



University of
Salford
MANCHESTER

**Disaster Scenario Optimised Link State Routing Protocol
for Disaster Recovery and Rescue Operations**

UMAR ALIYU

**School of Science, Engineering, and Environment
University of Salford, Manchester,
United Kingdom**

**Submitted in partial fulfilment of the requirements for the Degree
of Doctor of Philosophy (PhD) in Computer
Networks and Telecommunication**

2021

Table of Contents

Table of Contents	ii
List of Figures.....	viii
List of Tables	xiv
Declaration.....	xv
Publications	xvi
Acknowledgement	xvii
List of Abbreviations	xviii
Abstract.....	xx
Chapter 1	1
1.1 Introduction	1
1.2 Research Motivation	4
1.3 Definition of Research Problems	6
1.4 Research Aims and Objectives.....	7
1.4.1 The Research Aim.....	7
1.4.2 The Research Objectives.....	7
1.5 Research Methodology.....	8
1.6 Research Contribution.....	9
1.7 Thesis Structure.....	10
Chapter 2	10
2.1 Introduction	10
2.2 Wireless Network.....	10
2.3 MANETs Overview	11
2.3.1 History of MANET	12
2.3.2 Characteristic of MANET	13
2.3.3 Challenges of MANET	14

2.3.4	Applications of MANET.....	15
2.4	Routing Protocols in MANET	15
2.4.1	Classification of MANET Routing Protocols.....	16
2.4.2	Summary of MANET Routing Classification.....	37
2.5	Reason for Choosing Proactive over Reactive Protocols.....	39
2.5.1	Why OLSR over other proactive routing protocols.....	39
2.5.2	OLSR Version Adopted for Modification	40
2.5.3	Features and Functionalities of OLSR).....	42
2.6	Message Prioritisation Related Work.....	52
2.7	Chapter Summary.....	54
Chapter 3	56
	Literature Review of Networks for Disaster Recovery and Rescue Operations	56
3.1	Introduction	56
3.2	Disaster Recovery Networks.....	56
3.2.1	Pre-disaster Communication System	57
3.2.2	Post-Disaster Communication System.....	58
3.2.3	Summary of Reviewed Disaster Recovery Networks.....	82
3.2.4	Why MANET Based Disaster Solution over Deployable WLAN Based Solution 86	
3.3	Mechanism for Switching Smartphones to Disaster Mode.....	87
3.3.1	Steps 1 and 2: Weather Tracking Using Satellites.....	87
3.3.2	Step 3: Meteorologists Receive Weather Report	88
3.3.3	Steps 4 and 5: Mobile Service Providers Send Alert to Subscribers	91
3.4	Chapter Summary.....	94
Chapter 4	95
	Disaster Scenario Optimised Link State Routing Protocol (DS-OLSR) Design	95
4.1	Introduction	95

4.2 Design Assumptions of the Proposed DS-OLSR.....	95
4.3 Disaster Mode Process in Smartphones	97
4.3.1 Launching DS-OLSR through an embedded link.....	97
4.3.2 Manual Mechanism for Switching Smartphones to Disaster Mode	100
4.4 Internet Protocol (IP) Address Generation for DS-OLSR Devices.....	101
4.5 DS-OLSR Time Slices	102
4.5.1 Network Formation Time Slice (NFTS).....	103
4.5.2 Topology Propagation Time Slice (TPTS)	105
4.5.3 Message Time Slice (MTS)	105
4.5.4 Network Sleep Period (NSP)	106
4.5.5 Time Slice Duration.....	107
4.6 DS-OLSR and DS-OLSRMP Messages	108
4.7 Handling New Devices/Nodes	109
4.8 Proposed Disaster Management Server (DMS)	109
4.8.1 Hardware Requirement	110
4.8.2 Operating System.....	110
4.8.3 Database Management System	111
4.8.4 Internet Connectivity and Bandwidth	112
4.9 Addressing Network Partition.....	113
4.10 DS-OLSR Packet Format and Forwarding.....	114
4.10.1 DS-OLSR and DS-OLSRMP Packet Processing.....	115
4.10.2 DS-OLSR and DS-OLSRMP Packet Forwarding	116
4.11 DS-OLSR and DS-OLSRMP Repositories/Tables/Sets	116
4.11.1 Duplicate Set.....	117
4.11.2 Link Set.....	117
4.11.3 Topology Set.....	118
4.11.4 Contacts Set	119

4.11.5	Deviceinfo Set.....	119
4.12	ALERT Message.....	119
4.12.1	Destination.....	121
4.12.2	Message Size.....	121
4.12.3	Destination Address.....	122
4.12.4	Destination Phone Number.....	122
4.12.5	Message Octets.....	122
4.12.6	SMS Message Routing.....	122
4.13	SHHH Message Implementation.....	124
4.13.1	Current Time Slice.....	124
4.13.2	Current Timer Value.....	125
4.14	Modification to Hello and TC Messages Packet.....	125
4.14.1	Modification to Hello Message Packet.....	125
4.14.2	Modification to TC Message Packet.....	126
4.15	Chapter Summary.....	127
Chapter 5	128
5.1	Introduction.....	128
5.2	Simulation-Based Model.....	128
5.2.1	Network Model.....	129
5.2.2	Energy Consumption Model.....	129
5.2.3	Wi-Fi Simulation Setup.....	131
5.2.4	Mobility Model.....	134
5.3	Simulation Setup of Network Formation Scenario.....	135
5.3.1	OLSR/DS-OLSR Simulation Environment and Parameters for Network Formation Scenario.....	136
5.3.2	OLSR/DS-OLSR Simulation Results for Network Formation Scenario.....	138
5.4	Implementation of DS-OLSR in Disaster Area Network.....	140

5.4.1	Simulation Setup for Disaster Area Network	140
5.4.2	Results Analysis for Disaster Area Network	142
5.5	Chapter Summary.....	150
Chapter 6	152
	Disaster Scenario Optimized Link State Routing Protocol and Message Prioritization (DS-OLSRMP).....	152
6.1	Introduction.....	152
6.2	Proposed DS-OLSRMP Structure and Main Features	152
6.2.1	ALERT Message Packet Format Modification.....	154
6.2.2	Implemented Models	156
6.3	Simulation Setup and Results Analysis.....	162
6.3.1	Simulation Setup.....	163
6.3.2	Results Analysis.....	164
6.4	Chapter Summary.....	173
Chapter 7	174
	Performance Evaluation and Validation	174
7.1	Introduction.....	174
7.2	Analytical Validation	174
7.3	Numerical Energy Consumption.....	177
7.4	Routing Control Overhead Computation	181
7.4.1	Periodic Message routing overhead	181
7.4.2	Routing Overhead due to Packet failure	182
7.4.3	Triggered update message.....	183
7.5	Packet Delivery Ratio (PDR) Computation	187
7.6	End-to-End Delay Computation.....	190
7.6.1	Transmission Delay (T_d).....	190
7.6.2	Propagation Delay (P_d)	190

7.6.3	Queueing Delay /Waiting-Time (Q_d).....	191
7.6.4	Processing Delay (P_c).....	191
7.6.5	Overall Delay in a node (D_n)	191
7.6.6	Overall Delay in a Hop (D_h)	191
7.6.7	End-to-End Delay (EED).....	192
7.7	Chapter Summary.....	201
Chapter 8	202
	Conclusion and Future Work	202
8.1	Conclusion.....	202
8.2	Future Work	205
References	207
Appendices	218
	Appendix A: NS - Simulation Command and Some Screenshot of Simulation Environment	218
	Appendix B: Simulation Results for Network formation	220
	Appendix C: Simulation Results for Disaster Scenario	221
	Appendix D: Calculated Results	224

List of Figures

Figure 1-1: Showing classical flooding (left) and MPR flooding (right) (Adjih et al., 2003)...	3
Figure 1-2: A power transmission tower felled by Hurricane Maria (Gallucci, 2018).....	5
Figure 1-3: Puerto Ricans checking their phones for cellular signal (Intellengencer, 2017). ...	5
Figure 1-4: AT&T using an LTE-equipped drone to reconnect some Puerto Ricans (ArsTechnica, 2017).	5
Figure 1-5: The Main Steps of Research Process	9
Figure 2-1: MANET routing protocols base on network structures	16
Figure 2-2: Showing classical flooding (left) and MPR flooding (right) (Adjih et al., 2003).	19
Figure 2-3: Example of Fisheye State Routing Protocol with sample Topology Table (Gerla, 2002).....	20
Figure 2-4: Only 3 non-leaf nodes flood messages generated by node A (R. Ogier et al., 2004)	21
Figure 2-5: Sample routing table for TBRPF (R. Ogier et al., 2004)	22
Figure 2-6: Sample routing tables for DSDV nodes (He, 2002).....	23
Figure 2-7: DSDV routing table with broken link detected by Node B (He, 2002)	24
Figure 2-8: Node B advertises changes to its' routing table to Node A (He, 2002).....	24
Figure 2-9: Sender sends packets to rendezvous node which in turn forwards to Destination (Cheng et al., 2010).....	25
Figure 2-10: Propagation of RREQ and RREP from Source node S to Destination node D using AODV (Rajkumar et al., 2012).....	28
Figure 2-11: Propagation of Route Discovery Message from Source node S to Destination node D (Johnson et al., 2007)	29
Figure 2-12: DAG with height value of each node in the network towards the destination node (Alotaibi & Mukherjee, 2012)	30
Figure 2-13: Flooding Cluster Heads with RREQ packets from Cluster Member 2 (Source: (Safa, Artail, & Tabet, 2010)	32
Figure 2-14: Representation of Routing Zone with $p=2$ and Node S as the Node in Question (Beijar, 2002).....	33
Figure 2-15: Overview of LANMAR indicating logical subnet and a Landmark Node (Nong, 2014)	35
Figure 2-16: (a) LAR Scheme1 and (b) LAR Scheme2 (Alotaibi & Mukherjee, 2012)	37

Figure 2-17: OLSRv1 source code repository showing number of commits, branches, releases and contributors (Andreas et al., 2017b).....	41
Figure 2-18: OLSRv2 source code repository showing number of commits, branches, releases and contributors (Tonnesen Andreas, Lopatic Thomas, & Kaplan Aaron, 2017a)	41
Figure 2-19: Searching for olsrv1 returned 123 results. (Retrieved August 13, 2019)	41
Figure 2-20: Searching for olsrv2 returned 976 results. (Retrieved August 13, 2019)	42
Figure 2-21: MPR selection process (blue phone selected red phones as MPRs).....	51
Figure 3-1: Two-tier Hierarchical Network (W. Lu et al., 2007)	69
Figure 3-2: Network Architecture of E-DARWIN (Raj et al., 2014)	70
Figure 3-3: Network Architecture of P2Pnet (Y.-N. Lien et al., 2009)	71
Figure 3-4: Logical Architecture of P2Pnet (Y. N. Lien, Li-Cheng, & Yuh-Sheng, 2009)	72
Figure 3-5: MANET Based Three-Tier Cellular Network (Vo et al., 2015)	74
Figure 3-6: HELPER development/deployment prototype/scenario (Jagannath et al., 2019). 75	
Figure 3-7: Message transmission in the architecture of DTN over MANET (Nishiyama et al., 2014).	76
Figure 3-8: Deployment and usage scenarios for Relay-by-smartphones (Nishiyama et al., 2014).....	76
Figure 3-9: Teamphone deployment scenario (Z. Lu et al., 2017)	77
Figure 3-10: LBGD-AODV architecture (M. Iqbal, 2010).....	78
Figure 3-11: SDN-DTN Blended Architecture (Hoque et al., 2020).....	79
Figure 3-12: Disaster Scenario of Deployed Drone-Base Small Cells (K. Ali et al., 2020)....	80
Figure 3-13: Intelligent Resource Deployed Network Approach (Xiaoyan Wang et al., 2020)	81
Figure 3-14: ISG-ECN Deployment Model (Xiaoyan Wang et al., 2020)	82
Figure 3-15: Automated Process for Switching Smartphones to Disaster Mode	89
Figure 3-16: NOAA Satellite Tracking the Atlantic Ocean (NOAA, 2019b)	89
Figure 3-17: NOAA Satellite Tracking the Central Pacific (NOAA, 2019b).....	90
Figure 3-18: NOAA Satellite Tracking the Eastern North Pacific (NOAA, 2019b).....	90
Figure 3-19: US National Weather Service warning for Hawaii (NOAA, 2019c).....	91
Figure 3-20: Sample WEA message alert. The alert followed by loud alarm (FCC, 2019)....	91
Figure 3-21: Cell broadcast setting in Android 7.1 (Forum, 2019).	92
Figure 3-22: CBS message flow in GSM/UMTS/LTE/5G.....	93
Figure 4-1: Sample WEA message alert with link to lunch DS-OLSR application.	99
Figure 4-2: Diagrammatical Representation of DS-OLSR Time Slices System	103

Figure 4-3: NFTS: Message and Duration.....	104
Figure 4-4: TPTS: Message and Duration	105
Figure 4-5: MTS: Message and Duration	106
Figure 4-6: NSP: Message and Duration	106
Figure 4-7: Operating System support of olsrd (Andreas et al., 2017a).....	110
Figure 4-8: Anchored buoy with solar panels and sensors for monitoring environment and water quality (LISICOS, 2019).....	113
Figure 4-9: Directional flow of SMS from MANET to Internet	115
Figure 4-10: GSM basic character set (ETSI, 2019a).....	123
Figure 4-11: Message routing from DMS to recipient outside the disaster zone	124
Figure 5-1: Simulation System Specification - Dell Inspiron laptop running Ubuntu 18.04.3.....	135
Figure 5-2: NS-3 Python Visualizer showing node placement.....	137
Figure 5-3: Energy Consumption for Network Formation Scenario	139
Figure 5-4: Routing Control Overhead for Network Formation Scenario.....	139
Figure 5-5: Disaster Area Network Model (Aschenbruck et al., 2009).....	140
Figure 5-6: NS-3 Python Visualizer showing node placement.....	141
Figure 5-7: Energy Consumption for Disaster Area Network in Static Scenario.....	143
Figure 5-8: Energy Consumption for Disaster Area Network in Mobility Scenario (1m/s – 2m/s)	144
Figure 5-9: Energy Consumption for Disaster Area Network in Mobility Scenario (5m/s – 12m/s)	144
Figure 5-10: Routing Control Overhead for Disaster Area Network in Static Scenario	145
Figure 5-11: Routing Control Overhead for Disaster Area Network in Mobility Scenario (1m/s – 2m/s)	145
Figure 5-12: Routing Control Overhead for Disaster Area Network in Mobility Scenario (5m/s – 12m/s)	146
Figure 5-13: Packet Delivery Ratio for Disaster Area Network in Static Scenario.....	147
Figure 5-14: Packet Delivery Ratio for Disaster Area Network in Mobility Scenario (1m/s – 2m/s)	147
Figure 5-15: Packet Delivery Ratio for Disaster Area Network in Mobility Scenario (5m/s – 12m/s)	148
Figure 5-16: End-to-End Delay for Disaster Area Network in Static Scenario.....	149

Figure 5-17: End-to-End Delay for Disaster Area Network in Mobility Scenario (1m/s – 2m/s)	149
Figure 5-18: End-to-End Delay for Disaster Area Network in Mobility Scenario (5m/s – 12m/s)	150
Figure 5-19: DS-OLSR simulation commands retrieved from .bash_history file	151
Figure 5-20: OLSRv1 simulation commands retrieved from .bash_history file	151
Figure 6-1: Each device sends ALERT message for routing to Device F via MPR D. Device B Battery life is low hence ALERT message from Device B is prioritized	153
Figure 6-2: MPR D equally prioritizes response from Device F to Device B for delivery	153
Figure 6-3: Once Device B messages are delivered, MPR D forwards remaining messages from Devices A, C and E to Device F	153
Figure 6-4: Finally, response from Device F is forwarded to Devices A, C and E	154
Figure 6-5: Sample values for priority and status fields for new ALERT message from sender B to recipient F	155
Figure 6-6: Sample values for priority and status fields for message status notification from recipient F to sender B	155
Figure 6-7: Message prioritization process	158
Figure 6-8: Request Order and Priority Order	159
Figure 6-9: Message prioritization process	159
Figure 6-10: NS-3 Python Visualizer showing node placement for DS-OLSRMP	163
Figure 6-11: Comparison of Energy Consumption for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Static Scenario	166
Figure 6-12: Comparison of Energy Consumption for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (1m/s – 2m/s)	167
Figure 6-13: Comparison of Energy Consumption for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (5m/s – 12m/s)	167
Figure 6-14: Comparison of Routing Control Overhead for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Static Scenario	168
Figure 6-15: Comparison of Routing Control Overhead for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (1m/s – 2m/s)	168
Figure 6-16: Comparison of Routing Control Overhead for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (5m/s – 12m/s)	169
Figure 6-17: Comparison of Packet Delivery Ratio for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Static Scenario	169

Figure 6-18: Comparison of Packet Delivery Ratio for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (1m/s – 2m/s).....	170
Figure 6-19: Comparison of Packet Delivery Ratio for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (5m/s – 12m/s).....	170
Figure 6-20: Comparison of End-to-End Delay for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Static Scenario.....	171
Figure 6-21: Comparison of End-to-End Delay for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (1m/s – 2m/s).....	172
Figure 6-22: Comparison of End-to-End Delay for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (5m/s – 12ms).....	172
Figure 7-1: Comparison of the Calculated and Simulated Energy Consumption in Static Scenario.....	180
Figure 7-2: Comparison of the Calculated and Simulated Energy Consumption in Mobility Scenario (1m/s – 2m/s).....	180
Figure 7-3: Comparison of the Calculated and Simulated Energy Consumption in Mobility Scenario (5m/s – 12m/s).....	181
Figure 7-4: Comparison of the Calculated and Simulated Control Overhead in Static Scenario.....	186
Figure 7-5: Comparison of the Calculated and Simulated Control Overhead in Mobility Scenario (1m/s – 2m/s).....	186
Figure 7-6: Comparison of the Calculated and Simulated Control Overhead in Mobility Scenario (5m/s – 12m/s).....	187
Figure 7-7: Comparison of the Calculated and Simulated Packet Delivery Ratio in Static Scenario.....	189
Figure 7-8: Comparison of the Calculated and Simulated Packet Delivery Ratio in Mobility Scenario (1m/s – 2m/s).....	189
Figure 7-9: Comparison of the Calculated and Simulated Packet Delivery Ratio in Mobility Scenario (5m/s – 12m/s).....	190
Figure 7-10: Markov Chain for the M/M/1/K queue (Oechsner, 2020).....	193
Figure 7-11: Markov Chain for the M/M/1 queue (Oechsner, 2020).....	194
Figure 7-12: Comparison of the Calculated and Simulated End-to-End Delay in Static Scenario.....	199
Figure 7-13: Comparison of the Calculated and Simulated End-to-End Delay in Mobility Scenario (1m/s – 2m/s).....	200

Figure 7-14: Comparison of the Calculated and Simulated End-to-End Delay in Mobility Scenario (5m/s – 12m/s)200

List of Tables

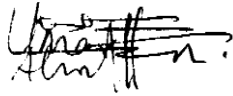
Table 2-1: Summary of MANET Routing Classification	38
Table 2-2: Packet format for OLSR (Clausen & Jacquet, 2003)	43
Table 2-3: OLSR Hello Message Format (Clausen & Jacquet, 2003).....	48
Table 2-4: OLSR TC Message Format (Clausen & Jacquet, 2003)	48
Table 2-5: OLSR HNA Format (Clausen & Jacquet, 2003).....	48
Table 2-6: OLSR MID Format (Clausen & Jacquet, 2003).....	49
Table 3-1: Summary of Reviewed Disaster Recovery Networks	82
Table 4-1: Redesigned OLSR Packet Header	96
Table 4-2: DS-OLSR Time Slices, messages and duration	107
Table 4-3: DS-OLSR Time Slices, Messages and Duration.....	109
Table 4-4: Sample Screen output on DMS showing which device requires replacement.....	114
Table 4-5: DS-OLSR unified packet header (new: in Red Colour).....	114
Table 4-6: Sample Duplicate Set record	117
Table 4-7: Sample Link Set records.....	118
Table 4-8: Sample of Topology Set records	118
Table 4-9: Sample of Contact Set records	119
Table 4-10: Sample of Deviceinfo Set record.....	119
Table 4-11: ALERT message packet format	121
Table 4-12: SHHH message packet format	124
Table 4-13: DS-OLSR Hello message packet	125
Table 4-14: DS-OLSR TC message format	126
Table 5-1: OLSRv1/DS-OLSR Simulation parametres for Network Formation Scenario....	137
Table 5-2: Simulation parametres for Disaster Area Network	141
Table 6-1: Improvement to Alert Message Packet Format.....	154
Table 6-2: Applicable Message Priorities and their Values.....	157
Table 6-3: Allocation of Message Slice Duration (MSD) to Priorities	162
Table 6-4: Simulation Parameters Message Prioritization.....	164
Table 7-1 : Description of OSLR Packet Header.....	175
Table 7-2: Parameters for Calculation of Energy Consumption.....	179
Table 7-3: Parameters for Calculation of Control Overhead	185
Table 7-4: Explanation of Terms for the End-to-End Delay Model.....	192
Table 7-5: Parameters for End-to-End Delay Calculation.....	199

Declaration

I declare that this research is solely my own work and has not been submitted in support of any previous application for award of higher degree. Therefore, I take ownership of the entire research. The contribution of other researchers being published and unpublished used in completion of this research has been duly acknowledged with appropriate credit.

NAME: Umar Aliyu

SIGNATURE:

A handwritten signature in black ink, appearing to read 'Umar Aliyu', with a horizontal line drawn through it.

DATE: December 2021

Publications

1. Aliyu, U., Tavruri, H., Hope, M., Halilu, A. G., (2020). “DS-OLSR – Disaster Scenario Optimized Link State Routing Protocol”. 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), 1-6. IEEE Computer Society, Porto, Portugal. July 20-22.
2. Aliyu, U., Tavruri, H., Hope, M., (2021). “Message Prioritisation for Disaster Scenario Optimized Link State Routing Protocol”. Salford Postgraduate Annual Research Conference 2021 (SPARC 2021), University of Salford, Salford, UK, 31st June – 1st July 2021.
3. Halilu, A. G., Hope, M., Tavruri, H., & Aliyu, U. (2020). “Optimized QoS Routing Protocol for Energy Scavenging Nodes in IoT”. 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), 1-6. IEEE Computer Society, Porto, Portugal. July 20-22.

Acknowledgement

First and foremost, I remain praiseful, thankful and grateful to ALLAHU subhanahu wata'ala who in His endless mercies made it possible for me to embark-on and complete this research work. My greatest appreciation goes to my able supervisor: Professor Haifa Takruri for her motivation, guidance, continued support, and constructive comments that made this research a successful one. I am extremely happy to have her as my supervisor. I would also like to express my gratitude to Petroleum Technology Development Fund (PTDF) for providing the financial support needed for this research. A Special thanks to my beloved parent, family, relatives and friends for their faithful prayers, counsel, encouragement, and support throughout my research. Not enough words to express my appreciation. Similarly, I would like to extend my gratitude to the university academic staff, staff of Clifford Whitworth Library, especially Sherwin Anne, IT help desk and the entire research community of the University of Salford for their wonderful support and collaboration during my research period.

List of Abbreviations

AODV	Ad-Hoc On-Demand Distance Vector
AP	Access Point
BTS	Base Transceiver Station
CBC	Cell Broadcast Centre
CBE	Cell Broadcast Entity
CBS	Cell Broadcast Service
COW	Cell-on-Wheel
CP	Critical Priority
DMS	Disaster Management Server
DSDV	Destination Sequenced Distance Vector
DS-OLSR	Disaster Scenario Optimized Linked State Routing
DS-OLSRMP	Disaster Scenario Optimized Linked State Routing and Message Prioritisation
D2D	Device-to-Device
DRT	Directional Routing Table
DRN	Disaster Recovery Network
DSR	Dynamic Source Routing
ECC	Emergency Control Centre
ERC	Emergency Response Centre
EU	End User
EV	Emergency Vehicle
FCC	Federal Communication Commission
HNA	Host Network Association
HP	High Priority
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
LP	Low Priority
LS	Link State
LOS	Line of Sight
MANET	Mobile Ad-Hoc Network

MID	Multiple Interface Declaration
MP	Medium Priority
MP-OLSR	Multi Point Optimised Link State Routing
MSS	Mobile Switching Station
MTS	Message Time Slice
MORRP	Mobile Orthogonal Rendezvous Routing Protocol
MPR	Multi Point Relay
MTS	Message Time Slice
NFTS	Network Formation Time Slice
NIB	Network-in-Box
NOAA	National Oceanic and Atmospheric Administration
NS-3	Network Simulator 3
NSP	Network Sleep Period
OLSR	Optimized Linked State Routing
OLSRv2	Optimised Link State Routing Version 2
P2P	Peer-to-Peer
QoS	Quality of Service
RT	Rescue Team
SMS	Short Message Service
SMSCB	Short Message Service Cell Broadcast
SMSPP	Short Message Service Point-to-Point
SPR	Shortest Path Routes
TBRPF	Topology Dissemination Based on Reverse-Path Forwarding
TC	Topology Control
TIROS	Television Infrared Observation Satellite
TPTS	Topology Propagation Time Slices
UMs	Mobile Users
USSD	Unstructured Supplementary Service Data
WEA	Wireless Emergency Alerts
WSN	Wireless Sensor Network

Abstract

The success of disaster recovery and rescue operations depends largely on effective communication. Unfortunately, the communication infrastructures are among the first victims of most natural disasters such as tsunami, floods, fire, and earthquakes as well as artificial disasters (human-made) caused by terrorist attacks and war. In this emergency condition, water, food, shelter, medical helps, and protections are required; the effort and strength needed to save lives and provide disaster victims with these basic needs must be quickly organised via an effective and reliable disaster communication network. Mobile ad-hoc networks (MANETs) enable rescuers, disaster victims and rescue volunteer workers to communicate when disasters cripple/impair communication infrastructures as the technology require to set up the network is already available in their smart phones. However, provision of a temporary OLSR protocol driven MANET for survivors to communicate often affects their device battery energy, since message routing and network flooding are prominent requirements of OLSR protocol. This unpleasant situation makes it difficult to use mobile devices for extended periods. As a result, this Thesis examines MANET's popular Optimized Link State Routing (OLSR) protocol and identifies current energy and overhead challenges facing the protocol and modifies the protocol to create a new energy and overhead friendly OLSR protocol called Disaster Scenario Optimized Link State Routing (DS-OLSR) protocol to allow communication needs during disaster recovery and rescue operations.

DS-OLSR introduces the concept of Time Slices (TSs) which confines OLSR messages (Hello, TC, HNA), and of course ALERT message (a new message type created specifically for DS-OLSR) into their respective TSs. The act of compartmenting messages into TSs greatly reduces message synchronization problems, which in turn minimises associated control overheads and energy requirement of the process. DS-OLSR equally modifies OLSR packet header through the addition of a new field, namely Originator ID (device's phone number) and introduces message prioritisation in DS-OLSR based on devices' Battery life called DS-OLSRMP. The introduction of Originator ID leads to the elimination of Multiple Interface Declaration (MID) messages of OLSR and message prioritisation technique extends the lifetime of low battery devices.

The proposed routing protocols (DS-OLSR and DS-OLSRMP) were initially implemented in NS-3 and compared with both OLSRv1 and OLSRv2. The simulation results showed that both DS-OLSR and DS-OLSRMP performed better than both versions of OLSR as it achieves considerable energy saving, improved packet delivery, reduced routing overhead in both sparse and dense network simulation scenarios. Analytical results were obtained through mathematical models and were compared with the simulation results which proved that the new routing techniques achieve considerable energy savings along with reduction in routing overheads, thereby extending lifespan of low battery devices, and improving message delivery, leading to a better mental state of such victims during disaster recovery and rescue operations.

Chapter 1

1.1 Introduction

It is obvious that our today's world depends more and more on mobile communications in many of our social and economic activities, and the communications infrastructure are subject to unintentional failures caused by natural catastrophic disasters, such as tsunami, floods, fire and earthquakes, as well as intentional failures caused by artificial disasters (human-made), such as terrorist attacks and war (Vasseur, Pickavet, & Demeester, 2004). Such disasters cause many casualties and destroy or damage the communication infrastructures which brought about the need of network for disaster recovery and rescue operations.

Catastrophic disasters create emergency condition and cause physical, mental, and social disorder. In these emergency conditions, water, food, shelter, medical help and protection are required, and the effort and strength needed to provide the disaster victims with these basic services must be quickly organised via an effective and reliable communication network (Narayanan & Ibe, 2012). The main thing to be worried about in such situations is the ability to establish an efficient disaster recovery network that can allow communication among different independent rescue team members and disaster victims as fast as possible due to the importance of information exchange in such emergency situations. Large scale disaster required coordination efforts ranging from public institutions such as military, police, fire fighters and medical team personnel, and more other different organisations such as volunteer workers and disaster survivors. The success of this coordination depends heavily on efficient network for disaster recovery. The process of managing disaster and other emergency conditions are generally hierarchical, but may be simple and self-organised (Hartikainen & Harnesk, 2009). According to Oberg, Whitt, and Mills (2011), the management of disaster and other emergency conditions involved four different stages: Preparedness, Response, Recovery and Mitigation. However, the adoption of these phases will depend on the nature of the disaster (natural or artificial/human made).

A network for disaster recovery and rescue operation is a network that can be configured easily with few steps using wireless devices such as smart phones, laptops, tablets and effectively supports urgent communication needs for disaster recovery operations (Minh & Yamada, 2015). Mobile Ad-hoc Network (MANET) has been realised as the simplest and effective way

to allow communication during disaster recovery and rescue operations. Moreover, the technology requires to set up the network is already available in the smart phones of rescuers, disaster victims as well as rescue volunteer workers who help the rescuers with first-hand information on the rescue operations.

Routing protocols for MANETs communication are no longer the exclusive purview of academia. Indeed, practical demands for MANETs communication (especially in the aftermath of major disasters) encouraged software developers and hardware manufacturers to create solutions that enable MANET communication. One of such solution is the Optimized Link State Routing (OLSR) protocol (Clausen & Jacquet, 2003). OLSR is developed for mobile ad hoc networks (MANET) (Clausen & Jacquet, 2003). It is an optimization of link state routing (LSR) adapted to the requirements of a MANET. OLSR is a proactive routing protocol, in proactive routing; each node has one or more tables that contain the latest information of the routes to any node in the network. Each row in the table has the next hop for reaching a node/subnet and the cost of this route. Each OLSR node selects a set of its one-hop neighbour nodes as multipoint relays (MPRs). Only elected MPRs can forward control traffic, intended for dispersal into the entire network. This approach reduces the number of transmissions required when flooding control traffic, which is a great improvement or optimization over classical flooding algorithm used by epidemic protocol (Clausen & Jacquet, 2003) as shown in Figure 1-1.

A change in topology is propagated through all nodes in the network; this task is handled by MPRs which announce the link state information of their selectors in the network, leading to a recalculation of the shortest path routes (SPR) to all destinations in the network. Link state information is sent periodically via control messages. This announces to the entire network that the announcing MPR can reach the node or nodes that elected it as an MPR. MPRs are included in route calculation; the result of such calculation provides the route from a given node to any destination in the network.

From the preceding, it is easy to deduce that MPRs form the backbone of the OLSR protocol, since they are responsible for forwarding control messages through associated links, along with message routing on behalf of their electors. This implies mobile devices acting as MPRs are subjected to heavy CPU, memory, and communication subsystem usage. This eventually precipitates rapid draining of battery energy, leading to network partitioning (since a whole lot of MPRs devices will switch off), thereby reducing the overall lifespan of the entire network.

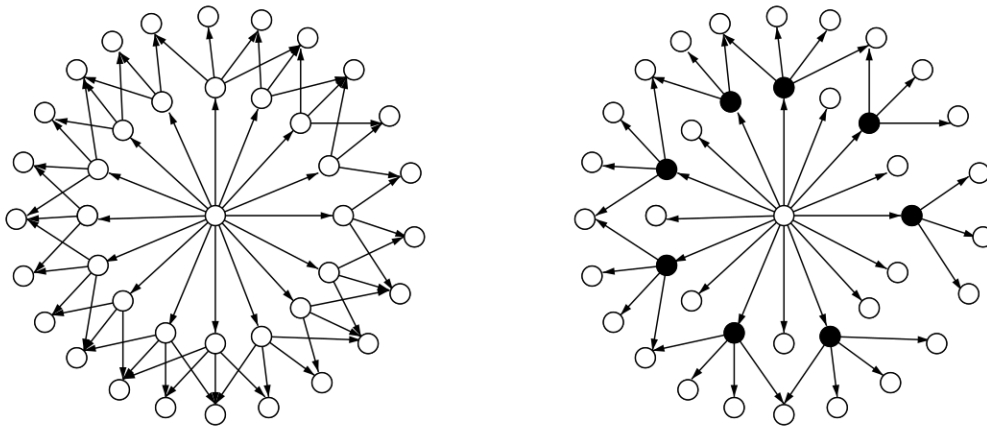


Figure 1-1: Showing classical flooding (left) and MPR flooding (right) (Adjih et al., 2003).

A major challenge facing OLSR is the concept of overworked MPRs, these MPRs often route network traffic on behalf of other nodes, which causes a severe drain to stored battery energy, and eventual shutdown. Another challenge is network overhead, caused by excessive propagation of control messages, which are responsible for link sensing and reporting. The latest version of OLSR called OLSRv2 (Clausen, Dearlove, Jacquet, & Herberg, 2014), recommends the existence of two MPRs, one to handle network flooding of control messages and another to handle message routing on behalf of electors. This distributed approach is intended to reduce the current workload of a single MPR in classic OLSR. However, the problem of overhead caused by control messages was not handled. The prominent role played by MPRs in OLSR made it both a saviour and a curse. A saviour when MPRs are properly represented all over the network and a curse when a single MPR route and flood messages on behalf of several nodes, leading to network collision which forces batteries to drain faster as each node will keep trying to retransmit previous packet.

This research examines MANET's popular Optimized Linked State Routing (OLSR) protocol. It identifies current energy and overhead challenges facing the protocol and modifies the protocol to create a new energy and overhead friendly OLSR protocol for MANET.

The rest of this chapter is organized as follows. Section 1.2 explains the motivation of this research. Section 1.3 presents definition of the problems. Section 1.4 explains the research aim and objectives. Section 1.5 provides the research methodology to address the identified problems. Section 1.6 explains the research contributions.

1.2 Research Motivation

Network for disaster recovery and rescue operations has become a necessity for every society especially in areas with commonly occurring natural and artificial (human-made) disasters for effective communication. Disaster creates emergency condition and causes physical, mental, and social disorder. In this emergency condition, water, food, shelter, medical helps, and protections are required, and the effort and strength needed to provide disaster victims with these basic services must be quickly organised via an effective and reliable communication network. Since early 1990s, networks for emergency response and disaster recovery operations were put into consideration (Morrison, 2011). Similarly, after the event of September 11 attacks, Disaster network recovery have gained much research attention. However, most of these early researches focus on design and implementation of network for emergency response and disaster recovery operations based on restoration of telecommunication infrastructure (Andersson & Kafle, 2014) using expensive and non-flexible technologies. In addition, some of the networks proposed are only accessible to rescue team members but not available to disaster victims and rescue volunteer workers who help the rescuers with fist hand information about the disaster. MANET and Multi-hop D2D communication has been realised as the simplest and effective way to allow communication during disaster recovery and rescue operations.

The MANET and Multi-hop D2D Communication has been largely studied over the years because of its enormous challenges. Furthermore, research on MANET and Multi-hop D2D communication for disaster recovery and rescue operation were put into consideration. However, most of this research do not focus on the major challenge (energy) of the networks during disaster recovery and rescue operation. For example, Both Nishiyama, Ito, and Kato (2014) and Qin, Mi, Dong, Peng, and Sheng (2016) focused on multi-hop D2D communication network using OLSR protocol to route network traffic. However, the major drawback of their research is the assumption that users can recharge their devices at will, nonetheless, some disaster scenarios challenged this assumption, especially where power grids are equally damaged.

The truism of the above was demonstrated when in 2017, Hurricane Maria struck Puerto Rico and wiped out 95% of the island's power grid (Night, 2017) along with most of the communication infrastructure as in Figures 1-2 through 1-4.



Figure 1-2: A power transmission tower felled by Hurricane Maria (Gallucci, 2018)



Figure 1-3: Puerto Ricans checking their phones for cellular signal (Intellengencer, 2017).



Figure 1-4: AT&T using an LTE-equipped drone to reconnect some Puerto Ricans (ArsTechnica, 2017).

The few users of mobile devices shown in Figure 1-3 may be seeking cellular signal to contact loved ones, perhaps to inform them that they survived the hurricane. Unfortunately, none of them seems to have had any success connecting to the network when the picture was taken.

It is very important to provide reliable and energy friendly communication network to survivors in the aftermath of a disaster. Simple text messages to rescue teams, loved ones, colleagues and business partners reduces the uncertainty over a trapped victim in a disaster zone. Such messages will allow them to go about their lives with a better frame of mind. On the other hand, provision of a temporary OLSR protocol driven MANET for survivors to communicate often affects their device battery energy, since message routing and network flooding are prominent requirements of OLSR protocol. Therefore, participating in the disaster network directly affect battery energy of communication devices.

The aforementioned research motivation led to design of an energy friendly routing protocol through optimization of classic OLSR. The new protocol reduces energy consumption and less flooding of the network with control messages. This approach maintains the disaster zone network allowing victims to send and receive messages until they are rescued.

1.3 Definition of Research Problems

This research suggests appropriate modification to reduce OLSR control overhead, thereby minimising the overall energy consumed by both network and individual nodes, without sacrificing QoS performance. The research problems are classified as follows:

Problem 1:

OLSR is constantly busy routing control messages in the background (regardless of user messages), thus, the continuously background routing constitutes a drain on bandwidth and battery (McCabe, Cullen, Fredin, & Axelsson, 2005). Unfortunately, rapid draining of battery energy is still a major problem even with the recent incarnation of OLSR called OLSRv2 (Clausen et al., 2014), since it maintains background routing of control messages. Consequently, this research investigates novel approaches that can lower the energy consumption of OLSR devices/nodes.

Problem 2:

Survivors communicating over a disaster MANET are sometimes subject to communication connection errors. Clausen (2004) identified the cause of these errors in OLSR protocol as transient or temporary loss of routes to other parts of the network, often due to collision. Message collision occurs when messages become synchronize or coordinated, for example, a node may wish to report a change in its set of MPR via HELLO message, which may trigger a network control message (TC message) in a set of neighbouring nodes, this would lead to collision since the receiving node is already busy with the HELLO message (Clausen, 2004).

Problem 3:

Low battery energy devices often experience quick power failure which restricts their ability to communicate for longer time during rescue operations. They equally overwhelm the network with messages if they did not get response or delivery report on time because their communication device battery energy is running low.

This research investigates solutions that reduces control overhead and message collision amongst nodes in OLSR protocol and extend the lifespan of low battery energy devices for effective disaster recovery network.

1.4 Research Aims and Objectives

1.4.1 The Research Aim

The aim of this research is to develop a novel approach that reduces the energy consumption of OLSR protocol and improves the efficiency of networks for disaster recovery and rescue operations, along with increasing the successful delivery of message to destination node.

1.4.2 The Research Objectives

Achieving the stated aims require the fulfilment of the following objectives:

1. To develop an extensive review of MANET routing protocols and existing disaster recovery networks with special attention to MANET using OLSR for disaster recovery network.

2. Design a Cell Broadcast Entity software (CBE) algorithm that incorporates a link which can launch Disaster Scenario Optimised Link State Routing Protocol (DS-OLSR) on user's smartphone.
3. Design software algorithms that retrieve smartphone number, Battery life and IP address for use by DS-OLSR
4. Build messaging capabilities into DS-OLSR to reduce overhead and packet loss through collision.
5. Build a partitioning system called Time Slices (TS) that partitions OLSR messages into their respective time slices to reduce message collision, overheads, and extends smartphone battery lifespan.
6. Implement the proposed scheme in a network simulation and compare the results with that of OLSRv1 and OLSRv2.
7. Develop a mathematical model to validate the simulation results.

1.5 Research Methodology

A scientific research methodology has been implemented for this research as it utilizes simulation and mathematical models based on hypotheses, experiments, and theories. The main process of the research methodology is defined in Figure 1-5. However, the methodology may be updated when the need arises for better process of solving the research problem. It includes the following stages:

1. Review previous literature.
2. Identify research gaps/problems, then study and analyse these problems.
3. Designing heuristic and algorithms to address the research problem.
4. Study simulator and implement the proposed solution in a simulation environment using several scenarios and evaluate the results.
5. Develop a mathematical model to validate the simulation results.
6. Modify, enhance, and improve the model to improve results by 50% or more.
7. Completing the PhD research.

This methodology technique helped in achieving the aim and the objectives of the research. The main steps of the research process are as shown in Figure 1-5.

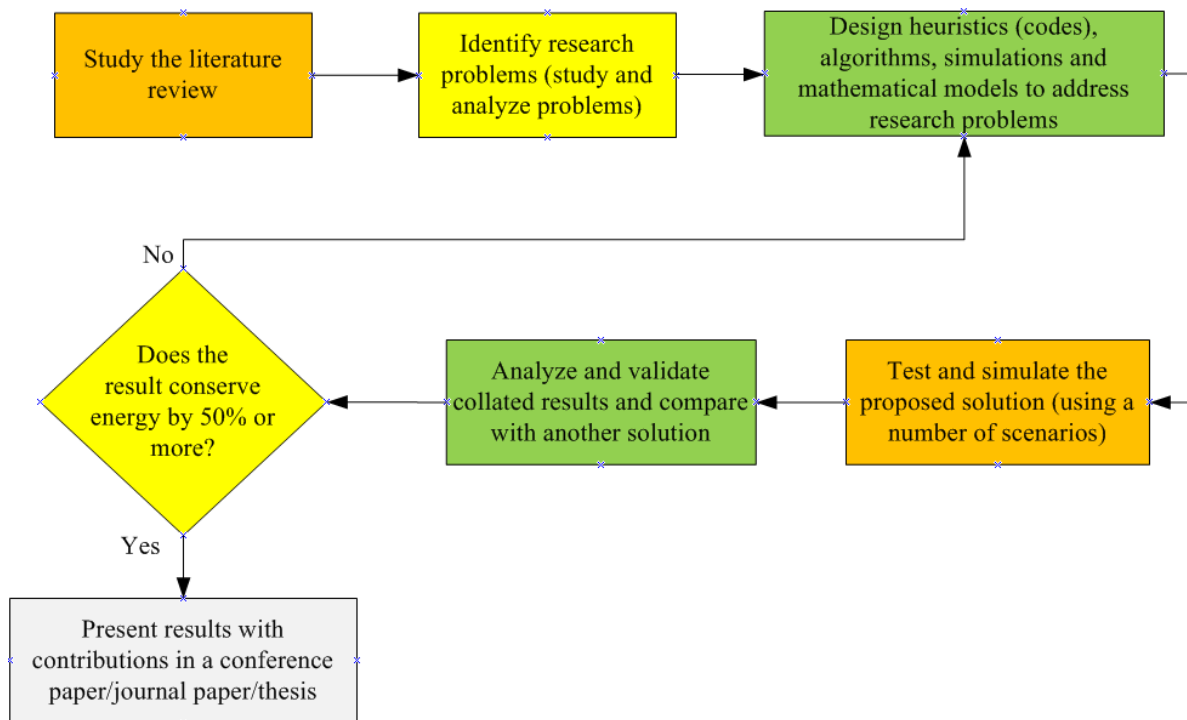


Figure 1-5: The Main Steps of Research Process

1.6 Research Contribution

The main contributions of this research are attributed toward addressing the challenges mentioned in the research definition of the problem Section. That is, reduction of the energy consumption and routing overhead of OLSR nodes for effective communication during disaster recovery and rescue operations. This research achieves this feat by modification of OLSR protocol and introduction of Time Slices (TSs). The TSs contribute to the reduction of overhead caused by overhearing and continuous broadcast control messages by OLSR, leading to over 50% energy conservation as compared to OLSRv1 and OLSRv2). The main contributions of the research are listed below:

1. Redesigned OLSR packet header through the addition of a new field, namely Originator ID (hold device's phone number). The introduction of Originator ID leads to the elimination of Multiple Interface Device (MID) messages.
2. A novel approach to reduce overhead in both sparse and dense networks, through the introduction of message specific Time Slices (TSs) which encapsulates HELLO, Topology Control (TC) and Host Network Association (HNA) messages within their respective time slices (TS). This approach prevents nodes from flooding the network with a different message which does not belong to the current TS, thereby improving link quality due reduction of crosstalk and funnel problem.

3. Modification of packet data sets by including two additional fields, namely Originator ID (PHONE_NO) and BATTERY_LEVEL. The Originator ID provides human readable device information across the network, allowing victims to recognise the sources of their messages and in case of availability of internet connection, it will be used by the victims to send and receive messages. The ability to uniquely identify each device via Originator ID renders OLSR MID messages obsolete, since devices with multiple interfaces will always include the same Originator ID/phone number, which forces recipients to accept a single message from any of the multiple interfaces, and quietly drop the rest. In addition, the BATTERY_LEVEL along with the device Network_Assignment enable Rescue Team (RT) to plan service offloading when rescuing victims whose phones act as MPR.
4. Introduction of a new message type for DS-OLSR called ALERT. This message ensures DS-OLSR devices sends and receives messages without additional overhead since ALERT message type occurs within its specific Time Slice (TS).
5. Introduction of message prioritization to DS-OLSR. The message prioritisation scheme further improves energy conservation, extend lifespan of low battery nodes, and improves mental state of victims with such devices in the aftermath of a disaster.

1.7 Thesis Structure

This Section presents the outline of the thesis organisation which consists of eight (8) Chapters.

Chapter 1 introduces the thesis with background information on the research. Followed by the motivation of research, definition of research problem, research aim and objective, research methodology and main contributions of the thesis.

Chapter 2 Presents overview of MANET including MANET history, characteristic, challenges, and applications. In addition, the provides an intensive review of classification of MANETs routing protocols with special attention to the routing protocol under optimisation (OLSR) describing the reason for choosing proactive OLSR over reactive protocols, OSLR version adapted for modification and details review of OLSR features and functionalities.

Chapter 3 presents comprehensive review of different networks for disaster recovery and rescue operations, starting with type of disasters and how successful disaster operation depends largely on effective and reliable disaster communication system. The review of disaster

recovery networks based pre and post disaster communication systems is equally presented. Finally, the Chapter concludes with review of the process of switching mobile devices to disaster mode for effective and efficient disaster communication.

Chapter 4 started with the presentation of the DS-OLSR design assumptions then proceeded with the process of switching smart phones to disaster mode. IP Address, Battery life, phone number generation scheme for DS-OLSR and DS-OLSR Time Slices with their respective messages are proposed in this Chapter. In addition, How DS-OLSR handles nodes that attempt to join the network after NFTS, proposed Disaster Management Server as well as simple approach for handling network partition in DS-OLSR were equally presented. DS-OLSR and DS-OLSRMP repositories, packet format and forwarding process, Alert and Shhh messages and modification of Hello and TC messages wraps up the Chapter.

Chapter 5 presents the implementation of the proposed DS-OLSR in NS-3 simulation environment describing the implementation models, simulation set up and analysis of the proposed scheme as compared to OLSRv1.

Chapter 6 proposes message prioritisation techniques for DS-OLSR that prioritises message from low battery devices. The Chapter describes the DS-OLSRMP structure and main features highlighting the proposed modifications to Alert message and implemented models. Simulation setup and results analysis were equally present to evaluate the performance of the proposed scheme as compared to DS-OLSR, OLSRv1 and OLSRv2.

Chapter 7 presents analytical validation of the proposed routing protocol based on the metrics used in the simulation. The Chapter compares the performance of the proposed DS-OLSRMP in both simulation and mathematical models based on energy consumption, routing control overhead, packet delivery ratio and End-to-End delay.

Chapter 8 provides major research conclusions and recommendations for future research.

Chapter 2

Historical Background of the Mobile Ad-hoc Networks and its Routing Protocols

2.1 Introduction

This Chapter presents the overview of MANET including MANET history, characteristic, challenges, and applications, all in Section 2.3. The Chapter proceeded with intensive review of classification of MANETs routing protocols with special attention to the routing protocol under optimisation (OLSR) in Section 2.4. Section 2.5 describes reason for choosing proactive OLSR over reactive protocols, OLSR version adapted for modification and details review of OLSR features and functionalities. The remaining part of the Chapter presents related work on message prioritisation scheme.

2.2 Wireless Network

Wireless network has become a choice for effective communication not only because of its successive development but also for continued decrease in price and great opportunity for users to change locations with less or no changes to their businesses. For instance, mobile wireless networks allowed mobile device users to move across states and nations yet stayed connected as long as they are within a cell coverage area with good reception. Mobile wireless network is divided into two types namely: infrastructure and infrastructure-less.

Infrastructure wireless network is a form of wireless network that allow computers, smartphones, and other wireless devices to communicate wirelessly with one another within the coverage area of an access point. The activities of such wireless devices are coordinated, controlled, and managed by a centralised base station or access point. On the other hand, the infrastructure-less wireless network allows such devices to dynamically discover, negotiate and communicates among themselves without the intervention of base station or access point. The network is independent of any fixed or prevailing network infrastructure, thus the wireless devices served as routers and utilised neighbouring nodes to relay information for out of coverage devices. MANETs and Wireless Sensor networks are examples of infrastructure-less wireless network.

2.3 MANETs Overview

First and foremost, the term Ad Hoc has been originated from Latin which means “for this situation or to be used for a special purpose” and that is why it sometimes used to describe things that are formed without previous plan and to be use for specific purpose. According to Roy (2010), this category of mobile wireless networks are refers to as Mobile Ad-hoc Network (MANET). In other words, MANET is a form of Ad-hoc network that allow wireless mobile devices to communicate among themselves autonomously without network infrastructure or base station.

As a result of fast development of wireless communication, Mobile Ad-hoc Network (MANET) has become one of the most interesting research areas not only in academia and telecommunication industries but also in disaster relief organisations. This is because the technology has been realised as the most suitable techniques to allow communication needs during disaster recovery and rescue operations. The term MANET has been defined by different scholars in different concepts. Even though, the words and sentences used are quite different in character, but the implications are not so fundamentally different. For example, Anjum, Noor, and Anisi (2015) defined MANET as a group of related mobile devices that are capable of arbitrary and dynamic movement without necessarily having a specific infrastructure or fixed base station. Similarly, Kumari, Kumar, and Bajaj (2018) defined MANET as independent, infrastructure-less and self-organising network of mobile devices. Yong et al. (2010) described the technology in terms of network of multi-hop communication as they defined MANET as a collection of two or more wireless devices that convey information from one mobile device to another without established or centralised infrastructure. It can be deduced that MANET is a wireless communication network which allow users in close proximity to communicate without the need of centralised infrastructure, and that is why it’s sometimes called a baseless network. Wireless devices in MANET network are capable of detecting the presence of other close proximity devices, setup necessary configuration to allow communication, maintain connectivity of the Ad-hoc network and have the ability to add or drop connection to and from the network. Such flexible features allows enormous applications of MANET in different areas such as disaster and emergency conditions, military battlefield, classroom, meeting and conferences (Alslaim, Alaqel, & Zaghloul, 2014).

2.3.1 History of MANET

The development of MANET could be classified into first, second, third (Bang & Ramteke, 2013) and of course fourth generations. These generations of MANET vary in terms of their features, design requirement and implementation period.

The first generation of MANET was developed by Defence Advance Research Project Agency (DARPA) dates back in 1972 with the aimed of allowing communication needs between various divisions of military personnel using packet-switched radio communication in an infrastructure-less hostile environment (Bang & Ramteke, 2013). It was called Packet Radio Network (PRNET) as it is based on RF (Radio Frequency) technology for packet transmission at 400kbps via omnidirectional spread spectrum. The PRNET used the combination of Areal Locations of Hazardous Atmospheres (ALOHA) and Carrier Sense Medium Access (CSMA) techniques for medium access and a form of distance vector routing (Ramanathan & Redi, 2002) which were highly scalable. The second generation of MANET came into existence between 1980s to mid-1990s when the MANET were further improved and implemented with the aimed of introducing packet switch network to the mobile battlefield in an infrastructure-less environment (Yi, 2010). It was called SURAN (Survival Adaptive Radio Network) and the network proved the performance of radios by making them resilient to electronic attack, cheaper, smaller and power economical with improved scalable algorithms.

The third generation of MANET emerged in the 1990s with the concept of introducing MANET in commercial applications (non-military) with notebook computers and many other viable communication equipment based on radio wave technology, and at the same time term ad-hoc network itself was adopted by IEEE 802.11 sub-committee (Ramanathan & Redi, 2002). In the last quarter of 1990s and earlier 2000s, a lot of work has been conducted related to the ad-hoc standard and intelligent equipment were put in place such as plug-in and play technology that allows the establishment and management of personal WLAN even in an areas that are not designed for such communications (Chaudet, Dhoutaut, & Lassous, 2005). Furthermore, a media access protocol was standardised by the IEEE 802.11 sub-committee based on collision avoidance and endured hidden nodes for designing MANET prototypes using notebooks and 802.11 PCMCIA cards. MANET's commercial applications were launched with the implementation of Bluetooth to transmit within short distance between earlier and mid-2000s, which allowed quick communication among personal area network users to substitute the use of wired network (Bang & Ramteke, 2013). The next generation of MANET required the

capability of handling high mobility of mobile devices (Ho, Ho, & Hua, 2010), low energy and security in order to support the different forms of emerging applications such mobile sensor networks, network for disaster recovery operations as well as vehicular network.

2.3.2 Characteristic of MANET

A MANET is an autonomous, temporary, spontaneous network of mobile devices with non-fixed infrastructure which are free to move randomly and may be found in buildings, campuses, aircrafts, ships, cars, trucks or in an open space (Vijayalakshmi & Sweatha, 2016). The network consists of wireless devices such as smart phones, iPads, laptops or MP3 players with routing capabilities that are equipped with antennas transmitting or receiving from all directions (omnidirectional), one direction (point-to-point) or both (Alsumayt, 2017). MANET system operates as a standalone fashion in an infrastructure-less environment or in an associated fashion connected to gateways and interface with a fixed network (Roy, 2011). The following are some of the characteristics of MANET:

Infrastructure-less and Autonomous: In MANET, mobile devices do not depend on established infrastructure or base station. Therefore, each device operates as both host that can send and receive data, services or application, and a router that can route information on behave of other nodes (Vijayalakshmi & Sweatha, 2016).

Dynamic Topology: In MANET, mobile devices move arbitrarily at different speeds; consequently, the topology changes randomly and rapidly at irregular time (M. Yadav & Uparsiya, 2014). As the nodes move around detects the present of other nodes and establish routing among themselves creating network dynamically.

Multi-hop Routing: In MANET, every mobile device act as a router and forwards packet on behave of other devices in an out of coverage communication (Vijayalakshmi & Sweatha, 2016). This allowed the transmission of packet through one or more nodes until the packet reaches a destination node.

Distributed Operation: In MANET, the control of the network is distributed or shared between the mobile devices as there is no backbone network for the control of the MANET operation (Aarti, 2013). The mobile devices involved in MANET are responsible for

coordination and control of the network operation. The distributed nature of MANET's operation eliminates the risk of single point of failure in more centralised networks.

Light Weight Terminal: In MANET, most of the devices used are mobile with low power storage, less memory size and low CPU capability (Aarti, 2013). These limits the operations of the network to specific areas.

Energy Constrained: In MANET, all or most of the mobile devices completely depend on batteries carried by the nodes or other form of exhaustible source of energy (Vijayalakshmi & Sweatha, 2016). Despite the numerous research on energy preservation in MANET, more research is required to optimise the network for better energy utilisation, particularly as related to MANET for disaster recovery and rescue operations.

Network Scalability: Most of MANET applications involved large network comprises of tens of thousands devices as can be found in sensor networks and combat or tactical networks (Vijayalakshmi & Sweatha, 2016). Such mobile devices move arbitrarily at different speeds and has the capability to add and drop connection to and from the network which attributed to the scalable characteristic.

Shared Physical Medium: The overall wireless communication medium is usually access by any device equipped with appropriate radio interface and enough resources which in turns limits the channel restriction.

2.3.3 Challenges of MANET

In addition to the challenges of radio communication (noise, interference and fading) that MANETs are exposed and inherited from conventional wireless communication system, there are other challenges which includes and not limited to routing as a result of dynamic topology, energy efficiency as all or most MANET devices depend largely on batteries or other form of exhaustible source of energy for their operations (Vijayalakshmi & Sweatha, 2016), and more security threats than centralised network (Aarti, 2013) such as eavesdropping, attacks, denial of service and spoofing. Despite the security challenges, the decentralised nature of MANET provide the benefit of addition strength against single point of failure in centralised (wire and wireless) network (Vijayalakshmi & Sweatha, 2016).

2.3.4 Applications of MANET

Unlike centralised/infrastructure wireless network, MANETs are applicable to be use in places without network infrastructure or where the infrastructure has become unavailable as a result of disaster. With the development in wireless communication and increase of mobile devices, there are many possible applications where MANET would be more advantageous than infrastructure networks such as in military battlefield (Vijayalakshmi & Sweatha, 2016), network for disaster recovery and rescue operations, policing as well as places where quick and temporary communication and collaboration is required (Ibrahim, King, & Pooley, 2009).

2.4 Routing Protocols in MANET

Data packets need to move from originating source to the destined receiver. Routing protocols operating within a router's network layer provides the means of routing messages between two nodes: sender and receiver (Jayanti, 2014). It is an important function for any network, whether it is wired or wireless. However, the protocols designed for routing data packets in wired and wireless networks have completely different characteristics. Routing protocols for wired networks neither need to handle mobility of nodes within the network nor minimize the communication overhead, because of their high bandwidths (Chaubey, 2013).

An important distinction between routing protocols for wired or wireless *infrastructure* network and MANET on the other hand is the requirement for centralized routers which controls the entire network. Nodes in MANETs do not require special routers hence, each node must perform routing functions in order to forward packet to a destination (Hinds, Ngulube, Zhu, & Al-Aqrabi, 2013). Additional features of MANET routing protocol include support for mobility (the ability of nodes to move around), resource constraints (Chaubey, 2013) and diverse applications (Ibrahim et al., 2009). Therefore, routing protocols need to be specifically designed for MANETs with the many possible application in mind. This indeed has been an area of focus of research for almost two decades as Hong, Xu, and Gerla (2002) is one of the oldest research(that gives a basic overview of the routing concept) and still more research are on-going as one of the most recent and detail research is that of S. Ali, Ahmed, and Raza (2019) as well as Oksiiuk and Krotov (2019). Each of this research adopts somewhat different approaches. However, this research will concentrate on the foremost classes of the MANET routing protocol.

2.4.1 Classification of MANET Routing Protocols

MANET routing protocol can be classified base on network structure, communication model, routing strategy and state information (A. Yadav & Joshi, 2012). Some researchers classify MANET routing protocols according to routing strategy, i.e., proactive (or table-driven), reactive (or on-demand) and hybrid (a fusion of both table-driven and on-demand routing algorithms) (Lalar & Yadav, 2017) (Chaubey, 2013). On the other hand, another group of researchers classified MANET routing protocols according to the network structure, since network structures affects design and operation of the routing protocols and also determine the performance with regards to scalability (Hong et al., 2002) (Verma & Soni, 2017).

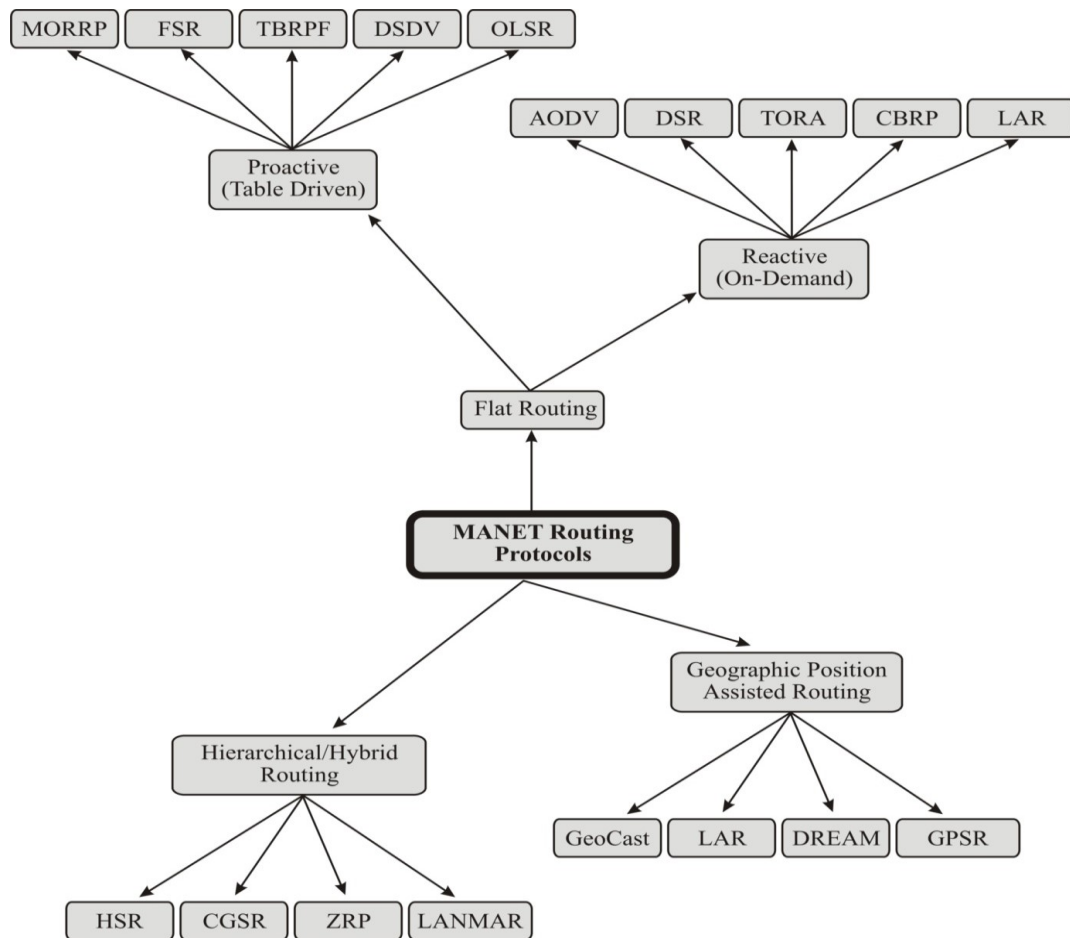


Figure 2-1: MANET routing protocols base on network structures

Figure 2-1 presents three broad categories for determining MANET routing protocols based on protocol underlying structure, design, and operation of the protocol as well as scalability under increasing load or additional nodes. The following sub-sections introduced each routing category with highlight of the key approaches.

2.4.1.1 Flat Routing Protocol

Flat routing protocols disseminate information as needed to any MANET node that can be reached. The key feature of the routing protocol category is discovery of best route hop by hop to a destination (A. Yadav & Joshi, 2012). Flat routing protocols are divided into two broad categories, proactive and reactive protocols.

2.4.1.1.1 Proactive Routing Protocols

Proactive routing protocols mandate nodes to establish routes to other nodes *in advance*. Hence every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node (Mbarushimana & Shahrabi, 2007). Therefore, nodes consult their own routing table for route from itself to a particular destination. Optimised Link State Routing (OLSR) is a renowned proactive routing protocol (Clausen & Jacquet, 2003). Others include Fisheye State Routing (FSR) (Gerla, 2002), Mobile Orthogonal Rendezvous Routing Protocol (MORRP) (Cheng, Yuksel, & Kalyanaraman, 2010), Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) (R. Ogier, Templin, & Lewis, 2004), Destination Sequenced Distance Vector (DSDV) (He, 2002). Such approaches of routing protocols generate substantial amount of maintenance traffic to maintain up to date routing tables. Equally, the routing table maintained by mobile nodes increase with the increase of network size. Also participating nodes are required to keep the entities of their routing table even during ideal time. Despite the scalability issues, proactive approach of routing has many advantageous properties that make it suitable for low latency and high message throughput applications such as low latency route accessibility as the route is already available and QoS path maintenance and support. The proactive routing protocols are discussed in the following sub-sections.

2.4.1.1.1 Optimized Link State Routing (OLSR)

Optimized Link State Routing (OLSR) protocol is a form proactive routing protocol based on link state and developed for mobile ad hoc networks (MANET) (Clausen & Jacquet, 2003). It is an optimization of link state routing (LSR) adapted to the requirements of MANET that maintain route in advance to all other nodes in a network and make them available upon needed. Each node has one or more tables that contain the latest information of the routes to any node in the network. Each row in the table has the next hop for reaching a node/subnet and the cost of this route. Each OLSR node selects a set of its one-hop neighbour nodes as multipoint relays (MPRs) and only elected MPRs can forward control traffic, intended for dispersal into the entire network. This approach reduces the number of transmission required when flooding control traffic, which is a great improvement or optimization over classical flooding algorithm used by epidemic protocol as in Figure 2-2 (Clausen & Jacquet, 2003).

A change in topology is propagated through all nodes in the network; this task is handled by MPRs who announce the link state information of their selectors in the network, leading to a recalculation of the shortest path routes (SPR) to all destinations in the network. Link state information is sent periodically via control messages. This announces to the entire network that the announcing MPR can reach the node or nodes that elected it as an MPR. MPRs are included in route calculation; the result of such calculation provides the route from a given node to any destination in the network.

From the preceding, it is easy to deduce that MPRs form the backbone of the OLSR protocol, since they oversee forwarding control messages about associated links, along with message routing on behalf of their electors. This implies mobile devices acting as MPRs are subjected to heavy CPU, memory, and communication subsystem usage. This eventually precipitates rapid draining of battery energy, leading to network partitioning (since a whole lot of MPRs devices will switch off), thereby reducing the overall lifespan of the entire network. Nonetheless, OLSR is a major improvement over other flooding algorithms such as epidemic routing, where network messages are often repeated unnecessary, with a single node receiving the same message from several nodes as in Figure 2-2.

A major challenge facing OLSR is the concept of overworked MPRs, these MPRs often route a lot of network traffic on behalf of other nodes, which causes a severe drain to stored battery energy, and eventually shutdown.

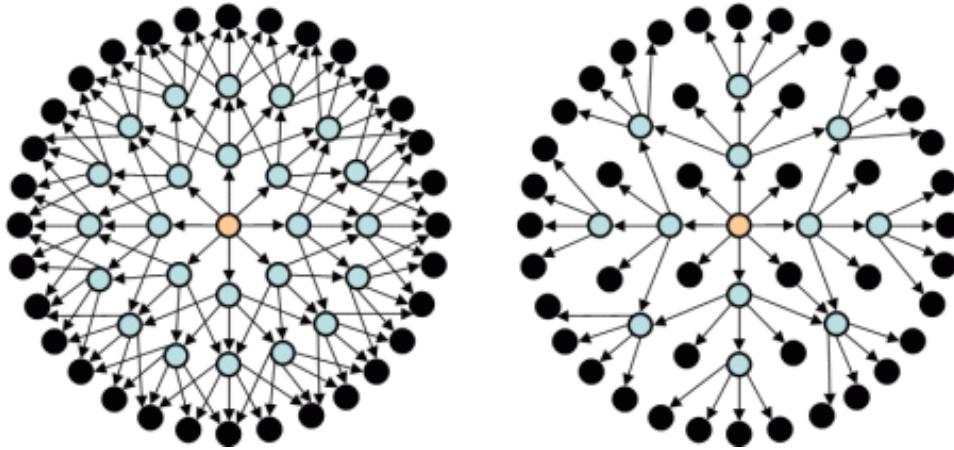


Figure 2-2: Showing classical flooding (left) and MPR flooding (right) (Adjih et al., 2003)

The latest version of OLSRv2 draft document (Clausen et al., 2014) recommends the existence of two MPRs, one to handle network flooding of control messages and another to handle message routing on behalf of electors. This distributed approach is intended to reduce the current workload of a single MPR in classic OLSR. The prominent role played by MPRs in OLSR made it both a saviour and a curse. A saviour when MPRs are properly represented all over the network and a curse when a single MPR route and flood messages on behalf of several nodes, leading to network collision which forces batteries to drain faster, since each node will keep trying to retransmit previous data. However, rapid draining of battery energy is still a major problem even with the recent incarnation of OLSR called OLSRv2.

2.4.1.1.1.2 Fisheye State Routing Protocol (FSR)

Fisheye State Routing (FSR) (Gerla, 2002) introduces the concept of *scopes* in a bid to reduce routing update overheads in large MANETs. Each node within a scope stores the Link State for every destination in the network. It periodically broadcasts the Link State (LS) update of a destination to its neighbours with a frequency that depends on the hop distance to that destination. The Periodical broadcasts of LS info are conducted in different frequencies depending on the hop distances (Mishra, Singh, & Tripathi, 2019). The further the distance, the less frequent the broadcast, while smaller hop distance receives more frequent broadcasts.

The fisheye scope is defined as the set of nodes that can be reached within a given number of hops (Gerla, 2002). An example of a fisheye scope (at node A) of hop 2 and 3 is shown in Figure 2-3.

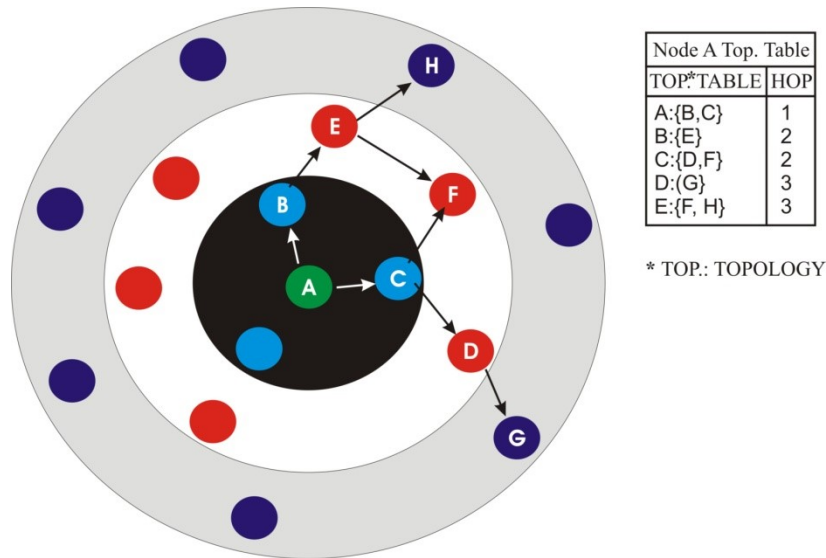


Figure 2-3: Example of Fisheye State Routing Protocol with sample Topology Table (Gerla, 2002)

Note that in Figure 2-3, node E can be reached through B from A with 2 hops and through F with 3 hops. Since the minimum path length is 2, node E is within the fisheye scope of node A. Scopes that will cover the entire network can be created by setting multiple hop radius. Each node is expected to maintain both topology and routing tables of its neighbours. The Topology table records the topology information obtained from the link state message and represents each destination as an entry in the table. On the other hand, the routing table provides the next hop information to forward the packets for the other destinations in the network. Entries are updated when topology table is changed. However, FSR was never released to the public as a stand-alone routing protocol, and its specification was never finalized (Gerla, 2002). The base principle was included in the widely popular OLSRd daemon, which is an open source implementation of the OLSR routing protocol (Shenbagapriya & Kumar, 2014).

2.4.1.1.1.3 Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)

Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) (R. G. Ogier, 2002) is a proactive, link-state routing protocol designed for MANETs. It provides multi-hop routing along shortest paths to each destination. Each node computes a source tree showing paths to all reachable nodes based on partial topology information stored in its topology table; this is achieved via a modification of Dijkstra's algorithm (Hill, 2015) (R. Ogier et al., 2004). TBRPF attempts to minimize overhead by enforcing partial report of source trees by nodes to their

neighbours under low bandwidth, while the full source tree is reported under high bandwidth (R. Ogier et al., 2004).

Neighbouring nodes are discovered using differential HELLO messages. Each link-state update is broadcast reliably along a dynamic min-hop-path tree rooted at the source (for instance source A – see Figure 2-4) of the update.

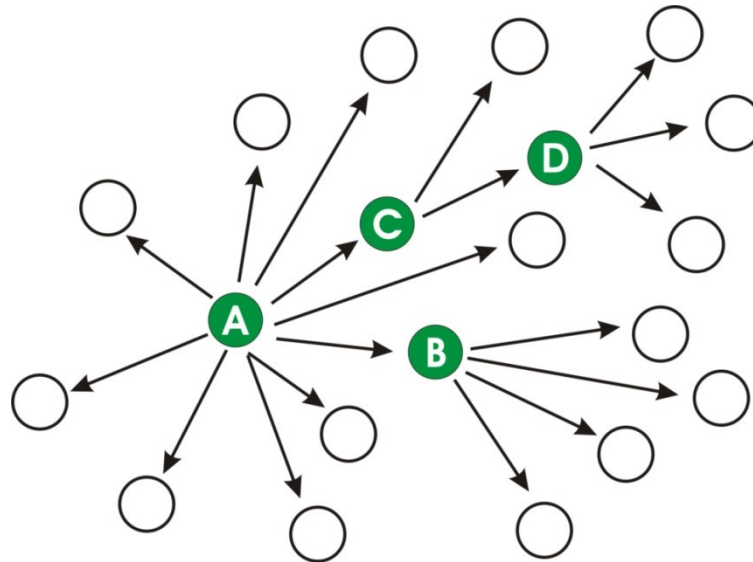


Figure 2-4: Only 3 non-leaf nodes flood messages generated by node A (R. Ogier et al., 2004)

Differential HELLO messaging approach reports only changes in the status of neighbouring nodes; hence HELLO messages are much smaller than those of other link-state routing protocols such as OSPF. Only non-leaf nodes forward update messages in TBRPF, non-leaf nodes are like OLSR MPRs. Unlike MPRs which are limited to 2-hop nodes, non-leaf nodes are limited to a min-hop-path which changes dynamically. A typical routing table for TBRPF is shown Figure 2-5.

