A Framework for Traffic Flow Survivability in Wireless Networks Prone to Multiple Failures and Attacks

by

Owoade Ayoade Akeem

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

in the subject of

Computer Science

at the

School of Computing, College of Science, Engineering and Technology,

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Professor Isaac O. Osunmakinde

March 2022

DECLARATION

Owoade Ayoade Akeem

Student number: 50781529

PhD

A Framework for Traffic Flow Survivability in Wireless Networks Prone to Multiple Failures and Attacks

I declare that the thesis is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the thesis to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

Signature

24th August 2022

Date

DEDICATION

I dedicate my PhD to God Almighty for making this research possible. I also dedicate this work to my late sister: Princess Suliat Asabi Owoade and my late father: Prince Rasaq Oyebanji Owoade.

ACKNOWLEDGEMENT

From an academic standpoint, I would like to thank my supervisor, Professor I. O. Osunmakinde. You were amazing and greatly aided me in completing this study. You will always be remembered for being a part of one of the most memorable moments of my life. Thank you for your help and dedication to this research project. Thank you for all of your critical reading, unwavering support, oversight, and commitment to excellence. Thank you for never giving up on me.

I learned how to produce decent academic papers and give presentations at academic conferences thanks to his advice and instruction and I am astounded by his generosity and skills because the trust he inculcated in me as a student as he shared much more knowledge with me. Being a straightforward person, I always knew where I stood with all of his reviews, which made it much easier for me to concentrate. Professor I. O. Osunmakinde is also a candidate person who expects high standards from his trainees, and I am grateful for his dedication, assistance, accessibility, and mentorship. His intellectual competence for seeing the ultimate outcome from the beginning, as well as his classroom instruction and supervisory style, truly inspired me.

I also wish to acknowledge the administrative support from Estelle De Kock: thank you for all your help. It is not often that someone other than the supervisor, family, and friends is thanked for their help, but you have been there to help with any admin issues that arose during this programme.

In fact, finishing my doctorate at UNISA was a privilege because of the wealth of training and information available to university students pursuing post-graduate degrees. I recall attending UNISA-sponsored seminars and workshops that aided in the production of good dissertations and provided financial assistance to students. These are just a few of the resources made available by the school/department to assist me and my classmates in conducting investigations, and I am grateful for them.

Throughout this journey, my wife, Dr. Latifat Ronke Owoade, and our children, Ajibade, Martin, and Muhammed-Shefiq Owoade, have been my pillars of support. My other supporters, were my mother (Wosilat Anke Owoade) and my brother (Alhaji Biliaminu Owoade), your encouragement has helped me through this degree.

I appreciate my senior colleagues who have been supportive and encouraged me throughout the process of this research work: Professor A. A. Arigbabu, Professor Banjo and Professor Adeogun. I acknowledge my colleagues in the department for their support: Mrs Abimbola, Dr. Ogundile, Dr. Ogunbanwo and Dr. Ogunsanwo, you people are good friends. I cannot forget my friend in the department of Physics, Mr Kolawole Egunjobi.

ABSTRACT

Transmitting packets over a wireless network has always been challenging due to failures that have always occurred as a result of many types of wireless connectivity issues. These failures have caused significant outages, and the delayed discovery and diagnostic testing of these failures have exacerbated their impact on servicing, economic damage, and social elements such as technological trust. There has been research on wireless network failures, but little on multiple failures such as node-node, node-link, and link–link failures. The problem of capacity efficiency and fast recovery from multiple failures has also not received attention.

This research develops a capacity efficient evolutionary swarm survivability framework, which encompasses enhanced genetic algorithm (EGA) and ant colony system (ACS) survivability models to swiftly resolve node-node, node-link, and link-link failures for improved service quality. The capacity efficient models were tested on such failures at different locations on both small and large wireless networks. The proposed models were able to generate optimal alternative paths, the bandwidth required for fast rerouting, minimized transmission delay, and ensured the rerouting path fitness and good transmission time for rerouting voice, video and multimedia messages. Increasing multiple link failures reveal that as failure increases, the bandwidth used for rerouting and transmission time also increases. This implies that, failure increases bandwidth usage which leads to transmission delay, which in turn slows down message rerouting.

The suggested framework performs better than the popular Dijkstra algorithm, proactive, adaptive and reactive models, in terms of throughput, packet delivery ratio (PDR), speed of transmission, transmission delay and running time. According to the simulation results, the capacity efficient ACS has a PDR of 0.89, the Dijkstra model has a PDR of 0.86, the reactive model has a PDR of 0.83, the proactive model has a PDR of 0.83, and the adaptive model has a PDR of 0.81. Another performance evaluation was performed to compare the proposed model's running time to that of other evaluated routing models. The capacity efficient ACS model has a running time of 169.89ms on average, while the adaptive model has a running time of 1837ms and Dijkstra has a running time of 280.62ms. With these results, capacity efficient ACS outperforms other evaluated routing algorithms in terms of PDR and running time. According to the mean throughput determined to evaluate the performance of the following routing algorithms: capacity efficient EGA has a mean throughput of 621.6, Dijkstra has a mean throughput of 619.3, proactive (DSDV) has a mean throughput of 555.9,

and reactive (AODV) has a mean throughput of 501.0. Since Dijkstra is more similar to proposed models in terms of performance, capacity efficient EGA was compared to Dijkstra as follows: Dijkstra has a running time of 3.8908ms and EGA has a running time of 3.6968ms. In terms of running time and mean throughput, the capacity efficient EGA also outperforms the other evaluated routing algorithms.

The generated alternative paths from these investigations demonstrate that the proposed framework works well in preventing the problem of data loss in transit and ameliorating congestion issue resulting from multiple failures and server overload which manifests when the process hangs. The optimal solution paths will in turn improve business activities through quality data communications for wireless service providers.

Keywords: Wireless Network; Multiple failures; Rerouting; Resilience; Enhanced Genetic Algorithm (EGA); Ant Colony System (ACS); Traffic Flows; Attack; Optimal Path; Restoration.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OABBREVIATIONS AND ACRONYMS

ACO	Ant Colony Optimization (Algorithm)
ABC	Artificial Honey Bee
ACS	Ant Colony System (paradigm)
ADPV	Adaptive Disjoint Path Vector
AI	Artificial Intelligence
AODV	Ad-hoc On-Demand Distance Vector
ARA	ACO based Routing Algorithm
AR-TORA-FCS	Adaptive Repair Temporally Ordered Routing Algorithm Flood Control Strategy
ATM	Asynchronous Transfer Mode
AUC	Authentication Centre
AWN	Ad-hoc Wireless Networks
BANT	Backward Ant
B-AODV	Backward AODV
BER	Bit Error Rate
BPSA	Backup Path Set Selection Algorithm
BSC	Base Station Controller
BTS	Base Transceiver Station
CH	Cluster Head
CSFR	Collaborative Single Node Failure Restoration (algorithm)
CTRNN	Continuous Time Recurrent Neural Network
DAG	Directed Acyclic Graph
DSDV	Destination Sequenced Distance Vector (protocol)
DSR	Dynamic Source Routing
DV	Distance Vector
EA	Evolutionary Algorithm

ECM	Evolutionary Computing Model
EGA	Enhanced Genetic Algorithm
EIR	Equipment Identity Register
EMPSO	Energy-aware Multipath Routing Strategy Based on Particle Swarm Optimization
FANT	Forward Ant
FF	Fireflies
GA	Genetic Algorithm
G-AODV	Grade-AODV
GHz	Giga Hertz
GSR	Global State Routing (protocol)
HLR	Home Location Register
HNN	Hopfield Neural Network
HSR	Hierarchical State Routing (protocol)
IoT	Internet of Things
IP	Internet Protocol
ISDN	Integrated Service Digital Network
L2L	Link to Link
LET	Link Expiration Time
LP	Linear Programming
LS	Link State
MANET	Mobile Ad-hoc Networks
Mbps	Megabits per second
MSC	Mobile Switching Centre
N2N	Nose to Node
N2L	Node to Link
OLSR	Optimised Link State Routing

PDR	Packet Delivery Ratio
PSO	Particle Swarm Optimisation
QoS	Quality of Service
RERR	Route Error
RF	Radio Frequency
RNN	Recurrent Neural Network
RREQ	Route Request Packets
RSA	Routing and Spectrum Assignment (algorithm)
RT-TORA	Real Time Temporally Ordered Routing Algorithm
SCA	Spare Capacity Allocation
SI	Swarm Intelligence
STAR	Source Tree Adaptive Routing Protocol
TORA	Temporally Ordered Routing Algorithm
TSP	Travelling Salesman Problem
VLR	Visitor Location Register
WRP	Wireless Routing Protocol
WSN	Wireless Sensor Network

CHAPTER 1: INTRODUCTION

1.1 THEORETICAL BACKGROUND AND MOTIVATION

The world is becoming more reliant on wireless services, yet wireless connectivity's capacity to control this demand is under question. Failures have an impact on not only the current voice but also the future voice, video, multimedia, and data use, and it may also stifle new wireless applications like high-speed internet access and e-business. As wireless and mobile technology become more important in emergency situations, network outages become life-or-death situations. For wireless networks to be survivable in the event of failures, network survivability comes into play. The resilience of a network to perform its intended set of activities in the face of network equipment failure that result in a system shutdown, as measured by the variety of infrastructures affected, the quantity of users affected, and the extent of the equipment failure.

Much of the research on network resilience concentrates on link failure safety, assuming that nodes in the network are reliable. To deal with equipment failures within a node, a transmission node, for example, uses one-plus-one safety of its switching and monitoring system, or a node has a spare node. However, because both one-plus-one nodes are usually in the same place, they are prone to catastrophic failure [1]. When a disaster strikes, such as an earthquake, all system components in the surrounding area are impacted or annihilated. The most prevalent types of failure in a wireless network are multilink and single link failures. As a result, when dealing with failures, the safety of these two types of failures should not be overlooked. The following four types of failures are some of the most common in wireless networks:

- Link failures: This happens whenever a network's link device fails [2]. This problem can be solved by introducing a new link or rerouting and redistributing traffic from a broken link to other still working links with enough capacity to carry the extra traffic from the failed link.
- Node failures: This happens when a device at the network's node fails, such as a hub or switch [3]. It can also be considered as the simultaneous failure of all of a node's neighboring links. One method of defending in case of node failure is to deploy at least one backup appliance capable of quickly replacing a functioning item that is acting as a node.

- Single failures: In a network, this happens whenever one device or link fails at the same moment [4]. Network restoration models are meant to protect solitary or single network elements from single failures, premised on the belief that such multiple failures, though rare, are not entirely impossible occurrence(s).
- Multiple failures: When numerous pieces of equipment, nodes, or links fail at the same time, simultaneous network failures can occur [5]. Network restoration models are meant to safeguard two or more network components from multiple failures, with the assumption that, while rare, multiple, relatively close failures are not unheard of. While the bulk of the failures were single failures, one study [6] discovered that around 30% of unplanned failures (which account for 80% of all failures) contain multiple linkages, which is a substantial finding that requires attention. Furthermore, several failures might cause a large amount of service disruption. As a result, it is critical to devise strategies that safeguard the network from not only single but multiple failures[7].

Many past network failures and associated systems have occurred due to disasters that have caused major problems. In addition, the slowness with which they were discovered and diagnosed has increased their influence in terms of active service, economic loss, and human variables like technological confidence [8]. Failures of wireless networks pose a serious hazard to corporations and government operations. For example, owing to *Hurricane Irma*, the following generalisations show the percentage of cell towers out of operation in Florida, the US Virgin Islands (USVI), Texas, and Puerto Rico. However, the hurricane season's yearly occurrence has generated major resilience and recovery planning by telecom operators in the United States, and as a result, public-sector-led warning, preparation, relief, and recovery operations have achieved enhanced resilience and speedier recovery. Operators must be ready and have all of the requisite reserves on hand to quickly re-establish service. These years of interconnections have resulted in quick recovery timeframes in hurricane-affected areas of the United States mainland as a result of innovations like Cells-on-Wheels, portable energy reserve, and dispersed fuel technologies which have become commonplace in the US telecom business. The US Virgin Islands, on the other hand, was hit hard by both *Hurricanes Irma* and *Maria* in a short period of time, which resulted in a near-complete destruction of telecom device. In the aftermath of *Hurricane Maria*, the same was true for Puerto Rico, and both regions went through blackouts for longer durations. Compared to Florida which within a week of the disaster had, 97% of cell towers back online, after the

massive storm had knocked down 27% of them [9]. Figure 1.1 depicts the percentage of cell towers out of operation each day in Florida (along with the date the site went out of operation).

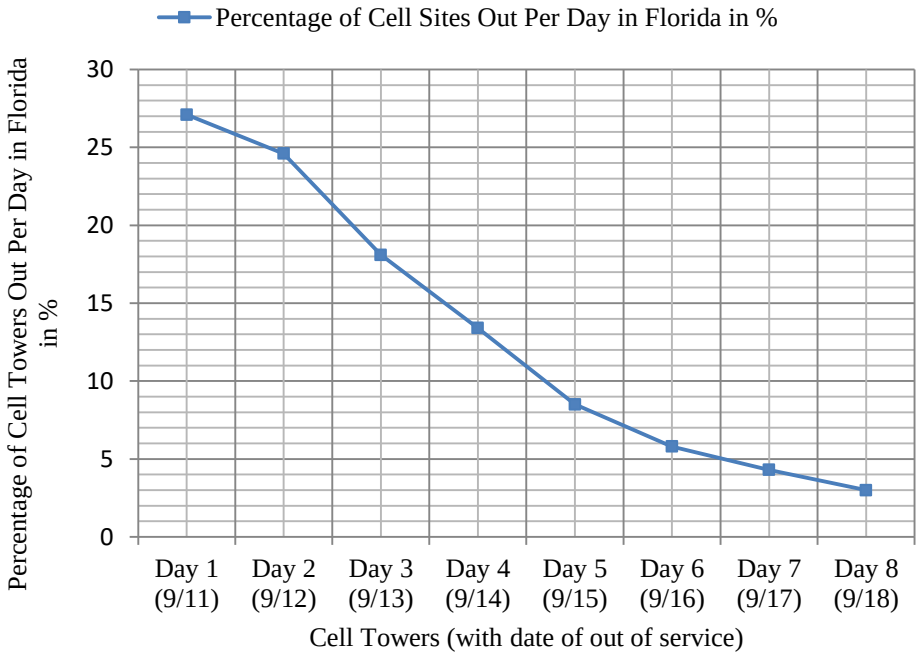

Figure 1.1: Percentage of cell sites out per day in Florida: (adapted from [9])

Figure 1.2, however, depicts the percentage of cell towers out of operation each day in Puerto Rico and the US Virgin Islands following *Hurricane Irma*. The data illustrates that while the number of cell stations out of operation each day in Puerto Rico has steadily improved, the percentage of cell towers out in the US Virgin Islands has continued to rise at approximately 50%.

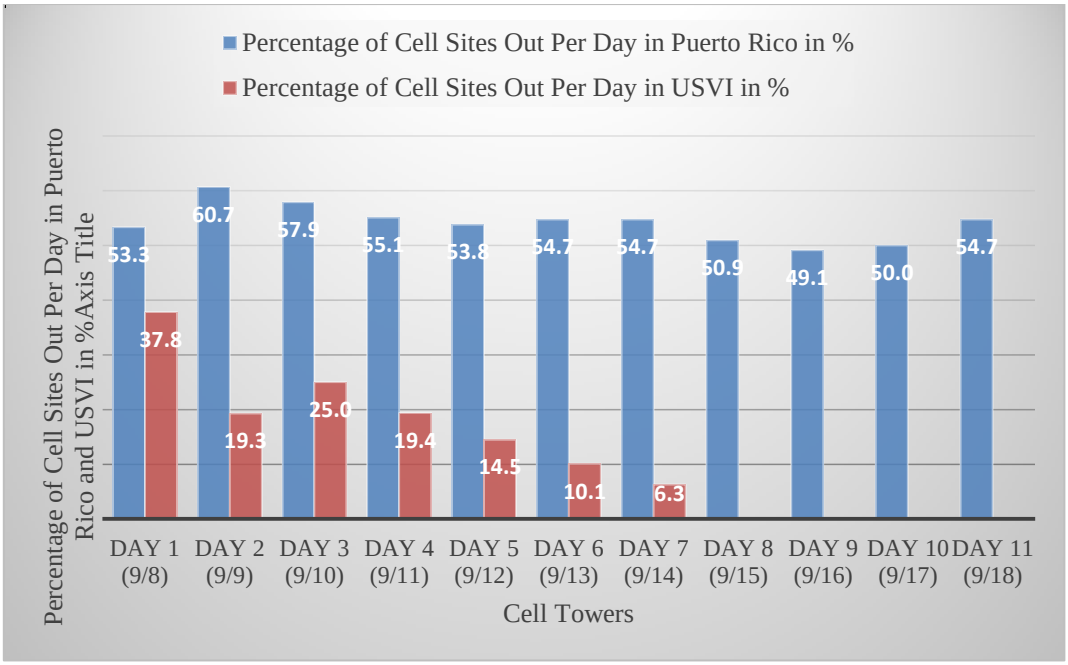

Figure 1.2: Percentage of cell towers out per day in Puerto Rico and USVI: (adapted from [9]).

Figure 1.3 illustrates that *Hurricane Harvey* had little effects on the network, as only 1.7% of cell towers were still damaged on the eleventh day. However, some localities within a declared disaster zone were severely hit. Several Texas counties, for instance, all experienced cell failures of more than 50%.

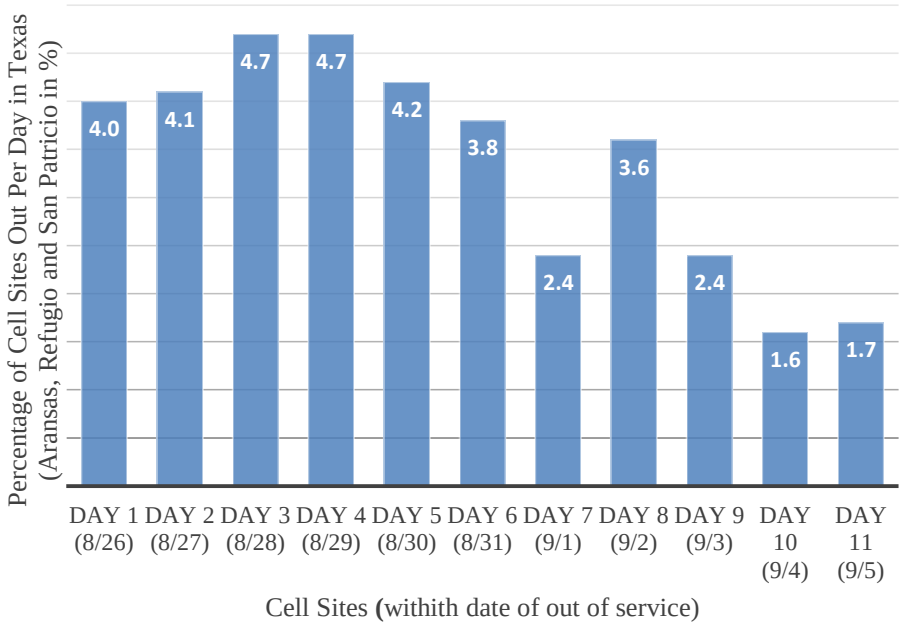

Figure 1.3: Percentage of cell towers out per day in Texas counties (adapted from [9], 2018).

1.2 PROBLEM STATEMENT

Network failures could not be accommodated especially during this Covid-19 pandemic where communications were required to go fast [10] [11]! Despite the prior research on network survival, the current approaches are challenged owing to the four-fold degree of resilience required in network survival, technological advancement in networking, natural disasters in unprecedented times and the proliferation of network attackers.

Figure 1.4 depicts the consequences of failures in wireless cellular network intercommunication. It should be noted that any of the following failures can cause network failure:

- Mobile switching centre (MSC) failure;
- Base station controller/base station (BSC/BS) failure;
- Link failure; and
- Home location register/visitor location register (HLR/VLR) failure.

When such a failure occurs in network X, customers from network Y are unable to use network X's roaming services. Similarly, network Z using network X's group membership facility becomes unavailable, when network X fails owing to various failure scenarios.

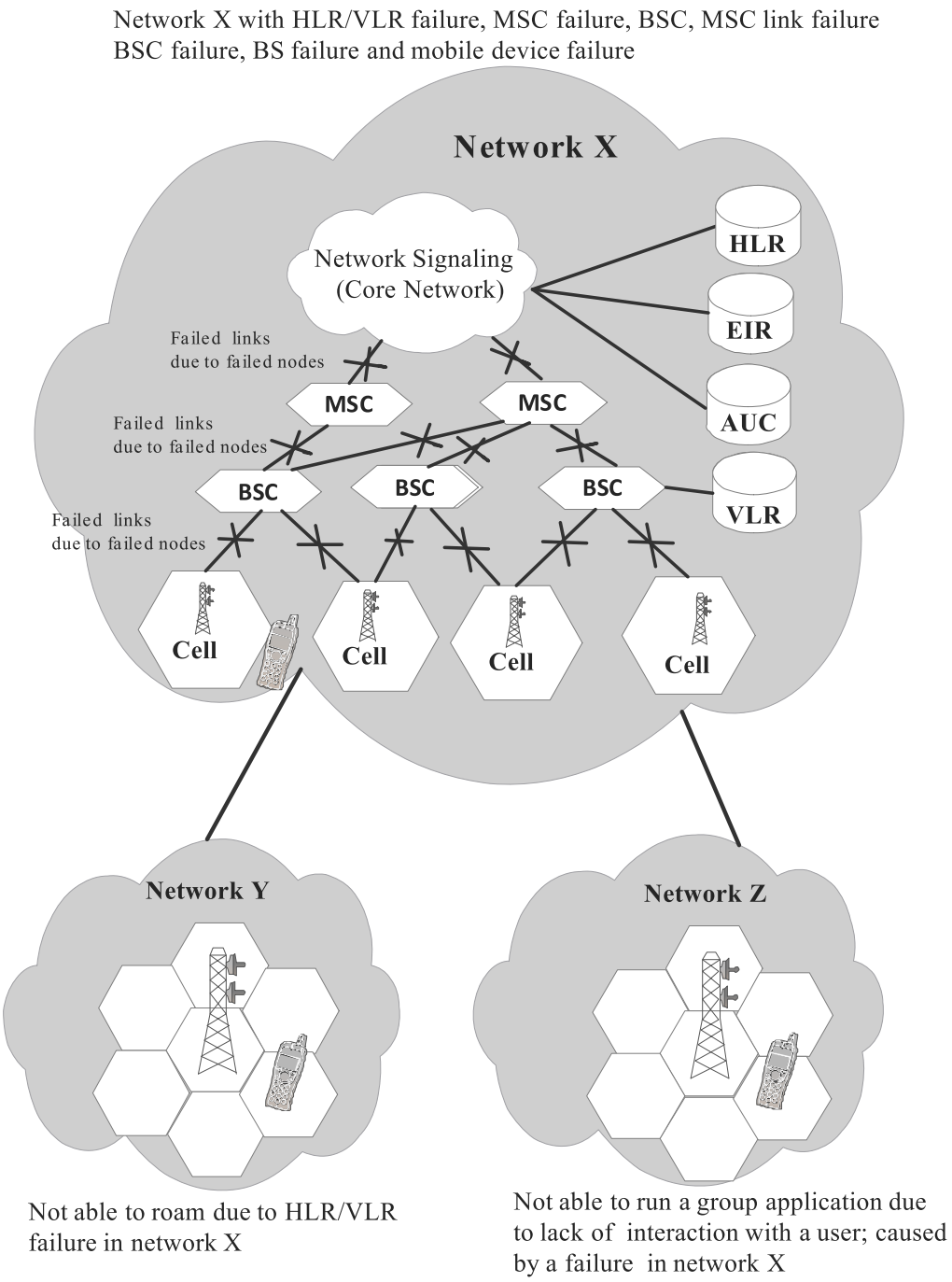

Figure 1.4: The consequences of failures in wireless cellular network (adapted from [12])

Among different mechanisms for solving the network failures, an investigation has revealed that not enough work has been done extensively on node-node, link-link and node-link failures. In the literature, various failed restoration approaches have been presented, each with its own set of network models. The problems or /gaps have been identified as the rationale for motivation or /improvement of existing survival techniques:

1.2.1 In the traffic flow of wireless networks, there are node-node, node-link, and link-link failures that need to be addressed.

