing from GW to a non-leaf GN which is at two hop distance from gateway node. Ethernet traffic is introduced using the Spirent Test Center traffic generator and the client port of receiving node is connected to Spirent equipment to measure the packet loss and packet delay. The traffic sent through the gateway is configured to be of specific frame length, priority and data rate. Once the link is removed the traffic flows through the secondary path as per resiliency scheme in SWMN nodes and at the same time calls for network re-configuration. The change in the traffic path due to link removal must not result in packet loss but there may be slightly increase in packet delay. The secondary path taken by the traffic can be observed from the WCC topology visualization. Finally, after the network re-configuration the visualization must show the most optimum path for the traffic to the destination node. The topology used to verify the link removal scenario is given in Figure 5.9, where the link between node 6 an node 7 is removed.

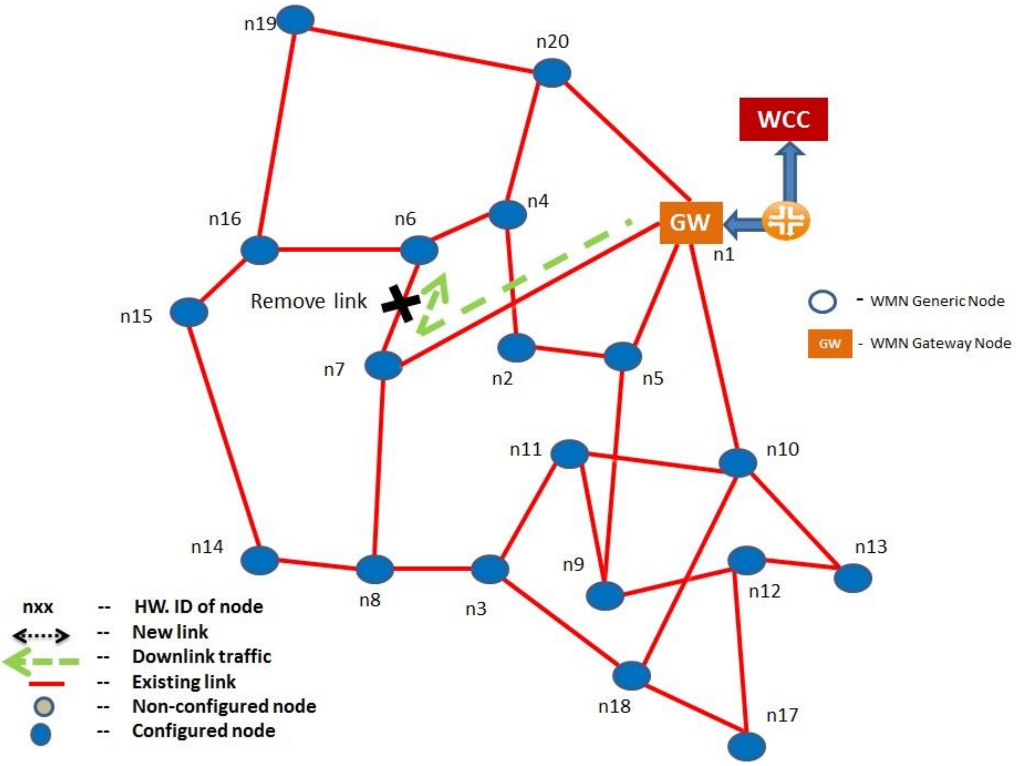


Figure 5.9: Test topology with link removed between node (n6) and node (n7).

5.1.4 Domains split or merge

Objective and background

Once the topology optimizer receives the physical topology information it will group the SWMN nodes into domains containing one or more gateway nodes. The network size in SWMN system is constrained by the complexity of link schedule computation and also by requirement to maintain network-wide scheduling scheme. Therefore, a large SWMN network is divided into smaller entities. These domains operate on each of their own specific link-schedule. The current implementation of optimizer algorithm considers number of

SWMN nodes in a SWMN domain as the optimization parameter to perform splitting or merging of domains. Moreover, the topology optimizer also implements the functionality to handover SWMN nodes from one domain to another to balance the domain formation. The basic verification tests of domain formation include increasing the node count in domain to enable domain split and vice versa to validate domain merge functionality. This can also be achieved through introducing a new gateway node in a network with huge node count for domain split and removing one of the existing gateway nodes from the current network.

Method for testing domain splitting

The optimization of mesh network by topology optimizer which involves splitting of domains can be verified by using a network topology with a single domain containing two gateway nodes and number of generic nodes less than the maximum allowed nodes in a single domain. In the next step, a group of generic nodes are added to this initial topology in such a way that number of nodes in the domain is greater than domain node count limit. This causes the single domain to split into two domains. The presence of two domains can be verified by observing nodes in the simulator output. The value of maximum allowed nodes in a domain is a configurable parameter in the WCC, which can be set to verify splitting of domains.

Method for testing domain merging

Merging of domains is the opposite of domain splitting where the topology optimizer merges two or more smaller domains into a single large domain for effective utilization of shared resources. The initial test setup for this test scenario consists of two domains with one gateway in each domain and the sum of generic nodes in both domains must be slightly greater than configured maximum node count in domain. In the next step, a small group of nodes are removed from either of the domains causing the domains to merge when the total number of nodes in the mesh network satisfies maximum node count value in a single domain. The process of merging can be observed in simulator output. This is further validated by the inclusion of all the nodes in the second domain merged into a single domain in the WCC visualization.

5.1.5 Scalability

Objective and background

Scalability is a very important requirement in the mobile backhaul given the expected almost exponential increase in the number of base stations and a step towards heterogeneous networks as explained in Chapter 3. The SWMN concept provides a scalable backhaul solution enabled through the topology optimization performed by WCC. In addition to the previously described basic domain split and domain merge operations, the basic verification tests for scalability inclde identifying the maximum limit on the number of nodes that can be accommodated in a single domain, total number of nodes and total number of domains in SWMN that could be handled by WCC.

Method for testing scalability with respect to the number of nodes in a domain

The validation method to test the scalability of nodes in a domain involves configuring the maximum allowed node count in a single domain to a high value such that WCC is no longer able to accommodate newly added nodes in a single domain. Thus, the initial network topology consists of single domain with one gateway and a large number of generic nodes. Following this, a large group of SWMN generic nodes are added to the network and an optimum number of nodes that can be accommodated in a single domain are identified. This can be inferred from the simulator visualization which represents the different node states from non-configured state to scheduled state. Also, the log messages in the WCC Linux terminal provide the count of number of nodes in the mesh network.

Method for testing scalability with respect to number of nodes in a SWMN area

The basic verification to analyze the maximum number of nodes that can be handled by WCC starts with a topology with five or more domains each containing a gateway node and total of forty or more generic nodes. In the next step, large groups of generic nodes are added randomly to the existing mesh network to an extent that WCC is no longer able to detect any more nodes. This threshold value can be determined from the simulator visualization which differentiates between nodes included/excluded in the SWMN area.

5.2 Study on validation systems

In order to validate SWMN concept, a suitable emulation and/or simulation platform is required. In terms of selecting an emulation platform, many solutions from Cisco and Juniper offer the required hardware processing capabilities but their operating software could not be altered to the needs of SWMN concept. The other solution is to use a General-purpose processor system as nodes. These nodes may be inter-connected using hub or switches and networking could be implemented using network socket programming APIs (Application Programming Interface). This solution fits perfectly to all the needs of SWMN concept except for the requirement of providing gigabit data rates. Therefore, the solution sought after and used in the validation are the systems that employ a network-processor. These systems provide the flexibility of a general-purpose processor along with the required packet forwarding capability similar to Application Specific Integrated Circuit (ASIC). Finally, the Lanner MR-730 with Octeon network-processor from Cavium Networks was chosen as emulation platform [**42**].

Meanwhile, to test the topology management function in emulation platform, it is required to have large number of Lanner MR-730 units for larger topologies. But due to high cost of these units, it is not feasible to validate large topologies in emulator platform. Thus, simulator platform needs to be used for larger networks while the emulator platform can be used for small networks. Since the SWMN concept does not employ a standardized set of protocols, usage of existing simulators such as Network Simulator (NS) and OPNET require additional programming and challenges to adapt to the SWMN protocols. For example, NS implements two different languages, Object Tool Command Language (TCL) in control plane and C++ in data plane which simulates the packet processing in simulator. This adds up to the challenge of working and debugging in two different planes [**42**]. Moreover, some of the simulators are proprietary which makes it difficult to alter their code. Thus, a dedicated new simulator for implementing specific topology management functions was selected as the complementary validation approach to emulation. Python was selected as the programming environment because of the rich python libraries, which help in easy implementation of complex event handling structures, time management and link modeling.

5.3 Test setup

The validation test setup involves using both hardware emulation platform and software simulation platform. Emulator or simulator is used based on the size of the topology and existence of traffic in the network in the test scenario.

5.3.1 Emulator environment

The emulator environment mainly consists of Lanner MR-730 Cavium network processors representing SWMN nodes, Ethernet cables for wired link and an experimental millimeter wave radio system for wireless links interconnecting the nodes. The Lanner MR-730 network processors are equipped with Octeon Quad-core CN5230 processor [**48**] [**42**].

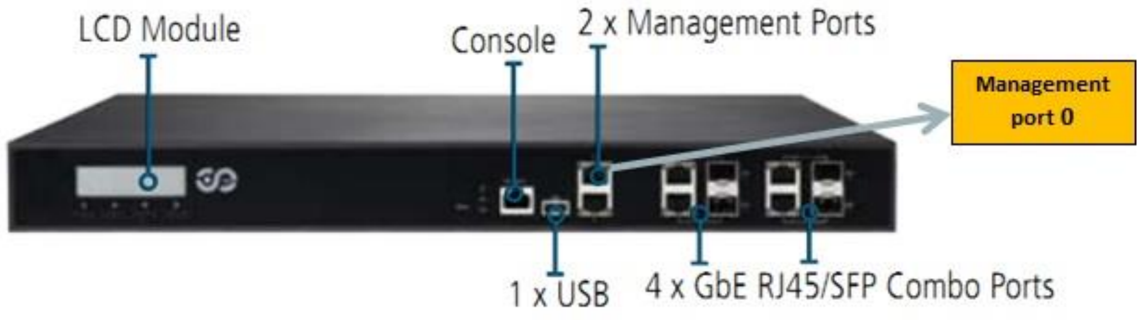


Figure 5.10: Lanner MR-730 Network Processor Platform.

These Lanner MR-730 units are loaded with proof-of-concept software called the SWMN Protocol Engine (PE) and are arranged according to given partial mesh topology. Each Lanner MR-730 consists of two Fast Ethernet ports, four Gigabit Ethernet ports with facility for optical transceiver. The two Fast Ethernet ports are used for management access, i.e. one is used for system access and the other is used for client traffic e.g. traffic from base stations. The four Gigabit Ethernet ports emulate the wireless links between the SWMN nodes when these nodes are joined with Ethernet cables. In terms of storage, Lanner units offer Serial ATA interface and a Compact Flash interface. To load the SWMN PE software, a Compact Flash Card of 4-gigabyte is partitioned into two separate planes. One of the planes is loaded with Linux image and binary file for data plane of SWMN PE software and the other plane with file system of Linux. Furthermore, Cavium Networks also offers extensive set of C-libraries which help in controlling certain set of features that the chipset offers e.g. Quality of Service features [**42**] [**48**].

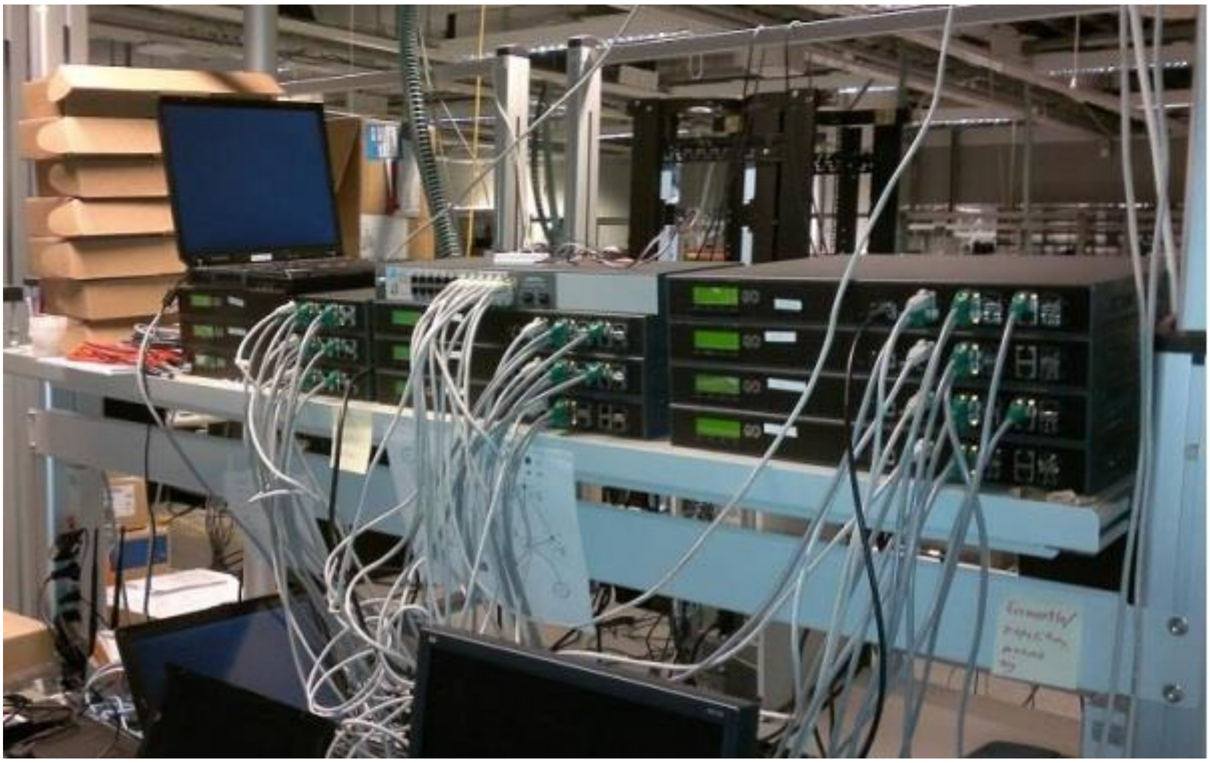


Figure 5.11: Wireless mesh network with Lanner MR-730 units in NSN Mobile Backhaul Advanced laboratory.

Figure 5.11 shows the proof-of-concept demonstrator system with Lanner MR-730 network processor platforms arranged in partial mesh topology through Ethernet cabling. During the validation process Ethernet cabling is used to emulate the wireless links between SWMN nodes. Ethernet cabling ensures reliable and less loss during communication between nodes when compared to varying characteristics of wireless medium. Thus the SWMN concept has also been successfully validated using real wireless link by replacing few Ethernet connections with millimeter wave wireless links [**40**].

The SWMN nodes are synchronized based on IEEE 1588v2 PTP. For this, the SWMN nodes are connected to an external switch to which a desktop computer is also connected such that a LAN is formed where PTP synchronization messages are exchanged by PTP daemon software in the nodes and the desktop computer. The desktop computer is configured to be the master clock and the nodes as slave clocks. Periodically the master clock sends the synchronization messages for the slave clocks to synchronize. Then control plane of the PE software in the SWMN nodes sends the PTP-corrected time information regularly to data plane for schedule synchronization.

The traffic used in the SWMN network is Ethernet traffic with support for specifying the required QoS through VLANID and PCP fields in the 802.1Q header. The VLANID specifies the destination node in the mesh and the PCP value represents the Quality of Service class. The traffic is injected into SWMN nodes through the client management port. The traffic sources that could be used to introduce traffic are Spirent Test Center traffic generator and PackEth software in Linux PC. The Spirent Test Center provides extensive set of measurement tools to conduct rigorous performance testing. Additionally, it allows data of desired traffic type, data rate, frame length and priority to be injected into client port of a SWMN node and receive at client port of another SWMN node to perform traffic analysis. Traffic generation through PC involves usage of vconfig and ifconfig utilities to modify VLANIDs and IP address configuration which ensures that right kind of Ethernet packet is sent through the client port of Lanner MR-730 equipment [**42**].