As promising as TBRPF protocol is, it was never widely adopted by the research community, one of the reasons being the decision by the copyright owner (Standard Research Institute (SRI) International) to limit access until TBRPF became a standard. This decision was succinctly justified by Ogier in 2002 during Internet Engineering Task Force (IETF) MANET Working Group meeting, he wrote in his PowerPoint presentation of TBRPF features the following words *“Our patent rights statement (included in the draft) protects SRI **only** if TBRPF does not become an IETF standard. (Why should SRI give up its rights in this case?)”*.

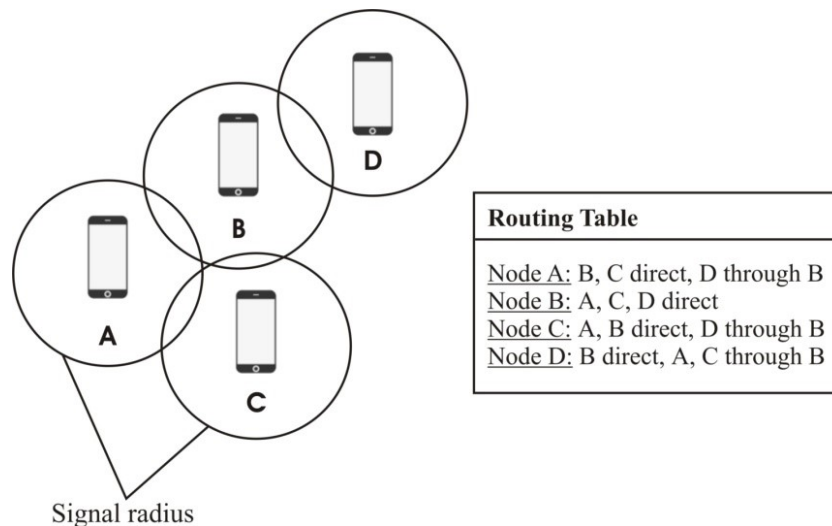


Figure 2-5: Sample routing table for TBRPF (R. Ogier et al., 2004)

If TBRPF (or any part of it) becomes a standard, anyone can use it for any purpose for free” (R. G. Ogier, 2002). Although IETF has accepted TBRPF as a standard (RFC 3684) (R. Ogier et al., 2004), the standard is labelled experimental and researchers are invited to comment on it. Nonetheless, researchers have moved on with OLSR and other Open-Source protocols. It is noteworthy that NS-3 does not have native simulation modules/libraries for TBRPF.

2.4.1.1.4 Destination Sequenced Distance Vector (DSDV)

Destination Sequenced Distance Vector (DSDV) is a proactive, table-driven protocol where all nodes maintain a routing table entry for every other destination in the network. A typical route table entry contains next hop for a destination, number of hops to reach the destination, a sequence number, and the time the entry was recorded (Saudi, Arshad, Buja, Fadzil, & Saidi, 2019). DSDV adopts classic Bellman-Ford routing algorithm and improves on the Routing Information Protocol (RIP) by solving routing loop problem (He, 2002). Bellman-Ford routing algorithm is similar to Dijkstra's algorithm (Hill, 2015), but it works with graphs in which edges can have negative weights (Dijkstra support positive weighted values only). DSDV routing tables are populated through the following updates:

Broadcast Routing Updates: These updates are incremental and occurs when new nodes join the network, or when a node leaves the network and creates link breakage. The update fits into a single packet and occurs frequently.

Full Dump updates: These updates contain the whole routing table of a node; transmission may take multiple packets and it is sent infrequently.

Figure 2-6 represents routing tables for three mobile devices running DSDV. Sequence numbers are generated even if there is a link between two devices. Odd numbers are used to represent link failure between devices. Generally, sequence numbers are generated and advertised by each node in the network, however, when a node detects broken link between itself and another node, it increments the sequence number of the out-of-range node by 1 and advertises the new odd numbered sequence number (see figures 2-7 and 2-8).

Entries having the same sequence numbers over a fixed period are considered outdated. Such entries as well as the routes using those nodes as next hops are deleted. The installed time value determines when to delete an entry (He, 2002).

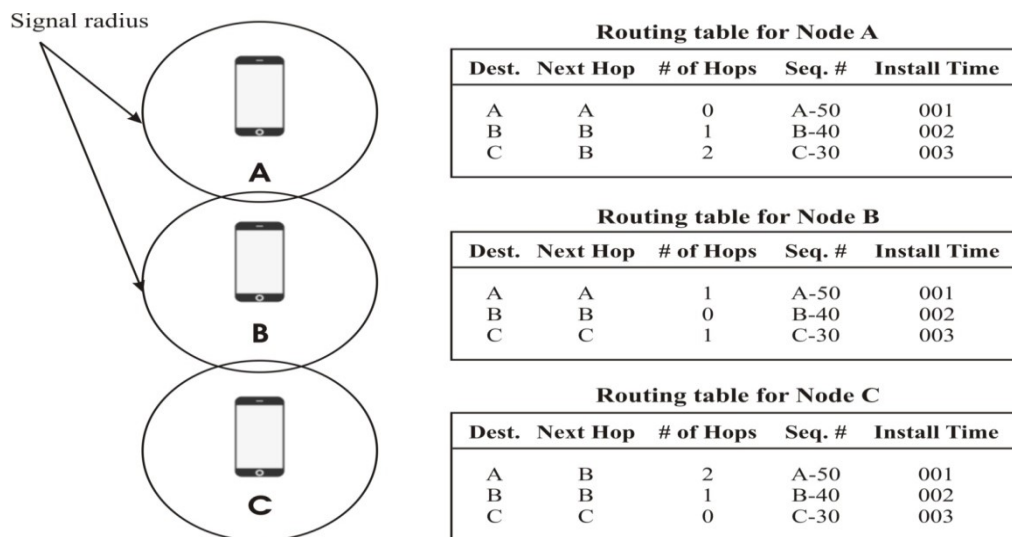


Figure 2-6: Sample routing tables for DSDV nodes (He, 2002)

In Figure 2-7 above, node B detected a broken link between itself and node C, this triggers a modification to node B's routing table. It increments node C sequence number by 1 and deleted the old entry with the old number. Thereafter it advertises such modification to accessible nodes in the network (see Figure 2-8), which caused node A to equally delete node C's old entry and record the new one.

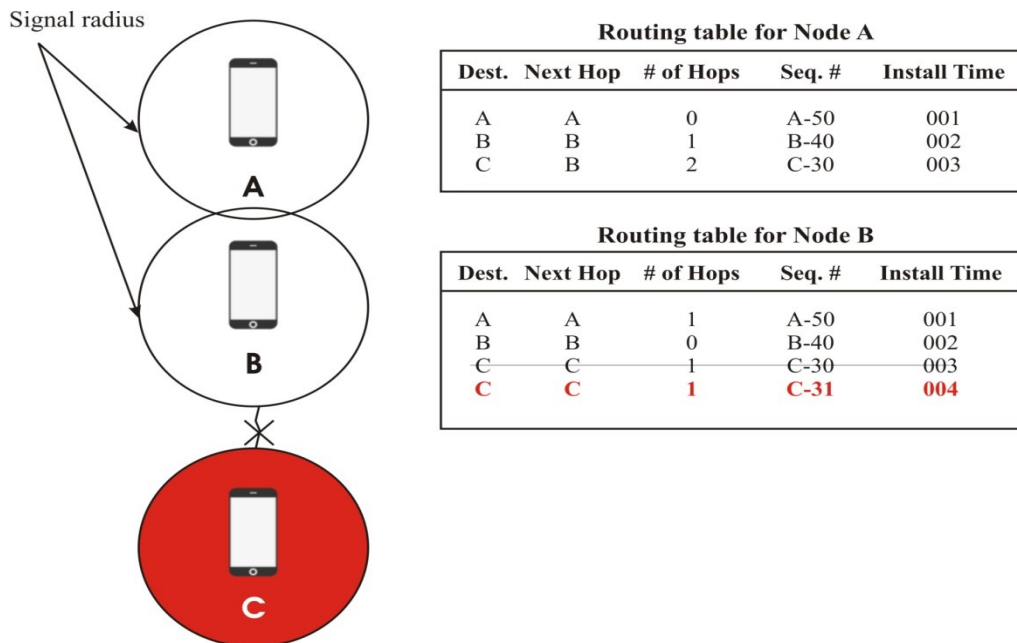


Figure 2-7: DSDV routing table with broken link detected by Node B (He, 2002)

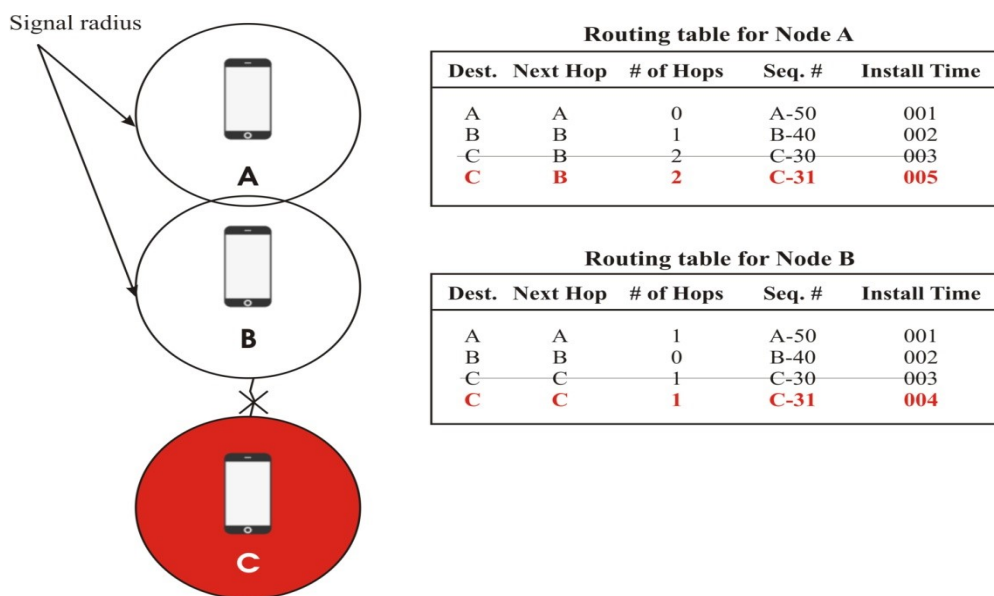


Figure 2-8: Node B advertises changes to its' routing table to Node A (He, 2002)

2.4.1.1.1.5 Mobile Orthogonal Rendezvous Routing Protocol (MORRP)

Mobile Orthogonal Rendezvous Routing Protocol (MORRP) (Cheng et al., 2010) is derived from Orthogonal Rendezvous Routing Protocol (ORRP) (Cheng, Yuksel, & Kalyanaraman, 2009). ORRP is originally designed as a routing protocol for fixed wireless mesh networks; it utilizes directional communications via directional antennas or free-space optical (FSO) communication devices (Gibson et al., 2004). Both directional antennas and FSO devices allow

ORRP to adopt line of sight (LOS) when routing messages (Cheng et al., 2009). LOS allows ORRP to organize nodes around its 2-D Euclidian space. Nodes are partitioned along an imaginary pair of orthogonal lines centred at different points; any node located at the intersect points (rendezvous points) will forward packets as shown in Figure 2.-9. Nodes periodically send ORRP announcement packets orthogonally around the network, nodes that receives the packets stores the route to the source of the ORRP announcement and the node it received the announcement from (previous hop).

In summary, messages are sent to the sender's 1-hop neighbours using the direction antenna or interface that faces the neighbour. Neighbouring nodes are imagined to reside on orthogonal lines; hence a packets hop until it gets to the rendezvous point node where it can be routed to the destination node (Cheng, Yuksel, & Kalyanaraman, 2007).

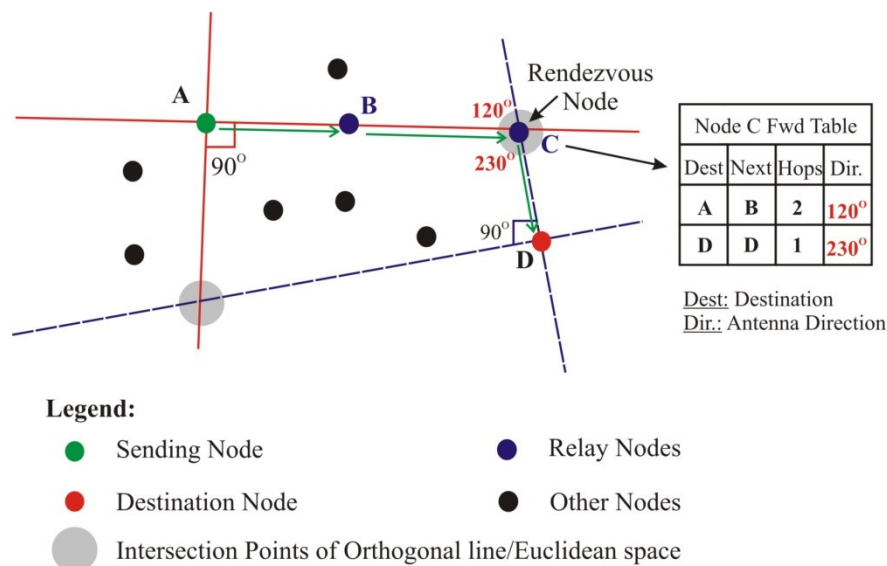


Figure 2-9: Sender sends packets to rendezvous node which in turn forwards to Destination (Cheng et al., 2010)

MORRP extended ORRP by incorporating support for mobility. Cheng et al. (2010) discovered that the **high reachability** value of classic ORRP dropped from 98% to 42% in a mobile environment. The researchers solved mobility problems encountered with classic ORRP through a new kind of routing table called Directional Routing Table (DRT). The table stores information using both Near Field DRT and Far Field DRT to populate DRT. MORRP use Near Field DRT to match for nodes that are 2-3 hops away and Far Field DRT for nodes that are further away.

A major drawback of MORRP is that directional antennas and FSO hardware for mobile devices (phones, laptops, and tablets) are not yet mainstream (Xian Wang, Hsu, & Jin, 2008). Again, unlike OLSR protocol, research works on MORRP are still largely theoretical and not yet implemented on actual portable mobile devices (Cheng et al., 2010).

2.4.1.1.2 Reactive Routing Protocols

Reactive (on-demand) routing protocols mandates nodes to establish route to a destination only when they are required (Alotaibi & Mukherjee, 2012). Once a communication route is required, the source node initiates route discovery process (which is required for every unknown destination) (Kodole & Agarkar, 2015). The process is initiated by flooding the network with request packet using route discovery mechanism (Szücs & Wassouf, 2018). Any node that receives the route request packets replies if it has the routing information, otherwise the route request will be rebroadcasted, and the process continues until all possible routes have been scrutinised. When a route to a particular destination is identified, the source node will maintained route until the route becomes unavailable or no longer required (Mishra et al., 2019). Active routing table may become worthless because of nodes mobility and therefore, reactive routing protocols need to conduct route maintenance. Furthermore, route discovery process in reactive protocols occurs each time a node want to send data and suffers high message latency in expense of initial route discovery procedure as the route lookup incurred some time (Yi, 2010). Nevertheless, reactive routing technique can dramatically reduce routing overhead of a network if the frequency of route discovery is relatively low. Reactive routing protocols are suitable for networks with low and medium traffic and are more appropriate to large networks that proactive routing techniques (Kodole & Agarkar, 2015). Ad-hoc on demand Distance Vector (AODV) (Das, Belding-Royer, & Perkins, 2003) and Dynamic Source Routing (DSR) (Johnson, Hu, & Maltz, 2007) are renowned reactive routing protocols. Others include Temporary Ordered Routing Algorithm (TORA) (V. Park, 2001) and Location Aided Routing (LAN) (Ko & Vaidya, 2000). The routing techniques are discussed in the following sub-sections.

2.4.1.1.2.1 Ad-hoc On-Demand Distance Vector (AODV)

Ad-hoc On Demand Distance Vector (AODV) Routing Protocol (Das et al., 2003) is one of the most popular reactive MANET routing protocols that established routes only on-demand.

AODV does not maintain routing table but only build the table whenever a node wants to communicate with another node (Rajkumar, Kasiram, & Parthiban, 2012). Three (3) route messages are used in AODV routing procedure: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) (Munisha Devi, 2018). Route discovery process starts when a node requires a route to a particular destination by broadcasting a RREQ. When the RREQ message received by a destination node or a node that knows a usable route to the destination, then a RREP packet will be generated in form of unicast and send to the source node (Mohseni, Hassan, Patel, & Razali, 2010).

A RERR message (Liu, Yang, & Wang, 2013) is used to notify neighbouring node when there is link failure during communication time. Once AODV is enabled, every node stores the information of its next hop for packet transmission. A source node originates RREQ broadcast packets for unknown destination which includes some parameters, for example source and destination addresses, unique RREQ ID and most recent known sequence number of destination node (Liu et al., 2013). This information allows loop and RREQ duplicate free operation. For example, RREQ ID allows neighbouring nodes to check if they previously received same request and sequence number is used to determine the freshness of a route. TTL (Time-To-Live) is also used in AODV to reduce network traffic (Karaulia & Bharot, 2014). A RREQ packet begins with small number of Link Lifetime (LLT), let say LLT=1 and then increased to LLT=2 if the destination route is not found using the initial LLT. Upon receives of RREQ, an AODV node checks the availability of fresh route to destination. However, if there is no active route available, then a broadcast of the RREQ packet will be send to its neighbours for active route identification (Karaulia & Bharot, 2014). During this process, all nodes that received the RREQ stores a route back to the source node as the originator of the RREQ. Once the node with a valid route receives the RREQ, a RREP packet is generated and sent to the source node as unicast and intermediary nodes (Liu et al., 2013) along the path of RREQ update records with sequence numbers of the destination. The propagation of RREQ and RREP from Source node S to Destination node D using AODV is shown in Figure 2-10.

Despite the benefits of AODV such as reduced message overhead, less storage space for routing information and the use of sequence number to determine the freshness of a route (Rajkumar et al., 2012), but yet it uses flooding techniques which results to redundant retransmission and of course, nodes experience high delay during route discovery process (Kodole & Agarkar, 2015) and as such transmission delay increases with the increase network capacity.

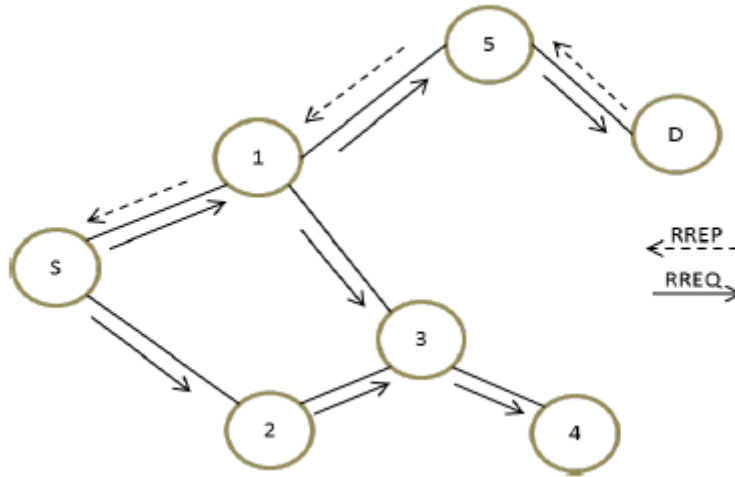


Figure 2-10: Propagation of RREQ and RREP from Source node S to Destination node D using AODV (Rajkumar et al., 2012)

2.4.1.1.2.2 Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is an on-demand routing techniques that uses source routing mechanism (Kaur, 2011) whereby source node includes complete route from source to destination node in the packet (Johnson et al., 2007) which requires nodes to determine all nodes a packet traverses to a destination. As identified in RFC 4728 (Johnson et al., 2007), each node is required to maintain a route cache containing source routes that are familiar by all other nodes and continually update the route cache as new route to the source node is observed. DSR consist of two major operational phases called route discovery and route maintenance (Mishra et al., 2019). For route discovery, when a node has a packet for transmission, it look-up to its route cache for available route to the destination. If the node does not have a valid route, then a route discovery process will be initiated by broadcasting RREQ message to neighbouring nodes. The RREQ contains the destination address as well as the list of intermediate node addresses that the message passes through. Each node that received the message will check it routing cache for available route to the desire destination. However, if there is no valid route found, a local broadcast will be retransmitted by the receiving node adding it self-address to the route record (Mishra et al., 2019). A RREP message is usually generated as soon as the RREQ reaches either the target node or middle node that has the valid route to the destination. The route discovery process of the DSR techniques is shown in Figure 2-11.

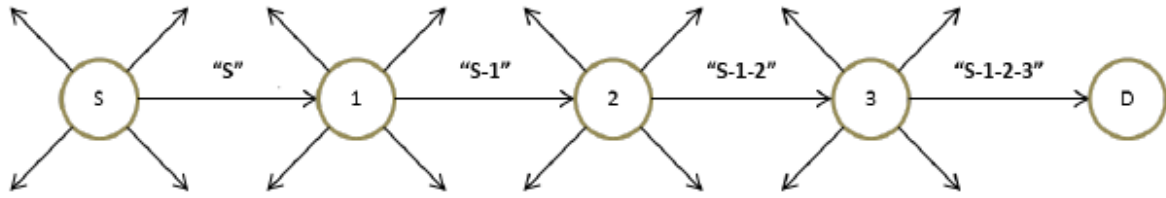


Figure 2-11: Propagation of Route Discovery Message from Source node S to Destination node D (Johnson et al., 2007)

Once a route is identified and established between source and destination nodes, the complete path that a packet needs to pass through the destination will be specified in the packet header (Rajkumar et al., 2012). Intermediate nodes are responsible for forwarding messages as it is in the message source route. Equally, they are responsible for the next hop recipient verification. When a broken link is found, a route error (RERR) message will be generated and sent to the originator of the message (Kaur, 2011). The RERR contains the address of the RERR originator and the address of the un-reachable node. Once the source node receives the RERR, a route cache check will be conducted for a valid route otherwise a route discovery process will be initiated to send a new RREQ. As mentioned earlier, DRS uses the techniques of source routing, and this allows source node to determine all sequence of nodes that each packet passes through. Consequentially, the sequence of the nodes are required to be included in every packet header which result to routing overhead (Mishra et al., 2019). However, in terms of benefit, the techniques allow intermediate nodes to easily learn different route from the source routes included in packets as route identification is generally an expensive task in respect to bandwidth, energy and time. In addition, the source routing technique reduces routing loops as the determination of complete transmission route is done by a single node instead of node-by-node decision.

2.4.1.1.2.3 Temporary Ordered Routing Algorithm (TORA)

Temporary Ordered Routing Algorithm (TORA) is a highly adaptive, distributed and loop-free routing protocol (V. Park, 2001) that is based on link reversal algorithm and source initiated concept (Islam, Riaz, & Tarique, 2012). The routing algorithm is designed to reduce the reaction of topology alteration by localising routing related information to a set of devices that are close to the topology change location (V. D. Park & Corson, 1997). Route creation, route maintenance and route erasure are the three main operations of TORA (Mohseni et al., 2010). Routing packet from source to destination nodes using TORA requires a sequence of direct

link between the source node and the destination node leaving intermediate nodes with the task of maintaining heights which is measured based on the number of nodes between the intermediate nodes to destination node (Alotaibi & Mukherjee, 2012). The assignment of height metrics is carried out by the use of Directed Acyclic Graph (DAG) rooted at the destination node (Mishra et al., 2019). Each node maintains a rational direction of its link to destination node using the height metric value, and the direction of the logical links is determined from a node with highest height metric value to a node with lowest height metric value (Reddy, Vishnuvardhan, & Ramesh, 2013). The DAG creation is shown in Figure 2-12. The arrows between nodes indicate the direction of wireless links from the node with highest height to the lowest height node toward destination. This signifies that, data packets are routed to a neighbouring node with lower height metric than the height metric of the forwarding node (Alotaibi & Mukherjee, 2012). In other words, a node can only forward data packet to neighbouring with height metric lower than its own height. As mentioned earlier, the height of every node represents the number of nodes a packet needs to pass through, and this information is stored by each node once the DAG process is completed. The stored information can be reused by the intermediate node to speed up the next DAG creation. In addition, removal or failure of nodes can be easily resolved by switching to an alternate route without the intervention of source node. One of the major drawbacks of this protocol is the dependency on intermediate nodes lower layer for some functionalities (Reddy et al., 2013), such as dependency on synchronised clock between nodes for Ad-hoc network.

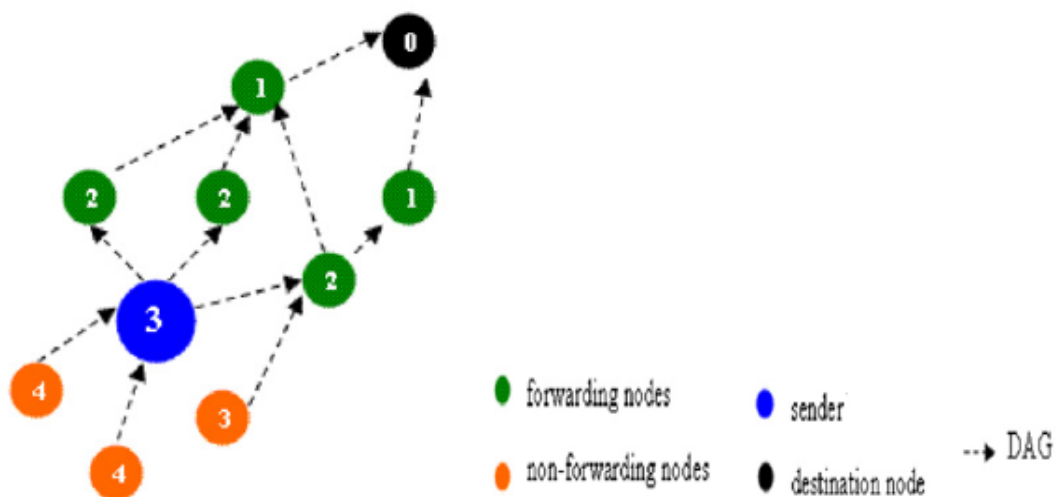


Figure 2-12: DAG with height value of each node in the network towards the destination node (Alotaibi & Mukherjee, 2012)

2.4.1.1.2.4 Cluster Based Routing Protocol (CBRP)

Cluster Based Routing Protocol (CBRP) is a form of On-Demand routing Protocol that allow node to form clusters (Jiang, 1999) whereby each cluster is headed by a master node or what is referred to as cluster head, that maintains and manages connection and communication within cluster as well as with other clusters (Yu, Qi, Wang, & Gu, 2012). At start, all CBRP nodes are in “undecided” mode. For a node to join a cluster, a time-out period and hello message will be broadcasted. Once the message is received by a cluster head, then the cluster head will reply back with a triggered Hello message and the undecided node will change its status to Member node (Khatkar & Singh, 2012). However, an undecided node announces itself as a cluster head in subsequent Hello message for failure to receive a triggered Hello message after several repeated joining process in time-interval.

The major components of CBRP operations are Cluster Formation, Cluster Discovery (Adjacent) and routing which is entirely distributed (Jiang, 1999). The routing protocol proactively obtains its 2 hop topological information via the exchange of Hello messages. However, the protocol function reactively as it gets route information only when needed in three (3) phases namely: route discovery, packet routing and route removal (Jiang, 1999). Each node in CBRP maintains neighbouring table contains neighbour’ ID, link status (Uni/Bi-Directional), Role (Cluster Head/Member) and periodically broadcast the information in Hello message (Jiang, 1999). The information of all Cluster members is kept with Cluster Head and that of all Cluster heads of its neighbouring clusters. When a source node requires to send a packet and no active route found in its routing table, then a Route Discovery will be initiated by sending RREQ message to Cluster Head. The Cluster Head will check if it has the destination in its local cluster otherwise it will flood the RREQ to it neighbouring Cluster heads which in-turns, if not found in their local clusters broadcast it to their neighbouring cluster heads as shown in Figure 2-13. A RREP message will be send as a reply whenever the destination is found. However, the source node will activate an exponential back-off If no RREP message received within the time interval and resend the RREQ packet again (Yu et al., 2012). The main disadvantage of this routing algorithms is the routing overhead attached to cluster formation and its maintenance. Furthermore, inconsistent routing information are maintained by some nodes as a results of long propagation delay and inter cluster routing information is shared by Cluster Heads only.

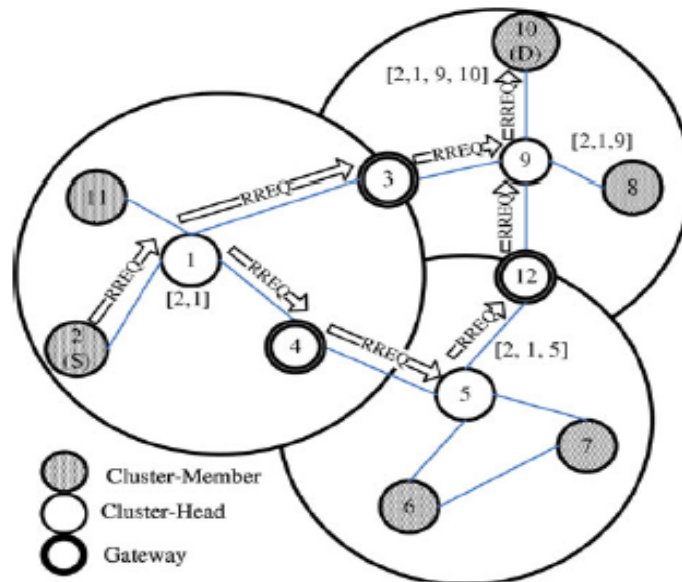


Figure 2-13: Flooding Cluster Heads with RREQ packets from Cluster Member 2
 (Source: (Safa, Artail, & Tabet, 2010))

2.4.1.2 Hybrid Routing Protocols

Hybrid routing protocol combines the concept of both proactive and reactive routing techniques in an attempt to utilise the advantages of the routing schemes to overcome their weaknesses (Pandey, Ahmed, Kumar, & Gupta, 2006) such as network overhead in proactive and latency problem in reactive (Khatkar & Singh, 2012). The general idea behind the routing techniques is the ability to divide network into different zones whereby proactive routing protocol is used for route establishment within a zone and reactive routing protocol is responsible for outside zones routing (Mishra et al., 2019), which is quite appropriate for large networks where a huge number of nodes are involved. In an effort to overcome mobility issues, Hybrid routing schemes use proactive routing to establish routes in low mobility nodes while reactive routing for high mobility nodes (Boukerche et al., 2011). However, the performance of routing techniques depends largely on the optimal distribution of the two techniques on network nodes. Even though the routing scheme suffers from complexity in operation, it reduces route setup latency for nearby nodes and low routing overhead for far away destinations (Reddy et al., 2013). Zone Routing Protocol (ZRP) (Pearlman & Haas, 1999) is the most popular Hybrid routing protocol.

2.4.1.2.1 Zone Routing Protocol (ZRP)

Zone Routing Protocol (ZRP) (Pearlman & Haas, 1999) is a form of hybrid routing algorithms that divides network topology into zones with the aim of utilising the techniques of reactive

and proactive protocols for intra-zones and inter-zones routing on the basis of the merits and demerits of these protocols. The routing zones expressed in hops with a radius p which is defined separately for each node (Bejar, 2002) and there may be overlapping zones as much as possible to help in route optimisation (Boukerche et al., 2011). Figure 2-14 illustrated the route discovery process of ZRP whereby all nodes are within the routing zone of node S except node K. It can be seen from the Figure again that zones is defined in hops but not in physical distance and the circle around the subject node is used to denote the radius of the node (Pearlman & Haas, 1999).

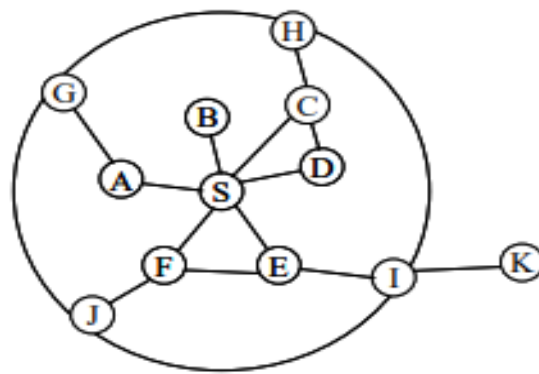


Figure 2-14: Representation of Routing Zone with $p=2$ and Node S as the Node in Question (Bejar, 2002)

As mentioned earlier, the protocol uses Intra-zone Routing Protocol (IARP) or proactive node discovery mechanism for route discovery in intra-zone communication while inter-zone routing protocol (IERP) or reactive mechanism route discovery between two or more different zones. Therefore, data packet can be delivered instantly for nodes of the same zone as the nodes kept routing information for all nodes. However, if the source and the destination nodes are in different zones, then a reactive route discovery mechanism will be called out for suitable route. Even though the routing scheme suffers complexity in operation, but reduces route discovery latency for nearby nodes and low routing overhead for far away destinations (Reddy et al., 2013).

2.4.1.3 Hierarchical Routing Protocols

Hierarchical routing techniques organise network into group of nodes called clusters or zones whereby each cluster is headed by a gateway or head to improve the efficiency and scalability of the routing (Szücs & Wassouf, 2018). Some scholars are on the view that cluster approaches

are limited to two hierarchical levels while hierarchical approaches supports more than two level (Alotaibi & Mukherjee, 2012). However, the responsibility of maintaining connectivity between nodes within cluster is assigned to cluster heads as cluster members can only communicate with their own head and with other members within their cluster (Hong et al., 2002). Similarly, gateways are responsible for managing the inter clusters communication as only gateways communicate with two or more cluster heads that belongs to different clusters.

Hierarchical routing protocol may implement hybrid routing mechanism. For example, reactive routing mechanisms may be used for inter clusters routing while proactive mechanism can be used for routing within a cluster (Boukerche et al., 2011). This approach increases scalability and reduces maintenance traffic as failure of node or topology change affects only the cluster in question but not the entire network, and can be fixed easily with intra cluster update packets (Hong et al., 2002). Hierarchical routing approach seems to work well with high density networks as it provides low routing overhead, quick route setup time and easy nodes failure or topology changes adaptation. However, cluster heads need to be carefully selected as they may cause bottleneck issue in terms of handling high traffic. Furthermore, the routing technique consumed power in large cluster network, which may virtually compromise the performance of the routing scheme (Mishra et al., 2019) (Alotaibi & Mukherjee, 2012). Examples of routing techniques in this category are Landmark Ad-hoc Routing (LANMAR) (Pei, Gerla, & Hong, 2000), Hierarchical State Routing (HSR) (Patel, Elleithy, & Rizvi, 2009) and Distributed Dynamic Routing (DDR) (Nikaein, Labiod, & Bonnet, 2000) and the most popular of them is discussed below.

2.4.1.3.1 Landmark Ad-hoc Routing (LANMAR)

Landmark Ad-hoc Routing (LANMAR) is an efficient hierarchical routing protocol that has the features of Fisheye State Routing (FSR) (Gerla, Hong, & Pei, 2000) which designed to reduce the amount of routing entries required and routing update overhead in a high density ad-hoc network (Y.-Z. Lee et al., 2005). It was initially used in fixed WAN which required a pre-defined multi-level hierarchical addressing scheme (Pei et al., 2000). LANMAR routing techniques partitioned network nodes into logical subnets whereby each subnet contain nodes that are likely to move as a group with common objectives such as rescue team members and medical team members in disaster area (Pei et al., 2000). Each logical subnets elects a node to serve as a landmark dynamically and of course each node keeps only routing information of

nodes within its scope and land mark nodes (Boukerche et al., 2011) as in Figure 2-15. This makes the routing protocol suitable for large ad-hoc networks as it significantly reduces routing update overhead and the size of routing tables. The main idea behind LANMAR scheme is the ability to avoid routing information flooding by allowing nearby nodes to exchange routing information at higher frequency with source node whereas faraway nodes exchange at lower frequency (Nong, 2014).

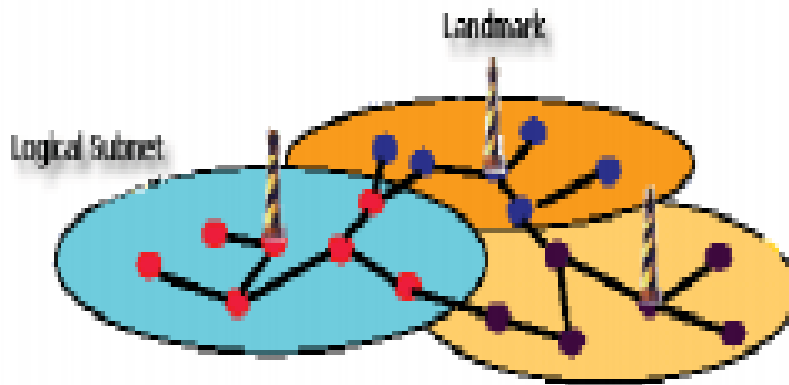


Figure 2-15: Overview of LANMAR indicating logical subnet and a Landmark Node (Nong, 2014)

During the process of packet transmission, LANMAR nodes forward packet directly to destinations within their scope otherwise the packet will be routed to a nearest landmark node toward the destination. Proactive routing protocols such as FSR, OLSR and TBRPF are used for routing within local scope (Y.-Z. Lee et al., 2005). Therefore, two forms of routing tables are kept by every node: Local routing table (for direct routes to nearby destination) and Landmark routing table (for routes to all Landmarks of all the subnets).

2.4.1.4 Geographic Routing Protocol (GRP)

Geographical Routing Protocol (GRP) is a form of routing techniques that uses node locations to route packets to a destination rather than network addresses (Raval & Shah, 2011). GRP uses Global Positioning System (GPS) to determine the location of nodes (Zhiyuan, 2009). However, if a node is unable to determine its actual location as a result of been situated inside rooms or buildings. Consequently, the assumption that every node knows its location fails and such node will not be able to send or receive information. The main benefit of this routing techniques is that nodes do not necessarily needs to have full knowledge of network topology

but its own location and the location of destination node (Alotaibi & Mukherjee, 2012). Using this information, a packet will be successfully delivered to destination without prior route discovery or complete topology knowledge.

In GRP, there are three routing strategies: Single-Path, Multi-Path and Flooding (Alotaibi & Mukherjee, 2012). The first strategy transmits one copy of message from source to destination node via a single defined route. Contrary to the Single-Path, Flooding strategy implements broadcast techniques where the same messages are flooded all over the network via different routes. As single-path and flooding strategies are two extreme approaches of GRP, Multi-path strategy tend to strike a balance between the solutions whereby few copies of the original message are created and routed toward destination via different routes. Location-Aided Routing (LAR) (Ko & Vaidya, 2000), Greedy Perimetre Stateless Routing (GPSR) (Karp & Kung, 2000) and Blind Geographic Routing (BGR) (Witt & Turau, 2005) are examples of protocols that use nodes location to route packet and the most popular of them is discussed in the following sub-section.

2.4.1.4.1 Location-Aided Routing (LAR)

Location-Aided Routing (LAR) is a form of Geographical Routing protocol that adopts on-demand routing techniques with an attempt to minimise control message overhead by utilising location information of nodes generated through GPS technology (K. Singh, Sharma, & Singh, 2015). LAR techniques also adopted the concept of request zone and expected zone (Chavan & Srikanth, 2012) to reduce flooding by modifying the route discovery procedure to be carried out based on the request zones and expected zones. LAR Scheme1 and LAR Scheme2 (Alotaibi & Mukherjee, 2012) are the most popular routing algorithms for LAR techniques that are based on zone calculations: Request zone and Expected zone, as shown in Figure 2-16.

LAR Scheme1 uses the expected zone or location during the process of route discovery to determine a request zone (Alotaibi & Mukherjee, 2012). The request zone in Scheme1 is the rectangular area that includes the current location of the source node and the expected zone for the destination node as in Figure 2-16. LAR Scheme2 uses the previous location information of the destination node as a requirement for defining request zone which indirectly embedded in route request message.

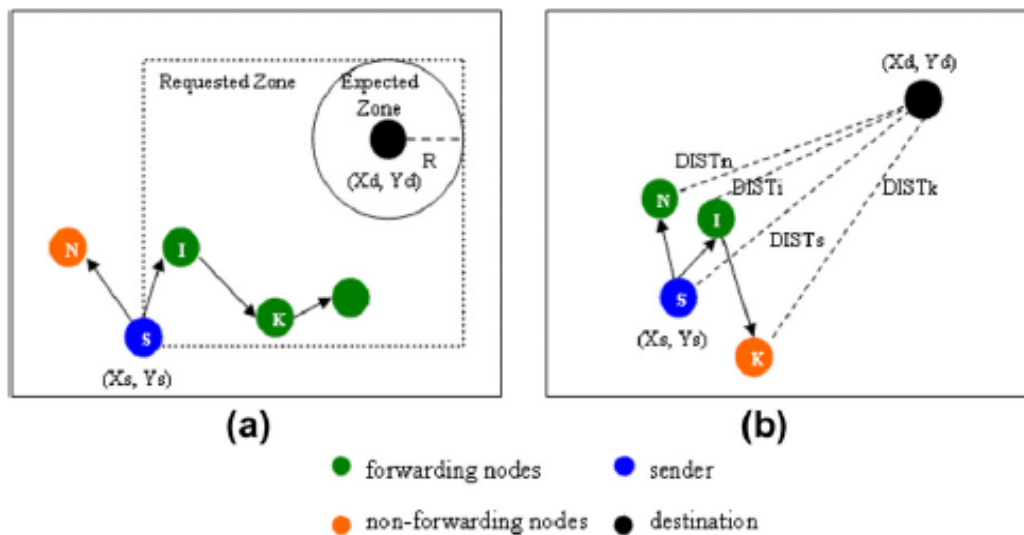


Figure 2-16: (a) LAR Scheme1 and (b) LAR Scheme2 (Alotaibi & Mukherjee, 2012)

As a limitation, the LAR techniques has a large request zone, and it floods packet over the large area which leads to wastage of network resources. For example, any node (such as node N) outside the rectangle in Figure 2-16(a) will not forward the received route request packet that initiated from node S (Alotaibi & Mukherjee, 2012) and as such, the route request message will be discarded.

2.4.2 Summary of MANET Routing Classification

The MANET routing classification is summarised in Table 2-1 highlighting their differences in terms of routing structure, control traffic, route discovery procedure, bandwidth requirement, power consumption as well as advantages and disadvantages of each routing class. This summary will help researchers to select a suitable routing protocol that meets their requirement.

As discussed in the following sub-section, this research is interested in disaster network with low latency that can organised routes before they are needed, utilise Battery life of nodes to prioritise message delivery and make Battery life of the devices available to rescue teams for strategic rescue operations.

Table 2-1: Summary of MANET Routing Classification

Features	Proactive (Table Driven)	Reactive (On-Demand)	Hybrid	Hierarchical	Geographical
Routing Structure	Flat Routing	Flat Routing (except CBRP)	Flat Routing	Hierarchical	Greedy Forwarding Routing
Control Traffic	High	Low	Lower than Proactive and Reactive	Medium	Medium
Route Discovery	Periodically	On-Demand	Partially	Partially	Partially (Depends on nodes location)
Route Availability	Always Available	Available On-Demand	Available (Within Zones)	Partially	Based on Nodes Location
Latency	Low (Established routes in advance)	High (Established routes when needed)	Intra-Zones: Low. Inter-Zones: High	Depend on Nodes location	Depends on Nodes location
Bandwidth Usage	High	Low	Moderate	Low	High
Energy Consumption	High	Low	Moderate	Moderate	Low
Scalability	Efficient for up to 100 nodes	Efficient for up to few hundred nodes	Designed for large network (up to 1000 nodes)	Designed for large network (1000 nodes and more)	Designed for large network (1000 nodes and more)
Storage Requirement	High (Due to use of routing Table)	Low (Depend on the number of routes required)	Moderate (High for intra-zone and inter-zone)	Moderate	Moderate
Weaknesses	-Overhead maintenance traffic -Storage requirements increase with the increase of network size - Nodes keep the entities of their routing table even during ideal time	-Suffers high message latency in expense of initial route discovery procedure - Routes is not always up to date	-Suffers complexity in operation -High message latency for inter-zone -Routing overhead for intra-zone	-Proper selection of Cluster Head -Routing technique consumed power in large cluster network	-Every node must know its location -

Strengths	-Low Latency -Routes are always available	-Less routing overhead -Efficient recourses utilisation -Suitable for large network	-Reduces route setup latency for nearby nodes - low routing overhead for far away destinations	-Topology changes affect only the cluster in question -Low routing overhead - Quick route setup time -Suitable for large networks	-Nodes do not necessarily need to have full knowledge of network topology but its own location and the location of destination node.
------------------	--	---	---	---	--

2.5 Reason for Choosing Proactive over Reactive Protocols

Enumerated below are the motivations for choosing proactive as the protocol to modify:

1. **Route Availability:** The ability to organize routes before they are needed is important during search and rescue operations, this feature permit a victim to view reachable neighbours or RT member from the list of nodes known to the routing and organise frequent “reachable” contacts in a contact list. Route availability closely mimics the way we work as humans, that is knowing whom to call.
2. **Device Battery life:** The BATTERY_LEVEL along with the device Network_Assignment enable Rescue Team (RT) to plan service offloading when rescuing victims whose phones act as MPR. Battery life is equally used to prioritize message delivery for low battery energy nodes, over those with higher Battery lifes.
3. **Latency:** Proactive provides rapid connectivity between nodes, thus, a sender can quickly commence sending data to an intended recipient simply because the route has been calculated in advance. High latency during disaster recovery communication will frustrate victims and RT members, thus it is better to adopt a protocol with a low latency.

2.5.1 Why OLSR over other proactive routing protocols

Optimised Link State Routing Protocol (OLSR) is a well-known and widely used MANET and D2D Multi-hop proactive routing protocol that is not only implemented on many simulation tools but also on actual portable mobile devices. While other proactive routing schemes have resolved particular issues of routing in MANET, the implementation of such protocols is

largely theoretical and not yet implemented on real life mobile devices. For example, the requirement of directional antennas and free-space optical (FSO) hardware for mobile devices (phones, laptops, and tablets) in proactive Mobile Orthogonal Rendezvous Routing Protocol (MORRP) limited its real-life implementation. In addition, proactive Fisheye State Routing Protocol (FSR) was never released to the public as a stand-alone routing protocol, and its specification was never finalized. In fact, its base principle was included in the widely popular OLSRd daemon, which is an open source implementation of the OLSR routing protocol (Shenbagapriya & Kumar, 2014).

For adaptability purpose, the proposed modification of this research uses nodes battery life, Time Slices, and cross-layer metrics to reduce message collision, improve link quality and increase the overall performance of disaster recovery operations have been easily integrated with OLSR. Therefore, this research focuses on optimisation of OLSR as the routing protocol in MANET for energy friendly disaster communication network.

To meet the stated requirements in Section 2.5, the researcher analysed the available MANET routing protocols as indicated in Table 2-1 and concluded that a proactive OLSR routing protocol is the best routing protocol for this research.

2.5.2 OLSR Version Adopted for Modification

The reason for selecting OLSRv1 over OLSRv2 is borne out of the need to reduce the number of MPR devices required by each node, whose battery energy may likely drain faster due to routing control overhead. OLSRv2 expects each node to select two MPRs, thus control traffics are routed through the first MPR, while normal data are routed through the second MPR. This approach is designed to conserve the battery of MPR devices; however, the approach did not prevent overhearing along with the associated overhead. Thus, OLSRv2 did not address the problem of overhearing, which will cause both MPRs to eventually run out of battery energy. In addition, since OLSRv2 is an improvement of OLSRv1, this research decides to focus on improving OLSRv1, with the belief that the improvement could excel OLSRv2 in energy conservation. Moreover, the proposed routing scheme (DS-OLSR) can easily be ported to OLSRv2 since the algorithm operates mostly at reducing network overhead caused by overhearing.

Interestingly, vast number of OLSRv1 projects exists, such as US Naval Research Solution (Research, 2019) and Github projects (Tonnesen Andreas, Lopatic Thomas, & Kaplan Aaron, 2017b) as in Figure 2-17. This implies a higher number of developers have contributed more codes to OLSRv1 than OLSRv2 as shown in Figures 2.17 and 2.18. This development created several usable and “stable” versions of OLSRv1 software, especially for Linux/Android operating system for smartphones. Robust simulation module in NS-3 (nnsam, 2019).

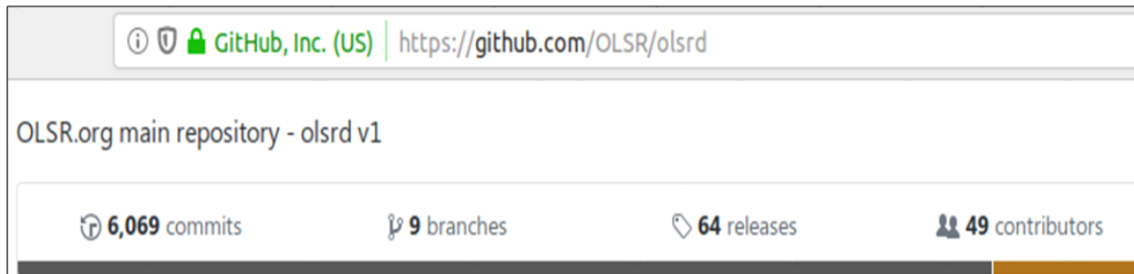


Figure 2-17: OLSRv1 source code repository showing number of commits, branches, releases and contributors (Andreas et al., 2017b)

Although OLSRv1 has a wider and varied codebase, nonetheless, the number of papers on OLSRv2 far outweighs those written on OLSRv1 by a ratio of 976 to 123 or 1 to 0.1 as in Figure 2.17 and Figure 2.18. Unfortunately, the extensive papers on OLSRv2 did not translate to wider and varied code implementation (see Figures 2.19 and 2.20).

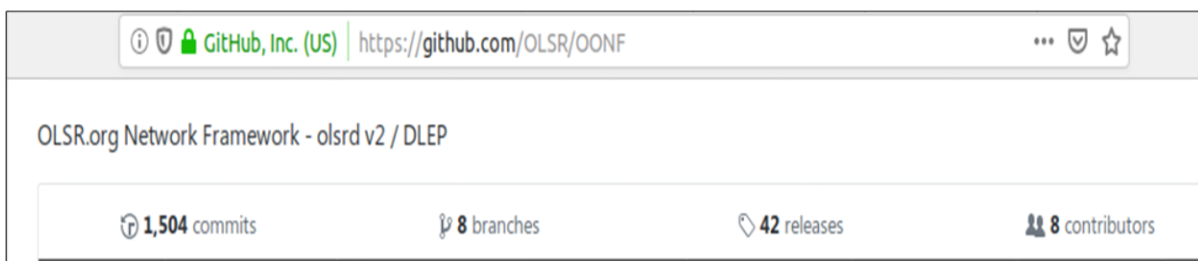


Figure 2-18: OLSRv2 source code repository showing number of commits, branches, releases and contributors (Tonnesen Andreas, Lopatic Thomas, & Kaplan Aaron, 2017a) .

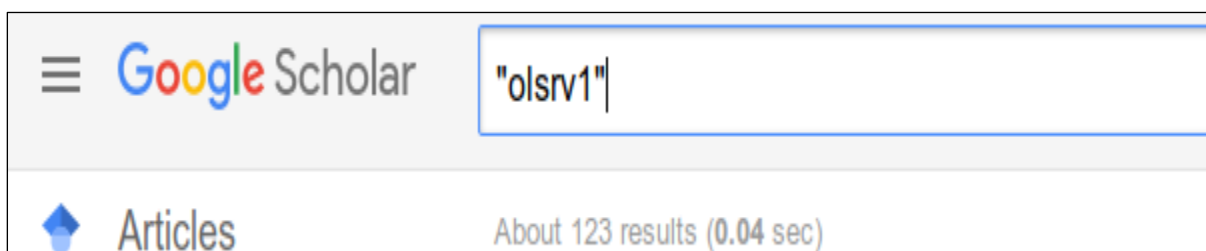


Figure 2-19: Searching for olsrv1 returned 123 results. (Retrieved August 13, 2019)

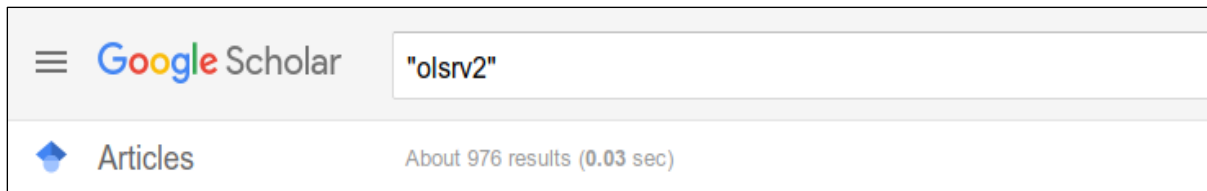


Figure 2-20: Searching for olsrv2 returned 976 results. (Retrieved August 13, 2019)

2.5.3 Features and Functionalities of OLSR)

As discussed in Section 2.3.1.1.1.1 of MANET routing protocol, Optimized Link State Routing (OLSR) protocol is a form of proactive routing protocol based on link state and developed for mobile ad hoc networks (MANETs) (Clausen & Jacquet, 2003). It is an optimization of link state routing (LSR) adapted to the requirements of MANET that maintain route in advance to all other nodes in a network and make them available upon needed. Each node has one or more tables that contain the latest information of the routes to any node in the network.

Two major challenges facing OLSR are the concept of overworked MPRs (these MPRs often route a lot of network traffic on behalf of other nodes which causes a severe drain to stored battery energy, and eventual shutdown), and network overhead (caused by excessive propagation of control messages, which are responsible for link sensing and reporting). In OLSR, nodes are constantly busy routing control messages in the background (regardless of user messages) thus, constitutes a drain on bandwidth and battery (McCabe et al., 2005), and sometimes results to temporary loss of routes. Clausen (2004) identified the cause of these errors in OLSR protocol as message collision. Message collision occurs when messages become synchronize or coordinated, for example, a node may wish to report a change in its set of MPR via HELLO message, which may trigger a network control message (TC message) in a set of neighbouring nodes that are already broadcasting Hello message. This would lead to collision since the receiving node is already busy with the HELLO message (Clausen, 2004). As a result, this research is interested in modifying the OLSR packet format and messages to achieves tremendous energy savings along with drastic reduction in overheads for effective network for disaster recovery and rescue operation.

2.5.3.1 OLSR Packet Format and Forwarding

OLSR communicates using a unified packet format for all data related to the protocol (Clausen & Jacquet, 2003). The purpose of this is to facilitate extensibility of the protocol without

breaking backwards compatibility. This also provides an easy way of piggybacking different "types" of information into a single transmission, and thus for a given implementation to optimize towards utilizing the maximal frame-size, provided by the network. These packets are embedded in UDP datagrams for transmission over the network. Each packet encapsulates one or more messages. The messages share a common header format, which enables nodes to correctly accept and (if applicable) retransmit messages of an unknown type.

Messages can be flooded onto the entire network, or flooding can be limited to nodes within a diameter (in terms of number of hops) from the originator of the message. Thus, transmitting a message to the neighbourhood of a node is just a special case of flooding. When flooding any control message, duplicate retransmissions will be eliminated locally (i.e., each node maintains a duplicate set to prevent transmitting the same OLSR control message twice). Furthermore, a node can examine the header of a message to obtain information on the distance (in terms of number of hops) to the originator of the message. This feature may be useful in situations where, e.g., the time information from a received control messages stored in a node depends on the distance to the originator. Table 2-2 displays the basic layout of any Packet in OLSR.

Table 2-2: Packet format for OLSR (Clausen & Jacquet, 2003)

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Packet Length										Packet Sequence Number																					
Message Type					Vtime					Message Size																					
Originator Address																															
Time to Live					Hop Count					Message Sequence Number																					
MESSAGE																															
Message Type					Vtime					Message Size																					
Originator Address																															
Time to Live					Hop Count					Message Sequence Number																					
MESSAGE																															

Packet Header: Packet length and Packet sequence number are the two Packet headers in OLSR (Clausen & Jacquet, 2003).

Packet Length: The length (in bytes) of each packet is stored in this field.

Packet Sequence Number: The Packet Sequence Number (PSN) is incremented by one each time a new DS-OLSR/OLSR packet is transmitted. PSN enable nodes to identify newer packets and reject expired packets with lower PSN.

Message Headers: As shown in Table 3-1, OLSR has seven (7) message headers namely: Message Type, VTime, Message Size, Originator Address, Time to Live, Hop Count and Message Sequence Number. The following sub-sections briefly discussed the OLSR Message headers.

Message Type: This field indicates which type of message is stored in the packet's "MESSAGE" segment. In OLSR message types are in the range of 0-127. The popular messages for OLSR are HELLO, Topology Control (TC), Multiple Interface Devices (MID) and Host Network Association (HNA).

Vtime (Validity Time): In OLSR, this field indicates the validity period of a message, which is how long a message is to be considered valid unless a more recent update to the information is received. Validity period countdown commences from the moment a node receives a message.

Message Size: This field contains the size of the message stored within MESSAGE segment. It is counted in bytes and measured from the beginning of the "Message Type" field to the beginning of the next "Message Type" field, or in the absence of more messages, to the end of the packet.

Originator Address: The originator address of a node is the interface IP address selected by the node as its Main IP Address. For example, nodes with multiple interfaces must select the IP address of any of the interfaces as its Main IP Address. The selected originator address is immutable. This field SHOULD NOT be confused with the source address from the IP header, which is changed each time to the address of the intermediate interface which is re-transmitting this message. The Originator Address field MUST *NEVER* be changed in retransmissions.

Time To Live: This field contains the maximum number of hops a message will be transmitted. Devices can limit the scope of a broadcast by setting this field to a value that is greater than 1. Thus, a value of 5 implies the broadcast will not be retransmitted after the fifth device receives the message. Each device is expected to decrement the Time to Live value by 1 before retransmitting. A value of 1 implies the message will not be retransmitted.

Hop Count: Hop Count determines the number of hops a message passes from the moment it was sent. This value is set to 0 by the message originator and incremented by 1 before retransmission by recipients.

Message Sequence Number: While generating a message, the "originator" node will assign a unique identification number to each message. This number is inserted into the Sequence Number field of the message. The sequence number is increased by 1 (one) for each message originating from the node. Message sequence numbers are used to ensure that a given message is not retransmitted more than once by any node.

2.5.3.2 OLSR Packet Processing and Forwarding

It should be noted that processing and forwarding messages are two different actions conditioned by different rules. Processing relates to using the content of the messages, while forwarding is related to retransmitting the same message for other nodes of the network (Clausen & Jacquet, 2003).

2.5.3.2.1 OLSR packet processing

Upon receiving a basic packet, a node examines each of the "message headers" and based on the value of the "Message Type" field, the node can determine the fate of the message (Clausen & Jacquet, 2003). A node may receive the same message several times. Thus, to avoid re-processing of some messages which were already received and processed, each node maintains a Duplicate Set. In this set, the node records information about the most recently received messages where duplicate processing of a message is to be avoided. For such a message, a node records a "Duplicate Tuple" (D_addr, D_seq_num, D_retransmitted, D_iface_list, D_time), where D_addr is the originator address of the message, D_seq_num is the message sequence number of the message, D_retransmitted is a boolean indicating whether the message has been already retransmitted, D_iface_list is a list of the addresses of the interfaces on which the message has been received and D_time specifies the time at which a tuple expires and MUST be removed.

2.5.3.2.2 OLSR Packet Forwarding

The value contained in each message header (as extracted from a packet) determines the fate of a message along with the level of interaction with the message originator and or sender (sender refers to the node that forwarded the message on behalf the originator).

Clausen and Jacquet (2003) identified the following default forwarding algorithms:

1. *If the sender interface address of the message is not detected to be in the symmetric 1-hop neighbourhood of the node, the forwarding algorithm MUST silently stop here (and the message MUST NOT be forwarded).*
2. *If there exists a tuple in the duplicate set where:*
 $D_addr == \text{Originator Address}$
 $D_seq_num == \text{Message Sequence Number}$

Then the message will be further considered for forwarding if and only if:

$D_retransmitted$ is false, AND the (address of the) interface which received the message is not included among the addresses in D_iface_list

3. *Otherwise, if such an entry does not exist, the message is further considered for forwarding.*

If after those steps, the message is not considered for forwarding, then the processing of this section stops (i.e., steps 4 to 8 are ignored), otherwise, if it is still considered for forwarding then the following algorithm is used:

4. *If the sender interface address is an interface address of a MPR selector of this node and if the time to live of the message is greater than 'T', the message MUST be retransmitted (as described later in steps 6 to 8).*
5. *If an entry in the duplicate set exists, with same Originator Address, and same Message Sequence Number, the entry is updated as follows:*

$D_time = \text{current time} + \text{DUP_HOLD_TIME}.$

The receiving interface (address) is added to D_iface_list .

$D_retransmitted$ is set to true if and only if the message will be retransmitted according to step 4.

Otherwise, an entry in the duplicate set is recorded with:

D_addr = Originator Address

D_seq_num = Message Sequence Number

D_time = current time + DUP_HOLD_TIME.

D_iface_list contains the receiving interface address.

D_retransmitted is set to true if and only if the message will be retransmitted according to step 4.

If, and only if, according to step 4, the message must be retransmitted then:

- 6. The TTL of the message is reduced by one.*
- 7. The hop-count of the message is increased by one*
- 8. The message is broadcast on all interfaces (Notice: The remaining fields of the message header SHOULD be left unmodified.)*

2.5.3.3 OLSR Messages

Hello, Topology Control (TC), Host Network Association (HNA), Multi-Interface Declaration (MID) messages (Clausen & Jacquet, 2003), are required messages type for OLSR core functionality.

Every OLSR device sends HELLO messages as soon as the network comes into existence. HELLO messages enable devices to know and advertise the link state of neighbouring devices. Devices that are beyond the broadcast range of a sending device are reachable via multiple hops. However, this is only possible if both devices have information regarding each other (namely their interface main addresses). Multi Point Relays (MPRs) are responsible for advertising such link state information across the OLSR network. MPRs advertises link state of nodes via a Topology Control (TC) message. MPRs are selected from amongst a node's 1-hop neighbours, the chosen MPR must have a 1-hop relationship to a selector's 2-hops neighbours.

Nodes or devices that possess two or more OLSR connected communication interfaces (such as two wireless interfaces) MUST advertise both interfaces via a Multiple Interface Device

message (MID). Each MID message MUST include the main address designated by the multi-interfaced device as the preferred medium of communicating with other nodes in the network. MID messages enable recipients identify the designated main address to use when communicating with a multi-interfaced device.

Table 2-3: OLSR Hello Message Format (Clausen & Jacquet, 2003)

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Reserved										Htime										Willingness											
Link Code					Reserved					Link Message Size																					
Neighbour Interface Address																															
Neighbour Interface Address																															
: : : :																															

Table 2-4: OLSR TC Message Format (Clausen & Jacquet, 2003)

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ANSN										Reserved																					
Advertised Neighbour Main Address																															
Advertised Neighbour Main Address																															
: : : :																															

Table 2-5: OLSR HNA Format (Clausen & Jacquet, 2003)

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Network Address																															
Network Mask																															
Network Address																															
Network Mask																															
...																															

Table 2-6: OLSR MID Format (Clausen & Jacquet, 2003)

0										1										2										3			
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1		
OLSR Interface Address																																	
OLSR Interface Address																																	
: : : :																																	

Finally, a device that possess two communication interfaces, in which only one interface is connected to the OLSR network MUST send a Host Network Association message (HNA). HNA messages are often sent by devices or nodes that act as a gateway to a non-OLSR network (such as the Internet). Non-OLSR interface are excluded from receiving OLSR specific messages (such as HELLO, TC, and MID), however, information provided by HNA messages allow devices within the OLSR network to communicate with devices that are outside the OLSR network. The format of the OLSR core functionality messages is shown in Table 2-3 through Table 2-6.

2.5.3.4 OLSR Repositories/Tables/Sets

OLSR nodes accumulates information about the network through the exchange of the OLSR core functionality messages such as Hello, TC, HNA and MID messages (Clausen & Jacquet, 2003). These messages are stored according to the following:

1. **Link Set:** A link set is maintained by each node as a record ("Link Tuples" in OLSR parlance) of responses to its Hello messages. The following fields are recommended by OLSR: L_local_iface_addr, L_neighbor_iface_addr, L_SYM_time, L_ASYM_time, and L_time. L_local_iface_addr is the address of the record keeping node, L_neighbor_iface_addr is the address of the neighbor node with whom the sender shares a link, L_SYM_time is the time that determines if a link to a neighbor is still symmetric, L_ASYM_time is the time that determines if a link to a neighbor is still asymmetric, finally L_time is the time that determines a record has expired and MUST be removed.
2. **Neighbour Set:** A node records a set of "neighbor tuples" (N_neighbor_main_addr, N_status, N_willingness), describing neighbors. N_neighbor_main_addr is the main address of a neighbor, N_status specifies if the node is NOT_SYM or SYM.

N_willingness in an integer between 0 and 7 and specifies the node's willingness to carry traffic on behalf of other nodes.

3. **2-hop Neighbour Set:** A node records a set of "2-hop tuples" (N_neighbor_main_addr, N_2hop_addr, N_time), describing symmetric (and, since MPR links by definition are also symmetric, thereby also MPR) links between its neighbors and the symmetric 2-hop neighborhood. N_neighbor_main_addr is the main address of a neighbour, N_2hop_addr is the main address of a 2-hop neighbor with a symmetric link to N_neighbor_main_addr, and N_time specifies the time at which the tuple expires and *MUST* be removed. In a node, the set of 2-hop tuples are denoted the "2-hop Neighbour Set".
4. **MPR Set:** A node maintains a set of neighbours which are selected as MPR. Their main addresses are listed in the MPR Set.
5. **MPR Selector Set:** A node records a set of MPR-selector tuples (MS_main_addr, MS_time), describing the neighbours which have selected this node as a MPR. MS_main_addr is the main address of a node, which has selected this node as MPR. MS_time specifies the time at which the tuple expires and *MUST* be removed. In a node, the set of MPR-selector tuples are denoted the "MPR Selector Set".
6. **Topology Set:** Nodes in OLSR are familiar with the MANET topology by maintaining a topology set. Data for populating the set are gathered from TC messages. Topology set records "Topology Tuple" for each destination in the network using the following fields: T_dest_addr, T_last_addr, T_seq, and T_time . T_dest_addr is the interface address of a node that can be reached via 1-hop from the node (MPR) whose interface address is stored in T_last_addr, T_seq is a sequence number generated with sending the message, this is different from the message sequence number. Finally, T_time determines when the record expires and MUST be deleted.
7. **Duplicate Set:** This table is responsible for storing information that prevents retransmission of a transmitted message. OLSRv1 specify the following fields for a "Duplicate Tuple": D_addr, D_seq_num, D_retransmitted, D_iface_list, and D_time. D_addr stores the originator address of the message originator, D_seq_num contains the message sequence number, D_retransmitted indicates if the message has been retransmitted, values are stored in Boolean, thus 0 for false and 1 for true, D_face

represents a list of interface addresses on which the message has been received, and finally, D_time determines the removal time of a tuple that has expired.

- 8. Multiple Interface Association Set:** For each destination in the network, "Interface Association Tuples" ($I_iface_addr, I_main_addr, I_time$) are recorded. I_iface_addr is an interface address of a node, I_main_addr is the main address of this node. I_time specifies the time at which this tuple expires and ***MUST*** be removed.

2.5.3.5 MPR Selection Process

Each device/node selects an MPR from their 1-hop neighbours, a node wishing to select an MPR examines the number of 1-hop neighbours that reports links to 2-hops neighbours of the node. Thus, MPRs are selected based on their advertised links along with Willingness to act as an MPR (Clausen & Jacquet, 2003). A node with a willingness level of WLL_NEVER – will NOT be selected as an MPR even if it advertises links, the energy level of a device often affects its willingness to act as an MPR. In the same vein, a device that fails to report any link will NOT be considered as an MPR candidate. For example, in Figure 2-21, node D selects nodes E and G as MPRs because they report the most links to D's 2-hop neighbours. Node A is not chosen as an MPR because the only reachable node of Node A is Node B, which is also reachable by Node E.

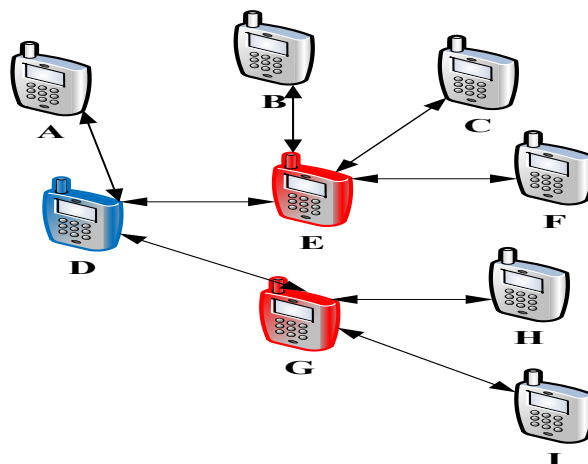


Figure 2-21: MPR selection process (blue phone selected red phones as MPRs)

As mentioned earlier, this research is interested in message prioritisation scheme to further improves energy conservation, extend lifespan of low battery nodes, and improves mental state

of victims with such devices in the aftermath of a disaster. Therefore, related research on message prioritisation is presented in the following Section.

2.6 Message Prioritisation Related Work

The related work discussed in this Section covers the key areas of this research work, namely: message prioritization and energy conservation in MANETs. However, most research on message prioritization do not focus on the major challenge (energy) of networks during disaster recovery and rescue operations as they mainly focused on message prioritization based on message type, size, and context information. Nonetheless, some disasters go beyond destroying telecommunication infrastructure as they equally cripple/impair power grids and leaves locals with neither network nor power.

Aggarwal and Nagrath (2013) propose optimizing Delay Tolerant Network (DTN) via message prioritization. Their paper proposes using a device buffer and routing time-to-live (TTL) value as parameters to store and forward messages using three message levels: high priority, medium priority, and low priority. Messages are assigned unique IDs along with a unique priority in the following order (M3, 1) or (M1, 2), or (M2, 3). Where M3 is the message ID and 1 is the message priority. Thus, message M3 has a priority level of *high*, M1 *medium* and M2 has a priority level of *low*. The researchers equally adopted TTL as a second parameter that determines message prioritization. Thus, a high priority message such as (M2, 1) can become low priority if the TTL is 2, that is (M2,1) (2). This implies the message will be relegated to second place in favour of a medium/low priority message with a higher TTL value, for example (M1,2) (10). The authors proposed using an initial TTL value of 10, which is decreased by 2 during each update cycle. However, the paper has not considered residual battery energy of nodes for priority decision nor optimize the energy consumption of their network as they limited to prioritization of messages based on buffer size and TTL value.

Lieser, Richerzhagen, Luser, Richerzhagen, and Steinmetz (2019) studies the impact of message prioritization in ad-hoc network disaster communication system. Undesirable interactions between message prioritization in Delay Tolerant Network (DTN) and dynamic disaster scenarios were identified based on their previous field trial. Furthermore, the authors develop a message prioritization algorithm that integrates 3 prioritization schemes, namely: Static, Adaptive and None, to accommodate changes in message importance and frequency over time. A generic architecture has been equally proposed to evaluate prioritized DTNs using

different disaster scenarios and attributes, such as message sizes and type were assumed to be pre-assigned via mobile apps running on mobile devices. Their simulation results showed that emergency messages with high priority are favoured over low priority messages.

Content based filtering and prioritization of emergency messages in the aftermath of a disaster is proposed by Bhattacharjee, Basu, Roy, and Bit (2016). To achieved segregation and prioritization of messages according to their importance, natural language processing (NLP) based filtering has been used for filtering and prioritization. Filtered messages were disseminated using priority enhanced-PRoPHET routing protocol over Delay-Tolerant Network (DTN). The authors used real WhatsApp messages exchanged between rescue team members during Nepal earthquake disaster recovery and rescue operation in 2015, to classified messages based on content into five different priorities: Sentimental, Conversation, Situational, Resource Allocation and Resource Requirement. Resources Requirement and Situational messages has been allocated as priorities 5 (highest) and 4 (next highest) respectively. This is because most of the messages in both priorities are assumed to represents extremely need of resources for survival and decision-making information. ONE simulator was used to implement and evaluate the performance of their proposed techniques and the results suggested that their protocol performed better than famous DTN routing protocols such as PRoPHET, MaxProp, Epidemic and Spay-And-wait in terms of delivery of prioritized messages and routing overhead. However, the authors do not consider device battery energy level for priority computation.

Waheb A Jabbar, Ismail, and Nordin (2014) proposed Multipath Battery-Aware routing protocol called MBA-OLSR, an enhanced energy efficient version of Multi-path OLSR (MP-OLSR) without loss of performance. MP-OLSR was proposed to address routing issues such as scalability, transmission instability and security whereas MBA-OLSR to optimize energy consumption and quality of service (QoS). MBA-OLSR uses residual battery of devices as metrics for finding initial cost of multiple routes. The inclusion of the device battery was achieved by modification of HELLO and TC messages to add Type Length Value (TLV) mechanism for network aware battery information. EXata 3.1 Simulation was used to evaluate the performance of the MBA-OLSR as compared to MP-OLSR. The modification to attach energy information of nodes as metric for link cost computation enhanced energy efficiency without sacrificing QoS and it performed better than MP-OLSR in terms of end-to-end delay and packet delivery ratio. The authors developed multipath scheme and efficient energy aware

routing protocol by considering devices battery energy as a metric for route selection. However, they did not prioritize message delivery based on residual battery energy nor extend the lifespan of devices with low battery energy.