The self-organizing nature of wireless networks necessitates communication between nodes. Each network node operates as a router and terminal, transferring packets to next available nodes. Owing to the network's design and self-organising nature of some wireless networks for example wireless ad-hoc networks (wireless sensor networks) and the node's evolving behaviour, link and node failures are common, and maintaining connectivity is a challenge due to interference, mobility, radio channel effect, and battery constraints [13].

Wireless networks are not resistant to severe conditions and are susceptible to failure for a variety of reasons. Failure of nodes causes the network to be partitioned into small portions, limiting node connectivity, and causing a delay in wireless network traffic flow. Since restorative techniques are so important, several ways have been offered in the literature so far. These techniques, on the other hand, do not place emphasis on a homogenous distribution of nodes prior to failure [14]. To address the gap in the literature, a recovery algorithm is required to focus on preparing nodes ahead of failure by restoring node and link connections when rerouting is required to retransmit traffic flow in a wireless network.

Existing wireless network restoration models focus on single failures and do not clearly indicate what kind of multiple failures they would address, for example node-node, node-link, and link-link failures in wireless network traffic flow. As a result, there is a gap where robust model can fix such issues.

1.2.2 Additional capacity for wireless network failures must be used to maintain a steady network.

When resources are not evenly allocated it causes many challenges in the routing and rerouting of traffic. This has particularly contributed to failure problem in node-node, node-link and link-link [15] which are responsible for scheduling alternative paths and to provide spare network capacity that ensure communications services are available at all times in a variety of occurrences. The spare capacity allocation (SCA) problem is a complex multi-constraint optimisation problem.

The majority of transmission failures are ascribed to a lack of spare capacity allocation, as low SCA causes node/link failures and makes message rerouting difficult when single node,

single link, multiple nodes, and multiple links failures occur[16]. Since most work does not integrate failure restoration by addressing spare capacity allocation, SCA has always been a difficulty in resolving wireless network failures. This creates a gap, which this research was able to fill by generating alternative routes in real time using heuristics that compute the bandwidth needed to reroute packets.

The Asynchronous Transfer Mode (ATM) was a packet-based protocol that used high-speed switching of small fixed-size packets (the ATM cell) to allow for both Quality of Service control and switching while minimising queuing and congestion. The goal of ATM is to provide faster switching and line rates. ATM networks can be either wired or wireless. WATM stands for wireless ATM network [17]. This research part concentrated on wireless ATM networks. Spare capacity is used to generate an alternative path with the required bandwidth to reroute messages in the event of failures or attacks.

1.2.3 Challenges of attacked wireless networks that, cascade to link failures of video transmission.

Since wireless networks are vulnerable to a range of connection assaults, increased attacks on wireless networks have caused cascaded link failures which result in failure in transmitting video message [18], and typical network security approaches are ineffective on them. Multiple failures in any wireless network are typically caused by localised attacks, target attacks, and random failures [19]. A complete security solution must be constructed for these networks to resolve wireless network restrictions, untrustworthy transmissions, and deployment in open areas, unprotected nature, and scarce resources. Such a solution would enhance subscriber confidence in wireless networks [20].

1.2.4 The challenge for rerouting of multimedia messages for node-link failure in IoT networks.

Multimedia-oriented internet of things (IoT) offers smooth and real-time video, audio, and image data transmission between devices in the real world. In the IoT environment, there are many challenges to overcome, these include:

- limited IoT devices;
- intermittent IoT network connections;
- heterogeneous device dynamism and expandability in video encoding;

- bandwidth insufficiency in video transfer; and
- achieving application exact quality of service in video transmission [21].

All these issues typically result in node-link failures in IoT networks, and they require immediate attention using robust optimisation techniques.

What has gained more attention is the need for diverse multimedia applications based on the IoT that has expanded as the IoT network. In this regard, multimedia systems have been made possible thanks to the advancements in various IoT network devices. However, the number of challenges that have hampered the performance of IoT networks in transmitting multimedia messages have also increased exponentially. For example, low-powered devices and a lack of required bandwidth have contributed to node and link failures in IoT networks, affecting multimedia message transmission. For instance, a small increase in packet loss can have a major impact on video download time, which increases the chance of playback interruption [22]. Although, users can use devices with different capacities (such as smart phones, smart watches, and notepads), new protocols must be designed to work in resource-constrained devices due to power, memory, and computational limits. Wireless network protocols must also be developed to create a set of energy-saving measures to optimise the performance of low-power IoT devices.

Various multimedia materials; namely, real-time audio and video, are expected to make up a considerable portion of the data sent on wireless network. Finding a solution for slightly elevated video communication in limited delay settings while working with devices that have limited hardware resources, such as nodes connected by links, is difficult and prone to failure. Video programming, unlike the distributed communication platform, is the most significant barrier to video transmission for restricted internet of things devices, and therefore video programming accounts for 90% of overall latency [23]. Ultimately, therefore, to have seamless transmission of video messages, an optimisation technique is required to tackle the problem.

In order for IoT to provide excellent services, the problem that needs to be rectified for quick rerouting of multimedia messages is the bottleneck created by the failure of a node-link in an IoT network.

1.2.5 Lack of guidelines for future researchers on wireless network survival analysis.

A three-fold research is required to better understand the following aspects:

- how a resilient wireless network is built and maintained to withstand attacks and multiple failures;
- what role optimisation techniques play in this system; and
- how they can be used more effectively to assist telecoms companies in designing and maintaining resilient wireless networks? [24].

Practitioners and academic researchers working on wireless network survivability have tried a variety of intervention techniques to improve wireless network survivability. To resolve issues, one solution uses optimisation techniques, which are particularly useful for wireless network subscribers. However, the scholarly literature reveals a trend of contradictory conclusions when it comes to the effects of wireless network survival. Some earlier researches, for example, have found significant and favourable effects of optimisation strategies, whereas others have not. As a result, more investigation is required [25].

Since there has been little research on wireless network survivability; it is difficult to design all possibilities for improved study or a blueprint for wireless network methods of research that academics and practitioners can mutually use. As a result, the failure to develop a blueprint exacerbates the negative consequences of unresolved issues.

1.3 RESEARCH OBJECTIVES

This study's main purpose is to address the difficulties outlined:

To establish a framework for traffic flow survivability in wireless networks prone to multiple failures and attacks.

The following five sub-objectives help to support this:

1. To design a swarm intelligence system that resolves multiple failures in wireless ATM networks in order to survive node-node failures. This sub-objective is linked to wireless ATM networks because the first experiment to test the effectiveness of the capacity efficient ACS model was performed on a wireless ATM network. The ATM is the primary standard technology for broadband communications in wireless infrastructure. However, the advancement of wireless networks that support user mobility, as well as the high demand for multimedia and, in particular, internet-based applications, has prompted new research into the integration of ATM with wireless, namely the wireless ATM

(WATM). ATM has the benefits of high efficiency and QoS support for users, and when combined with wireless networks, it can provide mobility-supported high frequency multimedia services. WATM can be thought of as an extension of a wired backbone network with wireless access flexibility and mobility support. The WATM standardisation process has begun within the ATM Forum and ETSI (European Telecommunication Standards Institute), with assistance from other standardisation organisations such as the IETF (internet Engineering Task Force). The traditional wired network serves as the backbone of the WATM network. As a result, we regard a WATM network as a modified version of a wired ATM network that includes new wireless links and equipment.

2. To design a swarm intelligence resilience system based on resource effectiveness and rapid recovery in order to manage node-node failure problems swiftly and improve wireless network service quality.
3. To investigate the resilience of an evolutionary computing paradigm focused on resource effectiveness and on-demand recovery in IoT networks to quickly handle node-link failures.
4. To develop an enhanced genetic algorithm (EGA) that focuses on capacity efficiency and fast restoration in order to quickly handle link-link failures on a wireless network.
5. To devise methods for generating a complete blueprint for wireless networks failure survivability research designs that academics and practitioners can use in the future. This is meant to make it easier to spot additional key wireless network survival issues that are not covered in this study but still need to be looked at.

1.4 QUESTIONS FOR RESEARCH

To achieve the required results, the following research questions are posed:

How can a swarm intelligence and evolutionary computing-based system model be designed to withstand traffic flows in wireless networks prone to breakdowns and attacks?

Secondary research questions:

1. How can a swarm intelligence system designed to resolve multiple failures in WATM networks survive node-node failures?

2. How can a swarm intelligence survivability model that is centered on resource effectiveness and quick recovery be built to quickly solve node-node, node-link and link-link failure issues and improve wireless network quality of service (QoS)?

3. How can an evolutionary computing paradigm focused on capacity efficient and on-demand recovery help IoT networks quickly recover from node-link failures?

4. How can a capacity-efficient and fast-restoration enhanced genetic algorithm (EGA) be built to quickly repair cascaded links (link-link) failures on a complex node network?

5. How can a detailed blueprint for wireless network survivability research be conducted and built to provide insights for both future academics and practitioners to protect wireless network subscribers?

1.5 CONTRIBUTIONS TO RESEARCH

1.5.1 Contributions to the body of scientific knowledge

The following are key contributions to the body of knowledge on wireless network survivability made by this study:

- Design of a new suggested capacity efficient EGA and ACS model based on quick restoration, which could help wireless network users survive multiple network failures including node-node, link-link, and node-link failures.
- Extensive studies were conducted to determine appropriate paths with the requisite bandwidth for rerouting packets on networks that ranged from zero failure to numerous failure scenarios.
- Data from simulation trials are used to undertake investigational assessments of the suggested model. These tests indicated that the ACS model is reliable for rerouting voice messages, whereas the EGA model is reliable for sending video and multimedia communications.
- The open research structure on wireless network survivability owing to failures is this researcher's view on the wireless network survivability literature that reveals network survivability topics. These have gotten little attention in research, resulting in research issues to establish a blueprint for wireless network failure survivability study concerns. The goal of this study was to look at different optimisation routing algorithms in wireless networks in order to identify gaps that future wireless researchers might use as a starting point for their research.

- This research serves as a prototype for Africa's telecommunication service providers, particularly as a response to making wireless networks fault-tolerant during this pandemic period when emergency transmissions are required. The proposed capacity efficient EGA and ACS model is intended to be used in the resolution of wireless network failures caused by attacks.

1.5.2 Declaration of publications as a result of this research

The following publications were developed, submitted, and accepted by several reputable conference proceedings and journals as part of this research project:

Accredited journals/ book chapters

1. A. A. Owoade and I. O. Osumakinde (2021) Resilient Rerouting in IoT Systems with Evolutionary Computing. In: Artificial Intelligence in Intelligent Systems. **Lecture Notes in Networks and Systems**, CSOC 2021, (LNNS), Volume 229, pp 194–211, ISSN 2367-3370; ISBN: 978-3-030-77445-5, Springer Nature Publishing (Scopus indexed).

2. A. A. Owoade and I. O. Osunmakinde (2019) "Surviving node-node failures within wireless networks for a near optimal ant colony system message re-routing" *Int. J. Mobile Network Design and Innovation, (IJMNDI), Inderscience Publisher. Vol. 9, Nos. 3-4, 2019, (*Elsevier Scopus indexed) **ISSN online**:153-181

3. A. A. Owoade and I. O. Osunmakinde, "Analyzing Research Trends on Survivability of Wireless Networks Prone to Failures" submitted to International Journal of Wireless Information Networks, Springer Publishers, (Scopus indexed).

Accredited conferences

1. A. A. Owoade and I. O. Osunmakinde: "Fault-tolerance to Cascaded Link Failures of Video Traffic on Attacked Wireless Networks" *IST-Africa 2021 Conference Proceedings*, South Africa, pp. 1 – 11, ISBN: 978-1-905824-67-0, IEEEXplore.

2. A. A. Owoade and I. O. Osunmakinde: Resilience and Survivability ATM Node-Node network failures using ant colony swarm intelligent modeling. *Proceeding of SAI conference, London, United Kingdom*, 2016, pp. 165-172, IEEE ISBN 978-1-4673-8460-5/16, IEEEXplore.

1.6 ETHICAL CONSIDERATIONS IN RESEARCH

In research, ethical considerations are a set of principles that guide your research designs and practices. When collecting data from people, scientists and researchers must always follow a set of rules. Understanding real-life phenomena, studying effective treatments, investigating behaviors, and improving people's lives are all common goals of human research. What you choose to research and how you conduct that research are both important ethical considerations.

These factors were considered during the course of this research work:

- Safeguarding the rights of research participants
- Improve research validity
- Keep scientific integrity

Ethical issues were observed as part of this study, as mandated. The UNISA granted ethical clearance for this work under the reference number 2021/CSET/SOC/036.

This researcher confirms that this is his original work, that all sources used or quoted in it were properly referenced and cited, and that no data or results were falsified.

This dissertation was not forged or plagiarised in any way, and Turnitin software was used to detect any plagiarism. Citations and referencing were done with Mendeley referencing software.

1.7 SCOPE AND CONTEXT OF THE STUDY

1.7.1 Research scope

The scope of this study includes the following network failures:

- Node to Node (N2N) - The failure is caused by a failure of equipment at a network node, for example, switches or routers. A node failure can also be described as the simultaneous failure of all of a node's neighbouring links. One method of defending node failure is to install one or more piece of redundant equipment that can quickly replace active equipment acting as a node.

- Link to Link (L2L) - Link failure occurs when a link element in a network fails. A link failure problem can be solved by adding a new link or redirecting and

redistributing traffic from a broken link to other functioning links with enough capacity to carry the increased load from the failed link[2].

- Node to Link (N2L) - Multiple network failures can occur when several pieces of equipment, nodes, or links fail at the same time [2]. Network restoration models are designed to safeguard networks from multiple failures by providing protection for two or more network parts, with the concept that, while unusual, multiple, near-simultaneous failures are not unheard of.

1.7.2 Research limitations

This research was limited to wireless networks having N2N, L2L, and N2L failures, with investigations conducted on various network sizes and topologies. The suggested model's resilience was evaluated on such failures in various places on wireless networks, with the models being implemented in Java.

The study also has the following limitations:

- A full-scale project necessitates more manpower and takes more time to complete.
- More funding is required for the project to expand beyond the scope of the study.
- Obtaining recent publications has been costly because all of the papers required to conduct the research are not readily available for free.

1.8 SYNOPSIS OF RESEARCH

Table 1.1 presents the layout of the dissertation.

Table 1.1: Synopsis of research

CHAPTER	TITLE	DESCRIPTION
Chapter 2	Review of the literature and theoretical background	As part of this study, literature has been read to explain various network survivability tactics, problems, and performances, as well as to explore various survivability models. This section contains an introduction and a brief overview of the restoration procedures employed in this investigation. This chapter also identifies gaps in the existing literature.
Chapter 3	Open research structure on survivability of wireless network due to failures	This chapter provides a survey of wireless network optimisation routing topics to uncover previously unexplored and understudied areas such as swarm-based, evolutionary algorithm, adaptive, and reactive optimisation routing.

Chapter 4	Methodology and research design	The chapter covers the study's methodology and design in detail.
Chapter 5	Investigations on several survivability models, such as the EGA and ACS frameworks. Comparative evaluation of various survivability models also discussed.	The following investigations were performed, the N2N, L2L, and N2L both in small and large networks using the EGA and ACS models are discussed in detail in this chapter. The performance evaluation criteria for various survivability models were discussed in detail in this chapter. It also presents various survivability strategy evaluation measures in order to indicate areas where future research should be focused. To demonstrate the virtues and shortcomings of each survivability model, a comparison of multiple survivability models, including EGA and ACS, is performed.
Chapter 6	Conclusion and future directions	This chapter concludes the study by identifying its limitations and discussing how the research questions were addressed. The contributions of the study in terms of theoretical and methodological elements are discussed. There are suggestions for future work.

1.9 CHAPTER SUMMARY

In telecom businesses where it has been used, wireless network survivability has made a significant contribution to service quality. However, there are some requirements that must be followed for adoption to be simple. Adoption is heavily influenced by system specification. This chapter focused on wireless network survivability, showing some of the real-world issues faced by wireless network failures caused by hurricanes in some industrialised countries, as depicted in Figures 1.1, 1.2, and 1.3, and how this impacts the telecommunications industry. The research objectives are specified to focus on the topics to be covered and the goals to be achieved.

The research questions that are relevant to the research objectives are also developed. The focus of the study is explicitly stated in the contexts of how the research questions are posed and this is addressed at the end. The study's shortcomings are addressed to shed more light on the areas that were left out. This chapter also includes a chapter plan for the rest of the research.

CHAPTER 2: THEORETICAL AND LITERATURE BACKGROUND

2.1 PRELIMINARIES/INTRODUCTION

The literature reviewed in relation to the study subject is discussed in this section. Internet sites and other information sources were also used as extra sources of information in some circumstances. Other sources of information were explored to determine the arguments for and against wireless network survivability models, as well as related concepts and words; namely, journal articles, periodicals, wireless network websites, and books. The literature discussed many forms of wireless network survival models, as well as the limitations that these models face.

2.2 WIRELESS AND /DIGITAL NETWORK SURVIVABILITY STRATEGIES

Network survivability is the study of a physical network topology's availability, dependability, and reliability. It has been considered when it comes to military leadership, control, and cellular technologies since the 1970s [24]. In the past few years, after the increased need for distributed networks such as wireless networks, there has been a sharp increase in involvement in network survival. Network survivability is an important feature of dependable communication in wireless networks, as it allows systems to keep network connectivity in the face of attacks, malfunctions, or natural disasters in an effective and timely way.

Survivability is a crucial network property that ensures a given level of data transmission. The process for transferring data or the protocol that transports data from source to destination is usually what determines the degree of survivability [26].

A critical topic is the attainment of a higher dependability efficiency in tolerable wireless networks. This is especially vital for mission-critical dynamic systems, where data loss due to traffic disturbances caused by malfunctions is serious. Survivability techniques for wireless networks are often categorised into two categories: safeguarding and restoring [27].

- In terms of safeguards, protection necessitates the purchase of additional equipment and the allocation of resources for backup reasons apart from the primary ones. There are various distinct types of safeguards:
    - One-plus-one, where communication is divided evenly 50 by 50 between main and backup resources;

- 1:1; N: M, where N up to M main resources distribute backup reserves for future usage; and
- N: M, where N backup resources are shared for recovery reasons by up to M primary resources. Since the backup resources in protection schemes are predefined and reserved, recovery is quick.

- The process of recovering from a network failure is known as restoration. Restoration can be reactive, (in which case the backup configuration is generated after a failure), or proactive, (in which case the backup configurations are pre-calculated and appropriate resources are reserved for a set of failures).

2.2.1 Recovery strategy routing

Restoration techniques are used as route maintenance operations in all routing algorithms. If an outage is found on the previously used path, the variable is specified. The radius switches around the desired location for which hubs are permitted to do nearby restoration are expressed here. The new path's length is compared to the old path's length when the nearby restoration is completed and a new route is discovered. If the new route has more nodes, the origin receives a forwarding error (RERR) signal to notify it of the adjustment. The origin could choose to keep the current path or start a fresh path discovery procedure after getting the RERR [28].

2.2.2 Adaptive strategy routing

At every layer, the restoration method is suited for automated network configuration activation, culminating in a self-configuring scheme that adjusts to switching fault conditions. Since repair of flaws can occur at many levels, one consideration is to identify which traffic restoration pairs should really be employed at every component, as well as how this relates to the entire system’s architecture. There are two fundamental ways for determining a backup route for restoration as a thorough example of adaptive restoration tradeoffs at the traffic layer:

- An alternative route can be calculated ahead of time.
- A dynamic search for a backup path can be computed in real time.

Restoration is ensured under the pre-planned technique, as well as a backup for each connection set up when it is first assigned [29]. Signalling messages are delivered after being notified of a network breakdown in the dynamic search method, and alternate paths are

selected based on the analysis of the signal. Backup connections are stored for recovery reasons in the pre-planned method.

2.2.3 Routing in proactive restoration strategy

Proactive recovery mechanisms, on the other hand, determine restoration parameters in advance, based on predicted outages, and then spread the parameters across the network. When a network loss is detected, the recovery mechanism chooses one of the pre-calculated settings based on the nature of the failure. As a result, proactive recovery does not necessitate routing convergence time after a failure if the failure is covered by the pre-calculated settings [30]. When the failure is not factored into the pre-calculation, however, the recovery mechanism is unable to fully recover from the failure. As a result, when calculating the recovery parameters for the proactive mechanism, the network failures that are expected to occur must be carefully identified.

2.2.4 Routing in reactive restoration strategy

When network nodes notice network faults, reactive recovery techniques compute routing configurations and broadcast them throughout the network to converge routing. By leveraging dynamic methods in determining and spreading other channels following detection of failures, the nodes may accept various types of faults simply and without failure prediction [30]. Since fresh routing information is often communicated hop-by-hop, one of the major flaws of reactive recovery systems is that it takes a long time for routing convergence following failures.

2.2.5 Routing with Dijkstra algorithm strategy

One of the best short path algorithms is Dijkstra's ‘label algorithm’, which was proposed in 1959. Examples of ‘label algorithm’ applications are: multi-point routing; surveying and mapping science; the shortest path of logistics and transport; the intelligent transportation system; the expressway network toll collection, and so on [31].

The shortest path problem can be solved using a variety of algorithms [32]. Firstly, the algorithm of Dijkstra, and or the Floyd-Warshall algorithm is the second algorithm. The Bellman-Ford genetic algorithm (GA) is a third-generation algorithm that was developed by Bellman and Ford.

Dijkstra's algorithm, one of the most well-known techniques for finding the shortest path, operates on a weighted graph with non-negative edge weights. This algorithm is used by the majority of applications that strive to find the shortest path. Dijkstra's technique can find all shortest paths from a single point to all other points in a network, resulting in a single network. The state of each node is used by the algorithm to classify it. A node's state is made up of two elements: its distance value and its status label.

- A node's distance value is a scalar that represents an estimate of the distance between nodes ‘s’.
- The status label specifies whether a node's distance value is equal to the shortest distance to node 's' or not.
- If a node's distance value equals the shortest distance from another node *‘s’*, the node's status label is permanent.
- Otherwise, a node's status label is only temporal. The method keeps track of step-by-step modifications and node status updates.