For the purpose of validation the topology varies from one test case to other, however a common reference topology used is a real-life small deployment topology in Arlington Heights, a suburb of Chicago. Due to the limitation of number of GbE port in Lanner MR-730, the Arlington Heights topology had to be slightly modified to accommodate the limitations of the emulator platform.

Wireless mesh protocol software

The protocol software in the Lanner MR-730 platform mainly consists of data plane running on one of the Octeon processors cores and control plane in separate Octeon core as is depicted in Figure 5.12. The control and data plane are written in C programming language. The control plane is configured to run in daemon mode on top of Debian Linux. During the operation of a SWMN node, the control plane is responsible for synchronization and neighbor discovery procedures. Whenever the node receives a configuration message from WCC, the control plane parses it to extract route and link schedule information. This information is used to compute local forwarding table, path preferences and scheduling so that it is used by data plane to forward packets. The communication between control planes of any two SWMN nodes is through the Link State Update messages.

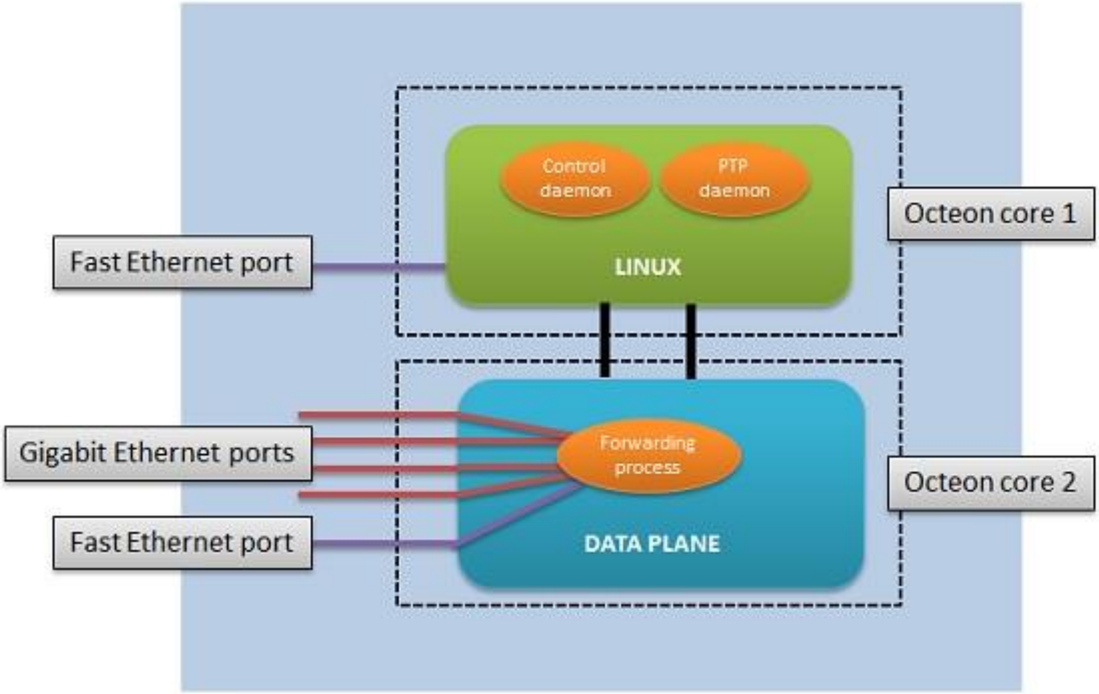


Figure 5.12: SWMN protocol software running on Octeon processor [42**].**

The data plane handles all the packet forwarding tasks between the gigabit Ethernet ports and also packets from client management port, also known as User-to-Network (UNI) interface. The data plane sends link status information to control plane by performing low level link testing. The communication between the control plane and data plane is through shared boot memory blocks or internal messaging provided by the Octeon processor. The protocol software also offers a comprehensive set of debugging options which can be used to validate the proof-of-concept system.

5.3.2 WCC SW

The WCC software is implemented using Python programming language. This software consists of route and link-schedule computing algorithm, and the intelligence to carry out topology management functions. Additionally, it is responsible for establishing and maintaining a logical connection with the gateway backhaul nodes. This connection is used to send network configuration and obtain topology change information from gateway nodes.

To observe the topology management functions performed by the WCC, a graphical visualization, which depicts the active network topology, computed routing paths and link-schedule information is implemented in the WCC PoC software.

5.3.3 Simulator Environment

As mentioned earlier, in order to verify the WCC functionalities and performance parameters such as scalability among other things, usage of only emulation platform is not feasible. Moreover, in complex topologies, the link addition/removal and node addition/removal involves laborious tasks such as manually unplugging/plugging the Ethernet wires and powering up/shutting down the nodes. This requirement led to the development of a simulator platform for simulating large topologies with multiple SWMN domains and various network growth and failure scenarios. The simulator is written in Python and is based on SimPy discrete–event simulator. The simulator is able to randomly construct and modify topology incrementally based on simple deployment, failure and repair probability models. To offer flexibility, automation, and repeatability in creating and executing test scenarios, the simulator provides script based topology generation along with events to toggle the states of nodes or links. A mix of both random and script based topology generation is also possible. The topology generation and modification is made simpler through an interactive Graphical User Interface (GUI) webpage which is implemented using JavaScript (d3js), HTML and Cascading Style Sheets (CSS). The webpage receives or sends topology updates from or to the simulator through a webserver written in Python. The simulator implements most of control plane functionalities such as TCP connection to WCC, handling of Topology Change Report (TCR) and configuration message among other things. Additionally, it partly models the network connectivity to WCC to ensure that TCRs from the nodes are able to reach WCC. Furthermore, the simulator uses networkx and matplotlib python libraries for graph functions and visualization respectively. Through this visualization, the simulator is able to display the current physical topology and states of nodes and links in the network. The simulator visualization depicts nodes, links and their various states such as broken, scheduled and unscheduled and the domain of a node. Figure 5.13 shows an example of simulator visualization along with the notation followed for representing nodes, links and their states.

To track the events occurred in topology, the simulator creates an event log which stores the duration, event type and the event related information. This event log can be further fed as an input script to the simulator to reproduce the test scenario. The types of events supported by the simulator are creating a node, toggle node state, create a link and toggle link state.

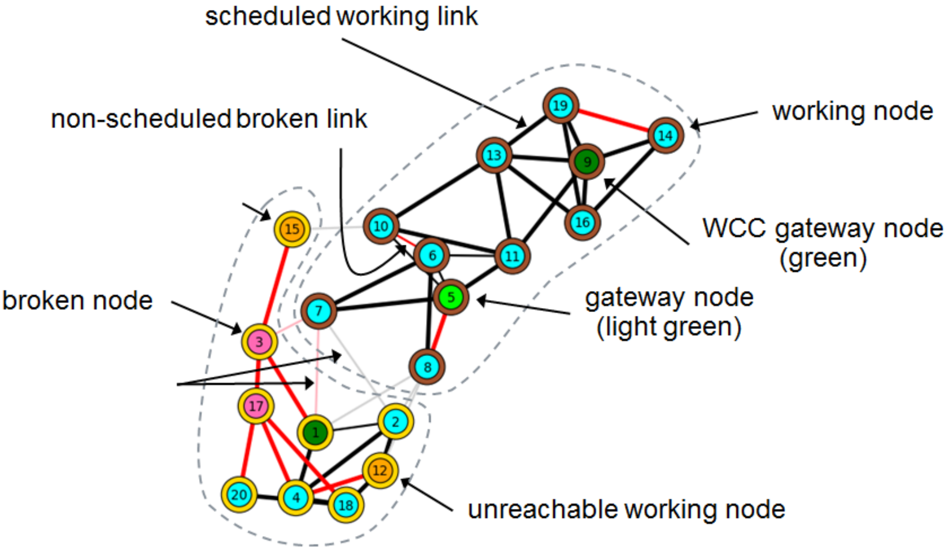


Figure 5.13: Sample topology in simulator visualization

5.4 Summary

This section describes the test specification and design for the different topology management functions implemented in the WMN centralized controller (WCC). The defined test cases validate the correct operation of the topology manager in scenarios of autonomous network build-up, node/link addition, node/link removal and domain split/domain merge. Furthermore, the scalability of WCC was also verified to ensure that the topology manager is capable of handling large topologies and future node additions. To decide on the system to be used for testing, various validation systems were considered, but, finally a dedicated topology simulator was developed to simulate the specified topology management scenarios. The simulator is built using python libraries, and also contains an interactive graphical user interface for easy creation of various network scenarios. An emulator platform consisting of Lanner MR-730 running the SWMN PE was also used during the verification process to prove the working of topology management functions in the network scenarios involving traffic.

6 TEST RESULTS

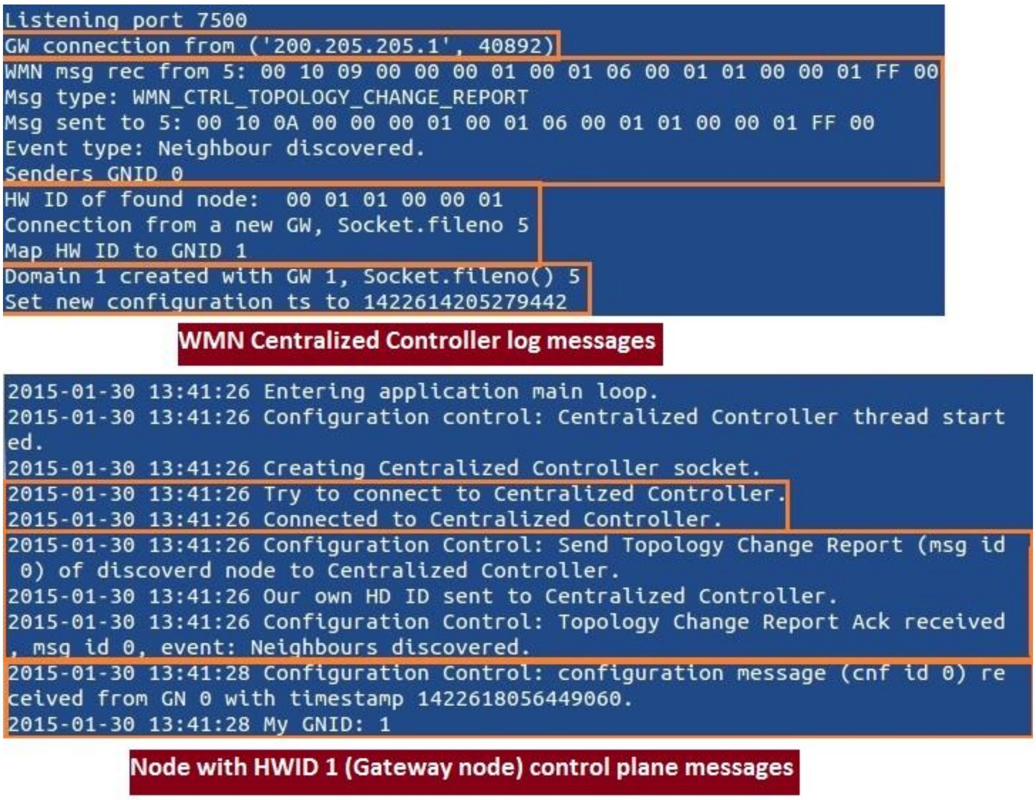
The validation environment and the test cases to validate the topology management functionalities have been presented in Chapter 5. In this chapter, the results of the test cases are discussed in detail.

Sections 6.1 to 6.4 provide the validation results of validation and their analysis. Section 6.5 draws conclusion on the overall findings in the validation process and mentions the future research topics in this concept.

6.1 Autonomous network build-up

Results of autonomous network build-up

As mentioned earlier in Section 5.1.1, the motive behind this scenario is to verify the ability of autonomous network build-up in the proof-of-concept demonstrator system. To conduct the validation, the process starts off with running the WCC program in a Linux PC that has its Ethernet port connected to the management port of Lanner MR-730 unit which acts as a gateway. This step is followed by the powering up the gateway node and generic nodes incrementally along with connecting the GbE mesh ports of the nodes with Ethernet cables. However, the SWMN system offers the flexibility in order of deployment by allowing the generic nodes to be powered on first and connecting the gateway node last. In Figure 6.1, it can be observed from the highlighted WCC log messages that whenever there is a change in the physical topology WCC receives a Topology Change Report (TCR) message. Similarly, from the gateway’s control plane messages, we can observe that when a gateway node is powered up, it tries to connect to WCC through a TCP socket and then sends a TCR with its own Hardware ID (HWID) to WCC. Upon receiving the TCR, WCC performs topology management procedures and sends a configuration message to the gateway node. The topology diagram produced by the WCC visualization is an effective tool in illustrating the incremental network build-up. It is also useful in verifying the number of links and nodes included in the active topology after topology optimization. Figure 6.2 shows the incremental network build-up starting from only the gateway node till the detection of all the 6 nodes mentioned in the test scenario. The final topology diagram in Figure 6.2 also shows the optimum route for Ethernet traffic of two different priority classes with orange color link.



```
Listening port 7500
GW connection from ('200.205.205.1', 40892)
WMN msg rec from 5: 00 10 09 00 00 00 01 00 01 06 00 01 01 00 00 01 FF 00
Msg type: WMN_CTRL_TOPOLOGY_CHANGE_REPORT
Msg sent to 5: 00 10 0A 00 00 00 01 00 01 06 00 01 01 00 00 01 FF 00
Event type: Neighbour discovered.
Senders GNID 0
HW ID of found node:  00 01 01 00 00 01
Connection from a new GW, Socket.fileno 5
Map HW ID to GNID 1
Domain 1 created with GW 1, Socket.fileno() 5
Set new configuration ts to 1422614205279442
```

WMN Centralized Controller log messages

```
2015-01-30 13:41:26 Entering application main loop.
2015-01-30 13:41:26 Configuration control: Centralized Controller thread start
ed.
2015-01-30 13:41:26 Creating Centralized Controller socket.
2015-01-30 13:41:26 Try to connect to Centralized Controller.
2015-01-30 13:41:26 Connected to Centralized Controller.
2015-01-30 13:41:26 Configuration Control: Send Topology Change Report (msg id
 0) of discoverd node to Centralized Controller.
2015-01-30 13:41:26 Our own HD ID sent to Centralized Controller.
2015-01-30 13:41:26 Configuration Control: Topology Change Report Ack received
, msg id 0, event: Neighbours discovered.
2015-01-30 13:41:28 Configuration Control: configuration message (cnf id 0) re
ceived from GN 0 with timestamp 1422618056449060.
2015-01-30 13:41:28 My GNID: 1
```

Node with HWID 1 (Gateway node) control plane messages

Figure 6.1: Control message exchange between gateway node and WCC during gateway node installation.