Waheb A. Jabbar, Saad, and Ismail (2018) presented a hybrid multi-path and multi-criteria energy and QoS aware OLSR protocol called MEQSA-OLSRv2, to handle limited energy resources, traffic congestion and mobility of nodes in mobile ad-hoc network (MANET) and wireless sensor networks (WSN) convergence scenarios of Internet of Things (IoT) networks. MEQSA-OLSRv2 techniques combined multiple criteria including residual battery, node's lifetime, node's idle time, queue length and node's speed into single metric for MPR selection and routing decision. Unlike existing techniques, MEQSA-OLSRv2 ranked nodes based on multi-criteria node rank metric (MCNR) that aggregated energy and QoS related parameters into an extensive metric to reduce multiple constrain complication and avoid routing overhead generated by broadcasting multiple parameters. However, the authors retained main characteristics of MP-OLSRv2 and MBQA-OLSR such as residual energy and hybrid multi-path routing. The MEQSA-OLSRv2 has been implemented in EXata simulator and the simulation results showed that it can significantly reduce energy and improve QoS in common MANET and WSN scenarios. in MEQSA-OLSRv2, energy consumption during packet routing has been considered and load balancing is equally achieved via multiple paths. However, message prioritization based on device' Battery life was not considered, and complexity of multiple metrics will result to increase in routing overhead and therefore not suitable for dense network.

Several related works have been proposed to optimize OLSR for energy efficiency. Similarly, different route and messages prioritization schemes were equally proposed. However, most of them mainly focused on prioritization based on message type, size, and context information, and to ensure effective communication during disaster recovery and rescue operations, priority techniques that can extend lifespan of low battery devices and prioritize their communication plays a significant role.

2.7 Chapter Summary

This Chapter presented overview of MANETs highlighting the history of MANETs, characteristic, applications and challenges which gives the basic understanding on how MANETs came into play, it features and areas of strength and weakness. In MANET, mobile devices do not depend on

established infrastructure or base station. Therefore, each device operates as both host that can send and receive data, services or application, and a router that can route information on behalf of other nodes with the use of routing protocols. Thus, intensive review of MANETs routing protocols have been presented. This gives the opportunity to identify suitable routing protocol for this research. The routing protocol under optimisation (OLSR) has been thoroughly discussed emphasising on operational aspect, the version of OLSR adapted for modification and reason for considering proactive OLSR than reactive routing protocols. Finally, related work on message prioritisation were equally presented as this research is interested in prioritising message based on devices Battery life to extend the lifespan of low battery nodes and avoid overall network partition. The next Chapter presents background research on disasters and review of networks for disaster recovery and rescue operations.

Chapter 3

Literature Review of Networks for Disaster Recovery and Rescue Operations

3.1 Introduction

Energy efficient communication networks has become a necessity for every society, especially in areas with commonly occurring natural and artificial (human-made) disasters. However, most research focuses on design and implementation of network for emergency response and disaster recovery operations based on restoration of telecommunication infrastructure using expensive and non-flexible technologies, such as complete network infrastructure in box or on car. This Chapter presents review of different networks for disaster recovery and rescue operations, starting with type of disasters and how successful disaster operation depends largely on effective and reliable disaster communication system in Section 3.1. Secondly, the review of disaster recovery networks based on pre, and post disaster communication systems is presented in Section 3.2. Finally, Section 3.3 concludes this Chapter with review of the process of switching mobile devices to disaster mode for effective and efficient disaster communication.

3.2 Disaster Recovery Networks

Network for disaster recovery and rescue operation is a network that can be configured easily with few steps using wireless devices such as smart phones, laptops, tablets and effectively supports urgent communication needs for disaster recovery operations (Minh & Yamada, 2015). Conventionally, Walkie-Talkie or two-way terrestrial technologies has been used for rescue and recovery operations due to their strong voice communication (W. Lu, Seah, Peh, & Ge, 2007). Y. N. Lien, C. Li-Cheng, et al. (2009) argued that Walkie-Talkie is one of the most suitable, portable, and effective system for emergency communication. Walkie-Talkies makes used of Push-To-Talk (PTT) service that allows the broadcast of voice message in form of small bursts to all receivers on the communication channel (W. Lu et al., 2007). However, Walkie-Talkie is an old communication technology and has several limitations that make it ineffective system for disaster recovery operations. For example, Y. N. Lien, Hung-Chin, and Tzu-Chieh (2009) stated that, Walkie-Talkie may not be available to rescue volunteer workers in the early hours of disaster recovery and rescue operations, and this volunteer workers feeds

the trained professional rescue teams with the first-hand information required for the rescue operations. Furthermore, the technology supports only analog voice, and as such it is very difficult for the system to adapt delivery of multimedia data in a critical emergency condition (W. Lu et al., 2007). Moreover, there is no privacy in communication as broadcasted voice is received by everyone on the channel, and retransmission of conversation is requested manually due to its analog system (Y. N. Lien, C. Li-Cheng, et al., 2009). Another form of early communication system that may serve as an emergency network recovery is Ham Radio, which is used for internet backup service when the existing internet is down (Y. N. Lien, J. Hung-Chin, et al., 2009). However, the popularity of Ham Radio technology in many countries is less than Walkie-Talkie. For instance, in Taiwan, the availability of the technology is limited to only handful of Ham Radio stations because of its long-time of stringent regulation (Y. N. Lien, C. Li-Cheng, et al., 2009). Therefore, the need for effective network for disaster recovery and rescue operation that can support the communication needs to save and rescue lives and properties in disaster areas is highly recommended.

Network for emergency communications can either be pre-disaster network (prior to occurrence of disaster) which comprises of preparedness and mitigations that provides warning and measures to minimise or prevent a disaster, and post-disaster network (aftermath a disaster) which comprises response and recovery action during and after catastrophic condition (Raffelsberger & Hellwagner, 2013). The two forms of network for the emergency communication are discussed in the Subsections below.

3.2.1 Pre-disaster Communication System

As stated earlier, pre-disaster communication system is a form of disaster communication system that performs the function of catastrophic warning/signal, advisory and cautionary actions that helps in disaster preparedness and mitigation. Over the years, many researchers have examined and developed several pre-disaster communication solutions for emergency signal/warning prior to occurrence of disasters. For example, Remote sensors, Radio-Acoustic sound system, lightning sensors, and seismic sensor (Van Westen, 2000) are pre-disaster solutions that sends warning/signal regarding the occurrence of disaster. The advancement in communication technology provides mobile device users with embedded fire detecting capabilities and relevant sensors to send catastrophic warning via terrestrial or satellite communication system (Anjum, Noor, & Anisi, 2017). This research considered some aspect

of pre-disaster communication system. However, its limited to the use of Wireless Emergency Alert (WEA) via Short Message Service Cell Broadcast (SMSCB) to launch DS-OLSR through an embedded link as discussed in Section 3.4. The review of post disaster communication systems is presented in the following Subsection.

3.2.2 Post-Disaster Communication System

A post-disaster communication system is a form of disaster communication system that can be configured easily with few steps and effectively supports urgent communication needs for disaster recovery operations (Minh & Yamada, 2015). During or in the aftermath of a disaster, the conventional communication system may be disrupted or completely damaged. As a result, a rapidly deployable emergency networks are required to restored connectivity and allow communication needs for effective disaster recovery operation. However, deployable networks by rescue team cannot covered the entire disaster areas and as such, infrastructure less communication system (such as MANET) that can be configured easily with few steps and effectively supports urgent communication needs for disaster recovery operations are imperative and is the area of interest of this research.

Since early 1990s, networks for emergency response and disaster recovery operations were put into consideration (Morrison, 2011). For example, In early 1991s, AT&T Mobility: A Telecommunication company that provides wireless services to over 155.7 million subscribers in the US, formed a program called AT&T Network Disaster Response (NDR) to support communication if disaster destroys the city's Telecommunications office (Morrison, 2011). The AT&T's Network Disaster Recovery (NDR) solution combines telecommunication infrastructure on trailers, recovery software applications, and professional rescue team members from the AT&T. Each machinery vehicle contains a complete telecommunication system as it is in the AT&T office, while the engineering software applications allowed the deployed components to take the services of the disastrous buildings. The professional rescue teams create and establish connections, manages, and control the recovery system.

The Network for disaster recovery provides AT&T Mobility with a reliable and predictable way of responding to catastrophic loss of communication infrastructure with the help of inventory network technology trailers, recovery software applications, as well as well-trained professionals' teams as a telecommunication disaster responder (Morrison, 2011). Therefore, it is recommended for service providers in developing countries like Nigeria and places with

commonly occurring disasters to have such network recovery system for emergency response and disaster recovery operations.

Although, AT&T Mobility did not take into consideration that the disaster network can only be helpful to rescue teams and disaster victims when their mobile phone has power as some disasters go beyond crippling/impairing communication infrastructures, for example, some disaster scenarios equally cripple power grids, which make it impossible for survivors to recharge mobile communication devices.

Similarly, after the event of September 11 attacks, the Network for disaster recovery and rescue operations has gained much research attention. However, most of the early research focus on design and implementation of network for emergency response and disaster recovery operations based on restoration of telecommunication infrastructure using expensive and non-flexible technologies. In addition, some of the networks proposed are only available to rescue team members but not available to disaster victims and volunteer workers in the early hours of disaster recovery and rescue operations, and of course this volunteer workers feeds the trained professional rescue teams with the first-hand information required for successful rescue operations.

Over the years, deployment of movable WLAN access points on emergency vehicles (Ohyama, Kaneko, Asano, & Hamaguchi, 2012), cellular base stations in-box (Nokia, 2015) and on-wheel (David, 2015) satellite system (Calarco, Casoni, Paganelli, Vassiliadis, & Wódczak, 2010), MANET (Raj, Kant†, & Das, 2014) and so on, are commonly used for emergency response and disaster recovery operations. Thus, this research considered related work on the different wireless technologies without restriction to enables the understanding of historical background and how each technology supports communication needs for disaster recovery and classified the disaster recovery network according to the following categories:

3.2.2.1 Deployable Cellular Network for Disaster Recovery operations

Cellular network is a pre-existing wireless network infrastructure that provides efficient, mobile, and stable communications. However, the cellular infrastructures are subject to unintentional failures caused by natural catastrophic disasters, such as tsunami, floods, fire and earthquakes, as well as intentional failures caused by artificial disasters (human-made), such as terrorist attacks and war (Vasseur et al., 2004). As a result, many researchers proposed the

deployment of entire cellular base station on emergency vehicle to provide the required cellular network service in disaster area when the existing base stations were damaged, and allows communication needs for rescue teams as well as disaster victims. For instance, Sakano et al. (2013) proposed a network architecture called disaster-resilient network using specially designed MDRUs (movable and deployable resources units). The MDRU network can accommodate modularized communication equipment for network connection, information processing and storage, and can rapidly move or transported to a disaster area within a reasonable short time to launch ICT services required for rescue operations.

The authors simplified the network architecture by dividing it into three layers namely: network facility, network, and platform layers. Each of the MDRU units contains modular functionalities. According to Vishwanath, Greenberg, and Reed (2009) the modular functionalities are required for an effective performance of disaster resilient network. MDRUs are transported by helicopter, trailers, or any other vehicle to the disaster areas on a network facility layer. Furthermore, each MDRU is a box or container, carrying equipment of ICT services including routers/switches, wireless/wired receivers and transmitters, servers, power distribution units and probably air conditions. Moreover, every MDRU forms a wireless access point around it to allow wireless device connectivity. Existing fibre optics are used to establish connection between the MDRU and the nationwide networks. The system is efficient for emergency response and disaster recovery operations because of its fast network installation and launching of ICT services in disaster areas, and most importantly it remote operations and maintenance, thus reducing the number of professional staff needed after deployment. However, the nature of disaster environment attributed to limited resources (such as power and bandwidth) and varying traffic demand which may lead to repetitive reconfiguration of shortest path algorithms (Mao, Tang, Fadlullah, & Kato, 2019).

Similar to the MDRU deployable network, Li, Miyazaki, Wang, Guo, and Zhuang (2017) presented a network for disaster recovery and rescue operations called “*Vehicle-Assist Resilient Information and Network System for Disaster Management*” to reconnect isolated devices and servers during disaster recovery operation. The authors considered a disaster scenario whereby the affected region is divided into different separated communities. The disaster management at the centre of the region performs the function of sensing, collecting information and transmitting to targeted affected areas. A dedicated mobile app is used to search safe routes, generate SOS report, and request resources by users such as food, water and medical resources.

Equally, a mobile server is dedicated to received and automatically match resources to assign rescue task. The communication between nodes and servers is allowed by a vehicle-assisted network that can be vehicle refitted as MDRUs (Sakano et al., 2013). The authors proposed an online algorithm to address the challenge of unpredictable tasks attached to disaster areas and limited mobile station with the objective of maximising the weight of conducting tasks. An extensive simulation was used to evaluate the performance of the online algorithm. However, there is need for energy friendly network that can preserve power for both network and end users.

Hazra et al. (2019) presented a novel disaster network architecture to address resource-constrained in post disaster environment. The idea behind their research is to efficiently allocate the limited network resources across different group (such as rescue teams, survivors, volunteer workers as well as disaster victims) during disaster recovery and rescue operation. For the proposed system to intelligently share such resources, the authors formulated the problem of network resources allocation as a non-linear programming optimisation problem (NLP) and proved that is a NP-Hard. Subsequently, an effective sub-optimal heuristic was used by the authors to solve the problem in polynomial time based on Dargapur, India real map using ONE simulator. The simulation results indicated that the proposed disaster network performed better than unplanned network architecture in terms of network latency and delivery probability. The proposed techniques efficiently allocated network resources across different groups such as Data mule (DM), Shelter point, information Drop Box (IDB), Master Control Station (MCS) and rescue volunteers. However, the researchers did not take into consideration of the paramount challenge (Energy) of communication networks in disaster area. For example, the deployed base station and IDB may suffer from power scarcity as most large scales disasters also damages power grids and left the affected areas blackout. Other challenges include device failure and memory overflow if the network resources are not properly allocated.

Ohyama et al. (2012) proposed the use of vehicles as network node for emergency communication in disaster area. The main drawback of their temporary disaster information network is lack of practical use of DSRC (Dedicated Short-Range Communication) system in countries with commonly occurring natural and artificial (mam-made) disasters like Nigeria. However, the system has been already in used in Europe and America. For example, DSRC system IEEE 802.11p operating at 5.8 GHz bands, ARIB STD-75 operating at 5.8 GHz bands and ARIB STD-109 operating at 760 MHz bands (IEEE Standards Association, 2010).

As can be seen from Figure 3-6, Research and Development (R&D) disaster temporary network allow mobile roadside units (Mobile RSU) and Vehicle on-board equipment (Vehicle with OBE) to serve as a network node in multi-hop network communication, whilst rescue teams and disaster victims should use their smart phones to access services. The network was designed to cover areas which includes disaster spots, hospitals and refuges that are in area of two kilometres (KM) direction of ten places and intend to configure and connect the disaster temporary communication network using the survived communication infrastructure within thirty minutes after the arrival of the emergency vehicles in the disaster area. Another limitation of the proposed network is that the vehicles carrying network base stations cannot cover all affected areas and the assumption that such vehicle will also serve disaster victims fails. Therefore, it is key to a successful disaster recovery operation to allow connectivity between victims and rescuers using short range radios.

Minh and Yamada (2015) presented a field evaluation process to verify and validate the feasibility of WLAN based multi-hop network for disaster recovery. The research work was based on their previous papers such as on-the-fly establishment of multi-hop access network for disaster recovery, Tree-based disaster recovery multi-hop wireless access network and toward commodity wireless Multi-hop Access Networks. Similar studies were also carried out by other researchers. For example, Câmara, Frangiadakis, Filali, Loureiro, and Roussopoulos (2009) proposed the virtual access point (VAP) technique implemented on mobile nodes to extend the coverage area of alive access points for further connectivity. The idea behind their research is to leverage virtual access points to function as a store carry-forward node in a delay tolerance network to opportunistically improve transmission rate without considering the continuity of the internet connection. The network topology is designed to extend internet connectivity to disaster victims who were left disconnected. The backbone network and the base station have been damaged, disabling internet access to the users in the disaster area. Instantly, the wireless devices that are close to the alive or surviving access points, such as mobile node 1 (MN1), established connection with the still alive access point as in Section B. The still alive access point initiates on-fly establishment of multi-hop access point (OEMAN) by asking the MN1 to download the required software which will transform MN1 into a virtual access point, and therefore extending internet access to other wireless devices. Subsequently, the OEMAN software will automatically be installed on any wireless device that associates with a virtual access point. As a result, every wireless device, becomes a virtual access point providing internet service to its vicinity, as in Section C.

After a catastrophic disaster, many parts of network infrastructure such as routers, access point, and base stations have been damaged, and victims in that area: PC1, PC2, M1, and M2 could not access the internet through their conventional routes. Thus, the disaster victims can neither inform the rescue teams nor their families about their safety status. The designed proposed a simple approach where on-side wireless devices can connect to each other and then link to a still alive access point, such as access point 1 (AP1) to access the internet. A wireless device is transformed into a virtual access point (VAP) by the used of in-built wireless interface card (WIF) to provide connectivity to the nodes in its coverage area. In other words, each intermediate wireless device such as PC1, PC2 and PC3, works simultaneously as both common station (STA) and virtual access point (VAP) using their in-built single physical wireless interface card (WIF). The proposed disaster network had multi-hop communication in mind that extend connectivity to out of coverage devices. However, the researcher did not consider power constraint as such devices that served as relays are subject to heavy CPU, memory, and communication subsystem usage. This eventually precipitates rapid draining of battery energy, leading to network partitioning thereby reducing the overall lifespan of the entire network.

Current Nokia LTE Network-in-Box (NIB) product supports 3GPP Release 11, and provides an excellent communication system for public protection and disaster operations (Nokia, 2015). The network comprises of a flat architecture of complete LTE network contains one node (eNodeB) representing base station, and supports easy configuration and deployment for network recovery and disaster operations. David (2015) argued that deployed LTE network can effectively facilitates communication needs for rescue teams in disaster area.

He further describes the LTE network in form of COW (Cell-on Wheels) and CIAB (Cell-in-a-Box) where entire base stations could be carried on emergency vehicles to provide required cellular network coverage in disaster area and allows communication needs for rescue teams as well as disaster victims. The major drawback of such disaster networks is the capability of the vehicle carrying the network base station cover the entire disaster areas as some affected areas have turned to no-drive areas. In addition, aftermath a major disaster, such network can only be relevant if and only if the victim's device has battery energy.

In Summary, deployable cellular network for disaster recovery and rescue operation provides communication services to rescue teams, rescue volunteers and disaster victims in some disaster scenarios. However, the techniques offers limited opportunity as the vehicles carrying

the cellular towers have constrained mobility (Z. Lu, Cao, & La Porta, 2016). In addition, the necessary logistics of deploying the network and keeping it functioning properly in an emergency required some intensive work. For example, some disasters go beyond crippling/impairing communication infrastructures as some scenarios equally cripple power grids such as Hurricane Maria struck Puerto Rico that wipe out 95% of the island's power grid (Night, 2017), along with most of the communication infrastructure which made it impossible for survivors to recharge mobile communication devices. In such cases, the deployed network requires an alternative power system such as solar panels or power generator which will also require constant fuel refilling to keep the generator functioning. As a result, an energy efficient disaster recovery network that can reduce the overall energy consumed both by the entire network and individual nodes is required for effective and efficient disaster recovery operation.

3.2.2.2 Satellite Based Disaster Recovery Network

Satellite communications has been widely used for long distance communication (hundreds of kilometre) and supports multimedia data transmission at the speed of 41Mbps and 12Mbps for return and forward links respectively (Jahir, Atiquzzaman, Refai, Paranjothi, & LoPresti, 2019). The satellite network provides access to both fixed and mobile terminals through various frequency bands such C-Bands and Ku Bands. The fixed terminals (such as VSAT) can achieve the data rates of 1.5Mbps or more while mobile terminals based on Mobile Satellite Service (MSS) can achieve up to 256Kbits data rate and usually deployed on automobiles, trucks, cars, airplanes and ships (Aijaz, Aghvami, & Amani, 2013).

Many researchers proposed the use of satellite technology to allow communication needs during disaster recovery and rescue operation as the network provides robust, flexible and reliable high speed connections (Kose, Koytak, & Hascicek, 2012). For example, Uchida, Takahata, Shibata and Shiratori (2012) proposed NDN network (Never Die Network) consisting of a satellite network and a cognitive wireless network (CWN) so that an effective possible links and routes are selected for emergency communication during disaster. The user is connected to the content server via mobile wireless node, and the nodes consists of different heterogeneous wireless standards such as IEEE802.11a/b/g/n. In the event of severe earthquake, a satellite system can be used to support temporary connections, and it also served as a node alive checker. The best possible links selection adapts an extended AHP method (Analytic Hierarchy Process) by a change of user policy and network environment during

catastrophic disaster. If the user environment or network environment can be changed, an appropriate route selection is proposed to be conducted by AODV (Ad-hoc On-Demand Distance Vectors) method with Min-Max analytic hierarchy process (AHP) values. The proposed network considered how rescue operations and area affected by disaster could be greatly assisted and communicated by a robust network connectivity, but they did not consider energy consumption of the network as the network itself can only be helpful when the end user devices have power.

Wódczak (2012) and Calarco et al. (2010) presented satellite based disaster network that shows how satellite communication system will be integrated to E-SPONDER (A project co-funded under security program by European Commission) to ensure continuous communication between first responders and operation centres such as Emergency Operation Centre, EOC and Mobile Operation Centre, MEOC during disaster recovery and rescue operation. The research uses European Telecommunication Standards Institutes (ETSI) DVB-RCS standards (matured open source satellite communication standard) (Morello & Mignone, 2006) for full duplex satellite communication link between EOC and MEOC that allows the speed of 10Mbps for downlink and 2Mbps for uplink transmission.

The main idea behind the E-SPONDER project is to provide a reliable, secure and interoperable ICT infrastructure that can allow communication needs for first responders during disaster recovery operation by incorporating state of the art wireless technology and cutting-edge information systems (Calarco et al., 2010). To achieve secured communication infrastructure, a two level of CA (certificate of authority) authentication is used in the network to reduce DoS (denial of service) attack and enforced authentication with authorisation. In addition, the issue of third party or central authority for secure key management was handled by allowing users to distribute certificates among themselves. To achieve communication interoperability, the authors introduced the so-called all connected techniques to facilitates continuous link between first responders, EOC and MEOC, and standard radio access technologies such as LTE, 3G, IEEE 802.11, Satellite communication and WiWAX with inter system mobility protocol (IEEE 802.21) as well as MANET techniques were used to provide best possible connectivity based on network available, location and service characteristic. Aside the limitations of satellite communication system, the researchers did not take into consideration of the paramount challenge (Energy) of communication networks in disaster area as considered by this research.

Thomasson et al. (2008) and Skinnemoen, Hansen, and Jahn (2007) presented an open disaster network architecture proposed by WISECOM (Wireless Infrastructure over Satellite for Emergency Communications) European project with a specific focus on integrating broadband satellite solution with terrestrial mobile radio networks such as GSM, UMTS and WiFi. WISECOM project is an initiative that came up with global requirements for disaster recovery network and discussed the important of satellite system for emergency communication. WISECOM architecture uses lightweight and readily deployable wireless technologies with location-based services to allow communication needs during disaster recovery and rescue operation. The authors proposed the use of aerospace distributed platform for emergency rescue applications and modelled the problem based on inter-operability of all participating networks according to their respective functions. The aerospace segment with terrestrial backbones were integrated with ad-hoc terrestrial networks for data connections and assisted localisation. Although the authors did not give details of their model in both papers, but it can be understood that their main focus is to integrate broadband satellite solution with terrestrial mobile radio networks for emergency communication. Therefore, the need effective disaster communication system that can save energy for both network and users is highly required.

Dervin, Buret, and Loisel (2009) proposes a satellite-based communication specifically for disaster recovery and rescue operations. The model uses underlay transmission of emergency satellite signals into frequency bands of transparent primary satellite telecommunication system and combined the satellite-based system with heterogeneous network depending on the nature of disaster. To allow low power emergency transmission and ensure primary signal is not affected by inter-system interference as several emergency services including mission alerts and voice communications are proposed, a wide band spreading (Dervin, Buret, & Loisel, 2008) is used. The wide band spreading was also used to superpose low power transmission over another satellite in the same Ku band frequency to increase efficiency. The authors analysed two scenarios of emergency transmission superpose to a broadcast mission over 36 MHz channel and a frequency multiplexed primary carriers over 36 MHz channel. The analysis shows that 20 kbps data rates can efficiently transmitted over 36 MHz channel to and from man-pack emergency terminals without impacting the performance of primary system. Besides broadcasting emergency information to handheld terminals, the authors argued that the solution can allow transmission at a very low data rate ranging from 10 to 100 bps without interactivity. The proposed solution handled transmission of low power emergency signals using transparent satellite communication system. However, rapid drainage of nodes battery is still a major

problem and as such, an energy friendly technique that can maintained disaster network until victims are rescued is needed.

Del Re, Morosi, Jayousi, and Sacchi (2009), Del Re (2011), Re (2012), described a Satellite-Assisted Localisation and Communication System for Emergency Services, SILICE: an Italian National Research Project. The SILICE project was funded by Italian Ministry of University and Research with the aim of developing a reconfigurable and cooperative navigation disaster communication system attaining a global coverage of emergency terrain by connecting affected areas with unaffected areas. Equally, the project presented a heterogeneous solution that allows integration of different communication system with HAPs (satellite and high-altitude platforms) and terrestrial network to support communication and navigation systems.

The architecture comprises of Emergency Control Centre (ECC), Emergency Vehicle (EV), and First Responder (FR) which reflects the features of real-life disaster scenario. Disaster services such as preparedness, mitigation, response, and recovery are proposed to be handled by satellite-terrestrial cooperation. This services are achieved with the help of anchor node that shared satellite data traffic with first rescuers on MANET using ODMRP protocol: a MANET routing protocol that assures high reliability and scalability (Viswanath, Obraczka, & Tsudik, 2005).

To define reconfiguration and flexibility of user terminals to cope with the requirements of navigation and communication, NAV/COM, the Authors recommended the used of software-defined radio for efficient interoperability. However, the main focus of the authors is integration of satellite-terrestrial communication system to allow communication, localisation and monitoring services for emergency communication without taken into consideration of factors that usually affects the performance of emergency networks such as power consumption routing, network congestion (Onwuka, Folaponmile, & Ahmed, 2011), logistics etc.

Y.-M. Lee, Ku, and Ahn (2010) presented a satellite communication system as a core network for disaster recovery and rescue operations, which can be used for different applications dependent on the needs and efficient technologies deployed to allow interoperability. The authors argued that a satellite communication system should be designed to allow configuration mixed operation of star and full mesh topology. This will allow the deployment of different disaster technology and coverage of the entire disaster zones. The proposed network comprises of satellite, satellite gateways, VSATs, disaster situation control office (DSCO) stations and

handheld terminal. However, they do not consider aside from the long propagation delay of satellite communication, the so-called terminals will not be available to both disaster victims and rescue volunteer who gives first-hand information about disasters. Furthermore, most major disasters (as targeted by this research) go beyond destroying terrestrial core-network as it also cripple power grids (de Onís, 2018) which may affects the energy supply for the deployed network.

Peng, Yan, Liu, and Deng (2009) present a multi-media emergency command network based on satellite IP link, aimed to use emergency mobile command to improve the efficiency of integrated emergency communications, dispatching and strategic disaster decision analysis. The proposed system can transmit geological disaster information (video and audio) at any time via satellite IP link. This makes it possible for rescuers to form different spots to communicate among themselves through video conference to resolve emergency issues at the same time. In addition, the network can equally be used to allow communication need for various disaster scenarios including floods and fire break, (aid direction of safe routes). However, energy-aware techniques are needed to keep the network and user devices running until all lives and properties are rescued.

In summary, satellite communication system has been used for long distances communication of hundred kilometres and proven to be suitable for disaster recovery and rescue operations. However, beside the long propagation delay of satellite communication which result to long packet processing delay (Jahir et al., 2019), and poor network due to cloud covers in some disaster (such as storm or hurricane), the solution (such as satellite phones) may not be available to disaster victims and volunteer workers in the aftermath of a disaster. Although, there are other satellite-based disaster network (Mao et al., 2019), (Uchida, Takahata, Shibata, & Shiratori, 2012), (Del Re et al., 2009) that are used to extend coverage outside disaster area or connect diverse disaster spot, yet there is need for energy friendly disaster network that can preserve energy for both network and end user devices.

3.2.2.3 MANET-Based Disaster Recovery Network

MANETs are applicable to be used in places without network infrastructure or where the infrastructure has become unavailable as a result of disaster. With the development in wireless communication and increase of mobile devices penetration, users move around with their smart phones or keep them in places where they can be easily accessed even when disaster strike.

Such devices are equipped with wireless radio technologies including Wi-Fi, Wi-Fi Direct, GPS and sensors, and are used to establish temporary network called MANET without necessarily relying on conventional network infrastructure.

MANET provides an attractive solution that allow communication needs during disaster recovery and rescue operations. Over the years, much research has been carried out to address the challenges of MANET for efficient disaster recovery operations. Among the earlier research is the work of S. Singh, Woo, and Raghavendra (1998) who presented a simulated research using power-aware metrics for efficient routing to increase network and nodes life time. W. Lu et al. (2007) designed a two-tier Hierarchical Network for rescue operations using hybrid MANETs.

The design had communication among rescue teams and with their headquarters in mind. However, their approach is completely different from this research approach, as they examine two categories of network scenarios that allowed multimedia traffic among rescue teams and with their headquarters using three wireless technologies: GEO satellite, WLAN and WiMax, and multi-media software applications, in particular, VoIP. Rescue team members communicate with each other as well as with their headquarters located in a faraway place as in Figure 3-1.

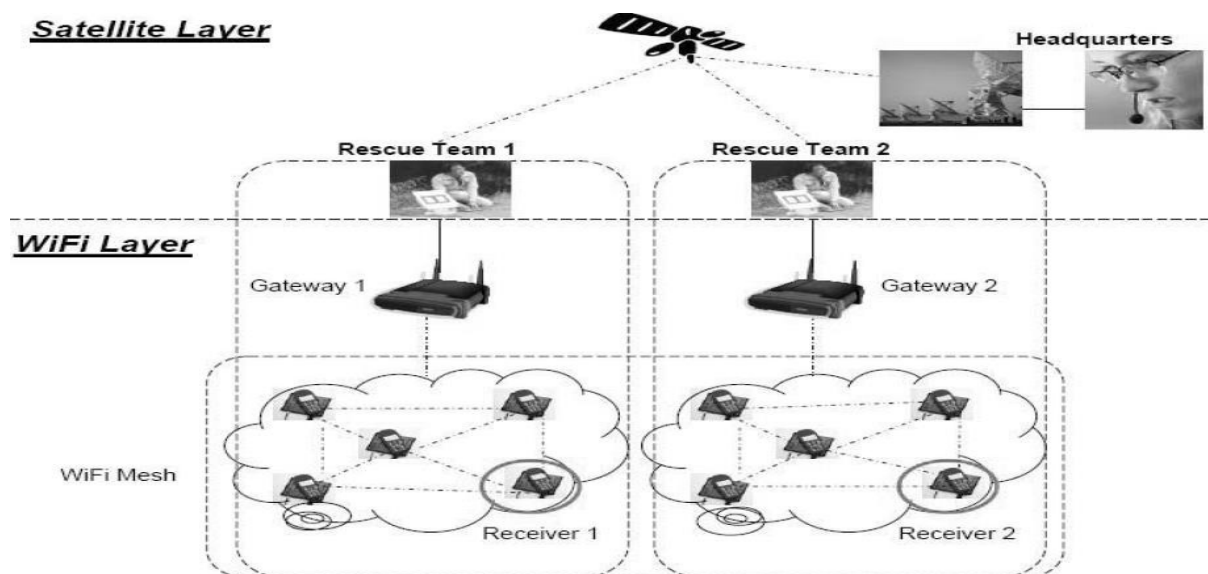


Figure 3-1: Two-tier Hierarchical Network (W. Lu et al., 2007)

However, it could be a better solution if the research considers preserving the power consumption of both the network and the nodes as the solution can only work when the devices

involved have power, as intended by this research. In addition, Multi-hop MANET running optimised link state routing protocol (OLSR) is used for intra team members' communication, while communication among rescue team members and the headquarters is achieved using satellite link. However, OLSR protocol constantly busy routing control messages in the background (regardless of user messages), thus, the continuously background routing constitutes a drain on bandwidth and battery energy. According to the authors, the design was validated using a real field deployment, and simulated using Qualnet simulator to determine an appropriate parameter for further performance studies. In the actual field test, the rescue team members are connected using virtual private network, to minimise the requirement of gateway and protocol translation and therefore, all MANETs devices seems to be in the same MANET.

Raj et al. (2014) proposed a novel architecture called E-DARWIN (energy aware disaster recovery network) using WLAN tethering technology. The idea behind their work is to use the WLAN tethering ubiquitously available on smart phones and tablets to configure a MANET for the purpose of data collection in disaster area. The novel mechanisms aid in creation of the MANET, collection, and distribution of data among the wireless devices with minimum delay. As shown in Figure 3-2, the remote ECC (emergency command centre) is the central component of the recovery network. It receives data from the disaster affected area, analyses, and coordinates rescue teams accordingly. ECC assumed to becomes operational as soon as disaster occurs.

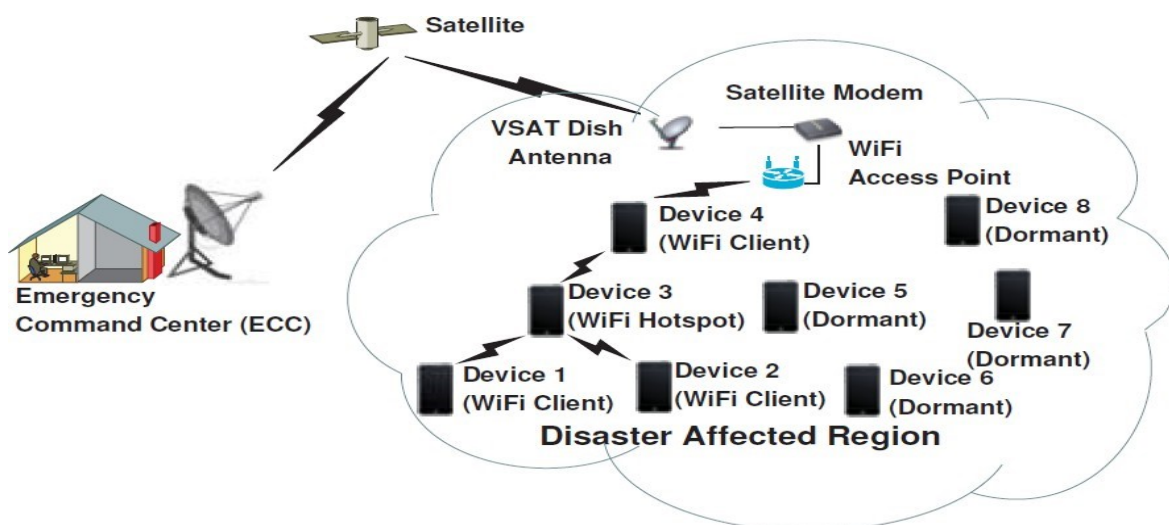


Figure 3-2: Network Architecture of E-DARWIN (Raj et al., 2014)

The disaster recovery network is composed of various interconnected components formed by wireless devices of the disaster victims. The main function of the wireless devices is to collect

data for the disaster affected area, store and forward the data to the emergency command centre (ECC). The authors used a technique called: Distributed coalition formation game, to extend network lifetime by using available energy and network participation to share data capturing task. However, authors used Wi-Fi tethering to setup the MANET which is not viable to setup multi-hop communication network which is important for disaster recovery networks. Furthermore, the energy preservation techniques were implemented based on assumptions which is against the real-life implementation of disaster network. Similarly, no plan to preserved energy consumption of nodes that are crucial to the connectivity. And as such, disaster network that can preserved power consumptions for both network and user devices until all victims are rescue is needed.

Y.-N. Lien, Jang, and Tsai (2009) designed MANET based group emergency communication network called P2P, for rescue teams in both natural and artificial disasters. The P2P network is a peer-to-peer server-less system based on infrastructure-less wireless network (MANET) to allow temporary cluster communication as shown in Figure 3-3. They constructed the network using WLAN-ready notebooks while other nodes have satellite communication capability to provide internet access to other nodes. However, energy-aware techniques are needed to keep the network and user devices running until all lives and properties are rescued.

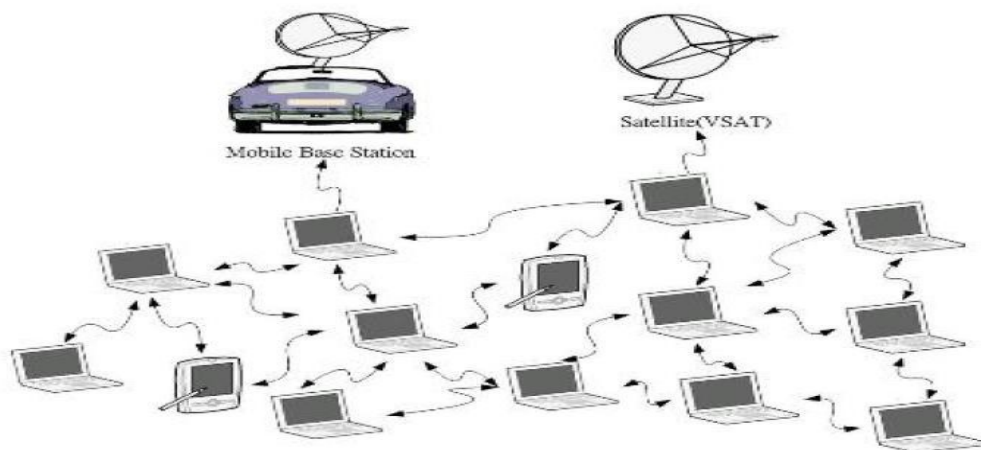


Figure 3-3: Network Architecture of P2Pnet (Y.-N. Lien et al., 2009)

Y. N. Lien, C. Li-Cheng, et al. (2009) also designed and implemented an emergency network recovery system called single hop Walkie-Talkie communication technology to allow emergency communication needs of rescue operations in early hours of catastrophic disasters. The emergency network is very simple and can easily setup by non-trained personnel in disaster area. Thus, it is suitable for disaster recovery operations. They designed an intermediary layer

between Network layer and Transport layer, known as Network services layer, to allow network services at application layer as shown in Figure 3-4.

The new intermediate layer was used to create three networking modes: U1net (Uncontrolled One-Hop Cluster Communication System), UKnet (Uncontrolled K-Hop Cluster Communication System) and CKnet (Controlled K-Hop Cluster Communication System). U1net and UKnet nodes facilitates emergency communication by allowing nodes to broadcast data to it neighbouring nodes without any authorization enforcement. However, U1net operates in one-hop distance, while UKnet in K- hop distance, which covers more than one hop. On the other hand, CKnet is the most developed and advanced approach that can effectively support services such as VoIP.

Layer	Functional Modules					
Application Systems	Disaster Rescue Info Sys		Mobile Learning Sys.		Battle Field Manage. Sys.	
Application Functional Modules	FTP/HTTP /Telnet/etc.	PTT	VoIP	P2P Streaming	Location-Aware Applications	
Transport	TCP	UDP	Partial-Reliable TCP	Partial-Reliable UDP	Hop-by-hop TCP	P2P Multicasting
Network Service	Uncontrolled Single-Hop Group Communication Network (U1net)		Uncontrolled K-Hop Group Communication Network (UKnet)		Controlled K-Hop Group Communication Network (CKnet)	
Network Routing	Ad Hoc Network		Mesh Network		VANET	
Physical	RF Positioning System		Wi-Fi	WiMAX		

Figure 3-4: Logical Architecture of P2Pnet (Y. N. Lien, Li-Cheng, & Yuh-Sheng, 2009)

The reason for developing the three networking modes is because, a disaster recovery operation requires a reliable emergency network that can be setup easily, and in the event of disaster, there is not enough time to deploy a full functional network and therefore, a simplest network such as U1net and UKnet can be deployed quickly to support communications within short range in the early hours of rescue operations. Meanwhile, if time permitted, CKnet mode can be deployed to launch a more advanced and effective system to support full communications needs for the rescue operations as identified by the authors.

Kanchanasut et al. (2008) presented a disaster network project called Digital Ubiquitous Mobile Broadband OLSR (DUMBO II) that uses MANET for aftermath disaster operations. The disaster network: DUMBO was designed to allow VoIP, video streaming and short messages to be transmitted simultaneously from a central command centre, CCC to rescue

workers using different wireless devices such as laptop and personal digital assistants, PDAs. As a result of DUMBO I limitation, Tuk-Tuk, long tail boats and motorcycles were used for high mobility and rapid topology changes. Furthermore, OLSR parameters were adjusted to allow mobile nodes to get more frequent updates of topology changes and neighbourhood information for better connectivity to all participating elements of the DUMBO II network. To deploy internet connected MANET, like this research, DUMBO II disaster network setup a two interface (wireless and LAN) machine as OLSR gateway whereby LAN interface is connected to internet to allow communication with headquarter devices, while the wireless interface is used for MANET connectivity.

The authors deployed nested network mobility (NEMO) topology for network coverage extension via Mobile Router (MR). The MRs has two interfaces namely: Egress and Ingress. Egress interface is used for MANET while the Ingress interface is used as an access point and as such, each MANET device has the capability to act as MANET device and exchange topology information with other MRs. The network demonstrated a concept of extending internet connectivity for post disaster recovery and rescue operation with changing topology using long tailed boats, motorcycle etc. However, changing OLSR parameters for nodes to get more frequent updates of neighbourhood and topology information may result to message collision. Message collision occurs when messages become synchronize or coordinated, for example, a node may wish to report a change in its set of MPR via HELLO message, which may trigger a network control message (TC message) in a set of neighbouring nodes, this would lead to collision since the receiving node is already busy with the HELLO message (Clausen, 2004). In addition, provision of a temporary OLSR protocol MANET for disaster communication often drains device battery energy, since message routing and network flooding are prominent requirements of OLSR protocol, and such devices depend solely on their battery for power. Therefore, the protocol (OLSR) needs to be optimised to preserved energy for both network and users' devices during rescue operation.

Vo, Duong, and Guizani (2015) presented a Quality of Sustainability (QoSus) model for MANET based on existing three-tier cellular network. The proposed network is designed specifically to be deployed in the aftermath of a disaster to allow communication needs between different Mobile Units (MUs) for quick disaster response, high interoperability, and high capacity of contents delivery. In addition, the authors considered a three-tier cellular network comprises of Base Stations (BS), Femtocells (FC, low power base station for indoor) , and

several Mobile Users (UMs) connected to establish a MANET to solve high QoS of MANET via optimisation problems as shown in Figure 3-5. The model was simulated, and the results demonstrated that MANET if supported by femtocaching and D2D communication techniques can reduce BS workload for quick response during disaster recovery operation. The researchers demonstrated how nodes with highest energy resources and better channel gain will serve as a relay node but did not provide techniques to preserve the power of the nodes as intended by this research.

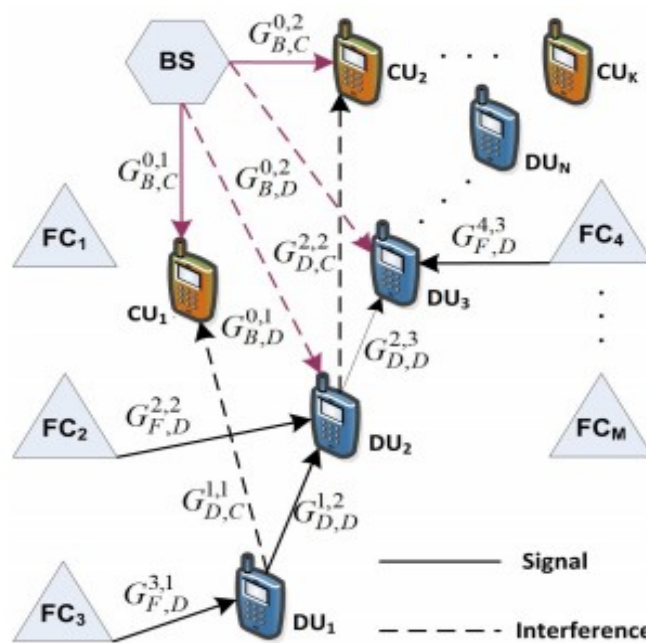


Figure 3-5: MANET Based Three-Tier Cellular Network (Vo et al., 2015)

Jagannath et al. (2019) developed an end-to-end (hardware and software) disaster communication solution that allows text and voice messages amongst end users (EUs) and between EUs and emergency responders (ERs) in the aftermath of disasters that cripples primary communication infrastructure. The cross-layered solution is called Heterogeneous Efficient Low Power Radio (HELPER). HELPER's goal is to provide a kit that households can deploy in the aftermath of cellular service going offline, each kit sets up ad-hoc communication between neighbours and with the emergency response centre (ERC), while HELPERS deployed at homes are stationary, ERs are equipped with mobile HELPERS which could be used to communicate with victims. The HELPER network is equally boosted by HELPER drones that take over when there is node failure. A major challenge with HELPER is the assumption that each HELPER device has enough electricity to operate and thus can operate continuously. Moreover, HELPER equally assumed victims are strong enough to attach HELPER kits to their

home after a disaster, nonetheless, the most challenging feature of HELPER is the need to purchase the kit in the first place, when users can simply use their mobile phones without spending extra cash on specialized gadgets. HELPER development/deployment prototype/scenario is shown in Figure 3-6.

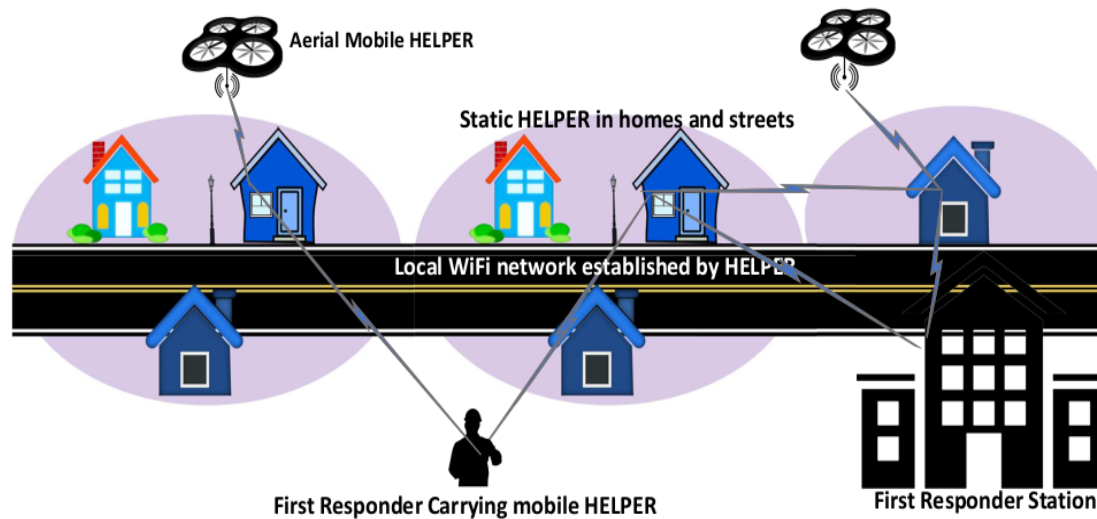


Figure 3-6: HELPER development/deployment prototype/scenario (Jagannath et al., 2019)

Relay-by-smartphone was proposed by Nishiyama et al. (2014) as a backup communication platform in the event of the primary network going offline in the aftermath of a disaster. Relay-by-smartphone adopts D2D communication via MANET (using OLSR or epidemic routing) or via delay/disruption-tolerant networks (DTNs) and opportunistic networks (OppNets). The primary messaging mode supported is text messages, mainly from emergency response teams as a medium of providing information on supplies, however, text message can equally be sent outside the network if an enabling technology exists. The key strength of Relay-by-smartphone is the extension of mobile devices in the possession of victims as the communication terminals. However, like HELPER, it assumed victims can recharge their mobile devices using handheld solar panels, this is the case in developed regions, but unfortunately does not apply in locations like Puerto Rico and the Bahamas, these locations suffered terrible hurricane related disasters which crippled communication and power infrastructures, thus Relay-by-smartphone did not attempt to lower energy consumed by routing algorithms. Relay-by-smartphone deployment and usage scenarios are captured in Figure 3-7 while the cross-layer communication diagram is captured in Figure 3-8.

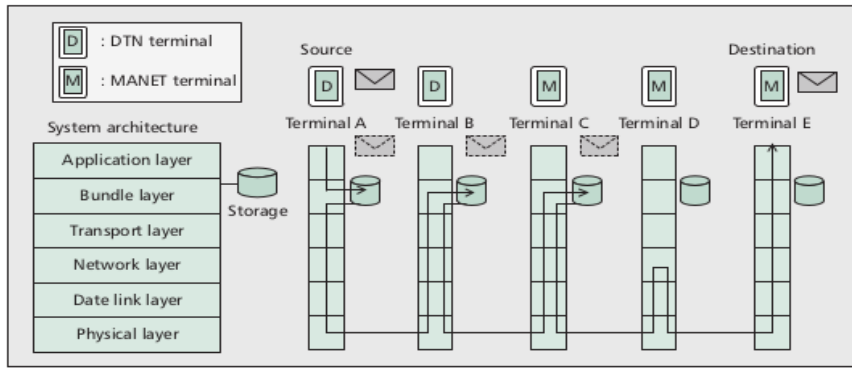


Figure 3-7: Message transmission in the architecture of DTN over MANET (Nishiyama et al., 2014).

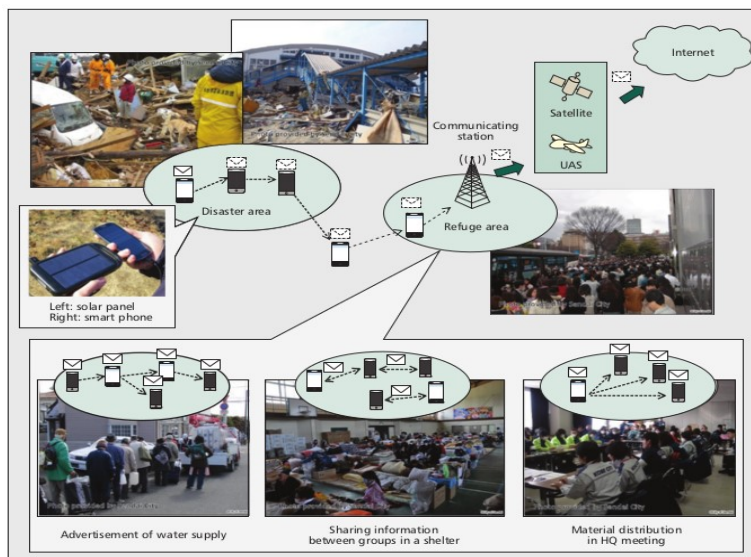


Figure 3-8: Deployment and usage scenarios for Relay-by-smartphones (Nishiyama et al., 2014)

Z. Lu, Cao, and La Porta (2017) proposed a cross-layer communication solution designed around AODV routing. Their proposed solution is called Teamphone, it is designed to enable search and rescue operations in the aftermath of a disaster as in Figure 3-9. Unlike Nishiyama et al. (2014) and (Jagannath et al., 2019), Teamphone attempts to reduce routing related energy via scheduled sleep within clusters of smartphones. Thus, each smartphone forward messages meant for rescue teams to the cluster head whose turn is to stand on guard while other nodes are sleeping. The cluster head sends accumulated messages as soon as the communication device of a rescue team comes within range. Teamphone equally stores the last known location of a victim's smartphone, however, a major drawback with Teamphone's location identification is that the last location stored before cellular network propagation went off might be the victim's office while the victim is trapped in his or her home. In addition, a scenario was

presented to rescue trapped victims in their houses, and they argued that the design was implemented using AODV instead of proactive routing protocol due to frequent network changes in disaster environment, nonetheless trapped victims cannot move until they are rescued.

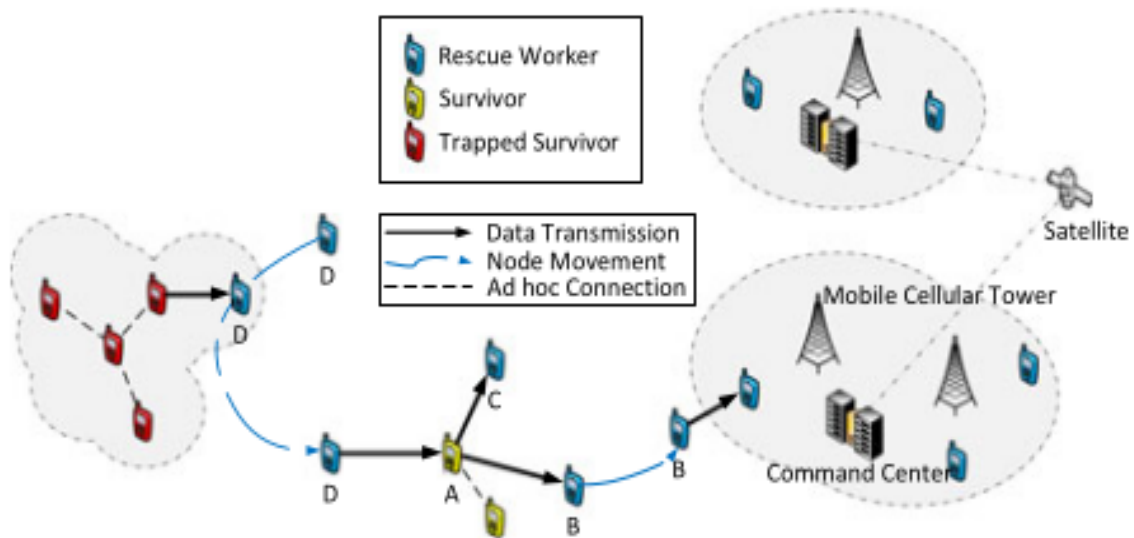


Figure 3-9: Teamphone deployment scenario (Z. Lu et al., 2017)

M. Iqbal (2010) modified AODV to support effective multimedia communication of Wireless Mesh Network (WMN) amongst emergency teams during search and rescue operations, or in the aftermath of a disaster. The resultant modification (called Load-Balanced Gateway Discovery routing protocol or LBGD-AODV) enables efficient multimedia communication by using multiple gateways to route multimedia traffic, while equally providing load balancing functionalities for Internet traffic. The drawback of their research is unfairly communication is restriction to rescue team members which implies victims will not be able to communicate the safety to rescue teams or loved ones as intended by this research.

In addition, the research did not take into consideration of the paramount challenge (power) of most disaster network areas, and as such, a disaster network that can provide both rescue teams and victims with communication infrastructure with energy friendly technique that can maintained disaster network and preserve device battery until victims are rescued is needed. Figure 3.10 presents LBGD-AODV architecture.

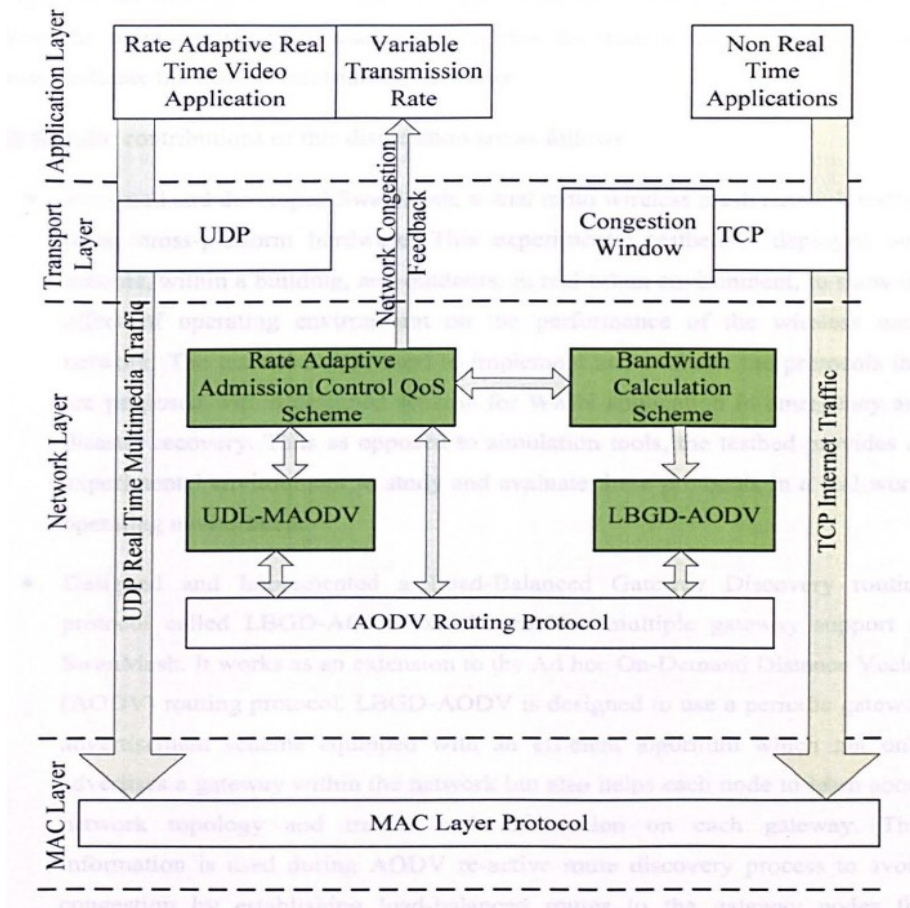


Figure 3-10: LBGD-AODV architecture (M. Iqbal, 2010)

Hoque, Razu, Islam, and Amin (2020) proposed a Software Defined Network (SDN) integrated with Delay Tolerant Network (DTN) for disaster recovery and rescue operations. To guarantee message delivery for crucial time, the authors introduced four layers namely: Victim nodes, DTN trend, Control station and DTN layer as shown in Figure 3-11. Victim nodes and DTN layers are DTN enabled devices (such as mobile phones) and bundle of storage/convergence layer, respectively. Monitoring application that monitors the entire network and provide feedback to controller for better performance is represented by DTN trend. The network was evaluated in a simulation environment using ONE simulator and the results showed that convergence SDN-DTN can efficiently improve message delivery rate. However, the proposed scheme defined different service request but has no defined priority for the various service requests. In addition, the new layers created as more network overhead and the authors do not consider any power preservation techniques as intended by this research.

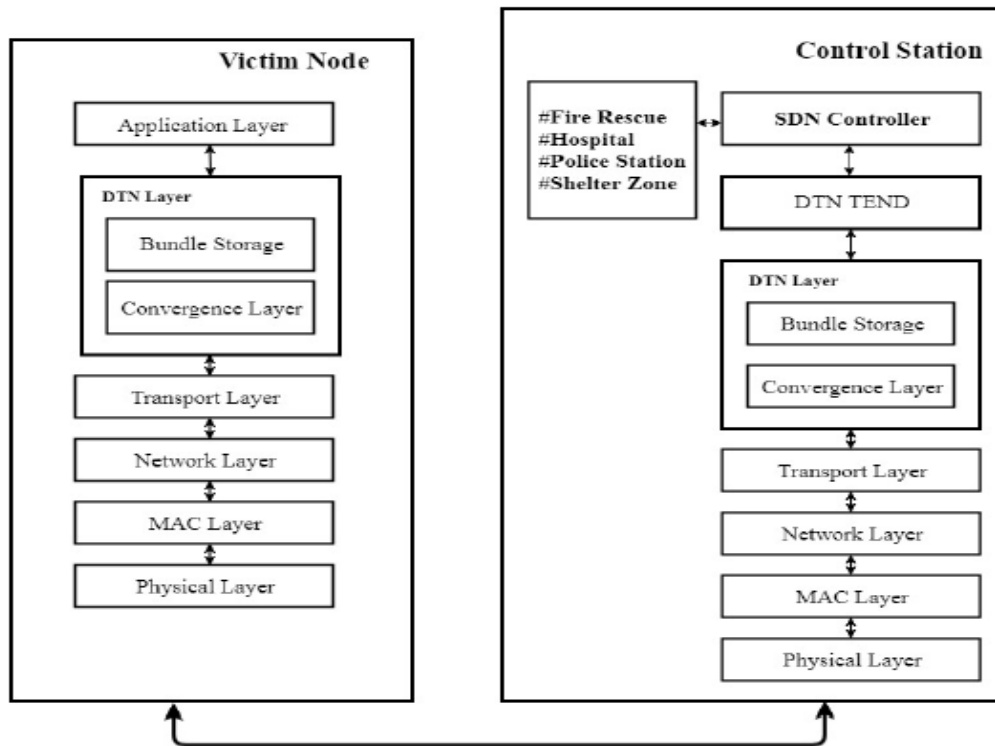


Figure 3-11: SDN-DTN Blended Architecture (Hoque et al., 2020)

K. Ali, Nguyen, Vien, Shah, and Raza (2020) presented ad-hoc drone-based resilient disaster communication architecture to increase the number of nodes to be served by drone small cells (DSCs) and prioritizes communication of rescue teams and vulnerable individuals. A matching game algorithm is used based on one-to-many scheme to match different nodes to determine effective link with optimal throughput using several deployed DCSs. To prioritize and improve channel accessibility for first responders and vulnerable individuals within disaster zones, the authors redesigned MAC layer and used dynamic priority techniques that classifies and prioritizes communication for critical node once connection between users in disaster area and drones are established. The authors argued that the introduction of DSCs as shown in Figure 3-12 plays a vital role in re-connecting disaster victims and rescue teams to achieve coordinated rescue activities. The results of their simulation showed a better performance of their proposed system as it reduced channel access delay for emergency communication to 1ms for sparse and 3ms or less for dense networks, respectively. Utilization of drone small cells (DSCs) and prioritization of emergency communication during disaster recovery and rescue operations is highly beneficial as it provides adaptability, mobility, and flexibility to extend coverage and improve throughput. However, the article did not optimize nor evaluate the energy consumption of the techniques and such networks can only be helpful when the end user device has power.

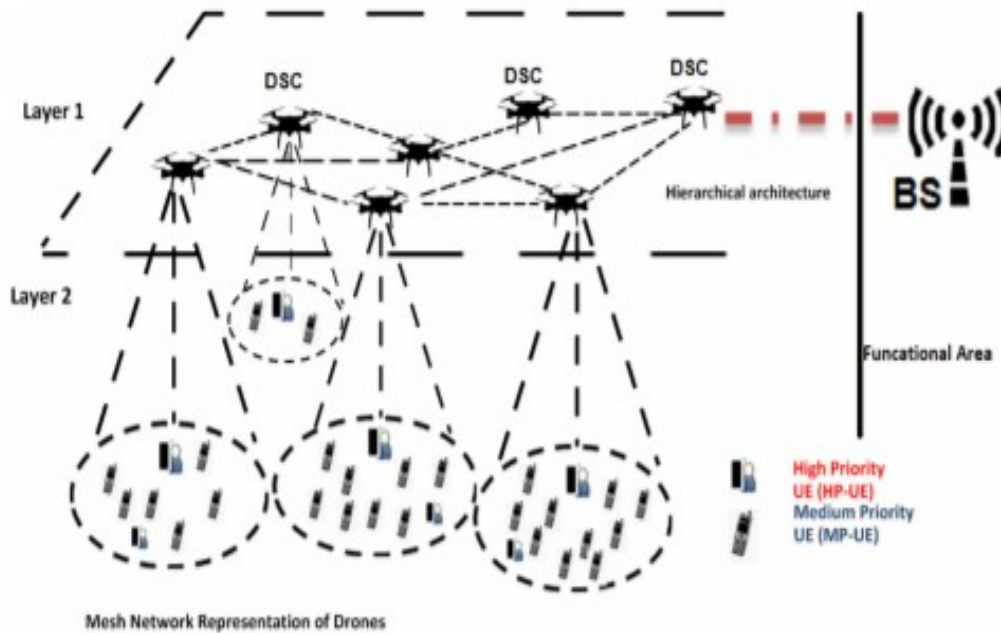


Figure 3-12: Disaster Scenario of Deployed Drone-Base Small Cells (K. Ali et al., 2020)

Xiaoyan Wang et al. (2020) proposed an optimised mobile resources deployment units in disaster areas and predictive population system to predict post disaster population. This allows appropriate distribution of relay nodes to cover the entire disaster population. The main idea behind their approach is the utilisation of crowd dynamics to estimate fine-grained distribution population in the aftermath of a major disaster, thereby guiding network scheduling. The approach of the post disaster network scenario is presented in Figure 3-13 displaying how the intelligent resource deployment network is formed by utilising crown big data. The intelligent scheme was evaluated in a real-life environment and the results showed reduction in estimated error for population distribution by 56% - 69% as compared to regressive models and that limited number of relays can efficiently cover large population. Similar to Hoque et al. (2020), the research did not optimize nor evaluate the energy consumption of their techniques and such scheme can only be helpful when the end user device has power. In addition, most major disasters equally damage power grids which necessitate the requirement for energy efficient disaster network especially in places with commonly occurring of natural and human-made disaster.

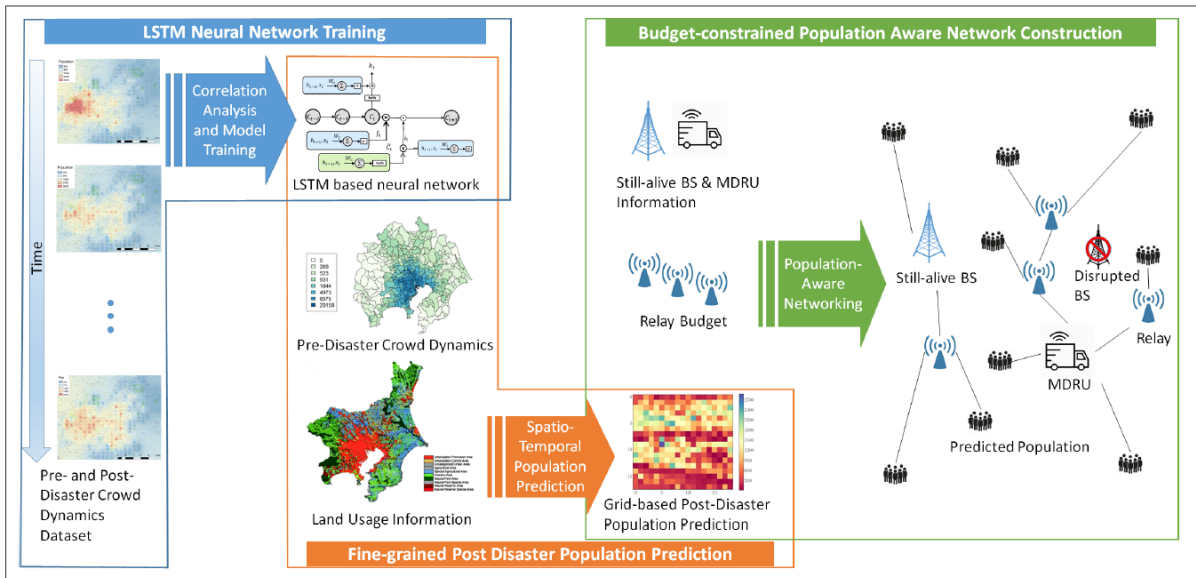


Figure 3-13: Intelligent Resource Deployed Network Approach (Xiaoyan Wang et al., 2020)

J. Zhou, Zhou, Kang, and Tu (2021) presented a post disaster communication network called: *integrated satellite ground-emergency construction network (ISG-ECN)*. The network is divided into two parts namely: satellite portable station and ground mesh network as shown in Figure 3-14. The authors adopted a portable design that can be easily deployed by rescuers to support communication needs during disaster recovery and rescue operations. External communications are achieved using satellite station via local area network, while ground mesh network is used for communication with the disaster zone. Another interesting part of their emergency communication network is the evaluation of the system in real life disaster environment (including flood and earthquake) which evident that the scheme will be set quickly and support multi-user access. However, thirty (30) minutes set up time is not efficient for post disaster communication network as such networks required to be simple and can easily setup by non-trained personnel in disaster area within shortest possible time (Minh & Yamada, 2015) (Y. N. Lien, J. Hung-Chin, et al., 2009), as intended by this research. Another drawback of their disaster communication network is an assumption that nodes will be equipped with Unattended Power Source (UPS) and rechargeable energy battery to relay and maintain communication in the aftermath of a disaster. However, victims can simply use their mobile phones to connect to energy friendly network without spending extra cash on specialized gadgets and maintain communication until they are rescued as proposed by this research.

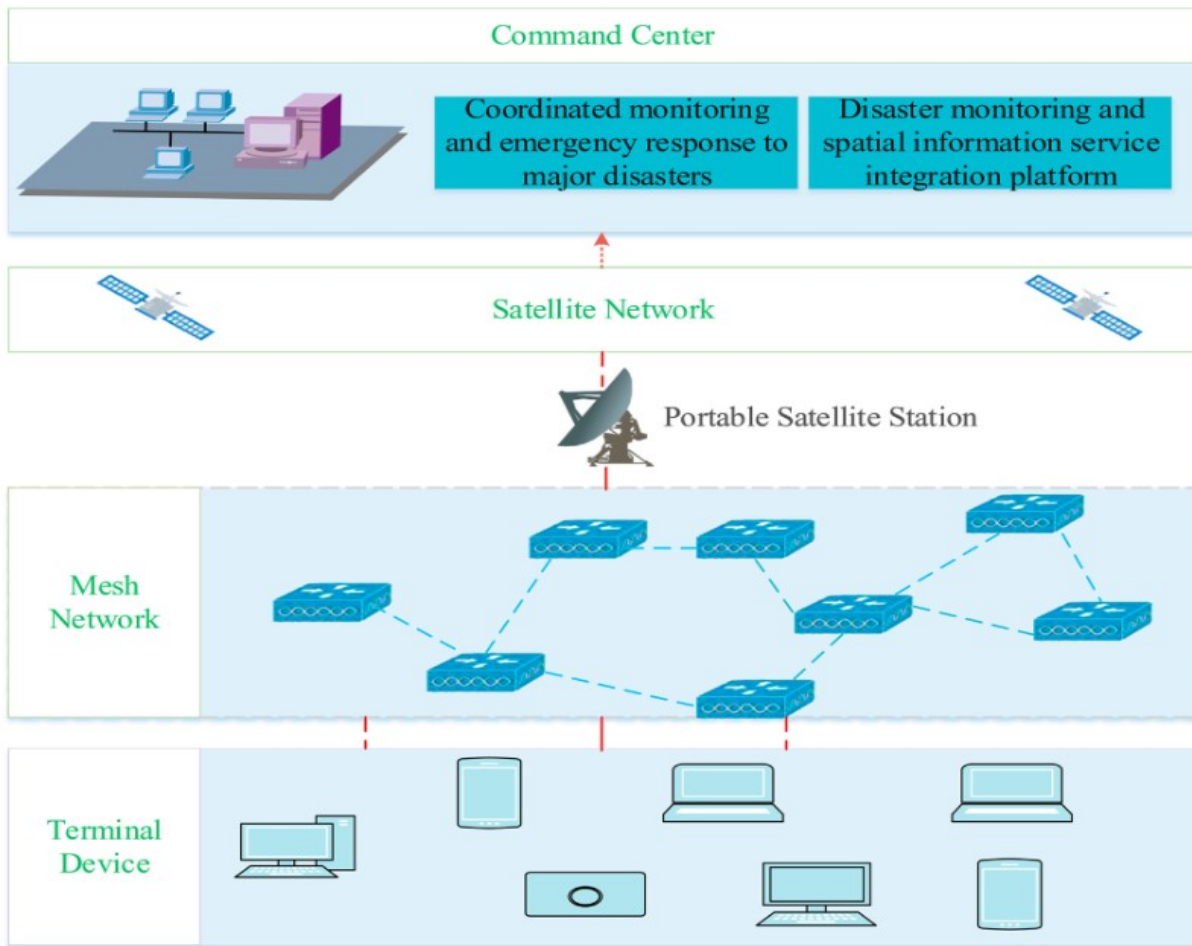


Figure 3-14: ISG-ECN Deployment Model (Xiaoyan Wang et al., 2020)

3.2.3 Summary of Reviewed Disaster Recovery Networks

The reviewed disaster recovery networks are summarised in Table 3-1 highlighting the author(s) name and date, network type, key features, disaster recovery network (DRN) specific and energy efficiency. The Table point out clearly that less research has been carried out to optimise energy for disaster recovery network, and as such, an energy efficient disaster recovery network that can reduce the overall energy consumed both by the entire network and individual nodes is required for effective and efficient disaster recovery operation.