2.2.6 Identifying literature gaps

Studies have begun to express interest in wireless network survivability strategies; however, some areas require further investigation, such as the use of optimisation models in resolving wireless network failures. This study has succeeded in bridging the gap by developing a swarm intelligence and evolutionary computing model (ACS & EGA) that may be used to resolve N2N, L2L, and N2L problems in wireless networks. The literature on some wireless networks and optimisation methodologies is sparse, and there is little comparison across the various wireless networks. However, as mentioned in section 1.5.2, this study has contributed substantially to filling those gaps that exists in the literature by means of articles published in reputable conferences and journals.

Another limiting aspect is the time lag between some of the researchers in the field of wireless networks optimisation models, as most of the studies were completed not more than a decade ago, despite the fact that some of the articles were published recently. Other than the optimisation models employed in various types of failure restoration in the literature, 45 others concentrated on theoretical frameworks with little practical application.

2.3 ROUTING IN RECOVERY STRATEGY

2.3.1 Recovery strategy background

In this section, some of the most well-known resilience methods suggested in the literature are reviewed here in detail as type of survivability strategy. A survivability strategy usually focuses on a specific form of failure. In general, failures can be either node failures, link failures or service node failures (such as access points, gateways, base stations, or cluster heads). There is a need to distinguish between conventional network nodes and service nodes because a service node's failure has a greater impact on the network since it impacts all related nodes. In other words, this concentrates on measures that alleviate the consequences of failures rather than the causes of failures.

2.3.2 Recovery strategy challenges

There are four obstacles and issues associated with various survivability approaches: Extensibility; Connectivity to a wireless network; Paths that are disjointed versus paths that are interleaved; and Local vs end-to-end restoration. Each of these are discussed [26].

- **Extensibility**

The main source of scalability issues is proactive protection systems. This is due to the use of redundant network resources to forward redundant data units, which ensures survival. There are two issues with such plans. The first is squandered resources. The second issue is that of the generated overhead. Duplication's high overhead can influence network speed and eventually lead to congestion, which becomes more noticeable as the number of protected sessions grows. In other words, when the number of communication sessions increase, existing proactive protection measures do not scale well. Erasure codes or network coding can be used to reduce the impact of duplication. The fundamental benefit of these strategies is that they eliminate duplication, resulting in a higher useful throughput.

- **Connectivity to a wireless network**

The minimal max flow between any two nodes in the network is defined as network connectivity, which is equivalent to the minimum link cut between any two nodes in the network. The concept can potentially be expanded to include the smallest node cut. That is, network connectedness is defined as the smallest number of nodes (or links) required to partition a network into two components A and A′, with no node in A connected to a node in A′ and vice versa. Alternatively, a network is considered to be connected if any pair of nodes in the network has a path between them. Furthermore, the concept can be expanded to K-

connectivity, in which a network is said to be K-node (link) linked if any pair of nodes in the network has K-node (link) disjoint pathways connecting them. Network connection is an important network feature that directly influences the network survivability. This is because the number of different paths that can be established between two nodes is limited by network connectivity. Node placement methods or topology management strategies can be used to attain a given level of network connectivity.

- **Paths that are disjointed versus paths that are interleaved:**

The most common approach to proactive protection techniques is multipath routing. In multipath routing, k pathways are found between a source node (S) and a destination node (D). These paths might be node or edge disjoint, or interleaving, in which some edges are shared. When a data unit is transferred from the source to the destination, the source sends k copies of the data unit along the K pathways to the destination. If the pathways are not connected, each one sends a single copy to D. If failures occur on at most K-1 paths out of the disjoint K paths, data delivery will be successful. However, if any of the K pathways fail, all of the copies will be lost. A shared link does not carry all of the copies from all of the pathways if the paths are interleaving; instead, it only carries one of them, and the shared link's head node duplicates the data unit on all of the outgoing paths.

- **Local vs. end-to-end restoration**

When a failure is recognised, the recovery process begins. End-to-end restoration or local restoration are both viable options. In end-to-end restoration, a node that identifies a failure sends a specific message to the source. When the source receives this notification, it is their responsibility to find another route to the destination. Local restoration, on the other hand, begins at the access point that first notices the fault. In either scenario, the alternate path may already be stored in the source buffer or must be discovered. This is dependent on how much memory each node has set aside for routing information. The key benefit of end-to-end restoration is that it delivers the best alternative S-D path because the search for a new path is limited to the source and destination. However, because the notification message must be forwarded by all intermediate nodes on the path all the way back to the source, end-to-end recovery takes longer and wastes more bandwidth. Local recovery, on the other hand, may yield poor alternatives but is faster and more efficient. Both strategies are employed in some circumstances. Until a new end-to-end path is established and used by the source, local restoration can be employed as a first aid to help packets in transit reach their destination instead of being dropped.

2.3.3 Comparisons of various routing in recovery strategies

Table 2.1 shows various algorithms used in recovery strategies in wireless network routing. The factors considered are routing overhead, power required, multi-path, delay, bandwidth required, and recovery time. The routing algorithms considered are: Ad Hoc On-Demand Distance Vector (AODV), Destination Sequence Distance Vector (DSDV), and The Optimal Link State Routing Protocol (OLSR), Wireless Routing Protocol (WRP). Temporally Ordered Routing Algorithm (TORA), Dynamic Source Routing (DSR) and Adaptive Disjoint Path Vector (ADPV).

Table 2.1: Comparison of various algorithms used in recovery strategies in wireless networks

Algorithms	Routing Overhead	Power Required	Multi-path	Delay	Bandwidth Required	Recovery time	Comment	Drawback
Reactive (AODV)	Medium	Minimal	No	Minimal	Minimal	More	Source-based repair	There is more time to fix.
Proactive (DSDV)	Minimal	High	No	Medium	High	More	Source-based repair	There is more time to fix.
Proactive (OLSR)	Minimal	High	No	Medium	High	More	Source-based repair	There is more time to fix.
Proactive (WRP)	Minimal	High	No	Low	High	Minimal	Source-based repair	The fixing time is short.
Reactive (TORA)	Medium	Minimal	No	More	Minimal	More	Source-based repair	There is more time to fix.
Reactive (DSR)	Medium	Minimal	No	More	Minimal	More	Source-based repair	There is more time to fix.
Adaptive (ADPV)	Medium	High	Yes	Medium	High	Minimal	Source-based repair	It requires more memory

2.4 ROUTING IN ADAPTIVE RESTORATION STRATEGY

2.4.1 The adaptive restoration strategy background

In an adaptive restoration strategy, restoration methods at each layer will be appropriate for autonomous invoking by networking devices, giving rise to a self-configuring system that adjusts to modifying failure environments. It has the capacity to recover faults at several layers. Recovery links are not set aside, so are not assured in adaptive restoration [33]. Multi-layer networks are a good example. The Adaptive Disjoint Path Vector (ADPV) is an example of an adaptive restoration routing protocol.

2.4.2 Adaptive restoration challenges

The ADPV is a flexible technique that adjusts to node failures and remaining energy. The purpose of ADPV is to maintain super-node connectivity in the event of node failures, and it accomplishes this by dynamically altering the transmission strengths of wireless sensor nodes. In the same way as all K-connectivity solutions [34]. These are as follows:

- It necessitates network redundancy and could only support the K-1 terminal outages.
- Furthermore, the ADPV requirement super-nodes interact directly and it is difficult to meet with all sensor devices.

2.4.3 Adaptive restoration strategies: Comparisons of different routing techniques

The adaptive (dynamic) algorithms can change their routing path based on factors such as search time, query hits, and message count. The routing table is dynamically updated in the dynamic algorithm, so no manual intervention is required. As a result, the dynamic routing algorithm can select a dynamic path from source to destination via intermediate routers. The "Distance Vector" and "Link State" routing algorithms are the best examples of such dynamic routing algorithms [35]. There are several advantages to adaptive routing over oblivious routing:

- Many adaptive routing strategies can quickly adapt to faulty network nodes or edges, whereas in oblivious routing, faulty nodes or edges may disconnect certain source-destination pairs, necessitating the computation of a new path system, which can be costly.
- The congestion of adaptive routing strategies may be preferred to that of oblivious routing strategies.

However, adaptive routing usually also has some weaknesses:

- A high degree of freedom in choosing a path for a packet may result in packet delays because it may take some time for the algorithm to converge on good paths.
- Adaptive routing may require more communication (because many of them require control packets) and may place significantly greater demands on hardware and software than oblivious routing.
- The analysis of adaptive routing is typically much more difficult than that of oblivious routing.

Table 2.2 compares several route options in adaptive restoration techniques.

Table 2.2: Comparison of various routing in adaptive restoration strategies

Algorithms	Routing Overhead	Power Required	Multi-path	Delay	Bandwidth Required	Recovery time	Comment	Drawback
Link State Routing Algorithm	Minimal	Minimal	Yes	High	High	Minimal	Source based repair	The fixing time is short.
Hot Potato Routing Algorithm	Minimal	Minimal	No	High	High	High	Source based repair	The fixing time is high
Distance vector Routing Algorithm	High	Minimal	Yes	High	High	Low	Source based repair	Fixing time is low

2.5 ROUTING IN PROACTIVE RESTORATION STRATEGY

2.5.1 Proactive restoration strategy background

It is necessary to pre-calculate recovery settings (routing tables) in proactive recovery mechanisms by assuming likely failures, and then distributing the settings throughout the network. When a network loss is detected, the recovery mechanism chooses one of the pre-calculated settings based on the nature of the failure. As a result, proactive recovery does not require routing convergence time after a failure if the failure is covered by the pre-calculated settings. When the failure is not factored into the pre-calculation, however, the recovery mechanism is unable to fully recover from the failure [30]. As a result, when calculating the recovery parameters for the proactive mechanism, the network failures that are expected to occur must be carefully identified. Traditional distance-vector and link-state protocols are used in the proactive protocols. These protocols ensure that the path to the destination is always available, ensuring that there is no delay when any node has to deliver packets. It can be used in interactive apps [36]. The following are the key strategies used in proactive protocols:

- increase the amount of topological information maintained at each node (to avoid loops and speed up protocol convergence);
- dynamically vary the size and frequency of route updates; and
- integrate Distance Vector (DV) and Link State (LS) features to improve floods.

Every node in a network using a proactive routing protocol has one or more tables that represent the overall topology of the network. These tables are updated on a regular basis to ensure that all nodes have the most up-to-date routing information. Topological information must be transferred between nodes on a regular basis to maintain up-to-date routing

information, resulting in a somewhat significant network overhead [37]. Routes, on the other hand, will always be available on demand. A proactive approach to mobile ad-hoc networks (MANET) routing aims to keep topological knowledge up to date at all times. In theory, all nodes should be aware of the entire network. This results in a persistent overhead of traffic routing, but no initial communication latency.

Proactive protocols include the Destination Sequenced Distance Vector (DSDV) protocol, Wireless Routing Protocol (WRP), Hierarchical State Routing Protocol (HSR), Source Tree Adaptive Routing Protocol (STAR), Optimised Link State Routing (OLSR), and Global State Routing Protocol (GSR). The proactive mechanism's redundancy ensures that the information reaches the intended destination even if there is a malfunction.

2.5.2 Proactive restoration challenges

The scalability issue is a flaw in this approach. This is due to using redundant network resources to forward redundant data units to, ensures survival. As a result, proactive recovery does not require routing convergence time after a failure if the failure is covered by the pre-calculated settings. When the failure is not factored into the pre-calculation, however, the recovery mechanism is unable to fully recover from the failure. As a result, when calculating the recovery parameters for the proactive mechanism, the network failures that are expected to occur must be carefully identified.

2.5.3 Comparisons of various routing in proactive restoration strategies

Table 2.3 shows the comparison of various routing in proactive restoration strategies

Table 2.3: Comparison of various routing in proactive restoration strategies

Algorithms	Routing Overhead	Power Required	Multi-path	Delay	Bandwidth Required	Recovery time	Comment	Drawback
Proactive (DSDV)	Minimal	High	No	Medium	High	More	Source-based repair	There is more time to fix.
Proactive (OLSR)	Minimal	High	No	Medium	High	More	Source-based repair	There is more time to fix.
Proactive (WRP)	Minimal	High	No	Minimal	High	Minimal	Source-based repair	The fixing time is short.

2.6 ROUTING IN REACTIVE RESTORATION STRATEGY

2.6.1 Reactive restoration strategy background

When network nodes notice network faults, reactive recovery techniques recalculate routing configurations and propagate them throughout the network to converge routing. By leveraging dynamic methods after detecting failures for the estimation and promulgation of substitute channels, the nodes may flexibly accept various types of network faults without failure prediction [30].

The ability of a reactive survivability tactic to know multiple paths ahead of time before an information exchange session begins is a strong point.

2.6.2 Reactive Restoration Challenges

Since fresh routing information is often communicated hop-by-hop, one of the major flaws of reactive recovery systems is that it takes a long time for routing convergence following failures.

2.6.3 Comparisons of various routing in reactive restoration strategies

Table 2.1 compares various reactive restoration routing strategies, and the reactive algorithms considered are AODV, TORA, and DSR, respectively.

2.7 SWARM INTELLIGENCE BASED ANT COLONY SYSTEM (ACS)

2.7.1 Ant colony system (ACS)

Marco Dorigo invented the Ant Colony System (ACS) algorithm to identify the best path in 1992. The algorithm is based on the foraging behaviour of ants. When foraging in the wild, ants usually take the quickest route from their nest to the food source. It is anticipated that there are many pathways from the nest to the food supply, as indicated in Figure 2.1. Initially, ants choose trails at random and leave pheromones in them. By perceiving the pheromones left behind on the path, the next ants will choose a path with a higher pheromone concentration. The greater the pheromone concentration in the path, the shorter the path length, and therefore more and more ants will eventually take this shortest path. Dorigo devised an ant colony system method to imitate ant foraging behavior based on this concept, which was first used to solve the traveling salesman problem (TSP) [38]. The goal of the traveling salesman problem is to discover the shortest path between N cities that passes

through each of them. M cities are chosen at random from the N cities at the start of the process. The M ants are then placed in M cities, with the city in which each ant is located being added to the ant's taboo table. The Kth ant selects the next city that is not in its taboo table based on the selection probability in each iteration of the algorithm and adds the passing city to its taboo table. The transition rule can be used to compute the selection chance of the kth ant transferring from city 'i' to city 'j' at time 't'.

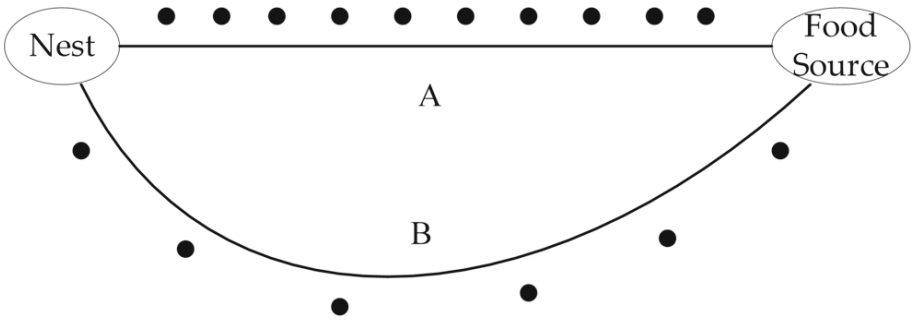

Figure 2.1: Ant foraging movements (adapted from [38]).

2.7.2 Initial pheromone concentration

Initial Pheromone concentration is represented in equation 1:

$$\tau_0 = \frac{1}{n\, L_{nn}} \tag{1}$$

A nearest neighbour heuristically determined the distance of the tour, which is L_{nn}, where n is the number of nodes in the network.

2.7.3 Local pheromone update

The local pheromone update is performed after each ant completes a selection, and the update formula is shown in equation 2:

$$\tau_{ij}(t+1) = (1-\rho).\tau_{ij}(t) + \rho.\tau_0 \tag{2}$$

where the decay parameter is $0 < \rho < 1$, and $\tau_0 = \frac{1}{nL_{nn}}$. L_{nn} is the distance of the tour by the nearest neighbour heuristic, where n is the number of nodes in the network and τ_{ij} is the initial values of the pheromone trails. By evaporating pheromone from the edges of each ant's tour, a local pheromone update rule encourages exploration of unused edges and avoids a local optimum. As a result, a local updating rule has the effect of making an already desirable edge less desirable for the next ant.

2.7.4 Global pheromone update

Only the edges of the global best ant's tour from the beginning of the trail will be modified the pheromone level using the global pheromone updating rule once all ants have built a tour.

$$\tau_{ij}(t+1)=(1-\rho).\tau_{ij}(t)+\Delta\tau_{ij}\ (t) \quad (3)$$

$$\Delta\tau_{ij} = \begin{cases} \frac{1}{L_{gb}}, \text{ if } (i,j) \in global\ best\ tour \end{cases} \quad (4)$$

Where L_{gb} is the length of the best tour in the world as measured from the trail's start.

2.7.5 Computation of edge attractiveness

Computation of edge attractiveness is shown in equation 5

$$\eta_{ij}=\frac{1}{d_{i,j}} \quad (5)$$

The distance between nodes 'i' and 'j' is denoted by'd'.

2.7.6 Computation of edge probability

Marco Dorigo et al. were the first to introduce and apply the ant system to TSP [39]. Each ant is initially placed on a node that is chosen at random. By applying the probabilistic transition method in equation 6 to an ant 'k' now at node 'i', it can choose to go to node 'j'.

$$P^{k}_{i,j}(t) = \frac{[\tau_{i,j}(t)]^{\alpha}[\eta_{i,j}]^{\beta}}{\sum_{i\epsilon J^{k}_{i}}[\tau_{i,j}(t)]^{\alpha}*[\eta_{i,j}]^{\beta}} \quad (6)$$

$\eta_{i,j}$ is the heuristic visibility of edge *(i, j)*, which is usually$1/d_{i,j}$, where $d_{i,j}$ is the distance between nodes i and j. When the ant arrives at node 'i'. $J_k\ (i)$ is a set of nodes that must be visited. α and β are two adjustable positive parameters that control the relative weights of the pheromone trail and of the heuristic visibility. If this parameter is set to 0, the closed vertex is more likely to be chosen. This strategy will cause the system to reach a state of stagnation, in which all of the ants will construct a sub-optimal tour. As a result, it appears that a trade-off between edge length and pheromone intensity is required. α and β are two parameters that define the pheromone trail's respective influence. The pheromone concentration on the link between nodes 'i' and 'j' is provided by τ_{ij}.

2.8 EVOLUTIONARY GENETIC ALGORITHM

2.8.1 Enhanced genetic algorithm (EGA)

The genetic algorithm is a met-heuristic way to solve different optimisation issues. It starts with a population of possible solutions that is produced at random. A chromosome, or simply

an individual, is a basic string of genes that represents an individual solution. A fitness function evaluates each member to assess its quality. The GA goes through three activities after generating the initial population: selection, crossover, and mutation [40]. The initial population is used to generate a set of possible solutions in the selection phase. Then, by crossover, two randomly selected chromosomes (parents) are used to make two kid chromosomes by exchanging genetic information between the parent chromosomes. The kid chromosomes are then subjected to a mutation procedure in order to achieve a better result. After the mutation is complete, the fitness function evaluates the kid chromosomes, and their values are compared to all of the previous generation's chromosomes. If the current children have higher fitness levels, their parent chromosomes are replaced. The proposed algorithm, like existing GA-based approaches, includes chromosome representation, initial population generation, fitness function determination, crossover and mutation operations.

In solving the wireless network failures, a heuristic is added to GA for better performance. This heuristic is the calculated required bandwidth along with the optimal rerouting path generated to reroute video messages. The added heuristic makes GA an enhanced genetic algorithm.

2.8.2 Chromosome value encoding

The interconnectivity of links is the chromosomal value representing a communication line, where the link cost is the distance between two nodes. Table 2.5 depicts how the pathways are represented.

Table 2.4: Sample chromosomes value encoding

Chromosomes	Links forming the chromosomes (Paths)
Path – 1	A – C – I – M – N
Path – 2	A – C – I – M – J – N
Path – 3	A – C – D – H – I – M – N
Path – 4	A – D – G – J – M – N
Path – 5	A – D – G – J – N
Path – 6	A – E – G – K – O – N
Path – 7	A – D – H – I – M – J – N
Path – 8	A – E – G – J – N

2.8.3 Fitness evaluation of network paths

The fitness function is used to judge the quality of a path inside the network, and the genetic algorithm seeks for the ideal path with the highest fitness. Equation 7 defines the fitness function, which includes computing efficiency and precision [41].

$$F_i = \frac{1}{\sum_{j=1}^{l_i-1} C_{g_i(j),g_i(j+1)} + \sum_{j-1}^{l_i-1} B_{g_i}(j)g_i(j+1)} \quad (7)$$

F_i stands for the fitness of paths (chromosome), $l_i$is the chromosome's link (path) cost, the node in the network path which is also gene is $g_i(j)$, C is the chromosome's path cost, and B is the bandwidth a chromosome requires to transmit a packet.

2.8.4 Selection from the collection of chromosomes

A rank–based fitness assignment was chosen as the selection method. Each network path's fitness is determined solely by the cost of the path, the needed bandwidth, and the number of nodes in the network path. As demonstrated in Equation 8, rating establishes a standard scale throughout the set of network paths.

$$Let\ p_i = \frac{f_i}{\sum f_j}. \quad (8)$$

Where p_i is the likelihood that variable 'i' will be chosen, f_i denotes the individual 'i' fitness and $\sum f_j$ denotes the total of all participants in the network's fitness path collection [42].

2.8.5 Operator of genetic crossover

The crossover operator combines subsets of both parent chromosomes to create kids with some genetic information from both parents. Crossover can be classified into two types: one (single) point and multipoint crossover. There is just one crossover site in a single point crossover, and there are multiple crossover sites in multipoint crossover [41]. Crossover looks at present solutions in order to come up with better ones. In the case of routing issues, crossover involves physically exchanging each route of the two chosen chromosomes in such a way that the child produced by the crossover will only be one route.

2.8.6 Genetic mutation operator

The mutation operator modifies genes at random to partially shift the solution pace to new regions. If the values of successive iterations are the same, mutation is performed [41]. It is possible that the crossover operation creates populations that are degenerate. A mutation operation is used to undo this. Inversion, insertion, reciprocal, omitting, exchange, and other mutation operations are examples of mutation operations. Inversion involves picking two random places and reversing the string between them. A node is placed at a random point in the string in the event of insertion. Nodes at two random places are exchanged in reciprocal exchange. The omitting mutation operator is used in this study, which is accomplished through mutating one chromosome/node at random within future group. The chosen gene is

then removed. For example, (A B C D E F H I G) is an example of a path that has (A, B..., H, I, G) nodes. The omitting operator is used to remove node 'B': (A B C D E F H I G) => (A C D E F H I G). The application of each type of mutation operator is determined on the issues at hand. For instance, if the interval between the start and finish points is minimal, an omitted mutation is preferable. Since transmission originates at the source node and ends at the destination node, the omitting mutation operator is used in this work to ensure that the source and destination nodes are not omitted.