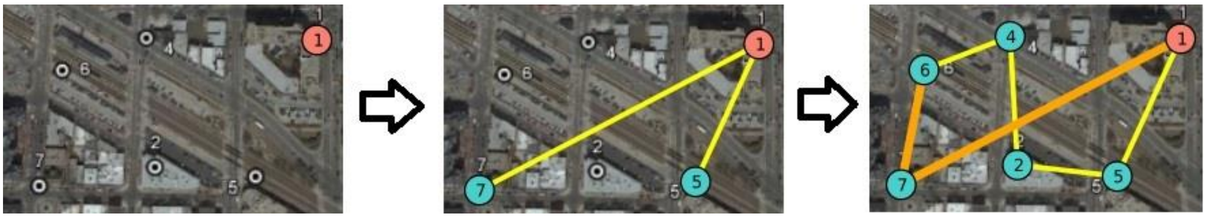
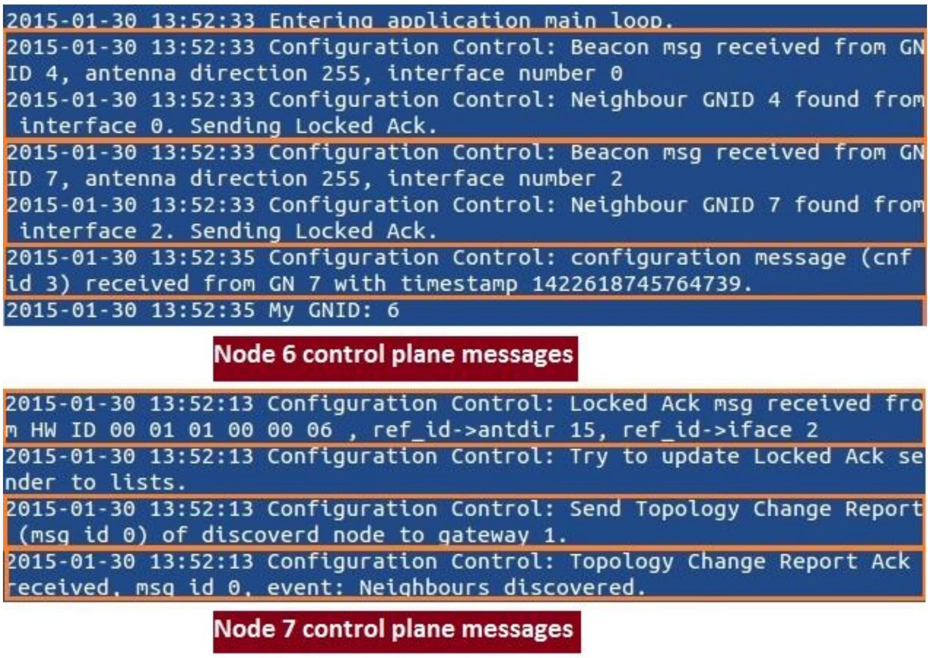


Figure 6.2: Active topology depicted by the WCC visualization tool.

Furthermore, the new node detection procedure mentioned in Chapter 5 is verified through control plane message exchange between new nodes and the nodes already existing in the SWMN. This can be seen in Figure 6.3 which shows the neighbor discovery procedure between node 6 and node 7, where node 6 is the new node added and the node 7 is already part of the mesh network. Upon addition of all the nodes, the computed routing and link-schedule information by the WCC is depicted in Figure 6.4 and 6.5. In the figures, we can observe that there are two alternate routes to the gateway node, also known as spanning trees and the link-schedule contains 4 time slots for data transmission.



```
2015-01-30 13:52:33 Entering application main loop.
2015-01-30 13:52:33 Configuration Control: Beacon msg received from GN
ID 4, antenna direction 255, interface number 0
2015-01-30 13:52:33 Configuration Control: Neighbour GNID 4 found from
 interface 0. Sending Locked Ack.
2015-01-30 13:52:33 Configuration Control: Beacon msg received from GN
ID 7, antenna direction 255, interface number 2
2015-01-30 13:52:33 Configuration Control: Neighbour GNID 7 found from
 interface 2. Sending Locked Ack.
2015-01-30 13:52:35 Configuration Control: configuration message (cnf
id 3) received from GN 7 with timestamp 1422618745764739.
2015-01-30 13:52:35 My GNID: 6
```

Node 6 control plane messages

```
2015-01-30 13:52:13 Configuration Control: Locked Ack msg received fro
m HW ID 00 01 01 00 00 06 , ref_id->antdir 15, ref_id->iface 2
2015-01-30 13:52:13 Configuration Control: Try to update Locked Ack se
nder to lists.
2015-01-30 13:52:13 Configuration Control: Send Topology Change Report
 (msg id 0) of discovered node to gateway 1.
2015-01-30 13:52:13 Configuration Control: Topology Change Report Ack
received, msg id 0, event: Neighbours discovered.
```

Node 7 control plane messages

Figure 6.3: Neighbor discovery procedure between Node 6 and Node7.

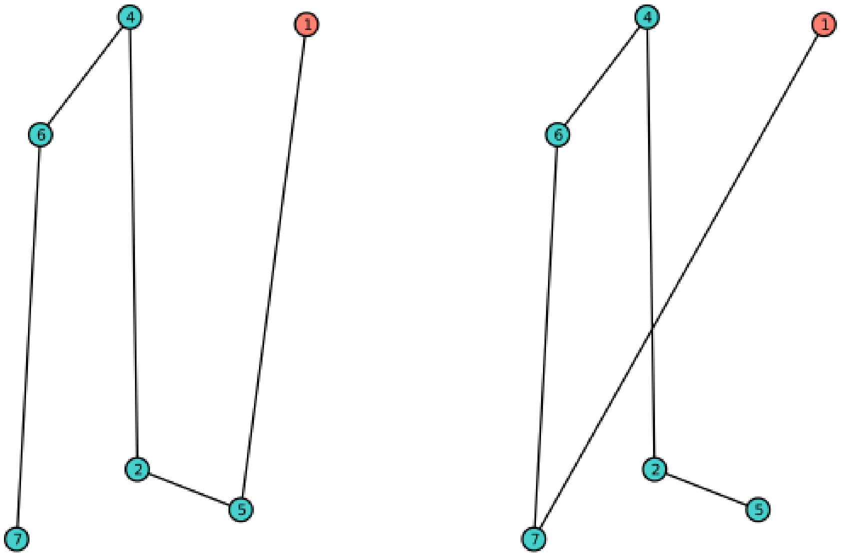


Figure 6.4: Routing paths for the test topology.

For verification of the routing information computed by the WCC, the client ports of node 1 and node 6 are connected to transmitting and receiving ports of the Spirent traffic generator for traffic measurements. Further, VLANID is provided in the configuration file of the WCC for communication between node 1 and node 6. Using the Spirent Test Center, the traffic to be sent is configured with the above mentioned VLANID, a priority (PCP) and a data rate. For the testing purpose, the configured VLANID value is 8 and PCP value is 5 (101), corresponding to high priority traffic e.g. video.

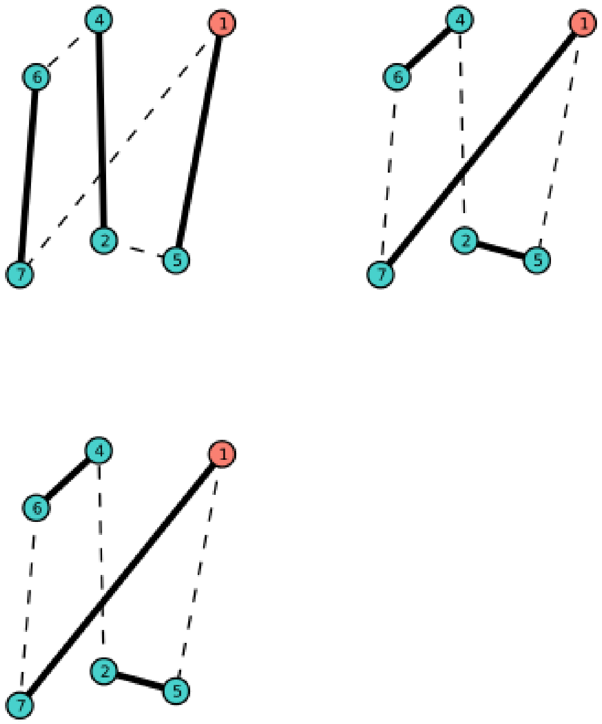
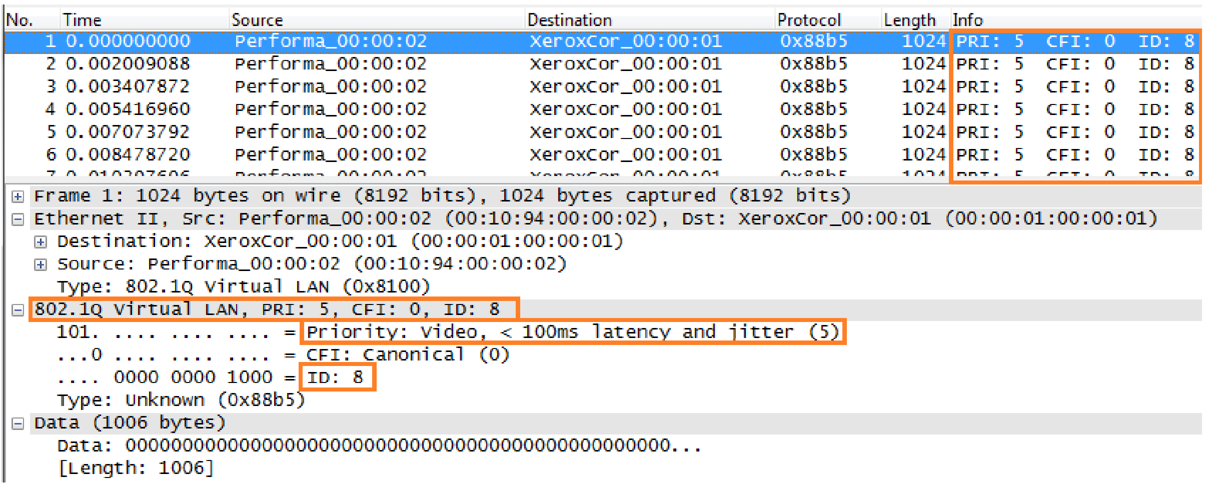


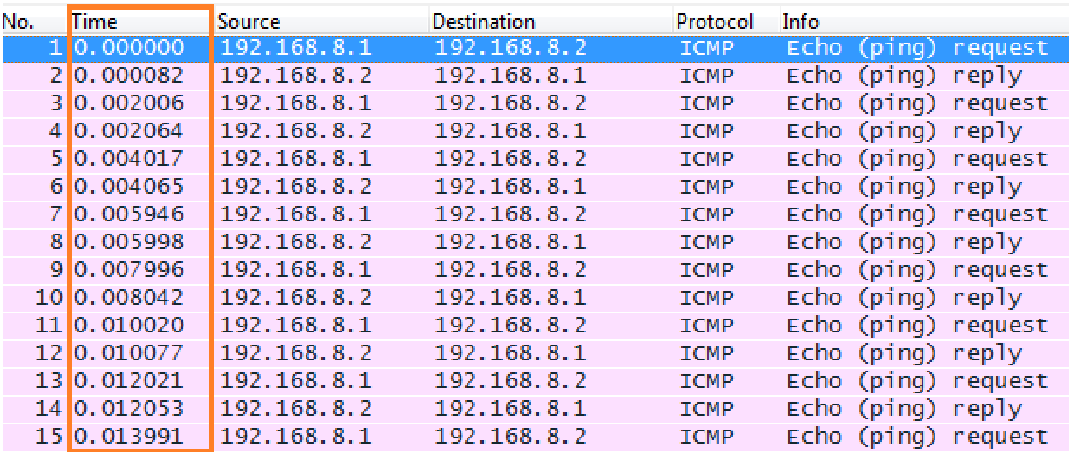
Figure 6.5: Link-schedule for test topology.



```
No.  Time          Source              Destination         Protocol  Length  Info
   1 0.000000000   Performa_00:00:02   XeroxCor_00:00:01   0x88b5      1024  PRI: 5  CFI: 0  ID: 8
   2 0.002009088   Performa_00:00:02   XeroxCor_00:00:01   0x88b5      1024  PRI: 5  CFI: 0  ID: 8
   3 0.003407872   Performa_00:00:02   XeroxCor_00:00:01   0x88b5      1024  PRI: 5  CFI: 0  ID: 8
   4 0.005416960   Performa_00:00:02   XeroxCor_00:00:01   0x88b5      1024  PRI: 5  CFI: 0  ID: 8
   5 0.007073792   Performa_00:00:02   XeroxCor_00:00:01   0x88b5      1024  PRI: 5  CFI: 0  ID: 8
   6 0.008478720   Performa_00:00:02   XeroxCor_00:00:01   0x88b5      1024  PRI: 5  CFI: 0  ID: 8
   7 0.010207606   Performa_00:00:02   XeroxCor_00:00:01   0x88b5      1024  PRI: 5  CFI: 0  ID: 8
⊞ Frame 1: 1024 bytes on wire (8192 bits), 1024 bytes captured (8192 bits)
⊟ Ethernet II, Src: Performa_00:00:02 (00:10:94:00:00:02), Dst: XeroxCor_00:00:01 (00:00:01:00:00:01)
  ⊞ Destination: XeroxCor_00:00:01 (00:00:01:00:00:01)
  ⊞ Source: Performa_00:00:02 (00:10:94:00:00:02)
    Type: 802.1Q Virtual LAN (0x8100)
⊟ 802.1Q Virtual LAN, PRI: 5, CFI: 0, ID: 8
    101. .... .... .... = Priority: Video, < 100ms latency and jitter (5)
    ...0 .... .... .... = CFI: Canonical (0)
    .... 0000 0000 1000 = ID: 8
    Type: Unknown (0x88b5)
⊟ Data (1006 bytes)
    Data: 000000000000000000000000000000000000000000000000...
    [Length: 1006]
```

Figure 6.6: Packet captured in Spirent test center.

Figure 6.6 shows the traffic received at the receiving port of Spirent test center. The reception of transmitted packets with proper mapping of VLANID and priority value as seen in Figure 6.6 verifies the correctness of the routing information. Furthermore, traffic with undefined VLANID was sent but was not received at the receiving port of the Spirent test center. Hence, the routing mechanism works as expected. In order to verify the link-schedule information, the client ports of node 1 and node 6 are connected to a Linux PC with VLANID configured to the value mentioned in WCC configuration file. The configured length of a transmission slot is 200 microseconds. This value is chosen because of the delay and throughput requirements laid down for 4G and 5G mobile networks. A longer transmission slot defies the delay requirement whereas in the case of a shorter slot, the throughput of data transmission is affected.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.8.1	192.168.8.2	ICMP	Echo (ping) request
2	0.000082	192.168.8.2	192.168.8.1	ICMP	Echo (ping) reply
3	0.002006	192.168.8.1	192.168.8.2	ICMP	Echo (ping) request
4	0.002064	192.168.8.2	192.168.8.1	ICMP	Echo (ping) reply
5	0.004017	192.168.8.1	192.168.8.2	ICMP	Echo (ping) request
6	0.004065	192.168.8.2	192.168.8.1	ICMP	Echo (ping) reply
7	0.005946	192.168.8.1	192.168.8.2	ICMP	Echo (ping) request
8	0.005998	192.168.8.2	192.168.8.1	ICMP	Echo (ping) reply
9	0.007996	192.168.8.1	192.168.8.2	ICMP	Echo (ping) request
10	0.008042	192.168.8.2	192.168.8.1	ICMP	Echo (ping) reply
11	0.010020	192.168.8.1	192.168.8.2	ICMP	Echo (ping) request
12	0.010077	192.168.8.2	192.168.8.1	ICMP	Echo (ping) reply
13	0.012021	192.168.8.1	192.168.8.2	ICMP	Echo (ping) request
14	0.012053	192.168.8.2	192.168.8.1	ICMP	Echo (ping) reply
15	0.013991	192.168.8.1	192.168.8.2	ICMP	Echo (ping) request

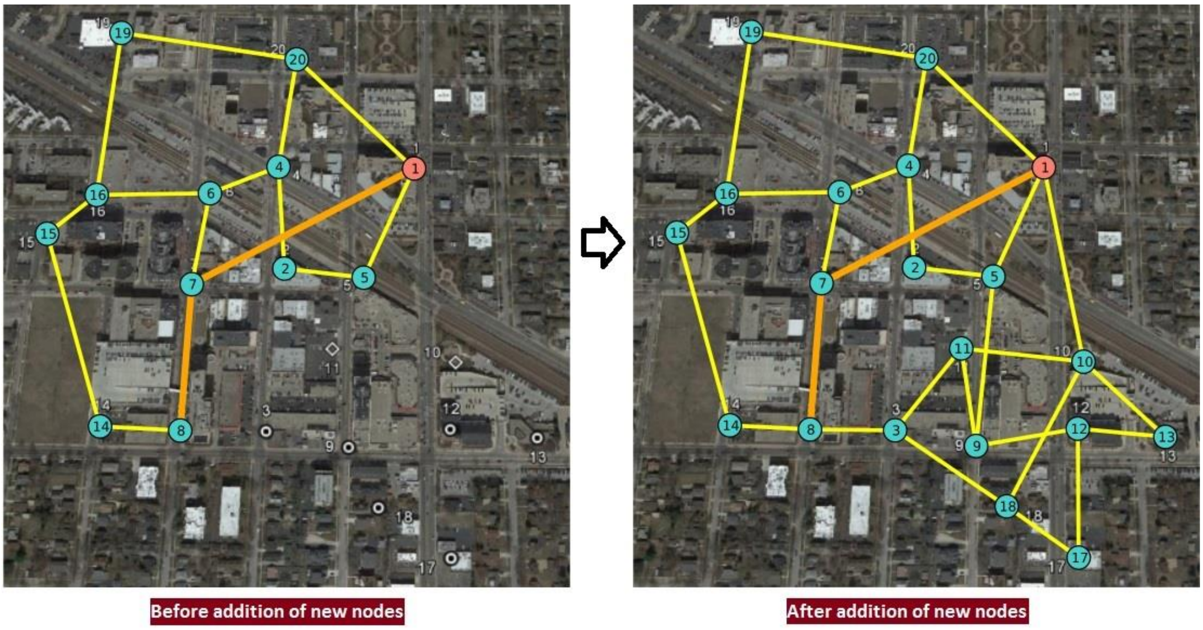
Figure 6.7: Packet captured for link-schedule verification in Wireshark.