Table 3-1: Summary of Reviewed Disaster Recovery Networks

Author(s) & Date	Network Type	Key Features	DRN	Energy Efficiency
Morrison (2011)	Deployable Cellular Network	Replacement of complete office telecommunication infrastructure on trailers.	√	-

Sakano et al. (2013)	Deployable Cellular Network and ICT service	Design of deployable MDRU on Helicopters and Trailers	√	-
Li et al. (2017)	Deployable Cellular Network and ICT service	Relay-Based cooperative network to reconnect isolated devices and location	√	-
Hazra et al. (2019)	Deployable Network on Cars	Network Architecture design to address resource-constrained in post disaster environment	√	-
Ohyama et al. (2012)	Deployable Network on Vehicle	Coverage extension using Mobile Roadside Units and Vehicle On-Board Equipment	√	-
Minh Quang Tran, Kien, Borcea, and Yamada (2014)	Deployment of on-the-fly establishment of multi-hop access network	On-fly Establishment of Multi-hop Access Point	√	-
Minh and Yamada (2015)	Deployable of WLAN Based Multi-hop Access Networks	Using Still-Alive access point to extend internet coverage	√	-
Nokia (2015)	Deployable LTE Network-in-Box (NIB)	Flat architecture of complete LTE network contains one node (eNodeB) representing base station supports 3GPP Release 11	√	-
David (2015)	Deployable COW (Cell-on-Wheel) Base Station	Entire LTE network in form of COW (Cell-on-Wheels) and CIAB (Cell-in-a-Box) to provide cellular network in disaster area	√	-
Uchida et al. (2012)	Satellite-Based Network	NDN (Never Die Network) consisting of a satellite network and a cognitive wireless network (CWN) so that an effective possible links and routes are selected using AODV	√	-
Wódczak (2012) and Calarco et al. (2010)	Satellite-Based E-SPONDER Network Project	Combined satellite communication system and E-SPONDER project with special attention to security	√	-
Thomasson et al. (2008) and	Satellite-Based WISECOM architecture	WISECOM with a specific focus on integrating broadband satellite	√	-

Skinnemoen et al. (2007)		solution with terrestrial mobile radio networks such as GSM, UMTS and Wi-Fi.		
Dervin et al. (2009)	Satellite-Based system with heterogeneous network	The model uses underlay transmission of emergency satellite signals into frequency bands of transparent primary satellite telecommunication system	√	√
Del Re et al. (2009), Del Re (2011), Re (2012)	Satellite-Assisted Localisation and Communication System for Emergency Services (SILICE)	Heterogeneous solution that allows integration of different communication system with HAPs (satellite and high-altitude platforms), terrestrial network and navigation systems	√	-
Y.-M. Lee et al. (2010)	Satellite-Based Network	Satellite communication system as a core network to allow interoperability between different network technology	√	-
Peng et al. (2009)	Multi-media emergency command network based on satellite System	Improving the efficiency of integrated emergency communications, dispatching and strategic disaster decision analysis	√	-
W. Lu et al. (2007)	MANET running OLSR	Two-tier Hierarchical Network to allow VoIP traffic among rescue teams and with their headquarters using three wireless technologies: GEO satellite, WLAN and WiMax	√	-
Raj et al. (2014)	MANET-Based E-DARWIN	Distributed coalition formation game techniques were used to extend network lifetime	√	√
Y.-N. Lien et al. (2009)	MANET-Based P2Pnet	Allow interoperability between nodes of different network technologies	√	-
Y. N. Lien, C. Li-Cheng, et al. (2009)	MANET-Based Network	Designed an intermediary layer between Network layer and Transport layer,	√	-

		known as Network services layer, to create three networking modes		
Kanchanasut et al. (2008)	MANET-Based DUMBO I and DUMBO II running OLSR	Coverage extension, mobility and internet sharing	√	-
Vo et al. (2015)	MANET-Based Quality of Sustainability (QoSus) of three-tier cellular network	Focused on three-tier cellular network comprises of Base Stations (BS), Femtocells (FC), and several Mobile Users (UMs) connected to establish a MANET to solve high QoSus of MANET via optimisation of problem	√	√
Jagannath et al. (2019)	MANET-Based HELPER	Cross-layered solution called Heterogeneous Efficient Low Power Radio (HELPER)	√	√
Nishiyama et al. (2014)	MANET-Based DTN	Relay-by-smartphone adopts D2D communication via MANET (using OLSR or epidemic routing) or via delay/disruption-tolerant networks (DTNs) and opportunistic networks (OppNets).	√	√
Z. Lu et al. (2017)	MANET-Based TeamPhone	TeamPhone attempts to reduce routing related energy via scheduled sleep within clusters of smartphones	√	√
Y. Wu, Xu, Lin, and Fang (2017)	MANET-Based OLSR's MPR selection process	Energy level of the node and the channel quality to influence MPR selection	√	√
M. Iqbal (2010)	MANET-Based Load-Balanced Gateway Discovery routing protocol (LBGD-AODV)	Multiple gateways to route multimedia traffic, while providing load balancing functionalities for Internet traffic	√	-
Santhi and Sadasivam (2011)	MANET-Based PAQMR	Power Aware QoS Multipath Routing protocol (PAQMR) that allow message routs based on bandwidth and available energy	√	√

Hoque et al. (2020)	MANET-Based SDN-DTN	Software Defined Network (SDN) integrated with Delay Tolerant Network (DTN) for disaster recovery and rescue operations	√	-
K. Ali et al. (2020)	Deployed Drone-Base Small Cells	Ad-hoc drone-based resilient disaster communication architecture to increase the number of nodes to be served and prioritizes communication of rescue teams and vulnerable individuals	√	-
Xiaoyan Wang et al. (2020)	MANET-Based Intelligent Resource Deployment Disaster Network	An optimised mobile resources deployment units for appropriate distribution of relay nodes to cover the entire disaster population.	√	-
J. Zhou et al. (2021)	MANET-Based ISG-ECN Deployment	<i>integrated satellite ground-emergency construction-network (ISG-ECN)</i> based on satellite portable station and ground mesh network	√	-

3.2.4 Why MANET Based Disaster Solution over Deployable WLAN Based Solution

In MANET, mobile devices do not depend on established infrastructure or base station. Therefore, each device operates as both host that can send and receive data, services, or application, and as router that can route information on behalf of other nodes. On the other hand, WLAN (wireless local area network) is a form of wireless network that allows wireless devices to communicate wirelessly with one another within the coverage area of an access point. The activities of such wireless devices are coordinated, controlled, and managed by the access point.

MANET is preferable for this research than WLAN because of the distributed nature of MANET's operation which eliminates the risk of single point of failure as in deployable WLAN. Although, deployable WLAN for disaster recovery and rescue operation provides communication services to rescue teams, rescue volunteers and disaster victims in some

disaster scenarios. However, the techniques offers limited opportunity as the vehicles carrying the WLAN have constrained mobility (Z. Lu et al., 2016). In addition, the necessary logistics of deploying the network and keeping it functioning properly in an emergency required some intensive work. For example, some disasters go beyond crippling/impairing communication infrastructures as some scenarios equally cripple power grids such as Hurricane Maria struck Puerto Rico that wipe out 95% of the island's power grid (Night, 2017), along with most of the communication infrastructure which made it impossible for survivors to recharge mobile communication devices. In such cases, the deployed WLAN requires an alternative power system such as solar panels or power generator which will also require constant fuel refilling to keep the generator functioning.

As discussed earlier, natural, and artificial disasters are unfortunately constant in our society. However, the ability to quickly report such incidence can save lives, properties, and communities. Thus, over the years, emergency numbers were incorporated into telephony systems, this permitted callers in an emergency to dial the emergency number specific to their country. Smartphones extended the system by allowing victims to dial emergency numbers even when the phone is locked. Sadly, emergency numbers require cellular infrastructure, hence they are unavailable when such infrastructures are crippled by disasters. Therefore, it becomes imperative to provide a mechanism which would automatically trigger disaster mode on subscribers' mobile devices and preserve their ability to contact rescue workers for help. Thus, the following Section review the process of switching mobile devices to disaster mode for effective and efficient disaster communication.

3.3 Mechanism for Switching Smartphones to Disaster Mode

In this section, the research reviewed automated mechanism that triggers disaster mode as shown in Figure 3.34. The stages are discussed as follows:

3.3.1 Steps 1 and 2: Weather Tracking Using Satellites

The desire to detect adverse weather conditions made USA to launch a weather satellite called the Vanguard 2 on February 17, 1959 (TIROS, 2016). A weather satellite is designed to monitor Earth's weather and climate from space. Satellites achieve this by either orbiting the Earth from pole to pole (polar orbiting) or by remaining stationary over the same spot (geostationary) while

covering the area under observation with different types of cameras that can monitor clouds, sand, dust, storms, snow, fire, etc (Toth & Buizza, 2019). Although Vanguard 2 was the first weather satellite to be launched into space, nonetheless it proved problematic in the area of data gathering due to its orbit. Hence the Television Infrared Observation Satellite Program (TIROS) (TIROS, 2016) became the first successful satellite to gather enough data during its 78 days in space. TIROS was launched on April 1, 1960.

Advances in weather reporting have made it possible for US National Oceanic and Atmospheric Administration (NOAA) to allow real time tracking of weather conditions across oceans such as Atlantic as in Figure 3.15, Central Pacific as in Figure 3.16 and Eastern North Pacific as in Figure 3.17 (NOAA, 2019b). Figure 3.15 reveals a disturbance off the coast of South America, the disturbance is caused by a low atmospheric pressure. Meanwhile, the Central Pacific area (Figure 3.16) reveals the presence of two tropical cyclones or storms; the storm called Erick is off the US Island of Hawaii, and occurred on the date the maps were retrieved, namely August 2, 2019.

Weather satellites in the US has made it possible for news networks to provide real time weather reports during hurricane season. Such reports often feature the hurricane's progress appearing on a large screen beside/behind the weather reporter. The report also features the coastal map of the US where the hurricane is expected to make landfall. A major difference between maps used by news networks and those in Figures 3-15 through 3-17 are colours/graphics. News networks deliberately enhance their maps with eye catching colours/graphics that enhances the plain maps that exists on NOAA website and *www.weather.gov*. Therefore, researchers hoping to see CNN and BBC "graphic" maps on these websites should restrain their expectations to the mostly infrared and water vapor weather maps (NOAA, 2019a).

3.3.2 Step 3: Meteorologists Receive Weather Report

Meteorologists in ground-based stations receive in real time the adverse weather condition spotted by weather satellites. Reported data are analysed and acted upon, for example, Tropical Cyclone Erick that was reported by NOAA satellite to be off the coast of Hawaii led the US National Weather Service to issue flooding alert for Hawaii on August 02, 2019 as in Figure 3-18 (NOAA, 2019c).

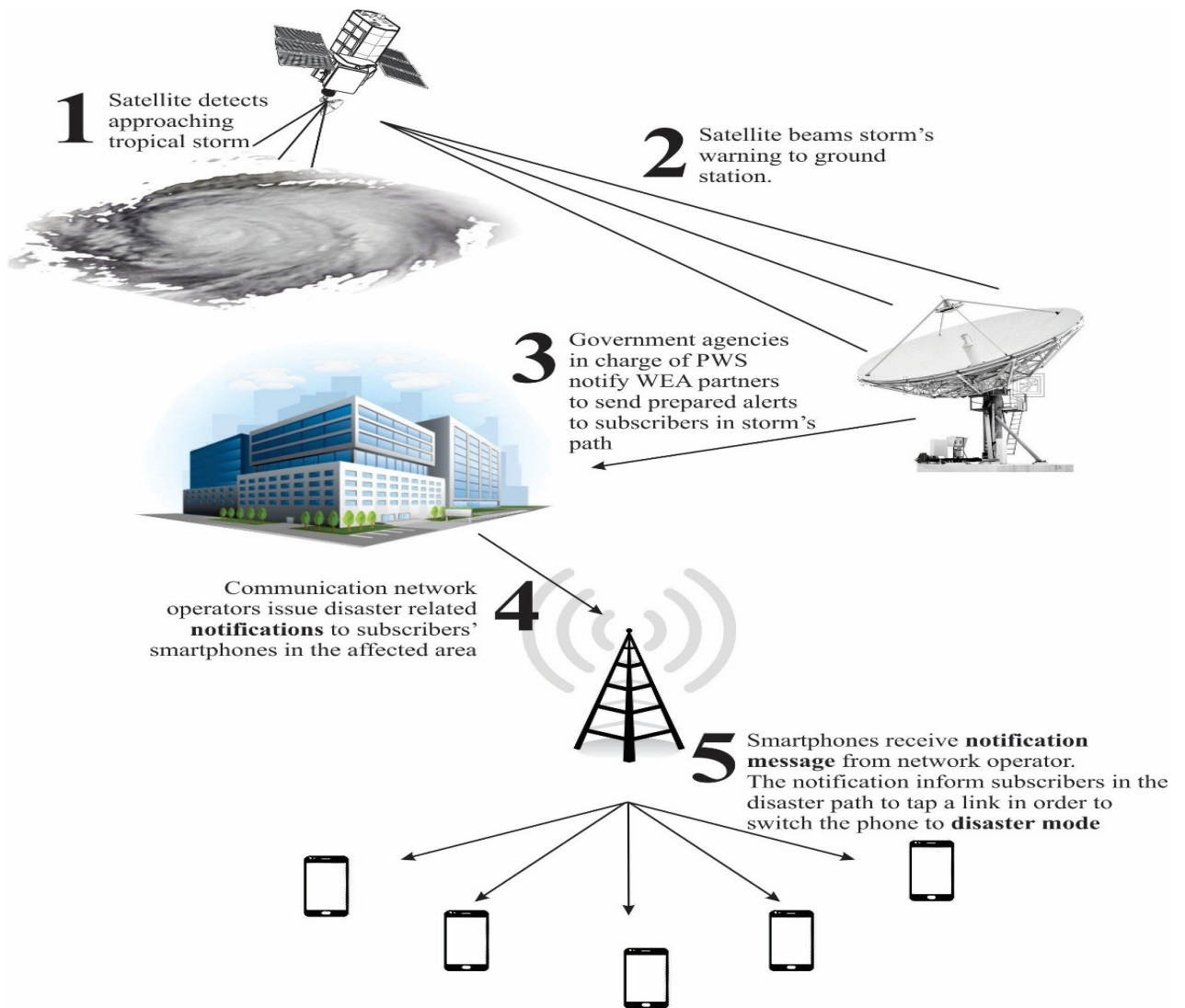


Figure 3-15: Automated Process for Switching Smartphones to Disaster Mode

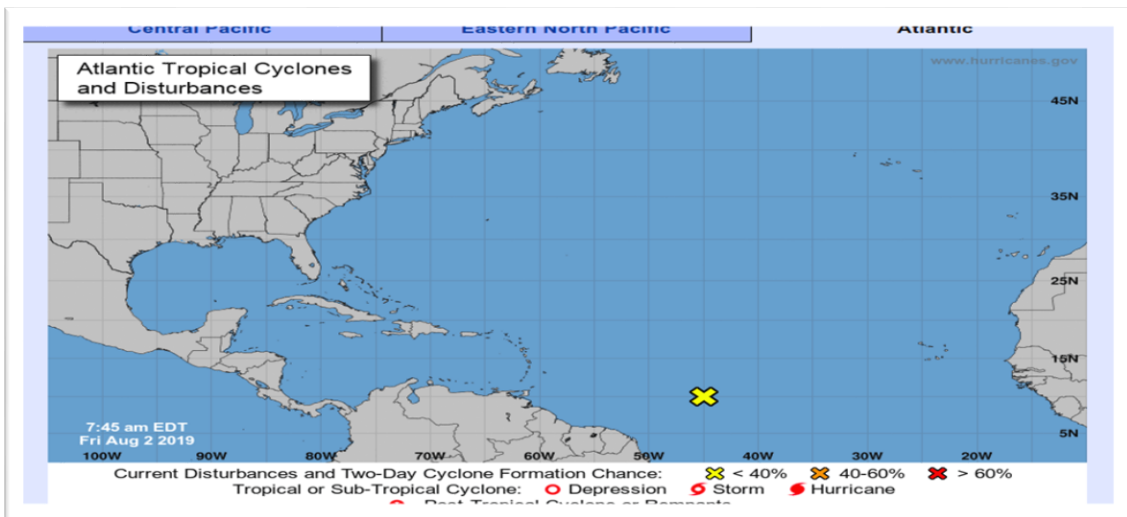


Figure 3-16: NOAA Satellite Tracking the Atlantic Ocean (NOAA, 2019b)

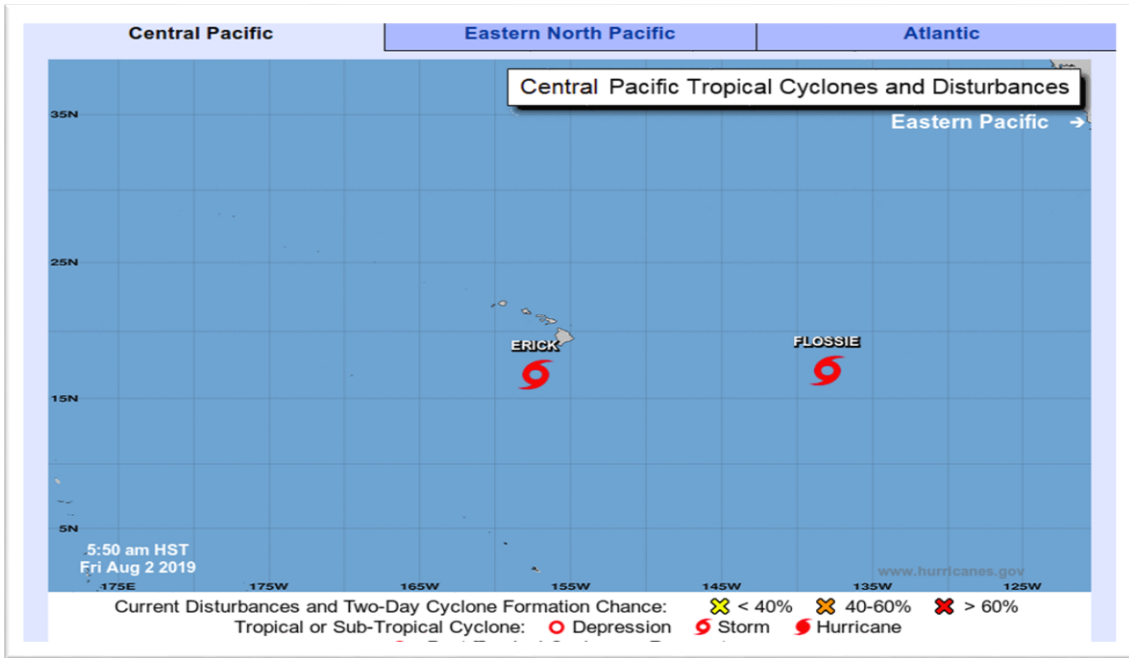


Figure 3-17: NOAA Satellite Tracking the Central Pacific (NOAA, 2019b)

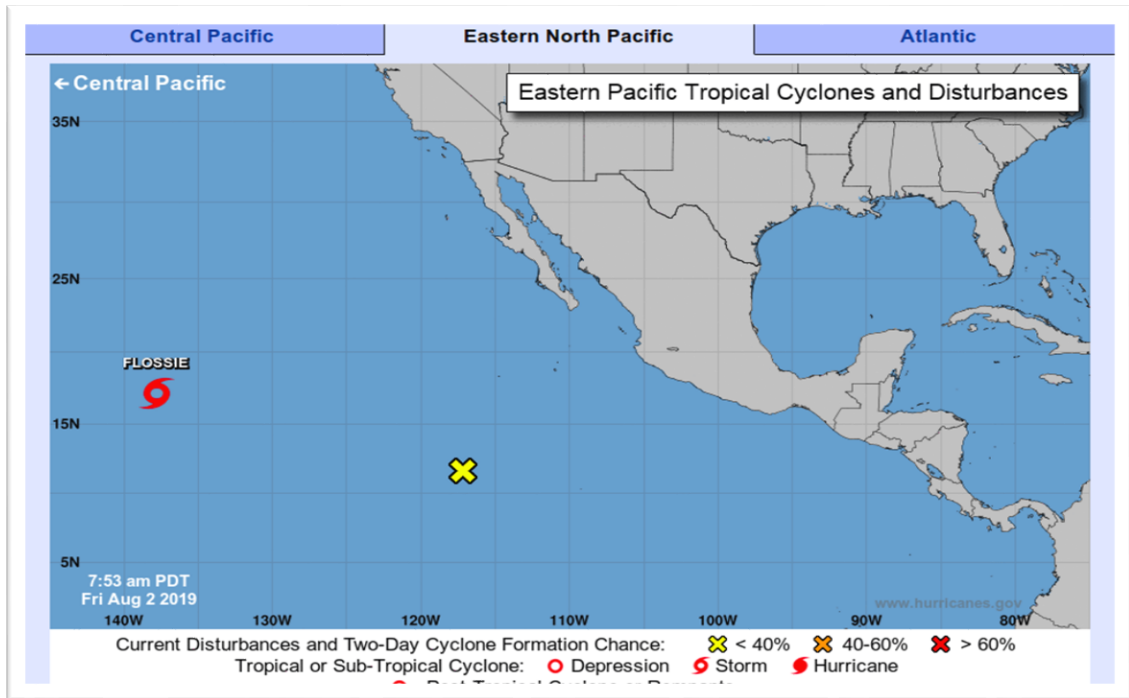


Figure 3-18: NOAA Satellite Tracking the Eastern North Pacific (NOAA, 2019b)

In other words, government agencies in charge of public water system (PWS) notify WEA partners to send prepared alert to subscribers in storm areas.



Figure 3-19: US National Weather Service warning for Hawaii (NOAA, 2019c)

3.3.3 Steps 4 and 5: Mobile Service Providers Send Alert to Subscribers

Although meteorologists do not directly warn cellular communication providers (such as AT&T) about approaching adverse weather condition, nonetheless, such information is made available on their sites or relayed by 24/7 news media (depending on the scope of the oncoming disaster). In the US, the scope of the oncoming disaster equally triggers emergency response from state and Federal Governments, such response includes sending an alert to all mobile subscribers in the path of the incoming weather condition (FCC, 2019). Such alerts are handled via Wireless Emergency Alerts (WEA), which is described by US Federal Communication Commission (FCC) on their frequently asked questions (FAQ) page as: “... a public safety system that allows customers who own certain wireless phones and other compatible mobile devices to receive geographically-targeted, text-like messages alerting them of imminent threats to safety in their area as in Figure 3-19. WEA enables government officials to target emergency alerts to specific geographic areas...” (FCC, 2019).

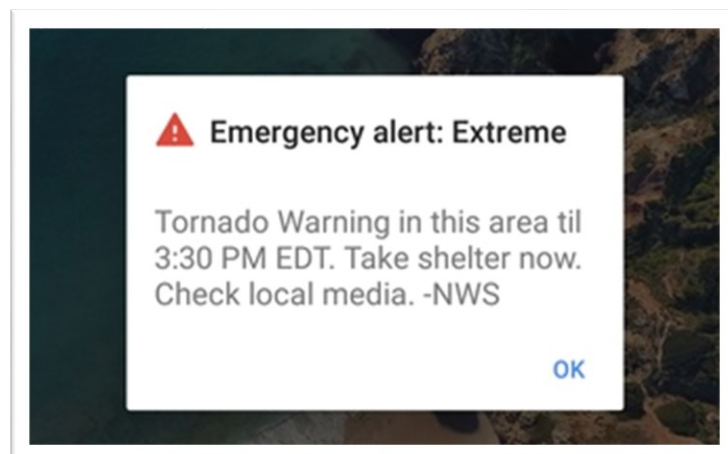


Figure 3-20: Sample WEA message alert. The alert followed by loud alarm (FCC, 2019)

WEA system uses Cell Broadcast Service (CBS) technology to send messages. Al-Dalahmeh, Al-Shamaileh, Aloudat, and Obeidat (2018) and Forum (2019) described this technology as: “... a mobile technology that allows messages (currently of up to 15 pages of up to 93 characters) to be broadcast to all mobile handsets and similar devices within a designated geographical area. The broadcast range can be varied, from a single cell to the entire network. ... Whereas the Short Message Service (SMS) is a one-to-one and one-to-a-few service, Cell Broadcast is one-to-many geographically focused service.” (Forum, 2019).

The CBS is similar to Teletex(UK)/Teletext(US) service offered on television (ETSI, 2019c) (Forum, 2019). Teletex permits a number of unacknowledged messages to be broadcast to all televisions within a particular region and the broadcast appear as pages of information on the television (Roizen, 1981), as TV remotes is used to view each page. Similarly, CBS permits one-way broadcast of CBS messages to multiple *compatible mobile phones* within a geographically or target area as in Figure 3-21. While Teletex messages are sent by TV broadcast stations, CBS messages on the other hand originates from a Cell Broadcast Entity (CBE), a CBE is a messaging application designed for composing SMSCB messaging and for splitting the message into page. Composed SMSCB messages are forwarded by the CBE to the Cell Broadcast Centre (CBC). The CBS parses the message, append serial number to the message and determines the geographical cell towers that will broadcast the message (based on selections made by the message composer) (ETSI, 2019c).

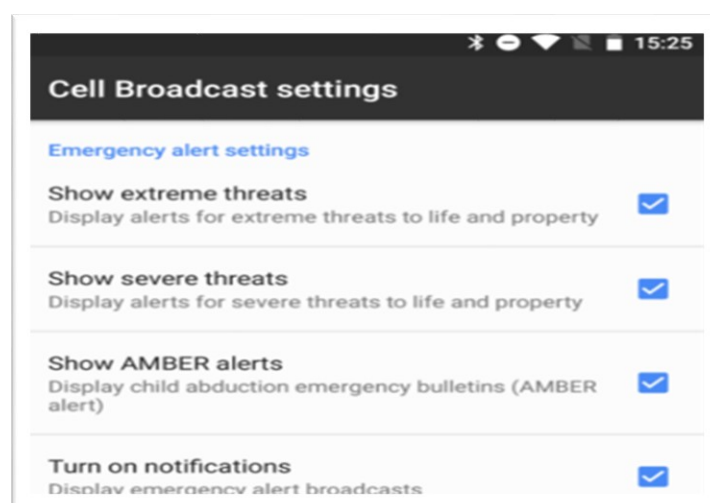


Figure 3-21: Cell broadcast setting in Android 7.1 (Forum, 2019).

As shown in Figure 3.22, If the network type is GSM, then the CBC forwards the message to a Base Station Controller (BS), or a Radio Network Controller (if the network is UMTS/LTE

that is 3G and 4G), both BSC and RNC eventually forwards the message to selected Base Transceiver Stations (BTSs) for broadcast. However, CDMA networks do not follow the CBE > CBC > BSC/RNC flow, rather the CBC forwards the message to a Mobile Switching Station (MSS, which then delivers the message to a BSC/RNC, finally, BSC/RNC delivers the message to selected Base Transceiver Stations (BTSs) for broadcast (One2Many, 2019).

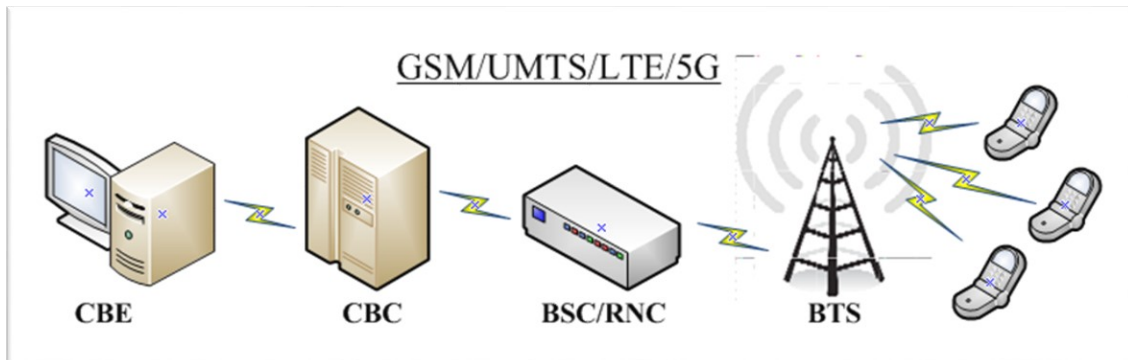


Figure 3-22: CBS message flow in GSM/UMTS/LTE/5G

Short Message Service – Cell Broadcast (SMSCB) is different from Short Message Service-Point to Point (SMS-PP). SMS-PP is from a sender to a recipient (the sender must select the recipient phone number), while SMSCB is from a BTS to multiple recipients within a geographically area (without specifying phone numbers). A major advantage of SMSCB is the ability to target a geographical area using **BTS** in the area to broadcast messages. Thus, emergency messages broadcast from cell towers in a geographically area will be received by phones within the coverage area **as at broadcast time**. SMS-PP on the other hand will deliver alerts using any cell tower to which the targeted phone number is connected to. Thus, users who are frequent travellers will end up receiving alerts outside the disaster zone if SMS-PP is used to deliver WEA.

Several WEA based SMS-CB challenges were identified by Francisco Sánchez, Jr. (The Liaison to the Director and Public Information Officer of Harris County, Texas USA) (Sanchez, 2017), in a letter to the FCC Chairman in 2017, which includes lack of support for multimedia content, capability for two-way interaction with WEA messages, and target geographical area accurately enough to make sure that distinct emergency message is being received by geographically adjacent groups. As a result, the FCC board mandated wireless service providers to improve location aware messaging and add support for multimedia alerts in WEA. This upgrade is scheduled for completion by November 30, 2019 as indicated in FCC letter to

US Cellular network providers (Fowikes, 2019) (Lisa, 2019). However, AT&T and other participants are kicking against the upgrade completion date, calling the upgrade expensive and time consuming, arguments which the FCC Chairman has rejected so far.

This research proposes using Wireless Emergency Alert (WEA) sent via SMSCB to launch DS-OLSR through an embedded link. This approach is similar to embedded links in SMS Point-Point (SMSPP) that launched a website, or an application as presented in Section 4.3.1.

3.4 Chapter Summary

This Chapter presents background research on disasters and networks for disaster recovery and rescue operations highlighting pre and post disaster communication systems. This is because the thesis considered both (pre and post disasters) system for efficient deployment of the proposed disaster network. Overview of disasters and how successful disaster operation depends largely on effective and reliable disaster communication system is presented in Section 3.2. The review of disaster recovery networks based pre and post disaster communication systems is presented in Section 3.3. Pre-disaster communication system is a form of disaster communication system that performs the function of catastrophic warning/signal, advisory and cautionary actions that helps in disaster preparedness and mitigation. However, this research is limited to the use of Wireless Emergency Alert (WEA) technology via Short Message Service Cell Broadcast (SMSCB) to launch DS-OLSR through an embedded link. On the other hand, a post-disaster communication system is a form of disaster communication system that can be configured easily with few steps and effectively supports urgent communication needs for disaster recovery operations. Previous work on different wireless technologies used in designing networks for disaster recovery and rescue operation without restriction on how each technology supports communication needs for disaster recovery operation were successfully analysed. The process for switching smartphone to disaster mode (DS-OLSR) were presented in Section 3.4 with special attention to WEA message technology. Although much research has been carried out on network for disaster recovery and rescue operations. However, only few considered the paramount challenge (Energy) of communication networks in disaster area. Therefore, this research looks forward to the provision of reliable and energy efficient link/device state information across disaster network. The next Chapter presents a novel design for implementation of the energy friendly solutions built upon a modification of OLSR version 1 (OLSRv1).

Chapter 4

Disaster Scenario Optimised Link State Routing Protocol (DS-OLSR) Design

4.1 Introduction

It is important to provide reliable and energy friendly communication network to survivors in the aftermath of a disaster. Simple text message to rescue teams, loved ones, colleagues and business partners reduces anxiety over a trapped victim in a disaster zone. Such messages will allow them to go about their lives with a better mental state. However, provision of a temporary OLSR protocol driven MANETs for survivors to communicate often affects their device battery energy, since message routing and network flooding are prominent requirements of OLSR protocol. For this reason, the proposed DS-OLSR design attempts to presents the modification of conventional OLSR protocol to minimise energy consumption and routing overhead of OLSR nodes for effective communication during disaster recovery and rescue operations.

This Chapter started with the presentation of the DS-OLSR design assumptions in Section 4.2. The process of switching smart phones to disaster mode is discussed in Section 4.3. Section 4.4 presents IP Address, battery, and phone number generation scheme for DS-OLSR. DS-OLSR Time Slices and their respective messages are presented in Section 4.5 and 4.6, respectively. Section 4.7 discusses how DS-OLSR handles nodes that attempt to join the network after Network Formation Time Slice (NFTS). Proposed Disaster Management Server is in Section 4.8. A simple approach for handling network partition is presented in Section 4.9 while Section 4.10 discusses DS-OLSR and DS-OLSRMP packet format and forwarding process. Section 4.11 describes DS-OLSR and DS-OLSRMP repositories. Section 4.12 and 4.13 describes Alert and Shhh messages, respectively. Modification of Hello and TC messages are discussed in Section 4.14 and Section 4.15 wraps up the Chapter with summary.

4.2 Design Assumptions of the Proposed DS-OLSR

To this research, the following assumptions are regarded as factual:

1. Each victim has one or more smart phones with Wi-Fi capability.
2. Each smart phone is running an instance of DS-OLSR service.

3. Each smart phone has DS-OLSR compliant messaging app that can send and receive messages by extracting Contact List created by DS-OLSR.
4. Cellular communication towers and power lines were destroyed; hence victims cannot communicate with one another and with RT, and neither can they recharge their mobile devices.

Consequently, this research proposes the following modification for energy friendly communication network during disaster recovery and rescue operations:

1. Redesigned OLSR packet header through the addition of a new field, namely Originator ID (device’s phone number) as in Table 4-1. The introduction of Originator ID provides human readable device information across the network, allowing victims to recognise the sources of their messages and in case of availability of internet connection, it will be used by the victims to send and receive messages. It equally leads to the elimination of OLSR multiple interface declaration (MID) messages.

Table 4-1: Redesigned OLSR Packet Header

0					1					2					3																
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Packet Length										Packet Sequence Number																					
Message Type					Vtime					Message Size																					
Originator Address																															
Originator ID																															
Time to Live					Hop Count					Message Sequence Number																					
MESSAGE																															
Message Type					Vtime					Message Size																					
Originator Address																															
Originator ID																															
Time to Live					Hop Count					Message Sequence Number																					
MESSAGE																															

2. The research reduces routing overhead by encapsulating HELLO, Topology Control (TC) and Host Network Association (HNA) messages within their respective Time Slices (TS). Thus, these broadcasts can only happen during their TSs.
3. Added two data sets namely, Deviceinfor and Contact Sets.

4. Modification of 1-hop and 2-hops data sets by including two additional fields, namely PHONE_NO and BATTERY_LEVEL.
5. Added a new message type called ALERT message to enable GSM 0.3.3.8 (ETSI, 2019a) encoded SMS communication.
6. Finally, the research uses “information exchange” between the routing protocol and a frontend messaging application. The proposed approach involves both applications having shared access to “information bases” or “data sets”. For example, the frontend messaging application extracts/generate the device IP address, phone number (originator ID) and Battery life. The extracted/generated info are saved into a “Deviceinfo Set”. This set will be readable by the routing protocol. In the same vein, the messaging frontend application will be able to read relevant routing table information generated by DS-OLSR (such as neighbourhood and network sets) which stores the originator ID (phone numbers) of RT and reachable neighbours.

4.3 Disaster Mode Process in Smartphones

Natural and artificial human-made) disasters have been steadily increasing all over the world, making it significant in providing reliable and energy friendly communication network to survivors in the aftermath of a disaster. However, the ability to quickly report such incidence can save lives, properties, and communities. Thus, over the years, emergency numbers were incorporated into telephony systems, this permitted callers in an emergency to dial the emergency number specific to their country. Smartphones extended the system by allowing victims to dial emergency numbers even when the phone is locked. Unfortunately, emergency numbers require cellular infrastructure, hence they are unavailable when such infrastructures are crippled by disasters. Therefore, it becomes imperative to provide a mechanism which would automatically trigger disaster mode on subscribers’ mobile devices and preserve their ability to contact rescue workers for help. The process of switching smartphone to the disaster mode is presented in the following Subsections.

4.3.1 Launching DS-OLSR through an embedded link

As mentioned in Section 3.4.3, this research proposes the use of Wireless Emergency Alert (WEA) via Short Message Service Cell Broadcast (SMSCB) to launch DS-OLSR through an embedded link. This approach is like embedded links in Short Message Point-to-Point

(SMSPP) that launches a website or an application. However, this can only be done if the Cell Broadcast Entity (CBE) is modified to permit embedding software links in the SMSCB emergency alert message.

4.3.1.1 Proposed modification to Cell Broadcast Entity (CBE) Messaging Application

As started earlier, this research proposes some modification to Cell Broadcast Entity (CBE) application that would allow emergency message initiators to add a link to the Cell Broadcast Centre (CBC) message that would launch DS-OLSR service as in algorithm 4.1.

Algorithm 4.1: CBE (Composing and Sending Application)

- 1: Begin:**
 - 2: Generate Message ID**
 - 3: Type and Format Notification Message**
 - 4: Get Notification Language**
 - 5: 1 = English**
 - 6: 2 = Portuguese**
 - 7: 3 = Spanish**
 - 8: Get Notification Action**
 - 9: 1 = Launch DS-OLSR**
 - 10: 2 = Do Nothing**
 - 11: Get Broadcast State**
 - 12: 1 = All**
 - 13: 2 = Rio de Janeiro**
 - 14: 3 = São Paulo**
 - 15: 4 = Minas Gerais**
 - 16: Get Broadcast Municipalities**
 - 17: 1 = All**
 - 18: 2 = List Municipalities from selected States**
 - 19: Get Broadcast Cities/Towns**
 - 20: 1 = All**
 - 21: 2 = List Towns from selected county**
 - 22: Get Broadcast Cell/BTS List**
 - 23: 1 = All**
 - 24: 2 = List Cells/BTSs from selected State and Town**
 - 25: Get Broadcast Duration**
 - 26: 1 = 24 hours**
 - 27: 2 = 48 hours**
 - 28: 3 = Custom (Get custom value from input device)**
 - 29: Get Broadcast repeat interval**
 - 30: 1 = 3 hours**
 - 31: 2 = 5 hours**
 - 32: 3 = Custom (Get custom value from input device)**
 - 33: Send Message to CBC**
 - 34: End**
-

The algorithm assumes radios on BTSs are configured based on their geographical and spread by States, Counties, and Towns. It equally proposes using **Notification Action** to determine if the SMSCB should include the link or not. It commences by typing of the notification alert message by an authorized staff. The staff is expected to select the notification action which the alert is expected to trigger on recipient's phones. Thus, a notification alert with message type 2 will not display any link. However, nonfiction alerts with message type 1 displays a link that the user can tap to launch DS-OLSR (see Algorithm 4.1).

4.3.1.2 Processing Links in Android

A sample of WEA message with link to launch DS-OLSR application is shown in Figure 4.1. The link starts with the app name: **dsolsr://**, this can be changed to **ds://**, or **app://**, the point is in Android as shown in Code Snippet 1, a developer can create a scheme to associate with the application (Android, 2019).

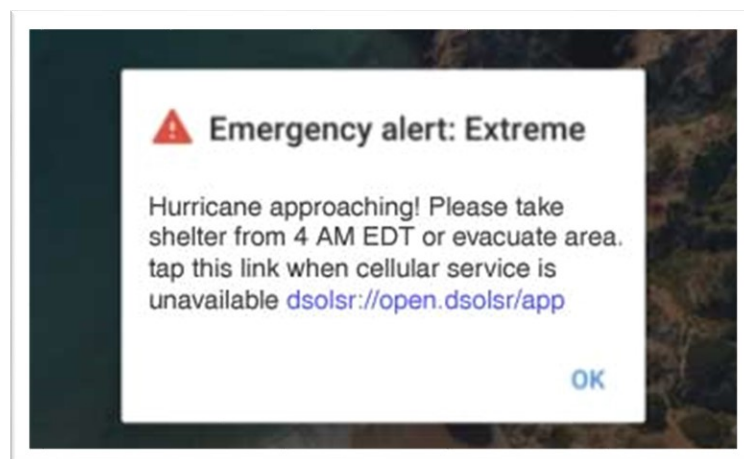


Figure 4-1: Sample WEA message alert with link to lunch DS-OLSR application.

Android Code Snippet 1: Launching DS-OLSR on Android Phones

```
<activity
  android:name="com.dsolsr.android.HaidarActivity"
  android:label="@string/title_dsolsr" >
  <intent-filter android:label="@string/filter_dsolsr_service_haidar">
    <action android:name="android.intent.action.VIEW" />
    <category android:name="android.intent.category.DEFAULT" />
    <category android:name="android.intent.category.LAUNCHER" />
    <data android:scheme="dsolsr"
      android:host="www.dsolsr.com"
      android:pathPrefix="/app" />
  </intent-filter>
</activity>
```

Such alerts will include instructions as to when and why a phone should be switched to disaster mode. The primary reason being the conservation of device's energy and connectivity to the disaster network. However, mobile operating system providers do not necessarily grant application developers direct access to cellular antenna, hence permission should be sought to gain access to cellular antenna functions without rooting the smartphone. The link processing code can be easily adapted on other mobile phones operating system such as IOS, windows etc.

4.3.1.3 Switching Mobile Phone to Disaster Mode

Subscribers who receive the notification simply tap the embedded link to switch their devices to disaster mode by launching DR-OSLR application. This application is responsible for initiating the entire DS-OLSR services. Once the DS-OLSR application starts, it checks the availability of cellular network, hence it displays message and exit if the network is available. However, if the cellular signal is unavailable, then it disables Bluetooth and Cellular network, then enables DS-OLSR messenger as in Algorithm 4.2, which in turn launches DS-OLSR routing service. It is important to prevent users from launching DS-OLSR while cellular signal exists since the availability of cellular signal implies communication infrastructure within the community is unaffected, and of course RT will prefer to use available cellular network for search and rescue operations.

Algorithm 4.2: Switching Mobile Phone to Disaster Mode

```

1: Begin:
2: Check cellular signal level
3: SignalLevel = get.OSTelephony.SignalStrength.getLevel()
4: If (signalLevel > 0)
5:     Alert ("You can still initiate and receive calls/messages")
6:     Exit
7: Else
8:     device.BluthoothAdapter.enable() = 0
9:     device.CellularAdapter.enable() = 0
10:    DS-OLSR.Message.enable = 1
11: Endif
12: End

```

4.3.2 Manual Mechanism for Switching Smartphones to Disaster Mode

In this section, the research examines the possibility of certain subscribers missing the notification alert sent by mobile network providers and proposed the used of Unstructured Supplementary Service Data (USSD), sometimes referred to as short code to enable such victims to switch their devices to disaster mode (DM). For example, some travellers on their

way to a disaster zone most likely would have not received the localized notification alert sent earlier to the disaster area (ETSI, 2019b). In addition, some locals within the disaster zone may miss the alert if their mobile devices are switched off (Al-Dalahmeh et al., 2018). Hence this research proposes using a short code to trigger disaster mode in such scenario.

USSD or Short codes are either network operator specific (for example codes provided by service providers to enable subscribers to check their account balance such as *556#), operating system specific (for example code to retrieve a device's IMEI number – such as *#06#) or application specific. Thus, short codes are either interpreted as typed or sent to mobile network operator for interpretation. A typical short code is made of hash (#) signs, asterisks (*) and numbers. Therefore, the research proposes using application specific code such as: ***##26072019.##***. Typing ***##26072019##*** will run the Android code snippet code 1 and initiate the process of launching DS-OLSR messenger as described in Algorithm 4.2.

Algorithm 4.3: Retrieve and Save Battery life and Phone Number

1: Begin:
2: Read NetworkInfo of Device
3: Read BatteryInfo of Device
4: Get TelephonyInfo of Device
5: Ipaddress = NetworkInfo(Wi-Fi)
6: BatteryLevel = BatteryInfo(getRemainingEnergy)
7: PhoneNo = TelephonyInfo(getPhoneNumber)
8:
9: Else
10: Save BatteryLevel, and PhoneNo to deviceinfo file
11: End If
12: End

Algorithm 4.3 displays the process of retrieving device's phone number and Battery life. This information is saved in a DS-OLSR devcieinfo file. It is imperative for the algorithm to execute before launching DS-OLSR service, else DS-OLSR will simply terminate if it is unable to locate its network configuration file. Thus, the algorithm will be coded and embedded in DS-OLSR Messenger, which is equally responsible for retrieving and storing both device's Battery life and phone numbers.

4.4 Internet Protocol (IP) Address Generation for DS-OLSR Devices

Several methods for generating IP addresses for MANETs exists and are divided into stateful (Günes & Reibel, 2002) (Nesargi & Prakash, 2002) (H. Zhou, Ni, & Mutka, 2003) (Mohsin & Prakash, 2002) and stateless (Perkins, 2000) (Vaidya, 2002) (Weniger, 2003) (Jeong, Cha,

Park, & Kim, 2003). Stateful address allocation requires nodes charged with allocating IP addresses to maintain an IP allocation table listing used and unused IP addresses. A major challenge facing stateful IP address allocation is the seamless management of the allocation table, which requires multiple energy dissipating flooding of the entire network with IP allocation status. These challenges far outweigh the benefit, which is a network without a single duplicate IP address. On the other hand, Stateless allocation allows each device to assign an IP address to itself, thereafter each device performs a network wide check to ensure a duplicate of its chosen IP address do not exist in the network. The initial simplicity of self-generated IP addresses is lost since the device must flood the network in order to detect a duplicate IP address. The art of flooding the network in a bid to detect duplicate IP addresses could happen repeatedly. Thus, a device will regenerate a new IP address and flood the network with duplicate detecting messages again and again until no duplicate is found.

Both stateful and stateless IP address allocation mechanism flood the network repeatedly with energy dissipating messages (which is inimical to disaster victims' phone). Therefore, this research considered IPv6 for seamless and conflict free IP generation. This has been achieved using IPv6 Model Library of NS-3 (Ns-3, 2021).

4.5 DS-OLSR Time Slices

Time slices are designed to reduce overhead and message collision in DS-OLSR. Message collision occurs when a TC message broadcast from node A synchronizes with a Hello message broadcast from node B. in other words, when messages become synchronize or coordinated, for example, a node may wish to report a change in its set of MPR via HELLO message, which may trigger a network control message (TC message) in a set of neighbouring nodes. This will lead to collision since the receiving node is already busy with the HELLO message This situation causes a race condition leading to energy consumption without delivering any routing results.

DS-OLSR messages are categorized into four Time Slices (TSs), these are:

1. Network Formation Time Slice (NFTS)
2. Topology Propagation Time Slice (TPTS)
3. Message Time Slice (MTS)
4. Network Sleep Period (NSP)

The diagrammatical representation of the DS-OLSR Time Slices is presented in Figure 4-2 and the various Time Slices are discussed in the following sections:

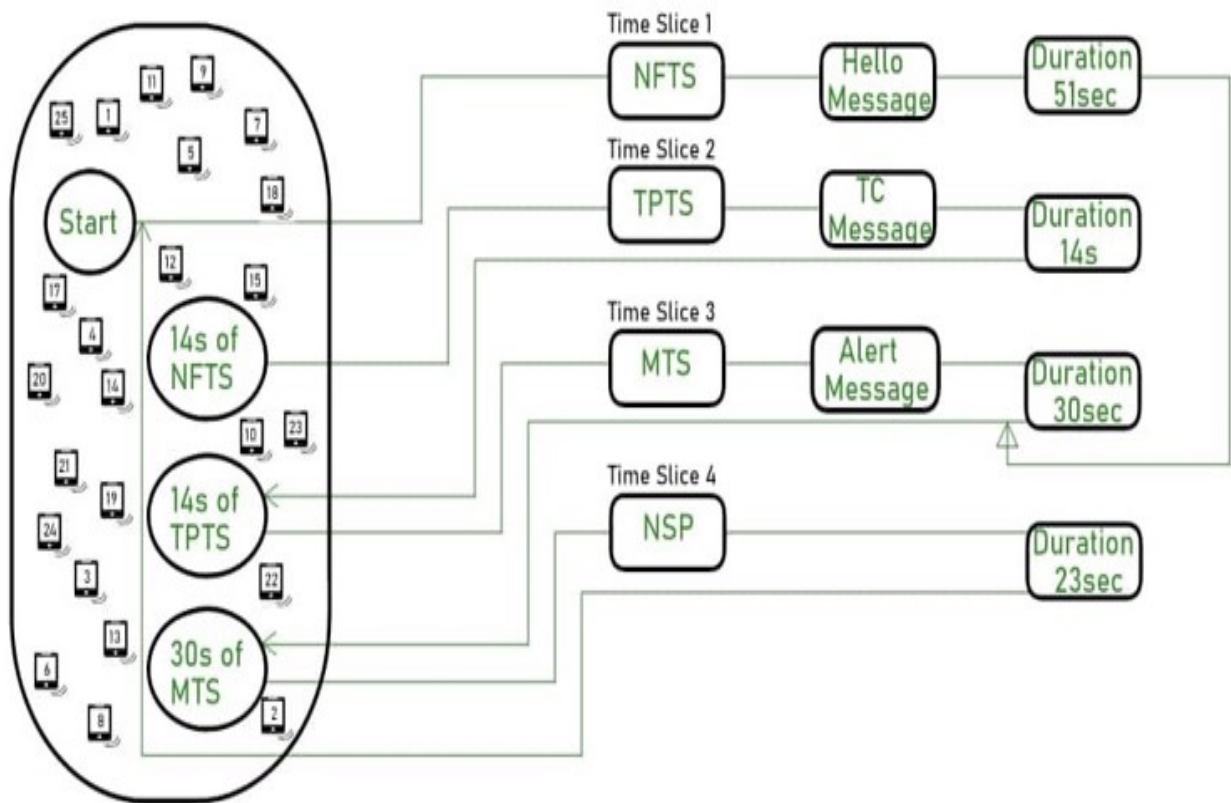


Figure 4-2: Diagrammatical Representation of DS-OLSR Time Slices System

4.5.1 Network Formation Time Slice (NFTS)

The Network Formation Time Slice (NFTS) controls access to the disaster MANET by preventing new nodes from automatically joining the MANET (as obtained in both OLSRv1 and OLSRv2). Thus, a new node wishing to join the network will not commence by broadcasting HELLO messages. However, it sleeps for a while, then scan the network to identify the current TS. The node will only connect to the network if the message it receives during the current TS is Hello message.

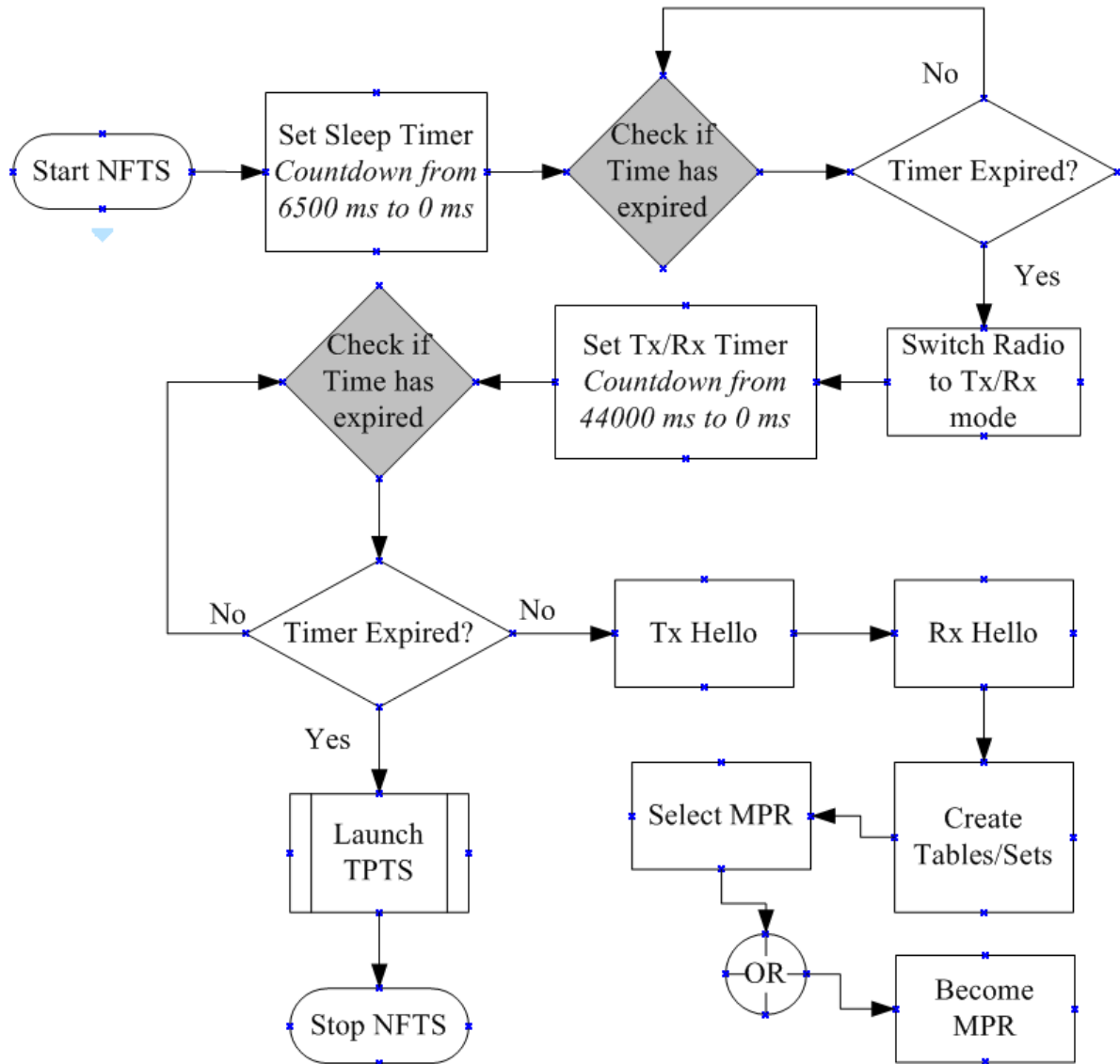


Figure 4-3: NFTS: Message and Duration

Hello message is the only permissible message during NFTS. This process is presented in Figure 4.3. The flowchart depicts NFTS and Hello message implementation with the duration of 14 second. Two timers are used during NFTS, the first timer lasts 6500 ms as the remaining 500 ms allow the radio to switch to transmit and receive mode (making a total of 7000 ms). Thereafter the timer that controls the duration of Hello messages and related process (shortest path computation, MPR selection, table creation etc.) commences. The expiration of NFTS launches Topology Propagation Time Slices (TPTS) as discussed in the following sub-section.

4.5.2 Topology Propagation Time Slice (TPTS)

The Topology Propagation Time Slice (TPTS) takes over from NFTS as it permits nodes to broadcast and receive both HNA and TC messages. The flowchart in Figure 4.4 depicts processes of the TPTS. The TPTS uses two timers namely: TC and HNA Timers that used in broadcasting TC and HNA messages, respectively. Each timer lasts 7000ms accruing 14 seconds as the total duration of TPTS. The timers are independent periods for sending (Tx) and receiving (Rx) TC and HNA messages. Each process checks the timer every 1ms for expiration. However, the execution of the TS ceases once timer expires and it trigger the commencement of next TS (Message Time Slice).

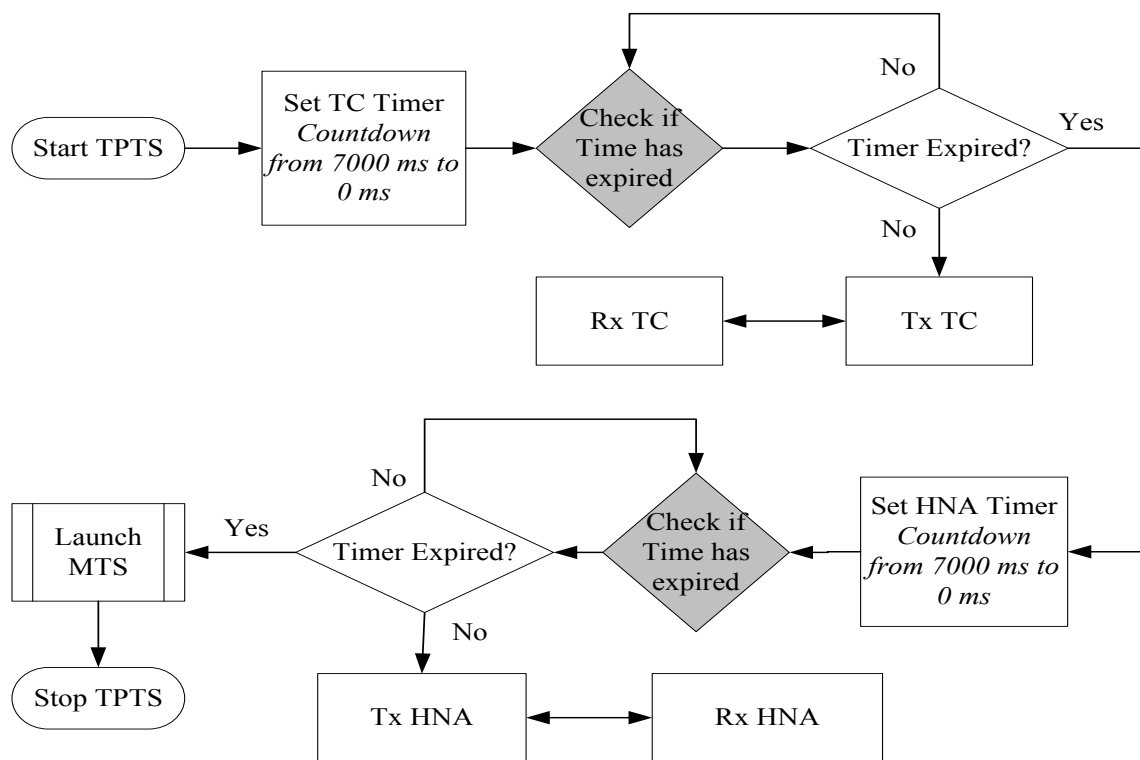


Figure 4-4: TPTS: Message and Duration

4.5.3 Message Time Slice (MTS)

The Message Time Slice (MTS) commences after TPTS, which allow nodes to send and receive ALERT messages, the MTS process as in Figure 4.5 has the longest timer amongst DS-OLSR Time Slices as it lasts for 30000ms. The timer is deliberately configured to allow enough possible time to send and receive messages. Network Sleep Period (NSP) process is launched as soon as MTS timer expires.

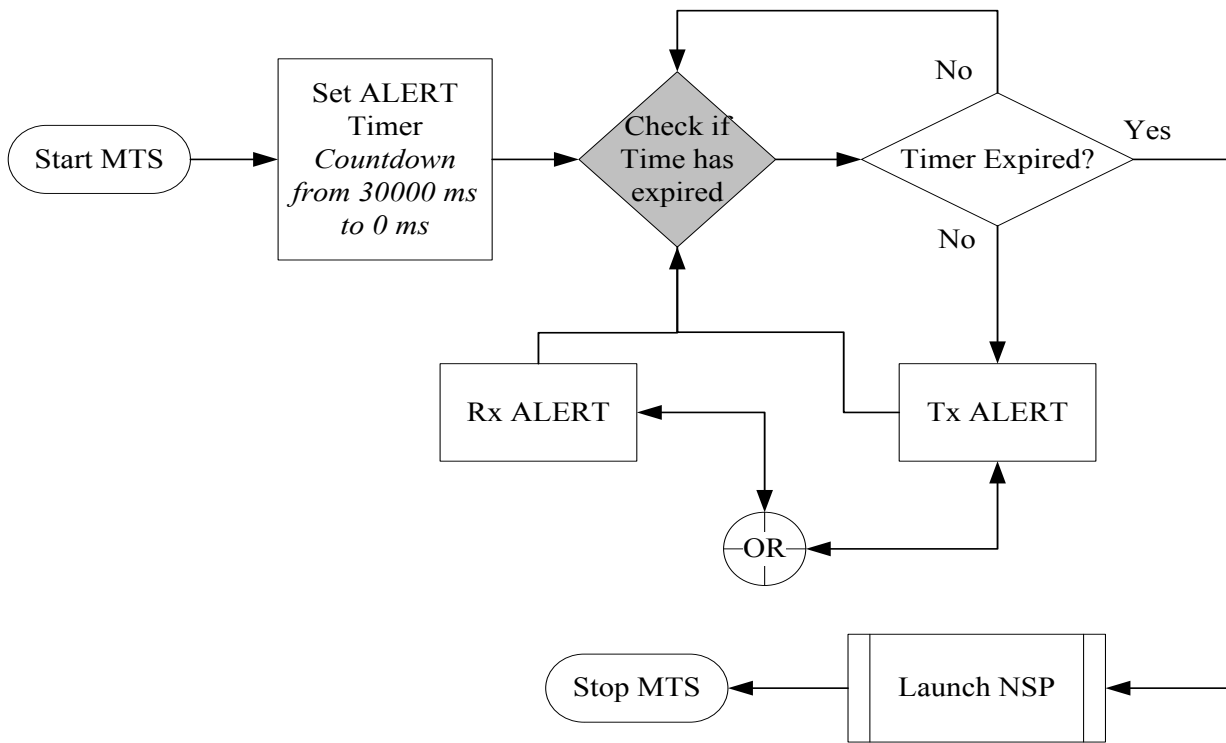


Figure 4-5: MTS: Message and Duration

4.5.4 Network Sleep Period (NSP)

The final TS is the NSP, this period conserves network energy by forcing nodes to switch their transceivers to sleep mode for extended periods. Thereafter the process activates NTFS. NSP process as in Figure 4.6 uses the second longest timer in DS-OLSR time slices.

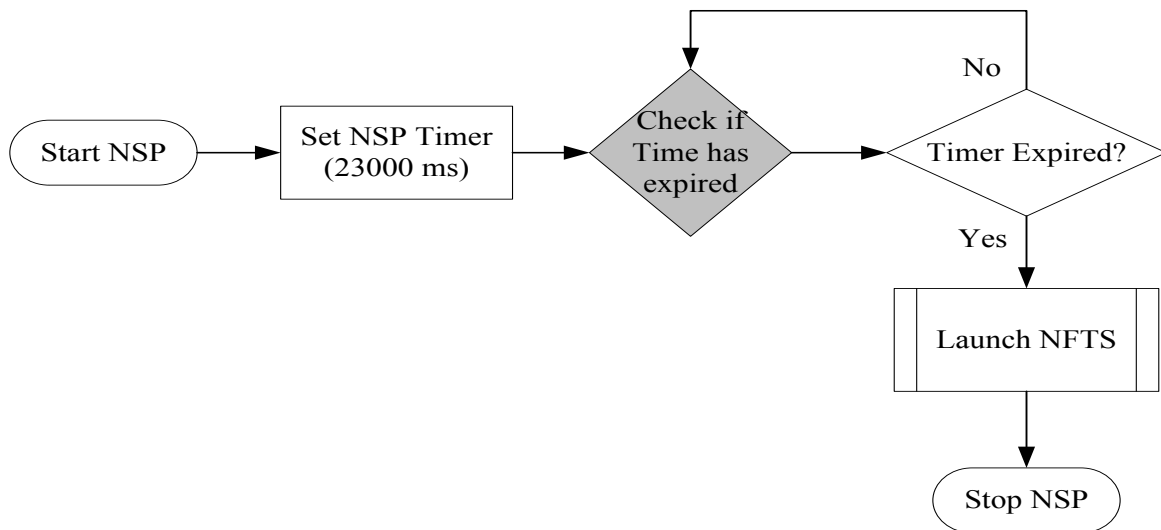


Figure 4-6: NSP: Message and Duration

The timer lasts 23000ms during which every device that went through the three TSs power down their radio to sleep mode. NFTS cycle is restarted as soon as NSP timer expires.

4.5.5 Time Slice Duration

Each device/node activates a system timer during each TS. The value of each timer is the product of the total TS in milliseconds. The various Time Slices with their corresponded messages and durations are presented in Table 4.2. The final TS (MTS) is followed by 23 seconds of MANET-wide sleep. This period is known as Network Sleep Period (NSP) and it is immediately followed by 7 seconds of NFTS sleep mode, aggregating the total to 30 seconds of MANET wide sleep. However, this TSs duration is used as example and recommended by this research as it strike balance between battery conservation and message delivery. Thus, longer TSs will affect the ability of victims and rescuers to rapidly exchange messages.

$$Time_{ms} = 1000 \quad (4-1)$$

$$TS_{NFTS} = Time_{ms} \times 58 = 58000 \text{ ms} \quad (4-2)$$

$$TS_{TPTS} = Time_{ms} \times 14 = 14000 \text{ ms} \quad (4-3)$$

$$TS_{MTS} = Time_{ms} \times 30 = 30000 \text{ ms} \quad (4-4)$$

$$NSP = Time_{ms} \times 23 = 23000 \text{ ms} \quad (4-5)$$

The TS period cease to exist immediately after the timer expires, this automatically triggers the next TS. However different nodes use different timers as shown is Table 4.2.

Table 4-2: DS-OLSR Time Slices, messages and duration

Time Slice	Nodes	Mode	Duration (Seconds)
Network Formation Time Slice (NFTS)	All	Sleep	7
	All	Tx / Idle Rx	51
Topology Propagation Time Slice (TPTS)	MPRs	Tx / Idle Rx	7
	MPRS/GATEWAY (HNA node)	Tx / Idle Rx	7
	Other nodes	Idle Rx	14
Message Time Slice (MTS)	All	Tx / Idle Rx	30

4.6 DS-OLSR and DS-OLSRMP Messages

DS-OLSR and DS-OLSRMP messages are grouped into Time Slices (TSs) and each TS has a specific messages and duration as presented in Table 4-3. The first TS for any device joining the network is the Network Formation Time Slice (NFTS). This TS has the duration of 51 seconds, whereby first 7 seconds, (actually, 6.5 seconds) of NFTS spent in sleep mode (the remaining 0.5 seconds is used to switch the transceiver to Tx mode). This is important in a disaster zone where new nodes join the network intermittently, thus maintaining absolute radio silence prevent new nodes from interfering with ongoing communication. The remaining 44 seconds is dedicated to broadcasting messages permitted during NFTS and it is broadcasted every 1 seconds. The only message permitted during the NFTS is Hello message, thus each device broadcast their respective Hello messages and identify their 1-hop and 2-hops neighbours. Each node ceases from broadcasting the Hello messages at expiry of NFTS, thereafter the entire network switches to low power listening mode (idle mode) allowing selected MPRs to broadcast their electors in the next TS. NFTS launches the next TS before exiting.

The NFTS is closely followed by Topology Propagation Time Slice (TPTS) which permits the propagation of TC and HNA messages only. MPRs propagates both HNA and TC messages across the network. The TPTS related messages come to an end after 14 seconds, in which 7 seconds for TC messages and the remaining 7 seconds for HNA messages. The message broadcast occurs every 5 seconds. The expiration of TPTS trigger the commencement of Message Time Slice.

The Message Time Slice (MTS) allow the transmission of SMS encoded messages from the sender to recipients within or outside the MANET. SMS encoded messages meant for loved ones outside the disaster zone are handled by the Disaster Management Server (DMS). The DMS routes these messages via Internet SMS gateways, using http/https links of the Internet SMS service provider. A total of 30 seconds is allocated for MTS messages.

MTS launches the network sleep period (NSP) upon timer expiration. As mentioned earlier, this period commences a MANET-wide powering down of node to sleep mode for 23 seconds to conserve energy and proceed to NFTS sleep period making the total of 30 seconds of entire MANET sleep period.

Table 4-3: DS-OLSR Time Slices, Messages and Duration

Time Slice	Message	Duration (Seconds)
Network Formation Time Slice (NFTS)	Sleep mode	7
	Hello	51
Total		58
Topology Propagation Time Slice (TPTS)	TC	7
	HNA	7
Total		14
Message Time Slice (MTS)	ALERT	30
Total		30

4.7 Handling New Devices/Nodes

DS-OLSR and DS-OLSRMP proposes two ways of handling nodes that attempt to join network after NFTS as follows:

First Approach: Any node that receives “Hello message” from a new node will broadcast a “Shhh message” to the node as discussed in Section 4.13. This message will contain the current TS along with current timer counter value. This would enable the new node to configure its’ own timer against the next NFTS cycle. A major disadvantage of this approach is that nodes break from their normal operations to attend to the late comer.

Second Approach: The second approach (adopted by DR-OLSR and DS-OLSRMP) prevents the node from sending any message, rather the new node listens periodically until it detects a HELLO message. To conserve energy, the new node switches to sleep mode periodically, this continues until it receives a response. Sleep periods for devices that wish to join the DS-OLSR and DS-OLSRMP MANET is computed as follows:

$$Sleep_Duration_{node} = Seconds_{NFTS} \div 2 \quad (4-6)$$

4.8 Proposed Disaster Management Server (DMS)

The Disaster Management Server (DMS) permit DS-OLSR/DS-OLSRMP devices to send SMS messages to recipients outside the disaster zone via internet SMS aggregator. The following sub-section outline the minimum specification requirement of the DMS.

4.8.1 Hardware Requirement

1. Minimum of Intel Corei2 motherboard (a Corei2 can easily run Linux OS, which in turn can run olsrd, a software implementation of OLSRv1).
2. Two network interfaces: USB/Wired Ethernet and wireless. The wireless interface will act as the DS-OLSR interface, while the USB/Wired Ethernet interface will act as the gateway to the Internet.
3. Any Internet connectivity method is permitted provided it can connect via wired or Ethernet.

4.8.2 Operating System

1. Any operating system that can execute OLSRv1(olsrd) (Andreas et al., 2017b) code can equally execute the proposed code for DS-OLSR and DS-OLSRMP code since it is derived from OLSRv1. However, current source codes for olsrd are optimized for compilation and execution on Android and Linux operating systems (Andreas et al., 2017b). Figure 4-17 displays a screen capture from a portion of olsrd readme file showing olsrd compilation status per operating system.

COMPONENT/OS	Linux	Win32	FreeBSD	NetBSD	OpenBSD	OSX
olsrd	++	++	++	++	++	?
olsr_switch	++	++	++	++	++	?
PLUGINS						
bmf	++	+/?	++	++	++	-
dot_draw	++	+/?	++	++	++	++
dyn_gw	++	+/?	+/-	+/-	+/-	++
dyn_gw_plain	++	+/?	+/-	+/-	+/-	++
httpinfo	++	++	++	++	++	++
mini	++	+/?	++	++	++	++
nameservice	++	+/?	++	++	++	++
pgraph	++	++	++	++	++	++
quagga	++	-/-	++	++	++	?
secure	++	++	++	++	++	++
txtinfo	++	++	++	++	++	++

LEGEND: ++ = compiles/runs
+/- = compiles/does not work
- = does not compile
? = unknown

Figure 4-7: Operating System support of olsrd (Andreas et al., 2017a).

The Figure revealed the fact that olsrd components/service (olsrd and OLSR _ switch) easily compiles under Linux, Windows (32 bits), FreeBSD, NetBSD, and OpenBSD. However, the

compilation status for Apple OSX is unknown. While olsrd component/service enjoys a compilation success ratio of 5:6, the same cannot be said of olsrd plugins. Only Linux operating system supported all 11 olsrd plugins followed by FreeBSD/NetBSD/OpenBSD/OSX with a support ratio of 8:11, Windows (32 bits) has the lowest support ratio of 4:11. As a result, this research proposed the used of Linux as an operating system for the DS-OLSR.

OLSRd is a software implementation of OLSR protocol that is optimized for Mobile ad hoc networks. It is designed to run multiple devices, such as commercial of the shelf routers, smartphones, or normal computers. Olsrd executes as a service on host computers and attaches itself to the OLSR port (698). OLSR_switch on the other hand is an application that contains a set of commands that can be used to launch olsrd service. The application is a traffic router that will allow multiple olsrd instances to connect and communicate over TCP via the loopback interface.

2. The operating system MUST NOT share the Internet interface with the DS-OLSR and DS-OLSRMP network as this would quickly overwhelm the MANET since various applications on victim's smartphone will compete to connect to the Internet.

4.8.3 Database Management System

DS-OLSR and DS-OLSRMP proposed the used of SQLite to create and manage DS-OLSR and DS-OLSRMP tables. SQLite is a small, fast, self-contained, high-reliability and full-featured SQL database engine (SQLite, 2019). It is the most used database engine in the world which is built into all mobile phones and most computers, and it is equally bundled with countless other applications that people use every day (SQLite, 2019). The database management system for DS-OLSR and DS-OLSRMP will contain an SQLite database with the following Tables:

Victims Table

This Table MUST contain fields that will uniquely identify each victim's device in the network. Important fields are PHONE_NO, Allocated_IP, MP_Relay, Network_Assignment and BATTERY_LEVEL.

1. PHONE_NO field identifies the victim's phone number.
2. Allocated_IP identifies the main address of victim's smartphone.

3. MP_Relay identifies the MRs used by victim's device to route messages, this information is used by the DMS to deliver ALERT messages to victims.
4. Network_Assignment identifies the service rendered by a device to the DS-OLSR network. Recommended values are NONE if no service is offered and MPR if the device is an MPR. This information allows RT to identify critical nodes in the network and monitor their Battery life for offloading.
5. BATTERY_LEVEL identifies the Battery life of each smartphone in the network. The BATTERY_LEVEL along with the network_assignment enable RT to plan service offloading when rescuing victims whose phones act as GR as in section 4.9.4.

SMS Table

This table contains SMS sent by victims. The following fields are IMPORTANT: PHONE_NO, Allocated_IP, MP_Relay, message, destination, and status.

1. PHONE_NO field identifies the victim's phone number.
2. Allocated_ip identifies the main address of victim's smartphone.
3. MP_relay identifies the GRs used by victim's device to route messages, this information is used by the DMS to deliver ALERT messages to victims.
4. Destination identifies SMS destination phone number.
5. Status identifies message delivery status. Valid values are SENT if the message has been sent and UNSENT.

The SMS table is populated from ALERT messages transmitted to the DMS.

4.8.4 Internet Connectivity and Bandwidth

Satellite Internet access is the preferred internet connectivity chosen to route Internet SMS from victims in the disaster zone to recipients outside the disaster zone. Satellite internet access is an internet access provided via communication satellite to individual users through geostationary satellite. Although satellite connectivity has a higher propagation delay, yet it is cheap, easy to setup and very suitable for simple SMS routing as high bandwidth is not required for sending such messages. Since the bandwidth will not be shared with the MANET, the research recommended minimum of 1 Mb/s bandwidth (PSAV, 2019).

4.9 Addressing Network Partition

Network partitioning occurs when a key MPR device switches off due to low battery thus making it impossible for victims to relay traffic or communicate with the DMS. DS-OLSR and DS-OLSRMP provides a simple approach of dealing with network partition by using the information provided by Topology Control table. This information enables RT to monitor the Battery life of each device in the network as its displays on the screens connected to the DMS using colours to connote which key device requires backup or replacement. As shown in Table 4-4, an MPR device with 45% battery energy level will have a red background indicating urgent replacement requirement, while a device with 50% battery will have a yellow background indicating needs of preparation for replacement requirement.

A device operating as an important MPR with low Battery life will require a backup plan against failure and the plan involves the deployment of anchored buoys to which a mobile device and backup battery are attached as shown in Figure 4-8. The anchored buoys are deployed in two circumstances: when a victim serving as a key MPR is to be rescued or before the victim's phone goes off because of low Battery life. Thus, the victims relaying through the affected MPR will be able to switch connection to the device mounted on the lifebuoy, which is reporting a constant battery energy of 100%.