2.9 SPARE CAPACITY ALLOCATION (SCA)

2.9.1 Resources allocation on wireless networks

A capacity allocation module in a wireless communication system selectively allocates portions of a total authorised capacity among a plurality of nodes, each of which has an enabled capacity. If a first condition exists, the capacity allocation module allocates a first authorised portion of the total capacity to at least one of the nodes, and a second, different authorised portion of the total capacity to that node if a second condition exists [43]. In one case, the capacity allocation module increases the allocated capacity for one node while decreasing the allocated capacity for at least one other node, ensuring that the total allocated capacity among the plurality of nodes remains within an authorised total capacity limit. In one case, such changes are mandated by pre-selected license terms. In another case, the modifications are made dynamically in response to changes in traffic load conditions at one or more of the nodes. Changing the total authorised capacity is one example of how to provide even more customisation.

2.10 STRUCTURE OF VOICE/VIDEO/MULTIMEDIA MESSAGE

A transmission message consists of the following parts as indicated in Figure 2.2: A header contains identifier and routing information like body length and message type identity. A message body contains the actual content of the message. It contains a fixed part and floating part. This section is created to describe the structure of messages being transmitted (voice, video and multimedia messages). The capacity efficient ACS and enhanced genetic algorithm (EGA) models' rerouting power is tested using voice and video messages.

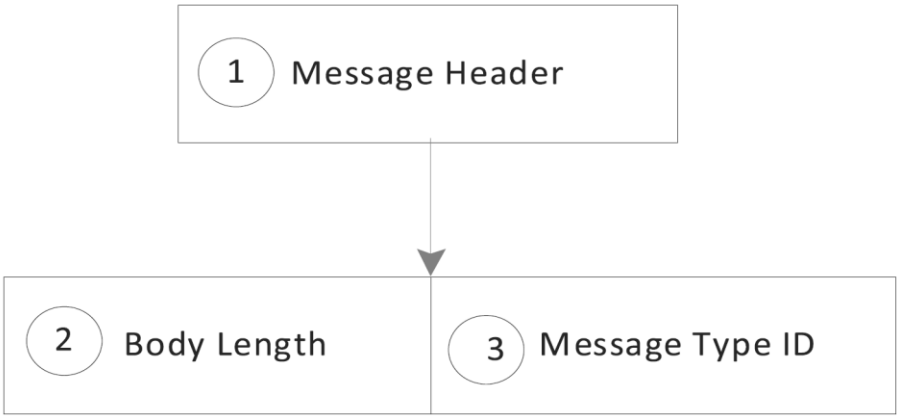

Figure 2.2: A message's structure (adapted from [28]).

2.11 CHAPTER SUMMARY

This chapter begins with a comprehensive overview of wireless network survivability, including recovery strategies and challenges that contribute to recovery strategy issues. It also addressed the gaps that future wireless network optimisation researchers will need to fill. The chapter also includes discussion of the structure of wireless network messages, such as voice, video, and multimedia messages.

This chapter ends with survivability of wireless networks prone to failures based on the reviewed literature. It also mapped out an open research structure covering various wireless network challenges such as single link failure, single node failure, multiple links failure, multiple nodes failure and multiple node-links failure. These failures are also explored, and the optimisation options for resolving them. This open research framework will serve as a guide for future researchers looking into various concerns of wireless network optimisation models.

CHAPTER 3: ASSESSMENT OF EXISTING RESEARCH ON THE SURVIVABILITY OF FAILURE PRONE WIRELESS NETWORKS

3.1 INTRODUCTION

Wireless network service providers and network operators are increasingly concerned about the viability of their networks. Internet of Things (IoT), mobile ad-hoc networks (MANET), wireless asynchronous transfer mode (WATM) networks, sensors networks, satellite communication networks, cell phone networks, and terrestrial microwave networks, among others, are examples of non-infrastructure and infrastructure-based wireless networks. Critical services in these wireless networks should be available at all times, even if unfavorable events like attacks, natural disasters, or common failures occur. Packet transmission over wireless networks has always been difficult owing to failures that have always happened due to various types of wireless network connectivity difficulties. These failures have created severe disruptions, and the slow detection and diagnosis of these failures has exacerbated their impact in terms of operational service, financial loss, and human factors like as technological confidence [8].

There are several sorts of failures: failure of a single link, a single node, multiple links, multiple nodes, single node-links failure, and multiple node-links failure. In order to avoid a prolonged network breakdown, various approaches have been proposed in the literature for wireless network survival; some of these techniques used are swarm intelligence, evolutionary algorithms, reactive, proactive, and adaptive routing optimisation techniques.

Swarm Intelligence (SI) is a burgeoning topic of research that contains a more optimal method to problem resolution than the traditional technique in practically all engineering domains. The SI is derived from imitations of social behaviours gained from insects and animals, such as ant colony optimization (ACO), Artificial Honeybee (ABC), Fireflies (FF), and Honey Bot [44]. The field of ‘Ant Algorithm’ investigates models that are learned from seeing the behavior of real ant colonies, in which the ACO is the field of ‘Ant Algorithm’ studies models that are learned from observing the behaviour of real ant colonies. The SI is presently regarded as one of the most promising artificial intelligence (AI) techniques, with a steady increase in scientific interest, due to its many advantages. This is backed by the growing number of effective SI research outputs, as well as the rapidly growing number of swarm intelligence conferences and journals.

The evolutionary algorithm is another optimisation tool that is used to optimise wireless networks. Metaheuristic algorithms, such as evolutionary algorithms, are used to tackle complicated optimization issues. Despite the fact that they were presented decades ago, their application to real-world optimization issues necessitates substantial computational resources that were not available at the time [45]. Modern computers and laptops with multi-core architectures can now perform millions of operations per second, allowing evolutionary algorithms to be used in a variety of scientific fields. They are based on the genetic operators' crossover and mutation to evolve a population of viable solutions. Many mobile multi-hop optimisation problems, such as topological management, broadcasting techniques, routing protocols, and mobility models, have been effectively solved using evolutionary algorithms.

The Ad-hoc On-Demand Distance Vector (AODV) is a well-known best reactive methodology for discovering the route as the topology changes. Routing packets from one wireless network to another is the most difficult problem. When a link in an active route breaks, the node upstream of the break has the option of repairing the link locally. When a link breaks, the upstream node (the mending node) classifies the link breaks and uses different procedures for different types of link breaks based on the status of its downstream node [46].

Another routing optimisation strategy to explore is the Adaptive Disjoint Path Vector (ADPV) algorithm. It's a flexible strategy that adjusts to node failures and remaining energy levels. The purpose of ADPV is to maintain super-node connectivity in the event of node failures, and it accomplishes this by dynamically altering the transmission strengths of sensor nodes [34]. The ADPV algorithm ensured reliable super connection between nodes via the Adaptive Disjoint Path Vector (ADPV) algorithm. The ADPV was divided into two stages: single initialisation and restoration [47]. When compared to the traditional DPV technique, they were able to achieve a two-fold improvement in super connection between nodes.

The Temporally Ordered Routing Algorithm (TORA) is a source-initiated, link-reversal-based adaptive routing strategy for highly dynamic mobile multi hop networks. This protocol can create routes quickly and cut communication overhead as much as possible by responding to topological changes with localisation. This means that instead of using the concept of the shortest path to select routes, TORA employs the 'direction of the next destination' to convey data [48]. As a result, there will be less processing and bandwidth utilisation. The source node travels to the destination through one or two paths that pass

through multiple intermediate nearby nodes. The TORA protocol has three basic processes: route formation, route maintenance, and route erasure.

The research question of this thesis, therefore, emanated from the views: “How can a detailed analysis on wireless network survivability research be conducted to build a blueprint to provide insights for both future academics and practitioners to guide wireless network subscribers?”

After detailed analysis, the following conclusions/methods are the main contributions of the research in this chapter:

- Conducting a thorough analysis of the literature on wireless network survivability research to identify unexplored areas of wireless network survival that lead to the proposal of various open research questions.
- Development of a framework to reflect a viewpoint on the wireless network survivability literature, to uncover hidden studies on wireless network survivability solutions applied to single and multiple failures that have received insufficient attention in the literature; to boost awareness; and to offer research challenges for future researchers.
- In terms of broader impact, the knowledge obtained from the analytics results serves as a roadmap for wireless network survivability research and training for academics and practitioners.

3.2 WIRELESS NETWORK SURVIVABILITY DESIGN AND CHALLENGES

By replacing wired infrastructure with wireless infrastructure and giving access to mobile devices, wireless network technology has reduced human effort in obtaining data at diverse locations. Since wireless networks must be available and efficient, network failures are one of the major obstacles to quality of service (QoS). Single link failure, single node failure, multiple links failure, multiple node failure, single node-links failure, and multiple node-links failure are some of these failures. Different wireless networks are discussed, as well as how these issues are resolved on different wireless networks.

3.2.1 Wireless asynchronous transfer mode (WATM) networks

In addition to the expanding volume of computer data, the wireless asynchronous transfer mode (WATM) has been developed as the standard for future networking that is expected to transmit speech, real-time video, and images. The WATM has made the digital network's

broadband integrated service a reality. It is a technology that provides bandwidth on demand, allowing for the overall flexibility and efficiency required for high-speed multi-service and multi-media networks [33]. Another advantage of the WATM networks is that they can be extended to a wireless scenario, known as wireless ATM. Wireless ATM technology's strength will be its ability to accommodate a variety of protocols, including Integrated Services Digital Network (ISDN) and Internet Protocols (IP).

3.2.2 Mobile ad-hoc networks (MANET)

A wireless mobile communication network made up of a set of mobile nodes equipped with wireless transceivers is known as an ad-hoc network. It is temporary and does not rely on pre-existing infrastructure. The network's mobile nodes communicate information using their own wireless transceivers; when the information is beyond of the communication range, other intermediary nodes can relay the information [49]. They can be widely employed in contexts where wired networks are unavailable or where communication is required just briefly, such as military applications, sensor networks, disaster assistance, and emergency response. Each node in a MANET serves as both a host and a router, and the nodes are connected by wireless channels in the network.

3.2.3 Internet of things (IoT) networks

The Internet of Things (IoT) is the next important stage in the evolution of the internet from a communication medium that connects computers to a platform that embraces common objects (things). This has the potential to change a variety of areas of the economy and society in general, such as enabling smart cities, smart transportation systems, intelligent energy supply management, and so on, all of which are enabled by data collected from sensors [50]. The IoT-based systems are prone to errors and are unstable, resulting in the formation of faults throughout the network and, in certain cases, misbehavior. Node, link, protocol conversion, and communication problems all cause many forms of defects in IoT networks. Failures can occur as a result of hardware and software malfunctioning in the devices. Network failures caused by node or link failures are the most serious. As such, an IoT network is made up of interconnected layers such as device, controller, restful services, gateway, internet, and storage, as well as computational layers [51].

3.2.4 Wireless sensor networks

Wireless sensor networks (WSNs) are made up of multiple sensor nodes that are used for a variety of purposes, including target tracking, pressure monitoring, health monitoring, and fire detection. Transducers, radio transceivers, and wireless interfaces make up the sensor nodes, which collect data from the environment. These low-cost, tiny sensors work together to build a network that performs activities according to their requirements. Various types of sensor nodes, such as biosensors and thermal, mechanical, magnetic, optical, and chemical sensors, can relate to node to detect the change or property of the environment. Since sensor nodes have limited battery life, memory, and computing power, and because they are located in remote locations, radio signals are employed to communicate between the source and the base-station [52]. The WSNs, in general, have little to no infrastructure and can be divided into two types: organised and unstructured sensor networks.

3.2.5 Satellite communication networks

One of the most dependable means of wireless communication is the satellite communication network. Long-distance communication, a vast coverage area, and customised communication contexts are all advantages of satellite communication networks over traditional wireless communications [53]. As a result, their importance in emergency applications is increasing with each passing year. This is especially true in the event of large-scale disasters that damage communication infrastructure. Even if only a few communication access points are accessible in the disaster-stricken area, additional demand may cause network congestion and overload. As a result, disaster relief efforts will be more practical and crucial if satellite communication is used.

3.2.6 Cell phone networks

A mobile phone network is a large area covered by radio waves. This area is then divided into cells of specific shapes and sizes, with one transceiver (also known as a base station) in each cell. Base stations are vital because they connect one cell phone user to the next, regardless of whether they are in the same cell or not; base stations are essentially large antennas at the top of a hill. Cells connect with one another using base stations, which provide radio coverage across a large area. This is possible if there are enough cells [54]. This allows a larger number of small portable or handheld network devices, such as mobile phones, laptops, navigation systems, and other similar devices, to communicate with each other as well as non-portable

network devices, such as land line telephones, desktop computers, and radios, located anywhere on the network. A transceiver can move between different cells while keeping the connection because the connection spans the whole geographical area that has been predetermined; however, if there is an area that the cells do not cover, a hard-handover will occur.

3.2.7 Terrestrial microwave networks

Microwave networks are primarily used in mobile base stations for service backhaul, sending signals to the base station controller (BSC) and mobile switching centre (MSC) for switching. When establishing prohibitively expensive optical networks, microwave communication networks are widely used. Microwave is widely used as a substitute when optical fibre deployment is difficult due to geographical or other constraints. Microwave is commonly used as a backup connection in optical transmission networks, and enterprise private networks [55]. Microwave technology is increasingly being used to deliver carrier Ethernet. The key advantages of microwave-based ethernet solutions are as follows:

- Quick setup time and easy crossing of city terrain
- Cost-effectiveness
- Flexibility
- Mature carrier-grade solution
- No cable cuts, faster recovery if damaged
- Better resilience to natural catastrophes like floods and earthquakes.

Microwave radio communications have become a critical component in the successful deployment of modern mobile networks, with over 60% of mobile base stations globally connected through microwave. Each radio site requires 25 Mbps, and with 100% of the radio sites, the maximum backhaul capacity required for the Multi base transceiver station (BTS) is 150 Mbps. Point-to-point communications are commonly carried out using microwave frequencies between 1 GHz and 100 GHz [47] along line-of-sight channels termed links within the broader spectrum of radio frequency (RF) communications. The propagation characteristics of these frequencies enable the transmission of large volumes of data between remote communication nodes without the need for wires.

3.3 FAILURES IN WIRELESS NETWORKS

Wireless network devices are prone to errors and are fragile, resulting in the production of defects throughout the network and, in certain cases, misbehaviour. Wireless network failures can take many forms, including node, connection, protocol conversion, and communication problems. Failures can occur as a result of hardware and software malfunctioning in the devices. Network failures caused by node or link failures are the most serious. Device failures, local network failures, controller failures, gateway failures, internet failures, and remote storage and processing failures are all possible in wireless networks [51]. Wherever a failure occurs, the wireless network will be rendered inoperable and useless.

3.3.1 Single link failure

When a link element in a wireless network fails, it is referred to as a single link failure. Adding a new link or redirecting and redistributing traffic from a broken link to other still working links with enough capacity to carry the additional traffic from the failed link can solve a link failure problem [2].

3.3.2 Single node failure

A single node failure occurs when one of the computing nodes in an array fails [56]. These events can be produced by a number of things, including a device being turned off for maintenance or crashing due to hardware failure. If a single node fails, for example, it may cause numerous nodes to fail if the failed node is a central node that controls other nodes in the network [57].

3.3.3 Multiple links failure

There are two frequent scenarios that can result in multiple links failing.

- On the network, an arbitrary link may fail, and before it can be repaired, another link fails, resulting in a multi-link failure sequence. In practice, two separate physical links may be routed through the same common conduit. When several links fail, a connection's backup capacity may be lost in the first failure, and the connection may become susceptible or unprotected when the second link fails [58]. The real-life example of multiple connections failure occurs when distinct fibre links share common failure structures, forming a shared-risk link group.

- And, after the light routes are routed on the physical topology, each physical fiber connection can handle several light paths via wavelength division multiplexing. Two or more light – routes could potentially share the same physical link. The failure of a single physical connection in a logical topology can result in the failure of numerous links.

3.3.4 Multiple nodes failure

When more than one node in an array of compute nodes fails, this is known as multiple node failure [56]. When more than one piece of equipment or node fails at the same time in a network, this is known as multiple node failure. To defend networks from multiple failures, network restoration models are designed to provide protection for two or more network elements, with the idea that, while unusual, multiple, near-simultaneous failures are not unheard of.

3.3.5 Multiple node-links failure

Single node-links failure is a process in which the failure of a node causes the failure of interconnected links in a wireless network. The capacity of nodes and links is severely constrained in this communication mechanism. When the load on a few nodes or links in the network exceeds their capacity, node-link failures can occur, and the entire network can be rendered inoperable [59]. It occurs when many node-link failures occur at the same time. That is, the failure of one node-link in a network causes the failure of two or more node-links.

3.4 PROPOSED WIRELESS NETWORK RESEARCH FRAMEWORK

Figure 3.1 shows how the proposed wireless network research framework, which includes many wireless networks, intends to develop optimisation strategies for surviving wireless network failures so that the network can continue to function. It also provides crucial information to network developers on the important phases of establishing a long-lasting wireless network.

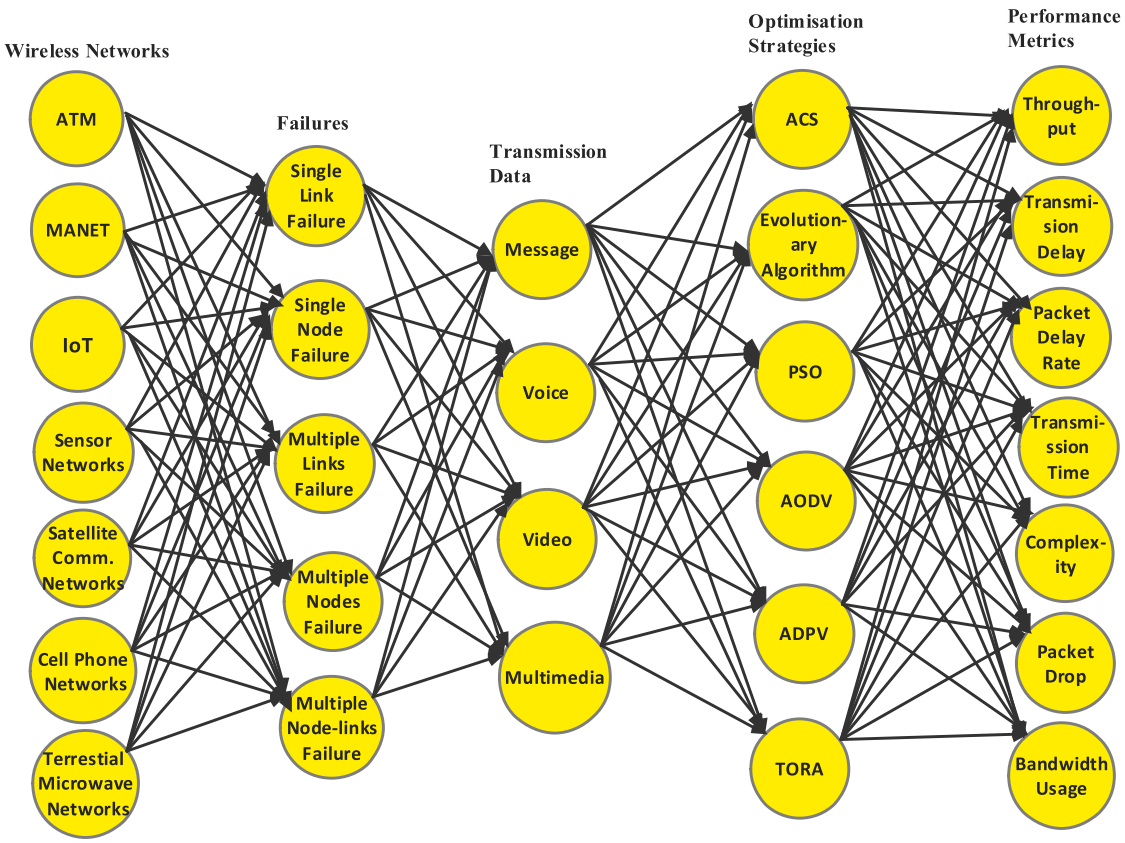

Figure 3.1: Proposed wireless network research framework

Following significant study into wireless network routing optimisation, a common routing optimisation framework was established that encompasses numerous wireless networks such as WATM, MANET, IoT, sensor network, satellite communication network, mobile phone network, and terrestrial microwave network. The proposed framework studies network routing failure challenges, and many forms of wireless network failures, including single link, single node, multiple links, multiple nodes single node-links, and multiple node-links failures, have been identified. These networks send out a variety of messages, including voice, video, and multimedia. As wireless network routing optimisation methods, the suggested framework recognised ACS, evolutionary algorithm (Genetic Algorithm), particle swarm optimisation (PSO), ad-hoc on-demand distance vector protocol (AODV), adaptive disjoint path vector (ADPV), and temporarilly ordered routing algorithm (TORA). The suggested method finds the best optimisation alternatives based on performance metrics.

Several optimisation strategies have been identified as a result of the literature review. This section discusses optimisation strategies and the various types of failures that these strategies can address.

3.5 ANT COLONY SYSTEM

The ant colony optimisation (ACO) algorithm has drawn the attention of a growing number of academics since the early 1990s, when the first ACO algorithm was presented, and several successful implementations are now available [44]. Furthermore, a considerable corpus of theoretical work is becoming available, providing academics and practitioners with important directions for future ACO implementations.

The ACO is a swarm intelligent (SI) algorithm that is useful in tackling discrete optimisation problems [60] and is inspired by the foraging behaviour of ants. Ant colonies have an emergent problem-solving tendency, such as food gathering, and this problem-solving nature has inspired the development of efficient routing algorithms, particularly in Ad-hoc Wireless Networks (AWN). While adapting ACO for routing on an ad-hoc wireless network, there are a few difficulties with ACO that must be solved. Owing to a condition known as ‘stagnation’, load balancing is one of the most significant challenges. Stagnation happens when all packets begin to travel on the best path and packets are lost owing to congestion. The ACO, therefore, employs a variety of approaches to address this issue [61]. This study will, therefore, examines various approaches for dealing with various sorts of failures in wireless networks.

3.5.1 Single link failure

One of the most prevalent issues in wireless networks is link failure. A lost link must be restored precisely and rapidly to minimise the consequences of the failure. Mohan, et al.,[62] have offered a strategy for addressing survivability during single link loss. This strategy reduces the amount of time it takes to recover from a single link loss. Alternative paths for data retransmission are calculated using the (ACO) algorithm and the neighboring shortest cycle. The link failure problem is discussed in [63], and the ACO algorithm is used to discover the shortest path when a link fails in a distributed context. The performance comparison between the ACO and Prim's algorithm after applying the ACO to the link failure problem reveals that the ACO algorithm helps to choose the shortest path in the smallest amount of time.

3.5.2 Single node failure

De Lima and Pavani [64] have proposed a routing and spectrum assignment (RSA) algorithm based on ACO with a crank back mechanism for resolving single node failures. This

algorithm is suitable for both the establishment of light-paths during normal network operation and the recovery of light-paths affected by single link or single node failures.