For purpose of testing, ping utility is used in a Linux machine connected to node 1 to send traffic with an interval of 200 microseconds. The received packets at node 6 are sniffed using Wireshark tool. From the computed link-schedule information in Figure 6.5, we can deduce that data transmitted from node 1 takes 3-4 transmission slots plus an additional control slot in the schedule to reach node 6. Hence, a packet transmission must occur in around 1 millisecond intervals. Thus, from the packet timestamps in Figure 6.7 we observe that transmission of ping packets occurs in about 1 millisecond with a slight deviation of few microseconds. The deviation is mainly caused due to timing inaccuracies between the Lanner MR-730 unit and the Linux PC. Overall, the link-schedule computed by the WCC and the scheduling mechanism work according to the SWMN concept in the demonstrator system.

6.2 Node addition/deletion

Results of nodes insertion/removal with ongoing traffic in mesh network

This test case is a typical scenario during deployment of base stations wherein there is an already established network infrastructure. Additionally, traffic is flowing in this network and new base stations are added to improve the coverage or offload the data traffic. In the case of node removal, the test case resembles a base station failure scenario or manual shutdown of base stations for energy saving. The addition of new nodes or removal of existing nodes is expected to not cause disturbance in the traffic flowing in the network. Additionally, all the added/removed nodes must be detected and included/excluded in/from topology management procedures such as topology optimization, and route and link-schedule computations. The verification process involves making traffic measurements during node insertion/removal and detection of all the nodes inserted/removed to/from the network respectively.


Before addition of new nodes

After addition of new nodes

Figure 6.8: Topology visualization showing the new nodes added into the mesh network.

To execute this test case, the initial test topology is setup by powering up the nodes and connecting them according to the given test topology. Once the initial topology is setup, the client ports of node 1 and node 8 Lanner MR-730 units are connected to the configured transmitting and receiving ports of Spirent test center. In the next step, the traffic in Spirent test center is configured with a data rate of 40 Mbps, priority of H2 (e.g. video) i.e. PCP value is 101 and VLANID of 10. Finally, traffic is measured for the duration of 60 seconds before and after nodes insertion/removal. Figure 6.8 shows the inclusion of newly added nodes into the active topology computed by the WCC which is depicted through the WCC visualization tool. The inclusion or exclusion of nodes in the active topology verifies that the nodes are included or excluded in the route and link-schedule computation.

Trial 1	**Measurement before addition of new nodes**	**Measurement after addition of new nodes**
Transmitted frames	287357	287357
Received frames	287357	287357
Dropped frames (%)	0	0
Average latency (microseconds)	983.713	1066.25
Minimum latency (microseconds)	357.01	515.99
Maximum latency (microseconds)	6675.77	19394.83
Trial 2		
Transmitted frames	287357	287357
Received frames	287357	287357
Dropped frames (%)	0	0
Average latency (microseconds)	1075.833	1229.135
Minimum latency (microseconds)	429.12	518.11
Maximum latency (microseconds)	6466.85	20217.91

Table 6.1: Traffic statistics from Spirent test center before and after insertion of new nodes.

It can be seen from the Table 6.1 that no packets are dropped during node insertion but there is a huge rise in the maximum latency in the measurements taken after node insertion. This is due to the peak delay caused during the broadcast of the new configuration message from WCC to all the nodes.

Similar to the node addition scenario, in the node removal scenario the nodes are removed from the network while the traffic is flowing in the SWMN network. Figure 6.9 represents the active topology from the WCC visualization tool verifying the exclusion of removed nodes from the network.

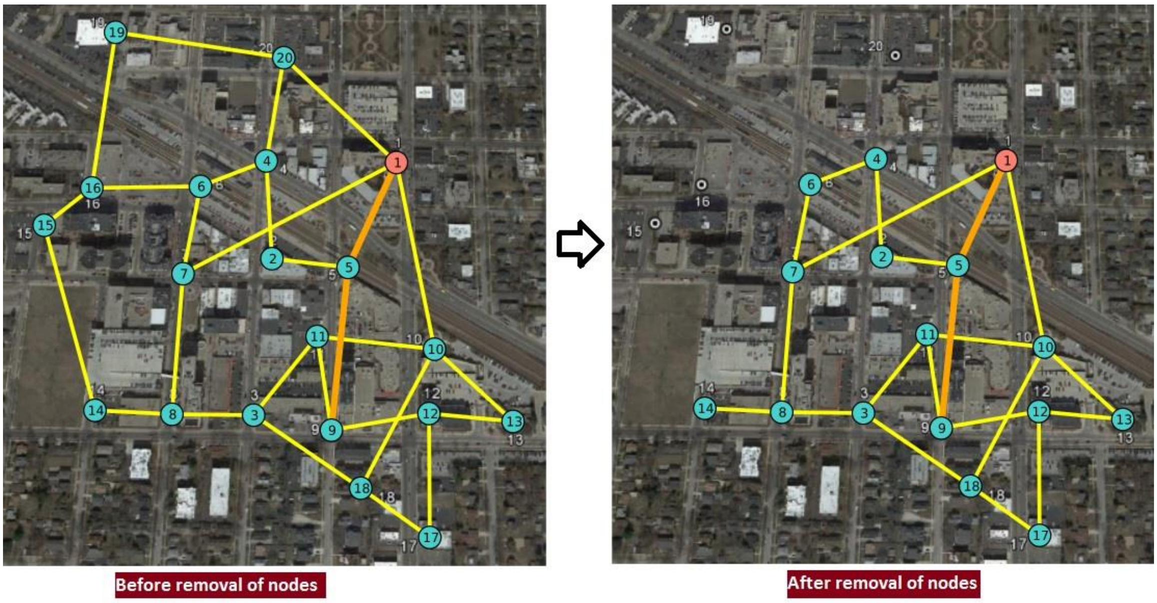


Figure 6.9: Topology verifying the removal of nodes from the mesh network.

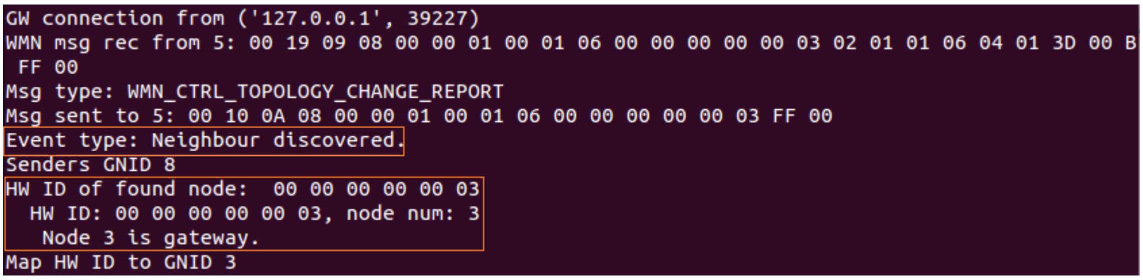
Trial 1	**Measurement before node removal**	**Measurement after node removal**
Transmitted frames	287357	287357
Received frames	287357	287357
Dropped frames (%)	0	0
Average latency (microseconds)	1176.015	1238.885
Minimum latency (microseconds)	516.9	599
Maximum latency (microseconds)	10348.96	19309.96
Trial 2		
Transmitted frames	287357	287357
Received frames	287357	287357
Dropped frames (%)	0	0
Average latency (microseconds)	1140.862	1228
Minimum latency (microseconds)	513.89	463.25
Maximum latency (microseconds)	11002.42	23794.76

Table 6.2: Traffic statistics from Spirent test center before and after removal of nodes.

For testing, the client ports of node 1 and node 9 are connected to Spirent test center and traffic is configured with the parameters used for the node addition scenario but with H3 (PCP value of 100) traffic priority class and VLANID of 11. The traffic measurements in Table 6.2 proves that ongoing traffic is unaffected by the removal of nodes from the mesh network by resulting in no packet loss. However, there is variation in the maximum latency before and after node removal due to the delay caused in distributing the new configuration message. The new configuration is always re-computed by the WCC due to the network topology change such as removal of node as in this test case. Thus it can be concluded that the topology manager works as expected when nodes are added into the network or removed from the network.

Results of gateway node insertion

Validation of the topology management functions during new gateway node insertion involves verifying the detection of newly inserted gateway node by the WCC, inclusion of new gateway in route and schedule computation and depicting the topology change in the visualization. This test case is verified using the simulator with initial test topology as shown in the Figure 5.5. The initial test topology is setup using a text file containing scheduled node and link addition events given as an input to the simulator. The simulator executes these events in the defined chronological order which is reflected in the visualization. This process can also be accomplished by manually creating the topology using the interactive GUI provided by the simulator. Once the initial test topology is created, a new gateway node is inserted using the input file with a properly timed node addition event which contains the node’s coordinates in the topology, event time, node type. Alternatively, the gateway can be added in the simulator GUI by clicking with keyboard key combinations on the point where the node is to be inserted. Following this step, the topology manager must be able to detect the new gateway node, which can be seen in the WCC log messages as shown in Figure 6.10.



```
GW connection from ('127.0.0.1', 39227)
WMN msg rec from 5: 00 19 09 08 00 00 01 00 01 06 00 00 00 00 00 03 02 01 01 06 04 01 3D 00 B
 FF 00
Msg type: WMN_CTRL_TOPOLOGY_CHANGE_REPORT
Msg sent to 5: 00 10 0A 08 00 00 01 00 01 06 00 00 00 00 00 03 FF 00
Event type: Neighbour discovered.
Senders GNID 8
HW ID of found node:  00 00 00 00 00 03
  HW ID: 00 00 00 00 00 03, node num: 3
   Node 3 is gateway.
Map HW ID to GNID 3
```

Figure 6.10: WCC log message indicating the detection of new gateway with HWID 3 inserted to the mesh network.

Upon detecting the topology change, the topology manager re-configures the network after re-calculating the active topology, routes and schedule information by taking the new gateway node into account. Figure 6.11 shows the change in topology with the gateway node with Hardware ID (HWID) 3 appearing in the re-configured active topology.

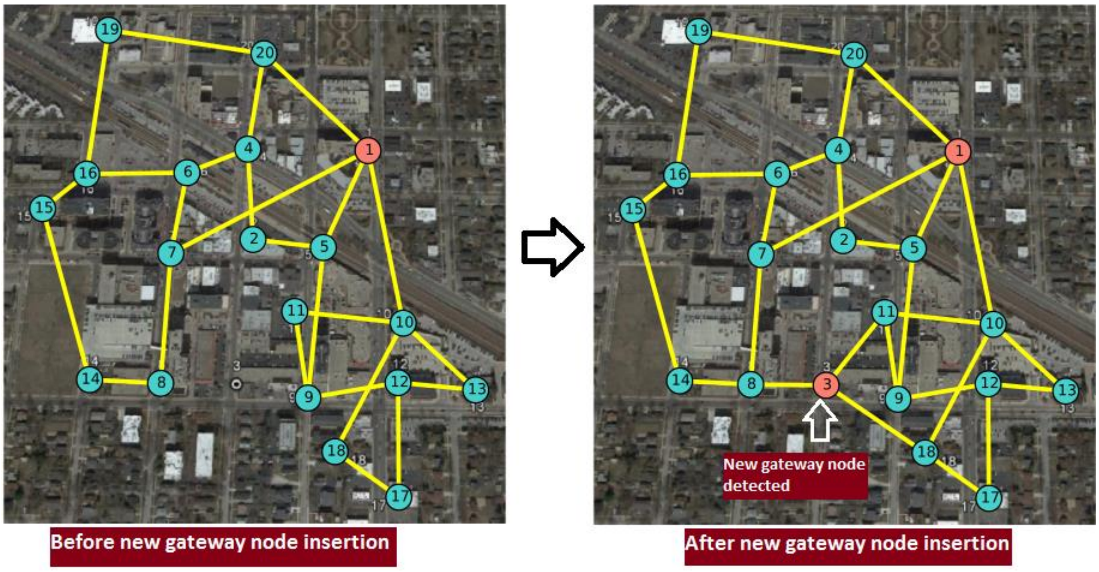
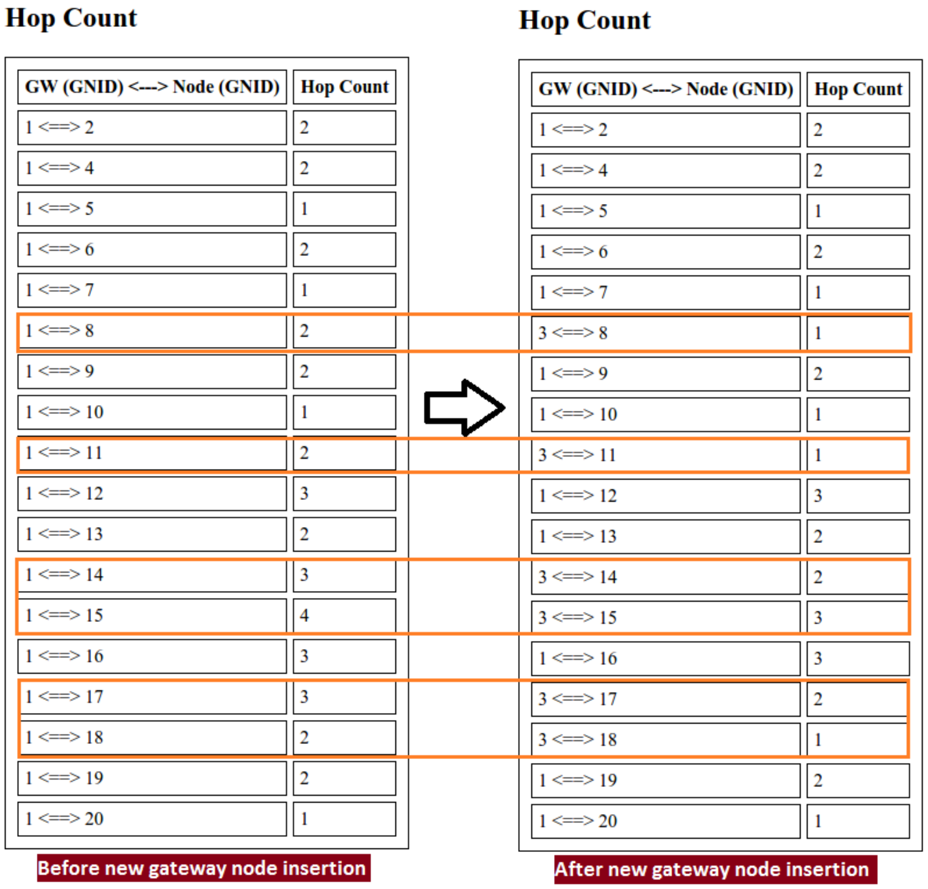

19
20
1
4
16
6
15
7
2
5
11
10
14
8
9
12
13
18
17
3
New gateway node detected
Before new gateway node insertion
After new gateway node insertion

Figure 6.11: WCC visualization depicting the change in topology due to new gateway insertion.