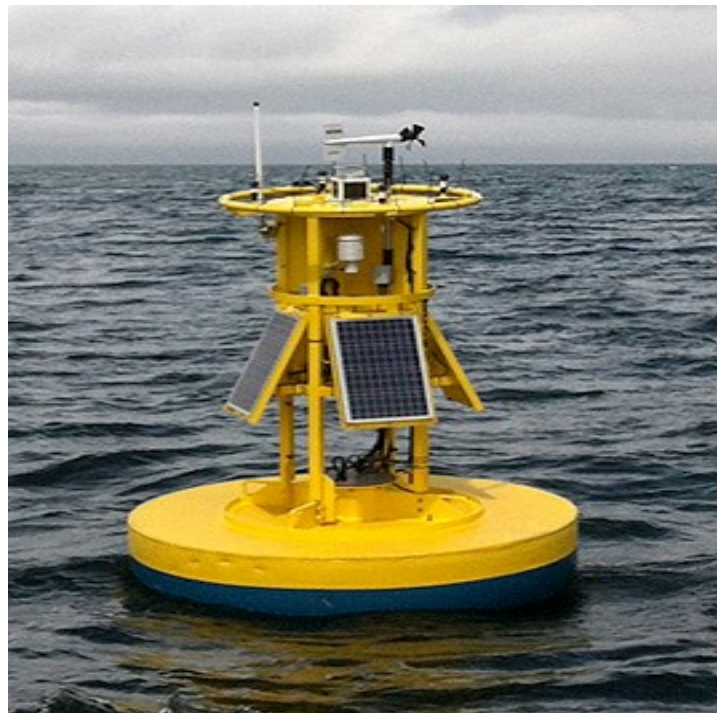


Figure 4-8: Anchored buoy with solar panels and sensors for monitoring environment and water quality (LISICOS, 2019).

Table 4-4: Sample Screen output on DMS showing which device requires replacement

Device IP	Phone Number	Battery life	Service
10.1.1.1	0801-xxx-xxxx	50%	MPR
10.1.1.2	0702-xxx-xxxx	80%	MPR
10.1.1.3	0821-xxx-xxxx	45%	MPR
10.1.1.4	0822-xxx-xxxx	60%	MPR

4.10 DS-OLSR Packet Format and Forwarding

As presented in Table 4-5, DS-OLSR retained OLSRv1 unified packet format. However, to improve the protocol for energy friendly routing and communication in disaster zone, the research made a single modification by adding **Originator ID** to hold device’s phone number. Like OLSR, data packets are embedded in User Datagram Protocol (UDP) for network transmission. Detail descriptions of OLSRv1 headers can be found in Section 3.4.1, while the proposed modification is discussed in the following Sub-Section.

Table 4-5: DS-OLSR unified packet header (new: in Red Colour)

0					1					2					3						
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Packet Length										Packet Sequence Number											
Message Type					Vtime					Message Size											
Originator Address																					
Originator ID																					
Time to Live					Hop Count					Message Sequence Number											
MESSAGE																					
Message Type					Vtime					Message Size											
Originator Address																					
Originator ID																					
Time to Live					Hop Count					Message Sequence Number											
MESSAGE																					

Originator ID

This field stores smartphone's phone number and users of multi-SIM devices may be able to manually SELECT their most recognized phone number as their originator ID (from the DS-OLSR messaging application).

The Originator ID provides human readable device information across the network, allowing victims to recognise the sources of their messages and in case of availability of internet connection, it will be use by the victims to send and receive messages. The ability to uniquely identify each device via Originator ID renders OLSR MID messages obsolete, since devices with multiple interfaces will always include the same Originator ID. Hence recipients will accept a single message from any of the multiple interfaces, and quietly drop the rest. Figures 4.9 represent communication flow from a victim's phone across the MANET through the DMS and finally to a recipient outside the disaster area. Although DS-OLSR recommends phone numbers to as Originator ID, it is equally possible for any network enabled device (such as laptops, iPods, SIM-less iPADS etc) that can generate a network-wide unique ID to implement.

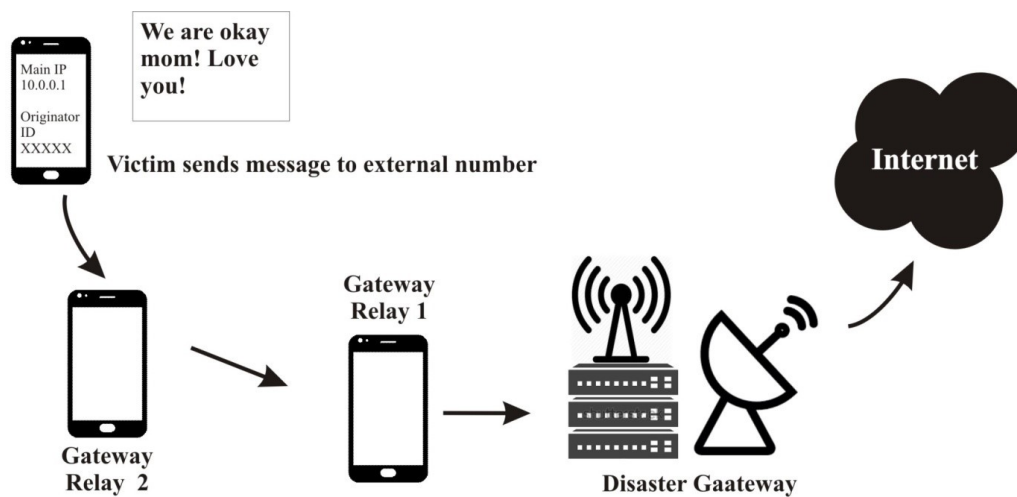


Figure 4-9: Directional flow of SMS from MANET to Internet

4.10.1 DS-OLSR and DS-OLSRMP Packet Processing

DS-OLSR and DS-OLSRMP adopts OLSR processing rules as discussed in Section 3.4.1 with the following proposed modifications:

1. To drop packets without Originator ID
2. To drop packets if message type does not belong to the current TS.

4.10.2 DS-OLSR and DS-OLSRMP Packet Forwarding

Just like the Packet Processing, DS-OLSR also adopted the OLSR forwarding rules as discussed in Section 3.4.1 with the following proposed modifications:

1. Do not forward packets whose Originator Address, Originator ID, and Message Sequence Number matches what is stored in the Duplicate set, since it implies the packet has been previously forwarded.

4.11 DS-OLSR and DS-OLSRMP Repositories/Tables/Sets

DS-OLSR and DS-OLSRMP retained 7 routing tables from OLSR as its dropped one (Multiple Interface Association Set) and added two new tables called: Contacts Set and Deviceinfo Set. Contacts Set contains C_addr, C_phone_num, C_battery_level and C_time fields. It provides DS-OLSR messenger with reachable contact list and the set is populated (by reading the tables and copying their content to the contact set) from existing OLSR bases, namely link set and topology information base. Deviceinfo Set stores the “Device Tuple” (in OLSR parlance) using the following fields: D_addr, D_phone_num, D_battery_level and D_time. The following are Tables/Sets used by both DS-OLSR and DS-OLSRMP:

1. Link Set
2. Neighbour Set
3. 2-hop Neighbour Set
4. MPR Set
5. MPR Selector Set
6. Topology Set
7. Duplicate Set
8. Contacts Set
9. Deviceinfo Set

As started earlier, Multiple Interface Association Set (for MID nodes) is not retained. This is because DS-OLSR uses device phone number, along with message sequence number to prevent duplicate message broadcast from the nodes with multiple interfaces. Another reason for dropping MID implementation is the preference of DS-OLSR and DS-OLSRMP to communicate via a single interface; in order to conserve energy in smartphones. In addition, beside the two new tables: Contact and DeviceInfo Sets, DS-OLSR also modifies Link Set,

Topology Set and Duplicate Set by adding phone number and Battery life fields. The proposed and modified Tables are discussed in the following Sub-Sections.

4.11.1 Duplicate Set

This table is responsible for storing information that prevents retransmission of a transmitted message. OLSRv1 (Clausen & Jacquet, 2003) specify the following fields for a "Duplicate Tuple": D_Addr, D_Seq_Num, D_Retransmitted, D_iface_list, and D_time. D_addr stores the originator address of the message originator, D_seq_num contains the message sequence number, D_retransmitted indicates if the message has been retransmitted, values are stored in Boolean, thus 0 for false and 1 for true, D_iface represents a list of interface addresses on which the message has been received, and finally, D_time determines the removal time of a tuple that has expired.

Duplicate set is modified for DS-OLSR by adding one additional field to the previous five, the new field is D_phone_num as shown in Table 4-6.

Table 4-6: Sample Duplicate Set record

D addr	D phone num	D seq num	D retransmitted	D iface list	D time
10.1.1.1	0802XXXXXXXX	10	1	10.1.1.2, 10.1.1.3, 10.1.1.4	10000 ms

4.11.2 Link Set

A link set is maintained by each node as a record ("Link Tuples" in OLSR parlance) of responses to its Hello messages. The following fields are recommended by OLSR: L_local_iface_addr, L_neighbour_iface_addr, L_SYM_time, L_ASYM_time, and L_time. L_local_iface_addr is the address of the record keeping node, L_neighbour_iface_addr is the address of the neighbour node with whom the sender shares a link.

L_SYM_time is the time that determines if a link to a neighbour is still symmetric, L_ASYM_time is the time that determines if a link to a neighbour is still asymmetric, finally L_time is the time that determines a record has expired and MUST be removed. Link set is modified for DS-OLSR by adding two field, namely L_neighbour_phone_num and L_neighbour_battery_level as shown in Table 4.7.

Table 4-7: Sample Link Set records

L_local_iface_addr	L_neighbour_iface_addr	L_neighbour_phone_num	L_neighbour_battery_level	L_SYM_time	L_ASYM_time	L_time
10.1.1.1	10.1.1.2	0802 xxxxxx	70%	10000 ms	10000 ms	10k ms
10.1.1.1	10.1.1.3	0803 xxxxxx	85%	10000 ms	10000 ms	10k ms
10.1.1.1	10.1.1.4	0801 xxxxxx	39%	10000 ms	10000 ms	10k ms

4.11.3 Topology Set

Nodes in OLSR are familiar with the MANET topology by maintaining a topology set. Data for populating the set are gathered from TC messages. Topology set records "Topology Tuple" for each destination in the network using the following fields: T_dest_addr, T_last_addr, T_seq, and T_time . T_dest_addr is the interface address of a node that can be reached via 1-hop from the node (MPR) whose interface address is stored in T_last_addr (Typically, T_last_addr is a MPR of T_dest_addr), T_seq is a sequence number generated with sending the message, this is different from the message sequence number. Finally, T_time determines when the record expires and MUST be deleted.

Table 4-8: Sample of Topology Set records

T_dest_addr	T_last_addr	T_dest_phone_num	T_last_phone_num	T_dest_battery_level	T_last_battery_level	T_seq	T_time
10.1.1.1	10.1.1.2	0802 xxxxxx	0702 xxxxxx	50%	80%	10	45k ms
10.1.1.1	10.1.1.3	0803 xxxxxx	0703 xxxxxx	45%	95%	30	45k ms
10.1.1.1	10.1.1.4	0801 xxxxxx	0701 xxxxxx	30%	77%	45	45k ms

Topology set is used by nodes to calculate routes to other nodes, DS-OLSR equally uses the information to populate contacts set. However, DS-OLSR modified topology set by introducing the following fields: T_dest_phone_num, T_last_phone_num, T_dest_battery_level and T_last_battery_level as captured in Table 4.8.

4.11.4 Contacts Set

In DS-OLSR, each node maintains a list of reachable phone numbers; this list is stored in the Contact Set as in Table 4-9. Contact Set data is collated from topology set. Contacts set is used by DS-OLSR messenger to identify reachable “survivors” within the disaster zone. Contact Tuple are stored in the following fields.: C_addr, C_phone_num, C_battery_level and C_time. C_addr is the interface address of the reachable node/device, C_phone_num is the device phone number, while C_battery_level is the device’s Battery life, C_time determines when this tuple is regarded as obsolete and MUST be deleted.

Table 4-9: Sample of Contact Set records

C_addr	C_phone_num	C_battery_level	D_time
10.1.1.2	0802 xxxxxx	50%	50000 ms
10.1.1.3	0803 xxxxxx	45%	50000 ms
10.1.1.4	0801 xxxxxx	30%	50000 ms

4.11.5 Deviceinfo Set

This set is created while switching the device to disaster mode (DM), DS-OLSR messenger is responsible for creating and updating this set. Deviceinfo set contains the following fields: D_addr, D_phone_num, D_battery_level and D_time. D_addr contains the device interface address, D_phone_num contains the phone number retrieved from the device, while D_battery_level contains the remaining Battery life at the time it was last retrieved. finally, D_time determines when this tuple is regarded as obsolete and MUST be UPDATED not deleted. D_time should be set configure for update every five minutes in order to retrieve and report the Battery life as show in Table 4-10.

Table 4-10: Sample of Deviceinfo Set record

D_addr	D_phone_num	D_battery_level	D_time
10.1.1.2	0802 xxxxxx	50%	5000 ms

4.12 ALERT Message

As stated earlier, DS-OLSR and DS-OLSRMP proposes embedding text messaging capability into OLSR in order to minimize overhead and improve energy conservation. ALERT messages use GSM SMS charset and shares another similarity with GSM by limiting messages to 160

characters. These characters are stored as a separate octet in groups (four octets per group or 32 bits per field). In DS-OLSR, they generally occupy a total of 40 octets.

Adding ALERT message to a routing protocol might look awkward and uncalled for (since it does not provide link or device state information). Nonetheless, folding ALERT message into DS-OLSR provides the following energy saving benefits:

1. Message Collation: Adding messaging capability to DS-OLSR permits MPRs to collate ALERT messages from 1-hop devices. ALERT messages are stored until the commencement of the Message Time Slice (MTS). This prevents panic survivors from flooding the network with messages while control messages are being sent.
2. Better Quality of Service (QoS): The ability to communicate via SMS within DS-OLSR and DS-OLSRMP improves overall network QoS, such as PDR and overall end-to-end delay. This is possible since the only message that runs during MTS is the ALERT message. Moreover, the message forwarding process prevents collision since only MPR nodes can transmit the message and of course the concept of TSS improves link quality by eliminating crosstalk and reduces funnel problem.

ALERT messages are composed and sent by victims or RT using the DS-OLSR messenger (which is installed on their smartphones). ALERT messages can be sent to any of the following recipients:

1. To other victims within the MANET
2. To RT for assistance
3. To anyone outside the disaster zone

DS-OLSR messenger collates and display phone numbers of devices in the MANET from the contacts set/table created by each node. ALERT messages composed by victims should contain location information along with any medical emergency which may warrant rapid evacuation of such victims. As started earlier, the technical relationship between DS-OLSR ALERT message and GMS/3GPP SMS specification (GSM 03.38) is the fact that, ALERT messages use GSM character set (ETSI, 2019a) for composing, encoding and decoding messages, along with limitation on the number of characters permissible in a message. However, ALERT messages within the MANET do not require the implementation of GSM infrastructure (such as SMSC – SMS Centre). ALERT message packet format is shown in Table 4.11. The key fields of the Alert message packet format are discussed in the following Sub-Section.

Table 4-11: ALERT message packet format

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Destination										Message Size										Reserved											
Destination Address																															
Destination Phone Number																															
1st Octet										2nd Octet										3rd Octet										4th Octet	
										:										:											
										:										:											
										:										:											
37th Octet										38th Octet										39th Octet										40th Octet	

4.12.1 Destination

Destination field is used to determine the destination of a message; valid values are listed below:

1 = Node or Device within the MANET (Disaster Zone)

2 = Node or Device outside the disaster zone.

Values for Destination are determined by the location of the contact number selected by the user. Thus, if a user selects a number from the list stored in contacts set, then the message Destination is determined to be “internal” or within the MANET (that is Destination = 1), while selecting the phone number from the phone contact list or manually typing or pasting a number stored in memory will force DS-OLSR to execute the following tests:

1. Check contacts set for the existence of the selected/pasted/typed number.
2. If number exists in contacts set, then Destination = 1
3. If number does NOT exist in contacts set, then Destination = 2

4.12.2 Message Size

Message size stores the number of characters contained in the ALERT message. The maximum value of Message Size is 160, while the minimum is 2, a message having a single octet is discarded by the DS-OLSR messenger, thus preventing unnecessary flooding of the MANET with incomplete or cryptic messages.

4.12.3 Destination Address

This field store the interface address of the smartphone that the ALERT message is destined, that is the target recipient. This address is different from the Originator Address, note that while Originator Address stores the interface of the sender, the destination address stores the interface of the receiver.

4.12.4 Destination Phone Number

This field store the phone number that the user selected while composing the message using DS-OLSR Messenger. In other words, it is the phone number of the message recipient. The Destination Phone Number is different from destination address as destination address stores the interface of the receiver.

4.12.5 Message Octets

Each character in an ALERT message is converted from human readable alphanumeric to the corresponding hexadecimal representation of such characters in GSM SMS Character Set (GSM 03.38) (ETSI, 2019a). A major advantage of GSM 7-bit character set is that it is already available on mobile phones in multi-lingual format, thus encoding each character in DS-OLSR 8-bit wide packet fields will not affect the character during the decoding process. For example, the following message: **Hello Haidar** is encoded using GSM 03.38 as: **48 65 6C 6C 6F 20 48 61 69 64 72** (the encoded values are in hexadecimal – Base 16). Thus, DS-OLSR converts the hexadecimal values into their respective binary values for transmission, each 7-bits value is preceded with a binary 0 before placement in their respective ALERT message fields. Thus, hexadecimal **6C** converts to 7-bit binary **1101100** but it is preceded by a binary 0 and becomes **01101100** – which is the value that DS-OLSR will use while transmitting. The character set for GSM 03.38 is shown in Figure 4.10.

4.12.6 SMS Message Routing

As mentioned earlier, ALERT messages meant for recipients outside the disaster zone are routed to the DMS for transmission via Internet SMS to the recipient. SMS sending websites are often directly connected to multiple Mobile Operators SMS Centres (SMSC) either through

	0	1	2	3	4	5	6	7
0	@	Δ	SP	0	i	P	z	p
1	£	_	!	1	A	Q	a	q
2	§	Φ	"	2	B	R	b	r
3	¥	Γ	#	3	C	S	c	s
4	è	Λ	¤	4	D	T	d	t
5	é	Ω	%	5	E	U	e	u
6	ù	Π	&	6	F	V	f	v
7	ì	Ψ	'	7	G	W	g	w
8	ò	Σ	(8	H	X	h	x
9	ç	Θ)	9	I	Y	i	y
10	LF	Ξ	*	:	J	Z	j	z
11	Ø	1)	+	;	K	Ä	k	ä
12	ø	Æ	,	<	L	Ö	l	ö
13	CR	æ	-	=	M	Ñ	m	ñ
14	Å	ß	.	>	N	Ü	n	ü
15	å	É	/	?	O	Ş	o	à

Figure 4-10: GSM basic character set (ETSI, 2019a)

Internet or via leased lines (engineersgarage, 2012). SMS centres receive messages sent by users and delivered to intended recipients. The SMS routing process with SMS originated from a device in the disaster zone, routed through the DMS and delivered via Internet to the SMSC of the recipient, and finally to the intended recipient is shown in Figure 4-11.

Internet SMS service providers make use of different internet protocols (HTTP, HTTPS, API etc) to route messages sent by authorized users. The example below uses “API” protocol along with a port address:

api.examplesmsgateway.com:8080/sendsms/singlesms?username=fema&password=dpass&destination=080xxxxxxx&sender=victim_phone_num&message=urlencode(“hello mom, am okay”);.

However, it is quite possible for Federal Emergency Management Authorities (FEMA) in every country to directly connect to the SMSC gateway of Mobile operators, instead of routing such messages via middlemen. Direct connection to SMSCs prevent blockage of SMS if Do Not Disturb (DND) is activated on recipient phones.

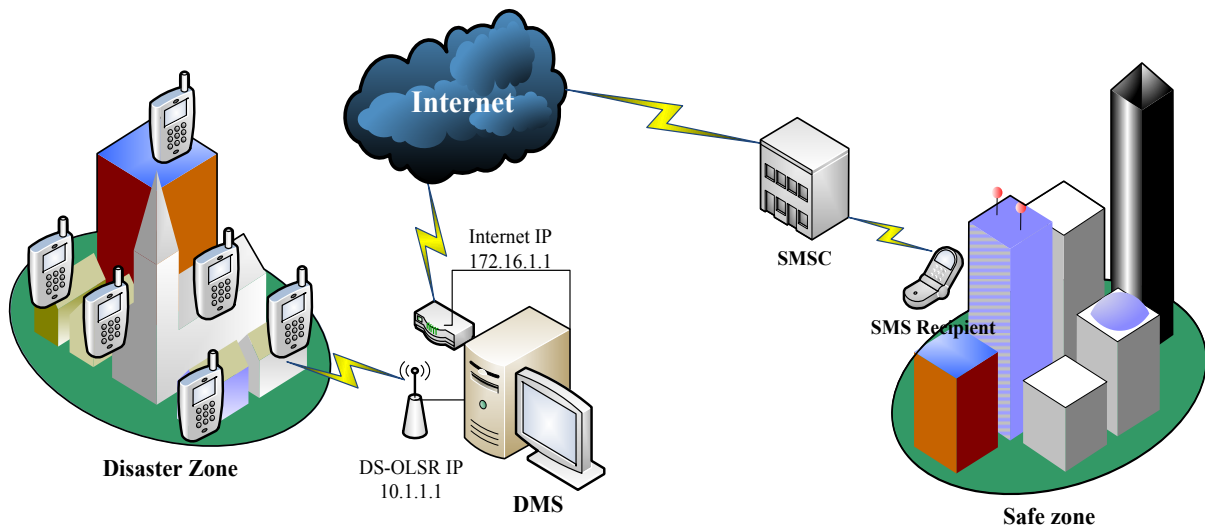


Figure 4-11: Message routing from DMS to recipient outside the disaster zone

4.13 SHHH Message Implementation

As stated earlier, Shhh message is one of the methods proposed by DS-OLSR to handle new nodes joining the network. New nodes are identified with their Hello broadcast. Thus, a new node broadcasting Hello message while other nodes have moved on to another TS such as TPTS or MTS will be sent a Shhh message to allow the new node to stop broadcasting Hello messages and reconfigures itself against the next NFTS period by setting its internal timer with the value passed via the Shhh message. SHHH message packet format is shown in Table 4-12. The key fields of the Shhh message are discussed in the following Sub-Sections.

Table 4-12: SHHH message packet format

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Current Time Slice										Current Timer Value										Reserved											
Destination Address																															
:																															

4.13.1 Current Time Slice

Current time slice field contains the current network TS value. Valid values are shown below:

1 = TPTS

2 = MTS

NFTS is excluded from the current time slice since Shhh message would only be sent in response to a new node observing its' own NFTS period while other nodes are observing either TPTS or MTS periods. This field is 8-bits in length.

4.13.2 Current Timer Value

The 8-bit current timer value field contains the timer value of the broadcasting node. As a recap, timer total values are presented below:

TPTS = 14 seconds (14,000ms)

MTS = 30 seconds (30, 000ms)

Thus, if a new node sends out a Hello message 50ms after the commencement of TPTS, then the current timer value it would receive in the Shhh message is 13,950ms.

4.14 Modification to Hello and TC Messages Packet

Hello and Topology Control (TC) messages are the major control messages of OLSR. Hello message is propagated for neighbour detection, link sensing and MPR selection signalling, while TC message is broadcasted by MPR nodes to advertise links to nodes that elected them as MPR. The modifications to the Hello and Tc messages packet format are as follows:

4.14.1 Modification to Hello Message Packet

As discussed in Section 2.5, Hello messages play a vital role in neighbourhood network formation, which cumulates with the selection of MPRs that are responsible for broadcasting the link and device state of every node in the network.

Table 4-13: DS-OLSR Hello message packet

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Reserved										Htime										Willingness											
Link Code					Battery life					Link Message Size																					
Neighbour Interface Address																															
Neighbour Interface Address																															
: : : :																															

Thus, DS-OLSR modified Hello message by including the device Battery life in the message header, this allows DS-OLSR to add the device Battery life in each link state broadcast so that the recipient of the Hello message to determine if it can select the broadcaster as an MPR. The modified Hello message packet is shown in Tables 4.13.

Battery life

The Battery life of each device occupies a very important position in DS-OLSR and DS-OLSRMP networks as it determines the selection of MPR nodes, use for prioritisation of message delivery for low battery energy nodes, and allow the rescue team to prioritise the rescue operation. In other words, including device Battery life in every Hello message extends lifespan of individual nodes, particularly the low battery nodes thereby avoiding network partition due to dead nodes.

OLSR groups related neighbour interface addresses by their Link Codes. Thus, DS-OLSR proposes using both Link Code and Battery life to determine organization of neighbour interface addresses and all neighbours with symmetric connections having 60 percent Battery life will be listed separately from those having 40% or lower. However, to reduce overhead brought about by too many messages, Battery life range could be introduced, thus all symmetric nodes with between 90%-75% would be better criteria which will reduce network overhead.

4.14.2 Modification to TC Message Packet

TC messages advertise links to nodes that elected the TC message sender as an MPR. Extending MPRs to equally propagate the Battery life of each device across the network will enable RT to know the Battery life of every device within the network and to determine either to deploy anchored buoys with a mobile device and backup battery or to urgently rescue the victims. Modification to the TC message packet is shown in Table 4-14.

Table 4-14: DS-OLSR TC message format

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ANSN										Battery life										Reserved											
Advertised Neighbour Main Address																															
Advertised Neighbour Main Address																															
:										:										:										:	

4.15 Chapter Summary

This Chapter presents the overall design process that is required for the successful deployment of DS-OLSR on the field by RT/victims, or in labs by researchers and finally by developers implementing DS-OLSR. The chapter started with DS-OLSR design assumptions and proceeded with the process of switching smart phones to disaster mode, from detection of incoming disaster to sending warning message embedded with link for initiating DS-OLSR application and connecting to DS-OLSR MANET. The design of the novel DS-OLSR is proposed for communication during disaster recovery and rescue operation, which redesigns OLSR packet header through the addition of a new field, namely Originator ID (device's phone number). The introduction of Originator ID leads to the elimination of multiple interface device (MID) message of conventional OLSR. The design attempts to reduce routing overhead by encapsulating HELLO, Topology Control (TC) and Host Network Association (HNA) messages within their respective Time Slices (TS). Thus, these broadcasts can only occur during their TSs. Modification of 1-hop and 2-hops data sets by including two additional fields, namely PHONE_NO and BATTERY_LEVEL are explained in the Chapter. How DS-OLSR handles nodes that attempt to join the network after NPTS, Proposed Disaster Management Server, simple approach for handling network partition and DS-OLSR and DS-OLSRMP packet format and forwarding process are equally explained. Finally, the design of Alert and Shhh messages and of course modification of Hello and TC messages were presented to wraps up the Chapter. The holistic solution is designed to enable communication continuity in the aftermath of a major disaster. The next Chapter presents the Implementation of the proposed DS-OLSR in NS-3 simulation environment.

Chapter 5

Implementation of the proposed DS-OLSR in a Simulation Environment

5.1 Introduction

The proposed DS-OLSR as defined in Chapter four is implemented in NS-3 (release 3.29) simulator. The implementation of the proposed routing protocol presented in this Chapter is in two forms: Network formation scenario and implementation of DS-OLSR in Disaster Area Network. The objective of the first simulation is to determine the amount of energy dissipated and control overhead during OLSR/DS-OLSR network formation process, while the second simulation is to evaluate the performance of the proposed scheme in a disaster related scenario as proposed by Aschenbruck, Gerhards-Padilla, and Martini (2009), which reflects real life disaster scenario. The Chapter is presented as follows: Section 5.2 discuss the overview of simulation-based model and proceeded with the description of the different implementation models used in evaluating the performance of the proposed routing protocol. Section 5.3 presents the simulation of network formation scenario comprises of the simulation setup and analysis of the proposed scheme as compared to OLSRv1. The implementation of the DS-OLSR in Disaster Area Network is presented in Section 3.4. This scenario validates the performance of the DS-OLSR based on energy consumption, control overhead, packet delivery ratio and end-to-end delay. All simulated scenarios were conducted using 50, 100, and 200 nodes density. Section 3.5 wraps up the Chapter with the Chapter summary.

5.2 Simulation-Based Model

Simulation is a method for modelling a system (problem) using a computer program. This method is usually cost effective, and it allows the evaluation of design alternatives, prediction of causes and results of certain actions, and identification of problem areas before implementation of actual system in a real life. In addition, simulation allows test and implementation of systems without much negative effects on the real system even if things go wrong. However, the simulation itself has some limitation as identified by Hope (2015), it may be hard to determine the right level of model complexity, statistical uncertainty in results and may be slow. For instance, two minutes real life could be two hours of simulation time. Simulation also involves studying the real system, and collection of data and parameters of the system to be modelled. Monte Carlo, Emulation, Trace-driven, Continuous-event and Discrete

simulations are common types of simulation. The simulation type for this research work is discrete event-driven simulation as the model involved creation of events on a network that are sorted by the simulated time by which the event should occur.

NS-3.29 has been chosen for this research work as it provides an open and flexible simulation environment for educative research activities. NS-3 is a discrete-event network simulator. This implies the simulator manages several events that are scheduled to execute at a specific simulation period. NS-3 executes events sequentially, thus as soon as an event is completed, the simulator will either move to the next event or will exit if there are no more events in the event queue. Events are generated and scheduled based on simulation code. Thus, the code can determine if the events scheduled for execution are large or small. For example, each node in OLSR generate a lot of messages, respond to messages, and maintain several tables – which translate to different events at different simulation periods.

5.2.1 Network Model

Mobile Ad-hoc networks are modelled using graph $G(V, E)$, where V and E represents sets of mobile nodes and arcs, respectively. The arc models the intersection or wireless radio range between pairs of nodes. Every node $A \in V$ communicates directly with set of neighbouring nodes within the range of its coverage area (Waheb A. Jabbar et al., 2018). However, relay nodes are used for nodes that are not within the coverage area of each other. In mobility scenarios, mobile devices move arbitrarily at different speeds; consequently, the topology changes randomly and rapidly at irregular time. As the nodes move around detects the present of other nodes and establish routing among themselves thereby creating network dynamically. The network is established via broadcast of control message from participating nodes autonomously. A typical hop length of E increases with the increased of nodes in set V , which in turns affects the performance of routing protocols. The proposed scheme is implemented in NS-3 version 3.29 and validated mathematically using relevant metrics in different network scenarios.

5.2.2 Energy Consumption Model

The release of NS-3 simulation software (release 3.29, as of August 21st, 2019) failed to provide built-in energy functions for OLSR implementations. Thus, it is impossible to know the energy cost of nodes without modifying OLSR modules. A researcher would expect that including

OLSR modules and any of the energy modules that ships with NS-3 in a simulation file is enough to capture OLSR network activities along with the energy cost of such activities. Unfortunately, this is not the case. Although this situation can be remedied by modifying NS-3 OLSR module, nonetheless, the cost of such an effort is enough to discourage researchers. To address this perennial problem, this research implemented a simple energy model that can be integrated into the NS-3 OLSR module.

The modification of the OLSR module were made in two important files that contain the actual routing logic of OLSR in NS-3: these files are **olsr-routing-protocol.cc** and **olsr-routing-protocol.h**. The first file contains the full C++ source code for OLSRv1 implementation in NS-3, while the second code contains function names and their parameters. The energy function was used to compute and display the energy cost of forming and maintaining OLSR, DS-OLSR and DS-OLSRMP networks in the simulation of different disaster scenarios.

Energy consumption modelling is very critical in network for disaster recovery and rescue operations as some disasters equally damaged power grids, and the communication nodes depends on limited battery energy for power. The configuration setting of this energy model plays a vital role in estimating the energy consumes by nodes during transmission., Receive, Transmit, Idle and Sleep are four states of mobile nodes in a wireless communication network and of course, every state consumes a specific amount energy. The energy model was based on Generic Radio Energy Model as highlighted in (Waheb A. Jabbar et al., 2018) and (Fotino et al., 2007), which defined the total energy consumption of a node as the sum of energy consumed in all states. Therefore, the energy consumed for each state of node is given as:

$$Tx_{Energy} = V \times Tx_{Current} \times Tx_{Time} \quad (5-1)$$

$$Rx_{Energy} = V \times Rx_{Current} \times Rx_{Time} \quad (5-2)$$

$$Idle_{Energy} = V \times Idle_{Current} \times Idle_{Time} \quad (5-3)$$

$$Sleep_{Energy} = V \times Sleep_{Current} \times Sleep_{Time} \quad (5-4)$$

Where Tx_{Energy} , Rx_{Energy} , $Idle_{Energy}$ and $Sleep_{Energy}$ are energy consumes during the states of transmit, receive, idle, and sleep, respectively. V is a default supply voltage as contained in Waheb A. Jabbar et al. (2018), (De Rango, Fotino, & Marano, 2008) and (Fotino et al., 2007), and $Tx_{Current}$, $Rx_{Current}$, $Idle_{Current}$ and $Sleep_{Current}$ are circuitry current in amperes for each state.

Tx_{Time} , Rx_{Time} , $Idle_{Time}$ and $Sleep_{Time}$ represent the time spent in each state. However, Transmit and receive energy is determined by signal transmission power from Physical layer (PHY.SET). therefore, due to external interference, we considered sensitivity degradation factor as modelled in Ehiagwina, Afolabi, Surajudeen-Bakinde, and Fakolujo (2019) to account for the signal degradation or power amplifier inefficiency factor as used in (Waheb A. Jabbar et al., 2018). In a general term, the total energy (E_T) consumed by a node to transmit and received packet is:

$$E_T = [Tx_{Energy} + Rx_{Energy} + Idle_{Energy} + Sleep_{Energy}] S_d \quad (5-5)$$

Where S_d represent the power amplifier inefficiency factor of the circuit power consumption. The energy model parameters for our study are set based on studies of Waheb A. Jabbar et al. (2018) and Ehiagwina et al. (2019). The energy function implementation enabled this research to capture and display the energy cost of OLSR, DS-OLSR, DS-OLSRMP networks.

5.2.3 Wi-Fi Simulation Setup

Wi-Fi technology is one of the available wireless technologies that allows computers, smartphones, and other wireless devices to communicate wirelessly with one another within the coverage area of one another or an access point. Almost two decade after its initial design, the Wi-Fi technology becomes one of most common ways for internet access (Hiertz et al., 2010), with an ubiquitous connection and inexpensive cost (Rattagan, 2016). The Technology was designed based on IEEE 802.11 standard and it is usually for indoor usage, such as offices, schools, homes, or shopping malls. In a normal Wi-Fi network, a client scans and associates to a WLAN that is created and broadcasted by an AP in its vicinity (Camps-Mur, Garcia-Saavedra, & Serrano, 2013). With the less-cost factor of Wi-Fi, most smartphones applications are designed to perform more background tasks (such as data backup, apps update etc.) when the phones are connected to Wi-Fi network, to enable the apps users take advantage of the Wi-Fi's less service cost (Rattagan, 2016). Since the cellular network is down, smartphone users are left with short-range radios communication options such as Wi-Fi and Bluetooth to a disaster MANET. The following reasons influenced this research to use Wi-Fi (in ad hoc mode) to evaluate the performance of the propose routing protocol.

Availability: The technology is already available in the smart phones of rescuers, disaster victims as well as rescue volunteer workers who help the rescuers with first-hand information on the rescue operation.

Propagation Range: Wi-Fi propagation range is between 1 to 250 meters , which is higher than Bluetooth (Jameel, Hamid, Jabeen, Zeadally, & Javed, 2018) and ZigBee (M. S. Iqbal & Al-Raweshidy, 2013). Longer propagation range is very important in a disaster, since it covers more affected areas.

Data Rate: Wi-Fi data rates (up to 54Mbps) is higher than both Bluetooth (up to 24Mbps) and ZigBee (20 to 250 kbps.). Thus, Wi-Fi is equipped to handle higher data that may be generated by victims during disaster recovery and rescue operation.

5.2.3.1 Wi-Fi Antenna Setup in NS-3

To ensure OLSR/DS-OLSR MPR nodes relay message on behave of their electors, the Wi-Fi radio power was deliberately degraded to make sure that resultant signal does not propagate beyond 50 metres. In addition, antenna transceiver was degradation by -1 to mimic the effect of walls and other environmental factors absorbing some of the Wi-Fi signal. Listed below are the NS-3 C++ code that was used for the Wi-Fi setup:

```
WiFiPhy.Set ("TxPowerStart", DoubleValue(16));  
WiFiPhy.Set ("TxPowerEnd", DoubleValue(16));  
WiFiPhy.Set ("TxPowerLevels", UIntegerValue(1));  
WiFiPhy.Set ("TxGain", DoubleValue(-5));  
WiFiPhy.Set ("RxGain", DoubleValue(-5));  
WiFiPhy.Set ("RxSensitivity", DoubleValue(-31.8));  
WiFiPhy.Set ("CcaEdThreshold", DoubleValue(-31.8));
```

TxPowerStart/TxPowerEnd

```
WiFiPhy.Set ("TxPowerStart", DoubleValue(16));  
WiFiPhy.Set ("TxPowerEnd", DoubleValue(16));
```

NS-3 TxPowerStart is the minimum available transmission level (dbm) (ns3::WifiPhy, 2019) available to the Wi-Fi antenna, while TxPowerEnd is the maximum available transmission level (dbm) which the antenna can draw. The antenna transmission starting power (TxPowerStart) is set at 16dBm, which is the same with transmission ending power

(TxPowerEnd), both settings store the minimum and maximum transmission power level of the Wi-Fi antenna. Higher power levels for both TxPowerStart and TxPowerEnd increases transmission range. However, increasing the power level for TxPowerEnd has no obvious effects on the transmission range, while increasing the power level of TxPowerStart alone forces NS-3 to terminate the simulation with the following error *“assert failed. cond=“m_txPowerBaseDbm <= m_txPowerEndDbm”, file=../src/Wi-Fi/model/Wi-Fi-phy.cc, line=794 terminate called without an active exception”*.

TxPowerLevels

```
WiFiPhy.Set ("TxPowerLevels", UIntegerValue (1));
```

TxPowerLevels stores the number of transmission power levels available between TxPowerStart and TxPowerEnd (ns3::WifiPhy, 2019), the value is 1 to ensure that both TxPowerStart and TxPowerEnd have the same value. Retaining TxPowerLevels as 1 when TxPowerStart is lower than TxPowerEnd throws the following error – *“assert failed. cond=“m_txPowerBaseDbm == m_txPowerEndDbm”, msg=“cannot have TxPowerEnd != TxPowerStart with TxPowerLevels == 1”, file=../src/Wi-Fi/model/Wi-Fi-phy.cc, line=803 terminate called without an active exception”*.

TxGain/RxGain

```
WiFiPhy.Set ("TxGain", DoubleValue(-10));
```

```
WiFiPhy.Set ("RxGain", DoubleValue(-10));
```

Both TxGain or Transmission Gain and RxGain or Reception Gain are measured in dB (ns3::WifiPhy, 2019). These values were set as -1 to mimic signal degradation due to walls and other environmental factors obstructing the signal flow. A negative value eliminates Tx and Rx gains, while a positive value increases Tx transmission range and Rx gain.

RxSensitivity

```
WiFiPhy.Set ("RxSensitivity", DoubleValue(-31.8));
```

The RxSensitivity (Reception Sensitivity) value represents a device’s default energy signal or noise level (in dBm) (ns3::WifiPhy, 2019). The PHY will only detect incoming signal if the dBm of the incoming signal is higher than RxSensitivity’s value. For example, if RxSensitivity = -31 then the PHY will not detect a signal level that is less than -31. It was discovered during simulation that higher RxSensitivity values allow better PHY detection of incoming signals.

An RxSensitivity value of -21.8 lead to complete silence of the entire network, not a single signal was detected by any of the nodes because the RxSensitivity value of -21.8 is too low.

CcaEdThreshold

WiFiPhy.Set ("CcaEdThreshold", DoubleValue(-32.8));

Clear Channel Assessment Energy Detection Threshold (CcaEdThreshold) contains the energy threshold (dBm) value that a non-Wi-Fi device must broadcast above to allow the PHY layer to declare CCA BUSY state. This check is performed on the 20 MHz primary channel only. Changing this value did not affect transmission and reception range/sensitivity in any way.

5.2.4 Mobility Model

There are different forms of movement in disaster area scenario including Random way point (RWP), heterogeneous area-based movement, movement on optimal path avoiding obstacle and nodes join and leave the scenario models (Aschenbruck et al., 2009). We used random way point (RWP) mobility model as it commonly used in evaluating MANETs and it also reflects the actual movement during disaster recovery and rescue operations. It was developed by Johnson and Maltz 1996 and it is based on random movement with various speeds over time. Mobile nodes choose a random destination and moves with a selected speed between zero to maximum speed (m/sec) toward the selected destination, pause for a specified period and repeat the process. Prior to our simulation, minimum and maximum speed of nodes can be set along with pause time to simulates real deployment scenarios. For static scenarios, nodes are deployed without any mobility metric. The mobility metric implemented in this research represent a mobility scenario with a particular value M as a function of relative motion of nodes as reported by Aschenbruck et al. (2009) and Solmaz and Turgut (2017).

$$M = \frac{1}{|N|} \sum_{i=1}^N \sum_{j=1}^N \frac{1}{T} \int_0^T |V_i(t) - V_j(t)| dt \quad (5-6)$$

Where N denotes the quantity of node pairs in a network, and it is the same as the total number of deployed nodes in a scenario. $V_i(t) - V_j(t)$ represents speed difference at time t between nodes i and j, and T is execution time in seconds.

5.3 Simulation Setup of Network Formation Scenario

The objective of this scenario is to determine the amount of energy dissipated and control overhead during OLSR/DS-OLSR network formation process. This process occurs when OLSR/DS-OLSR broadcast and receive HELLO, TC, MID (OLSR only) and HNA messages. Thus, the scope of each simulation in this scenario is the computation of the energy cost and control overhead of building and maintaining links between devices. The screenshot of the system specification used for the simulation is shown in Figure 5-1.

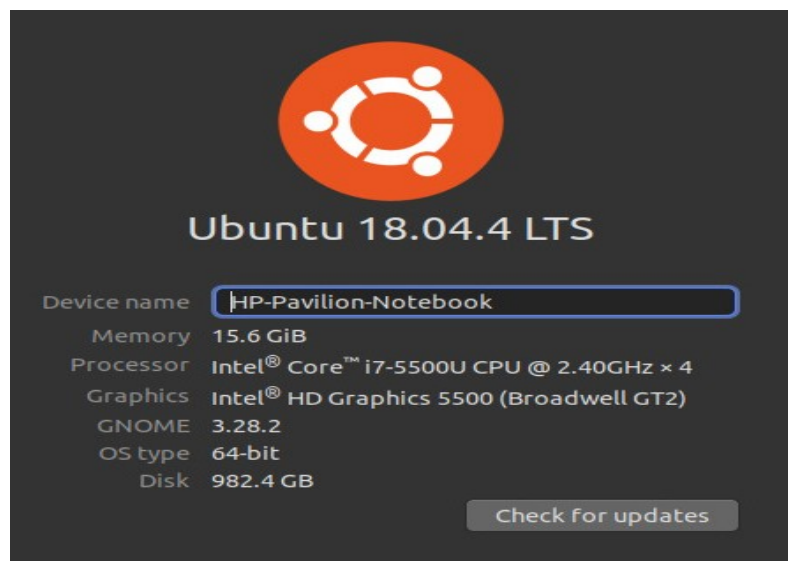


Figure 5-1: Simulation System Specification - Dell Inspiron laptop running Ubuntu 18.04.3.

NS-3 implementation of OLSR revealed a very interesting fact that HELLO messages are broadcasted every two seconds while TC, HNA and MID messages are broadcasted once in 5 seconds. Sending HELLO messages every two seconds ensures each device has known its 1-hop and 2-hop neighbours. Once this is done, MPR selection is computed (as discussed in Section 2.4.5) and TC messages are sent. The control messages are broadcasted for the following reason:

1. HELLO messages are sent by every node in the network at start-up.
2. Only nodes designated as MPR can send TC messages to advertise link states of nodes that are accessible to the MPRs.
3. HNA messages are sent to advertise the presence of a device that is connected to both the local OLSR network and non-OLSR network via multiple interfaces.
4. MID messages are sent to declare the presence of multiple interfaces on a node.

As discussed in Section 4.5, DS-OLSR messages are grouped into Time Slices (TSs) and each TS has a specific messages and duration. The first TS for any device joining the network is the Network Formation Time Slice (NFTS) with the duration of 51 seconds. The NFTS is closely followed by Topology Propagation Time Slice (TPTS) which permits the propagation of TC and HNA messages for the duration of 14 seconds. However, Message Time Slice for transmission of Alert messages is ignored as is out of scope of this scenario. Although it has been fully considered in the implementation of the proposed routing protocol in Disaster Area Network. The simulation environment and parameters are discussed in the following subsection.

5.3.1 OLSR/DS-OLSR Simulation Environment and Parameters for Network Formation Scenario

This section presents the implementation of DS-OLSR in NS-3 simulation environment and discussion of the simulation results that evaluates the amount of energy dissipated and control overhead during OLSR/DS-OLSR network formation process. Figure 5-2 is a screen capture of NS-3 Python Visualiser, showing the simulation environment of the network formation scenario. The simulation was executed for 180 seconds and compared DS-OLSR with OLSRv1 under different nodes density: 10, 50, 100 and 200 nodes in 1000m x 1000m simulation environments as presented in Table 5-1. Simulation time is not the same as real clock time, therefore due to hardware system limitation, all the simulations scenarios in this thesis use the simulation time of 180 seconds to allow monitoring and observability of the network. This is because the 180 seconds simulation time itself takes more than 5 hours to complete. In addition, the 180 seconds simulation time is within the range of simulation time that have been used to evaluate the performance of new systems in the literature (Waheb A. Jabbar et al., 2018), (Saravanan & Nithya, 2020), (Yellanki & Narasimham, 2020). The radio transmission range was set to 50m due to selected Wi-Fi setting and a generic energy model is used for both protocols (Waheb A. Jabbar et al., 2018). Other important parameters are NS-3 Command and Simulation Result File. The NS-3 command is an instruction passes to NS-3 *waf* file which is responsible for executing NS-3 simulation files. The portion of interest in each is the “>” (greater than symbol) this symbol instructs the operating system to direct the output of the results to a file and not on a screen, since the research is interested in using simulation results in spreadsheet graphs.

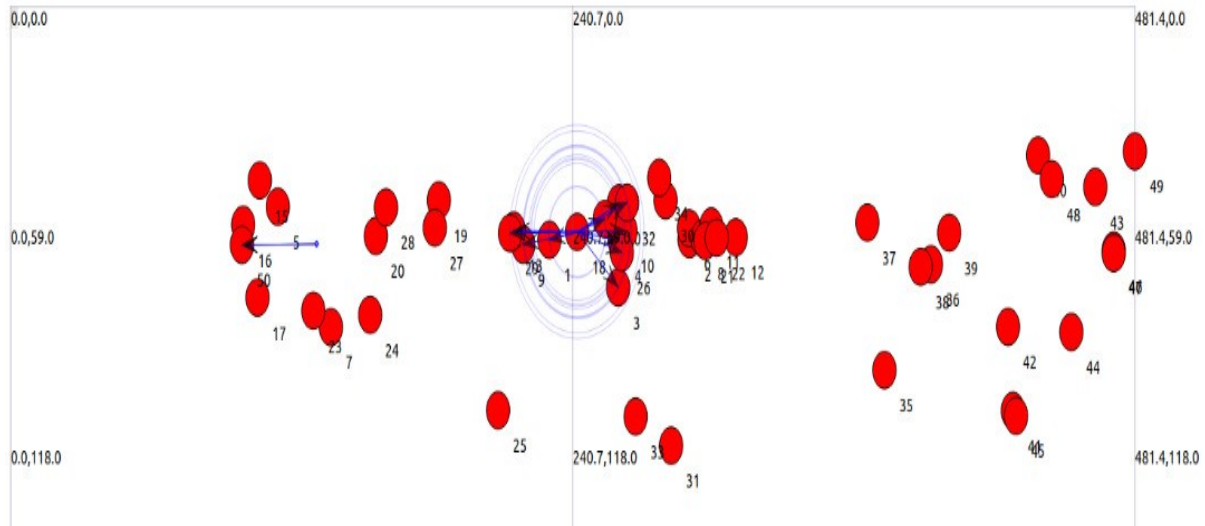


Figure 5-2: NS-3 Python Visualizer showing node placement

Table 5-1: OLSRv1/DS-OLSR Simulation parameters for Network Formation Scenario

Parameter	Value
Simulation Duration	180 seconds
Number of Nodes	10, 50, 100, and 200 nodes
Transmission Range	50 m
Nodes Deployment	Random positioning
Simulation Area	1000 x 1000 metres
Energy Model	Generic: $Tx_{Current} = 0.26A$ $Rx_{Current} = 0.18A$ $Idle_{Current} = 0.148A$ $Sleep_{Current} = 0.0094$ Supply Voltage = 5 Volt
OLSR SPECIFIC PARAMETERS	
Routing	OLSRv1
NS-3 Command	<code>./waf --run "olsr-classic --smsg=0" > olsr-50nodes-50m.txt</code> <code>./waf --run "olsr-classic --smsg=0" > olsr-100nodes-50m.txt</code> <code>./waf --run "olsr-classic --smsg=0" > olsr-100nodes-50m.txt</code>
Simulation Result File	olsr-50nodes-50m.txt olsr-100nodes-50m.txt olsr-200nodes-50m.txt
Control Message Intervals	$HELLO_{Interval} = 2$ seconds, $TC_{Intervals} = 5$ seconds, $MID_{Intervals} = 5$ seconds, $HNA_{Interval} = 5$ seconds
DS-OLSR SPECIFIC PARAMETERS	
Routing	DS-OLSR
NS-3 Command	<code>./waf --run "olsr-ds --smsg=0" > dsolsr-50nodes-50m.txt</code> <code>./waf --run "olsr-ds --smsg=0" > dsolsr-100nodes-50m.txt</code> <code>./waf --run "olsr-ds --smsg=0" > dsolsr-200nodes-50m.txt</code>
Simulation Result File	dsolsr-50nodes-50m.txt dsolsr-50nodes-50m.txt dsolsr-50nodes-50m.txt
Intervals	$HELLO_{Interval} = 1$ seconds, $TC_{Intervals} = 5$ seconds, $HNA_{Interval} = 5$ seconds
Time Slices	NFTS = 44 Seconds, TPTS = (TC = 7 Seconds and HNA = 7 Seconds)

The term after the “>” symbol defines the file where simulation results should be stored, and it is also used as a value for Simulation Result File. Notable difference in OLSR/DS-OLSR simulation parameters are Hello and TC/HNA Messages broadcast time Intervals and Time Slices that allow the messages to be broadcasted in their respective time interval. Unlike OLSR (with intervals of 2,5,5 and 5 seconds), DS-OLSR Hello, TC and HNA messages are broadcasted in the interval of 1, 5 and 5 seconds, respectively, while eliminating MID message as discussed in Chapter 4. Thus, the counter that monitors each TS will update itself every millisecond and seamlessly switches to the next TS at the appropriate time.

5.3.2 OLSR/DS-OLSR Simulation Results for Network Formation Scenario

To analyse the amount of energy dissipated and control overhead during OLSRv1/DS-OLSR network formation processes, the charts in Figures 5-3 and 5-4 compare the mean values of energy consumed and control overhead in total of 10 simulations by OLSRv1 and DS-OLSR when simulating 10, 50, 100 and 200 nodes. Unfortunately, the simulation of 200 nodes using OLSRv1 failed severally due to generation of massive control traffic that cannot be handled by the system. The results evident that DS-OLSR consumed less energy as compared to classical OLSR while setting up and maintaining the network. Consequently, energy dissipation rate for OLSR increases exponentially as the number of nodes in the network increases. This did not come as a surprise because OLSR nodes are always busy broadcasting Hello, TC, HNA and MID messages which in turns consumed energy. On the other hand, DS-OLSR lower energy dissipation can be directly attributed to DS-OLSR Time Slices (TSs) which encapsulated DS-OLSR control messages into their respective TS and the concept of MANET-wide sleep periods. Moreover, DS-OLSR uses the concept of the TSs to achieve low control overhead as compared to classical OLSR in all the three scenarios as presented in Figure 5-4. The routing overhead for OLSR increased badly with increase of nodes in the network. This is because each node broadcast Hello message every 2 second and each Hello message broadcast from one node will be heard by many other nodes in the network. In addition, MPR nodes also transmits TC messages every 5 second until the end of the simulation. The introduction of TSs reduces routing overhead drastically in DS-OLSR which enforces extended idle periods during which the entire network engages in low power listening mode or devices simply power off their transceivers for extended periods, thereby minimises the control overhead and reduces energy consumption.

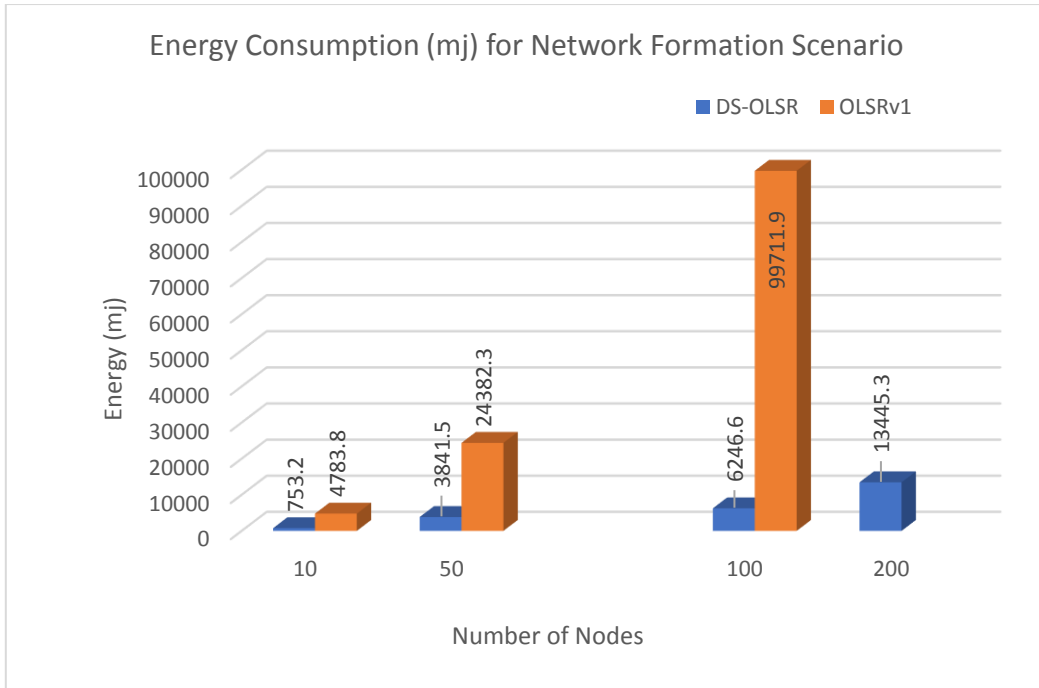


Figure 5-3: Energy Consumption for Network Formation Scenario

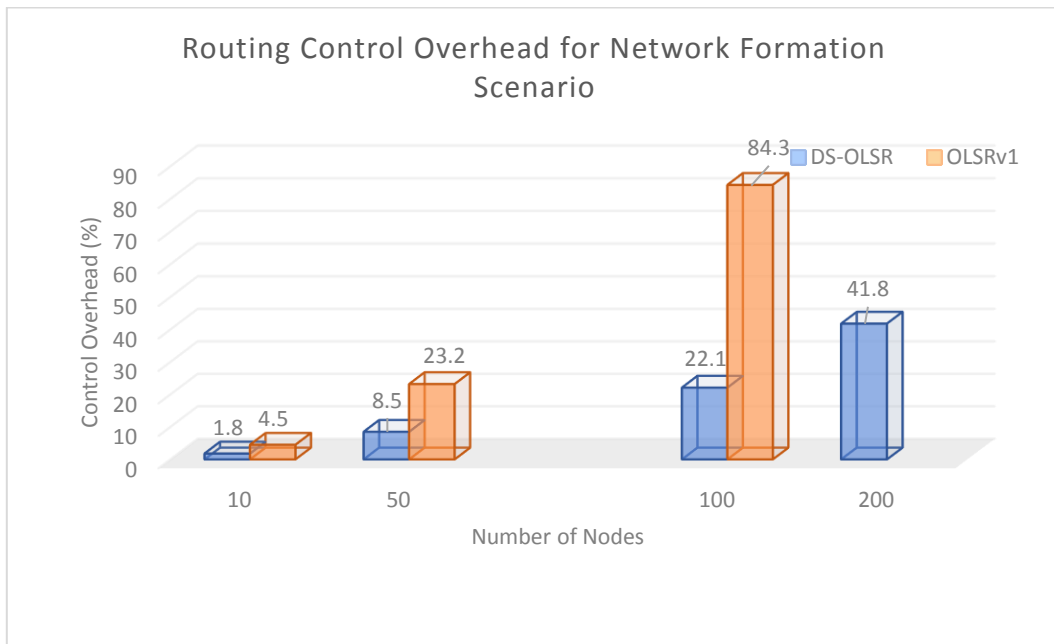


Figure 5-4: Routing Control Overhead for Network Formation Scenario

5.4 Implementation of DS-OLSR in Disaster Area Network

This Section present the implementation of DS-OLSR in Disaster Area Model (Aschenbruck et al., 2009). The disaster area as shown in Figure 5-5 is divided into 5 different sections: Disaster area, Command centre, Treatment area, clearing centre and No-go area, which reflects real life disaster scenario.

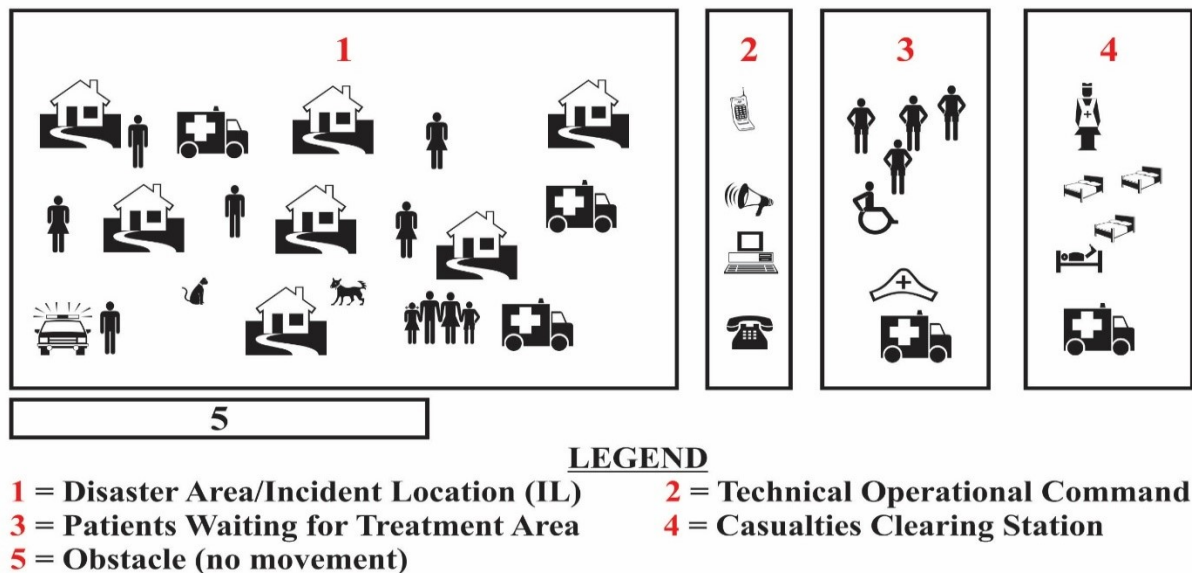


Figure 5-5: Disaster Area Network Model (Aschenbruck et al., 2009)

The results obtained are compared based on selected performance criteria with OLSRv1. First, we discuss the simulation setup and its environment, then highlight the selected performance evaluation metrics. Although, the simulation results are validated using analytical computation, however, in this section we wrap up with only analysis of the simulation results of DS-OLSR in comparison with OLSRv1 under the same parameters.

5.4.1 Simulation Setup for Disaster Area Network

As mentioned earlier, the performance of the proposed DS-OLSR is evaluated by simulations in NS-3.26. NS-3 is a discrete-event network simulator that manages several events using programming codes that are scheduled to execute at a specific simulation period. Figure 5-6 presents NS-3 python visualizer showing the implementation of the proposed DS-OLSR protocol. The simulation for both static and mobility scenarios and compared with OLSRv1 under different nodes density: 10, 50, 100 and 200 nodes in 1000m x 1000m simulation environments as presented in Table 5-2.

The radio transmission range was set to 50m due to selected Wi-Fi setting and a generic energy model is used for both protocols (Waheb A. Jabbar et al., 2018). As regards to mobility models, this research considered Random Way Point (RWP) with speed range of pedestrian (1m/s – 2m/s) (Aschenbruck et al., 2009).

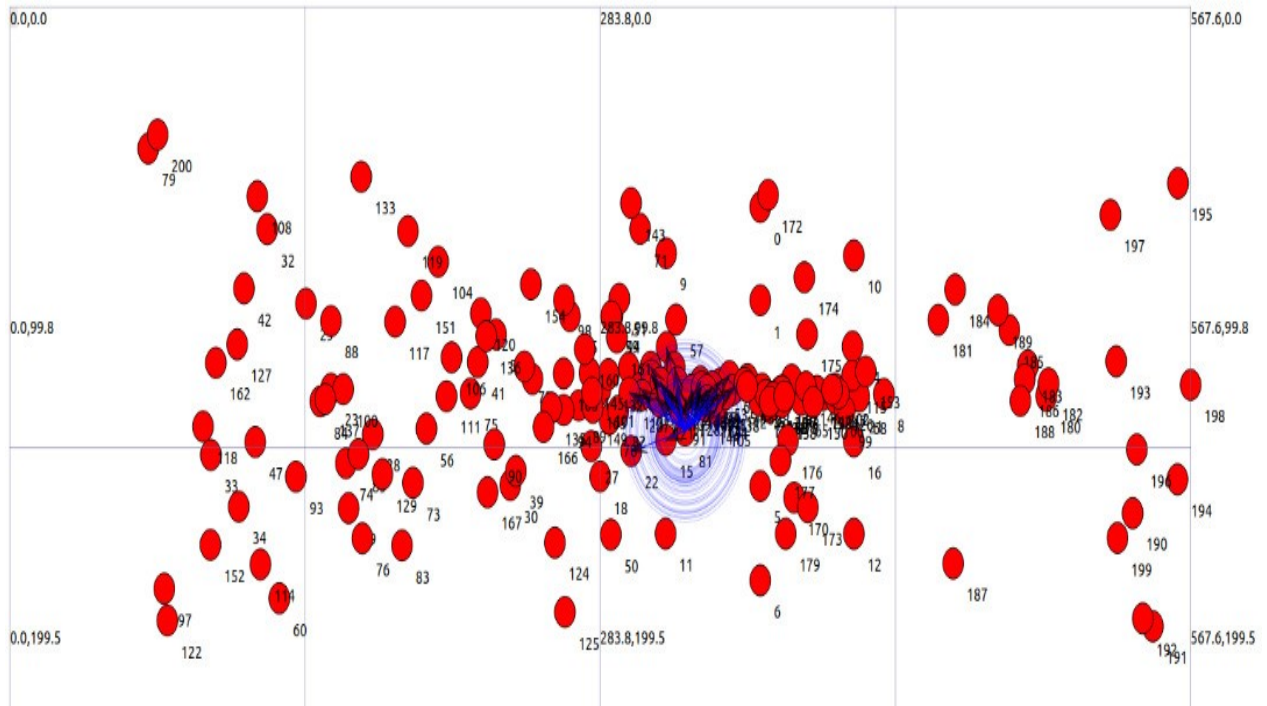


Figure 5-6: NS-3 Python Visualizer showing node placement.

Table 5-2: Simulation parameters for Disaster Area Network

Parameter	Value
Simulation Duration	180 seconds
Number of Nodes	10, 50, 100, and 200 nodes
Transmission Range	50 m
Nodes Deployment	Random positioning
Mobility Model	Random Way point, Min Speed 0, Max Speed 1m/s - 2m/s, and 5m/s – 12m/s, Pause Time 10s
Simulation Area	1000 x 1000 metres
Energy Model	Generic: $Tx_{Current} = 0.26A$ $Rx_{Current} = 0.18A$ $Idle_{Current} = 0.148A$ $Sleep_{Current} = 0.0094$ Supply Voltage = 5 Volt
Packet Size	512bytes
Routing Protocol	DS-OLSR/OLSRv1

This is because victims running at high speed during disaster recovery and rescue operation will result to high risk of injury. However, to accommodate the speed of rescuers who might be using vehicles, we also evaluate the proposed scheme with the speed range of vehicles (5m/s – 12m/s). The simulation was generally set up according to parameters used in Waheb A. Jabbar et al. (2018) except those parameters that are DS-OLSR specific.

5.4.2 Results Analysis for Disaster Area Network

The overall performance of the proposed DS-OLSR is thoroughly investigated and compared with OLSRv1 in disaster area model based on the simulation parameters mentioned earlier. The mean values of the energy dissipated in total of 10 simulations by nodes in both static and mobility scenarios were evaluated in comparison to the energy dissipated using OLSRv1 under the same parameters. The total packet delivery is also evaluated to ascertain the percentage of successfully transmitted packets against the number of packets sent in the networks. Furthermore, to compare the time required for a packet to be successfully transmitted from source to destination, we equally evaluated average end-to-end delay. Network size of 10, 50, 100 and 200 nodes and different nodes speed (Pedestrian: 1m/s – 2m/s and Vehicles: 5m/s – 12m/s (Aschenbruck et al., 2009)) has been selected as parameters in this study to evaluate the proposed scheme as it widely used to evaluate simulation studies in MANETs. When the network size and node speeds increase, the scalability of the proposed routing protocol will be evaluated to prove its performance. The simulation of 200 nodes using OLSRv1 failed severely due to generation of massive control traffic that cannot be handled by the system. However, in future the research intends to use a system with a better resource to compare the performance of the OLSRv1 using 200 nodes with DS-OLSRMP.

Figures 5-7, 5-8 and 5-9 represent mean values of energy dissipated in total of 10 simulations using DS-OLSR and OLSRv1 for 10, 50, 100 and 200 nodes in both static and mobility simulation scenarios. It is obvious from the simulation results that OLSRv1 reported high energy consumption as compared to DS-OLSR in all scenarios and of course, the energy consumption rate for the OLSRv1 increases exponentially with increased nodes in the networks. This huge energy consumption by OLSRv1 is attributed by continuous generation of massive control overhead traffic and constantly busy routing control messages in the background (regardless of user messages) as equally reported in Qin et al. (2016), the major energy consumption of their experimental work. The energy conservation by DS-OLSR is

because of Time Slices (TSs) that confine messages into their respective time thereby prevents control message retransmission as discussed in Chapter 4. It can also be observed from the simulation results that DS-OLSR demonstrates suitability for dense network as the energy consumption rate is not largely affected with the increase of nodes in the network. This is attributed to the fact that, DS-OLSR TSs plays an important role in reducing control overhead with associated energy consumption by enforces extended idle periods during which the entire network engages in low power listening mode.

To examine the energy conservation of the proposed routing protocol in real life disaster mobility scenarios, we evaluated the proposed technique under two mobility speeds: Pedestrian (1m/s – 2m/s) and Vehicles (5m/s – 12m/s) (Aschenbruck et al., 2009). Figures 5-8 and 5-9 reveals that the proposed DS-OLSR achieves lowest energy consumption in both pedestrian and vehicle speeds irrespective of the number of nodes. This is because DS-OLSR utilizes energy saving mechanism that is not available OLSR protocol. However, the performance of the DS-OLSR is slightly affected by the implementation of mobility metrics, particularly for 5m/s – 12m/s speed as the energy consumption increases due high movement of nodes in the networks. Although it is still reasonable considering the number of successful transmitted packets and compared to multipath routing protocols in (Nishiyama et al., 2014) and (Waheb A. Jabbar et al., 2018). In a general term, nodes changes position in mobility scenarios and of course, their routes randomly change over time, which requires further route calculation and complexity on topology sensing. In addition, MPR nodes expends more energy than normal nodes as they forward control and data packets to the entire network on behalf of their electors.

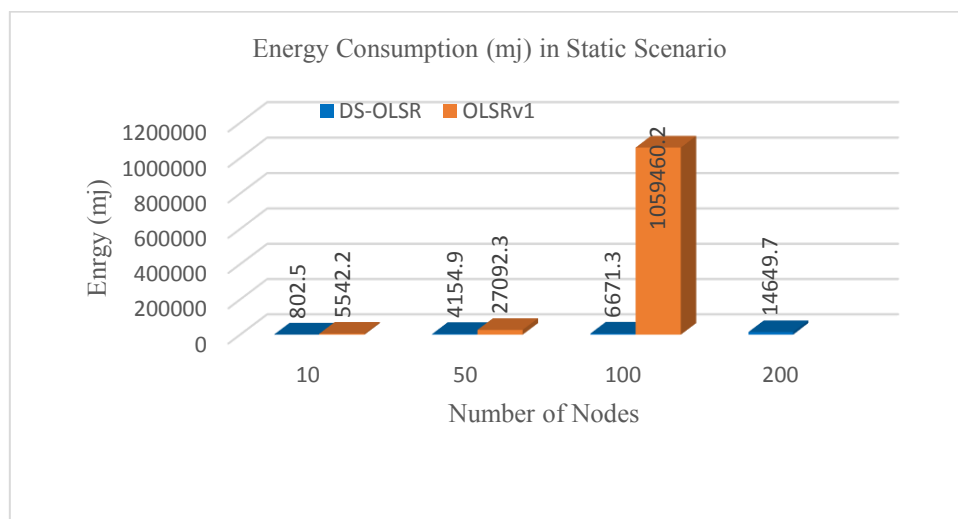


Figure 5-7: Energy Consumption for Disaster Area Network in Static Scenario

However, DS-OLSR take advantage of its TSs techniques which confines messages in their respective time and extended low power mode thereby minimises routing overhead and extends life spans of individual nodes and entire MANET a large.

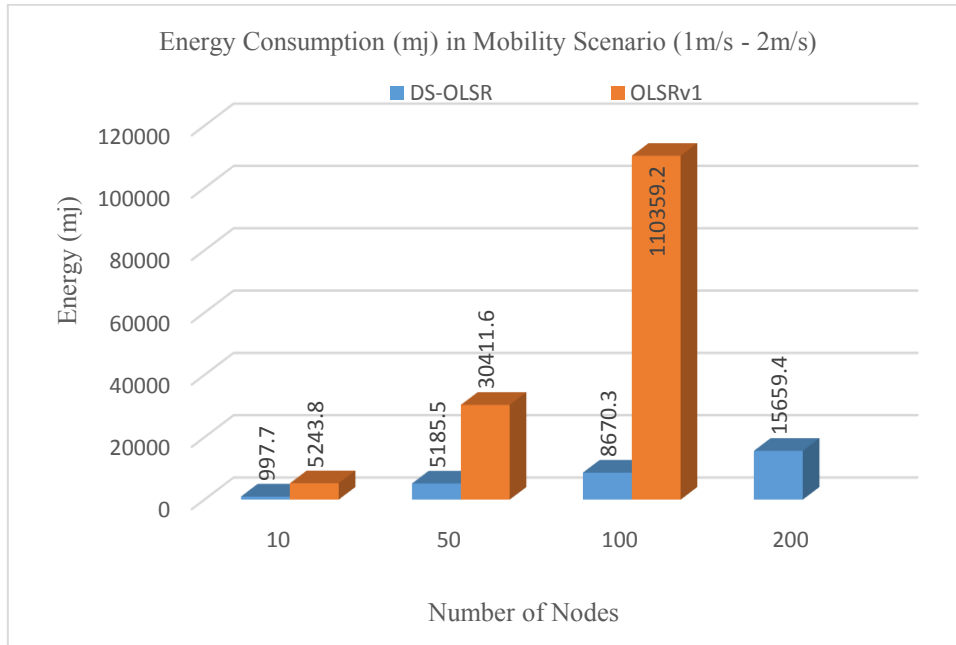


Figure 5-8: Energy Consumption for Disaster Area Network in Mobility Scenario (1m/s – 2m/s)

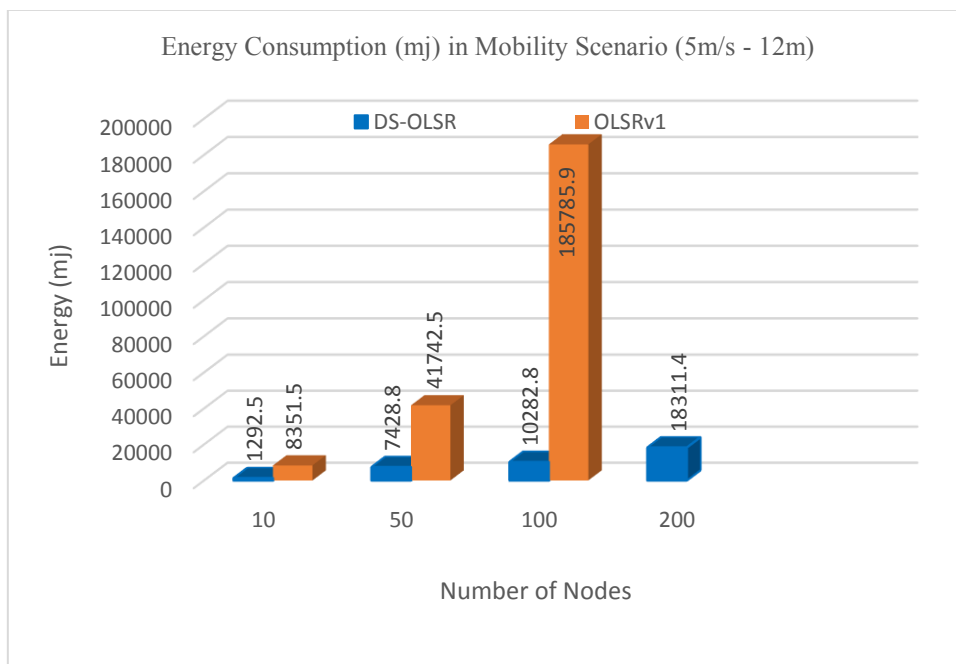


Figure 5-9: Energy Consumption for Disaster Area Network in Mobility Scenario (5m/s – 12m/s)

Figures 5-10, 5-11 and 5-12 represent mean values of control overhead in total of 10 simulations for DS-OLSR and OLSRv1, when simulating 10, 50, 100 and 200 nodes in both static and mobility scenarios.