3.5.3 Multiple links failure

Zhang, et al.,[65] have suggested ACO-based Routing Algorithm (ARA), a representative ACO-based routing protocol for wireless networks, for resolving multiple connections failure. The ARA is a basic ant colony optimisation meta-heuristic technique that is based on on-demand routing. There are three steps to the routing algorithm: route discovery, route maintenance, and route failure handling. In (ARA), the route discovery phase is developed similarly to AntNet. In the route discovery phase, forward ant (FANTs) and backward ant (BANTs) are deployed. The sender broadcasts the FANTs. Intermediate nodes identify duplicate FANTs by their sequence numbers and delete them. BANTs are formed and sent back to the source nodes after FANTs reach their destination nodes. To reduce the overhead imposed by using periodic ants, ARA employs data packets to maintain the route. When a node detects a link failure, it deactivates the link by setting the pheromone value to zero, and then it looks for a different connection. It warns its neighbours if this fails. This process is repeated until an alternate route is found or a route error notice is received by the source node. If there are still packets to send, the source node will start a new route discovery phase in this situation.

3.5.4 Multiple nodes failure

Multiple node failure can occur for a variety of reasons, including natural disasters or malevolent human activity [66], and several strategies are being researched to improve wireless network preparedness for such situations. Owoade and Osunmakinde [24] have presented an ant colony system (ACS) paradigm for resolving the failure of numerous nodes. When there was a failure between peering nodes in this architecture, a rerouting channel was supplied with specific performance assurances, for example sufficient bandwidth with minimal latency and overall great network resource use. The design incorporates sufficient variety and spare capacity to allow for the restoration of services at the intended service level in the event of capacity loss.

3.5.5 Multiple node-links failure

Bhatt et al.,[67] have suggested an unique multi-fault localization approach based on ant colony optimisation to handle multiple node-link failures in wireless networks. When

compared to existing localisation techniques, the ant colony optimisation-based multi-faults localisation mechanism has a low flooding time and warning packets, as well as a high success rate. The suggested approach is divided into two steps: (i) fault localisation using the ACO algorithm, and (ii) restoration, which helps to lower the network's loss rate. The ant applies the transition rule to each option. The initial step in this procedure is to generate a random number that will be used to determine whether the ant will exploit past pheromone deposits or try to find a new probable flaw. If the ant successfully traverses all of the alarms, it signifies that the search for the fault set was successful, and the global updating rule with positive feedback can begin. On the back path, the feedback ants use the global updating rule, while the forward ants use the global updating rule. When the feedback ant arrives at the source alarm, the algorithm is complete. A bidirectional link between nodes is assumed in the proposed approach, with a pair of unidirectional fibres running in opposite directions. The search packet comprising messages is periodically broadcast to each node of the network at every update interval to monitor the link state in normal operations.

In this study, the classic ant colony algorithm for mesh network routing optimisation has a poor convergence rate. Li and Peng [68] have suggested an enhanced ant colony algorithm-based multi-path routing system. To improve the speed of route optimisation, the protocol first includes a sorting algorithm based on the ant colony algorithm and introduces the idea of elite ants. Second, the multipath transmission of self-organising networks is investigated in this research. The simulation results show that, when compared to AODV, and Dynamic Source Routing (DSR) routing methods, the approach can quickly locate several high-quality paths with low overhead and fast convergence.

3.6 EVOLUTIONARY ALGORITHM

Nature-inspired algorithms are being developed by researchers to handle complex issues; for example, they have been widely used in network design. Iterative metaheuristics known as evolutionary algorithms (EAs) can be used to tackle NP-complete problems [40]. They usually work on a population of preliminary solutions to the problem, which are evolved simultaneously towards better ones. This evolution process is carried out by applying stochastic operators to the solutions, with the goal of simulating the natural evolution process. Individuals are assessed in order to determine the value of the solution they represent (the fittest individuals survive for the next generations). The EAs iterate on the collection of potential solutions until the termination condition is satisfied (usually, after the optimal

solution is found or several iterations are performed). Solutions are evolved using evolutionary operators such as parent selection, recombination (or crossover), and mutation in each iteration. Typically, the evolutionary operators used in the evolution of various EA families differ.

3.6.1 Single link failure

Biswas and Podder [69] have proposed a restoration technique with seamless communication that employs bit error rate (BER) evaluation of the alternative link and connects those links for data communication to overcome single link failure within the network in this study work. This suggested approach employs BER evaluation to determine the least BER value of an adjacent channel between two nodes in a given network, and in the event of a failure on any working network connection, all adjacent cycles between the failed link's end nodes are determined. The fittest path is then determined using the Genetic Algorithm (GA). The BER performance of the link is used as the primary criterion for choosing the best path. This is accomplished by designating neighboring cycles of the failed connection with the lowest BER value, and that adjacent cycle consists of the failed link's source and destination nodes, allowing the failed link to be bypassed and remain connected at all times.

3.6.2 Single node failure

When some of the sensor nodes in distributed sensor networks are broken, L. B. Bhajantri and N. N [70] have proposed using Genetic Algorithm (GA) to detect and recover node faults. The major goal of this project is to develop a fault tolerance mechanism that is both energy efficient and responsive to the network, using GA to detect defective nodes in the network based on energy depletion and node-to-node link failure. Faults at the node and network level are detected using the suggested fault detection paradigm.

3.6.3 Multiple links failure

Owoade and Osunmakinde [71] have investigated video traffic cascaded connection failures on attacking wireless networks. The goal of this study was to create an enhanced genetic algorithm (EGA) that focuses on capacity efficiency and fast restoration in order to quickly handle link-link failures. This fault-tolerant paradigm was evaluated for such failures on a complicated node network. The proposed approach provided optimal alternative routes and the bandwidth necessary for rapid rerouting of video stream.

3.6.4 Multiple nodes failure

According to Khosrowshahi and Shakeri [72], wireless sensor networks (WSNs) are made up of a collection of sensor nodes with limited capabilities. When WSNs are subjected to hostile conditions such as military zones or disaster areas, they may have multiple node failures and lose connectivity as a result of being partitioned into discontinuous parts. To restore connectivity, relay nodes (RNs) are introduced as an option. They are more expensive than sensors since they have higher mobility, power, and transmission range, and therefore they require a minimum number to be used. This research develops a genetic method to solve the problem of RN placement in a multiple disjoint network. The problem is reintroduced as the Steiner tree problem (an NP-hard problem) with the goal of identifying the smallest number of Steiner points where RNs should be inserted in order to restore connectivity. The GA method then minimises the number of RNs while also determining their position iteratively. In comparison to the best available work, investigational results show that the suggested GA can establish network connectivity with a fair number of RNs.

3.6.5 Multiple node-links failure

Since the IoT is vulnerable to irregular intervals failures, Owoade & Osunmakinde [73] investigated the robustness of capacity efficient GA and based on demand recovery to quickly handle link and node failures. The system was tested on link and node failures in large networks at various places. The proposed architecture could provide good alternate routes as well as the bandwidth required for speedy multimedia traffic rerouting.

A hybrid evolutionary algorithm is used in the proposed revolutionary, dynamic least cost multicast routing system for internet protocol (IP) networks. Under latency and bandwidth limits, Vijayalakshmi and Radhakrishnan, [74] find the multicast tree with the lowest cost. The proposed work can handle dynamic conditions such as changes in multicast group membership or node-link failures, and it employs two alternate crossover and mutation probabilities to ensure solution variety and rapid convergence. According to simulation results, the proposed protocol generates a dynamic multicast tree at a lower cost. According to the findings, the proposed technique has a greater convergence rate, a higher dynamic request success rate, and takes less time to execute than other current algorithms.

3.7 PARTICLE SWARM OPTIMISATION (PSO)

Dr. Eberhart and Dr. Kennedy invented Particle Swarm Optimization (PSO) in 1995 [70], inspired by the social behavior of species such as bird flocking or fish schooling, and used it to address the meta-heuristic optimization issue [75] from nature-inspired particle swarm optimisation (PSO). It is based on swarm intelligence, which was inspired by observing the activities of a flock of birds, namely their capacity to exploit and explore the search space for food. Particle swarm optimisation (PSO) is a straightforward algorithm. The variables adjust themselves after a number of iterations to the member whose value is closest to the solution. A pre-defined particle number, say NP, is used in the PSO method, which is known as a swarm. Every particle has the potential to solve a problem. In the d^{th} dimension of the search space, a particle P_i $1 \leq i \leq N_p$ has position X_i, d and velocity V_i, d, $1 \leq d \leq D$. For all particles, the dimension D is the same [76]. A fitness function assesses each particle to ensure that the solution is superior. Each particle maintains track of the dimensions in the issue space that are linked to the solution, which is its best fitness value so far.

3.7.1 Single link failure

Robinson and Rajaram [77] have suggested an energy-aware multipath routing strategy based on particle swarm optimisation (EMPSO) that solves optimisation problems using a continuous time recurrent neural network (CTRNN). To solve connect disjoint pathways in a MANET, CTRNN finds the best loop-free solution. The CTRNN is a path selection algorithm that generates a collection of optimal paths between source and destination. The (PSO) approach is primarily employed in CTRNN for recurrent neural network (RNN) training. To improve routing performance, the suggested approach uses reliability measures such as transmission cost, energy factor, and the best traffic ratio between source and destination. Using PSO to seek better connection quality nodes in the route discovery phase, optimal loop-free pathways can be found in this technique.

3.7.2 Single node failure

Manickavelu and Vaidyanathan's [78] MANET route recovery used a (PSO)-based node and link lifetime prediction technique. They pointed out that in traditional mobile ad hoc network (MANET) systems, route failure occurs in all route finding methods, resulting in data loss and communication overheads. As a result, routing must be done in accordance with the network's mobility. A (PSO)-based lifetime prediction technique for MANET route recovery

is proposed in this paper. Based on criteria such as relative node mobility and energy drain rate, this technique forecasts the lifetime of a link and node in the available bandwidth. The parameters have been obscured using predictions, and fuzzy rules have been developed to determine the node status. These data are designed to be shared among all nodes. As a result, before data transfer, the status of each node is confirmed. The performance of a route recovery mechanism is built in such a way that related routes are diverted to the strong nodes, even for a weak node.

3.7.3 Multiple links failure

Singh and Lobiyal [79] used the particle swarm optimisation (PSO) method to create energy-aware clusters with the best cluster head selection. In the end, the PSO lowers the cost of locating the best site for cluster head nodes. The PSO is implemented in the cluster rather than at the base station, making it a semi-distributed technique. The goal function's selection criteria are based on residual energy, minimal average distance from member nodes, and probable head node head count. In addition, the suggested energy model shows the impact of the predicted number of packet retransmissions. In this research work, swarm optimisation is used to discover the optimal cluster head (CH) position in order to reduce total energy use during packet transmission to the sink. Furthermore, the authors examine the impact of link failure probability on packet transmission and calculate the expected number of retransmissions along a sensor network path.

3.7.4 Multiple nodes failure

Currently, the range-free localisation algorithm is the most widely used node localisation approach, and it has achieved remarkable results. However, only a few methods are suitable for concave regions, and those that are available have flaws such as hop distance error, high time complexity, and so on. Meng et al., [80] present a two-stage PSO algorithm for wireless sensor node localisation in ‘concave regions’ to address these issues. Then they present a distance measurement approach based on comparable path search and intersection ratio in the first stage, which completes the initial localisation of unknown nodes using maximum likelihood estimate in the second stage. The modified PSO method is employed in the second stage to improve the original localisation findings from the first stage. The investigational results show that when the communication radius and beacon node ratio change, the algorithm's localisation error stays under 10% and the execution duration lasts about 20 seconds. As a result, the technique may achieve excellent localisation accuracy in wireless

sensor networks with ‘concave areas’ while consuming minimal computational resources and energy. As a result, sensor node service life can be considerably extended.

3.7.5 Multiple node-links failure

Abdel-Kader [81] has developed a new PSO-GA hybrid multicast routing algorithm that incorporates PSO and genetic operators and is customisable. The proposed hybrid technique combines the capabilities of PSO and GA to achieve a balance between natural selection and effective information sharing, resulting in a robust and fast solution space search. In the adjustable hybrid model, two driving parameters are used to maximise the performance of the PSO-GA hybrid by giving preference to either PSO or GA. The proposed approach includes a dynamic component that can handle dynamic scenarios originating from changes in multicast group membership or node-link failure without requiring the multicast tree to be reconstructed. The proposed hybrid method may overcome the drawbacks of particle swarm optimisation and genetic algorithms and produce improved QoS performance, according to simulation findings.

A mobile ad hoc network (MANET) is a dynamic network of mobile computers that operates without the need of any existing infrastructure. A MANET's nodes serve as hosts and routers. However, it is difficult to come up with reliable routing algorithms for MANETs. This challenge is addressed by disjoint multipath routing systems, which improve network stability, security, and longevity. Choosing the best multipath, on the other hand, is an NP-complete task. The Hopfield neural network (HNN) is offered as a multipath routing algorithm in this research work [82], with its parameters improved using the particle swarm optimisation (PSO) technique. The connection dependability estimation metric is the link expiration time (LET) between each two nodes. In single-phase route discovery, this method can locate either node-disjoint or link-disjoint paths. In terms of path set dependability and number of paths in the set, simulation findings show that the PSO-HNN routing algorithm outperforms the backup path set selection algorithm (BPSA).

3.8 AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

3.8.1 Single link failure

Kumar and Negi [83] offer a Backward AODV (B-AODV) for addressing single link failures that tries multiple route replies. (B-AODV), differs from other on-demand routing protocols

for Ad-hoc Networks in that it lowers path fail correction messages and achieves greater performance than AODV and other protocols. In terms of packet delivery ratio, power consumption, and communication delay, backward AODV performs well. Mobile devices roam independently in mobile ad hoc networks to make use of wireless connectivity and continuously changing network topology. The AODV is one of the most extensively researched on-demand ad-hoc routing systems. Most on-demand ad-hoc routing protocols, including AODV, use a single route reply along the reverse path. The route reply could not reach the source node due to a rapid change in topology, i.e., after a source node sends numerous route request messages, the node receives a reply message, especially on high-speed mobility.

3.8.2 Single node failure

Tong et al., [84] proposes an enhanced ad-hoc on-demand distance vector (AODV) routing protocol based on node-grade in wireless sensor networks to reduce node energy consumption. Grade-AODV (G-AODV) is an upgraded AODV that awards a grade to each node based on the hop distance between the node and the sink node. The closer a node is to the sink, the lower its grade. Each node is only allowed to accept route request (RREQ) packets from nodes with a higher grade than it. As a result, the proposed G-AODV can reduce node energy consumption in two ways: (i) unnecessary RREQ broadcast can be avoided, and (ii) each packet requires fewer network resources since route pathways with shorter hop distances are established.

3.8.3 Multiple links failure

Using a network-simulator 2, Azzuhri et al. paper [85] describes a parameterized approach to the ad-hoc on-demand distance vector (AODV) routing protocol. A flexible method was investigated on these two crucial roles by leveraging two AODV protocol functionalities, namely HELLO messages and local route repair, rather than a fixed option inside the default AODV protocol. In the event of a route failure, the HELLO message is used to detect broken links, while the local route repair in AODV is used to mend and discover alternate routes. Two functions were used to optimise AODV performance in this study. The first is the time it takes to identify a connection break using the HELLO message, and the second is the link break location parameter for AODV's local route repair.

3.8.4 Multiple nodes failure

A mobile ad-hoc network (MANET) is a peer-to-peer wireless network in which nodes connect without the use of infrastructure. Furthermore, nodes are free to join and leave the network at any moment, to migrate at random, and to organise themselves in any way they see fit. Owing to the nature of MANET, hostile and selfish nodes may attempt to compromise routing protocol functionality, making MANET vulnerable to security attacks and resulting in faulty routing. The authors Jassim et al., [86] offer R-AODV, an ad-hoc on-demand distance vector routing system based on trusted and shortest paths, and compare it to the AODV trust framework, which has already been used to solve the problem.

3.8.5 Multiple node-links failure

A search through the twelve journals database list in section 3.12; also discovered that multiple node-links failure research is not yet common in the AODV optimisation technique.

3.9 TEMPORALLY ORDERED ROUTING ALGORITHM (TORA)

The Temporally Ordered Routing Algorithm (TORA) is a distributed routing protocol that uses a set of link reversal algorithms to route traffic. The TORA can provide numerous loop-free routes to every destination using route design, maintenance, and erasure procedures. The TORA works effectively in networks with few traffic connections, but not so well in networks with many connections. Traffic congestion has resulted from excessive route maintenance, which in turn, has contributed to poor performance [87]. Traffic congestion is exacerbated by the routing overhead generated by the large number of traffic connections. The network localisation method establishes and maintains a localised network component, whereas the selective node participation strategy invites just a subset of nodes to join. When compared to the original TORA, the TORA upgrades result in an overall performance improvement in terms of packet delivery, routing overhead, and packet latency.

3.9.1 Single link failure

Ad-hoc networks' admitted poor quality of service suffers from frequent path breaks that necessitate network re-establishment across new paths due to its dynamically fluctuating network architecture. Ad-hoc networks are thus unsuitable for real-time interactive sessions, such as video or voice calls. The TORA is a multipath routing protocol for multi-hop

networks that is distributed, loop-free, and allows both source and destination-initiated routing. Hilal, et al., [88] have presented a token-based queue for TORA, dubbed RT-TORA, to provide better QoS guarantees for real-time link restoration in interactive applications. The RT-TORA routing algorithm outperforms the original TORA method in terms of average packet latency and delivery ratio, especially for networks with a large number of connections.

3.9.2 Single node failure

Lin, et al., [89] proposes an adaptive repair algorithm for TORA routing protocol based on flood control strategy (AR-TORA-FCS) to address TORA's weaknesses in routing maintenance, such as high overhead and delay, and to make the routing more suited for emergency and disaster relief networks. To begin, the self-repair process of the self-repair nodes in the directed acyclic graph (DAG) of TORA is turned into the optimal search issue for the optimal nodes, and the formula is constructed, based on the features of the uniform deployment of the nodes in the network. It is proven that the search result is the ideal solution of the process of searching for the optimal node using the Ray-Algorithm to search for the optimal node. The conditional threshold for initiating the self-repair process is then developed, as well as a conditional method for determining the self-repair process. The path repair is carried out before the path fails, and the mapping relationship between the repair process of self-repair nodes and the distance between the nodes is formed.

3.9.3 Multiple links failure

Vadivel and Bhaskaran [90] present a MANETs connections failure restoration with various techniques such as TORA, whereby packet loss can be caused by either link or node failure. Furthermore, bypass route selection strategies and bypass route congestion avoidance approaches are rarely addressed. To address these issues, these authors present an adaptive reliable and congestion-control routing protocol for MANETs that uses bypass route selection to resolve congestion and route faults. Numerous routes are built, and the shortest pathways are found among these for effective data transmission. Congestion is detected on the basis of connection, path utilization and capacity. When a source node detects congestion on a link along the path, it divides traffic over alternate paths using a traffic splitting function and the path availability threshold. If a node is unable to resolve the congestion, it uses the congestion indicator bit to notify its neighbours.

3.9.4 Multiple nodes failure

It is observed that TORA publications for resolving multiple nodes failure are not found. Most publications found on the article database did not solve multiple nodes failure.

3.9.5 Multiple node-links failure

After searching the journal's database, it was observed that no relevant publications on multiple node-links failure could be found.

3.10 ADAPTIVE DISJOINT PATH VECTOR (ADPV)

The Adaptive Disjoint Path Vector (ADPV) method is used in wireless networks. ADPV has resource-dense super-nodes as well as conventional sensor nodes that connect to the super-nodes. Unlike the static disjoint path vector (DPV) method, ADPV's main goal is to enable super-node connectivity in the event of node failures, which it achieves by dynamically changing the transmission intensities of sensor nodes [86]. The ADPV approach has two stages: a single initiatory phase at the start and restoration phases when the network's super-node connectivity is lost. During the initiation phase, a unique optimisation is employed to compute alternative routes based on the well-known set-packing problem, which are then used during the restoration phase. Extensive simulations have demonstrated ADPV's superiority in retaining super-node connectivity. This target is met by ADPV up to a sensor node failure rate of 95%.

3.10.1 Single link failure

Following a search of the journal's database, no relevant publications on single link failure were discovered.

3.10.2 Single node failure

In wireless networks, Wang et al., [30] have proposed an adaptive connectivity restoration from node failure. Nodes may fail as a result of the severe deployment circumstances and inadequate energy supply, affecting the network's connectivity. Since a single node failure (cut-vertex) destroys connectivity and divides a network into separate parts, the majority of present research focuses on this issue. Multiple node failure, on the other hand, would be disastrous for the entire network and would require prompt repair. Only a few researches

have been offered to deal with multiple cut-vertex failures, which are a subset of multiple node failures. As a result, this paper presents a comprehensive solution to the issue of node failure (single and multiple). The collaborative single node failure restoration algorithm (CSFR) is proposed to tackle the problem of single node failure using only cooperative communication; however, CSFR-M, which is an extension of CSFR, handles the single node failure problem more successfully by incorporating node motion.

3.10.3 Multiple links failure

There is no published information about how ADPV resolves or optimises multiple link failure in wireless networks.

3.10.4 Multiple nodes failure

Deniz et al., [91] have presented the adaptive disjoint path vector (ADPV) algorithm, which is an adaptive, energy-aware, and distributed fault resistant topology control solution for WSNs that are complex. There are resource-rich super-nodes as well as conventional sensor nodes that are expected to be connected to the super-nodes in this heterogeneous model. Unlike the static disjoint path vector (DPV) algorithm, ADPV's primary purpose is to provide super-node connectivity in the event of node failures, which it accomplishes by dynamically altering the sensor nodes' transmission strengths. The ADPV method comprises two stages: a single initial phase at the start and restoration phases that are triggered whenever the network's super-node connectivity is lost. During the initial phase, a unique optimisation based on the well-known set packing issue is used to compute alternative routes, which are then used during the restoration phase.

3.10.5 Multiple node-links failure

No papers were found on ADPV that addressed the failure of multiple node-links.

3.11 WIRELESS NETWORKS OPTIMISATION ANALYSIS AND RESULTS

A total of 320 journal publications were classified using a wireless network optimisation routing approach. The papers were judged solely on their publication year, the best routing technique used to publish them, and the frequency with which they appeared in specific journals.

3.12 TREND OF THE PUBLICATION YEAR

Rather than conference proceedings papers, the majority of this review is focused on journal articles. Only about 5% of the total material used was based on conference papers. Journals are commonly used by researchers and academics to share fresh knowledge and findings on wireless network optimisation tactics with the research community, hence they were picked for their high-quality content. A review of journal articles published between 2010 and 2020 was carried out. Journal papers were selected for their applicability to wireless network optimisation. Despite the fact that the method was subjective owing to the fact that studies published in non-English language research channels were eliminated due to language barriers, the literature review discovered publications in 12 internationally respected journals. The literature review laid the groundwork for understanding wireless network optimisation routing strategies, which will lead to the development of wireless network optimisation routing frameworks. Since there were few works on optimisation prior to 2010, 2010 was selected as the initial point for the study publishing. Since 2010, the number of articles on all aspects of optimisation routing approaches has increased significantly (see Figure 3.2). The following journals were selected for their importance to wireless network optimisation and routing:

(i) IEEE/ACM Transactions on Networking
(ii) IEEE Transactions on Evolutionary Computing
(iii) International Journal of Mobile Networks Design Innovation
(iv) Computer Networks
(v) Sensors
(vi) International Journal of Distributed Sensor Networks
(vii) Ad Hoc Networks
(viii) Journal of Computer Networks and Communications
(ix) Procedia Computer Science
(x) International Journal of Computational Intelligence Systems
(xi) Swarm and Evolutionary Computation
(xii) Journal on Wireless Communications and Networking

Figure 3.2 depicts the papers on optimisation routing algorithms spread on a yearly basis from 2010 through 2020; indicating an annual growth in wireless networks. It is observed that there is growth in the number of articles published on optimisation routing techniques

from 2010 to 2014. However, work-done in the field of optimisation routing technique appeared to drop in 2015s. There is exponential increase in the optimisation routing technique articles published between 2015 and 2019. The drop in number of publications in 2020 is attributed to the fact that some journals have not fully published their articles in the area of optimisation techniques as at the time of review.