Furthermore, this test case also validates the ability of the topology manager to take advantage of the newly inserted gateway node to optimize the routes and schedules between the SWMN nodes. This can be verified from Figure 6.12 that shows the difference between the number of hops taken for communication between the nodes before and after the new gateway node insertion. Thus, topology management functions performed due to gateway node insertion work as expected.



Hop Count

GW (GNID) <---> Node (GNID)	Hop Count
1 <==> 2	2
1 <==> 4	2
1 <==> 5	1
1 <==> 6	2
1 <==> 7	1
1 <==> 8	2
1 <==> 9	2
1 <==> 10	1
1 <==> 11	2
1 <==> 12	3
1 <==> 13	2
1 <==> 14	3
1 <==> 15	4
1 <==> 16	3
1 <==> 17	3
1 <==> 18	2
1 <==> 19	2
1 <==> 20	1

Before new gateway node insertion

Hop Count

GW (GNID) <---> Node (GNID)	Hop Count
1 <==> 2	2
1 <==> 4	2
1 <==> 5	1
1 <==> 6	2
1 <==> 7	1
3 <==> 8	1
1 <==> 9	2
1 <==> 10	1
3 <==> 11	1
1 <==> 12	3
1 <==> 13	2
3 <==> 14	2
3 <==> 15	3
1 <==> 16	3
3 <==> 17	2
3 <==> 18	1
1 <==> 19	2
1 <==> 20	1

After new gateway node insertion

Figure 6.12: Change in the hop count between SWMN nodes due to new gateway inserted into network.

Results of gateway node removal

The test case aims at validating the topology management function in case of gateway node failure. In a network that contains two gateways, if one of the gateways fails, only the remaining gateway must be taken into consideration for topology optimization, route and link-schedule computation. The verification of topology management functions performed during gateway node failure includes detection of the failure, comparing routes computed by the WCC before and after removing one of the gateway nodes and transition of auxiliary gateway to primary gateway in the simulator visualization.

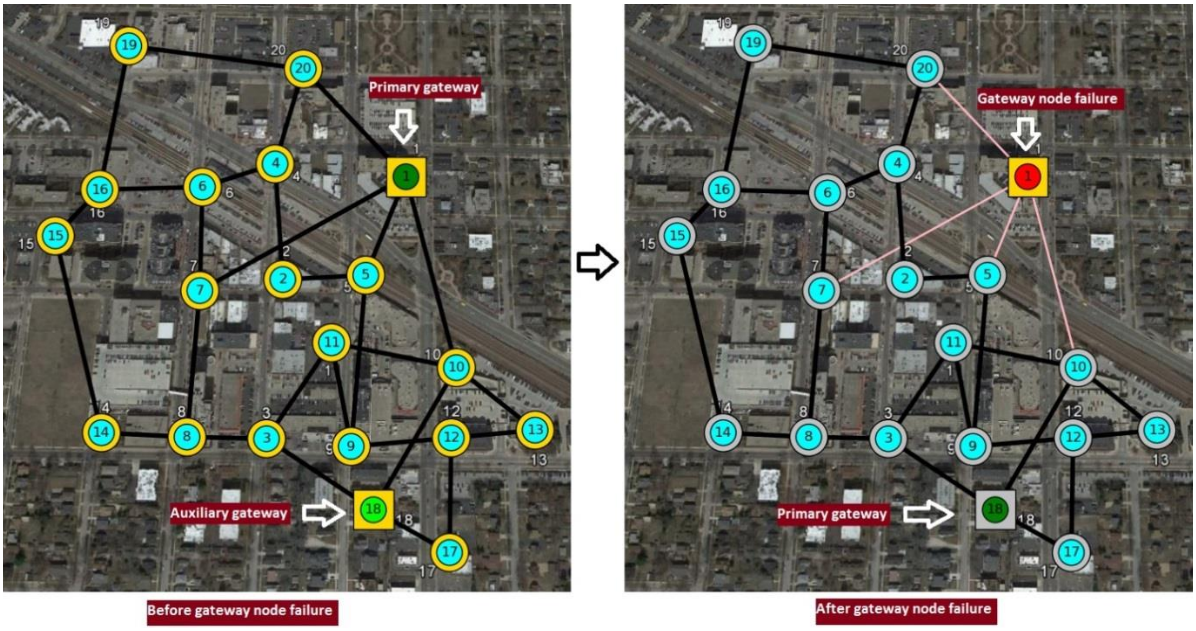


Figure 6.13: Simulator visualization depicting the gateway node failure in the network.

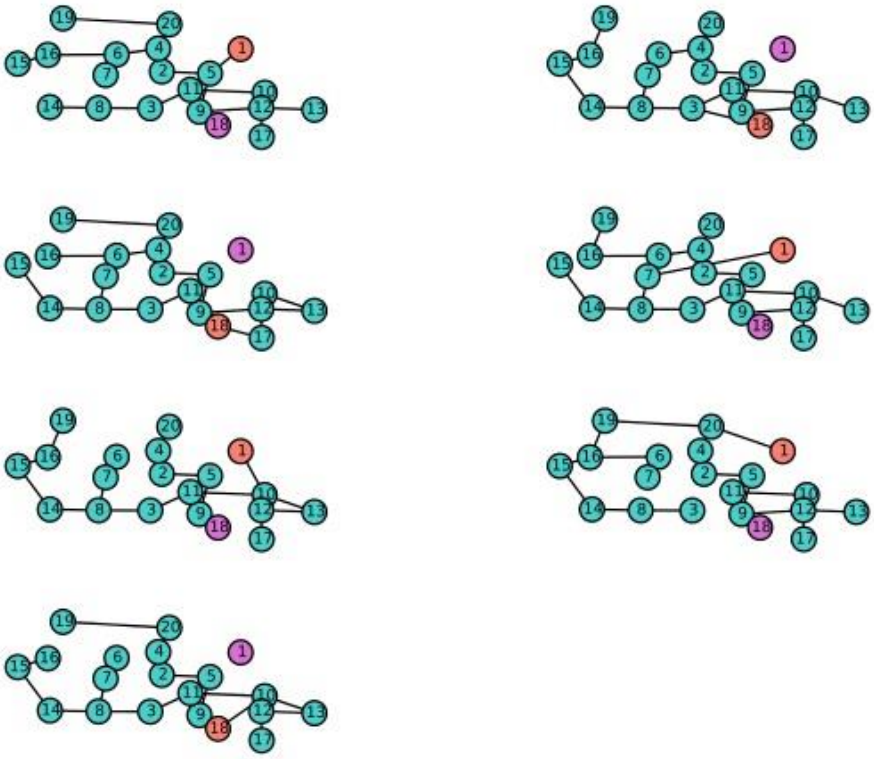


Figure 6.14: Alternative set of routes generated before gateway node removal.

The initial test topology provided in Chapter 5 for the gateway node removal is set up in a similar way as for gateway addition scenario. Upon setting up the initial topology in the simulator, the primary gateway (node 1) is removed from the topology. In Figure 6.13, the colored rings and squares around the nodes represent the domain to which the node belongs to. Also, the gateway nodes are differentiated from generic nodes by being represented as green nodes enclosed inside a colored square. It can be inferred from the simulator visualization that the auxiliary gateway takes the role of primary gateway upon existing primary gateway failure. The generated set of routes for the gateway node in Figure 6.14 and 6.15 can also be used to verify this test case scenario.

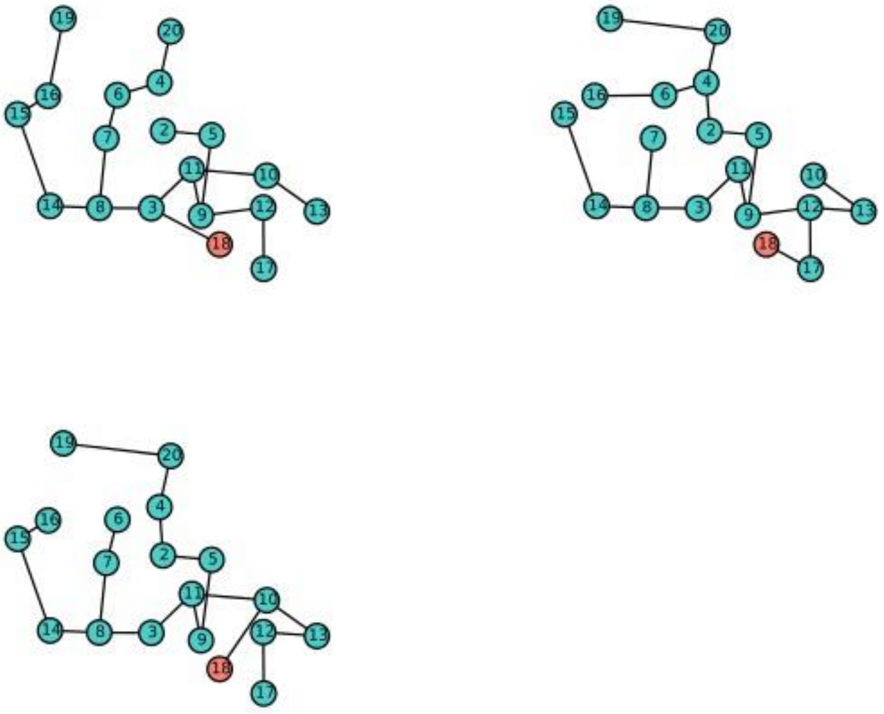


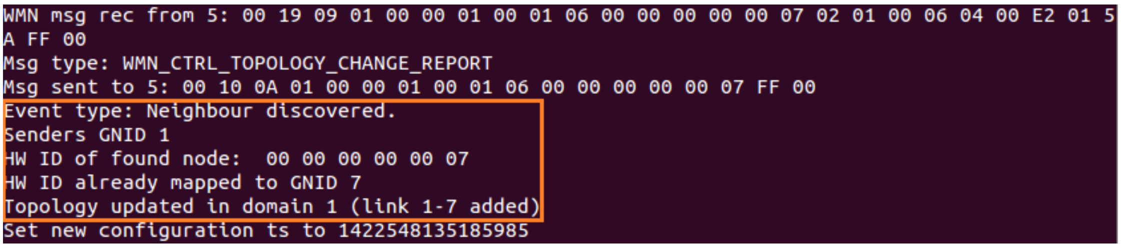
Figure 6.15: Alternative set of routes generated after primary gateway node removal.

In Figure 6.14, we observe that the routes were generated including the auxiliary gateway as part of route and topology optimization mechanisms but once the primary gateway is removed, the alternative set of routes generated contain routes originating only from the auxiliary gateway (node 18) as shown in Figure 6.15. This verifies detection of gateway node failure by the topology manager. Thus, the WCC is effective in handling the gateway node failure scenarios and works according to the concept.

6.3 Link addition/deletion

Result of testing inclusion of a link into active topology when discovering a new link

This test scenario serves as a mean to verify the topology optimization feature of WCC. The test case involves setting up the topology optimization parameters and adding a new link between two SWMN nodes already existing in the mesh network in such a way that topology optimizer includes the new link into active topology. Once the new link is added to active topology, the link can be scheduled for data transmission at times mentioned in the recomputed link-schedule information. The verification process involves examining the active topology and the WCC log messages to validate the new link addition. Initially, the test topology is setup as given in the Figure 5.7, and one of the topology optimization parameters such as the maximum number of links per node is set to 4 in the WCC configuration. In this test case, a new link is added between node 1 and node 7, by injecting a link addition event to the simulator. Here, the number of links in the end nodes is less than the max limit of 4. Thus, it can be assumed that the new link will be included in the active topology after topology optimization.



```
WMN msg rec from 5: 00 19 09 01 00 00 01 00 01 06 00 00 00 00 00 07 02 01 00 06 04 00 E2 01 5
A FF 00
Msg type: WMN_CTRL_TOPOLOGY_CHANGE_REPORT
Msg sent to 5: 00 10 0A 01 00 00 01 00 01 06 00 00 00 00 00 07 FF 00
Event type: Neighbour discovered.
Senders GNID 1
HW ID of found node:  00 00 00 00 00 07
HW ID already mapped to GNID 7
Topology updated in domain 1 (link 1-7 added)
Set new configuration ts to 1422548135185985
```

Figure 6.16: WCC log message indicating the new link added to the topology.

From Figure 6.16 it can be observed that WCC detects the new link added through a TCR sent by node 1 to WCC. Upon detection of change in physical topology, the physical topology is fed as an input to topology optimizer to calculate the active topology and the result of this can be observed in Figure 6.17. Thus, it can be seen that the new link is included into active topology and the topology optimizer module works as expected.

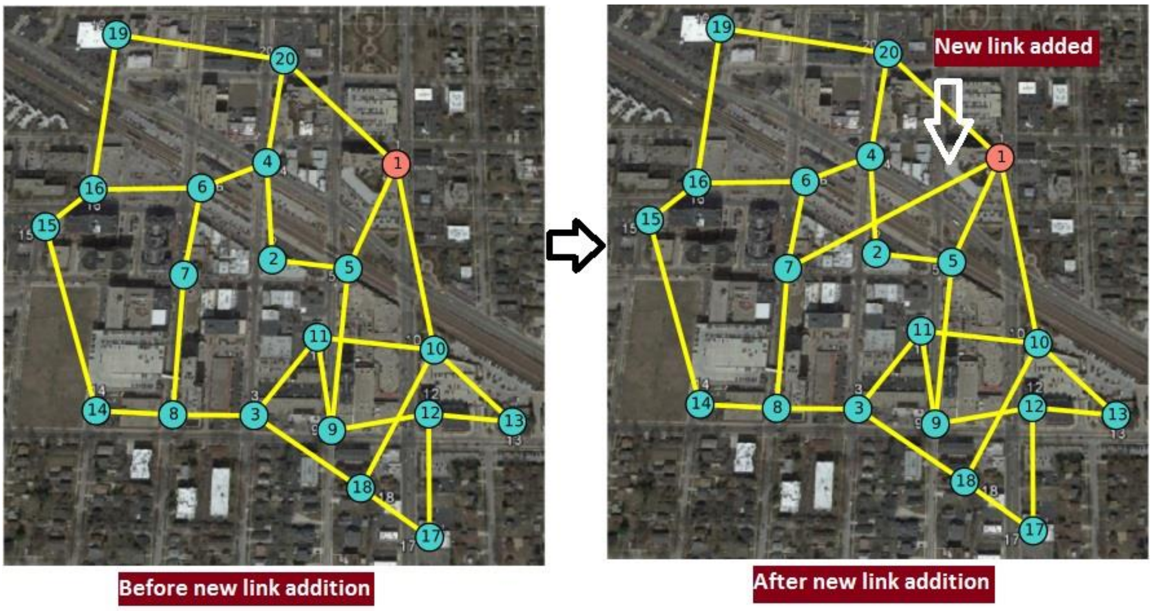
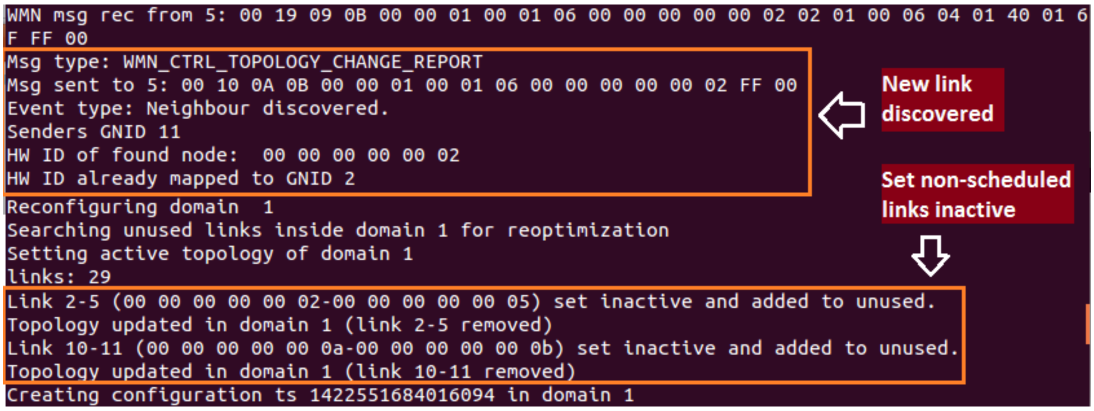


Figure 6.17: Change in active topology visualization due to new link addition.