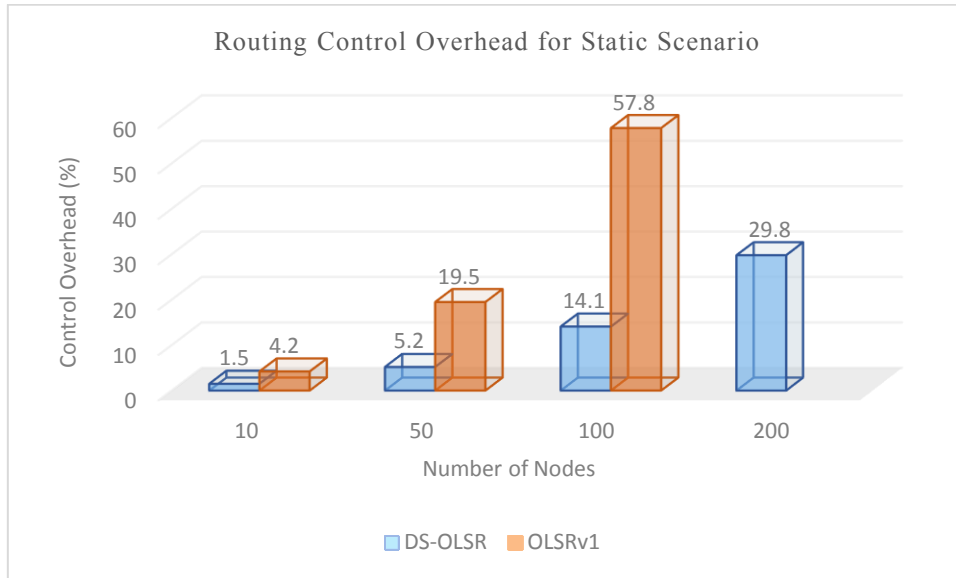


Figure 5-10: Routing Control Overhead for Disaster Area Network in Static Scenario

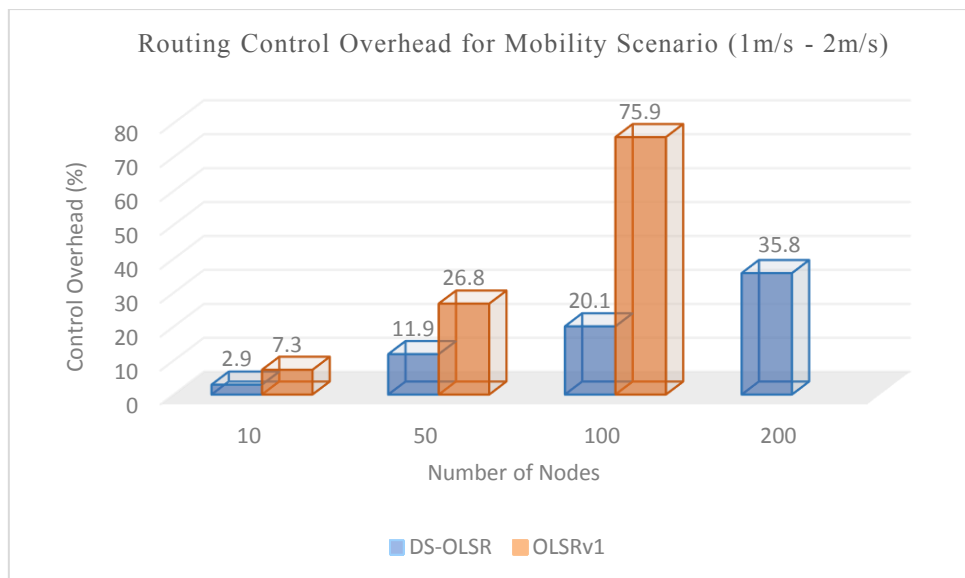


Figure 5-11: Routing Control Overhead for Disaster Area Network in Mobility Scenario (1m/s – 2m/s)

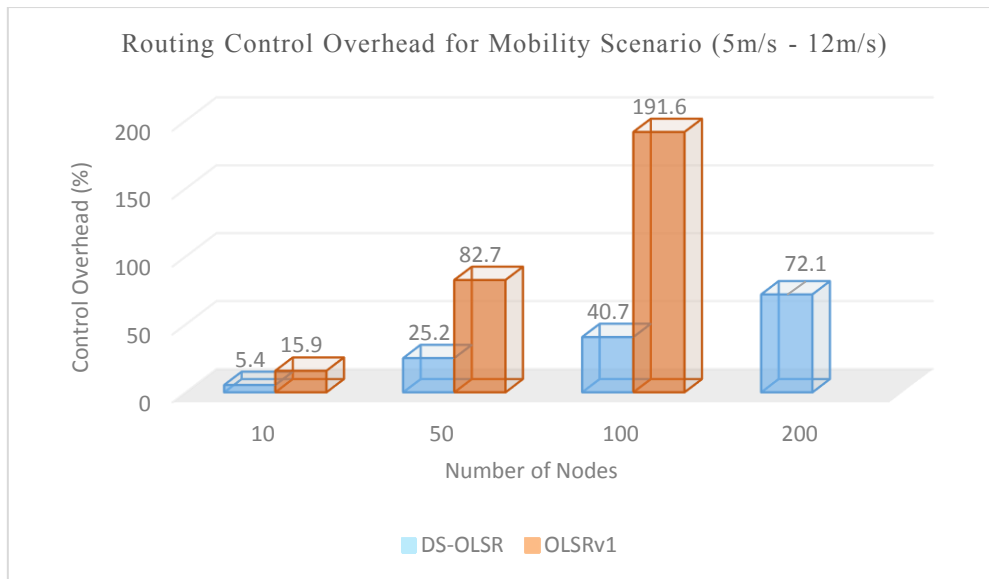


Figure 5-12: Routing Control Overhead for Disaster Area Network in Mobility Scenario (5m/s – 12m/s)

It can observe the superiority of DS-OLSR in all situations as it returns the lowest control overhead in all scenarios, regardless of nodes mobility speed and network size. This because of using Time Slices (TSs) encapsulates control message such as Hello, TC, and of course ALERT messages into their respective TSs which in turns reduces retransmission of fail packets caused by message collision. In addition, DS-OLSR eliminates the use of MID message as contained in OLSRv1 which is equally contributed to the high control overhead recorded by OLSRv1. Moreover, DS-OLSR maintains routing information for a longer time as explained in (Aliyu, Tadruri, Hope, & Halilu, 2020), thereby reduce continuous rebroadcasting of control messages as required by OLSR in every 2 seconds (Hello) and 5 seconds (TC, HNA, and MID).

Figures 5-13, 5-14, and 5-15 represent mean values of packet delivery ratio in total of 10 simulations for DS-OLSR and OLSRv1 when simulating 50, 100 and 200 nodes in both static and mobility scenarios. It was observed from the simulation results that OLSRv1 delivered less packets as compared to OLSRv1 in all scenarios. In addition, the packet delivery ratio for OLSRv1 drastically reduced with the introduction of high mobility (5m/s – 12m/s) in the networks, thereby resulting to huge increase in their end-to-end delay and control overhead. The packet delivery ratio of both protocols is very similar in the simulation of mobility scenario (1m/s – 2m/s) with 50 nodes, were nodes changes position slowly. However, DS-OLSR demonstrated efficiency in packet delivery in the simulation of dense networks as the packets delivered in the simulation of 100 nodes (85.5%) is more than what have been delivered in the simulation of 50 nodes (84.3%) using OLSR.

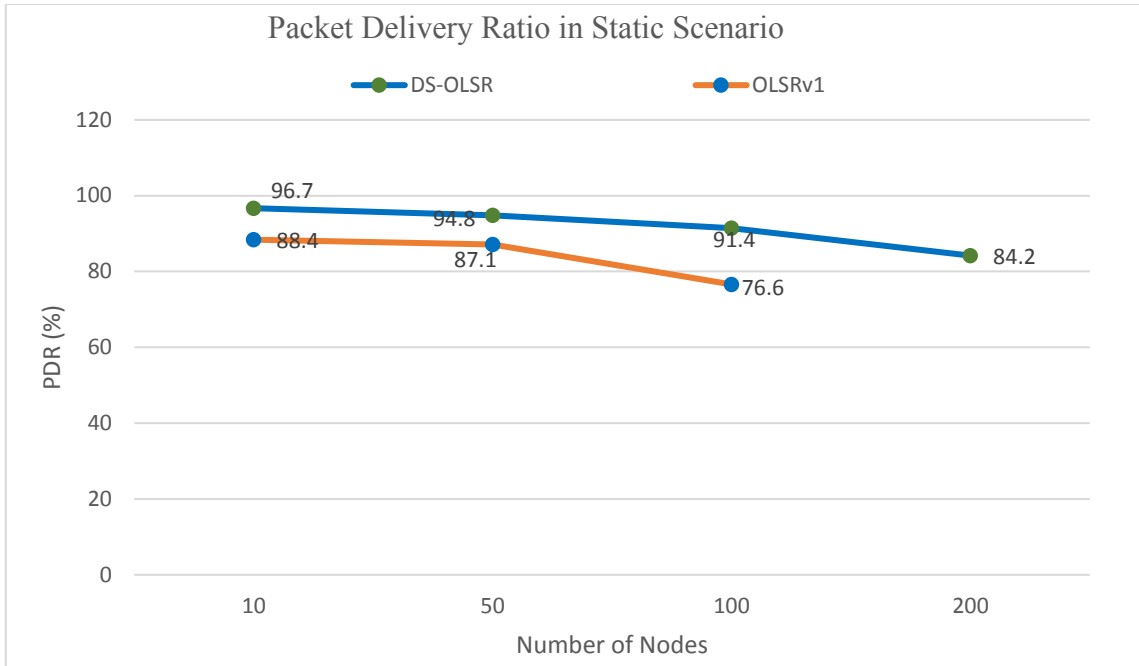


Figure 5-13: Packet Delivery Ratio for Disaster Area Network in Static Scenario

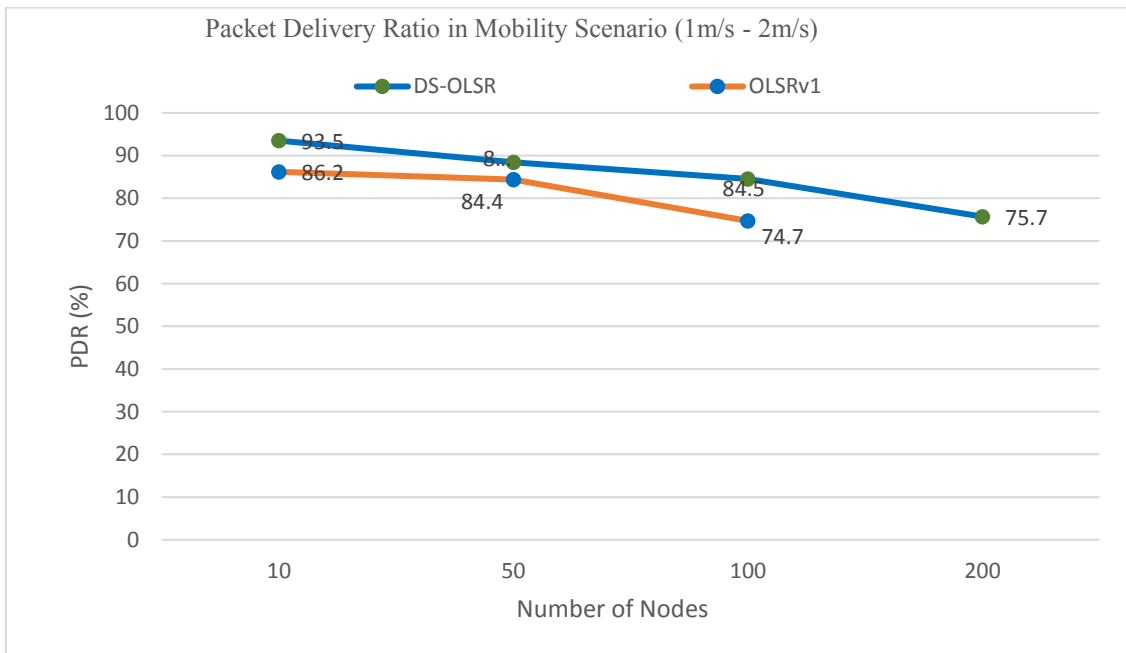


Figure 5-14: Packet Delivery Ratio for Disaster Area Network in Mobility Scenario (1m/s – 2m/s)

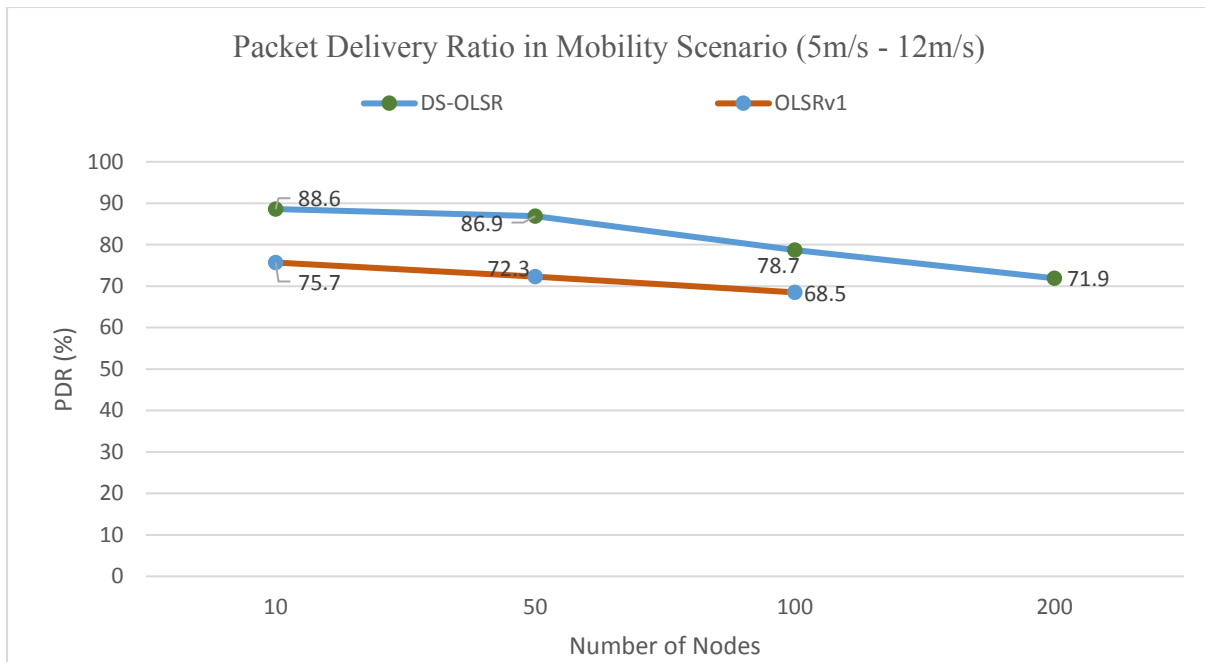


Figure 5-15: Packet Delivery Ratio for Disaster Area Network in Mobility Scenario (5m/s – 12m/s)

Similarly, the packet delivered in the simulation of 200 nodes (76.2%) using DS-OLSR is equally higher than what have been delivered in the simulation of 100 nodes (75%) using OLSR. This improvement is attributed to the concept of time slices which confines messages in their respective time. Although, the PDR for DS-OLSR decreases slightly with increase of node speeds (5m/s – 12m/s) in the networks. However, the PDR is far better than what was obtained in a similar OLSR optimisation research in (Prakash, Philip, Paulus, & Kumar, 2020) (Waheb A Jabbar et al., 2014). The DS-OLSR results confirms how the concept of TSs improves link quality by eliminating crosstalk and reduced funnel effect without compromising packets delivery in all the scenarios.

Figures 5-16, 5-17 and 5-18 represent mean values of end-to-end delay in total of 10 simulations for the DS-OLSR and OLSRv1 when simulating 50, 100 and 200 nodes in both static and mobility scenarios. It is obvious from the figures that the conventional version of OLSR reported higher end-to-end delay in all scenarios as compared to DS-OLSR. In addition, the end-to-end delay the OLSRv1 increases exponentially with increased of nodes in the networks. This is due to connection errors or temporary loss of routes to other parts of the network, often caused by packet collision, thereby resulting to massive increase in generation control packets, subsequently increased end-to-end delay in all the simulated scenarios. The end-to-end delay for DS-OLSR did not come as a surprise, because both schemes employed

the techniques of TSs that decreases the possibility of link failure and maintain routing information for a longer time discussed in (Aliyu et al., 2020). Therefore, data packets are not sent to unreliable routes, thereby reducing the delay time required for retransmissions.

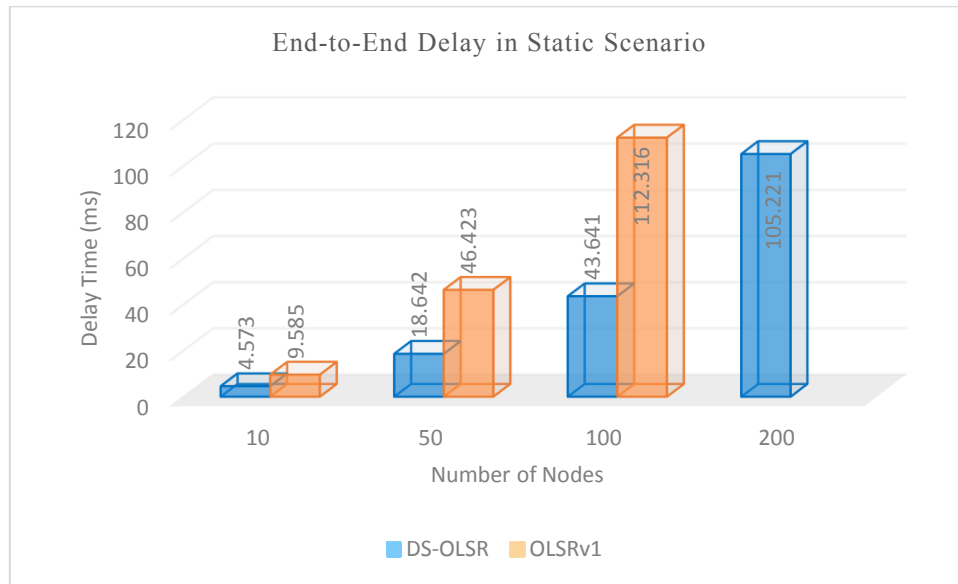


Figure 5-16: End-to-End Delay for Disaster Area Network in Static Scenario

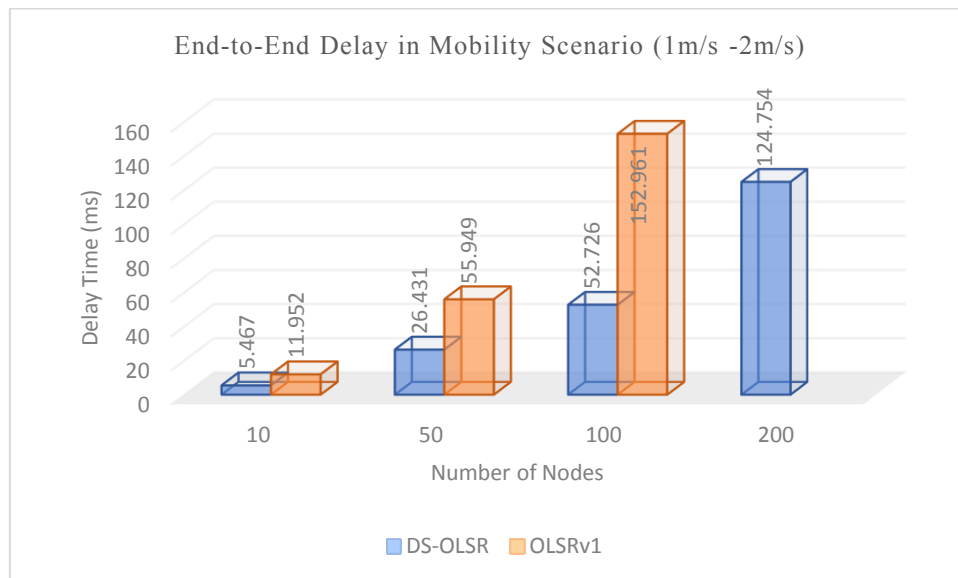


Figure 5-17: End-to-End Delay for Disaster Area Network in Mobility Scenario (1m/s – 2m/s)

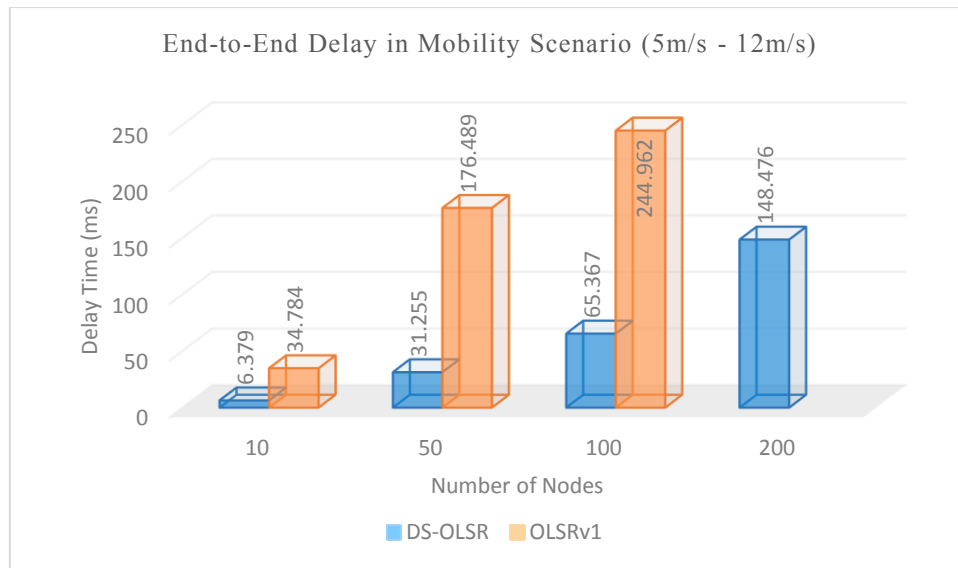


Figure 5-18: End-to-End Delay for Disaster Area Network in Mobility Scenario (5m/s – 12m/s)

5.5 Chapter Summary

In this Chapter, the implementation of the proposed D-OLSR is presented in two independent scenarios namely: Simulation of Network Formation and Disaster Area Network (Aschenbruck et al., 2009). The first simulation was conducted to determine the amount of energy dissipated and control overhead during OLSR/DS-OLSR network formation process, and therefore it is only energy consumption and control overhead that has been analysed. However, the second simulation is to evaluate the performance of the proposed scheme in a disaster related scenario as proposed by Aschenbruck et al. (2009), which reflects real life disaster scenario. Thus, in addition to energy consumption and control overhead, this scenario considered performance metrics including packet delivery ratio and end-to-end delay. All scenarios were simulated using 10, 50, 100 and 200 nodes. All DS-OLSR simulations executed seamlessly within a single terminal session as in Figure 5-19. However, the simulation of 200 nodes using OLSRv1 failed severally due to generation of massive control traffic that cannot be handled by the system. The reason for OLSR resource hungry execution in OLSR simulations with 200 nodes is attributed to the massive generation of OLSR routing overhead and NS-3 discrete event simulation mode of operations. Linux uses **.bash_history** file as a repository where every command typed in Linux terminal sessions are saved. Users can retrieve previous commands one at a time by pressing the navigation up arrow key.

The overall performance of the proposed DS-OLSR is thoroughly investigated and compared with OLSRv1 in network formation and disaster area model scenarios. The simulated scenarios

were implemented in both static and mobility models. As regards to mobility models, the proposed scheme considered Random Way Point (RWP) with speed range of pedestrian (1m/s – 2m/s) (Aschenbruck et al., 2009). This is because victims running at high speed during disaster recovery and rescue operation will results to high risk of injury. However, to accommodate the speed of rescuers who might be using vehicles, we also evaluate the proposed scheme with the speed range of vehicles (5m/s – 12m/s). Energy dissipated by nodes in both static and mobility scenarios were evaluated in comparison to the energy dissipated using OLSRv1 under the same parameters. The total packet delivery is also evaluated to ascertain the percentage of successfully transmitted packets against the number of packets sent in the networks. Furthermore, to compare the time required for a packet to be successfully transmitted from source to destination, we equally evaluated average end-to-end delay. All the simulation results indicates that DS-OLSR performs better than OLSRv1. This performance is attributed to the concept of TSs and elimination of MID messages which confines control messages into their respective, thereby improving link quality by eliminating crosstalk and reducing funnel effect without compromising QoS performance in all the scenarios. The next Chapter presents a novel message prioritisation technique for DS-OLSR that prioritises message based on nodes Battery life and evaluates the performance of the scheme with DS-OLSR, OLSRv1 and OLSRv2.

```

cd repos/ns-3/ns-3-dev
./waf --run "olsr-ds --smsg=0" > dsolsr-20nodes-200m.txt
./waf --run "olsr-ds-auto --smsg=0 --numNodes=20 --distance=100" > dsolsr-20nodes-100m.txt
./waf --run "olsr-ds-auto --smsg=0 --numNodes=20 --distance=50" > dsolsr-20nodes-50m.txt
./waf --run "olsr-ds-auto --smsg=0 --numNodes=50 --distance=200" > dsolsr-50nodes-200m.txt
./waf --run "olsr-ds-auto --smsg=0 --numNodes=50 --distance=100" > dsolsr-50nodes-100m.txt
./waf --run "olsr-ds-auto --smsg=0 --numNodes=50 --distance=50" > dsolsr-50nodes-50m.txt
./waf --run "olsr-ds-auto --smsg=0 --numNodes=100 --distance=200" > dsolsr-100nodes-200m.txt
./waf --run "olsr-ds-auto --smsg=0 --numNodes=100 --distance=100" > dsolsr-100nodes-100m.txt
./waf --run "olsr-ds-auto --smsg=0 --numNodes=100 --distance=50" > dsolsr-100nodes-50m.txt
exit

```

Figure 5-19: DS-OLSR simulation commands retrieved from .bash_history file

```

cd repos/ns-3/ns-3-dev
./waf --run "olsr-classic --smsg=0" > olsr-20nodes-200m.txt
./waf --run "olsr-classic-auto --smsg=0 --numNodes=20 --distance=50" > olsr-20nodes-50m.txt
./waf --run "olsr-classic-auto --smsg=0 --numNodes=20 --distance=100" > olsr-20nodes-100m.txt
./waf --run "olsr-classic-auto --smsg=0 --numNodes=50 --distance=200" > olsr-50nodes-200m.txt
./waf --run "olsr-classic-auto --smsg=0 --numNodes=50 --distance=100" > olsr-50nodes-100m.txt
./waf --run "olsr-classic-auto --smsg=0 --numNodes=50 --distance=50" > olsr-50nodes-50m.txt
exit
cd repos/ns-3/ns-3-dev
./waf --run "olsr-classic-auto --smsg=0 --numNodes=100 --distance=200" > olsr-100nodes-200m.txt
./waf --run "olsr-classic-auto --smsg=0 --numNodes=100 --distance=100" > olsr-100nodes-100m.txt
exit
cd repos/ns-3/ns-3-dev
./waf --run "olsr-classic-auto --smsg=0 --numNodes=100 --distance=50" > olsr-100nodes-50m.txt
reboot

```

Figure 5-20: OLSRv1 simulation commands retrieved from .bash_history file

Chapter 6

Disaster Scenario Optimized Link State Routing Protocol and Message Prioritization (DS-OLSRMP)

6.1 Introduction

DS-OLSR achieved drastic reduction in control messages overheads and energy consumption as compared to classic OLSR through the introduction of originator ID (holds smart phones' mobile number), ALERT message and Time Slices (TSs). TSs partition messages into their respective TS. Thus, control messages such as Hello, TC, HNA and ALERT (a new message type created for DS-OLSR) have their respective TSs, during which only a specific message type is permitted by DS-OLSR devices. However, low battery devices often experience quick power failure which restrict their ability to communicate for longer time during rescue operations. Therefore, adding ALERT message prioritization to DS-OLSR will further improve energy conservation, extend lifespan of low battery energy devices and improves mental state of victims with the low battery devices. This will equally prevent such victims from overwhelming the network with messages as their device battery energy dwindles. Building on our effort (Aliyu et al., 2020), this Chapter examines DS-OLSR ALERT message and proposes an innovative solution called Disaster Scenario Optimised Link State Routing Protocol and Message Prioritisation (DS-OLSRMP) that will prioritize messages based on device Battery life to improve energy efficiency and packet delivery during disaster recovery and rescue operations.

The Chapter is presented as follow: Section 6.2 describes DS-OLSRMP structure and main features highlighting the proposed modifications to Alert message and implemented models. Section 6.3 presents simulation setup and results analysis. Finally, Section 6.4 wraps up the Chapter with summary of the Chapter.

6.2 Proposed DS-OLSRMP Structure and Main Features

Prioritization is a famous technique that cut across different discipline. It is used in Disaster Scenario Optimized Link State Routing (DS-OLSR) Alert message to prioritized message delivery based on node's Battery life. Disaster Scenario Optimized Link State Routing and Message Prioritization (DS-OLSRMP) further extends DS-OLSR's superior energy saving

capabilities over classic OLSR (Aliyu et al., 2020), by extending the lifespan of communication devices with low battery energy. In addition, DS-OLSRMP in disaster environment will likely improve victim’s mental state by quickly responding to messages sent by low battery devices. Such rapid response may include a proposed rescue time, or where such victims should gather to receive supplies or shelter. Message prioritization requires MPR to send messages and deliver messages status reports based on the Battery life of each device. Prioritization process is shown in Figures 6-1 through 6-4.

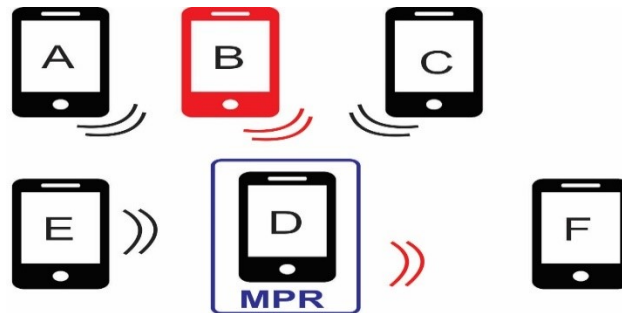


Figure 6-1: Each device sends ALERT message for routing to Device F via MPR D. Device B Battery life is low hence ALERT message from Device B is prioritized

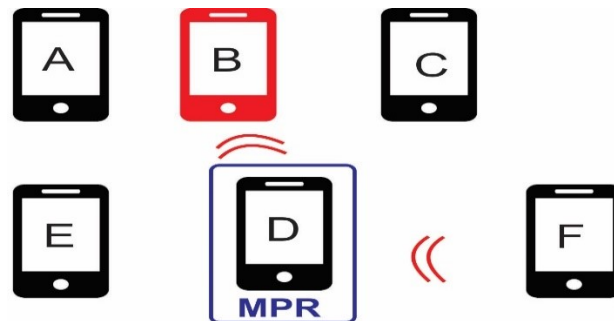


Figure 6-2: MPR D equally prioritizes response from Device F to Device B for delivery

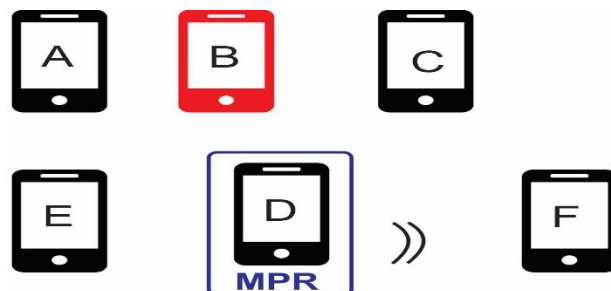


Figure 6-3: Once Device B messages are delivered, MPR D forwards remaining messages from Devices A, C and E to Device F

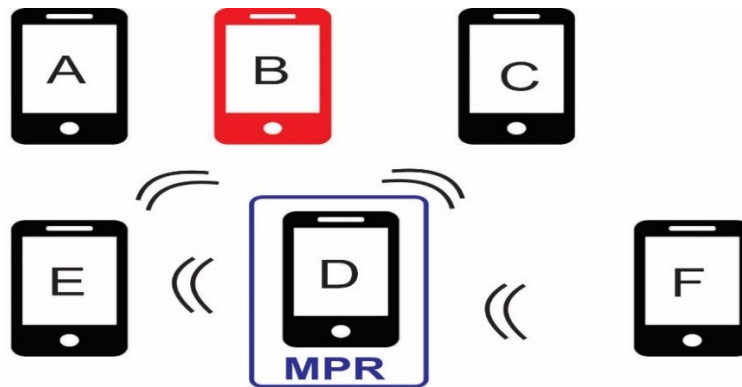


Figure 6-4: Finally, response from Device F is forwarded to Devices A, C and E by MPR D

6.2.1 ALERT Message Packet Format Modification

The proposed DS-OLSRMP modifies Alert message packet format as discussed in (Aliyu et al., 2020), to support message prioritization through the introduction of two new fields, namely priority and status fields as presented in Table 6-1 The new fields of the ALERT message are discussed in the following sub-sections.

Table 6-1: Improvement to Alert Message Packet Format

0										1										2										3			
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1		
Destination										Message Size										Priority										Status			
Destination Address																																	
Destination Phone Number																																	
1st Octet										2nd Octet										3rd Octet										4th Octet			
										:										:													
										:										:													
										:										:													
37th Octet										38th Octet										39th Octet										40th Octet			

6.2.1.1 Priority

Priority field stores the message priority based on the Battery life of the devices. The Battery life of any device running DS-OLSR can be retrieved from a new table called **device info set** (Aliyu et al., 2020). DS-OLSR messaging application periodically capture and stores the

Battery life of the communication devices (Aliyu et al., 2020), this allows the device info set to provide the most recent Battery life on demand.

6.2.1.2 Status

Status field provides message status to nodes that are expected to route messages between the sender and the recipient. A value of 1 inform nodes that the message originates from the sender and is destined to the recipient. While a value of 2 informs routing nodes that the message is a status notification (an acknowledgment) of an earlier message delivered to recipient from a sender.

Figure 6-5 presents a sample value for priority and status for ALERT message from sender B to destination F. Device B Battery life is between 1% and 33%. Hence its ALERT message has a priority value of 1, which translates to **critical priority**. The message is routed via MPR D to the target recipient (Device F).

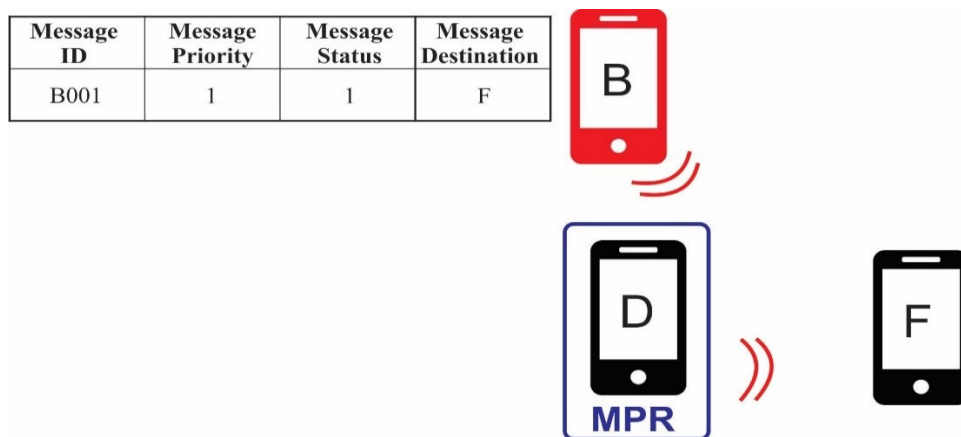


Figure 6-5: Sample values for priority and status fields for new ALERT message from sender B to recipient F

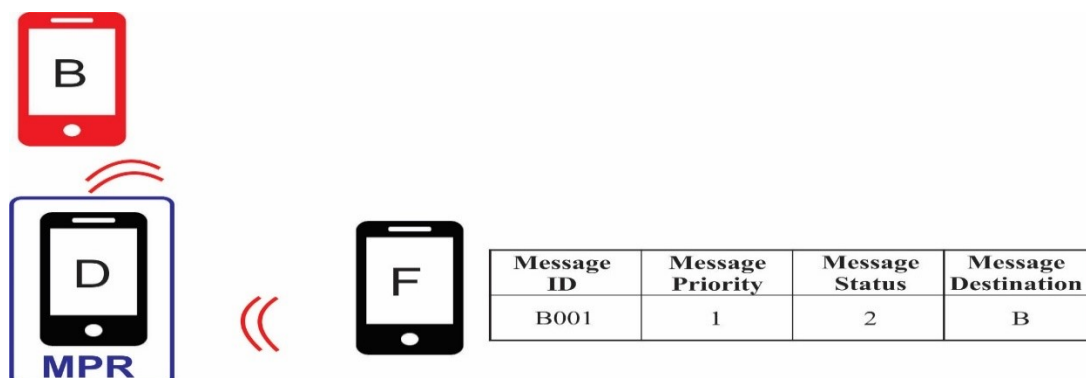


Figure 6-6: Sample values for priority and status fields for message status notification from recipient F to sender B

Device F response is captured in Figure 6-6. The response simply echoes back the message received, with **status** field set to **2** to connote the message is a status notification report or an acknowledgement of previously received ALERT message.

6.2.2 Implemented Models

In DS-OLSRMP, nodes use different models to measure the required parameters for executing the task of send, relay, and receive. The parameters are used by DS-OLSRMP to prioritize both message delivery and message status notification for devices with low battery energy. The research initially implemented the proposed scheme in a simulation environment based on disaster area model as proposed by Aschenbruck et al. (2009), and validated it using mathematical model. Network topology, number of nodes and other relevant metric (such as number of packets, energy model and mobility speed) are defined in different scenarios with an implementation of DS-OSLSMP routing protocol. A brief description of the implemented models as relates to the proposed modifications are discussed in the following sub-sections.

6.2.2.1 ALERT Message Prioritization model

As mentioned earlier, Alert message prioritization prioritizes both message delivery and message status notification for devices with low battery energy. Message status notification is an integral part of DS-OLSRMP prioritization process for search and rescue operations. This feature prevents victims from flooding the network with ALERT messages, especially when such victims are experiencing a dire emergency which unduly increases their panic level because their communication device battery energy is running low. Alert Message prioritization based on device Battery life $P(x_i)$ is given as:

$$P(x_i) = \begin{cases} x_1, & 1 \leq x_1 \leq 33 \\ x_2, & 33 < x_2 \leq 67 \\ x_3, & 67 < x_3 \leq 83 \\ x_4, & 83 < x_4 \leq 100 \end{cases} \quad (6-1)$$

Where x_1 , x_2 , x_3 and x_4 represent Critical, High, Medium, and Low priority nodes with their corresponded Battery life percentage. Applicable priorities based on Battery lives are enumerated in Table 6-2:

Table 6-2: Applicable Message Priorities and their Values

PRIORITY VALUE	PRIORITY DESCRIPTION	Device's Battery life (%)
1	Critical	1 – 33
2	High	33.1 – 67
3	Medium	67.1 – 83
4	Low	83.1 – 100

Algorithm 4.1 : Priority Decision

```

using namespace std;
int main()
{
float batteryLevel = DeviceInfo.GetBatteryLevel();
string priority;
if (batteryLevel >= 1 && batteryLevel <= 100)
{
    if (batteryLevel < 33)
    {
        cout << "Battery life is critical \n";
        priority = "critical";
    }
    else if (batteryLevel <= 67)
    {
        cout << "Battery life is high priority \n";
        priority = "high";
    }
    else if (batteryLevel <= 83)
    {
        cout << "Battery life is medium priority \n";
        priority = "medium";
    }
    else
    {
        cout << "Battery life is low prioritylow \n";
        priority = "low";
    }
}
else
{
    cout << "Battery life must be between 1 and 100 \n";
}
return 0;
}

```

The Battery life of any device running DS-OLSR can be retrieved from a new table called **device info set** (Aliyu et al., 2020) In DS-OLSRMP, the remaining Battery lives are classified according to their respective priority and attached in the priority field of ALERT message packet. Algorithm 1 presents the process of determine the priority class of nodes based on remaining Battery life percentage.

MPRs nodes are responsible for ALERT Message prioritization. ALERT messages collated by the MPRs are sorted based on battery energy level of each sending device. Figure 6-7 presents messaging prioritization process. Note that, MPR devices ensure critical priority devices send messages and receives status notification on such messages before other priorities (high, medium, and low priority nodes). This approach prevents such victims from overwhelming the network with messages as their device battery energy dwindles, thus reduces the overall traffic of the network.

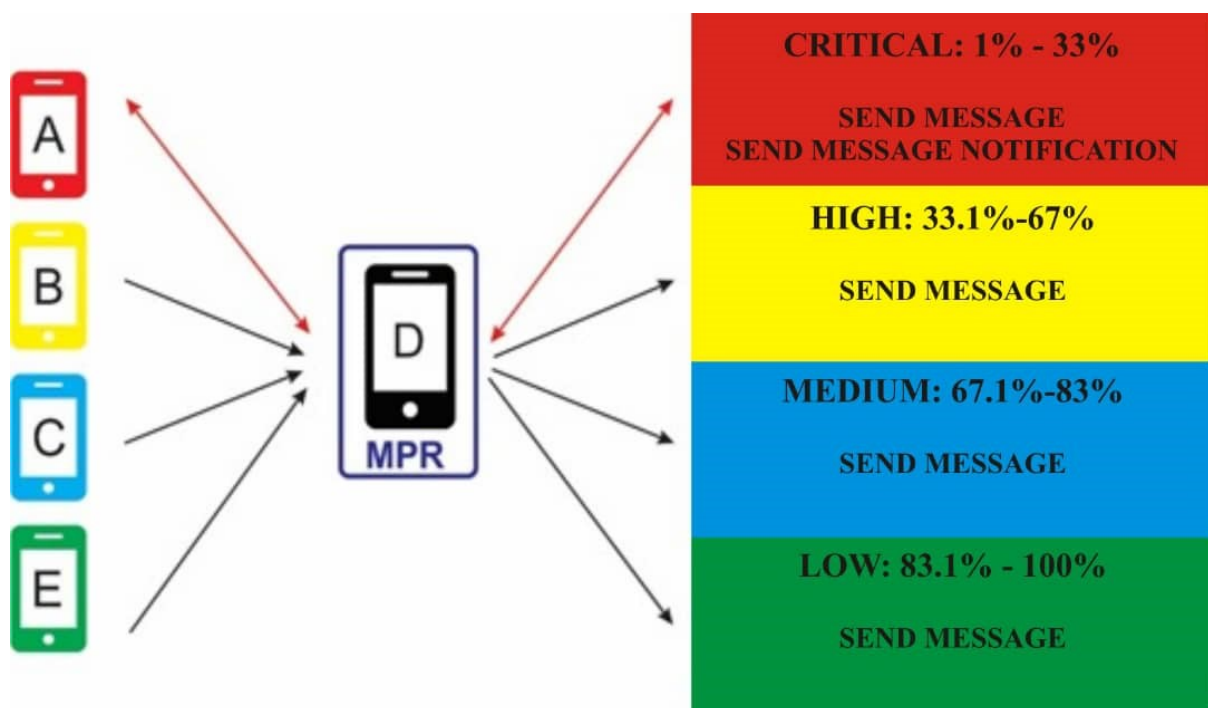


Figure 6-7: Message prioritization process

Figure 6-8 demonstrates message request order and priority order. Although device A is the third device to send Alert message for routing via MPR D, yet device A’s Alert message is the first to be routed by MPR D to the message recipient. This is possible because device D (MPR) must sort all Alert message according to priorities before routing to intended recipients.

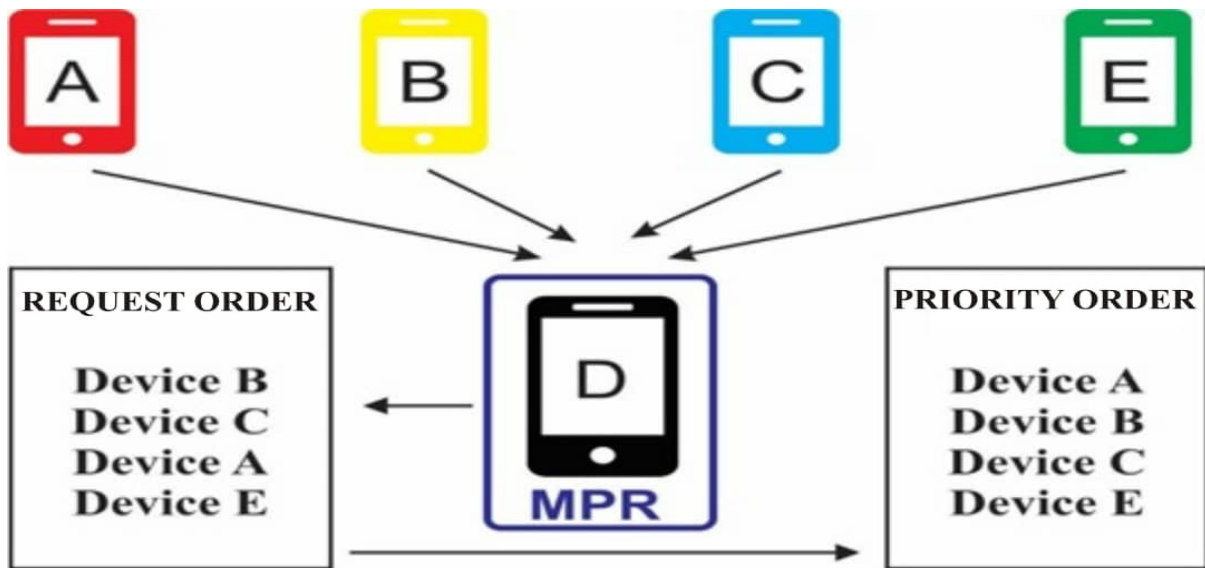


Figure 6-8: Request Order and Priority Order

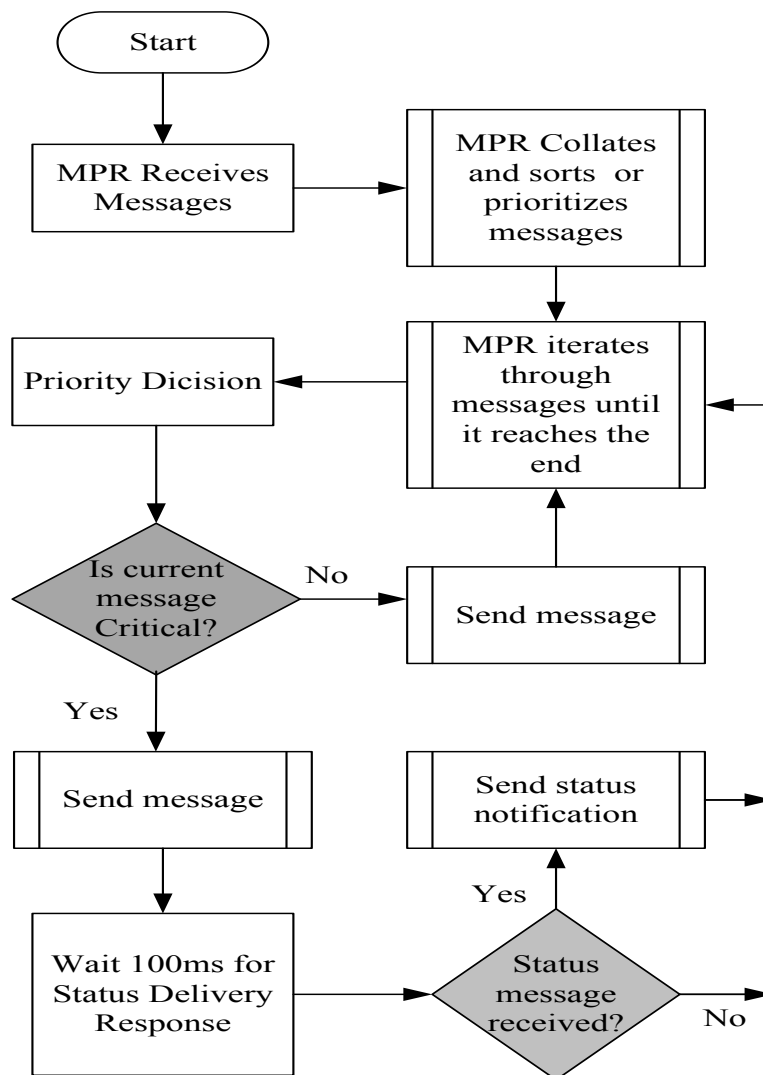


Figure 6-9: Message prioritization process

The flowchart in Figure 6-9 is a concise representation of the message prioritization process. As mentioned earlier, DS- OLSRMP message prioritization technique ensures only critical priority nodes sent and received instant message notifications on Alert message delivery. However, the process does not wait indefinitely for critical priority nodes to receive notifications, rather, it waits for 100ms and moves on to the next message if no feedback is received within the stipulated time (100ms). This approach prevents the MPR from waiting indefinitely for ALERT message status delivery report, especially when the intended recipient of such message is out-of-range.

6.2.2.2 DS-OLSRMP MPR Selection Procedure

The DS-OLSR MPR selection process has been optimized to allow only high Battery life nodes to be selected as MPR. This process has been achieved by modifying the concept of MPR willingness in the classical OLSR MPR selection scheme as in Algorithm. The mechanism selects middle, and low priority nodes to broadcast Topology Control (TC) messages to entire network rather than involving critical priority nodes, thereby reducing the amount of TC messages and its associated energy, subsequently increases the lifespan of the low battery nodes. The MPR willingness is represented by four priority values of willingness level: *WILL_NEVER* `1`, *WILL_LOW* `2`, *WILL_DEFAULT* `3`, *WILL_HIGH* `4`. When using DS-OLSRMP, these willingness levels are ranked on the bases of nodes battery energy level as used in the message prioritization scheme. Critical priority nodes will always set with the current energy level (EL_c) lower the minimum energy level (EL) threshold value (EL_{min}). therefore, such nodes are set to report willingness level of *WILL_NEVER* and will never involve in the TC message broadcasting as result of their critical Battery life percentage. On the other hand, nodes with the EL between 33.1% and 67% (high priority), 67.1% and 83% (medium priority), and 83.1 and 100% (low priority) respectively, are set to report willingness value based on their ranks, whereby low priority nodes with EL_c higher than 83% always report the maximum willingness value of *WILL_ALWAYS* and of course represents the best applicant for MPR as in Algorithm... The willingness level is broadcasted through HELLO message and each node selects its own MPR from its one hop neighbour based on the advertised willingness. The concept preventing low battery nodes from being selected as MPR in the DS-OLSRMP extends the lifetime of the low battery nodes and reduces connection error or temporary loss of routes to other parts of the network, often caused by packet collision, thereby resulting to massive increase in generation control overhead.

Algorithm 4.2: DS-OLSR MPR Willingness Process

Begin:

Require: Energy Level > EL_{min}

Ensure: Appropriate Battery life && Two-hop Nodes

EL_{max} ← the maximum energy level of node

EL_{min} ← the minimum energy level of node

$EL_c(i)$ ← the current energy level of node i

W_i ← willingness of node $i \in v$

Get $EL_c(i)$ of node i

 If $EL_c(i) < EL_{min}$ then

$W_i = WILL_NEVER$ //1

 Else if $EL_c(i) \leq 67$

$W_i = WILL_LOW$ //2

 Else if $EL_c(i) \leq 83$

$W_i = WILL_DEFAULT$ //3

 Else

$W_i = WIL_HIGH$ //4

End if

Return Willingness level

6.2.2.3 Message Slice Duration (MSD)

In DS-OLSR (Aliyu et al., 2020), the duration of Message Time Slice (MTS) is 30,000ms. However, different priority nodes have different Message Slice Duration (MSD) when using DS-OLSRMP. This is because the priority technique prioritizes message from devices with low battery energy and allow such nodes to switch to sleep mode after the specified time for energy conservation. The maximum battery energy percentage of each priority together with their MSD durations are used to obtain an appropriate MSD of the various priorities.

Let t_1 , t_2 , t_3 and t_4 represent the MSD of Critical, High, Medium, and Low priority nodes, respectively. Therefore, the MSD for all priorities, T_i is expressed as:

$$T_i = \frac{x_i \beta}{100} \quad \text{for } i = 1 - 4 \quad (6-2)$$

Where x_i is the maximum battery energy percentage for the various priority and β represent the duration of MTS (Aliyu et al., 2020). The MSD for the various priorities is calculated by equation (6-2) and the results obtained is presented in Table 6-3. The MSD for each priority is activated during DS-OLSR message time slice (MTS) duration.

Table 6-3: Allocation of Message Slice Duration (MSD) to Priorities

Priority	Message Slice Duration (MSD)
Critical	10,000ms
High	20,000ms
Medium	25,000ms
Low	Entire MTS (30,000ms)

6.2.2.4 Battery Model

Many researchers have presented different models for analysing battery service life and predicting the remaining battery capacity of nodes (Rong & Pedram, 2006). Battery provides current and voltage for the node's components including radio interface, memory cards, CPU, etc. As reported by (Waheb A Jabbar et al., 2014), Battery as storehouse of electrical charges losses its charge with decrease of electrical current (load) and the loss rate is given as a function of the load. The total energy consumed per cycle (E_{Cycle}) is the sum of the energy consumed by the various hardware component attached to a battery (Waheb A Jabbar et al., 2014) and is given as:

$$E_{Cycle} = E_{Trans} + E_{CPU} + E_{DC} + E_{Bat} \quad (6-3)$$

Where E_{Bat} denotes efficiency loss of battery charges while E_{Trans} , E_{CPU} , E_{DC} , E_{Bat} are the energy consumed by transceiver, Processor, and converter (DC-DC) respectively. All nodes in DS-OLSRMP are provided with a simple linear battery model based on coulomb counting technique (Rong & Pedram, 2006), to estimate residual battery energy of nodes at charge monitoring interval of 1 second. However, this research deliberately set different initial battery capacity of nodes in NS-3 to account for various priority classes of message prioritization.

6.3 Simulation Setup and Results Analysis

This section presents the implementation of DS-OLSRMP in NS-3 simulation environment and evaluates the performance of the proposed routing scheme based on disaster area network as proposed by Aschenbruck et al. (2009). It is the same model that was used for DS-OLSR implementation as presented in the previous Chapter. The results obtained are compared based on selected performance criteria with DS-OLSR (Aliyu et al., 2020), and with two other conventional schemes: OLSRv1 and OLSRv2. Firstly, this thesis discusses the simulation setup

and its environment, then highlight the selected performance evaluation metrics. Although, the simulation results are validated using analytical computation, but in this Chapter, analysis of the simulation results of DS-OLSRMP in comparison with DS-OLSR, OLSRv1 and OLSRv2 under the same parameters wraps up the Chapter.

6.3.1 Simulation Setup

As mentioned earlier, the performance of the proposed DS-OLSRMP is evaluated by simulations in NS-3.26 and validated using analytical analysis. Figure 6-10 presents NS-3 python visualizer showing the implementation of the proposed DS-OLSRMP protocol. The simulation for both static and mobility scenarios were executed and compared with DS-OLSR, OLSRv1 and OLSRv2 under different nodes density: 10, 50, 100 and 200 nodes in 1000m x 1000m simulation environments as presented in Table 6-4. Different initial battery capacity of nodes was deliberately set to account for various priority classes of message prioritization. In each DS-OLSRMP network scenario, nodes are randomly deployed into four different priority groups based on defined battery capacity. Therefore, 20% of the deployed nodes of each simulation has been assigned as Critical Priority (CP) nodes with Battery life between 1% and 33%, whilst 30% of the deployed nodes as High Priority nodes with Battery life between 33.1% and 67%.

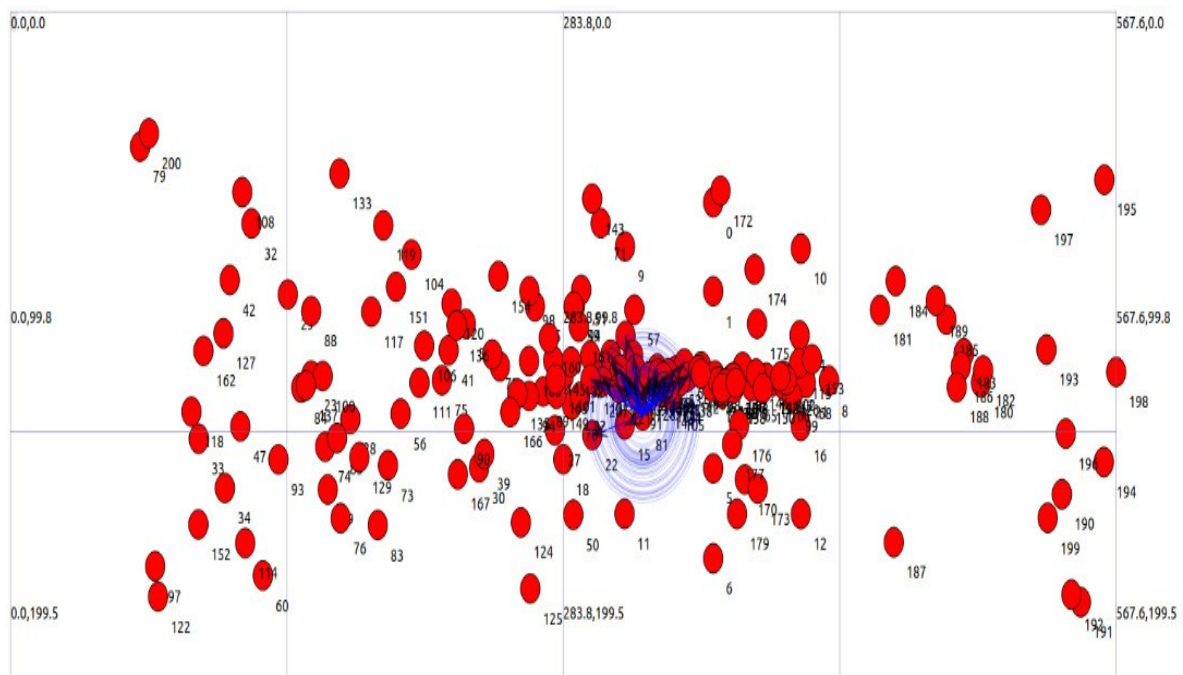


Figure 6-10: NS-3 Python Visualizer showing node placement for DS-OLSRMP

The remaining half of the deployed nodes have been shared between High Priority (HP) and Low Priority (LP) nodes, with 30% of the nodes assigned Battery life between 67.1% and 83% for the former, and 20% of LP nodes assigned Battery life between 83.1% and 100% for the latter. As regards to mobility models, we considered Random Way Point (RWP) with speed range of pedestrian (1m/s – 2m/s) (Aschenbruck et al., 2009). This is because victims running at high speed during disaster recovery and rescue operation will results to high risk of injury. However, to accommodate the speed of rescuers who might be using vehicles, we also evaluate the proposed scheme with the speed range of vehicles (5m/s – 12m/s). The simulation was generally set up according to parameters used by Waheb A. Jabbar et al. (2018) except those parameters that are DS-OLSR specific.

Table 6-4: Simulation Parameters Message Prioritization

Description	Parameters
Simulation Environment	1000m x 1000m
Number of Nodes	10, 50, 100 and 200
Nodes Deployment	Random positioning
Mobility Model	Random Way point, Min Speed 0, Max Speed 1m/s - 2m/s, and 5m/s – 12m/s [15], Pause Time 10s
Simulation Duration	180 Seconds
Transmission Range	50m
Packet Size	512byte
Mac Protocol	IEEE 802.11
Energy Model	$Tx_{Current} = 0.26A$ $Rx_{Current} = 0.18A$ $Idle_{Current} = 0.148A$ $Sleep_{Current} = 0.0094$ Supply Voltage = 5 Volt
Battery Model	Linear Battery Model
DS-OLSRMP SPECIFIC PARAMETERS	
Priority Classification	CP, HP, MP and LP
Battery Energy Level Distribution	CP (1% - 33%), HP (33.1% - 67), HP (67.1% - 83%), LP (83.1% - 100%)
Nodes Distribution to Priorities	CP=20%, HP=30%, MP=30%, LP=20%

6.3.2 Results Analysis

The overall performance of the proposed DS-OLSRMP is thoroughly investigated and compared with DS-OLSR, OLSRv1 (Aliyu et al., 2020), and OLSRv2 in disaster area model based on the simulation parameters mentioned earlier. The mean values of energy dissipated in total of 10 simulations by nodes in both static and mobility scenarios were evaluated in

comparison to the mean values of energy dissipated using DS-OLSR, OLSRv1 (Aliyu et al., 2020), and OLSRv2. The mean values of packet delivery is also evaluated to ascertain the percentage of successfully transmitted packets against the number of packets sent in the networks. Furthermore, to compare the time required for a packet to be successfully transmitted from source to destination, the research equally evaluated average end-to-end delay. Network size of 10, 50, 100 and 200 nodes and different nodes speed (Pedestrian: 1m/s – 2m/s and Vehicles: 5m/s – 12m/s (Aschenbruck et al., 2009)) has been selected as parameters to evaluate the proposed scheme as it widely used to evaluate simulation studies in MANETs. When the network size and node speeds increases, the scalability of the proposed routing protocol will be evaluated to prove its performance. As reported in our previous work in (Aliyu et al., 2020), the simulation of 200 nodes using OLSRv1 and OLSRv2 failed severely due to generation of massive control traffic that cannot be handled by the system. However, the researcher intends to use a system with a better resource in future to compare the performance of the OLSRv1 and OLSRv2 using 200 nodes with DS-OLSRMP.

Figures 6-11, 6-12 and 6-13 represent mean values of energy dissipated in total of 10 simulations by nodes using DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 for 10, 50, 100 and 200 nodes in both static and mobility scenarios. It is obvious from the simulation results that OLSRv1 and OLSRv2 reported high energy consumption as compared to DS-OLSR and DS-OLSRMP in all scenarios and of course, the energy consumption rate for the OLSRv1 and OLSRv2 increases exponentially with increased nodes in the networks. This huge energy consumption by both versions of the OLSR is attributed by continuous generation of massive control overhead traffic and constantly busy routing control messages in the background (regardless of user messages) as equally reported by Qin et al. (2016) as the major energy consumption of their experimental work.

The energy conservation by DS-OLSR is because of Time Slices (TSs) that confine messages into their respective time slots (Aliyu et al., 2020). It can also be observed from the simulation results for static scenario in Figure 6-11 that energy savings by DS-OLSR is further enhanced by the introduction of message prioritisation techniques as DS-OLSRMP indicates reduction in energy consumption as compared to DS-OLSR, with 25.2%, 21.8% and 20.9 % when simulating 10, 50, 100 and 200 nodes, respectively. The energy saving is because of the message prioritization techniques that ensures messages from CP nodes are delivered first before messages from other priority nodes (HP, MP, and LP) and that CP, and HP nodes

switches to sleep mode after 10,000ms and 20,000ms of MTS respectively, to conserved energy.

To examine the energy conservation of the proposed routing protocol in real life disaster mobility scenario, The proposed technique were evaluated under two mobility speeds: Pedestrian (1m/s – 2m/s) and Vehicles (5m/s – 12m/s) (Aschenbruck et al., 2009). Figures 6-12 and 6-13 reveals that the proposed DS-OLSRMP achieves lowest energy consumption in both pedestrian and vehicle speeds irrespective of the number of nodes. This attributed to the fact that, DS-OLSRMP utilizes energy serving mechanism that is not available in other protocols. However, the performance of the DS-OLSRMP is slightly affected by the implementation of mobility metrics, particularly for 5m/s – 12m/s speed as the energy consumption increases due high movement of nodes in the networks. Although it is still reasonable considering the number of successful transmitted packets and compared to DS-OLSR and multipath routing protocols (Nishiyama et al., 2014) and (Waheb A. Jabbar et al., 2018). In a general term, nodes changes position in mobility scenarios and of course, their routes randomly change over time, which requires further route calculation and complexity on topology sensing. In addition, MPR nodes expends more energy than normal nodes as they forward control and data packets to the entire network on behave of their electors. However, DS-OLSRMP take advantage of its prioritisation techniques to prioritise message from CP and select only high Battery life nodes (e.g MP and LP) as MPRs. This process increases the lifetime of low battery energy devices and reduces the total energy cost of the network.

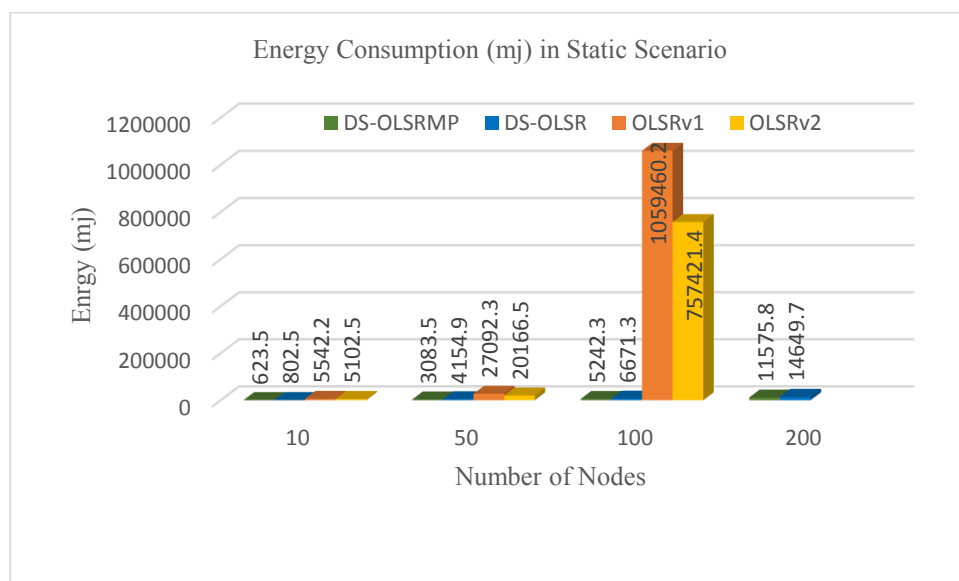


Figure 6-11: Comparison of Energy Consumption for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Static Scenario

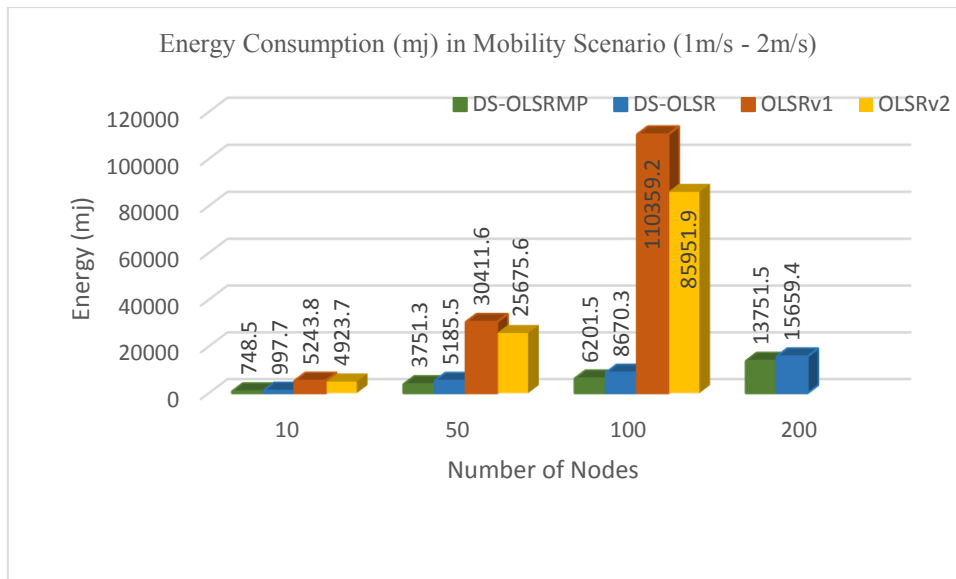


Figure 6-12: Comparison of Energy Consumption for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (1m/s – 2m/s)

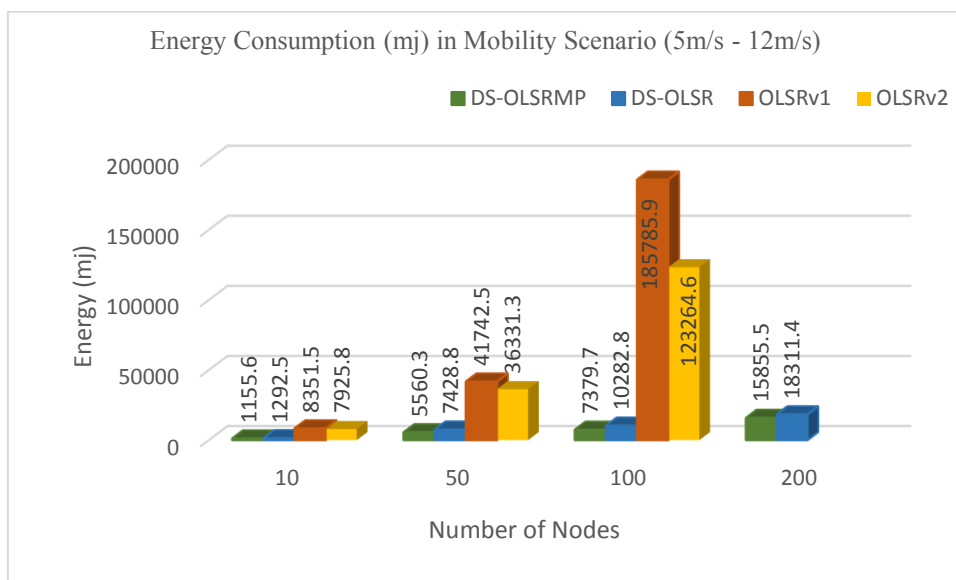


Figure 6-13: Comparison of Energy Consumption for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (5m/s – 12m/s)

Figures 6-14, 6-15 and 6-17 represent mean values of control overhead in total of 10 simulations for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 when simulating 10, 50, 100 and 200 nodes in both static and mobility scenarios. It can observe the superiority of DS-OLSRMP in all situations as it returns the lowest control overhead in all the scenarios, regardless of nodes mobility speed and network size. This achievement followed by DS-OLSR as it became second best routing protocol with less control overhead because both protocols share similar techniques. The results of DS-OLSRMP and DS-OLSR illustrated the important of using Time Slices (TSs) to encapsulates control message such as Hello, TC, and of course

ALERT message into their respective TSs. In addition, both protocols maintain routing information for a longer time (Aliyu et al., 2020), thereby reducing the delay time of packets transmission. These schemes limit message collision and the continuous rebroadcasting of control messages in both DS-OLSRMP and DS-OLSR and therefore reduces the overall routing overhead.