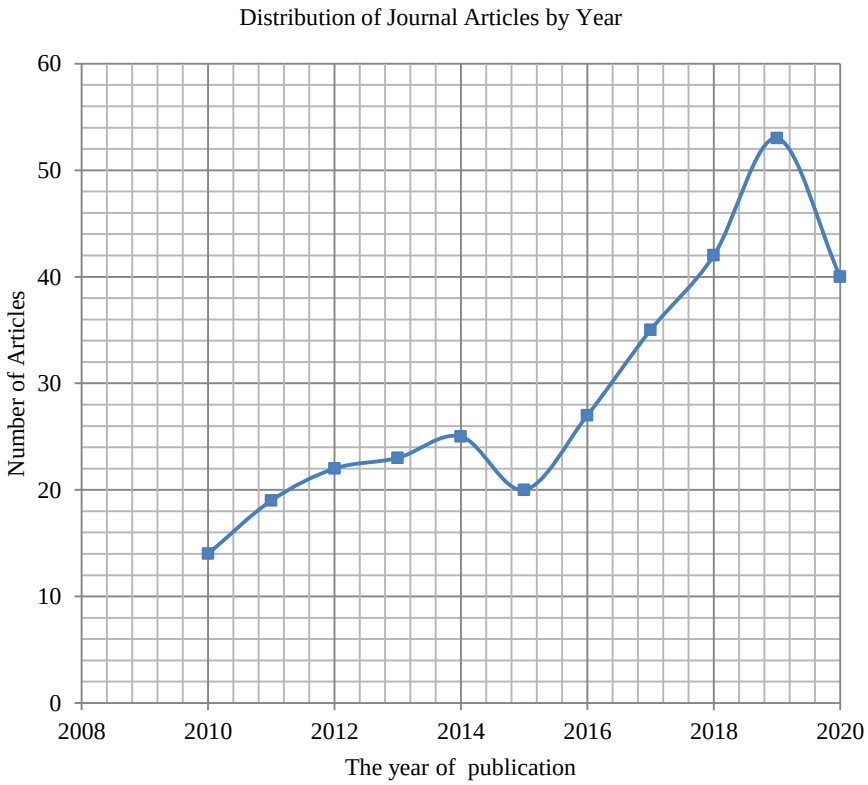

Figure 3.2: Distribution of papers per year

3.13 TOTAL PAPER TREND IN SELECTED JOURNALS

The number of wireless network papers published by journal is shown in Figure 3.3. With 11.2% of papers published in the *IEEE/ACM Transactions on Networking*, optimization routing strategies are the most popular. Most of its publications are based on network failures that have to do with sensor networks and MANETs. *Computer networks* has the second highest number of publications in the area of optimisation routing techniques. *The International Journal of Distributed Sensor Networks and Procedia Computer Science* have the third highest number of publications with 9.3%. Ad-hoc Networks take fourth position and most publications on failure restoration use many different methods. The *Journal of Wireless Communications and Networking, IEEE Transactions on Evolutionary Computing, Sensors and the Journal of Computer Networks and Communications* also published in the

area of optimisation routing technique. *The International Journal of Mobile Networks Design Innovation* has the least publication with 5.6%.

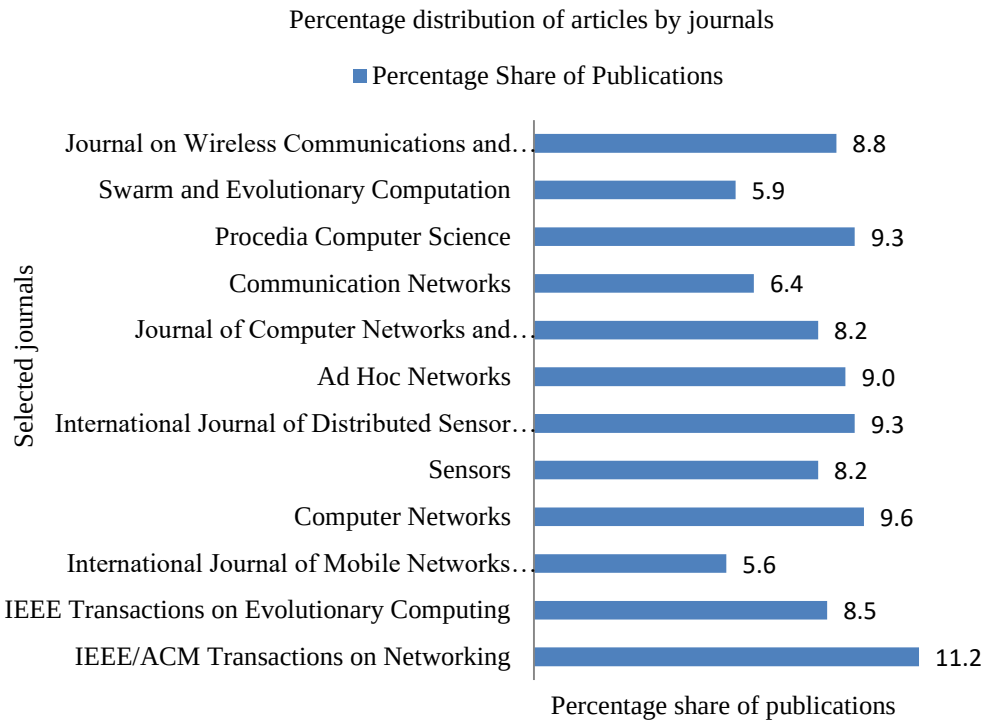

Figure 3.3: Journal trends in optimisation routing articles.

3.14 TREND OF OPTIMISATION ROUTING METHODS BY TOPICS

Figure 3.4 depicts the frequency of articles on optimisation routing algorithms from 2010 to 2020. The most popular topic was ant colony optimisation, which received 98 papers (24.9%), followed by particle swarm optimisation, which received 96 papers (24.4%), and ADPV optimisation technique is the least which received 19 papers.

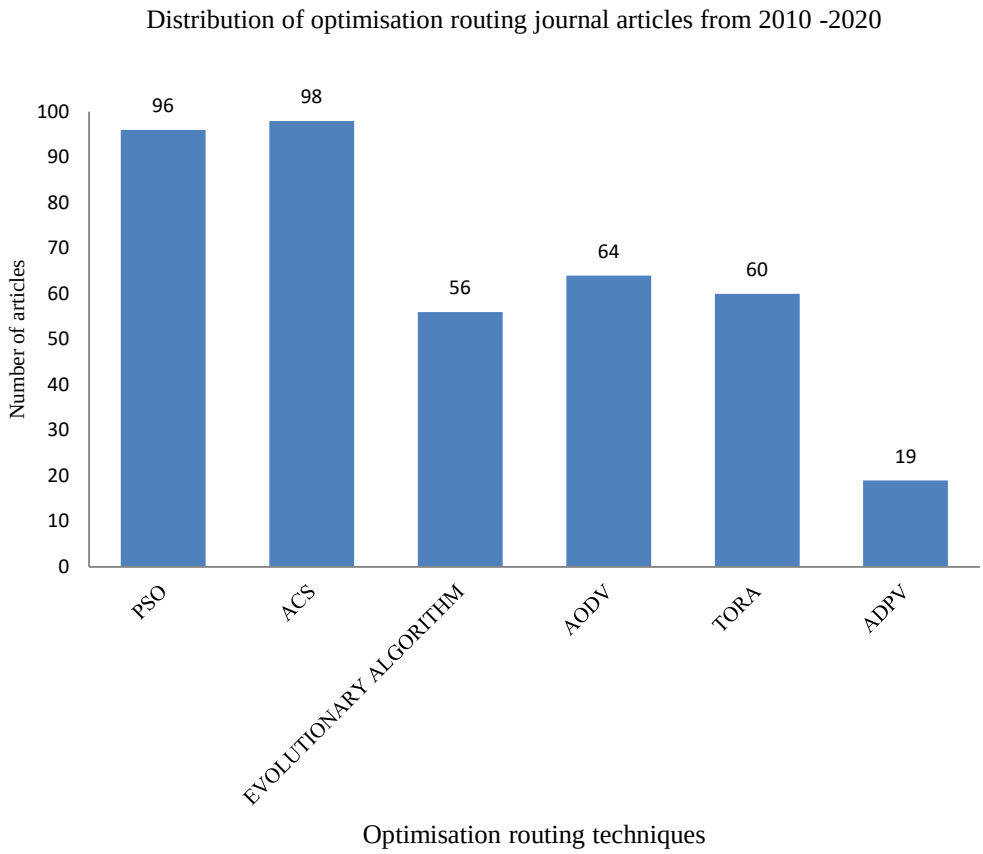

Figure 3.4: Trend of optimisation routing technique papers by topic.

3.15 SUB-TOPICAL TRENDS IN OPTIMISATION ROUTING TECHNIQUES

Figure 3.5 depicts the percentage of articles in the six categories of ACS optimisation routing strategy subjects. The majority of publications in the ACS optimisation category focused on single node failure (27%) followed by multiple node failure (22%), and single link failure (20%). Multiple node-links failure was the least popular subject, accounting for 13% of the total.

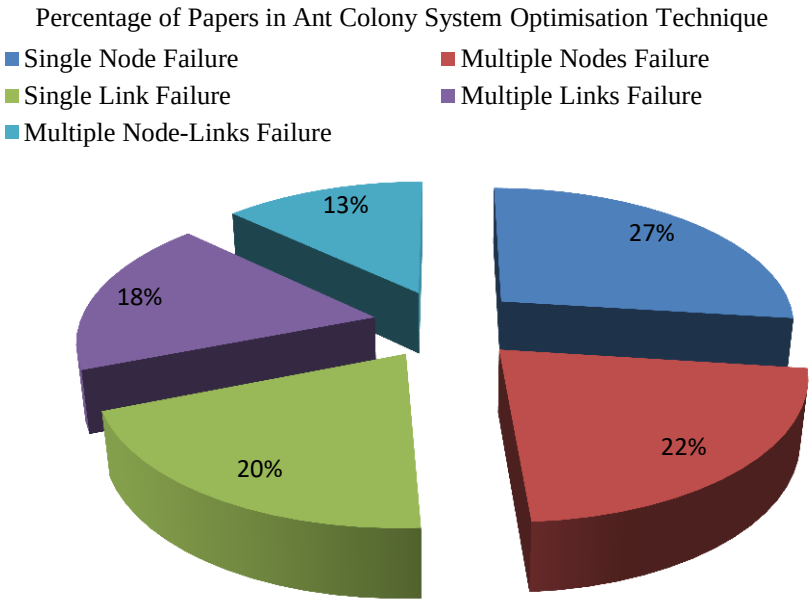

Figure 3.5: Percentage of ACS optimisation routing technique papers

Figure 3.6 depicts the percentage of articles in the six categories of evolutionary algorithm optimisation technique. Most papers in the evolutionary algorithm optimisation category focused on single node failure (25%) and multiple node failure (23%) of all publications. Multiple node-links failure was the least popular topic, accounting for 11% of the total strategies.

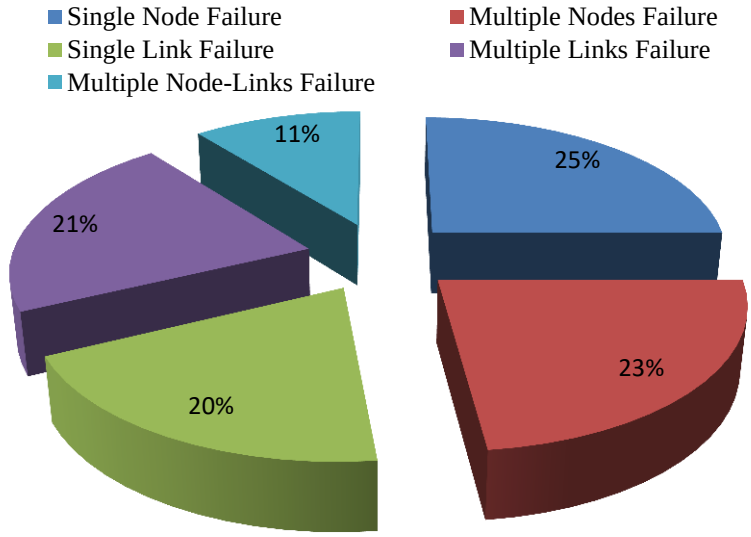

Figure 3.6: Percentage of evolutionary Algorithm optimisation routing technique papers

Figure 3.7 depicts the percentage of articles in the PSO optimisation strategy themes, which are divided into six categories. Single node failure accounted for 38% of PSO's total publication, while single link failure accounted for 21%. Multiple node-links failure was the least popular subject, accounting for 7% of the total.

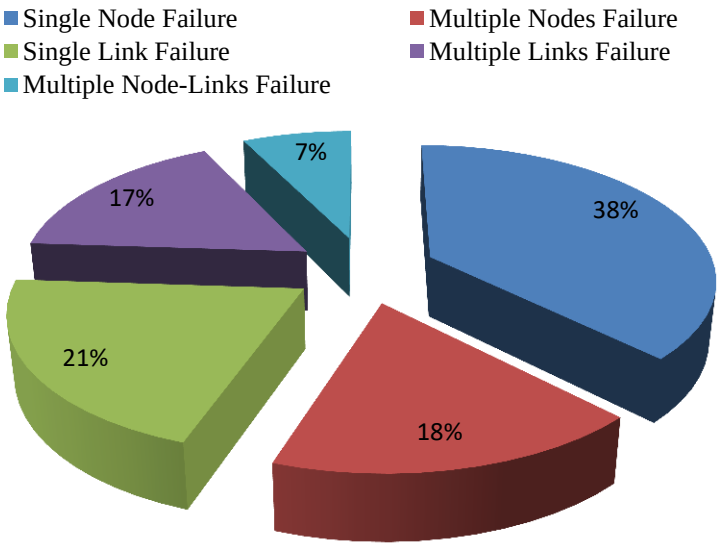

Figure 3.7: Percentage of PSO routing technique papers

Figure 3.8 depicts the percentage of articles in each of the six categories of AODV optimisation technique subjects. Single link failure accounted for 37% of AODV's publication, while multiple link failure accounted for 30%. The optimisation technique also addresses the failure of single and multiple nodes. There was limited number of articles on multiple nodes failure (14%). There were no articles on multiple node-links failure.

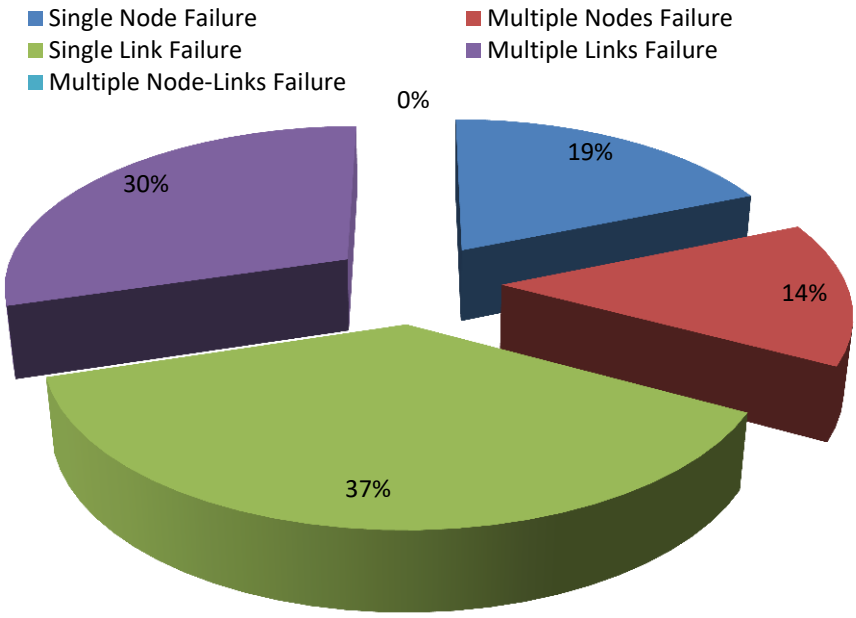

Figure 3.8: Percentage of AODV routing technique papers

Figure 3.9 depicts the percentage of publications in the TORA optimisation technique themes, which are divided into six categories. The TORA concentrated on single link failure, which accounted for 40% of the total, and multiple link failure, which accounted for 30%.

There were no papers on the failure of multiple nodes and multiple node-links. Other explanations can be found in Figure 3.9.

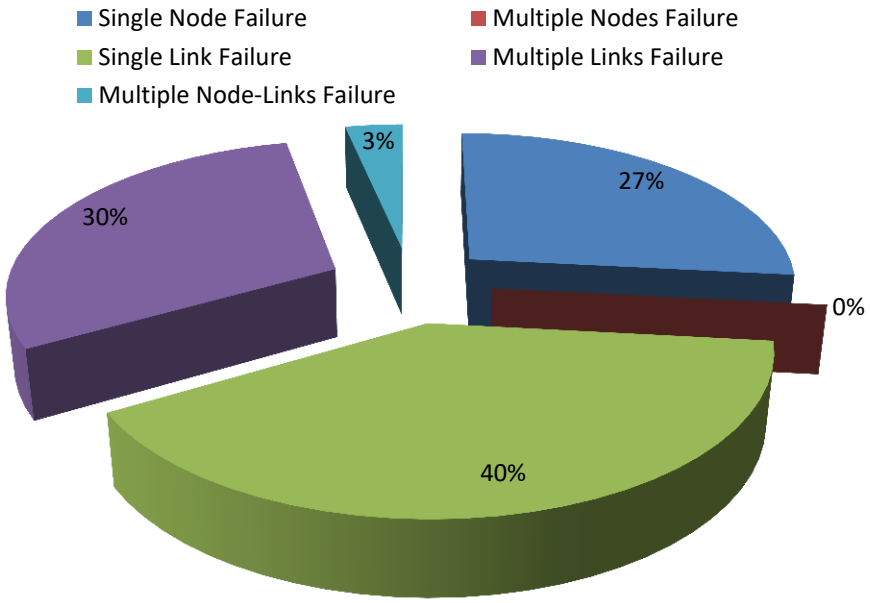

Figure 3.9: Percentage of TORA routing technique papers.

Figure 3.10 depicts the percentage of publications in the ADPV optimisation method themes, which were divided into six categories. The ADPV concentrated on single node failure, which accounted for 60% of articles, and multiple node failure, which accounted for 40%. There were no articles on link failures of any kind, whether single link, multiple links or multiple node-links.

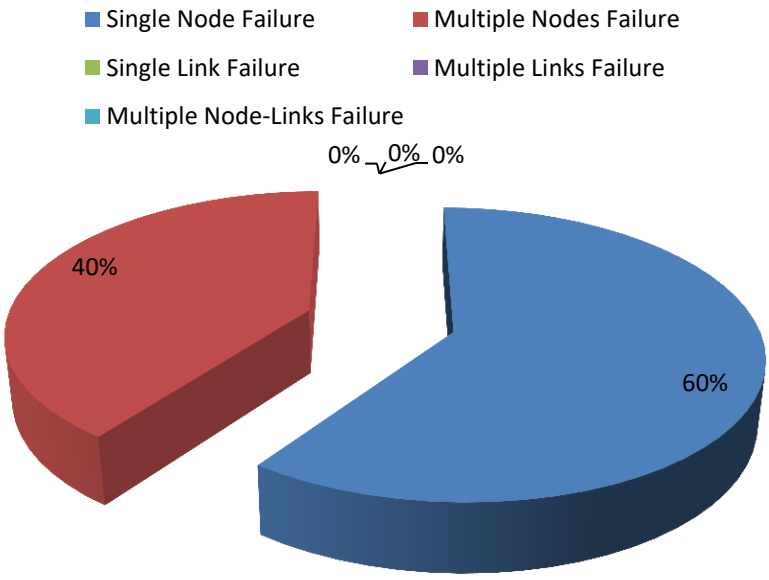

Figure 3.10: Percentage of ADPV routing technique papers.

3.16 METRICS FOR EVALUATING PERFORMANCE

Throughput, transmission delay, transmission time, packet delay rate, complexity, packet drop, and capacity are all measures used to evaluate the performance of a wireless network. These parameters influence the network's effectiveness and efficiency. When measuring performance metrics, keep the following in mind:

- The number of units of digital data that a system can handle in a given amount of time is referred to as throughput [92]. It is applicable to a variety of systems, including network systems.
- The time it takes the physical layer at the source to transfer packets over the link is known as transmission delay. This delay is caused by a number of variables, including the following: The number of active sessions, the link's transmission capacity, the MAC access delay, and the OS's context switch
- Transmission Time: this is the time it takes for a packet to go from sender to the receiver.
- Packet Delay Rate: the delay induced by the link's data rate.
- Complexity: is the time it would take for an algorithm to execute as a function of the length of the input. It calculates the time it takes for each expression of code in an algorithm to run.
- Packet Drop: Some packets are lost by routers due to congestion. Previously, this was done at random, resulting in inefficient multimedia traffic performance.
- Bandwidth Usage: Bandwidth refers to a network's ability to move data between devices or over the internet in a given amount of time. Data can be sent at a faster rate with more bandwidth.

An analysis of the most commonly used performance measures for evaluating the performance of a wireless network using the journals database from 2010 to 2020.

Figure 3.11 depicts some of the metrics used to assess wireless network performance. Bandwidth usage, packet drop, time complexity, throughput, packet delay rate, transmission time, and transmission delay are some of the metrics. Bandwidth use and throughput are the most commonly used metrics in wireless network evaluation, followed by packet delay rate. In most circumstances, transmission delay is also used. When evaluating the performance of wireless networks, complexity accounts for the smallest percentage.