Result of testing exclusion of a link from active topology when discovering a new link

This test case validates the topology optimization module by forcing the topology optimizer to optimize the links per node that can be active. Similar to link addition scenario, the initial network topology is built up according to the test topology given in Figure 5.8 and the optimization parameter of maximum number of links per node is set to 4. In the next step, a new link is added between existing SWMN nodes (node 2 and node 11), by injecting a link addition event to the simulator. It can be observed from the topology before link addition that node 2 and node 11 have the number of outgoing links equal to 4. Hence, adding an additional link between these nodes forces the topology optimizer to optimize the topology in such a way that the number of outgoing links in each node remains within the maximum limit of 4. The topology manager keeps track of the non-scheduled links i.e. links not included in the active topology and may re-activate these dormant links based on further changes in the topology, traffic conditions in the network and other network optimization parameters.



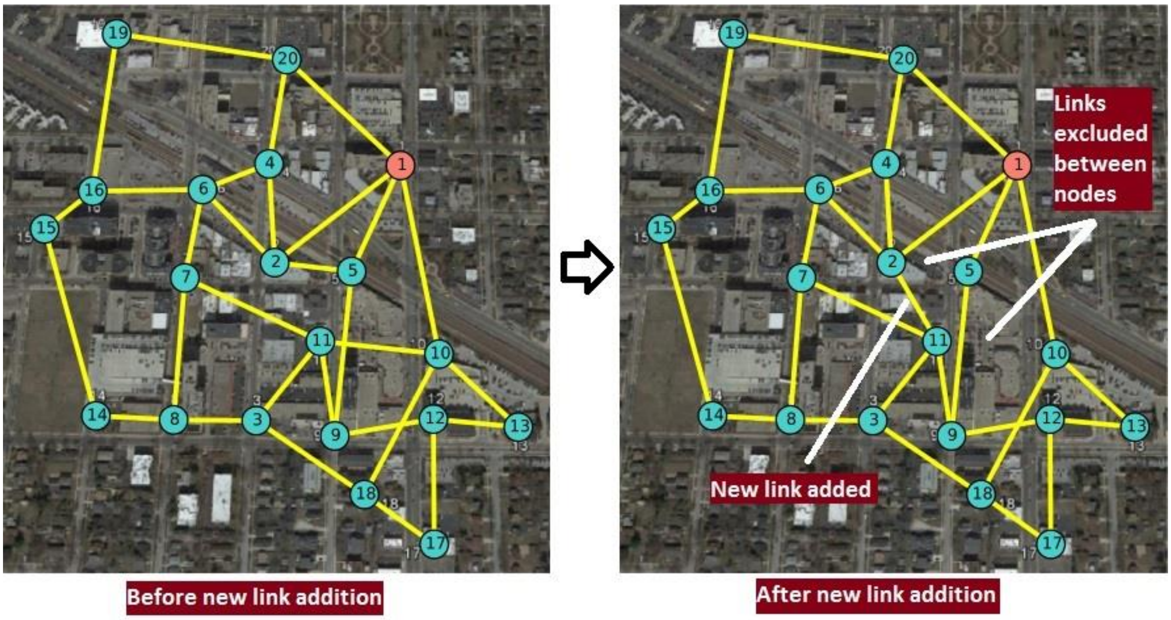
```
WMN msg rec from 5: 00 19 09 0B 00 00 01 00 01 06 00 00 00 00 00 02 02 01 00 06 04 01 40 01 6
F FF 00
Msg type: WMN_CTRL_TOPOLOGY_CHANGE_REPORT
Msg sent to 5: 00 10 0A 0B 00 00 01 00 01 06 00 00 00 00 00 02 FF 00
Event type: Neighbour discovered.
Senders GNID 11
HW ID of found node:  00 00 00 00 00 02
HW ID already mapped to GNID 2
Reconfiguring domain  1
Searching unused links inside domain 1 for reoptimization
Setting active topology of domain 1
links: 29
Link 2-5 (00 00 00 00 00 02-00 00 00 00 00 05) set inactive and added to unused.
Topology updated in domain 1 (link 2-5 removed)
Link 10-11 (00 00 00 00 00 0a-00 00 00 00 00 0b) set inactive and added to unused.
Topology updated in domain 1 (link 10-11 removed)
Creating configuration ts 1422551684016094 in domain 1
```

New link discovered

Set non-scheduled links inactive

Figure 6.18: WCC log messages indicating de-activation of link between nodes.

The verification of topology optimization involves examining the active topology visualization, WCC log messages indicating the links not included in the route and schedule re-computation and simulator topology depicting physical and active topology. As can be inferred from Figure 6.18, the new link added between node 2 and node 11 is detected but after re-optimization of topology, the link between node 2 and node 5 and also the link between node 10 and node 11 are excluded from active topology.



Before new link addition

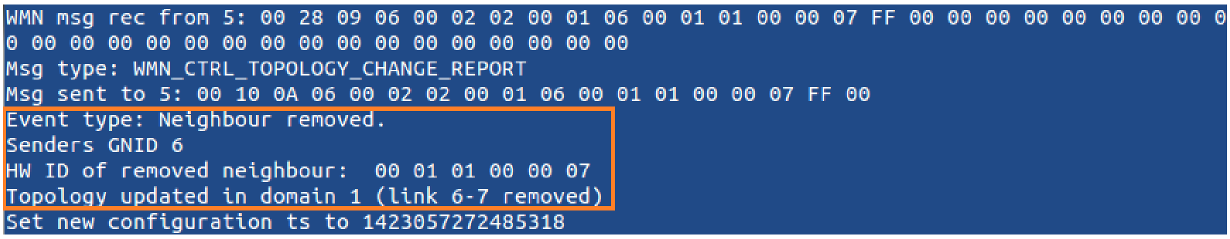
After new link addition

Figure 6.19: WCC visualization depicting the topology optimization due to addition of new link.

Figure 6.19, presents the change in the topology after addition of a new link between node 2 and node 11 resulting in network re-optimization. It can be observed from the topology diagram that the number of outgoing links in node 2 and node 11 is maintained at the configured maximum limit. Thus, it can be deduced that topology optimization mechanism correctly adheres to the maximum links per node as one of the optimization parameters.

Results of link removal between nodes with ongoing traffic in the link

This test scenario targets the case of prolonged or very frequent link breaks which requires the topology manager to intervene and re-compute and re-optimize the routing and schedule information. The verification of topology management procedures during link-breaks involves introducing a link break in a stable network and observing the re-configured topology. Furthermore, to measure the effect on traffic in the network while responding to link-breaks, traffic with low data rate is transmitted in the link which undergoes the link-break. For this test case, the emulation demonstrator platform is used with the initial topology given in Figure 5.9. The client ports of node 1 and node 6 are connected to transmitting and receiving ports of Spirent test center and L1 priority traffic of 20 Mbps data rate and with VLANID 8 is introduced for the duration of 120 seconds. Upon introducing the traffic in the link, a link break is created by unplugging the Ethernet cable between node 7 and node 6. The packet loss and delay are measured before and after the link-break.



```
WMN msg rec from 5: 00 28 09 06 00 02 02 00 01 06 00 01 01 00 00 07 FF 00 00 00 00 00 00 00 00 0
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Msg type: WMN_CTRL_TOPOLOGY_CHANGE_REPORT
Msg sent to 5: 00 10 0A 06 00 02 02 00 01 06 00 01 01 00 00 07 FF 00
Event type: Neighbour removed.
Senders GNID 6
HW ID of removed neighbour:  00 01 01 00 00 07
Topology updated in domain 1 (link 6-7 removed)
Set new configuration ts to 1423057272485318
```

Figure 6.20: WCC log messages indicating the link-break between node 6 and node 7.

It can be inferred from Figure 6.20 that the network is effective in detecting and notifying of the link-break through a topology change report sent by node 6. As a result of the topology change, the topology manager re-configures the topology by excluding the broken link from topology optimization, route and schedule re-computation phases. Upon re-configuration, the traffic is re-routed along the new optimum path as seen in Figure 6.21.

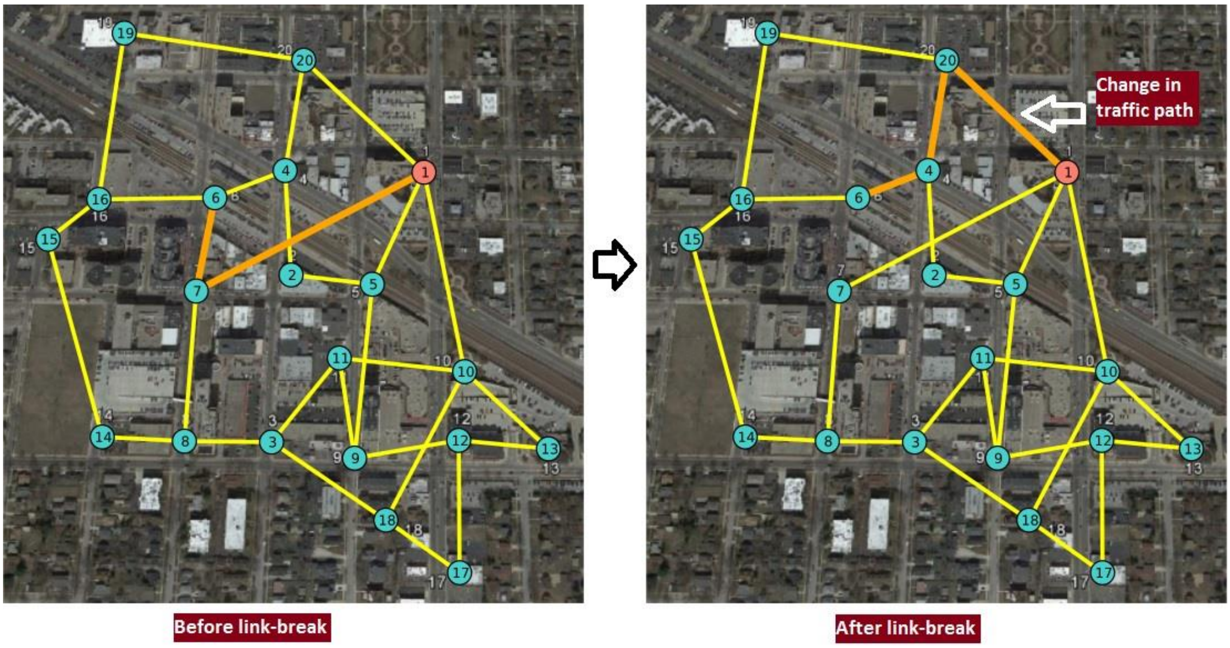


Figure 6.21: Topology visualization before and after link-break between node 6 and node 7.

Trial 1	Measurement before link-break	Measurement after link-break
Transmitted frames	287357	287357
Received frames	287357	285462
Dropped frames (%)	0	0.659
Average latency (microseconds)	1275.169	10448.872
Minimum latency (microseconds)	423.76	643.71
Maximum latency (microseconds)	14461.13	911309.78
Trial 2		
Transmitted frames	287357	287357
Received frames	287357	285489
Dropped frames (%)	0	0.650
Average latency (microseconds)	1184.338	10509.473
Minimum latency (microseconds)	423.31	593.58
Maximum latency (microseconds)	2243.06	911188.59

Table 6.3: Traffic statistics from Spirent test center before and after link-break.

From Table 6.3 we can observe that there is very small amount of dropped frames when there is a link-break. Packet loss is mainly due to delay in detecting Ethernet link-breaks and the timeout concept in the WCC to prevent unnecessary network re-configuration. Another noticeable change in traffic statistics is the huge rise in the mean latency because of peak packet delays occurring immediately when the Ethernet cable is unplugged and also during the network re-configuration. Overall, the link-break detection and the topology management functions due to link-break work as specified.

6.4 Domains split or merge

Result of testing domain splitting

As mentioned in Chapter 5, the SWMN nodes are grouped together forming SWMN domains. This is one of the steps in the topology optimization procedure which depends on an optimization parameter of maximum allowed nodes in a domain. In this test scenario we consider an initial topology with two gateway nodes and the total number of nodes less than the configured value of maximum nodes in a single domain. The initial test topology, shown in Figure 6.22, consists of 35 nodes while the maximum number of nodes under a domain is set to 40 nodes. This initial topology can be created by using the random node deployment feature of the simulator which takes the number of generic nodes, gateway node IDs and gateway node positions as parameters. Furthermore, links between randomly mounted nodes are generated using parameters such as the maximum number of links between nodes, minimum number of neighbors, minimum distance between neighbors and radio range. From Figure 6.22 it can be observed that all the nodes have been circled with a ring having the same color i.e. silver denoting that all the nodes belong to the same domain. In the next step, 6 generic nodes are added to initial topology. This causes the total number of nodes to be greater than the maximum limit in a domain, which results in the split of the domain into two after topology re-optimization. The process of domain splitting can be verified by Figure 6.23 which represents the simulator topology visualization after domain splitting.

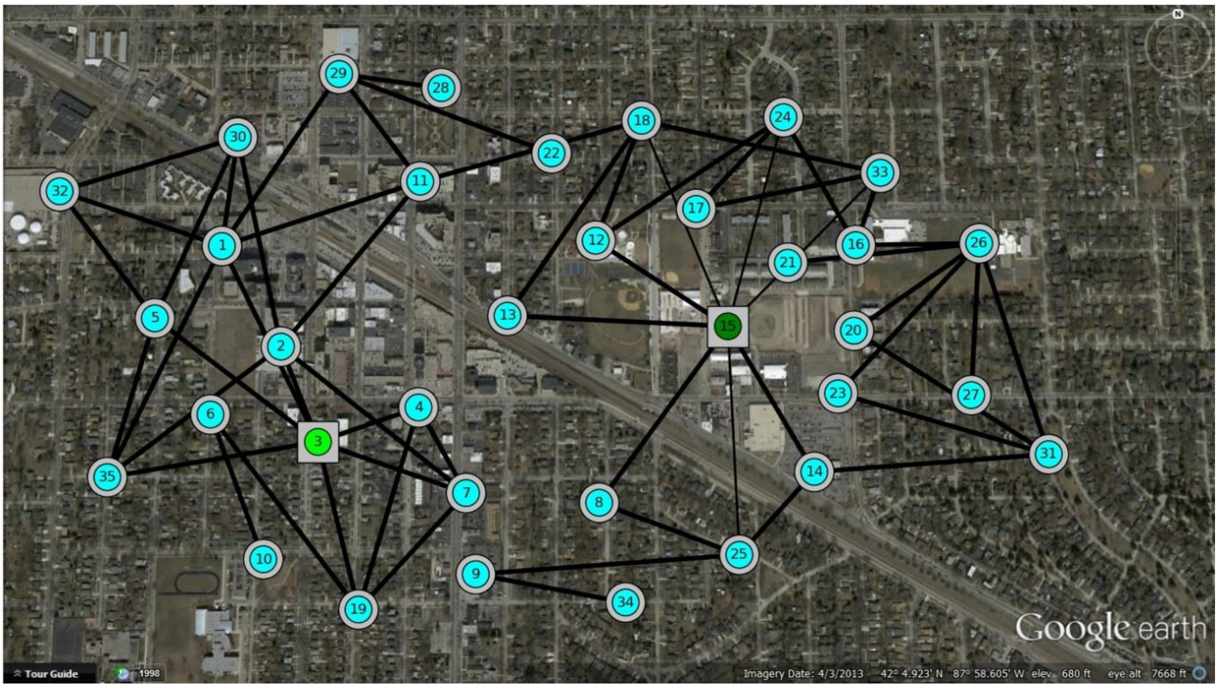


Figure 6.22: Initial topology with single SWMN domain in simulator visualization.