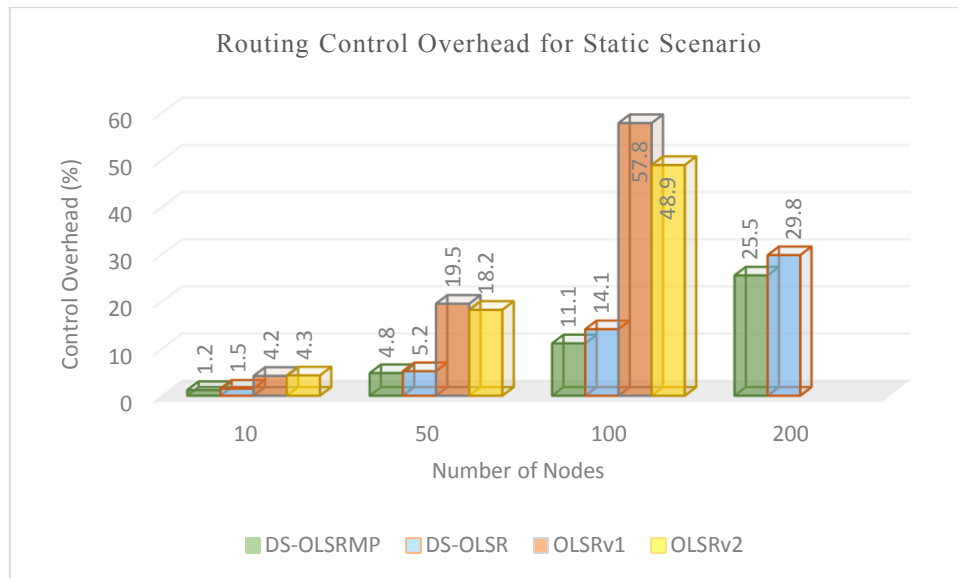


Figure 6-14: Comparison of Routing Control Overhead for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Static Scenario

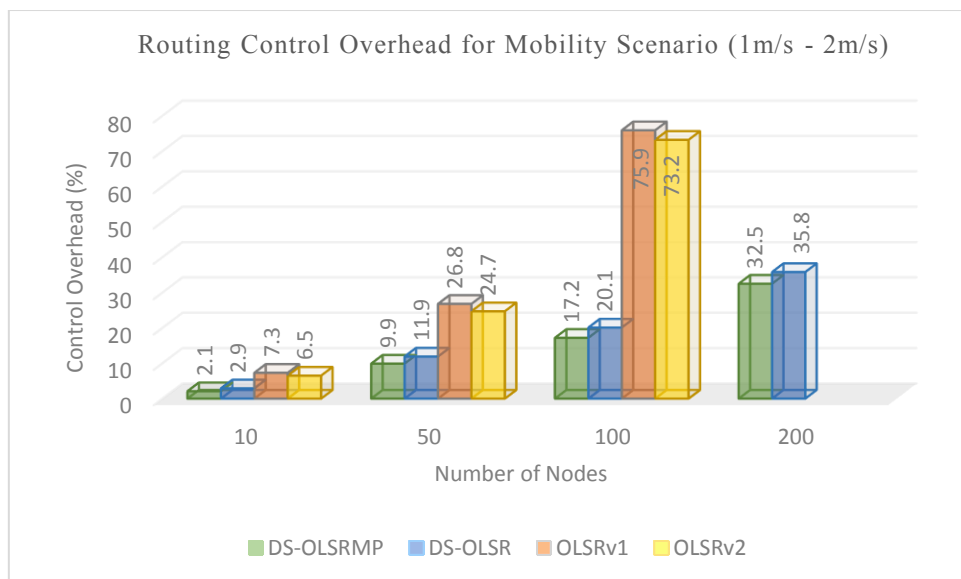


Figure 6-15: Comparison of Routing Control Overhead for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (1m/s – 2m/s)

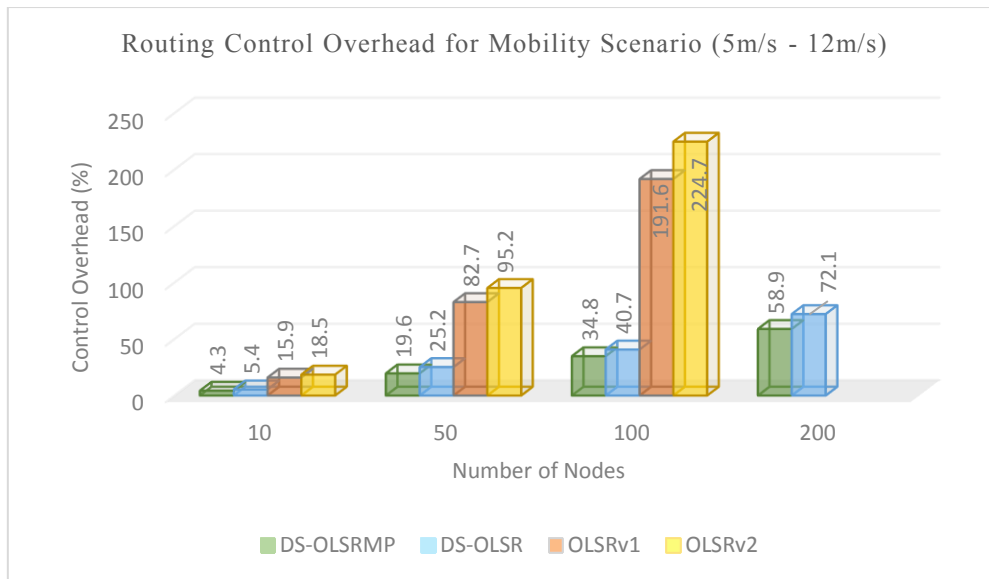


Figure 6-16: Comparison of Routing Control Overhead for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (5m/s – 12m/s)

Figures 6-17, 6-18, and 6-19 represent mean values of packet delivery ratio in total of 10 simulations for DS-OLSRMP, DS-OLSR, OLSRv1, and OLSRv2 with 10, 50, 100 and 200 nodes in both static and mobility scenarios. It can observe from the simulation results that both versions of OLSR delivered less packets as compared to DS-OLSRMP and DS-OLSR in both scenarios. In addition, the packet delivery ratio for OLSRv1 and OLSRv2 drastically reduced with the introduction of high mobility (5m/s – 12m/s) in the networks, thereby resulting to huge increase in their end-to-end delay and control overhead.

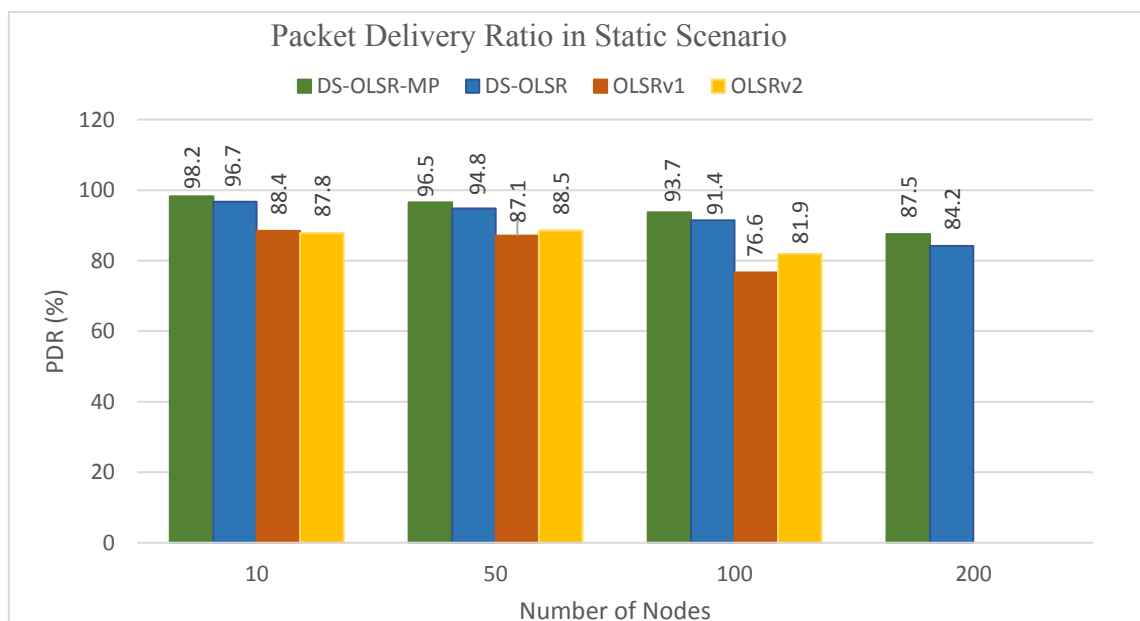


Figure 6-17: Comparison of Packet Delivery Ratio for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Static Scenario

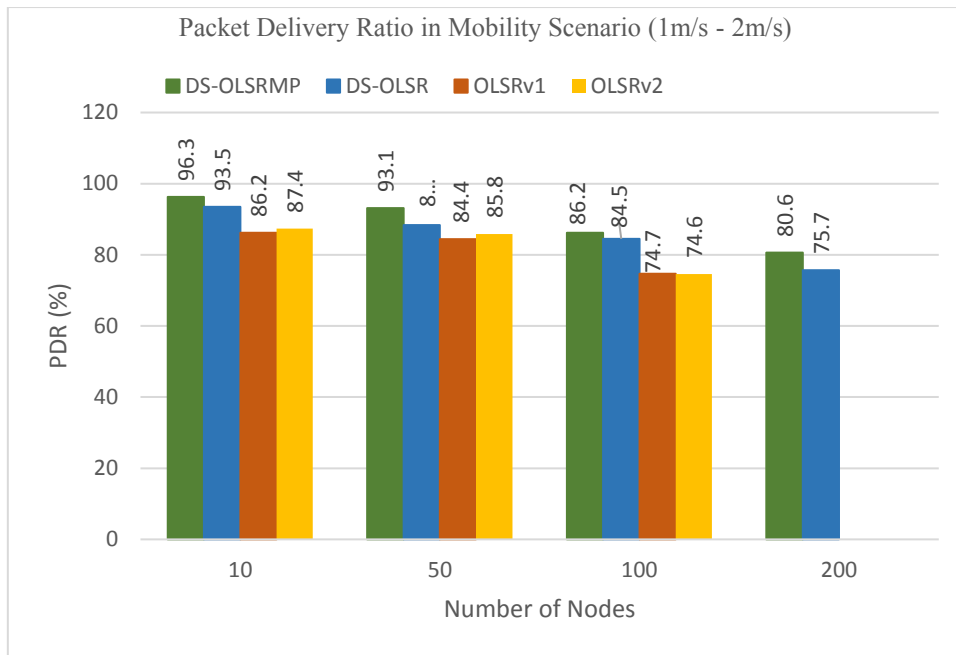


Figure 6-18: Comparison of Packet Delivery Ratio for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (1m/s – 2m/s)

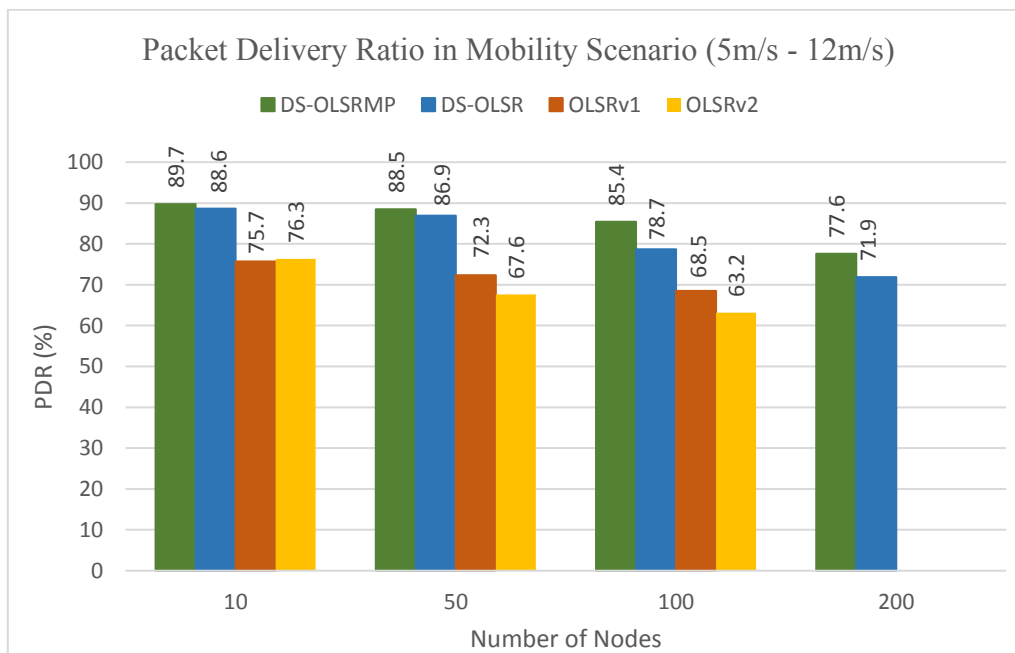


Figure 6-19: Comparison of Packet Delivery Ratio for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (5m/s – 12m/s)

The use of packet delivery prioritisation based on device Battery life extends lifespan of low battery devices and allows more packets to be delivered as DS-OLSRMP shows better packet delivery ratio as compared to DS-OLSR. The percentage of packet delivered by both protocols are similar in the simulation with 50 nodes for static scenario as shown in Figure 6-19. However, in the simulation of 100 and 200 nodes for mobility scenarios, DS-OLSRMP

demonstrated the capability of the proposed prioritisation scheme to prolonged lifetime of low battery nodes, thereby delivering more packets than DS-OLSR as shown in Figures 6-18 and 6-19. Although, the PDR for both protocols decreases slightly with increase of nodes and node speeds in the network, nonetheless the PDR is far better than what was obtained in a similar OLSR optimisation research by Prakash et al. (2020), and Waheb A. Jabbar et al. (2018). The DS-OLSR and DS-OLSRMP results confirms how the concept of TSs improves link quality by eliminating crosstalk and reduced funnel effect without compromising packets delivery in all the scenarios.

Figures 6-20, 6-21 and 6-22 represent mean values of end-to-end delay in total of 10 simulations for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 with 10, 50, 100 and 200 nodes in both static and mobility scenarios. It is obvious from the Figures that the conventional versions of OLSR reported higher end-to-end delay in both static and mobility scenarios as compared to DS-OLSRMP and DS-OLSR. In addition, the end-to-end delay for both OLSR versions increases exponentially with increased of nodes in the networks. This is due to connection errors or temporary loss of routes to other parts of the network, often caused by packet collision, thereby resulting to massive increase in generation control packets, subsequently increased end-to-end delay in all the simulated scenarios.

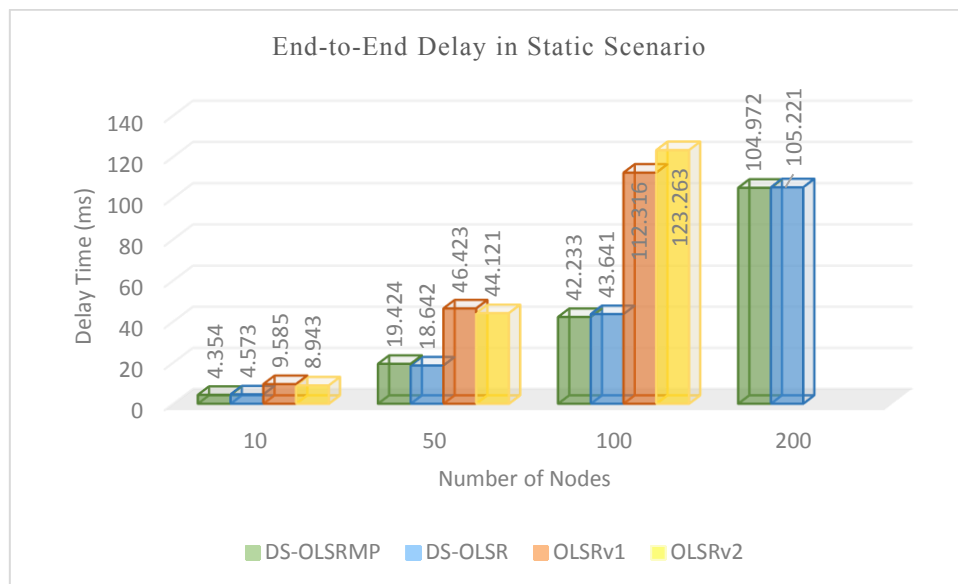


Figure 6-20: Comparison of End-to-End Delay for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Static Scenario

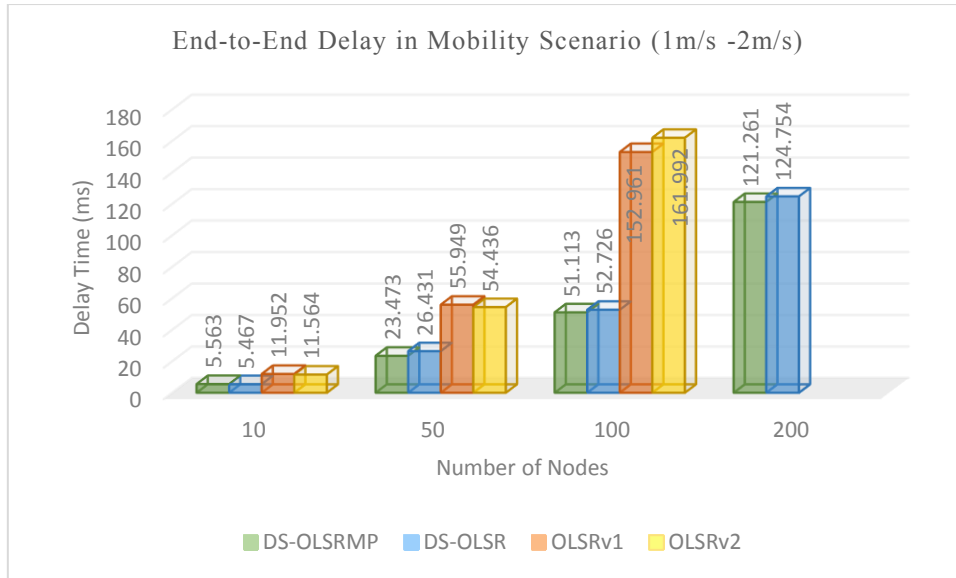


Figure 6-21: Comparison of End-to-End Delay for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (1m/s – 2m/s)

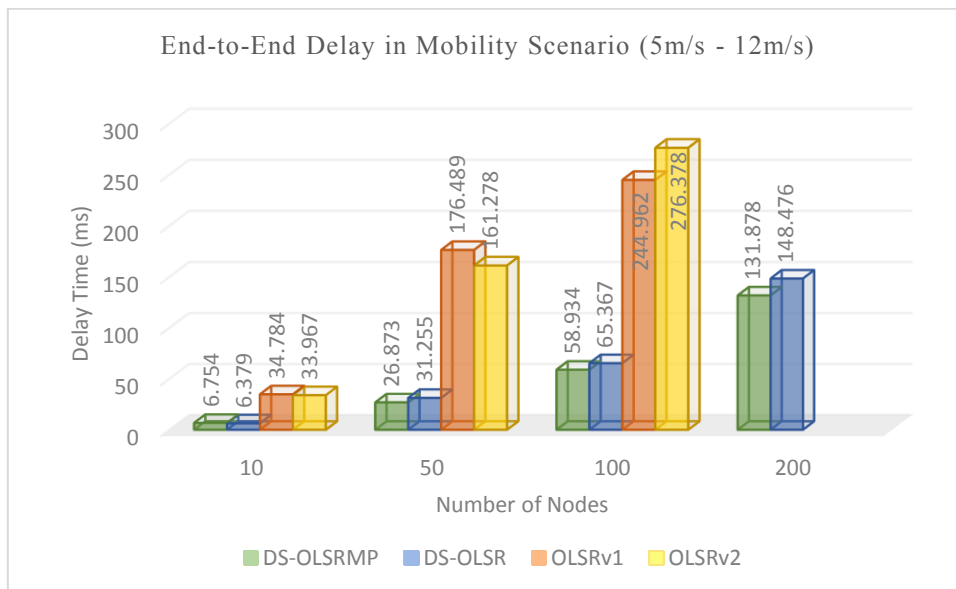


Figure 6-22: Comparison of End-to-End Delay for DS-OLSRMP, DS-OLSR, OLSRv1 and OLSRv2 in Mobility Scenario (5m/s – 12ms)

The end-to-end delay for DS-OLSRMP and DS-OLSR are very similar in all scenarios. This did not come as a surprise, because both schemes employed the techniques of TSs that decreases the possibility of link failure and maintain routing information for a longer time as in (Aliyu et al., 2020). Therefore, data packets are not sent to unreliable routes, thereby reducing the delay time required for retransmissions. DS-OLSRMP enhances energy efficiency by extending the lifespan of low battery energy devices without sacrificing major quality of

service metrics: PDR, average end-to-end delay and routing control overhead. Thus, it is highly recommended for communications in disaster related scenarios.

6.4 Chapter Summary

The proposed DS-OLSRMP as an extension to DS-OLSR, presented in this Chapter not only prioritize messages from devices with low battery energy but also extends the lifespan of communication devices with the low battery energy. It also improves overall energy conservation and packet delivery as compared to DS-OLSR, OLSRv1 and OLSRv2. In addition, DS-OLSRMP will likely improve disaster victim's mental state by quickly responding to messages sent by those whom devices are low in battery energy to prevent such victims from overwhelming the network with messages as their device battery energy dwindles. The message prioritization techniques classified mobile phones into four priority groups - Critical, High, Medium, and Low priorities, thereby prioritizing both message delivery and message status notification for devices with low battery energy. The simulation results show that energy consumption and packets delivery are notably improved using the message prioritization. The priority techniques also ensure that messages from CP nodes is delivered before messages from other priority nodes and that, CP and HP nodes switch to sleep mode after 10, 000ms and 20, 000ms of MTS, respectively. The next Chapter presents the validation of the proposed techniques mathematically and evaluated its performance as compared to another related research.

Chapter 7

Performance Evaluation and Validation

7.1 Introduction

The objective of this Chapter is to validate the simulation results of our proposed system using mathematical approach and evaluate its performance as compared to other related work. The proposed DS-OLSR and DS-OLSRMP was initially implemented in NS-3 using different simulation scenarios as presented in Chapter 5 and 6. The first simulation of DS-OLSR was conducted to determine the amount of energy dissipated during OLSR/DS-OLSR network formation process. Thereafter, the proposed approach was implemented in Disaster Area Model as proposed by Aschenbruck et al. (2009). To extend the lifespans and prioritize message delivery of low battery devices, DS-OLSRMP was proposed and equally implemented in NS-3. However, to avoid repetition, the validation of the simulation results is based on DS-OLSRMP because it is an extension of DS-OLSR that accommodates all features and functionalities of the proposed DS-OLSR with additional message prioritisation techniques. The rest of the Chapter is organised as follows: Section 7.2 presents the mathematical representation of DS-OLSR and DS-OLSRMP modifications. Section 7.3 presents numerical energy consumption model. Section 7.4 discusses the computation of routing control overhead. Packet delivery ratio and End-to-End delay computations are presented in Section 7.5 and 7.6, respectively. Finally, Section 7.7 wraps up the Chapter with summary.

7.2 Analytical Validation

The analytical validation is based on the metrics evaluated in the simulation of DS-OLSRMP, consisting of Control Overhead, Energy Consumption, Packet Delivery Ratio (PDR) and End-to-End Delay. In other words, the simulation parameters of the proposed DS-OLSRMP have been used to produce the mathematical results and compared it with the results of the simulation.

As mentioned earlier, the proposed DS-OLSRMP is an extension of DS-OLSR (Aliyu et al., 2020), that prioritises ALERT message delivery based on device battery energy level, thereby extending the lifespan of nodes with low battery energy. DS-OLSR (Aliyu et al., 2020), modifies OLSR unified packet format by adding Originator ID as a repository for smartphone's

phone number for energy friendly routing and communication in disaster zone. The initial OLSR unified packet format (P_{F0}) is mathematically presented as:

$$P_{F0} = \sum_{i=1}^9 P_{Hi} \quad (7-1)$$

The description of P_{F1} , P_{F2} , P_{F3} , ... P_{F9} is presented in Table 7-1.

Table 7-1 : Description of OLSR Packet Header

Notation	Description
P_{H1}	Packet Length
P_{H2}	Packet Sequence Number
P_{H3}	Message Type
P_{H4}	Validity Time
P_{H5}	Message Type
P_{H6}	Originator Address
P_{H7}	Time to Live
P_{H8}	Hop Count
P_{H9}	Message Sequence Number

The new packet format (P_{F1}) as proposed for DS-OLSR is expressed as:

$$P_{F1} = P_{F0} + O_{ID} \quad (7-2)$$

Where O_{ID} represent Originator ID as a repository for smartphone's phone number (Aliyu et al., 2020).

The Originator ID as discussed by Aliyu et al. (2020), provides human readable device information across the network, allowing victims to send and receive SMS using a known format (phone numbers). The ability to uniquely identify each device via Originator ID renders OLSR MID messages obsolete. This is because devices with multiple interfaces will always include the same Originator ID, which forces recipients to accept a single message from any of the multiple interfaces, and quietly drop the rest. The core functional messages of OLSR are mathematically presented as follows:

Let O_{MI} represent initial OLSR messages. Therefore,

$$O_{MI} = H_m + TC_m + HN_m + MD_m \quad (7-3)$$

Where H_m , TC_m , HN_m , and MD_m are Hello, TC, Host and Network Association and Multiple Interface Declaration messages. However, DS-OLSR proposes embedding text messaging capability called Alert Message (New message created for DS-OLSR) into OLSR (Aliyu et al., 2020), for energy efficient network for disaster recovery and rescue operation. This message ensures DS-OLSR devices sends and receives messages without additional overhead since ALERT message occurs within its specific Time Slice (TS) (Aliyu et al., 2020). Therefore, the new DS-OLSR messages (D_{SM}) is expressed as:

$$D_{SM} = O_{MI} - MD_m + A_m \quad (7-4)$$

Where A_m is Alert message type specific for DS-OLSR.

DS-OLSR (Aliyu et al., 2020) introduces the concept of Time Slices (TSs) which encapsulates DS-OLSR messages and Alert message into their corresponding Time Slices. The various Time Slices are Network Formation Time Slice (NFTS), Topology Propagation Time Slice (TPTS), Message Time Slice (MTS), Network Sleep Period (NSP) and can be express mathematically with their corresponded duration as:

$$TS(n_i) = \begin{cases} n_1, & 0 < n_1 \leq 51 \\ n_2, & 14 < n_2 \leq 28 \\ n_3, & 28 < n_3 \leq 58 \\ n_4, & 58 < n_4 \leq 81 \end{cases} \quad (7-5)$$

Where $TS(n_i)$ is the various DS-OLSR Time Slices with their corresponded durations and n_1 , n_2 , n_3 , and n_4 represent the duration of NFTS, TPTS, MTS and NSP respectively. A Time Slice period exit once its timer expires and it automatically triggered the starts of the next TS. However, the various TSs uses different duration as indicated in the step function in equation 7-5.

The low battery devices often experience quick power failure which restrict their ability to communicate for longer time during rescue operations. DS-OLSRMP proposes ALERT message prioritization to further improve energy conservation, extend lifespan of low battery energy devices and improves mental state of victims with the low battery devices. The mathematical expression of the message prioritization based on device battery energy level is presented in equation 7-5. As mentioned earlier, the analytical validation is based on the following metrics:

$$P(x_i) = \begin{cases} x_1, & 1 \leq x_1 \leq 33 \\ x_2, & 33 < x_2 \leq 67 \\ x_3, & 67 < x_3 \leq 83 \\ x_4, & 83 < x_4 \leq 100 \end{cases} \quad (7-6)$$

7.3 Numerical Energy Consumption

With respect to the Mobile Ad-hoc network model discussed in Section 5.2, the network connectivity parameters of MANET model represent the links between normal nodes, MPR nodes and a sink node is expressed mathematically as follows:

If a normal node e establishes a link with an MPR node y , can be written as:

$$a_{ij}^{ey} = \begin{cases} 1 & \text{a link on arc } (i j) \in A_{E \rightarrow My} \\ 0 & \text{Otherwise} \end{cases} \quad (7-6)$$

Where a_{ij}^{ey} is the arc (link) between normal node e and MPR node y , A represents a number of links (arcs). E is the vertices of normal node and My is the vertices of MPR node.

If a Normal node e establishes a link with a Sink node S , can be expressed as follows:

$$a_{ij}^{es} = \begin{cases} 1 & \text{a link on arc } (i j) \in A_{E \rightarrow S} \\ 0 & \text{Otherwise} \end{cases} \quad (7-7)$$

If an MPR node y establishes a link with a Sink node S , can be written as:

$$a_{ij}^{ys} = \begin{cases} 1 & \text{a link on arc } (i j) \in A_{My \rightarrow S} \\ 0 & \text{Otherwise} \end{cases} \quad (7-8)$$

If an MPR node y establishes a link with other MPR node x , can be expressed as:

$$a_{ij}^{yx} = \begin{cases} 1 & \text{a link on arc } (i j) \in A_{My \rightarrow Mx} \\ 0 & \text{Otherwise} \end{cases} \quad (7-9)$$

The numeric energy consumption model is based on Generic Radio Energy Model as highlighted in Waheb A. Jabbar et al. (2018) and Fotino et al. (2007), which defined the total energy consumption of a node as the sum of energy consumed during Transmit, Receive, Idle

and Sleep states. Considering the formular for energy consumed by each state as in equation (5-1), (5-2), (5-3), and (5-4).

Let T_C represent the sum of the default current of the various node's states and can be expressed as:

$$T_C = Tx_c + Rx_c + Idle_c + Sleep_c \quad (7-10)$$

Where Tx_c , Rx_c , $Idle_c$ and $Sleep_c$ are default transmit, receive, idle and sleep current, respectively. Let T_i represent nodes duration during transmit, receive, Idle and sleep modes.

Replacing the terms used in equations (5-5) and (6-2) by T_C and T_i , respectively. The total energy consumed by nodes to transmit and receive packet at time t can be expressed as:

$$E_T = \left[V * T_c \left(\frac{1}{n} \sum_{i=1}^4 \frac{x_i \beta}{100} \right) Nt \right] \quad (7-11)$$

The values for supply voltage v, T_C (Waheb A. Jabbar et al., 2018), (De Rango et al., 2008), (Fotino et al., 2007), x_i , (maximum battery percentage value for various priority groups) and β (duration of MTS) are presented in Table 7-2. As previously mentioned, transmit, and receive energy are determine by signal transmission power from Physical layer (PHY.SET). Therefore, due to external interference, this research considered sensitivity degradation factor as modelled by Ehiagwina et al. (2019) and equally used in the simulation to account for the signal degradation or power amplifier inefficiency factor S_d as used by Waheb A. Jabbar et al. (2018).

Sensitivity degradation is a function of receiver sensitivity degradation because of external interference causing power leakages (Ehiagwina et al., 2019). Sensitivity degradation affects the battery lifespan of nodes, and it is calculated as the function of noise raised due to external interference as shown in equation (7-12).

$$S_d = 10 \log \left(1 + 10^{\frac{I-N}{10}} \right) dB \quad (7-12)$$

Where I represent receive interference and N is a node received noise which is estimated by the expression in equation (7-13)

$$N = N_t + N_f + 10\log(BW) \quad (7-13)$$

Where N_t and N_f are nodes thermal noise and noise figure respectively, and BW is noise bandwidth. Therefore, the modified total energy consumed by nodes to transmit and receive packet at time t is presented in equation (7-14) and the values of the parameters as used in our simulation are presented in Table 7-2.

$$E_T = \left[V * T_c \left(\frac{1}{n} \sum_{i=1}^4 \frac{x_i \beta}{100} \right) S_d N t \right] \quad (7-14)$$

Table 7-2: Parameters for Calculation of Energy Consumption

Definition	Symbols	Value(s)
Supply Voltage	V	5V
Total current of various node's states	T_c	0.5974A
Maximum battery percentage for various priority group, for $i = 1-4$	x_i	33%, 67%, 83%, 100%
Duration of MTS	β	100%
Maximum Interference Level	I	-110 dBm
Noise Figure	N_f	8.5 dB
Thermal Noise	N_t	-87(10 nodes) -147(50 nodes), -150(100 nodes), -159(200nodes)
Noise Bandwidth	BW	11Mbps

The calculated results were obtained using the total energy consumption formular in equation (7-14) based on the parameters in Table 7-2. The model utilised a transmission rate of 3pct/sec over the duration of 180 seconds with the node density of 10, 50, 100, and 200 nodes as used in the simulation.

It can be seen from Figure 7-1 for static node settings, that the mean values of the energy consumed in the simulation is slightly higher than the mean energy consumption for the networks in mathematical model computation irrespective of the number of nodes in the network. This is due to unpredictable nature of network performance, and it is manifested as the simulated routing overhead is slightly greater than the calculated. The case is the same with the implementation of mobility function to the mathematical model as the total energy consumed in the simulation is marginally higher than the total energy consumption obtained in

the mathematical model computation, regardless of the number of nodes in the network. Like the simulation results, the introduction of mobility function affects the energy consumption of the mathematical model, particularly for 5m/s – 12m/s speed as in Figures 7-2 and 7-3. This is because in high mobility scenario, nodes constantly change position thereby causing re-initiation of route discovery and topology sensing, therefore more energy is required to generate further control messages. However, the energy consumed by the nodes in all scenarios is quite reasonable considering the number of successful transmitted packets and as compared to other OLSR research such as the studies of Nishiyama et al. (2014) and Waheb A. Jabbar et al. (2018).

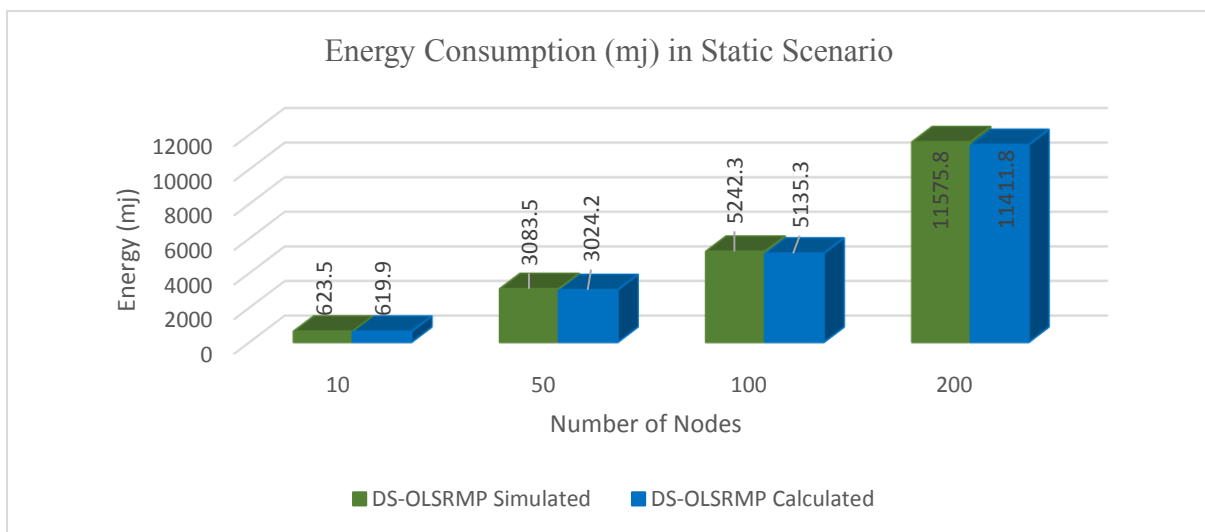


Figure 7-1: Comparison of the Calculated and Simulated Energy Consumption in Static Scenario

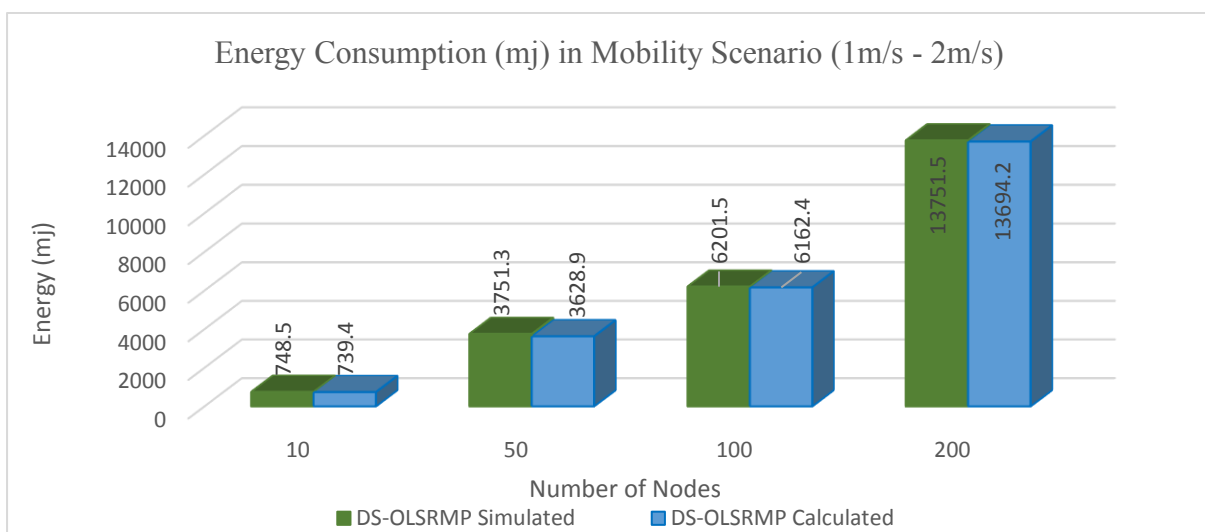


Figure 7-2: Comparison of the Calculated and Simulated Energy Consumption in Mobility Scenario (1m/s – 2m/s)

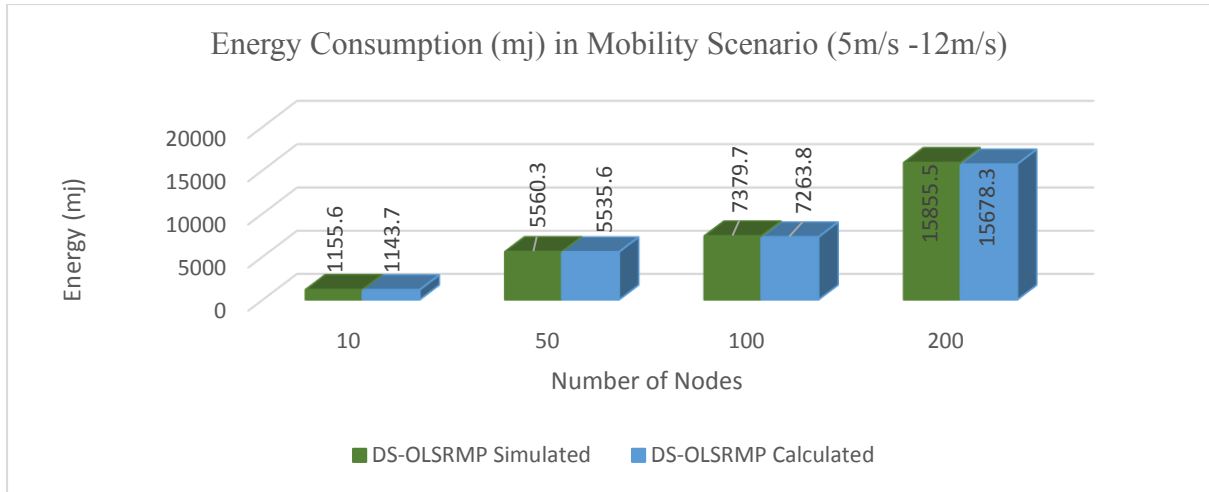


Figure 7-3: Comparison of the Calculated and Simulated Energy Consumption in Mobility Scenario (5m/s – 12m/s)

7.4 Routing Control Overhead Computation

Control overhead is very critical in evaluating the performance of MANET routing protocol for disaster recovery network. This is because control overhead constitutes major energy drainage, and most MANET devices depend largely on batteries or other form of exhaustible source of energy for their operations.

The control overhead of OLSR is the average bandwidth in bytes used for transmitting and receiving of control messages such as Hello and Tc (Xue, Jiang, & Hu, 2008). In other words, routing overhead is the sum of periodic messages, packets drops and triggered update messages (Mahmood et al., 2013), can be expressed as:

$$R_o = P_r + P_f + T_r \quad (7-15)$$

Where R_o represent routing overhead and P_r , P_f , T_r are periodic message, packets fail to reach destination and triggered update messages. These routing overhead metrics are discussed as follows:

7.4.1 Periodic Message routing overhead

Periodic messages are broadcasted constantly for link sensing, neighbour detection, and topology dissemination after every specific time. Periodic message overhead is termed as size

of routing table and periodic route update mechanism (Yang, Tian, & Yu, 2005), (Mahmood et al., 2013), can be written as:

$$R_o (P_r) = \frac{kn^3}{BT_{pr}} \quad (7-16)$$

Where $R_o (P_r)$ represent overhead due to periodic message update, k and n are the routing overhead impulse factor and number of nodes in a network, respectively. B is the transmission rate while T_{pr} is periodic message interval. However, the proposed DS-OLSR introduces the concept of Time Slices (TSs) which encapsulates DS-OLSR periodic messages and Alert message into their corresponding TSs thereby modifying the duration and periodic time of such messages as discussed in Aliyu et al. (2020). Therefore, the modified duration and periodic message interval can be written as:

$$T_{PR} = T_{pr} + T_s \quad (7-17)$$

Where T_{PR} is the modified periodic message duration and interval, while T_s is the duration of NFTS and TPTS (Aliyu et al., 2020).

Substituting the term used in equation (7-16) by T_{PR} we obtained:

$$R_o (P_r) = \frac{kn^3}{BT_{PR}} \quad (7-18)$$

Therefore, routing overhead due to the periodic message update $R_o (P_r)$ for DS-PLSRMP is expressed as:

$$R_o (P_r) = \begin{cases} \frac{kn^3}{BT_{PR}}, & 1 \leq T_{PR} \leq 14 \\ 0 & \text{Otherwise} \end{cases} \quad (7-19)$$

7.4.2 Routing Overhead due to Packet failure

Periodic route update is time specific within neighbourhood and allow nodes to compute routes to all destination in a network. If a node observes change between periodic route update, a triggered update message will be release and packet loss occurs over time. During periodic

route update interval T_{pr} , the number of packets failed to reach destination (Yang et al., 2005), is expressed as:

$$R_o (P_f) = \left[\sum_{P_i \in PA} \sum_{r=0}^{l_i} Q_r^l (T_{pr}) Na (T_{pr}) \right] \quad (7-20)$$

The above represents routing overhead due to packet failure $R_o (P_f)$ as a function of the following metrics:

Q_r^l : Probability that uplink state does not change to down link during first r hops.

T_{pr} : Periodic route update interval (time)

PA: All path in the network

$Na (T_{pr})$: Number of packets arriving at periodic route update time T_{pr} .

The concept TSs and preventing low battery nodes from being selected as MPR in the proposed DS-OLSRMP reduce connection errors or temporary loss of routes to other parts of the network, often caused by packet collision, thereby resulting to massive reduction in generation control overhead. Therefore, the modified $R_o (P_f)$ can be written by replacing the term in equation (7-20) by T_{PR} as:

$$R_o (P_f) = \left[\sum_{P_i \in PA} \sum_{r=0}^{l_i} Q_r^l (T_{PR}) Na (T_{PR}) \right] \quad (7-21)$$

7.4.3 Triggered update message

Triggered update message occurs upon connectivity or topology changes due to nodes mobility between two periodic updates. To reduce the number of packet loss in a network, routing protocols do not wait for succeeding periodic update to send topology changes, rather a triggered updates message will be issued to update nodes about these changes. Therefore, routing overhead due to triggered update (X. Wu, Sadjadpour, & Garcia-Luna-Aceves, 2007), is expressed as:

$$R_o(T_r) = \frac{\left\lceil \frac{T}{T_{pr}} \right\rceil}{\frac{T}{T_{pr}}} \quad (7-22)$$

Where $R_o(T_r)$ represents routing overhead due to triggered update and T is the triggered update message. Ceiling operator $\lceil \cdot \rceil$ is solved mathematically by accepting the possible highest value of $\left\lceil \frac{T}{T_{pr}} \right\rceil$. Suppose n number of nodes are mobile in a network, the total number of triggered updates can be expressed as:

$$R_o(T_r) = \sum_{i=1}^n \frac{\left\lceil \frac{T}{T_{pr}} \right\rceil}{\frac{T}{T_{pr}}} \quad (7-23)$$

The overall routing overhead is calculated by aggregating the respective values of equation (7-19), (7-21) and (7-23). Therefore, the overall control overhead can be expressed as:

$$R_o = \frac{kn^3}{BT_{PR}} + \left[\sum_{P_i \in PA} \sum_{r=0}^{l_i} Q_r^l(T_{PR}) Na(T_{PR}) \right] + \sum_{i=1}^n \frac{\left\lceil \frac{T}{T_{pr}} \right\rceil}{\frac{T}{T_{pr}}} i \quad (7-24)$$

However, probability that uplink state does not change to down link during first r hops Q_r^l is expressed as (N. Zhou, Wu, & Abouzeid, 2005):

$$Q_r^l(T_{PR}) = 1 - e^{-\frac{rT_{pr}}{\mu_k}} \quad (7-25)$$

Where r is the number of hops, e is exponential value and μ_k is the uplink time. Substituting equation (7-25) in (7-24) we obtained:

$$R_o = \frac{kn^3}{BT_{PR}} + \left[\sum_{P_i \in PA} \sum_{r=0}^{l_i} 1 - e^{-\frac{rT_{pr}}{\mu_k}} R_e(T_{PR}) \right] + \sum_{i=1}^n \frac{\left\lceil \frac{T}{T_{pr}} \right\rceil}{\frac{T}{T_{pr}}} i \quad (7-26)$$

As mentioned earlier, hello, TC, MID and HNA are four periodic messages of OLSR. Considering the fundamental theme of OLSR, Hello and TC messages are broadcasted every 2 and 5 seconds, respectively. However, in DS-OLSR (Aliyu et al., 2020) and DS-OLSRMP, these periodic messages have been modified and broadcasted under Network Formation Time

Slice (NFTS) and Topology Propagation Time Slice (TPTS) with the duration of 14 seconds in each network cycle (Aliyu et al., 2020), and transmission interval of 1 second (Hello) and 5 seconds (TC) messages. These can be translated as TC time interval is 5 times of Hello message time interval. Applying the values of NFTS and TPTS messages in the optimised routing overhead model in equation (7-26), we obtained:

$$R_o = \frac{kn^3}{BT_{PR}} + \frac{kn^3}{B * 5T_{PR}} + \left[\sum_{P_i \in PA} \sum_{r=0}^{l_i} 1 - e^{-\frac{rT_{pr}}{\mu_k}} R_e (T_{PR}) \right] + \sum_{i=1}^n \left[\frac{T}{T_{pr+5T_{pr}}} \right] i \quad (7-27)$$

Table 7-3: Parameters for Calculation of Control Overhead

Definition	Symbols	Value (s)
Bandwidth	B	11Mbps
Periodic route update time	T _{pr}	1s(Hello), 5s(TC)
NFTS and TPTS	T _s	14s
Triggered Update message	T	1.5
Routing overhead impulse factor	K	1
Number of Nodes	n	10, 50, 100, 200
Uplink Time	μ _k	28s
Successful packet received	R _e	3pck/sec
Number of hops	r	5
Exponential value	e	2.728

The percentage of the computed control overhead as compared to the simulated as presented in Figures 7-4, 7-5 and 7-6. This metric represents the ratio of DS-OLSRMP control messages (Hello, TC and HNA) that occurs during NFTS and TPTS (Aliyu et al., 2020). It can be observed from Figure 7-4 for static scenario that simulated control overhead is slightly higher with about 0.1, 0.1%, 0.4% and 1.1% for 10, 50, 100, and 200 nodes, respectively as compared to the computed control overhead. This could be attributed to the limitation of simulations as discussed in Chapter 4, and of course the unpredictable nature of wireless communication. For example, if you run 3 simulations using the same parameters and network setting, the results may not be the same due to influence of system hardware and some other factors that facilitates the execution of the simulation.

Under mobility scenarios, more control overhead is expected due to re-initiation of route discovery and topology sensing as shown in Figure 7-5 for pedestrian (1m/s – 2m/s) and in

Figure 7-6 for vehicle movement (5m/s – 12m/s). Again, it can be observed that the simulated control overhead is slightly higher than the calculated due to the adjustment in control message duration and interval. However, the difference between the simulated and computed control overhead is very negligible which can be compensated for error correction. Therefore, the mathematical model proof that DS-OLSRMP reduces routing overhead and it associated energy as compared to the two versions of OLSR (OLSRv1 and OLSRv2).

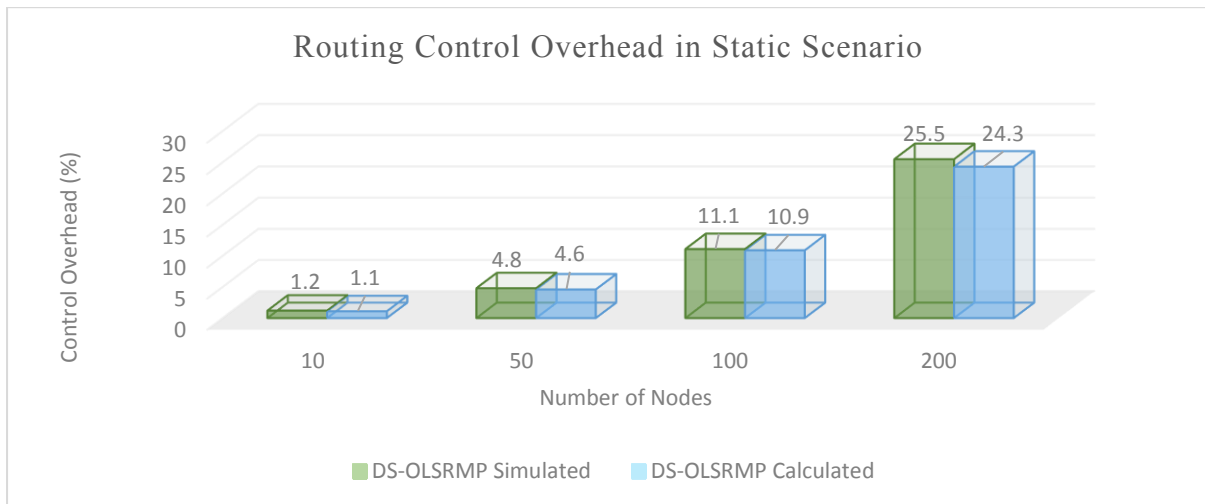


Figure 7-4: Comparison of the Calculated and Simulated Control Overhead in Static Scenario

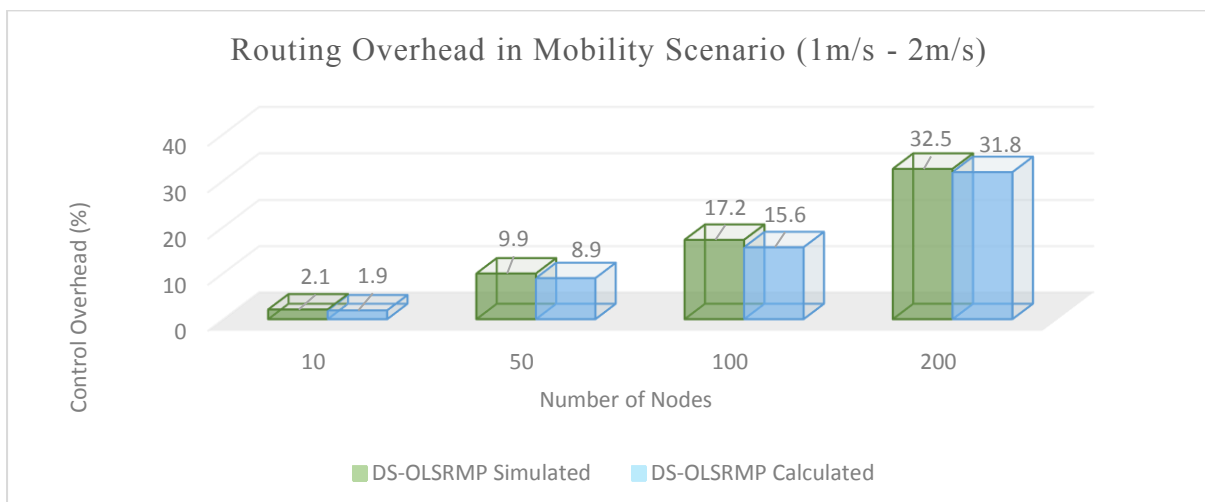


Figure 7-5: Comparison of the Calculated and Simulated Control Overhead in Mobility Scenario (1m/s – 2m/s)

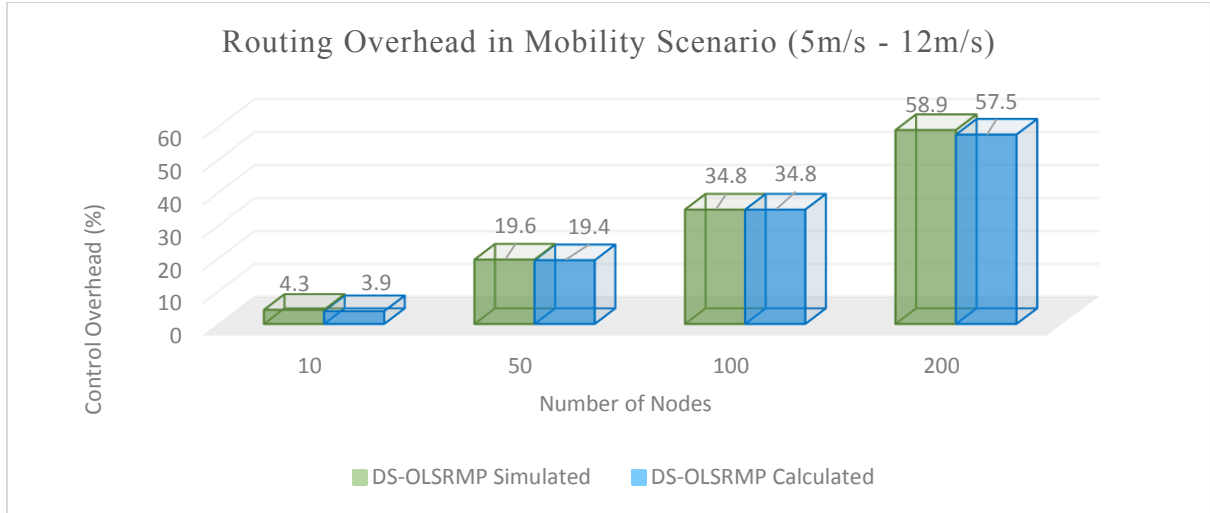


Figure 7-6: Comparison of the Calculated and Simulated Control Overhead in Mobility Scenario (5m/s – 12m/s)

7.5 Packet Delivery Ratio (PDR) Computation

This metric describes the transmission reliability of the proposed DS-OLSRMP. It refers to the percentage of the number of packets delivered successfully to sink node over the total number of data packet sent. it can be represented as:

$$PDR = \frac{\text{Total Packets Successfully Received}}{\text{Total Packets Sent}} \times 100 \quad (7-27)$$

However, to determine the total packets successfully received in a network analytically, we used a probability model called Bernoulli Probability Distribution (N. Zhou et al., 2005). Therefore, the probability that a packet is received successful over a network is expressed as:

$$R_p = \sum_{i=1}^{N^t} \alpha^{i-1} (1 - \alpha) = 1 - \alpha^{N^t} \quad (7-28)$$

Where N^t and α represents number of transmissions per second and probability of success, respectively (N. Zhou et al., 2005). From equation (7-28), the probability of packet transmission when $\alpha = 0$ is 1. This implying that, all transmitted packets are successfully received. However, the probability of packet transmission when $\alpha = 1$ is 0, implying total packet loss or none of the data packet were received. This can be expressed as:

$$R_p = \begin{cases} 1 & , \quad \alpha = 0 \\ 0 & , \quad \alpha = 1 \end{cases} \quad (7-29)$$

From equation (7-28), packet delivery ratio can be represented as:

$$PDR = \frac{R_e}{S_e} \times 100 \quad (7-30)$$

where R_e and S_e represents the total packets received and total packets sent in a network, respectively. Therefore, we calculate the total received packet as presented in equation (7-31).

$$R_e = R_p \times S_e \quad (7-31)$$

Furthermore, the total packet sent in the network S_e can be expressed as in equation (7-32)

$$S_e = \sum_{i=1}^n (nP_s T_t) \quad (7-32)$$

Where n , P_s and T_t are number of nodes, packet sent per second and duration of transmission. Using equation (7-30), the calculated PDR for DS-OLSRMP as compared with the simulated is presented below.

As mentioned earlier, the mathematical model was set up based on the simulation parameters with transmission rate of 3 packets per second per node. With respect to equation (7-30), Figure 7-7 represent the computed mean values of packet delivery ratio (PDR) as compared to the simulated PDR in static scenario. Unlike energy consumption and control overhead, the PDR in the mathematical model computation is slightly higher that the PDR in the simulation. The difference between the calculated and the simulate PDR is trivial and thus can be compensated for error correction.

The PDR is general effected with the implementation of mobility metric in the mathematical model as it does in the simulation model. The PDR were evaluated under two mobility speeds: Pedestrian (1m/s – 2m/s) and Vehicles (5m/s – 12m/s) (Aschenbruck et al., 2009). It can be seen from Figure 7-8 for pedestrian speed and Figure 7-9 for vehicle speed that the computed PDR is slightly higher than the simulated irrespective of the mobility speed and number nodes. However, like static scenario, the difference between the computed and simulated PDR is not

much and can be attributed to other factors that affects the simulation model that cannot quantify mathematically. Overall, the proposed routing scheme delivered more packets in both mathematical and simulation model as compared to the conventional versions of OLSR (OLSRv1 and OLSRv2) as well as compared to similar research by Prakash et al. (2020), and Waheb A. Jabbar et al. (2018).

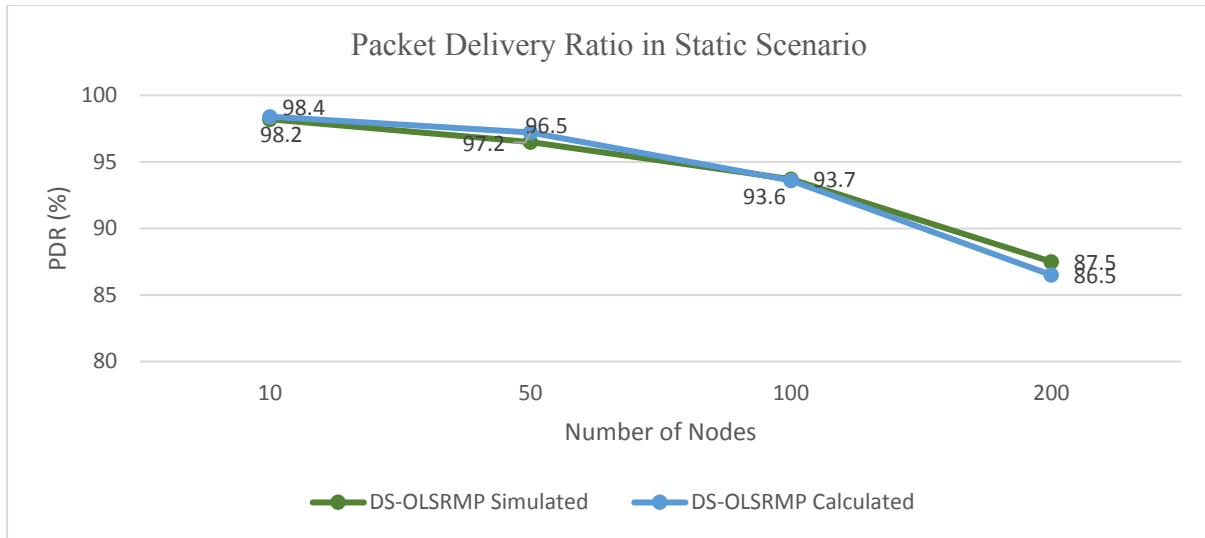


Figure 7-7: Comparison of the Calculated and Simulated Packet Delivery Ratio in Static Scenario

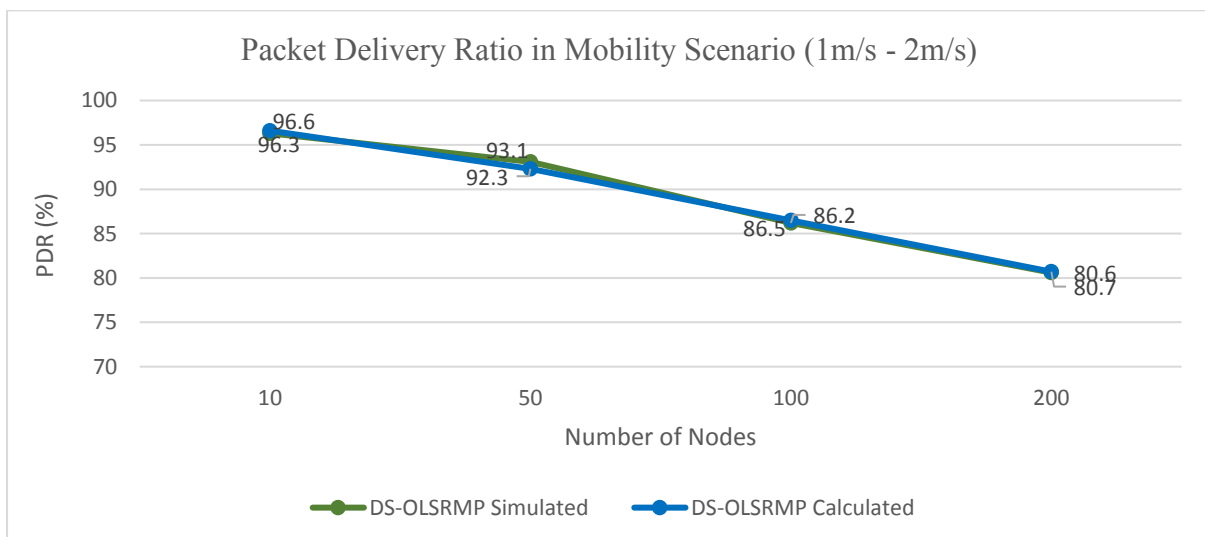


Figure 7-8: Comparison of the Calculated and Simulated Packet Delivery Ratio in Mobility Scenario (1m/s – 2m/s)

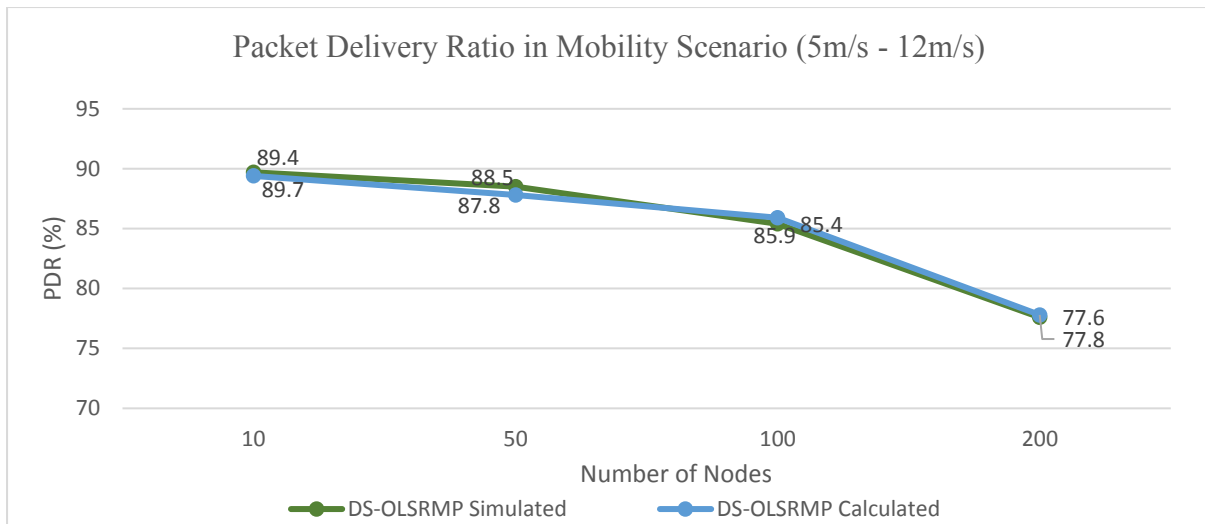


Figure 7-9: Comparison of the Calculated and Simulated Packet Delivery Ratio in Mobility Scenario (5m/s – 12m/s)

7.6 End-to-End Delay Computation

The process of transmitting packet in a conventional switching network from one endpoint to another involves partitioning the packets into smaller segment. The packets are sent separately and later packetized at destination. This process depends largely on number of intermediate nodes (such as hops or routers) and distance between the source and destination nodes. At each intermediate node, a packet suffers several delays (Oechsner, 2020), as discussed in the following sub-section:

7.6.1 Transmission Delay (T_d)

This delay refers to the time required to transmit all bits of packets of size, L over a transmission rate, R in bps. The transmission Delay (T_d) can be calculated as:

$$T_d = \frac{L}{R} \quad (7-33)$$

7.6.2 Propagation Delay (P_d)

This delay indicates the amount of time required for a packet to transverse network between source and destination nodes. It depends heavily on characteristic of the medium in place and the distance between the receiver and transmitter. In a wireless network, the characteristic of the medium is about 3×10^8 m/s, while using fibre optic, information travels through the distance

of the connected nodes with the speed of light, of about 2×10^8 m/s. if d is the distance between connected nodes and c represents medium characteristic, then propagation delay (P_d) can be expressed as:

$$D_p = \frac{d}{c} \quad (7-34)$$

7.6.3 Queueing Delay /Waiting-Time (Q_d)

This delay represents the time a packet spends in queue waiting for on-ward transmission. It strongly depends on the number of packets that required transmission. Queueing Delay (Q_d) is a function of transmission delay, T_d and average queue length, l_q and can be written as:

$$D_q = T_d * l_q \quad (7-35)$$

7.6.4 Processing Delay (P_c)

This delay refers to the time required by a node to analyse received packets. The analysis includes checking packets for error and destination. It completely hardware specific.

7.6.5 Overall Delay in a node (D_n)

This represents the total time spent by a packet in a node. It translated to the sum of transmission, queueing, and processing delay. Thus, it can be expressed as:

$$D_n = T_d + Q_d + P_c \quad (7-36)$$

7.6.6 Overall Delay in a Hop (D_h)

This delay is defined as the total time a packet spends in a hop. The overall delay in a hop is calculated as the sum of propagation delay and overall delay in a node, can be written as:

$$D_h = D_n + P_d \quad (7-37)$$

7.6.7 End-to-End Delay (EED)

This delay indicates the overall time a packet spent between source and destination nodes. This value depends on number of hops and other possible characteristics such as traffic load, retransmission, distance, etc. it can be expressed as:

$$EED = \sum_{\forall i} D_{h,i} \quad (7-38)$$

It can be observed from the above equations that some delays are static. In other words, they do not change over transmission time. However, queuing delay dominants variation in end-to-end delay and therefore, constitute the focus of our analysis in this research.

Table 7-4: Explanation of Terms for the End-to-End Delay Model

<i>Terms</i>	<i>Description</i>
γ	<i>Departure rates all Packets</i>
ψ	<i>Packet arrival rate (Aggregate)</i>
K	<i>Total number of packets in a system</i>
L	<i>Packet Length</i>
λ	<i>Traffic intensity</i>
R	<i>Transmission rate</i>
S	<i>Number servers (processors and transmitters)</i>
Q	<i>Packets in buffer ($K - S$)</i>
P_b	<i>Probability of Packet loss</i>
μ	<i>Poisson arrival process</i>
ρ	<i>System utilisation</i>
EN	<i>Expected number of packets in a system</i>
ED	<i>Expected Packet delay in a System</i>
ED_q	<i>Expected packet delay in a buffer</i>
EN_s	<i>Expected number of packets in a service</i>
EN_q	<i>Expected number of packets in a queue</i>
ED_s	<i>Expected packets delay in a server</i>
$P_e = \mu_0$	<i>Probability that a system is empty at a given time</i>
μ_i	<i>Probability that there are i number of packets at any arbitrary time</i>
$P_b = \mu_k$	<i>Packet loss probability</i>
$\rho = 1 - \mu_0$	<i>System utilisation or fraction of time in which node is actively transmitting packets</i>

If $N_p(t)$ represent network elements in terms of number of packets over time which strongly depends on the function of packet arrival rate, ψ and departure rate, γ . If a packet of a given

size s is sent over a network with a given transmission rate r , then the transmission delay is always the same. However, queueing delay or waiting time always differs as it usually depends on the size of buffer and the buffer state (number of packets in buffer before its arrival). This research derived the model of the end-to-end (EED) based on Oechsner (2020), as presented in Table 7-4.

In modelling network elements, we considered service transmission time as $S[T_s] = \frac{S[L]}{R}$, and maximum packets departure rate as $E\gamma = \frac{v}{S[T_s]}$, with $\lambda = \frac{\psi}{\gamma}$ as traffic intensity. Erlang notation of $M/M/S/K$ and $M/M/1$ is used for network model formation as in [28]. The first and second Ms denotes Poisson arrival and exponential distribution service time, respectively. S represents server and K is the buffer capacity.

Erlang notation of $M/M/S/K$ queueing system has been used for modelling telephone network in the past, where number of servers S represents number of active simultaneous calls in a cell or link (Oechsner, 2020). However, in a typical packet-based network, all links uses a single transmitter, thereby modelled based on $M/M/1/K$ queueing system. This system is a special case of the $M/M/S/K$ with $S = 1$ (single server). The relationship between system state and service state of the $M/M/1/K$ system is presented in Figure 7-10.

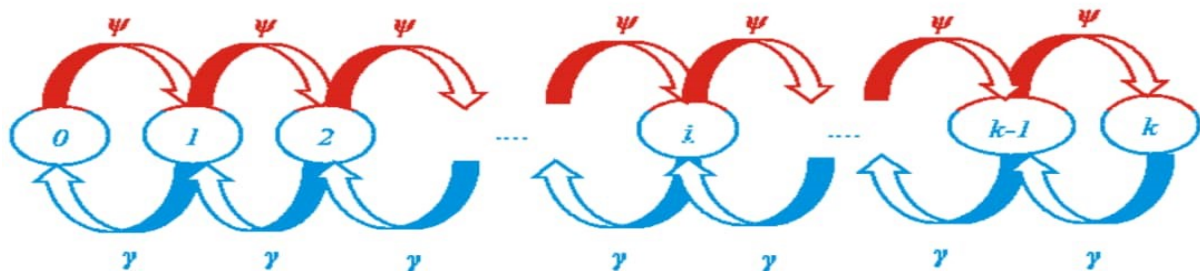


Figure 7-10: Markov Chain for the M/M/1/K queue (Oechsner, 2020)

On the other hand, $M/M/1$ system assumes nodes buffer size is large or infinite ($k = \infty$). This queueing system provides accurate model and allow estimation of different expected end-to-end delay via simple expression than $M/M/1/K$ system (Oechsner, 2020). Therefore, it is considered as a complementary queueing modelling technique can be used to test performance of new system with useful results. The Markov chain for the $M/M/1$ system is depicted in Figure 7-11. Note that, service rate exclusively depends on system state, meaning that busy server is because of high service rate.

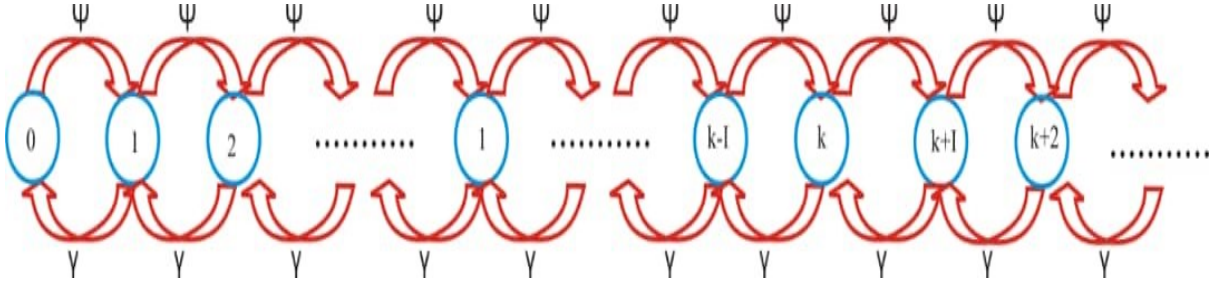


Figure 7-11: Markov Chain for the M/M/1 queue (Oechsner, 2020)

The $M/M/1/K$ queueing system as depicted in Figure 7-10 can be represented in terms of load balancing as follows:

$$\begin{aligned}
 \mu_0 \psi &= \mu_1 \gamma \\
 \mu_1 \psi &= \mu_2 \gamma \\
 &\dots \\
 \mu_{i-1} \gamma &= \mu_i \gamma \rightarrow \mu_i = \left(\frac{\psi}{\gamma}\right) \mu_{i-1} = \lambda \mu_{i-1} \rightarrow \mu_i = \lambda^i \mu_0 \\
 &\dots \\
 \mu_{k-1} \psi &= \mu_k \gamma
 \end{aligned}$$

The above equation indicates that nodes buffer size is very large or infinite ($k = \infty$). Utilizing a normalisation condition for equilibrium distribution, whereby the sum of all probability states is equal to 1, then the 0th state (initial state) probability of $M/M/1/K$ system is given by equation 7-39.

$$\mu_0 = \frac{1}{\sum_{j=0}^k \lambda^j} = \frac{1}{\frac{1 - \lambda^{k+1}}{1 - \lambda}} = \frac{1 - \lambda}{1 - \lambda^{k+1}} \quad (7-39)$$

However, the equilibrium distribution model for $M/M/1$ queueing system is like that of $M/M/1/K$ system, thus considering $K \rightarrow \infty$ that leads $\lambda^{k+1} = 0$, if $\lambda < 1$ as expressed in equation 7-40.

$$\mu_0 = \frac{1}{\sum_{j=0}^{\infty} \lambda^j} = \frac{1}{\frac{1}{1 - \lambda}} = 1 - \lambda \quad (7-40)$$

Having obtained the initial state (0th state) probability for both queueing systems, then the i^{th} probability the $M/M/1/K$ and $M/M/1$ are given by equation 7-41 and 7-42 respectively.

$$\mu_i = \lambda^i \mu_0 = \frac{(1 - \lambda)\lambda^i}{1 - \lambda^{k+1}} \quad (7-41)$$

$$\mu_i = \lambda^i \mu_0 = (1 - \lambda)\lambda^i \quad (7-42)$$

Furthermore, the probability of a packet lost due to overflow is the same as the probability that arriving packet meets state K (system) is full, and can be expressed as in equation 7-43 and 7-44 (Oechsner, 2020).

$$P_b = \mu_k = \frac{(1 - \lambda)\lambda^k}{1 - \lambda^{k+1}} \quad (7-43)$$

$$P_b = 0 \quad (7-44)$$

Similarly, we computed the average number of packets in the system (queue occupancy) when $\lambda \neq 1$ for $M/M/1/K$ and $\lambda < 1$ for $M/M/1$, as expressed in equation 7-45 and 7-46.

$$EN = \sum_{q=0}^k \mu_q q = \frac{\lambda}{1 - \lambda} - \frac{(k + 1)\lambda^{k+1}}{1 - \lambda^{k+1}} \quad (7-45)$$

$$EN = \sum_{q=0}^{\infty} \mu_q q = \frac{\lambda}{1 - \lambda} \quad (7-46)$$

It can observe that, when $\lambda = 1$ implying no packet in the buffer. However, our research considered μ_0 as initial packet and it is on the fact that, whenever a packet is received it meets other packet in the system, thereby necessitate the need for the computation. As mentioned

earlier, we utilized Poisson distribution arrival process for $M/M/1/K$ system to obtain the number of packets in the network using average time spent by packets in the system and arrival rate as expressed in the equation 7-47 through 7-52.

$$ED = \frac{EN}{\psi(1 - P_b)} \quad (7-47)$$

$$ED_q = \frac{EN_q}{\psi(1 - P_b)} \quad (7-48)$$

$$ED_s = \frac{EN_s}{\psi(1 - P_b)} \quad (7-49)$$

$$EN_q = \sum_{i=S+1}^K (i - S) * \mu_i = EN - EN_s \quad (7-50)$$

$$EN_s = \sum_{i=0}^K \min(i, S) * \mu_i \quad (7-51)$$

$$EN = \sum_{i=0}^K i * \mu_i \quad (7-52)$$

The above network model is based on $M/M/1/K$ queuing system of Markov chain which assumes the Poisson arrivals and distributed service times. However, as discussed in (Oechsner, 2020), $M/M/1$ queue system requires value of $\lambda < 1$ and nodes buffer size to be large or infinite ($k = \infty$). Finally, the system also requires low traffic intensity, thereby provides accurate model, and allow estimation of different expected end-to-end delay via simple expression than $M/M/1/K$ system. The queueing system occupancy can be written as in equation 7-53 through 7-58.

$$EN = \sum_{Q=0}^{\infty} \mu_Q Q = \frac{\lambda}{1 - \lambda} \quad (7-53)$$

$$EN_s = 1 - \mu_0 = \lambda \quad (7-54)$$

$$EN_q = EN - EN_s = \frac{\lambda}{1 - \lambda} - \lambda = \frac{\lambda^2}{1 - \lambda} \quad (7-55)$$

$$ED_s = \frac{EN_s}{\psi(1 - P_b)} = \frac{\lambda}{\psi} = \frac{1}{\gamma} \quad (7-56)$$

$$ED = \frac{EN}{\psi(1 - P_b)} = \frac{1}{\gamma(1 - \lambda)} = \frac{1}{\gamma - \psi} \quad (7-57)$$

$$ED_q = \frac{EN_q}{\psi(1 - P_b)} = \frac{\lambda^2}{\psi(1 - \lambda)} = \frac{\lambda}{\gamma(1 - \lambda)} = \frac{\lambda}{\gamma - \psi} \quad (7-58)$$

However, the DS-OLSRMP prioritises message delivery based on device battery energy level. In other words, packets are scheduled to overtake other packets in a queue. Priority scheduling system processes critical priority over packets from lower priorities. This can be achieved either by interrupting low priority packet processing for arrival of critical priority (pre-emptively) or finalising the current packet being processed even if it is a low priority packet, before considering the high priority (non-pre-emptive) (Oechsner, 2020). For the same priority packets, FIFO strategy will be considered.