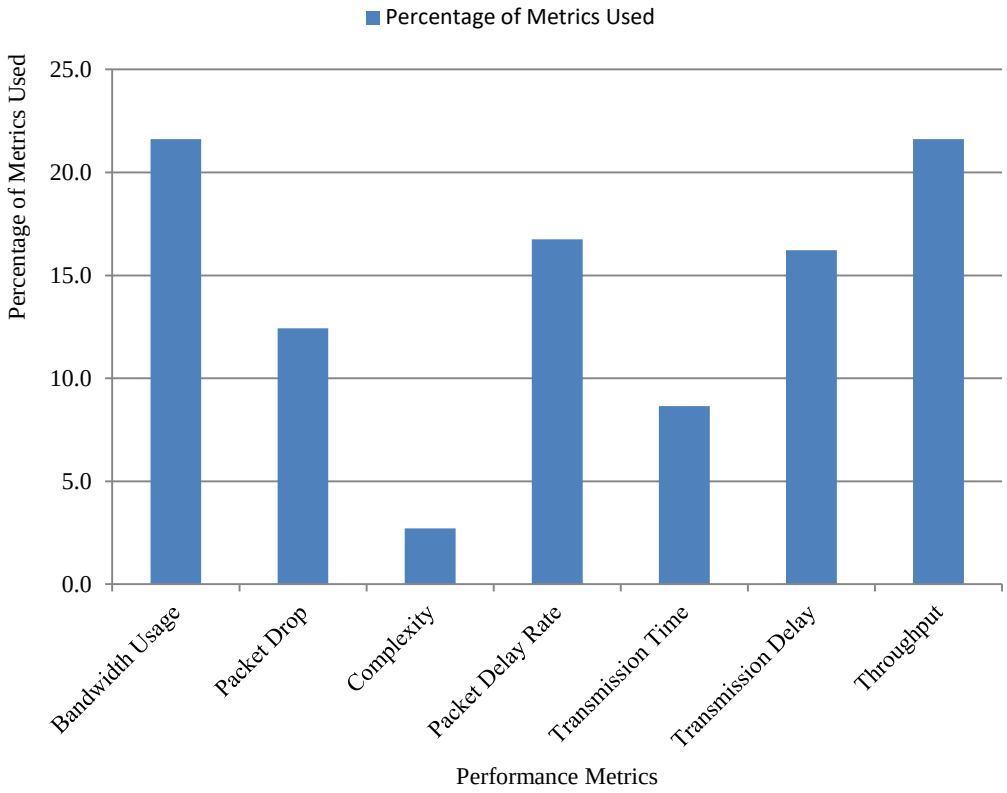

Figure 3.11: Wireless network performance evaluation metrics

The evaluation and validation parameters depicted in Figure 3.11 are used to assess and validate sub-objectives 2, 3, and 4 defined in chapter one. Since the parameters were only mentioned and explained in sub objective 5, which was stated in subsection 3.16.

3.17 RESEARCH GAPS COVERED

The findings of 11 years of research on optimisation routing algorithms have a lot of ramifications for future researchers. Between 2012 and 2020, there are about 20 or more publications in wireless network research (see Figure 3.2); and there are about 20 or more articles per year. However, with only a few articles accessible, the absorption of ADPV has not been properly examined (see Figure 3.4). Figure 3.1 depicts the seven wireless network themes that authors of wireless network routing protocols must consider when evaluating new wireless network routing protocols, as well as the optimisation routing strategies applicable to wireless networks. To indicate the research gaps in view of the literature analysis, the findings in Figures 3.5 to 3.10 indicate that wireless network optimisation routing protocols are required to address the following:

- Sub-topic of ACS routing strategies especially multiple node-links failure.

- Sub-topic of Evolutionary Algorithm routing strategies especially multiple node-links failure.
- Sub-topics of PSO routing strategies especially (a) multiple links failure and (b) multiple node-links failure.
- Sub-topics of AODV routing strategies especially (a) multiple nodes and (b) multiple node-links failure.
- Sub-topics of TORA routing strategies especially (a) multiple nodes and (b) multiple node-links failure.
- Sub-topics of ADPV routing strategies especially (a) single link (b) multiple links and (c) multiple node-links failure.
- In testing the performance of optimisation routing strategies, time complexity is rarely used, this can be seen in Figure 3.11. Throughput and bandwidth usage take larger percentage.
- The remaining gaps and their supporting research questions are stated in section 6.6 for future researchers.

3.18 CHAPTER SUMMARY

The purpose of this research is to examine various survivability solutions to failures in wireless networks in order to discover gaps that future wireless researchers may use as a starting point for their research. The failures of a single link, a single node, multiple links, multiple nodes, and multiple node-links were discovered and divided into sub-themes. The sub-themes were used to construct a wireless network routing system.

In Figures 3.4-3.10, it can be seen that ADPV and TORA optimisation techniques addressing failures have received little attention in the literature. Multiple node failures and failures of multiple nodes to link have also received little attention and should be investigated, particularly with potential ADPV techniques. Future studies could look at designing resilient, efficient, and accessible routing protocols that take into account all quality-of-service criteria. It is expected that this study will encourage wireless network designers and academics to investigate the proposed research questions in section 1.4 and other survivability approaches that consider message, voice and video transmissions.

CHAPTER 4: RESEARCH DESIGN AND METHODOLOGY (Capacity Efficient Evolutionary Swarm Survivability Framework)

4.1 INTRODUCTION

Survivability is commonly defined as a network's ability to deliver data successfully and on time even when there are system outages. Network survival is essential for providing network users with a continuous, seamless connection while preserving quality of service. Survivability is a network property, but it is only realised in conjunction with a data transfer session. A survivability approach essentially focused on a particular type of failure [26]. The most common types of failures are failure of nodes, links, and provider's nodes. It should be noted that the focus of this research is on survivability designs that improve the continued existence of wireless networks. Existing wireless network survivability models have been used to construct resilient networks, they do, however, have flaws which must be resolved. Section 2.3.2 discusses some of the existing wireless network survivability flaws.

This chapter proposes capacity-efficient EGA and ACS models for wireless network survival. As explained in section 1.3, the objective of the study is to create a survivable wireless network framework that will optimise the continued existence of traffic flows in wireless networks that are vulnerable to multiple failures and attacks. The sub-objectives listed in section 1.3 help to support the primary goal. The goal of this research is to go over the approach used to accomplish the targeted study goals as well as the research questions. In order to achieve specific research goals, a number of different approaches were used in this study.

4.1.1 Research philosophy and design

The set of beliefs concerning the nature of the reality being investigated is referred to as research philosophy, and the type of research philosophy used in a research study is determined by the knowledge being investigated [93].This investigation employs an experimental research design.

This research experimental philosophy, in particular, brings together two key elements:

- the types of questions and theoretical frameworks associated with philosophy in this research work;

- the kinds of experimental methods traditionally associated with psychology and cognitive science.

This study makes use of experimental data to back up positive claims about traditional questions, while others investigate how people normally think and feel as far as these questions are important.

4.1.2 Proposed capacity efficient evolutionary swarm survivability framework

Figure 4.1 depicts the proposed capacity efficient evolutionary swarm survivability framework as a method for constructing a wireless survivability network. The framework represents the EGA and ACS techniques' subsystems. This framework is used in the following investigations 1, 2, 3, and 4 in Chapter 5. Two models are used in the framework: capacity efficient EGA and capacity efficient ACS. Both of them generate alternative paths, and the best path is chosen for message rerouting with the calculated bandwidth. In both models, the one with the shortest path cost is selected as the rerouting path because rerouting is both faster and less expensive.

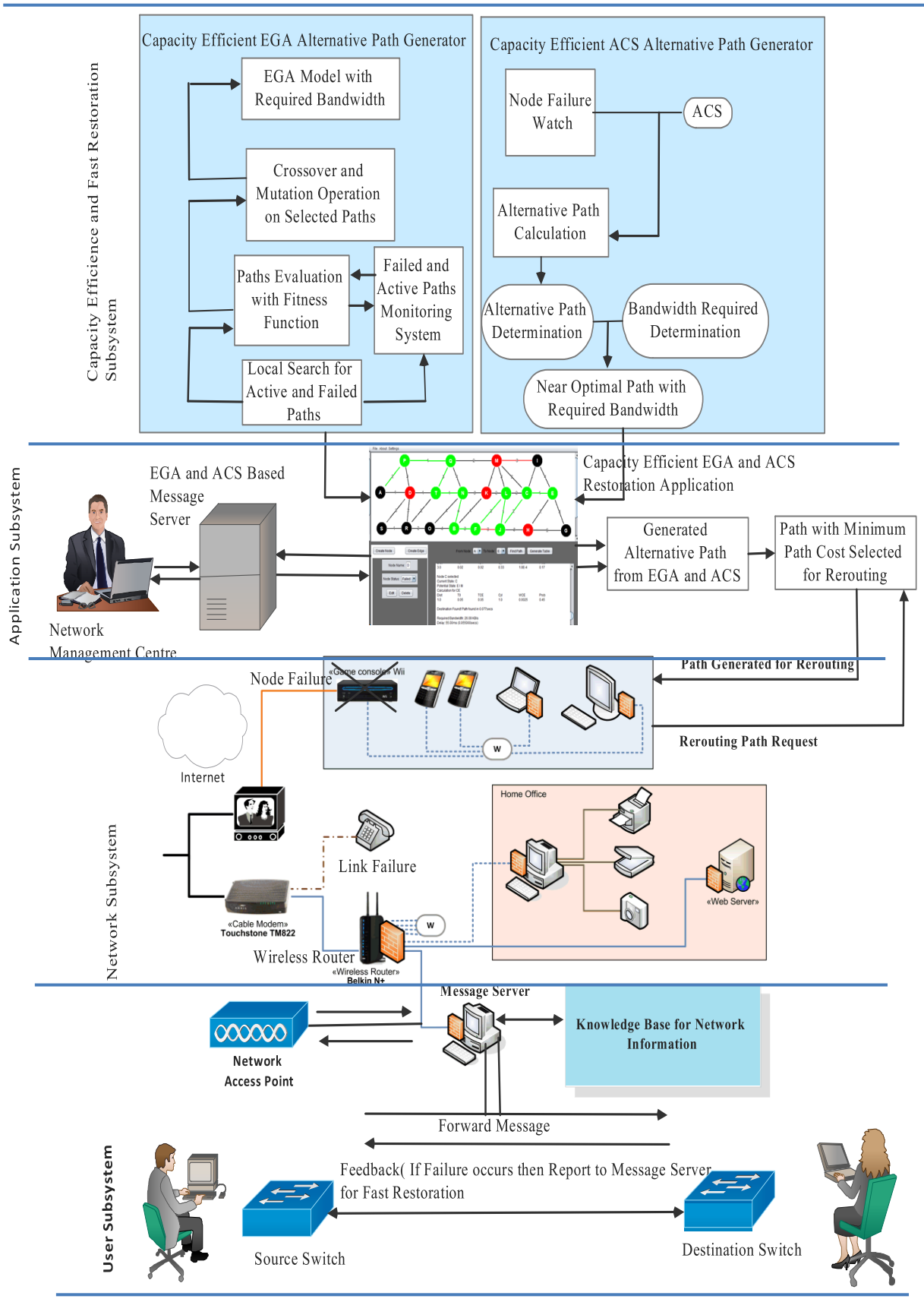

Figure 4.1: Capacity efficient evolutionary swarm framework for surviving network failures

Figure 4.1 depicts various subsystems designed to accomplish a resilient system, including the user layer, application layer, network layer, capacity efficient, and fast restoration layer. These are described as follows:

- **The subsystem layer of user**

This user subsystem layer, as depicted in Figure 4.1, was created to serve as a front end for network users to gain access to the network during network maintenance. In the event of a network failure, the subsystem is linked to both the capacity-efficient EGA and ACS models, allowing for effective network restoration. Because the user interface cannot be directly linked to the system backend, it is linked directly to the access point to avoid unauthorised access to system information and to prevent attackers from gaining access to the system.

- **The subsystem layer of application**

The subsystem layer is included to enable network configuration. In this scenario, the network's capacity efficient EGA and ACS restoration modules are installed to ensure the system provides alternate paths in the event of a network failure. The system resolves node-node, link-link, and node-link failures because the model combines capacity efficient EGA and ACS as shown in Figure 4.1. Message rerouting is made as simple as possible because an alternate path is generated in real time. The subsystem was created to synchronise the proposed capacity efficient EGA and ACS model’s software product in conjunction with the wireless communication, allowing for a simple transition from a failed path to an alternate path. Since this module is directly linked to the network subsystem, recovery is a breeze. In addition, because this subsystem is directly linked to the network backend, the application subsystem can run on top of the network operating system.

- **The subsystem layer of the network**

For the users' remote communication with the system, the network subsystem is directly connected to the wireless router, which is linked to the network access point (see Figure 4.1). The message server is directly linked to the access point that the user subsystem uses to connect their module. A wireless network subsystem could be an IoT network, an ATM network, or any other type of wireless network. The network used in this framework is connected with various wireless network devices to communicate from different paths of the system. The configuration adheres to ITU standards, with the wireless network protocol and

the capacity efficient EGA and ACS algorithms collaborating to minimise network outages by producing an alternate route for network rerouting.

- **The subsystem layer of capacity efficiency and fast restoration**

When a network failure occurs, this subsystem reroutes messages using two survivability models. Since transmission efficiency is required, the alternative path is computed using both the capacity efficient EGA and ACS optimising systems to produce the best alternative path. By capacity efficiency, to determine the bandwidth needed to convey a packet, a heuristic is incorporated on the network; namely, a voice message, video message, or multimedia message. The capacity-efficient EGA and ACS find a relatively close alternate route that avoids duplication and resource waste and allowing for rapid restoration. In order to resolve any type of path failure in a wireless network, this layer combines the best features of capacity efficient EGA and ACS to generate path with minimal path cost (Figure 4.1 displays the illustrations).

The capacity efficiency and fast restoration subsystem communicates alternate paths to both the network and the application subsystem because it contains the algorithms that generate alternate paths that must be sent to the application subsystem (wireless network monitoring system). When the application subsystem detects a failure, it sends an alternate path request to the network subsystem, allowing transmission to continue.

4.2 DEVELOPMENT OF THE SURVIVABILITY MODEL FOR CAPACITY EFFICIENT EGA

Figure 4.2 shows capacity efficient EGA sub-framework for wireless network survivability.

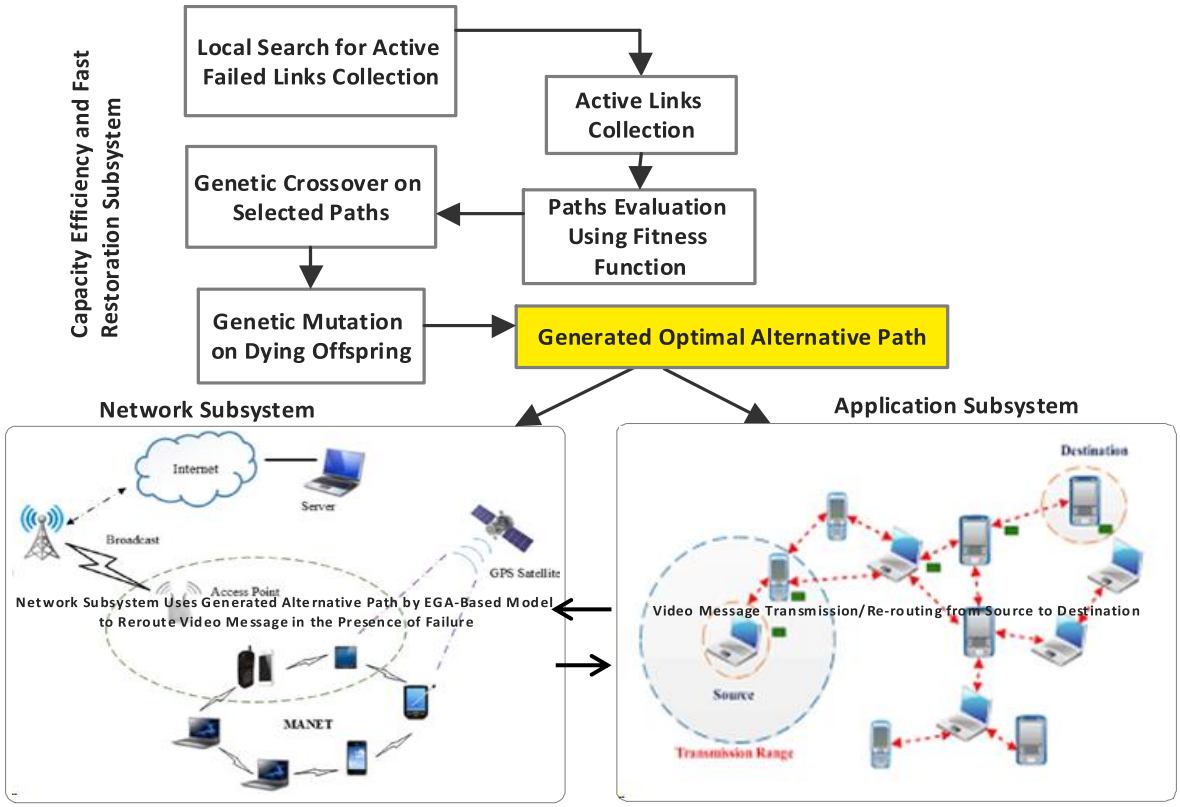

Figure 4.2: Framework for surviving multiple link–link failures.

4.2.1 Problem formulation for capacity efficient EGA model

The term ‘wireless network survivability’ refers to an examination of the usability, efficiency, and effectiveness of a physical network's topology. It is also a system's ability to provide services on an ongoing basis in the event of failure or other undesirable incidents, in accordance with the criteria established [94]. The network survivability models addressed in this research work take into account networks that are subject to certain adverse effects that can cause a transmission path failure, which is usually accompanied by an unexpected network variations services infrastructure, for example the bandwidth needed for transmission in the prevalence of failures that induce communication delays. When pairing links with relevant performance assurances fail in this model, like needed bandwidth with minimal resistance, it is critical to provide rerouting paths and maintain an absolutely great use of network resources. The proposed model incorporates sufficient diversity and spare capacity to tolerate capacity loss and enable systems to be restored at the demanded level of service. The assigned network is defined by G = (N, E), where N is the set of vertices, i.e., the

sum of terminals in the network, such as dedicated wireless network servers, and E is the series of links, or edge connections, that occur among hubs which can interact with one another, which are sometimes referred to simply by the network. Wireless links, radio signals, and optical fiber links, for example, could be used.

4.2.2 Capacity efficient EGA's objective function

Rerouting a packet on an attacked wireless system with minimal spare capacity is a major problem in the developing world, particularly in Africa. When a failure occurs as a result of a fraudulent attack, the packet must be rerouted immediately. Alternative paths with reduced latency must be provided, along with transmission constraints such as required bandwidth (B_{req}) to convey packet and to obtain the shortest path with minimum path cost (P_c) to achieve quick rerouting. As a result, in the event of a failure caused by an attack that poses a risk to economy all over the globe, the main trust of this work is to find an optimal alternative path to reroute a packet. Wireless network failure is caused by fraudulent attacks, errors in setup, power outages and wildfire outbreaks. In the event of a failure, this researcher proposes a capacity efficient EGA and ACS system which could be used to find the best alternative route for redirecting packets as fast as possible. The capacity efficient EGA model solves the optimisation problem. The solution could be either the simplest or the most complex. Both conditions are optimization issues. An optimisation problem has three components: judgment (decision) variables, a goal function, and limitations.

- **Judgment variables**: They are the parameters that could be controlled inside a model. Since there are n judgment parameters, they are denoted by the letters y_1, y_2,...., y_n..
- **Goal function**: This really is the challenge that is needed to improve or minimise. An optimal solution is denoted by the notation f (y_1, y_2,..., y_n). However, if the purpose is to optimise the performance of this activity, the notation could be written as $\max_{y_1,y_2,\dots,y_n} f(y_1, y_2, \dots, y_n)$ and, if the task should be mitigated, it is expressed as $\min_{y_1,y_2,\dots,y_n} f(y_1, y_2, \dots, y_n)$
- **Limitations**: These are assignment problems or limitations. The following are the mathematical tools::

  $k_1(y_1, y_2, \dots) \leq 0, \qquad k_2(y_1, y_2, \dots) \leq 0, \qquad k_3(y_1, y_2, \dots) \leq 0$

4.2.3 Mathematical justification for capacity efficient EGA model

If a wireless network link fails due to a fraudulent attack while a message is being transmitted from a transmitter mobile station to another (a recipient mobile station), to accomplish fast rerouting, the best path (P) to reroute the message from source to destination must be produced with the least amount of network delay. This means that the optimal rerouting path (P) is determined by the following constraints:

- Owing to the occurrence of link failures as a result of attacks, there is a limited bandwidth (B_{req} Kbytes/s). As a result, the required bandwidth (B_{req}) to reroute the message must be determined.
- The path cost is minimised in attempt to discover the smallest time rerouting path to minimise transmission delay.
- The capacity efficiency (C_{ef}) must be determined, that is focused on having enough bandwidth which transmit message. The transmission delay D is reduced because the shortest path has the lowest path cost (s). The goal of this work is to maximize favorable benefits through the selection of optimum value. This is an example of a linear programming (LP) issue that is an optimisation problem in which all of the objective functions are used to express functions and limitations. A linear function is denoted by $f(y_1, y, \ldots\ldots) = a_1 y_1 + a_2 y + \cdots + a_0$ where $a_1, a_2, \ldots\ldots, a_0$ are constants. An LP issue that maximizes the goal function, the work is interpreted as follows:

Optimise

$P_1 y_1 + P_2 y_2 + \cdots + P_n y_n$ (Goal function)

Restriction applies

$y_1 + y_2 + \cdots z_n \leq B_w$ (Bandwidth constraint)

$y_1 + y_2 + \cdots y_n \leq P_{cost}$ (Path cost constraint)

$y_1 + y_2 + \cdots y_n \leq C_{eff}$ (Capacity efficient constraint)

There are no negativity restrictions: $y_1 \geq 0,\ y_2 \geq 0, \ldots, y_n \geq 0$ (Non-signals cannot be transmitted by the model)

The optimisation statements with introduced heuristics are used to pick the best route with capacity efficient for best rerouting.

4.2.4 Algorithm for generating optimal alternative path in capacity efficient EGA model

The module is concerned with determining the best path to take by employing an improved genetic algorithm. This module receives a set of randomly generated paths as input. Every path is referred to as a chromosome, and every node or link on the network is called a gene. In summary, the algorithmic system provided in algorithm 1 is followed when generating an optimised alternative path in an EGA system.

Algorithm 1: Capacity efficient EGA for rerouting on communication network failures

Input: Transmission data (s, d, nodes, failed node(s), active nodes)
Parameters for EGA (*pop*, *Gen*, *p*M, *p*C)
"pop" is the population, *C* is path cost, g indicates the gene,
Indicates the number of nodes in the chromosomes, *W* indicates the video packet, *D* indicates message delay, $g_i = \text{nodes in the chromosome}$, a=
nodes number in the chromosome + path cost of the chromosome, 'S_n' indicates the transmitting node and 'd_n' indicates the receiving node, *pC* indicates crossover probability and *p*M indicates mutation probability, O_{AL} indicates an optimal alternative link, M_{PC} indicates minimal path cost, i, j=1,2,3…. n and B_{g_i} indicatess the bandwidth needed to send packets from the transmitter to the receiver respectively.