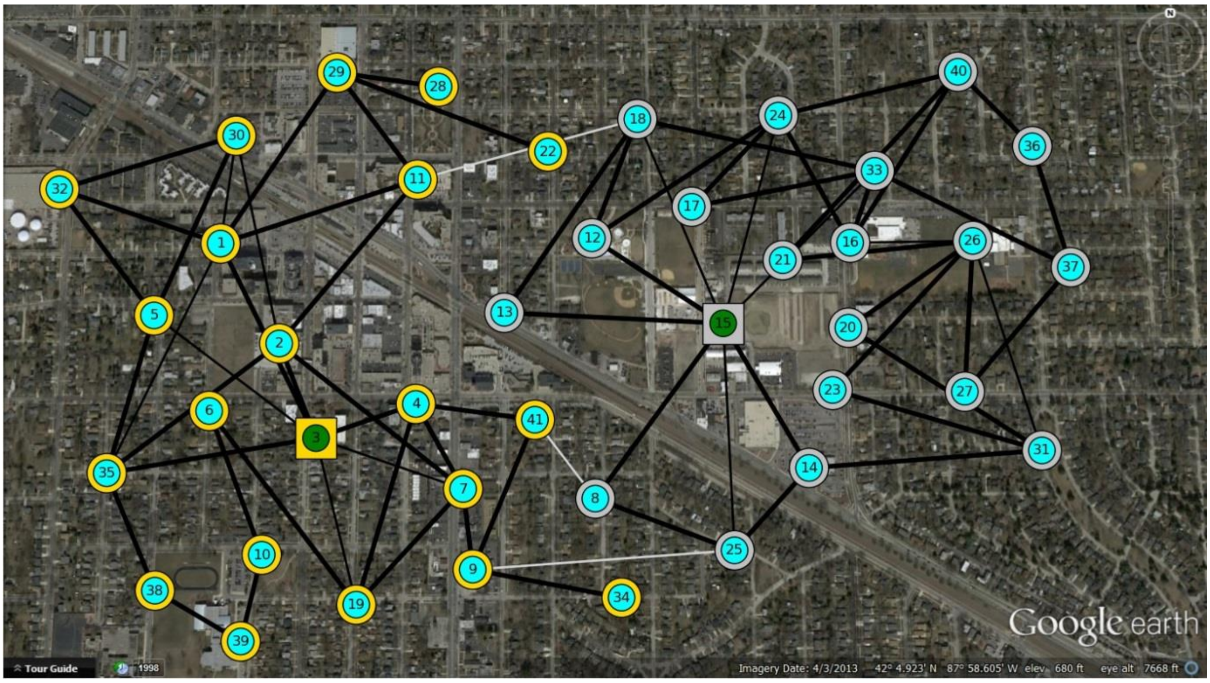


Figure 6.23: Domain split in the simulator topology visualization.

Figure 6.23 presents two SWMN domains differentiated by gold and silver rings around the nodes. All the nodes in with gold-colored rings communicate with WCC through gateway node 3 and have a different set of alternate routing paths and link schedules than the nodes with silver-colored rings. Meanwhile, nodes with silver-colored rings use gateway node 15 to communicate with WCC and vice versa for configuration message distribution. Thus, the operation of splitting up of domain as part of topology optimization works as described.

Result of testing domain merging

Similar to domain splitting, domain merge is also one of the tasks involved in topology optimization if two neighboring domains have the total number of nodes less than the configured maximum number of nodes in a domain. The initial test topology for testing domain merge can be setup more or less the same way as for domain split scenario. However, here the sum of number of nodes in the SWMN area must exceed the maximum domain size. Figure 6.24 shows the initial topology with 41 nodes with the maximum domain size of 40.

In the next step, 6 nodes are removed such that the total number of nodes in both domains combined becomes less than the maximum domain size. This causes the topology optimizer to merge the two domains into a single domain containing two gateway nodes. This can be verified from the topology visualization in the simulator as shown in Figure 6.25. The single-colored domain rings around nodes indicate the process of domain merging.

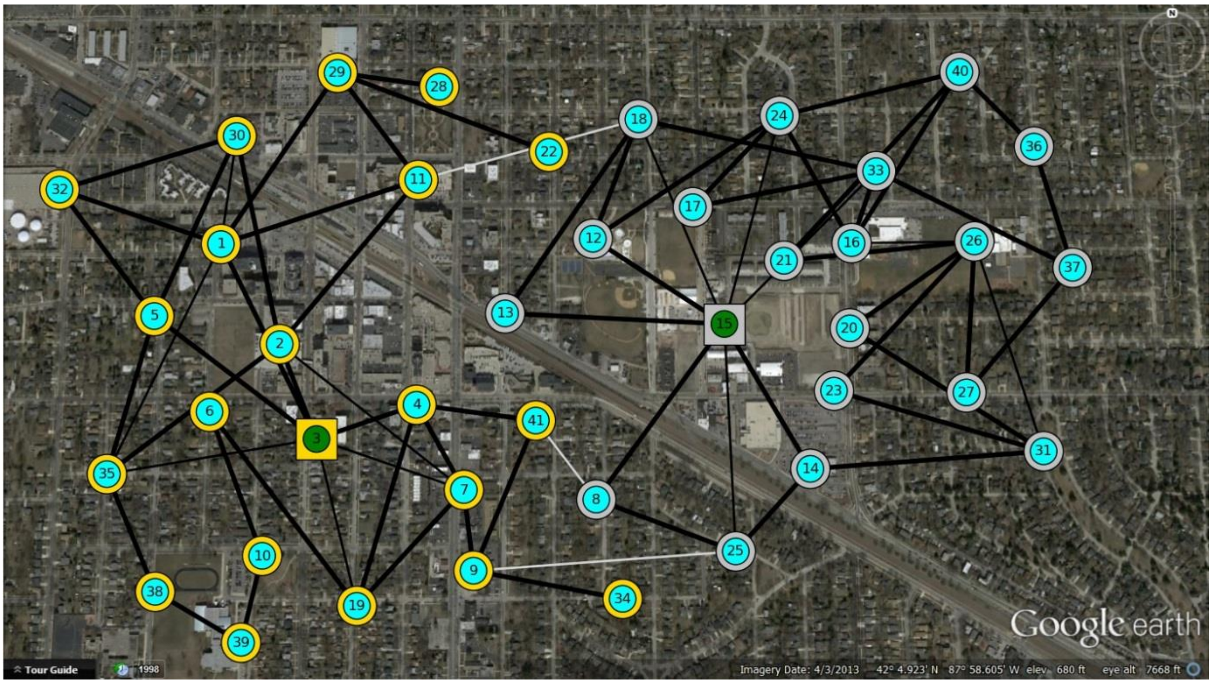


Figure 6.24: Initial topology with two SWMN domains in simulator visualization.

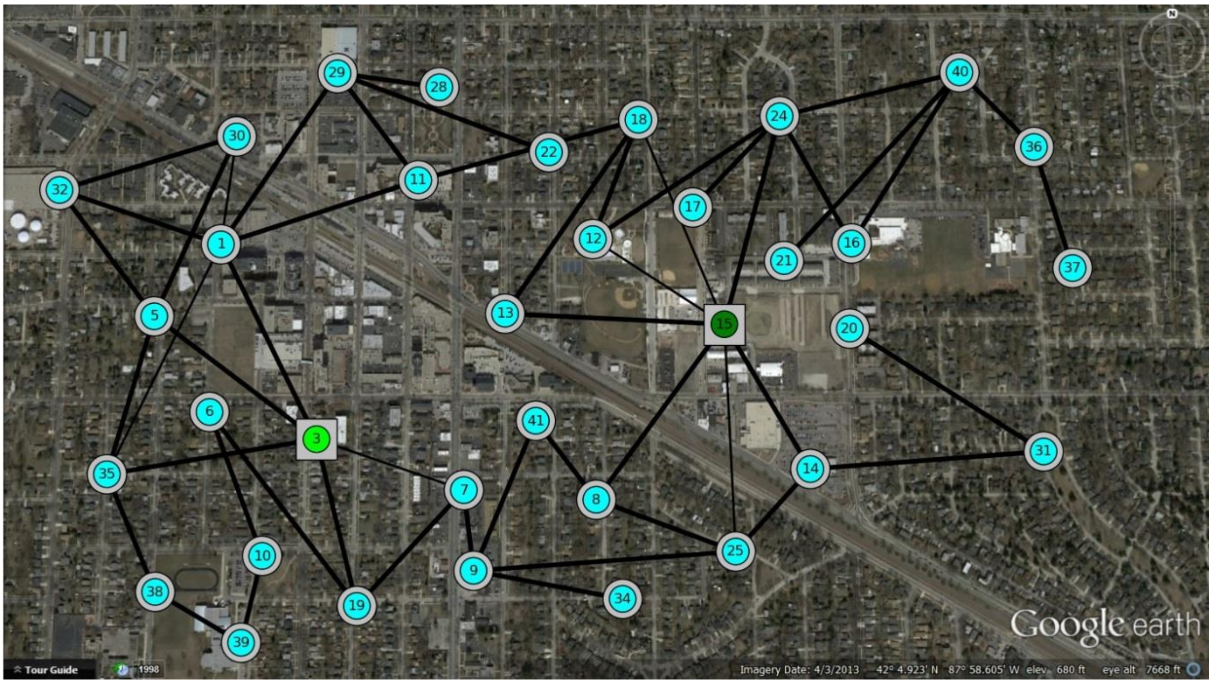


Figure 6.25: Domain merge in the simulator topology visualization.

6.5 Scalability

Results of testing scalability with respect to the number of nodes in a domain

The test scenario aims at validating the scalability in terms of the number of nodes that can be accommodated in a single domain containing one gateway node. The number of nodes in a domain has a direct relation to the configuration message size produced by WCC. In this test case, the maximum number of nodes in a domain is configured to 100 nodes, and the topology is created with a single gateway followed by randomly mounting 100 nodes. Ideally, all the nodes would be included into the domain. But the actual outcome of testing is visualized in Figure 6.26 which presents the topology output in the simulator. In Figure 6.26, it can be observed that all nodes are not configured by the WCC. Since the length of the configuration message produced by the WCC exceeded the maximum value of Ethernet frame size (1500 bytes) causing the topology build to be interrupted. A total of 70 nodes were included in the domain out of the 100 randomly deployed nodes. Additionally, re-computation time of route and link-schedules by WCC increases with the rise in number of nodes in a single domain.

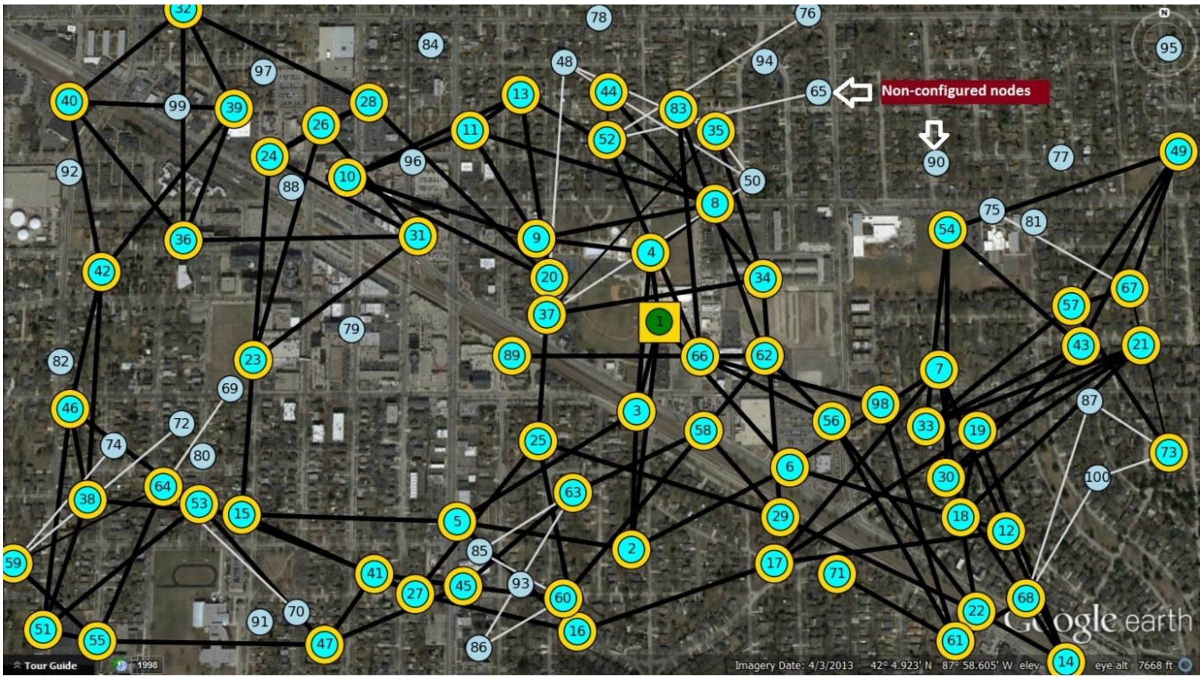
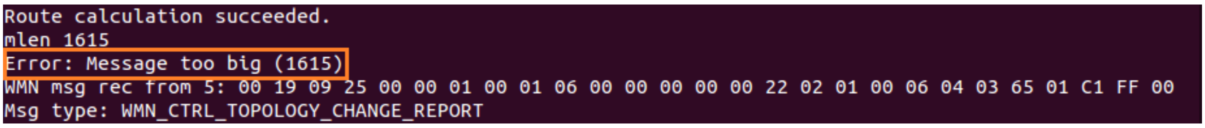


Figure 6.26: Topology visualization in simulator for testing scalability of nodes in a single domain.



```
Route calculation succeeded.
mlen 1615
Error: Message too big (1615)
WMN msg rec from 5: 00 19 09 25 00 00 01 00 01 06 00 00 00 00 00 22 02 01 00 06 04 03 65 01 C1 FF 00
Msg type: WMN_CTRL_TOPOLOGY_CHANGE_REPORT
```

Figure 6.27: WCC log message indicating the error during re-computation of configuration message.

Figure 6.27 presents the error message provided by the WCC in the event of too large configuration message size. However, by increasing the maximum message size in the configuration allows all the nodes to be configured and included in the domain but those setups would not be possible in real SWMN nodes without changing the structure and mechanism of how the new configuration from WCC is distributed to the network nodes. Overall, all the nodes get configured to a single domain as long as the configuration message fits in an Ethernet frame.

Results of testing scalability with respect to number of nodes in a SWMN area

This test case aims at validating the scalability of WCC in handling a large number of domains and nodes in a SWMN area. The verification process involves adding of nodes up to a point where WCC is no longer able to accommodate any more nodes in any of the domains. To test the limit of scalability, the number of randomly deployed generic nodes in the simulator is chosen to be 250. To make it possible for all the nodes to be configured by WCC, a total of 8 gateway nodes are used and the value of maximum nodes in a domain is set to 30. As a result, all the nodes are included in one of the 6 domains formed as shown in Figure 6.28. The domains are represented by gold, silver, white, brown, blue and black colored rings around the nodes. However, the limiting factor in this test case is the Generic Node Id (GNID) numbering scheme implemented in the current WCC PoC SW which restricts the maximum number of nodes in a SWMN area to a value of 255.