This research considered non pre-emptive system for modelling the expected queueing delay (ED_q) for DS-OLSRMP to prevent service interruption. The research adopted the previous

$M/M/1$ queueing system to model and drive the EDq with four priority groups: Critical, High, Medium, and Low. The service time distribution for priority group i is denoted as D_{si} , and ψ_i denotes packet arrival rate for this class. Therefore, $\mu_i = \psi_i D_{si}$, with $\mu = \sum_i \mu_i < 1$. The four (4) priority groups are based on a packet that just arrive and the time required to process the packet from priority before it. The average queening/waiting time for the various priorities can be expressed as:

$$ED_{qi} = \sum_{i=1}^4 \frac{\psi ED_s^2}{2(1 - p_i - p_{i-1})(1 - p_i - 1)} \quad (7-59)$$

The above assumptions are based on the theorems of Burkes and Jackson (Tsitsiashvili & Osipova, 2018), that proved $M/M/1$ queueing system follows poisson distribution which allow us to independently model the behaviour of network interfaces. The time a packet spent between source and destination nodes (end-to-end delay) is the sum of average time spends in each relay node or hop and the average delay of the packets in a network which is expressed in equation ...

$$EED = \sum_{\forall i} (ED_n + ED_{qi}) \quad (7-60)$$

Where ED_n and ED_{qi} are expected delay and expected queuing delay, respectively. We usually assume $ED_n = ED$. Substituting ED_n and ED_{qi} from equation 7-57 and 7-58 into equation 7-60 we obtained:

$$EED = \sum_{\forall i} \frac{1}{\gamma - \psi} + \frac{\lambda}{\gamma - \psi} \quad (7-61)$$

$$EED = \sum_{\forall i} \frac{1 + \lambda}{\gamma - \psi} \quad (7-62)$$

Furthermore, we incorporated hop count, H_i , number of nodes, n and time, t . The overall average end-to-end delay ($EDD_{overall}$) of our model is represented by equation 7-63. The parameter used in calculating the $EDD_{overall}$ is presented in Table 7-5.

$$EDD_{overall} = EDD * H_i * n * t \quad (7-63)$$

Table 7-5: Parameters for End-to-End Delay Calculation

<i>Variable</i>	<i>Value</i>	<i>Unit</i>
ψ	(30, 150, 300, 600)	<i>Packets/Seconds</i>
<i>Packet Size</i>	512	<i>Bytes</i>
$E[L]$	4096	<i>Bits</i>
R	11	<i>Kbps</i>
ED_s	0.00037236	<i>Seconds</i>
γ	2685.5731	<i>Packets/Seconds</i>
λ	$0 < \lambda < 1$	<i>Erlangs</i>
n	10, 50, 100, 200	-
t	180	<i>Seconds</i>
H_0	5	-

Figures 7-12, 7-13 and 7-14 represent the computed average end-to-end delay for DS-OLSRMP as compared to the simulated with 10, 50, 100 and 200 nodes in both static and mobility scenarios. This metric indicates the average time over all enduring packets that are transmitted from sending node to receiving node.

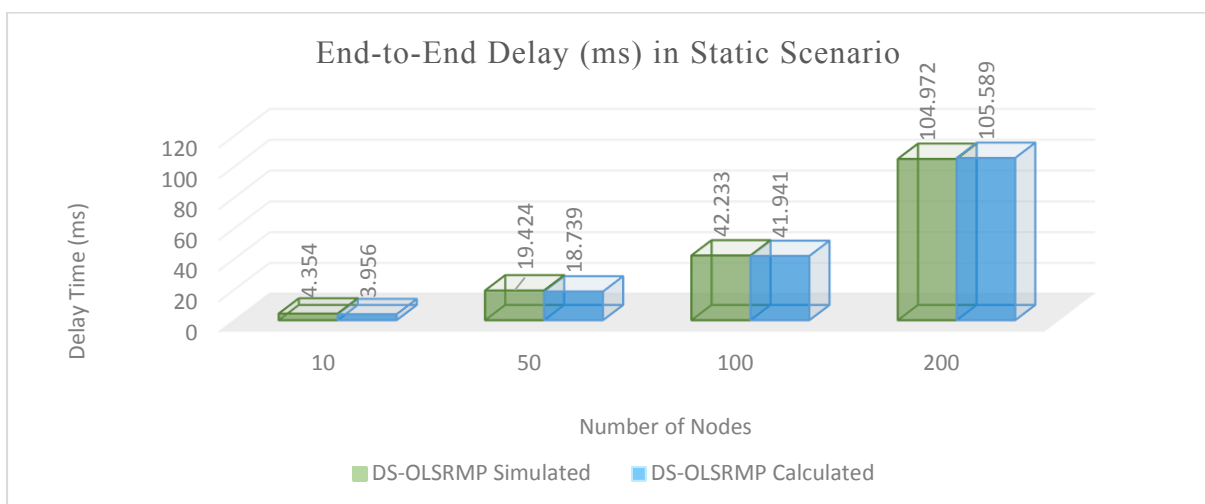


Figure 7-12: Comparison of the Calculated and Simulated End-to-End Delay in Static Scenario

It can be observed from the Figures that the end-to-end delay for both static and mobility scenarios are approximately the same in the simulation and mathematical model, except for 200 nodes in mobility scenarios with pedestrian speed of 1m/s – 2m/s and vehicle speed of 5m/s – 12m/s.

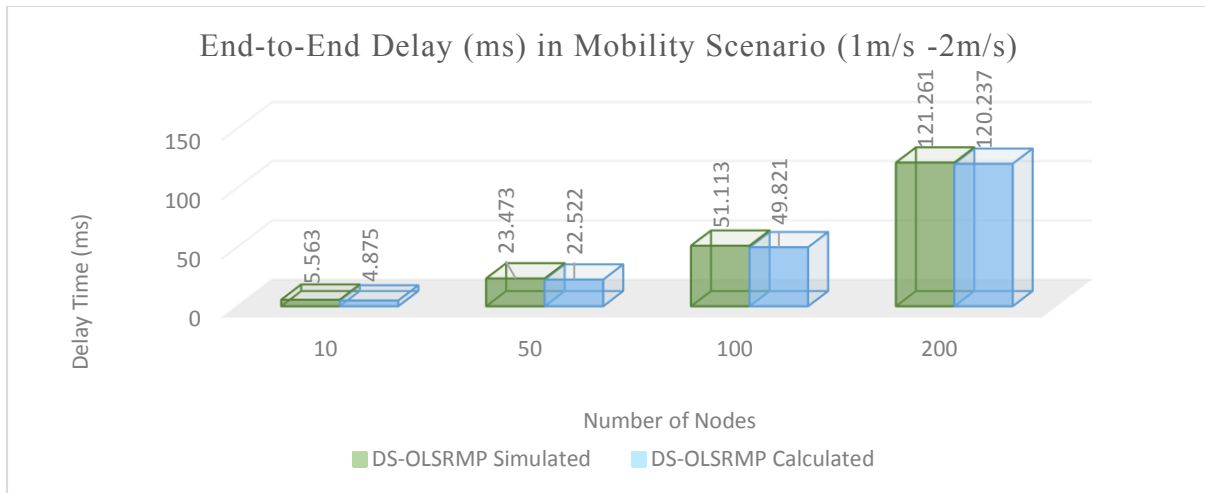


Figure 7-13: Comparison of the Calculated and Simulated End-to-End Delay in Mobility Scenario (1m/s – 2m/s)

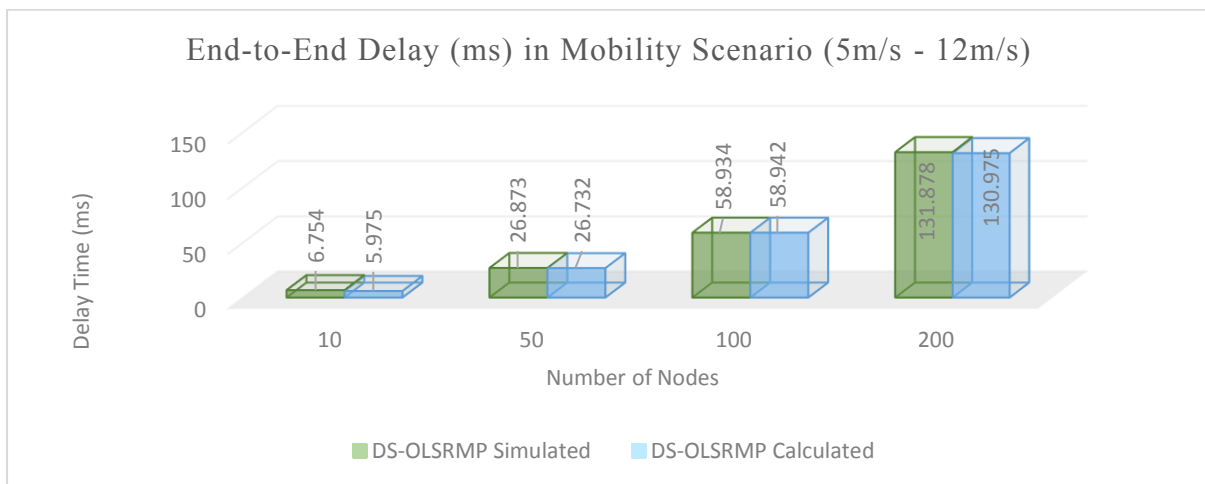


Figure 7-14: Comparison of the Calculated and Simulated End-to-End Delay in Mobility Scenario (5m/s – 12m/s)

The simulated delay shows a slightly higher result with about 0.6ms and 0.8ms for pedestrian and vehicle speeds, respectively as shown in Figures 7-13 and 7-14. The reason for the similarity in the end-to-end delay can be attributed to the concept of TSs that decreases the possibility of link failure and maintain routing information for a longer time in the simulation (Aliyu et al., 2020). The mathematical model proof that DS-OLSRMP reduces end-to-end

delay without sacrificing major quality of service metrics: PDR, energy consumption and routing control overhead.

7.7 Chapter Summary

In this Chapter, the validation of the proposed DS-OLSRMP is discussed through mathematical model which considered the modification of both DS-OLSR and DS-OLSRMP as well as performance evaluation metrics as used in the simulation. The proposed mathematical model was observed and evaluated based on energy consumption, routing control overhead, packet delivery ratio and average end-to-end delay, and compared with simulation results. It was observed that the simulated results of energy consumption, control overhead and end-to-end delay are slightly higher than the computed results. This could be attributed to the limitation of simulations as discussed in Chapter 4, and of course the unpredictable nature of wireless communication. For example, if you run 3 simulations using the same parameters and network setting, the results may not be the same due to influence of system hardware and some other factors that facilitates the execution of the simulation. However, the difference between the calculated and the simulate results is trivial and thus can be compensated for error correction.

Chapter 8

Conclusion and Future Work

8.1 Conclusion

In this thesis, DS-OLSR and DS-OLSRMP routing protocols has been proposed to minimise energy consumption of OLSR protocol and enhance network lifetime for effective communication during disaster recovery and rescue operations. Provision of temporary OLSR protocol driven MANET for survivors to communicate in the aftermath of a disaster often affects their device battery energy, since message routing and network flooding are prominent requirements of OLSR protocol. The objectives of the research were formulated and accomplished successfully to fulfil the research aim.

An intensive review of historical background of MANETs and it routing protocols have been conducted which gives the basic understanding on how MANETs came into play, it features, areas of strength and weakness, thereby providing opportunity to identified suitable routing protocol for this research. The routing protocol under optimisation (OLSR) has been thoroughly discussed with emphasis on operational aspect, version of OLSR adapted for modification and reason for considering proactive OLSR than reactive routing protocols. On the other hand, background research on disasters and networks for disaster recovery and rescue operations highlighting pre and post disaster communication systems without restriction has been critically analysed.

To provide reliable and energy friendly communication network to survivors in the aftermath of a disaster, the proposed routing protocol modified OLSR packet header through the addition of a new field, namely Originator ID (hold device's phone number) and utilises the concept of Time Slices (TSs) to manage and control the disaster network operation. The overall design process that is required for the successful deployment of DS-OLSR were discussed, starting with the process of switching smart phones to disaster mode, from detection of incoming disaster to sending warning message embedded with link for initiating DS-OLSR application and connecting to DS-OLSR MANET. The introduction of the Originator ID provides human readable device information across the network, allowing victims to recognise the sources of their messages and in case of availability of internet connection, it will be used by the victims to send and receive messages. In addition, it leads to the elimination of multiple interface device

(MID) message of conventional OLSR. The design attempts to reduce routing overhead by encapsulating HELLO, Topology Control (TC) and Host Network Association (HNA) messages within their respective Time Slices (TS). Thus, these broadcasts can only occur during NFTS and TPTS, thereby reduced message collision caused by message synchronisation. Modification of 1-hop and 2-hops data sets by including two additional fields, namely PHONE_NO and BATTERY_LIFE which allow prioritisation of message delivery based on node's Battery life. In addition, the Battery life information enables rescue team (RT) members to monitor the Battery life of each device in the network as its displays on the screens connected to the DMS using colours to connote which key MPR device requires backup or replacement. Furthermore, the design of the novel DS-OLSR embedded text message capability called alert message to minimise control overhead and improve energy conservation. DS-OLSR is a full-fledge disaster communication solution that provides a link between DS-OLSR messenger, and the routing layer tables that are created by the messenger and read by DS-OLSR. These tables contain the Battery life, IP address and other related device information. On the other hand, DS-OLSR messenger can equally access tables created by DS-OLSR, especially the Contacts list table which contains the phone number of reachable nodes in the MANET.

The proposed DS-OLSR was initially implemented in NS-3 based on two independent scenarios namely: Simulation of Network Formation and Disaster Area Network. The first simulation was conducted to determine the amount of energy dissipated and control overhead during OLSR/DS-OLSR network formation process, and therefore it is only energy consumption and control overhead that has been analysed. However, the second simulation scenario is to evaluate the performance of the proposed scheme in a disaster related scenario which reflects real life disaster scenario. Therefore, in addition to energy consumption and control overhead, this scenario considered performance metrics including packet delivery ratio and end-to-end delay. Each scenario was executed 10 times using 10, 50, 100 and 200 nodes where mean values of the results were used for evaluations. All DS-OLSR simulations executed seamlessly within a single terminal session. However, the simulation of 200 nodes using OLSRv1 and OLSRv2 failed severally due to generation of massive control traffic that cannot be handled by the system. The reason for resource hungry execution in OLSR simulations with 200 nodes is attributed to the massive generation of the OLSR routing overhead and NS-3 discrete event simulation mode of operations. The simulated scenarios were equally implemented in both static and mobility models. As regards to mobility models, the

proposed scheme considered Random Way Point (RWP) with speed range of pedestrian (1m/s – 2m/s) and vehicle (5m/s – 12m/s). All the simulation results indicates that DS-OLSR performs better than OLSRv1. This performance is attributed to the concept of TSs and elimination of MID messages which confines control messages into their respective, thereby improving link quality by eliminating crosstalk and reducing funnel effect without compromising QoS performance in all the scenarios. DS-OLSR achieved drastic reduction in control messages overheads and energy consumption as compared to classic OLSR through its novel mechanism. However, low battery devices often experience quick power failure which restrict their ability to communicate for longer time during rescue operations and thus DS-OLSRMP has been proposed.

The proposed DS-OLSRMP as an extension to DS-OLSR, not only prioritize messages from devices with low battery energy but also extends the lifespan of communication devices with the low battery energy. In addition, DS-OLSRMP improves overall energy conservation and packet delivery of nodes and may equally improve disaster victim's mental state by quickly responding to messages sent by those whom devices are low in battery energy to prevent such victims from overwhelming the network with messages as their device battery energy dwindles. The message prioritization techniques classified mobile phones into four priority groups - Critical, High, Medium, and Low priorities, thereby prioritizing both message delivery and message status notification for devices with low battery energy. The simulation results shows that energy conservation and packets delivery are notably improved using the message prioritization scheme as compared to DS-OLSR, OLSRv1 and OLSRv2. This achievement can be attributed to the fact that, priority techniques ensure that messages from CP nodes is delivered before messages from other priority and that, CP and HP nodes switch to sleep mode after 10, 000ms and 20, 000ms of MTS, respectively. The performance of the DS-OLSRMP has been validated using a novel mathematical model.

The analytical validation model is based on parameters and metrics evaluated in the simulation of DS-OLSRMP, consisting of Control Overhead, Energy Consumption, Packet Delivery Ratio (PDR) and End-to-End Delay. The mathematical model utilised a transmission rate of 3pct/sec over the duration of 180 seconds with the node density of 10, 50, 100, and 200 nodes as used in the simulation. The simulated and analytical results are approximately the same in both static and mobility scenarios and indicated that the performance of the routing protocol depends largely on various parameters such as network size and mobility speed. The mathematical

model proof that DS-OLSRMP enhances energy efficiency by avoiding the selection of low battery node as MPRs and prioritising their messages, thereby extending the lifespan of the low battery energy devices without sacrificing major quality of service metrics: PDR, average end-to-end delay and routing control overhead. Thus, it is highly recommended for communications in disaster related scenarios.

8.2 Future Work

Although conducting simulation and mathematical models have demonstrated the effectiveness of the proposed DS-OLSR and DS-OLSRMP in certain networks, as both techniques reduced energy consumption and control overhead of OLSR nodes. However, further experiment, and experiences (such as real Testbed) are needed to understand the effects of the proposed schemes in real life scenario. This is because both the simulation and mathematical models has limitations as the parameters used and other input values are based on assumption and previous research.

As mentioned in Section 2.5, this research decided to modify OLSRv1 over OLSRv2 to reduce the number of MPR nodes required by each node whose battery energy may likely drain faster due to routing control overhead. However, the DS-OLSR technique can be ported to OLSRv2 in future since both algorithm of the OLSR versions operates in the same format. Similarly, as mentioned in Section 5.3, the simulation of 200 nodes using OLSRv1 failed severally due to generation of massive control traffic that cannot be handled by the system. In future, a system with a better resource can be used to simulate and compare the performance of the OLSRv1 and OLSRv2 using 200 nodes with the proposed routing protocol. This will give a better picture of the improvement offered by the proposed routing protocol, particularly for dense network scenarios.

The proposed schemes were implemented in a pure MANET network in this thesis, further implementation in a typical Wireless Sensor Network (WSN) and MANET-IoT convergence scenarios are needed to evaluate the performance of the proposed routing protocol in network with devices from different manufacturers. Finally, the implementation of message priority techniques forces message from low priority nodes to stave indefinitely as far as there are messages from higher priority nodes. Therefore, a technique is required to achieve balance and give opportunity for low priority messages to get transmitted on time. The DS-OLSR and DS-OLSRMP technique can be implemented with some routing layer security to evaluate the effect

of security overhead on the proposed routing schemes. This is because security plays an important role in autonomous network such as MANETs and WSN, and therefore need to be considered when deploying such networks (Xiong & Hill, 2009). In addition, the proposed scheme was set to send 3 packets per second as a new system and for observation purpose, however, it will be implemented with a higher such as 8 and 16 packets per second to observe the impact of congestion and noise caused by higher data rate.

References

- Aarti, D. S. (2013). Tyagi, "Study Of Manet: Characteristics, challenges, application and security attacks". *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5), 252-257.
- Adjih, C., Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P., & Raffo, D. (2003). *Securing the OLSR protocol*. Paper presented at the Proceedings of Med-Hoc-Net.
- Aggarwal, A., & Nagrath, P. (2013). *Prioritization of Messages on Community based and Non Community based Protocols in DTN*. Paper presented at the 2013 Third International Conference on Advances in Computing and Communications.
- Aijaz, A., Aghvami, H., & Amani, M. (2013). A survey on mobile data offloading: technical and business perspectives. *IEEE Wireless Communications*, 20(2), 104-112.
- Al-Dalahmeh, M., Al-Shamaileh, O., Aloudat, A., & Obeidat, B. (2018). The Viability of Mobile Services (SMS and Cell Broadcast) in Emergency Management Solutions: An Exploratory Study. *International Journal of Interactive Mobile Technologies*, 12(1).
- Ali, K., Nguyen, H. X., Vien, Q.-T., Shah, P., & Raza, M. (2020). Deployment of drone-based small cells for public safety communication system. *IEEE Systems Journal*, 14(2), 2882-2891.
- Ali, S., Ahmed, A., & Raza, M. (2019, 30-31 Jan. 2019). *Towards Better Routing Protocols for IoT*. Paper presented at the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET).
- Aliyu, U., Takruri, H., Hope, M., & Halilu, A. G. (2020). *DS-OLSR-Disaster Scenario Optimized Link State Routing Protocol*. Paper presented at the 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP).
- Alotaibi, E., & Mukherjee, B. (2012). A survey on routing algorithms for wireless ad-hoc and mesh networks. *Computer Networks*, 56(2), 940-965.
- Alslaim, M. N., Alaqel, H. A., & Zaghoul, S. S. (2014). *A comparative study of MANET routing protocols*. Paper presented at the The Third International Conference on e-Technologies and Networks for Development (ICeND2014).
- Alsumayt, A. (2017). *Mitigate denial of service attacks in mobile ad-hoc networks*. Nottingham Trent University,
- Andersson, K., & Kafle, V. P. (2014, 10-13 Jan. 2014). *Disaster-resilient mobile network architecture*. Paper presented at the Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th.
- Andreas, T., Thomas, L., & Aaron, K. (2017a). <https://github.com/servalproject/olsr/blob/master/unmaintained/README>. Retrieved from <https://github.com/OLSR/olsrd/blob/master/unmaintained/README>
- Andreas, T., Thomas, L., & Aaron, K. (2017b). OLSR.org main repository - olsrd v1. Retrieved from <https://github.com/OLSR/olsrd>. Retrieved 13th August, 2019 <https://github.com/OLSR/olsrd>
- Android, D. (2019). Create Deep Links to App Content. Retrieved from <https://developer.android.com/training/app-links/deep-linking.html>
- Anjum, S. S., Noor, R. M., & Anisi, M. H. (2015). *Survey on MANET based communication scenarios for search and rescue operations*. Paper presented at the 2015 5th International Conference on IT Convergence and Security (ICITCS).
- Anjum, S. S., Noor, R. M., & Anisi, M. H. (2017). Review on MANET based communication for search and rescue operations. *Wireless Personal Communications*, 94(1), 31-52.
- ArsTechnica. (2017). An AT&T drone is now providing cellular service to people in Puerto Rico. Retrieved from <https://arstechnica.com/information-technology/2017/11/att-drone-brings-lte-access-to-hurricane-damaged-puerto-rico/>
- Aschenbruck, N., Gerhards-Padilla, E., & Martini, P. (2009). Modeling mobility in disaster area scenarios. *Performance evaluation*, 66(12), 773-790.

- Bang, A. O., & Ramteke, P. L. (2013). MANET: History, challenges and applications. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 2(9), 249-251.
- Beijar, N. (2002). Zone routing protocol (ZRP). *Networking Laboratory, Helsinki University of Technology, Finland*, 9, 1-12.
- Bhattacharjee, S., Basu, S., Roy, S., & Bit, S. D. (2016). *Best-effort delivery of emergency messages in post-disaster scenario with content-based filtering and priority-enhanced PROPHET over DTN*. Paper presented at the 2016 8th International Conference on Communication Systems and Networks (COMSNETS).
- Boukerche, A., Turgut, B., Aydin, N., Ahmad, M. Z., Bölöni, L., & Turgut, D. (2011). Routing protocols in ad hoc networks: A survey. *Computer Networks*, 55(13), 3032-3080.
- Calarco, G., Casoni, M., Paganelli, A., Vassiliadis, D., & Wódczak, M. (2010). *A satellite based system for managing crisis scenarios: The E-SPONDER perspective*. Paper presented at the 2010 5th Advanced Satellite Multimedia Systems Conference and the 11th Signal Processing for Space Communications Workshop.
- Câmara, D., Frangiadakis, N., Filali, F., Loureiro, A. A., & Rousopoulos, N. (2009). *Virtual access points for disaster scenarios*. Paper presented at the Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE.
- Camps-Mur, D., Garcia-Saavedra, A., & Serrano, P. (2013). Device-to-device communications with Wi-Fi Direct: overview and experimentation. *IEEE Wireless Communications*, 20(3), 96-104.
- Chaubey, N. (2013). Enhancement of security mechanism in design of mobile ad hoc networks using suitable security algorithm.
- Chaudet, C., Dhoutaut, D., & Lassous, I. G. (2005). Performance issues with IEEE 802.11 in ad hoc networking. *IEEE Communications Magazine*, 43(7), 110-116.
- Chavan, G., & Srikanth, V. (2012). *Zone Based Effective Location Aided Routing Protocol for MANET*. Paper presented at the International Conference on Advances in Information Technology and Mobile Communication.
- Cheng, B.-N., Yuksel, M., & Kalyanaraman, S. (2007). *Directional routing for wireless mesh networks: A performance evaluation*. Paper presented at the 2007 15th IEEE Workshop on Local & Metropolitan Area Networks.
- Cheng, B.-N., Yuksel, M., & Kalyanaraman, S. (2009). Orthogonal rendezvous routing protocol for wireless mesh networks. *IEEE/ACM Transactions on Networking (TON)*, 17(2), 542-555.
- Cheng, B.-N., Yuksel, M., & Kalyanaraman, S. (2010). Using directionality in mobile routing. *Wireless Networks*, 16(7), 2065-2086.
- Clausen, T. (2004). Comparative study of routing protocols for mobile ad-hoc networks.
- Clausen, T., Dearlove, C., Jacquet, P., & Herberg, U. (2014). *The optimized link state routing protocol version 2 (2070-1721)*. Retrieved from
- Clausen, T., & Jacquet, P. (2003). Rfc3626: Optimized link state routing protocol (olsr). *Experimental*, <http://www.ietf.org/rfc/rfc3626.txt>, 51.
- Das, S. R., Belding-Royer, E. M., & Perkins, C. E. (2003). Ad hoc on-demand distance vector (AODV) routing.
- David, C. (2015). *LTE Small Cell networks could support multiple public safety organisations*. Retrieved from <http://www.thinksmallcell.com/LTE/lte-small-cell-networks-could-support-multiple-public-safety-organisations.html>
- de Onís, C. M. (2018). Fueling and delinking from energy coloniality in Puerto Rico. *Journal of Applied Communication Research*, 46(5), 535-560.
- De Rango, F., Fotino, M., & Marano, S. (2008). *EE-OLSR: Energy Efficient OLSR routing protocol for Mobile ad-hoc Networks*. Paper presented at the MILCOM 2008-2008 IEEE Military Communications Conference.
- Del Re, E. (2011). *Integrated satellite-terrestrial NAV/COM/GMES system for emergency scenarios*. Paper presented at the 2011 2nd International Conference on Wireless Communication,

- Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE).
- Del Re, E., Morosi, S., Jayousi, S., & Sacchi, C. (2009). *Salice-satellite-assisted localization and communication systems for emergency services*. Paper presented at the 2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology.
- Dervin, M., Buret, I., & Loisel, C. (2008). *Very wide band satellite transmissions for emergency situations*. Paper presented at the 2008 4th Advanced Satellite Mobile Systems.
- Dervin, M., Buret, I., & Loisel, C. (2009). *Easy-to-deploy emergency communication system based on a transparent telecommunication satellite*. Paper presented at the 2009 First International Conference on Advances in Satellite and Space Communications.
- Ehiagwina, F., Afolabi, A., Surajudeen-Bakinde, N., & Fakolujo, O. (2019). Sensitivity degradation and antenna isolation analyses for a multi-operator global systems for mobile communication base transceiver stations. *Nigerian Journal of Technology*, 38(1), 177-184.
- engineersgarage. (2012). How SMS are sent from internet/ websites to mobile phones. Retrieved from https://www.engineersgarage.com/how_to/how-sms-are-sent-from-internet-websites-to-mobile-phones/
- ETSI. (2019a). Alphabets and Language-Specific Information (3GPP TS 23.038 version 15.0.0 Release 15). Retrieved from <https://www.tech-invite.com/3m23/tinv-3gpp-23-038.html>
- ETSI. (2019b). Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface (3GPP TS 44.012 version 15.0.0 Release 15). In.
- ETSI. (2019c). Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041 version 15.5.0 Release 15). In.
- FCC. (2019). Wireless Emergency Alerts (WEA). Retrieved from <https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea>
- Forum, C. B. (2019). What is Cell Broadcast? Retrieved from <http://www.cellbroadcastforum.org/whatisCB/>
- Fotino, M., Gozzi, A., Cano, J.-C., Calafate, C., De Rango, F., Manzoni, P., & Marano, S. (2007). *Evaluating energy consumption of proactive and reactive routing protocols in a MANET*. Paper presented at the IFIP Conference on Wireless Sensor and Actor Networks.
- Fowikes, L. M. (2019). Letter on WEA Geo-targeting Deadline to AT&T. Retrieved from <https://docs.fcc.gov/public/attachments/DOC-357812A1.pdf>
- Gallucci, M. (2018). Rebuilding Puerto Rico's power grid: The inside story. *IEEE Spectrum*.
- Gerla, M. (2002). Fisheye state routing protocol (FSR) for ad hoc networks. *draft-ietf-manet-fsr-03.txt*.
- Gerla, M., Hong, X., & Pei, G. (2000). *Landmark routing for large ad hoc wireless networks*. Paper presented at the Globecom'00-IEEE. Global Telecommunications Conference. Conference Record (Cat. No. 00CH37137).
- Gibson, G., Courtial, J., Padgett, M. J., Vasnetsov, M., Pas'ko, V., Barnett, S. M., & Franke-Arnold, S. (2004). Free-space information transfer using light beams carrying orbital angular momentum. *Optics express*, 12(22), 5448-5456.
- Günes, M., & Reibel, J. (2002). *An IP address configuration algorithm for zeroconf mobile multihop ad hoc networks*. Paper presented at the Proceedings of the International Workshop on Broadband Wireless Ad-Hoc Networks and Services.
- Hartikainen, H., & Harnesk, D. (2009). *A review of secure emergency communications: Technical and organisational aspects*. Paper presented at the Information Systems Research Seminar in Scandinavia: 09/08/2009-12/08/2009.
- Hazra, K., Shah, V. K., Bilal, M., Silvestri, S., Das, S. K., Nandi, S., & Saha, S. (2019). *A Novel Network Architecture for Resource-constrained Post-disaster Environments*. Paper presented at the 2019 11th International Conference on Communication Systems & Networks (COMSNETS).

- He, G. (2002). Destination-sequenced distance vector (DSDV) protocol. *Networking Laboratory, Helsinki University of Technology*, 1-9.
- Hiertz, G. R., Denteneer, D., Max, S., Taori, R., Cardona, J., Berlemann, L., & Walke, B. (2010). IEEE 802.11 s: the WLAN mesh standard. *IEEE Wireless Communications*, 17(1).
- Hill, S. (2015). *Network Technologies, Architectures and Design* University of Salford, Manchester, United Kingdom
- Hinds, A., Ngulube, M., Zhu, S., & Al-Aqrabi, H. (2013). A review of routing protocols for mobile ad-hoc networks (manet). *International journal of information and education technology*, 3(1), 1.
- Ho, A. H., Ho, Y. H., & Hua, K. A. (2010). Handling high mobility in next-generation wireless ad hoc networks. *International Journal of Communication Systems*, 23(9-10), 1078-1092.
- Hong, X., Xu, K., & Gerla, M. (2002). Scalable routing protocols for mobile ad hoc networks. *IEEE Network*, 16(4), 11-21.
- Hope, M. (2015). *Network Simulation and Programming* University of Salford, Manchester, UK.
- Hoque, M. A., Razu, M., Islam, T., & Amin, A. (2020). *SDN-DTN Combined Architecture in Post Disaster Scenario—A new way to start*. Paper presented at the 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS).
- Ibrahim, I. S., King, P. J., & Pooley, R. (2009). *Performance evaluation of routing protocols for MANET*. Paper presented at the 2009 Fourth International Conference on Systems and Networks Communications.
- Intelligencer. (2017). What Happens to the Internet After a Disaster? Retrieved from <http://nymag.com/intelligencer/2017/10/what-happens-to-the-internet-after-a-disaster.html>
- Iqbal, M. (2010). *Design, development and implementation of a high performance wireless mesh network for application in emergency and disaster recovery*. Kingston University,
- Iqbal, M. S., & Al-Raweshidy, H. S. (2013). *Performance evaluation of IEEE 802.15. 4 standard for low data rate ad hoc wireless sensor networks*. Paper presented at the 2013 International Conference on Control, Automation and Information Sciences (ICCAIS).
- Islam, M. S., Riaz, A., & Tarique, M. (2012). Performance analysis of the Routing protocols for video Streaming over mobile ad hoc Networks. *International Journal of Computer Networks & Communications*, 4(3), 133.
- Jabbar, W. A., Ismail, M., & Nordin, R. (2014). *MBA-OLSR: a multipath battery aware routing protocol for MANETs*. Paper presented at the 2014 5th International Conference on Intelligent Systems, Modelling and Simulation.
- Jabbar, W. A., Saad, W. K., & Ismail, M. (2018). MEQSA-OLSRv2: A Multicriteria-Based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT. *IEEE Access*, 6, 76546-76572. doi:10.1109/ACCESS.2018.2882853
- Jagannath, J., Furman, S., Jagannath, A., Ling, L., Burger, A., & Drozd, A. (2019). HELPER: Heterogeneous Efficient Low Power Radio for enabling ad hoc emergency public safety networks. *Ad Hoc Networks*, 89, 218-235.
- Jahir, Y., Atiquzzaman, M., Refai, H., Paranjothi, A., & LoPresti, P. G. (2019). Routing protocols and architecture for disaster area network: A survey. *Ad Hoc Networks*, 82, 1-14.
- Jameel, F., Hamid, Z., Jabeen, F., Zeadally, S., & Javed, M. A. (2018). A Survey of Device-to-Device Communications: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*.
- Jayanti, V. N. (2014). Routing Protocols in MANET: Comparative Study. *International Journal of Computer Science and Mobile Computing*, 3(7), 119-125.
- Jeong, J.-H. P., Cha, H.-W., Park, J.-S., & Kim, H.-J. (2003). Ad Hoc IP Address Autoconfiguration. draft-jeong-adhoc-ip-addr-autoconf-00. txt. *Internet Engineering Task Force, MANET working group*.
- Jiang, M. (1999). Cluster based routing protocol (CBRP). *IETF Internet-draft*.

- Johnson, D., Hu, Y.-c., & Maltz, D. (2007). *The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4* (2070-1721). Retrieved from
- Kanchanasut, K., Wongsardsakul, T., Chansutthirangkool, M., Laouiti, A., Tazaki, H., & Arefin, K. R. (2008). *Dumbo ii: a v-2-i emergency network*. Paper presented at the Proceedings of the 4th Asian Conference on internet Engineering.
- Karaulia, D. S., & Bharot, N. (2014). *Dynamic TTL Variance Foretelling Based Enhancement of AODV Routing Protocol in MANET*. Paper presented at the 2014 Fourth International Conference on Communication Systems and Network Technologies.
- Karp, B., & Kung, H.-T. (2000). *GPSR: Greedy perimeter stateless routing for wireless networks*. Paper presented at the Proceedings of the 6th annual international conference on Mobile computing and networking.
- Kaur, S. (2011). Performance Comparison of DSR and AODV Routing Protocols with Efficient Mobility Model in Mobile Ad-Hoc Network. *IJCST*, 2(2).
- Khatkar, A., & Singh, Y. (2012). *Performance evaluation of hybrid routing protocols in mobile ad hoc networks*. Paper presented at the 2012 Second International Conference on Advanced Computing & Communication Technologies.
- Ko, Y. B., & Vaidya, N. H. (2000). Location-Aided Routing (LAR) in mobile ad hoc networks. *Wireless Networks*, 6(4), 307-321.
- Kodole, A., & Agarkar, P. (2015). A survey of routing protocols in mobile ad hoc networks. *Multidisciplinary Journal of Research in Engineering and Technology*, 2(1), 336-341.
- Kose, S., Koytak, E., & Hascicek, Y. S. (2012). An overview on the use of satellite communications for disaster management and emergency response. *International Journal of Emergency Management*, 8(4), 350-382.
- Kumari, N., Kumar, R., & Bajaj, R. (2018). energy efficient communication using reconfigurable directional antenna in MANET. *Procedia Computer Science*, 125, 194-200.
- Lalar, S., & Yadav, A. K. (2017). Comparative Study of Routing protocols in MANET. *OJCST*, 10, 174.
- Lee, Y.-M., Ku, B.-J., & Ahn, D.-S. (2010). *A satellite core network system for emergency management and disaster recovery*. Paper presented at the 2010 International conference on information and communication technology convergence (ICTC).
- Lee, Y.-Z., Chen, J., Hong, X., Xu, K., Breyer, T., & Gerla, M. (2005). *Experimental evaluation of LANMAR, a scalable ad-hoc routing protocol*. Paper presented at the IEEE Wireless Communications and Networking Conference, 2005.
- Li, P., Miyazaki, T., Wang, K., Guo, S., & Zhuang, W. (2017). Vehicle-assist resilient information and network system for disaster management. *IEEE Transactions on Emerging Topics in Computing*, 5(3), 438-448. doi:10.1109/TETC.2017.2693286
- Lien, Y.-N., Jang, H.-C., & Tsai, T.-C. (2009). *A MANET Based Emergency Communication and Information System for Catastrophic Natural Disasters*. Paper presented at the 2009 29th IEEE International Conference on Distributed Computing Systems Workshops.
- Lien, Y. N., Hung-Chin, J., & Tzu-Chieh, T. (2009, 18-20 May 2009). *Design of P2Pnet: An Autonomous P2P Ad-Hoc Group Communication System*. Paper presented at the Mobile Data Management: Systems, Services and Middleware, 2009. MDM '09. Tenth International Conference on.
- Lien, Y. N., Li-Cheng, C., & Yuh-Sheng, S. (2009, 14-16 Dec. 2009). *A Walkie-Talkie-Like Emergency Communication System for Catastrophic Natural Disasters*. Paper presented at the Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on.
- Lieser, P., Richerzhagen, N., Luser, S., Richerzhagen, B., & Steinmetz, R. (2019). *Understanding the Impact of Message Prioritization in Post-Disaster Ad Hoc Networks*. Paper presented at the 2019 International Conference on Networked Systems (NetSys).
- Lisa, F. M. (2019). Letter on WEA Geo-targeting Deadline to Sprint. Retrieved from <https://docs.fcc.gov/public/attachments/DOC-357814A1.pdf>

- LISICOS. (2019). The Long Island Sound Integrated Coastal Observing System. Retrieved from https://lisicos.uconn.edu/about_artg.php
- Liu, S., Yang, Y., & Wang, W. (2013). Research of AODV routing protocol for ad hoc networks1. *AASRI Procedia*, 5, 21-31.
- Lu, W., Seah, W. K., Peh, E. W., & Ge, Y. (2007). Communications support for disaster recovery operations using hybrid mobile ad-hoc networks. *IEEE Conference*, 763--770.
- Lu, Z., Cao, G., & La Porta, T. (2016). *Networking smartphones for disaster recovery*. Paper presented at the 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom).
- Lu, Z., Cao, G., & La Porta, T. (2017). Teamphone: Networking smartphones for disaster recovery. *IEEE Transactions on mobile computing*, 16(12), 3554-3567.
- Mahmood, D., Javaid, N., Qasim, U., Khan, Z. A., Khan, A., Qurashi, S., & Memon, A. (2013). Modeling and Evaluating Performance of Routing Operations in Proactive Routing Protocols. *arXiv preprint arXiv:1309.4389*.
- Mao, B., Tang, F., Fadlullah, Z. M., & Kato, N. (2019, 20-24 May 2019). *An Intelligent Packet Forwarding Approach for Disaster Recovery Networks*. Paper presented at the ICC 2019 - 2019 IEEE International Conference on Communications (ICC).
- Mbarushimana, C., & Shahrabi, A. (2007). *Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks*. Paper presented at the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07).
- McCabe, A., Cullen, A., Fredin, M., & Axelsson, L. (2005). *A power consumption study of DSR and OLSR*. Paper presented at the MILCOM 2005-2005 IEEE Military Communications Conference.
- Minh, Q. T., & Yamada, S. (2015). Feasibility Validation of WiFi Based Multihop Access Network for Disaster Recovery. 473-477. doi:10.1109/waina.2015.40
- Minh Quang Tran, Kien, N., Borcea, C., & Yamada, S. (2014). On-the-fly establishment of multihop wireless access networks for disaster recovery. *Communications Magazine, IEEE*, 52(10), 60-66. doi:10.1109/MCOM.2014.6917403
- Mishra, A., Singh, S., & Tripathi, A. K. (2019). Comparison of Manet Routing Protocols.
- Mohseni, S., Hassan, R., Patel, A., & Razali, R. (2010). *Comparative review study of reactive and proactive routing protocols in MANETs*. Paper presented at the 4th IEEE International Conference on Digital Ecosystems and Technologies.
- Mohsin, M., & Prakash, R. (2002). *IP address assignment in a mobile ad hoc network*. Paper presented at the MILCOM 2002. Proceedings.
- Morello, A., & Mignone, V. (2006). DVB-S2: The second generation standard for satellite broad-band services. *Proceedings of the IEEE*, 94(1), 210-227.
- Morrison, K. T. (2011). Rapidly recovering from the catastrophic loss of a major telecommunications office. *Communications Magazine, IEEE*, 49(1), 28--35.
- Munisha Devi, N. S. G. (2018). Comparison analysis of MANET routing protocols to identify their suitability in smart environment. *International Journal of Engineering & Technology*.
- Narayanan, R. G. L., & Ibe, O. C. (2012). A joint network for disaster recovery and search and rescue operations. *Computer Networks*, 3347--3373.
- Nesargi, S., & Prakash, R. (2002). *MANETconf: Configuration of hosts in a mobile ad hoc network*. Paper presented at the Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies.
- Night, N. (2017, September 2017). NOAA Satellites. *NBC Highly News*. Retrieved from <https://twitter.com/NBCNightlyNews/status/912345728365842432>
- Nikaein, N., Labiod, H., & Bonnet, C. (2000). *DDR: distributed dynamic routing algorithm for mobile ad hoc networks*. Paper presented at the Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing.

- Nishiyama, H., Ito, M., & Kato, N. (2014). Relay-by-smartphone: realizing multihop device-to-device communications. *IEEE Communications Magazine*, 52(4), 56-65.
- NOAA. (2019a). GOES Imagery Color Enhancements. Retrieved from <https://www.goes.noaa.gov/enhanced.html>
- NOAA. (2019b). National Hurricane Center. Retrieved from <https://www.nhc.noaa.gov/>
- NOAA. (2019c). Watches, Warnings or Advisories for Hawaii. Retrieved from <https://alerts.weather.gov/cap/hi.php?x=1>
- Nokia. (2015). *LTE network in a box*. Retrieved from <http://networks.nokia.com/file/40441/lte-network-in-a-box>
- Nong, L. (2014). *Simulation Design and Analysis of LANMAR Routing Protocol*. Paper presented at the 2014 International Conference on Computational Intelligence and Communication Networks.
- ns3::WifiPhy. (2019). ns3::WifiPhy Class Reference. Retrieved from https://www.nsnam.org/doxygen/classns3_1_1_wifi_phy.html
- Ns-3. (2021). IPv6 model description. Retrieved from <https://www.nsnam.org/docs/models/html/ipv6.html>
- nsnam. (2019). NS-3 OLSR module. Retrieved from https://www.nsnam.org/doxygen/group_OLSR.html
- Oberg, J. C., Whitt, A. G., & Mills, R. M. (2011). Disasters will happen-are you ready? *IEEE Communications Magazine*, 49(1), 36-42.
- Oechsner, B. B. a. S. (2020). *Analysis of Packet Queueing in Telecommunication Networks*.
- Ogier, R., Templin, F., & Lewis, M. (2004). *Topology dissemination based on reverse-path forwarding (TBRPF)* (2070-1721). Retrieved from
- Ogier, R. G. (2002). Topology broadcast based on reverse-path forwarding (TBRPF). *Internet Engineering Task Force (IETF) draft, draft-ietf-manettbrpf-06. txt*.
- Ohyama, T., Kaneko, Y., Asano, K., & Hamaguchi, M. (2012, 24-27 Sept. 2012). *Multi-hop communication and multi-protocol gateway by using plural ITS*. Paper presented at the Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on.
- One2Many. (2019). Cell broadcast system. Retrieved from <https://www.one2many.eu/en/cell-broadcast/system-architecture>
- Onwuka, E., Folaponmile, A., & Ahmed, M. (2011). Manet: A reliable network in disaster areas. *J. Res. Natl. Dev. Transcampus*.
- Pandey, A., Ahmed, M. N., Kumar, N., & Gupta, P. (2006). *A hybrid routing scheme for mobile ad hoc networks with mobile backbones*. Paper presented at the International Conference on High-Performance Computing.
- Park, V. (2001). Temporally-ordered routing algorithm (TORA) version 1 functional specification. *Internet Draft, draft-ietf-manet-tora-spec-04. txt*.
- Park, V. D., & Corson, M. S. (1997). *A highly adaptive distributed routing algorithm for mobile wireless networks*. Paper presented at the Proceedings of INFOCOM'97.
- Patel, S., Elleithy, K., & Rizvi, S. S. (2009). *Hierarchically Segmented Routing (HSR) Protocol for MANET*. Paper presented at the 6th International Conference on Information Technology: New Generations ITNG.
- Pearlman, M. R., & Haas, Z. J. (1999). Determining the optimal configuration for the zone routing protocol. *IEEE Journal on Selected Areas in Communications*, 17(8), 1395-1414.
- Pei, G., Gerla, M., & Hong, X. (2000). *LANMAR: landmark routing for large scale wireless ad hoc networks with group mobility*. Paper presented at the Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing.
- Peng, W., Yan, C., Liu, X., & Deng, L. (2009). *Emergency command system for geologic disasters prevention*. Paper presented at the 2009 Fifth International Conference on Information Assurance and Security.

- Perkins, C. E. (2000). IP address autoconfiguration for ad hoc networks. *draft-ietf-manet-autoconf-01.txt*.
- Prakash, K., Philip, P. C., Paulus, R., & Kumar, A. (2020). A packet fluctuation-based OLSR and efficient parameters-based OLSR routing protocols for urban vehicular ad hoc networks. In *Recent Trends in Communication and Intelligent Systems* (pp. 79-87): Springer.
- PSAV. (2019). Bandwidth Calculator Retrieved from <https://www.psav.com/bandwidth-calculator>
- Qin, H., Mi, Z., Dong, C., Peng, F., & Sheng, P. (2016). *An experimental study on multihop D2D communications based on smartphones*. Paper presented at the 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring).
- Raffelsberger, C., & Hellwagner, H. (2013). *A hybrid MANET-DTN routing scheme for emergency response scenarios*. Paper presented at the 2013 IEEE international conference on pervasive computing and communications workshops (PERCOM workshops).
- Raj, M., Kant†, K., & Das, S. K. (2014). *E-DARWIN: Energy Aware Disaster Recovery Network using WiFi Tethering*. Paper presented at the Computer Communication and Networks (ICCCN), 2014 23rd International Conference.
- Rajkumar, G., Kasiram, R., & Parthiban, D. (2012). *Optimized QoS metrics and performance comparison of DSR and AODV routing protocols*. Paper presented at the IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM-2012).
- Ramanathan, R., & Redi, J. (2002). A brief overview of ad hoc networks: challenges and directions. *IEEE Communications Magazine*, 40(5), 20-22.
- Rattagan, E. (2016). *Wi-Fi usage monitoring and power management policy for smartphone background applications*. Paper presented at the Management and Innovation Technology International Conference (MITicon), 2016.
- Raval, T. J., & Shah, J. (2011). *Network density based analysis of geographic routing protocol for random mobility of nodes in manet*. Paper presented at the 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC).
- Re, E. D. (2012, 2-5 Oct. 2012). *Satellite communications for emergency*. Paper presented at the 2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL).
- Reddy, P. N., Vishnuvardhan, C., & Ramesh, V. (2013). An Overview on Reactive Protocols for Mobile Ad-Hoc Networks. *International Journal of Computer Science and Mobile Computing*, 2, 368-375.
- Research, U. N. (2019). OLSR Routing Protocol Implementation Retrieved from <https://www.nrl.navy.mil/itd/ncs/products/OLSR>
- Roizen, J. (1981). Teletext in the USA. *SMPTE Journal*, 90(7), 602-610.
- Rong, P., & Pedram, M. (2006). An analytical model for predicting the remaining battery capacity of lithium-ion batteries. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 14(5), 441-451.
- Roy, R. R. (2010). *Handbook of mobile ad hoc networks for mobility models*: Springer Science & Business Media.
- Roy, R. R. (2011). *Handbook of mobile ad hoc networks for mobility models* (Vol. 170): Springer.
- Safa, H., Artail, H., & Tabet, D. (2010). A cluster-based trust-aware routing protocol for mobile ad hoc networks. *Wireless Networks*, 16(4), 969-984.
- Sakano, T., Fadlullah, Z. M., Thuan, N., Nishiyama, H., Nakazawa, M., Adachi, F., . . . Kurihara, S. (2013). Disaster-resilient networking: a new vision based on movable and deployable resource units. *Network, IEEE*, 27(4), 40-46. doi:10.1109/MNET.2013.6574664
- Sanchez, F. (2017). Wireless Emergency Alerts. Retrieved from https://ecfsapi.fcc.gov/file/1071068050241/FCC_ExParteLetter-SIGNED_7-10-17.pdf
- Santhi, S., & Sadasivam, G. S. (2011). Power aware QoS multipath routing protocol for disaster recovery networks. *International Journal of Wireless & Mobile Networks*, 3(6), 47.

- Saravanan, T., & Nithya, N. (2020). *Mitigation of attack patterns based on routing reliance approach in MANETs*. Paper presented at the 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).
- Saudi, N. A. M., Arshad, M. A., Buja, A. G., Fadzil, A. F. A., & Saidi, R. M. (2019, 2019//). *Mobile Ad-Hoc Network (MANET) Routing Protocols: A Performance Assessment*. Paper presented at the Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017), Singapore.
- Shenbagapriya, R., & Kumar, N. (2014). *A survey on proactive routing protocols in MANETs*. Paper presented at the 2014 International Conference on Science Engineering and Management Research (ICSEMR).
- Singh, K., Sharma, A., & Singh, N. K. (2015). *Linear regression based energy aware location-aided routing protocol for mobile ad-hoc networks*. Paper presented at the 2015 International Conference on Computational Intelligence and Communication Networks (CICN).
- Singh, S., Woo, M., & Raghavendra, C. S. (1998). *Power-aware routing in mobile ad hoc networks*. Paper presented at the MobiCom.
- Skinemoen, H., Hansen, S., & Jahn, A. (2007). *Satellite-Based Infrastructure for Emergency Communications*. Paper presented at the 25th AIAA International Communications Satellite Systems Conference (organized by APSCC).
- Solmaz, G., & Turgut, D. (2017). Modeling pedestrian mobility in disaster areas. *Pervasive and Mobile Computing, 40*, 104-122.
- SQLite. (2019). What Is SQLite? Retrieved from <https://www.sqlite.org/index.html>
- Szücs, V., & Wassouf, M. (2018). *Modified MANET protocol to extend the emergency network*. Paper presented at the 2018 9th IEEE International Conference on Cognitive Infocommunications (CogInfoCom).
- Thomasson, L., Verelst, G., Deprey, S., Boutry, P., Berioli, M., & Courville, N. (2008). *Hybrid satellite-terrestrial based solutions for rapid deployment of wireless telecommunication networks in emergency situations*. Paper presented at the 15th Annual Conference of the International Emergency Management Society (TIEMS).
- TIROS. (2016). NASA Science. Retrieved from <https://science.nasa.gov/missions/tiros/>
- Toth, Z., & Buizza, R. (2019). Weather Forecasting: What Sets the Forecast Skill Horizon? In *Sub-Seasonal to Seasonal Prediction* (pp. 17-45): Elsevier.
- Tsitsiashvili, G., & Osipova, M. (2018). Generalization and extension of Burke theorem. *Reliability: Theory & Applications, 13*(1 (48)).
- Uchida, N., Takahata, K., Shibata, Y., & Shiratori, N. (2012). Never die network based on cognitive wireless network and satellite system for large scale disaster. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 3*(3), 74-93.
- Vaidya, N. H. (2002). *Weak duplicate address detection in mobile ad hoc networks*. Paper presented at the Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing.
- Van Westen, C. (2000). Remote sensing for natural disaster management. *International archives of photogrammetry and remote sensing, 33*(B7/4; PART 7), 1609-1617.
- Vasseur, J.-P., Pickavet, M., & Demeester, P. (2004). *Network recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*: Elsevier.
- Verma, N., & Soni, S. (2017). A Review of Different Routing Protocols in MANET. *International Journal of Advanced Research in Computer Science, 8*(3).
- Vijayalakshmi, D. S., & Sweatha, M. (2016). A Survey on History and Types of Manet. *International Journal of Emerging Trends in Science and Technology*03 (07), 4310-4315.
- Vishwanath, K. V., Greenberg, A., & Reed, D. A. (2009). *Modular data centers: how to design them?* Paper presented at the Proceedings of the 1st ACM workshop on Large-Scale system and application performance.

- Viswanath, K., Obraczka, K., & Tsudik, G. (2005). Exploring mesh and tree-based multicast. Routing protocols for MANETs. *IEEE Transactions on mobile computing*, 5(1), 28-42.
- Vo, N.-S., Duong, T. Q., & Guizani, M. (2015). *Quality of sustainability optimization design for mobile ad hoc networks in disaster areas*. Paper presented at the 2015 IEEE Global Communications Conference (GLOBECOM).
- Wang, X., Hsu, C. Y., & Jin, X. (2008). *Mobile free space optical communication system*. Paper presented at the Free-Space Laser Communication Technologies XX.
- Wang, X., Jiang, F., Zhong, L., Ji, Y., Yamada, S., Takano, K., & Xue, G. (2020). Intelligent post-disaster networking by exploiting crowd big data. *IEEE network*, 34(4), 49-55.
- Weniger, K. (2003). *Passive duplicate address detection in mobile ad hoc networks*. Paper presented at the 2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003.
- Witt, M., & Turau, V. (2005). *BGR: Blind geographic routing for sensor networks*. Paper presented at the Third International Workshop on Intelligent Solutions in Embedded Systems, 2005.
- Wódczak, M. (2012). *Autonomic cooperative communications for emergency networks*. Paper presented at the 2012 IEEE Globecom Workshops.
- Wu, X., Sadjadpour, H. R., & Garcia-Luna-Aceves, J. (2007). *Routing overhead as a function of node mobility: modeling framework and implications on proactive routing*. Paper presented at the 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems.
- Wu, Y., Xu, L., Lin, X., & Fang, J. (2017). *A new routing protocol based on OLSR designed for UANET maritime search and rescue*. Paper presented at the International Conference on Internet of Vehicles.
- Xiong, X., & Hill, S. (2009). *The Impact of Operating Frequency on Power Optimization for Wireless Sensor Networks Security*. Paper presented at the 2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies.
- Xue, Y., Jiang, H., & Hu, H. (2008). *Optimization on OLSR protocol for lower routing overhead*. Paper presented at the International Conference on Rough Sets and Knowledge Technology.
- Yadav, A., & Joshi, P. (2012). Performance of flat routing protocols in MANET. *International Journal of Electronics and Computer Science Engineering*, 1(4), 2035-2041.
- Yadav, M., & Uparosiya, N. (2014). Survey on MANET: Routing protocols, advantages, problems and security. *International Journal of Innovative Computer Science & Engineering*, 1(2), 12-17.
- Yang, P.-I., Tian, C., & Yu, Y. (2005). *Analysis on optimizing model for proactive ad hoc routing protocol*. Paper presented at the MILCOM 2005-2005 IEEE Military Communications Conference.
- Yellanki, P., & Narasimham, M. P. (2020). *Secure Routing Protocol for VANETS using ECC*. Paper presented at the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA).
- Yi, J. (2010). *Multipath routing protocol for mobile ad hoc networks*. Université de Nantes,
- Yong, B., Wencai, D., Zhengxin, M., Chong, S., Youling, Z., & Baodan, C. (2010, 25-27 June 2010). *Emergency communication system by heterogeneous wireless networking*. Paper presented at the Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on.
- Yu, J., Qi, Y., Wang, G., & Gu, X. (2012). A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution. *AEU-International Journal of Electronics and Communications*, 66(1), 54-61.
- Zhiyuan, L. (2009). *Geographic routing protocol and simulation*. Paper presented at the 2009 Second International Workshop on Computer Science and Engineering.
- Zhou, H., Ni, L. M., & Mutka, M. W. (2003). Prophet address allocation for large scale MANETs. *Ad Hoc Networks*, 1(4), 423-434.
- Zhou, J., Zhou, C., Kang, Y., & Tu, S. (2021). Integrated satellite-ground post-disaster emergency communication networking technology. *Natural Hazards Research*, 1, 4-10.

- Zhou, N., Wu, H., & Abouzeid, A. A. (2005). The impact of traffic patterns on the overhead of reactive routing protocols. *IEEE Journal on Selected Areas in Communications*, 23(3), 547-560.
- Oksiiuk, O., & Krotov, V. (2019). Analysis and choice of routing protocols in wireless Ad Hoc networks based on the use the neural network. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, 9.

Appendices

Appendix A: NS - Simulation Command and Some Screenshot of Simulation Environment

The following NS-3 *waf* command which is responsible for executing NS-3 simulation files as specified in the command.

```
./waf --run "olsr-ds-auto --numNodes=200 --traceFile = disaster 200 nodesstatic --txRange=50" --vis
```

The “vis” command provides graphic interface and animation of the simulation as in Figures B1 and B2

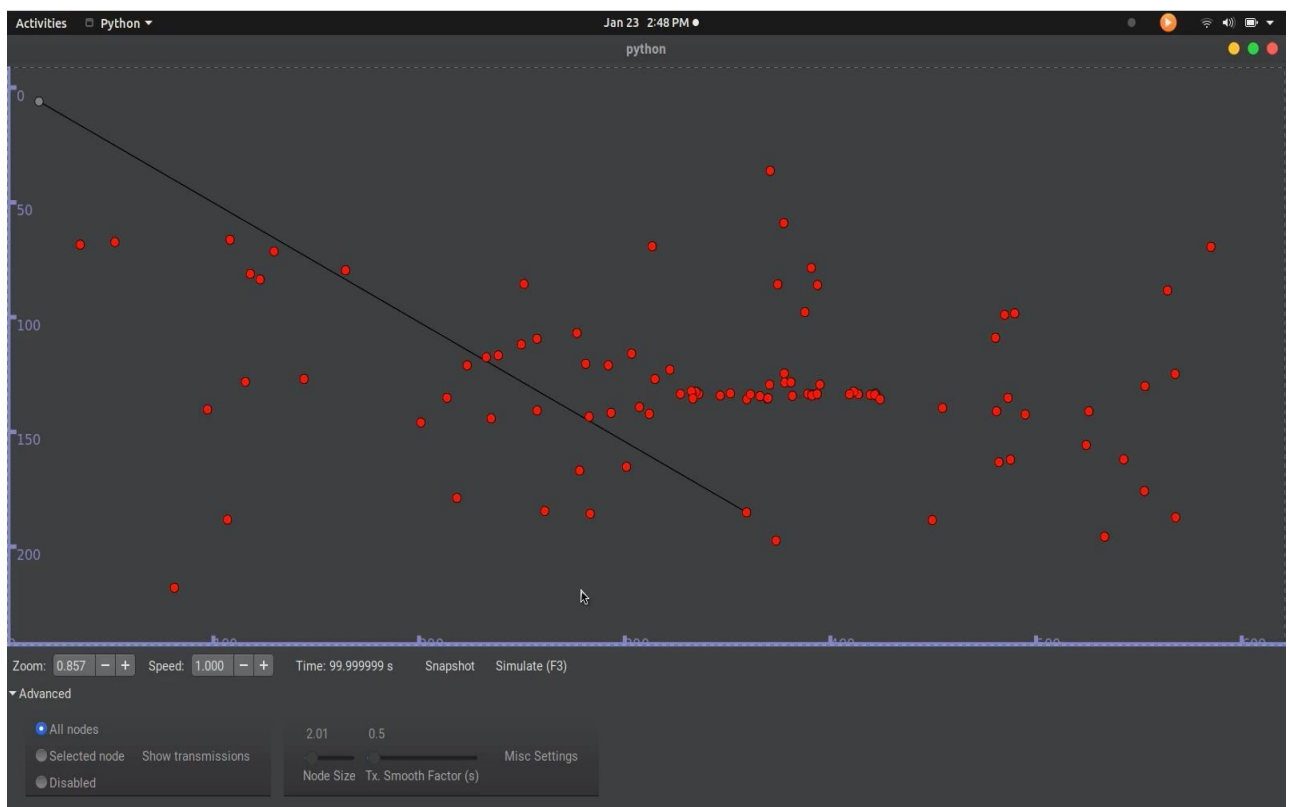


Figure B1: Sample of Python Visualiser of Network Simulation

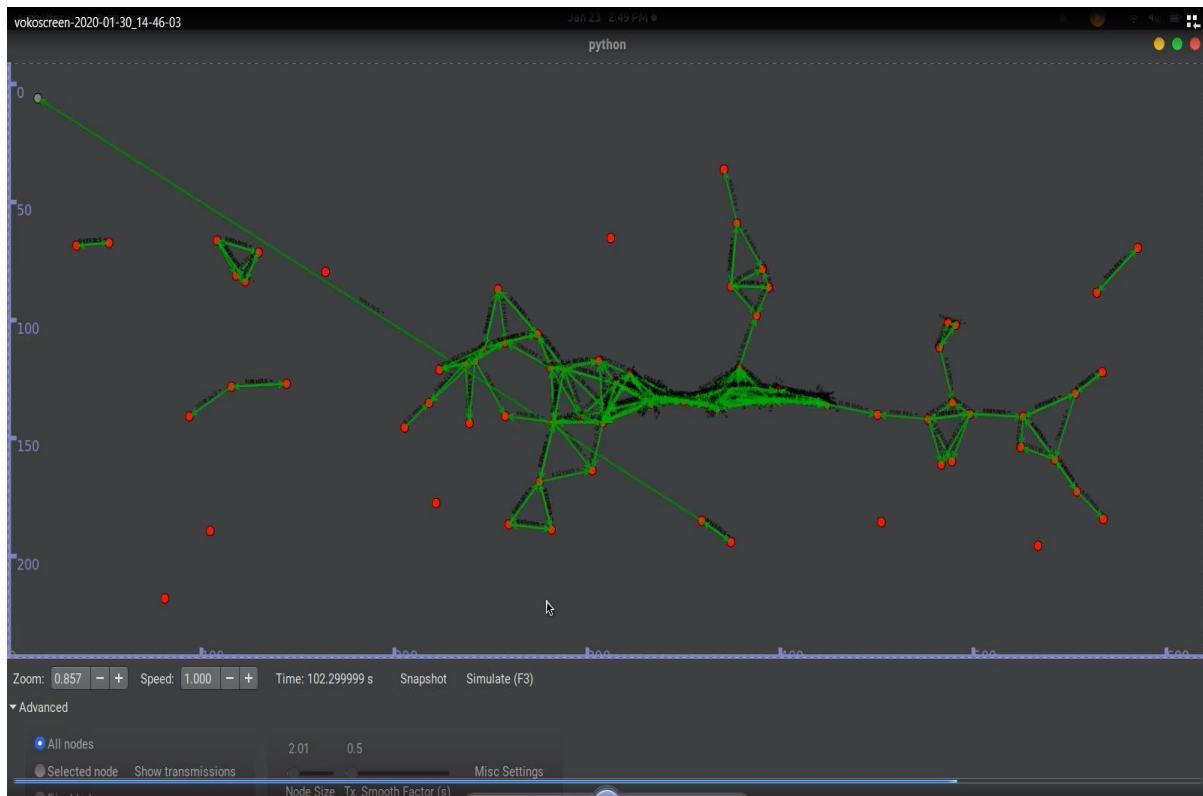


Figure B2: Sample of Python Visualiser During Network Formation Process

Definition of Default energy

```

#include <stdlib.h>
#include <time.h>

/// Tx Current
#define TX_CURRENTA          0.26

/// Rx Current
#define RX_CURRENTA          0.18

/// Idle Current
#define IDLE_CURRENTA        0.148

/// Sleep Current
#define SLEEP_CURRENTA       0.0094

```

Computation of Mobility Functions for 1m/s – 2m/s

```

sum =0
x = 1;% Minimum speed at nodes
y = 2;% Maximum speed at nodes
nodes = 200 % Number of nodes considered
V = (x-y).*rand(1,nodes)+a;% A vector representing speed at nodes
btw 1 and 4
k = 2
no_pairednodes = nchoosek(nodes,k)% This calculates the total number
of paired nodes
for i = 1:(length(V)-1)
    for j = i+1: length(V)
        sum = sum + abs(V(i)-V(j));
    end
end
(1/no_pairednodes)*sum

```

Computation of Mobility Functions for 5m/s – 12m/s

```

sum =0
x = 5;% Minimum speed at nodes
y = 12;% Maximum speed at nodes
nodes = 200 % Number of nodes considered
V = (x-y).*rand(1,nodes)+a;% A vector representing speed at nodes
btw 1 and 4
k = 2
no_pairednodes = nchoosek(nodes,k)% This calculates the total number
of paired nodes
for i = 1:(length(V)-1)
    for j = i+1: length(V)
        sum = sum + abs(V(i)-V(j));
    end
end
(1/no_pairednodes)*sum

```

Appendix B: Simulation Results for Network formation

Mean Values of Energy Consumption in Network Formation Scenario					
No. of Nodes	10	50		100	200
DS-OLSR	753.2	3841.5		6246.6	13445.3
OLSRv1	4783.8	24382.3		99711.9	

Mean Values of Routing Overhead in Network Formation Scenario					
No. of Nodes	10	50		100	200
DS-OLSR	1.8	8.5		22.1	41.8
OLSRv1	4.5	23.2		84.3	

Appendix C: Simulation Results for Disaster Scenario

Simulated Result for Energy Consumption

Mean Values of Energy Consumption in Static Scenario				
<i>No. of Nodes</i>	10	50	100	200
DS-OLSRMP	623.5	3083.5	5242.3	11575.8
DS-OLSR	802.5	4154.9	6671.3	14649.7
OLSRv1	5542.2	27092.3	1059460.2	
OLSRv2	5102.5	20166.5	757421.4	

Mean Values of Energy Consumption in Mobility Scenario (1m/s – 2m/s)				
<i>No. of Nodes</i>	10	50	100	200
DS-OLSRMP	748.5	3751.3	6201.5	13751.5
DS-OLSR	997.7	5185.5	8670.3	15659.4
OLSRv1	5243.8	30411.6	110359.2	
OLSRv2	4923.7	25675.6	85951.9	

Mean Values of Energy Consumption in Mobility Scenario (5m/s – 12m/s)				
<i>No. of Nodes</i>	10	50	100	200
DS-OLSRMP	1155.6	5560.3	7379.7	15855.5
DS-OLSR	1292.5	7428.8	10282.8	18311.4
OLSRv1	8351.5	41742.5	185785.9	
OLSRv2	7925.8	36331.3	123264.6	

Simulated Results for Routing Control Overhead

Mean Values of Control Overhead (%) for Network Formation Scenario				
No. of Nodes	10	50	100	200
DS-OLSRMP	1.2	4.8	11.1	25.5
DS-OLSR	1.5	5.2	14.1	29.8
OLSRv1	4.2	19.5	57.8	
OLSRv2	4.3	18.2	48.9	

Mean Values of Routing Control Overhead (%) for Mobility Scenario (1m/s - 2m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP	2.1	9.9	17.2	32.5
DS-OLSR	2.9	11.9	20.1	35.8
OLSRv1	7.3	26.8	75.9	
OLSRv2	6.5	24.7	73.2	

Mean Values of Routing Control Overhead (%) for Mobility Scenario (5m/s - 12m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP	4.3	19.6	34.8	58.9
DS-OLSR	5.4	25.2	40.7	72.1
OLSRv1	15.9	82.7	191.6	
OLSRv2	18.5	95.2	224.7	

Simulated Results for packet Delivery Ratio

Mean Values of Packet Delivery Ratio for Static Scenario				
No. of Nodes	10	50	100	200
DS-OLSR-MP	98.2	96.5	93.7	87.5
DS-OLSR	96.7	94.8	91.4	84.2
OLSRv1	88.4	87.1	76.6	
OLSRv2	87.8	88.5	81.9	

Mean Values of Packet Delivery Ratio for Mobility Scenario (1m/s – 2m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP	96.3	93.1	86.2	80.6
DS-OLSR	93.5	88.4	84.5	75.7
OLSRv1	86.2	84.4	74.7	
OLSRv2	87.4	85.8	74.6	

Mean Value of Packet Delivery Ratio in Mobility Scenario (5m/s - 12m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP	89.7	88.5	85.4	77.6
DS-OLSR	88.6	86.9	78.7	71.9
OLSRv1	75.7	72.3	68.5	
OLSRv2	76.3	67.6	63.2	

Simulated Results for End-to-End Delay

Mean Values of End-to-End Delay (ms) for Static Scenario				
No. of Nodes	10	50	100	200
DS-OLSRMP	4.354	19.424	42.233	104.972
DS-OLSR	4.573	18.642	43.641	105.221
OLSRv1	9.585	46.423	112.316	
OLSRv2	8.943	44.121	123.263	

Mean Values of End-to-end Delay for mobility Scenario (1m/s – 2m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP	5.563	23.473	51.113	121.261
DS-OLSR	5.467	26.431	52.726	124.754
OLSRv1	11.952	55.949	152.961	
OLSRv2	11.564	54.436	161.992	

Mean Values of End -to-end Delay for Mobility Scenario (5m/s - 12m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP	6.754	26.873	58.934	131.878
DS-OLSR	6.379	31.255	65.367	148.476
OLSRv1	34.784	176.489	244.962	
OLSRv2	33.967	161.278	276.378	

Appendix D: Calculated Results

Comparison of Simulated and Calculated Results of Energy Consumption

Simulated and Calculated Energy Consumption for Static Scenario				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	623.5	3083.5	5242.3	11575.8
DS-OLSRMP Calculated	619.9	3024.2	5135.3	11411.8

Simulated and Calculated Energy Consumption for Mobility Scenario (1m/s – 2m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	748.5	3751.3	6201.5	13751.5
DS-OLSRMP Calculated	739.4	3628.9	6162.4	13694.2

Simulated and Calculated Energy Consumption for Mobility Scenario (5m/s – 12m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	1155.6	5560.3	7379.7	15855.5
DS-OLSRMP Calculated	1143.7	5535.6	7263.8	15678.3

Comparison of Simulated and Calculated Results of Routing Control Overhead

Simulated and Calculated Control Overhead for Static Scenario				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	1.2	4.8	11.1	25.5
DS-OLSRMP Calculated	1.1	4.6	10.9	24.3

Simulated and Calculated Control Overhead for Mobility Scenario (1m/s – 2m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	2.1	9.9	17.2	32.5
DS-OLSRMP Calculated	1.9	8.9	15.6	31.8

Simulated and Calculated Control Overhead for Mobility Scenario (5m/s – 12m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	4.3	19.6	34.8	58.9
DS-OLSRMP Calculated	3.9	19.4	34.8	57.5

Comparison of Simulated and Calculated Results of Packet Delivery Ratio

Simulated and Calculated Packet Delivery for Static Scenario				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	98.2	96.5	93.7	87.5
DS-OLSRMP Calculated	98.4	97.2	93.6	86.5

Simulated and Calculated Packet Delivery for Mobility Scenario (1m/s – 2m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	96.3	93.1	86.2	80.6
DS-OLSRMP Calculated	96.6	92.3	86.5	80.7

Simulated and Calculated Packet Delivery for Mobility Scenario (5m/s – 12m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	89.7	88.5	85.4	77.6
DS-OLSRMP Calculated	89.4	87.8	85.9	77.8

Comparison of Simulated and Calculated Results of End-to-End Delay

Simulated and Calculated End-to-End Delay for Static Scenario				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	4.354	19.424	42.233	104.972
DS-OLSRMP Calculated	3.956	18.739	41.941	105.589

Simulated and Calculated End-to-End Delay for Mobility Scenario (1m/s – 2m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	5.563	23.473	51.113	121.261
DS-OLSRMP Calculated	4.875	22.522	49.821	120.237

Simulated and Calculated End-to-End Delay for Mobility Scenario (5m/s – 12m/s)				
No. of Nodes	10	50	100	200
DS-OLSRMP Simulated	6.754	26.873	58.934	131.878
DS-OLSRMP Calculated	5.975	26.732	58.942	130.975