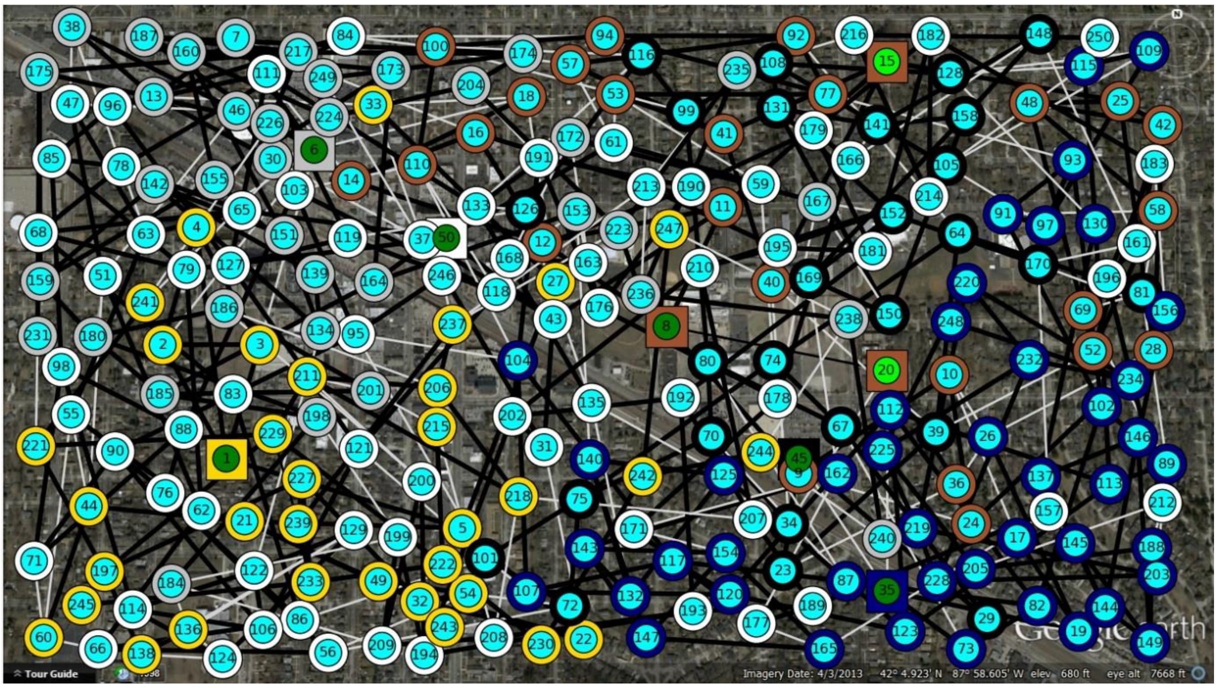

Tour Guide
Imagery Date: 4/3/2013 42° 4.923' N 87° 58.605' W elev 680 ft eye alt 7668 ft
Google earth

Figure 6.28: SWMN area with 250 nodes in simulator topology visualization.

6.6 Discussion and future work

The topology management functionalities of WMN Centralized Controller (WCC) have been properly validated and they work as described in the SWMN concept specifications. For the purpose of testing, both emulation and simulation platforms were used. The errors and inconsistencies found in WCC were used as a baseline for development towards a working product. The emulation platform using the Lanner MR-730 interoperates as intended with the WCC. However, in early stages of testing, minor bugs such as crashing of SWMN nodes due to a large configuration message size and large delays in node detection when using small schedule slot lengths were experienced. However, these bugs were resolved alongside the development of WCC and the PE softwares. The simulator platform was purely developed for extensive validation of topology manager module by mimicking only the control plane functionality of emulator nodes. The PE and WCC PoC code provided was of high quality and well documented. This was possible due to excellent programming efforts by VTT and accurate concept documentation and specification by Nokia Networks.

The overall objective of this testing process was to verify the topology management features supported by WCC during network deployment scenarios e.g. addition of nodes and links, and network changes due to node failures and link breaks. Furthermore, testing was needed to be carried out in traffic scenarios to justify that the concept works with traffic flowing in the network and does not require the traffic to be interrupted due to network expansion or maintenance. The results of the verification have been explained and the reasoning behind the results has been provided.

During the time of writing this thesis, the WCC PoC included modules such as route computation, link-schedule computation, basic topology optimization, network configurator and VC provisioning. With these modules, the WCC provides effective topology management mechanisms features, which facilitates autonomous network build-up and optimized network operation for a 5G mobile backhaul network. The modules which are yet to be defined and implemented in WCC include network status monitors, access control and energy saving control. The increased use of wireless SON techniques for the mobile backhaul requires strict authentication and access control of SWMN nodes being added to the network. The access control must make sure that a new node added is from a trusted source and prevent a rogue node from gaining access to the SWMN and cause harm to the transport and access network. At present, a framework of Authentication, Authorization, and Accounting (AAA) is under consideration for access control.

As mentioned earlier, Link State Update (LSU) messages are used to communicate between the SWMN nodes about the link state. In the current implementation, LSUs report link states but it would be beneficial for network monitoring if LSUs were to report interface specific packet loss, packet delay and jitter. This information could potentially be used by the WCC to estimate the overall traffic distribution and carry out capacity analysis. However, the throughput of network would be affected if all the LSUs were reported. Hence, it is necessary to filter the LSUs at the gateway node before reporting to WCC. As part of OAM scheme, the

WCC could use this information to monitor the network and carry out suitable topology management procedures.

Finally, from the perspective of an operator, there is a need for minimizing the energy costs. Therefore, effective energy saving mechanisms need to be implemented which help in reducing the power consumption by putting the least burdened nodes and links to sleep, and activating them when there is a demand. This leads to a challenge of developing smart energy saving algorithms that takes the network state as a parameter and go on to decide the links and nodes that need to be put to sleep, and to wake up so that the resulting routes and link-schedules are optimal.

6.7 Summary

The topology management modules implemented in WMN Centralized Controller at the time of writing this thesis were route computation, link-schedule computation, VC provisioning, topology optimizer, topology manager and WMN configuration. All topology management concepts implemented using these modules have been verified and they were proven to be feasible and realizable. The validation setups performed well in all the validation scenarios. No major bugs were found in the demonstrator or simulator systems. Minor bugs were experienced in the demonstrator system during early stages of testing, but they were resolved alongside the development of the WCC. Above all, it is noteworthy to mention that the software implementations in the nodes and in the WCC were of high quality and well documented. Future areas of research in this concept involve defining implementations of access control, network monitoring mechanisms and energy saving control mechanisms.

7 SUMMARY AND CONCLUSION

The mobile data consumption is increasing very rapidly and is set to increase even more in future. The main reasons behind this growth are the increased usage of smartphones and tablets, and access to mobile networks at an affordable price. To cope up with the capacity demand for the mobile data, mobile networks are evolving towards providing higher link capacity and user Quality of Experience. The third generation of mobile networks introduced to data rates of several megabits per second and an all-IP core with packet switched voice service. In fourth generation of mobile networks, flatter network architecture was introduced along with the higher data rates than in the previous generation networks. However, faster radio access and upgraded macro network capacity alone will not be able to tackle the whole capacity problem. The concept of heterogeneous networks introduced in the fourth generation of mobile networks is seen as an effective solution to increase coverage and capacity. The concept behind heterogeneous networks is cell densification, where small cells are used to enhance the coverage and capacity in a macro cell area. In fifth generation of mobile networks, transmission at millimeter wavelength band and sophisticated antenna technologies are being considered to achieve more capacity and higher throughput

A mobile backhaul is the connecting transport network between the radio access network and core network. The backhaul links mainly use copper cables, optical fibers and microwave links. Similar to access networks, the technology employed in backhaul networks has also evolved from TDM based technology and ATM to IP/packet based technology, offering more transport capacity in a cost effective manner. Providing a cost-effective mobile backhaul solution becomes challenging with the increasing deployments of small cell networks in a magnitude much greater than the number of deployed macro cells. Since small cells are also deployed in unconventional locations such as rooftops, street lamps and other utility poles, providing a wired backhaul solution is generally not possible. Wireless small cell backhauling methods involve for example the use of microwave or millimeter wave radio. However, an optimal backhaul solution for a small cell must satisfy the requirements of high throughput, low delay, high availability, resiliency and support for Quality of Service and traffic engineering.

The concept of Self-Optimizing Wireless Mesh Network (SWMN) as a backhaul solution for small cells is jointly studied and developed by Nokia Networks and VTT. According to this concept, the backhaul nodes residing in the base stations are connected in the form of a partial mesh using directional Point-to-Point millimeter wave radio links. This concept also employs self-organizing capabilities such as self-configuration in the form of automated neighbor discovery and link-establishment, self-healing through robust and automated resiliency scheme and self-optimization by offering provision for flexible QoS scheme, congestion control and load balancing mechanisms. In addition to these, the concept also includes a central intelligence called the Wireless Mesh Network Centralized Controller (WCC), which is responsible for topology management. Topology management is an automated mechanism to handle changes in the topology. This mainly involves topology configuration, optimization, route computation, link-schedule computation, network monitoring and energy saving mechanisms.

Testing of topology management functionalities was required alongside the development of WMN Centralized Controller. As part of my master’s thesis and to carry out testing on large topologies, it was necessary to develop a simulator, which could also help in creating complex network scenarios. For validating the SWMN system, extensive test cases were planned and executed, targeting each of the modules used in topology management. Furthermore, an initial part of my thesis also involved testing the feasibility of WCC on the proof-of-concept demonstrator system. The test cases designed to test the topology management functionalities involves autonomous network build-up with live traffic scenarios, node/link addition, node/link removal and domain splitting/merging.

Overall, in all of the test cases the WCC worked as specified, and the simulator and demonstrator system performed well throughout the validation process. No major errors were found in the WCC implementation. Minor bugs appeared in the demonstrator system in the initial stages of testing the feasibility, but these were resolved through extensive debugging. Thus, the main objective of this master’s thesis can be considered to be fully and successfully completed. The topics for future research in the development of WCC include network status monitoring, access control and energy saving mechanisms.

REFERENCES

[1] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2013–2018," 2014.

[2] Julius Robson, "Small Cell Backhaul Requirements," Next Generation Mobile Networks (NGMN), June 2012.

[3] Andrea Goldsmith, *Wireless Communications*.: Cambridge University Press, 2005.

[4] Ericsson, "Mobile Data Surpasses Voice," 2010.

[5] Ericsson, "Ericsson Mobility Report," 2014.

[6] Lourens O. Walters and P. S. Kritzinger, "Cellular networks: past, present and future," vol. 7, no. 2, p. 4, December 2000.

[7] Jyri Hämäläinen. Radio Communication Systems - General high level system architecture of mobile networks.

[8] Rajesh Chundury, "Mobile broadband backhaul:Addressing the challenge," Ericsson, 2008.

[9] Adachi Fumiyuki, "Wireless Past and Future - Evolving Mobile Communication systems," IEEE, 2001.

[10] Tinatin Mshvidobadze, "Evolution Mobile Wireless Communication and LTE Networks," IEEE, 2012.

[11] Pankaj Sharma , "Evolution of Mobile Wireless Communication Networks-1G to 5G as well as Future Prospective of Next Generation Communication Network," vol. 2, no. 8, pp. 47-53, August 2013.

[12] Amit Kumar, Yunfei Liu, Jyotsna Sengupta, and Divya , "Evolution of Mobile Wireless

Communication Networks:1G to 4G," vol. 1, no. 1, December 2010.

[13] Vasco Pereira and Tiago Sousa, "Evolution of Mobile Communications: from 1G to 4G," University of Coimbra, 2004.

[14] Jingyuan Zhang and Ivan Stojmenovic, "Cellular Networks," University of Alabama, University of Ottawa, Cananda, 2005.

[15] 3GPP. Releases. [Online]. http://www.3gpp.org/specifications/67-releases

[16] Harri Holma and Antti Toskala , *WCDMA For UMTS - HSPA Evolution and LTE*, 4th ed.: John Wiley & Sons Ltd., 2007.

[17] Sauter Martin. (2010, January) WirelessMoves - The Most Important 3GPP Features From Release 5 to 10. [Online]. http://mobilesociety.typepad.com/mobile_life/2010/01/the-most-important-3gpp-features-from-release-5-to-10.html

[18] 4G Americas, "4G Mobile Broadband Evolution," White Paper 2014.

[19] Rysavy Research, "Mobile Broadband Explosion," 4G Americas, 2013.

[20] Alcatel Lucent, "Introduction to Evolved Packet Core," White Paper 2009.

[21] Per Beming et al., "LTE-SAE architecture and performance," Ericsson, 2007.

[22] Alastair Brydon, "Summary of 3GPP Standards Releases for LTE," 2012.

[23] Afif Osseiran et al., "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *5G Wireless Communications Systems: Prospects and Challenges*, vol. 52, no. 5, pp. 26-35, 2014.

[24] Ericsson, "More than 50 Billion Connected Devices," 2011.

[25] Bernhard Raaf et al., "Vision for Beyond 4G Broadband Radio Systems," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International*

Symposium on, Toronto, 2011, pp. 2369 - 2373.

[26] Gerhard Fettweis and Siavash Alamouti, "5G: Personal Mobile Internet beyond: What Cellular Did to Telephony," , vol. 52, 2014, pp. 140-145.

[27] 4G Americas, "4G Americas' Recommendations on 5G Requirements and Solutions," White Paper 2014.

[28] Juniper Networks, "Mobile Backhaul Reference Architecture," 2009.

[29] Juniper Networks, "Universal Access and Aggregation Mobile Backhaul Design Guide," 2013.

[30] Esa Metsala and Juha Salmelin , *Mobile Backhaul*.: John Wiley and Sons, 2013.

[31] NGMN Alliance, "LTE Backhauling Deployment Scenarios," Next Generation Mobile Networks (NGMN), White Paper 2011.

[32] Orawan Tipmongkolsilp, Said Zaghloul, and Admela Jukan, "The Evolution of Cellular Backhaul Technologies:Current Issues and Future Trends," vol. 13, no. 1, pp. 97 - 113, February 2011.

[33] Small Cell Forum, "Backhaul Technologies for Small Cells," 2013.

[34] NGMN Alliance, "Guidelines for LTE Backhaul Traffic Estimation," Next Generation Mobile Networks (NGMN), White Paper 2011.

[35] AT&T Radio Technology Group, "Constrained Backhaul Simulations for Small Cells," 2012.

[36] (2012, July) 3GPP TS23.203 - Policy and charging control architecture.

[37] Ericsson, "Microwave Capacity Evolution," 2011.

[38] Pekka Wainio et al., "Mobile Networks Evolution for Individual Communications Experience(MEVICO) – Innovative Solutions for Mobile Backhaul," Celtic

Telecommunication Systems, 2012.

[39] Seppo Hamalainen, Henning Sanneck, and Cinzia Sartori, Eds., *LTE Self-Organising Networks (SON): Network Management Automation for Operational Efficiency*.: Wiley, December 2011.

[40] David T Chen, Joseph Schuler, Pekka Wainio, and Juha Salmelin, "5G Self-Optimizing Wireless Mesh Backhaul," in *IEEE Conference on Computer Communications*, 2015.

[41] Kari Seppänen, Pekka Wainio, and Tapio Suihko, "Self-optimizing Last Hop Backhaul Network for 5G ," in *WCM*, 2015.

[42] Tuomas Taipale, "Feasibility of wireless mesh for LTE-Advanced small cell access backhaul," Aalto University, Espoo, 2012.

[43] Kari Seppänen, "Detailed specification of directional WMN protocols and algorithms," 2010.

[44] Pekka Wainio et al., "Mesh SON Wireless Backhaul Baseline," Nokia Networks, 2014.

[45] Kari Seppänen , "Wireless Mesh Network, Algorithm Update," MEVICO, 2012.

[46] Kari Seppänen, "Analysis of existing ToP standards for WMN internal clock synchronization and time signal distribution," DiMeRTS, 2011.

[47] Jorma Kilpi, Jori Paananen, Kari Seppänen, Tapio Suihko, and Pekka Wainio, "TM+WCC concept functional specification," Nokia Networks, 2014.

[48] Lanner. (2012) MR-730 datasheet. [Online]. http://www.lannerinc.com/download-center/Datasheets/Network-Processing-Appliances/MR-730_DM