Output: O_{AL}, M_{PC}, B_{g_i}, D, T_t

1. Begin
2. As Candidate Solutions, generate a random population =*pop*
3. Create Chromosomes that are candidate solutions
4. Initialisation: C, S_n, d_n, B_{g_i}, D, Ch
5. Determine C=Sum $(l_1 + l_2 + \cdots + l_n)$; g_j=Sum $(g_1 + g_2 + \cdots + g_n)$
6. Calculate fitness = 1/(SUM($C_{g(j)} * g_i(j+1)) + SUM(B_{g_i} * g_j(j+1))$
7. $Calculate\ D = W / B_{g_i}$
8. *Calculate* $a = C + g_j$
9. $Calculate\ B_{g_i} = {}^{W}/_{(D-a)}$; Offspring-1, Offspring-2Parent-1, Parent-2
10. Create a new population. [Recent pop]
11. Analyse (ch) $= f_i / SUM(f_i)$ (*Ranking by Selection)
12. For i = 1 to size (pop) Do
    Select [parent1, parent2] from pop
    Crossover (parent1, parent2) with probability 0.5= [child1, child2]
    End Do
13. If Parent Fitness > Child Fitness then
    Apply Mutation Operator
    Replace Old pop
    End if
14. While the termination condition is not met Do 12 & 13
15. Determine new Pop Else
16. Determine **Output**: O_{AL}, M_{PC}, B_{g_i}, D, T_t
    End While

4.2.5 Numerical computation of multiple failure survivability in EGA model

Figure 4.3 depicts video traffic being transmitted over a wireless network connected with various nodes and dedicated point-to-point links to every other device. The links connect nodes for remote communication, which are made up of wireless routers and switches. When a link fails as a result of an attack, the message will not reach the destination node. To resolve the link failure, the capacity efficient EGA model searches the network for the next available two or more alternative links to form an optimal path and hybridises them to reroute the traffic. As a matter of fact, rerouting takes place in proportion to the bandwidth required to retransmit the packet. The analytical scenario in Figure 4.3 is represented by the transition diagram of Figure 4.4. The circles indicate various network nodes, while the transmission lines connecting nodes indicate the link. The failed links are marked with an X on the links MQ and FL. The link costs are randomly generated. A weighted graph is a graph with weighted edges. The weights may represent factors like cost or the distance required to travel between nodes. Weighted graphs are used to measure the cost of traveling between nodes, and help to find the shortest path between different nodes.

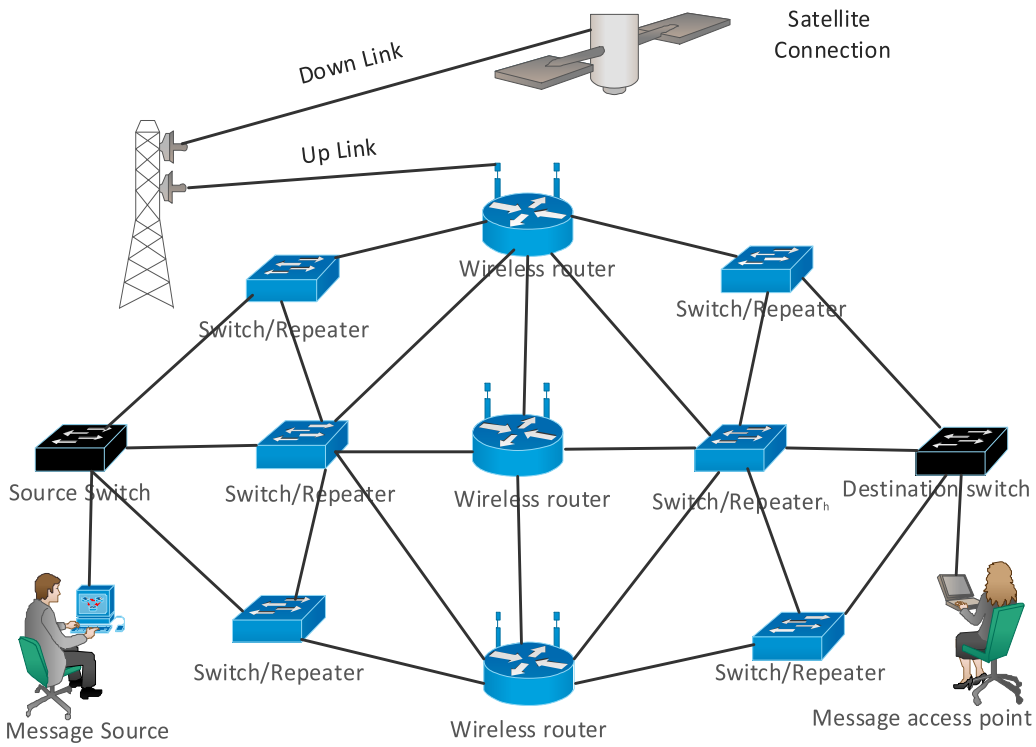

Figure 4.3: Link–link failures on video transmission

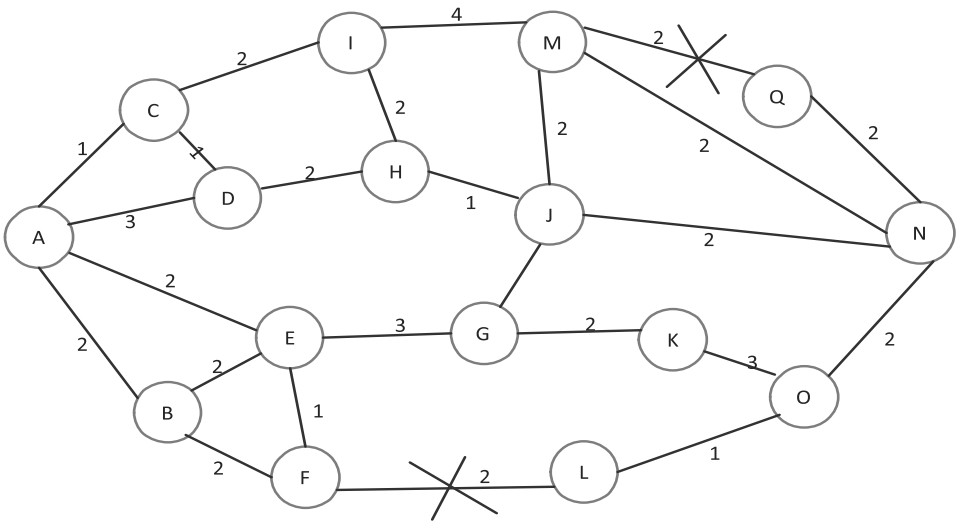

Figure 4.4: A state transition diagram representation of Figure 4.3

All available paths are generated, the paths represent the chromosomes and nodes and links represent the genes. The paths generated are candidate solutions.

[Step–1]: 1st Generated Population

Figure 4.5 shows the first generated population from the transition diagram of Figure 4.4

Path – 1: A – C – I – M – N; Path – 2: A – C – I – M – J – N; Path – 3: A – C – D – H – I – M – N; Path – 4: A – D – G – J – M – N; Path – 5: A – D – G – J – N; Path – 6: A – E – G – K – O – N; Path – 7: A – D – H – I – M – J – N; Path – 8: A – E – G – J – N

Figure 4.5: 1st Generated population

[Step–2]: Fitness

To generate a new generation, the fitness function and rank must be calculated in order to identify the fitted chromosomes for the new generation. Figures 4.6–4.10 depict the determination of path cost, the number of nodes in the chromosome to calculate the fitness value, and the bandwidth required. The network paths are being weighed by calculting the path cost of the path.

Path Cost: Path-1:$C_{g_i(j)} = 1 + 2 + 4 + 2 = 9$; Path-2= 11 ; Path-3= 12; Path-4= 11; Path-5= 9; Path-6= 12 ; Path-7= 15; Path-8= 10

Figure 4.6: Path cost determination

This is the number of nodes in a chromosome (path). Path-1: $g_i(j+1) = 5$; Path-2= 6; Path-3= 7; Path-4= 6; Path-5= 5; Path-6= 6; Path-7= 7; Path-8= 6

Figure 4.7: Node count in the path

[Step–3]: Bandwidth determination

The bandwidth needed to send video traffic across the paths is calculated using equations 10 and 11, as shown in Figure 4.8. If the video traffic is 500-bytes and 20-bytes is the IP header, the true video traffic size is '= (500-bytes – 20-bytes) = 480-bytes'.

For **Path – 1: A – C – I – M – N:** It takes 5 milliseconds for the packet to reach the 1st node, since there are 5 nodes in Path–1, then packet will be transmitted from transmitter to receiver in=5×5=25 milliseconds=0.0250 s.

$Path\ cost = 9$, (See figure 5), Delay=$\frac{9m}{0.\ 36m/ms}$=25 ms = 0.0250. From equation (5), p=5+9=14, α and β are taken to be 1, Required Bandwidth,

$B_{Req}=\frac{W}{D-a}=\frac{480}{25-14}=\frac{480}{11}$ = 43.60 Kbytes/s. The required bandwidth to transmit the traffic is 43.60 Kbytes/s.

Figure 4.8: Bandwidth determination

Fitness functions: Using equation (1) The Fitness function of $\text{Path} - 1 = \frac{1}{9*5+43.6*5} = \frac{1}{263} = 0.003800$ $\text{Path} - 2 = 0.00342$ 2; $\text{Path} - 3 =$ 0.003440	$\text{Path} - 4 = 0.003480$; $\text{Path} - 5 =$ 0.003800 $\text{Path} - 6 = 0.003680$; $\text{Path} - 7 =$ 0.002710 $\text{Path} - 8 = 0.003820$

Figure 4.9: Chromosomes fitness determination

Chromosome selection Using equation (2): Selection is done by ranking system. $\sum f_j = 0.0038 + 0.00342 + 0.00344 + 0.003 + 0.0038 + 0.00368 + 0.00271 + 0.00382$	The probability of selecting $\text{Path} - 1 = \frac{0.0038}{0.02815} = 0.13500$, $\text{Path} - 2 = 0.12150$, $\text{Path} - 3 = 0.12220$, $\text{Path} - 4 = 0.12360$, $\text{Path} - 5 = 0.13500$, $\text{Path} - 6 = 0.13070$, $\text{Path} - 7 = 0.09627$, $\text{Path} - 8 =$ 0.13570

Figure 4.10: Chromosomes ranking for optimal path selection

[Step–4]: New population (2nd Generation)

The high rank chromosomes are selected and 50% crossover probability is used, then Path-1, Path-5, Path-6 and Path-8 are selected. The chromosomes selected from the population size of eight are: Path – 1: A – C – I – M – N; Path – 6: A – E – G – K – O – N; Path – 5: A – D – G – J – N; Path – 8: A – E – G – J – M – N.

1st Crossover Operation: 1–point crossover is used to avoid node duplication.

Parent –1 : A – E – G – J – M – N; *Parent – 1 fitness=0.00382;* Parent – 2: A – D – G – J – N, **Parent –2 fitness=0.00380**

Crossover Point: G

Child1: A – E – G – J – N; Child2: A – D – G – J – M – N.

Parent–1 has a fitness of 0.00382 and Parent – 2 has a fitness of 0.00380 and as shown in the first crossover operation, Child–1 has a fitness of 0.00420 and Child–2 has a fitness of 0.00410 which shows an improvement in the two offspring. The two offspring are moved to the next generation.

2nd Crossover operation

In second crossover operation, Parent – 1 has the fitness of 0.00368 and Child –1 has a fitness of 0.00420 which shows an improvement in the offspring, therefore Child–1 is automatically moved to the next generation. Parent–2 has a fitness of 0.00380 and child–2 has a fitness of 0.00300 which means there is no improvement in Child–2, and then mutation operation needs to be performed.

Genetic mutation operator

The omitting mutation operator is applied, and the omitted node is Node "O", Node "O" is chosen randomly from the generated path which should not be source or destination nodes. Un–mutated Offspring

: A – D – G – K – O – N; Un–mutated Offspring fitness =0.0030 Mutated Offspring: A – D – G – K – N; Mutated Offspring fitness=0.0034, The path cost for mutated offspring is 10, number of node is 5, delay is 25ms, bandwidth is 48 Kbytes/s. The fitness =0.0034. The fitness of mutated offspring is better than the fitness of un–mutated offspring therefore the parent is moved to the next generation.

[Step – 5]: New population: 3rd generation

Path – 1: A – E – G – J – N with fitness 0.0042; Path – 2: A – D – G – J – M – N with fitness 0.0041. If crossover operation is done, offspring that are equal to parents will be produced and this leads to duplication, the optimal alternate route produced is: A – E – G – J – N.

4.2.6 Spare capacity allocation (SCA) for video message

Bandwidth is the amount of data that can be transmitted across a network connection. Congestion must be managed in order to ensure the flow's Quality of Service (QoS) in the produced path. Traffic jams might have happened as a result of:

- A lack of bandwidth provided for traffic transmission on the network path;
- Heavy workload on the network devices and high transmission request on the network paths, resulting in QoS degradation.

To determine the bandwidth required to transfer a video packet, use equation 9 to compute throughput [28].

$$B_{Required} = \frac{W}{D} \tag{9}$$

Equation 9 can be used to calculate the amount of bandwidth required between two linked network sites. The capacity of a video message to be transmitted is denoted by W, and the packet delay is denoted by D. Then, as shown in equations 10 and 11, the required bandwidth for a path with two or more nodes is calculated.

$$B_{Required} = \frac{W}{D\text{-}a} \tag{10}$$

$$a = f(n, I) = \lambda n + \omega I \tag{11}$$

Where 'a' is an undetermined function that depends on variables n & i, where n is the total amount of hubs in the network route and $I = \sum_n I_n$, is the total amount of link cost in a transmission path. Constant values are λ and ω. A link's delay is equal to its length 'm' divided by the propagation speed 's'.

4.2.7 Bandwidth required for video message transmission/rerouting

The bandwidth required to reroute the video message is alread calculated in Figure 4.8 of subsection 4.1.7.

4.3 DEVELOPMENT OF CAPACITY EFFICIENT ACS SURVIVABILITY MODEL

Figure 4.11 shows capacity efficient ACS sub-framework for wireless network survivability.

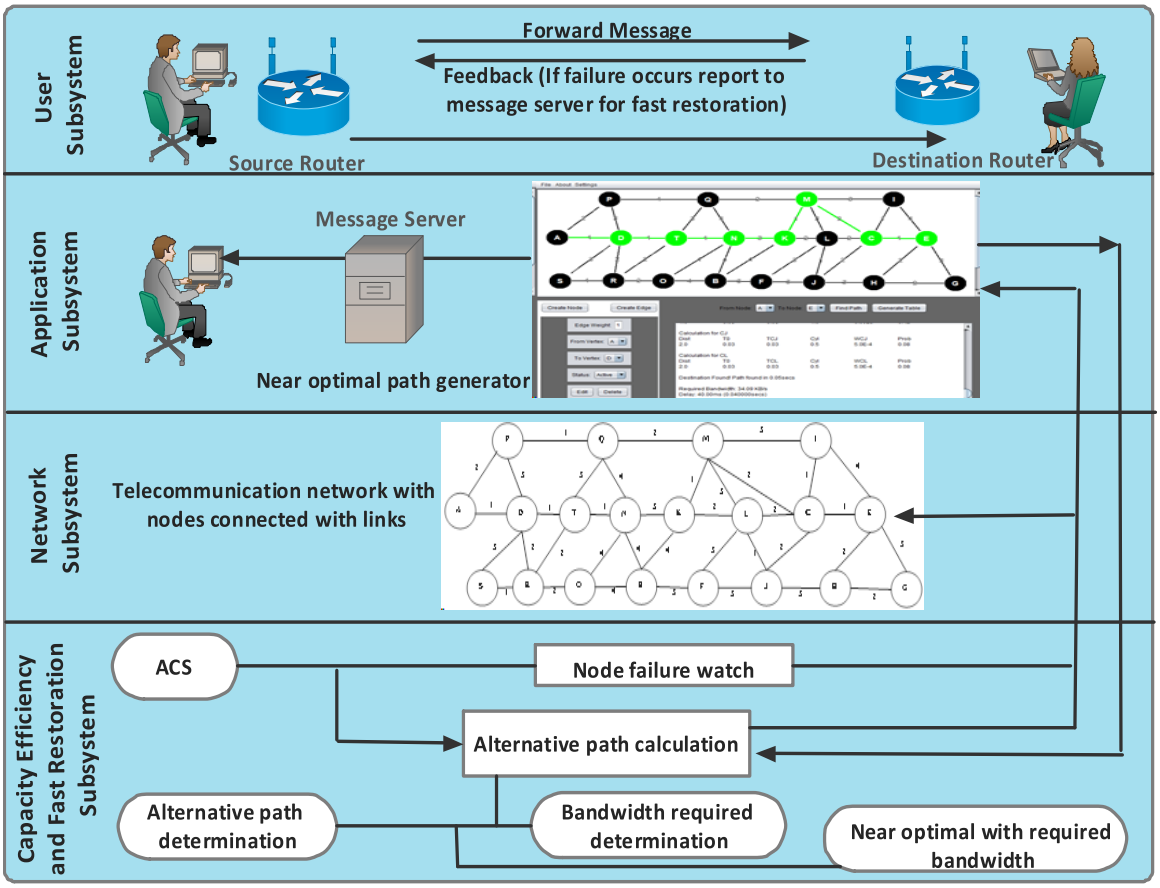

Figure 4.11: Surviving node-node failures framework

4.3.1 Problem formulation for capacity efficient ACS model

The capacity of a mobile device to consistently provide solutions in accordance in the case of a failure or other undesirable unforeseen circumstances is referred to as wireless network survivability [94]. The network survivability models considered in this research take into account networks subjected to certain unfavorable occurrence as path failures, which are usually accompanied by a dramatic switch in the network services supplies, like the channel capacity needed to transfer in the existence or absence of failures, giving rise in delay. Rerouting steadily restores the network, and the malfunctioning path recovers through the model's solutions. In this system, it is critical to include a rerouting path whenever a peer (p2p) node fails for certain right quality, such as bandwidth with minimal delay, and to ensure good overall network facilities usage. The model contains enough variety and spare capacity to tolerate capacity loss and allow for the recovery of traffic flow at demanded level of service. This network is a graph that is undirected.

The wireless network under consideration is represented by F = (N, L), in which N symbolises the devices connected to the network (vertices) and L symbolises the links connecting the devices (edges). The examples of devices are terminals or workstations, switches, hubs and routers on the network while connecting links are the transmission lines like microwave links, wireless-radios for data transmission.

4.3.2 Capacity efficient ACS model's goal function

The primary goal of the study is to identify the best alternate route with the best capabilities for rerouting a voice packet in the case of a fault. Sending a voice message over a low-bandwidth network is a crucial problem in the developing world, particularly in Africa. When a voice packet fails, it must be rerouted as soon as possible because voice data must be delivered to the addressee as soon as possible. Data transfer limitations, like adequate bandwidth (B_w), lower path cost (P_{cost}), shortest route and capabilities effectiveness are important considerations to take into account in initiating the best alternate route. For saving business activities, information must be relayed as quickly as possible. The main goal of the study is to locate the best alternate route to retransmit a packet in the case of a fault caused by main characteristics failures of wireless connections that endanger business operations all over the globe. Communication breaks, hardware faults, software malfunctioning, operator defects, catastrophic events, and malware issues are examples of failure attributes. This researcher proposes a capacity-efficient ACS capable of producing a best possible alternate route to redirect data in the case of failures in the quickest time.

The suggested system, most importantly, could be used to resolve the issue of optimisation. The goal is to select the most effective route among all viable options. The most effective route can be either the simplest or the most complex. Both of these scenarios are optimisation issues. Linear programming is a problem-solving method that uses computational equations to express and fix issues, could be used to address optimisation problem. An optimisation problem is made up of three parts: variables for making decisions, a goal function, and limitations. These three components are used to create a mathematical model.

- **Judgment variables**: They are the parameters that could be controlled inside a model. Since there are n judgment parameters, they are denoted by the letters h_1, h_2,...., h_n..

- **Goal function**: This really is the challenge that researchers' want to improve or minimise. An optimal solution is denoted by the notation f (h_1, h_2,..., h_n). Optimisation of the performance of this activity can be achieved using the notation: $\max_{h_1,h_{2,\dots},yh_n} f(h_1, h_2, \dots, h_n)$ and, the expression $\min_{h_1,h_{2,\dots},h_n} f(h_1, h_2, \dots, h_n)$ can be used.
- **Limitations**: These are assignment problems or limitations. The following are the mathematical tools::

  $k_1(h_1, h_2, \dots) \leq 0, \qquad k_2(h_1, h_2, \dots) \leq 0, \qquad k_3(h_1, h_2, \dots) \leq 0$

4.3.3 Mathematical justification for capacity efficient ACS model

In the event of a node failure in which a voice packet needs to be sent from transmitter to receiver, the best route (P) to reroute the packet from transmitter to receiver needs to be produced within lowest delay to attain rapid rerouting. This means optimal rerouting path (P) is determined by the following constraints:

- Owing to the occurrence of failed nodes, amount of bandwidth (B_w Kbytes/s) available is limited. As a result, the required bandwidth (B_w) to reroute the message must be determined.
- The path cost is minimised to accomplish the fastest delivery rerouting path to minimise transmission delay.
- The capacity efficiency (C_{ef}) must be determined, that is focused on having enough bandwidth for routing and rerouting packets. The transmission delay D is reduced because the shortest path has the lowest path cost (s). The goal of the research is to maximise favorable benefits through the selection of optimum value. A linear function is denoted by $f(h, h_2, \dots\dots) = a_1h_1 + a_2h_2 + \cdots + a_0$ where $a_1, a_2, \dots\dots, a_0$ are limitations. For this presentation LP that optimise the objective function as follows:

Optimise

$P_1h_1 + P_2h_2 + \cdots + P_nh_n$ (Goal function)

Restriction applies

$h_1 + h_2 + \cdots h_n \leq B_w$ (Bandwidth constraint)

$h_1 + h_2 + \cdots h_n \leq P_{cost}$ (Path cost constraint)

$h_1 + h_2 + \cdots h_n \leq C_{ef}$ (Capacity efficient constraint)

There are no negativity restrictions $h_1 \geq 0,\ h_2 \geq 0, \ldots, h_n \geq 0$ (The model cannot transmit non signals).

In terms of solving this optimisation problem, the proposed model is used to generate the optimal alternative path together with the heuristics added to calculate the sufficient bandwidth required to transmit the message.

4.3.4 Algorithm for generating optimal alternative path in capacity efficient ACS model

The module is concerned with determining the best path to take using an Ant Colony System. This module receives a set of randomly generated paths as input.

Algorithm 2: Capacity Efficient ACS for Rerouting on Communication Network Failures

Input: network information (S_n, d_n, number of nodes, failed node(s), active nodes) Parameters for ACS (α, β, ρ, t), Parameters for Bandwidth (ʎ,ω, a) 'Path' implies the candidate solution, *C* implies path cost of a path, *W* implies voice size, *D* implies delay, $g_i =$ node count in a path, a= (number of nodes in a path) + (path cost of the path), 'S_n' implies transmitter node and 'd_n' represents the receiver node, O_{AL} implies an optimal alternative path, P_T implies path fitness i, j=1,2,3…. n, k=1, 2, 3. …. n and B_{g_i} implies the bandwidth needed to send messages from transmitter to receiver respectively.

Output: O_{AL}, P_T, B_{g_i}, D, T_t

1. Begin
2. Generate Random Paths as Candidate Solutions = *path*
3. A: Starting State
4. N: Terminating State:
5. When all states have been visited at least once: Terminating condition
6. A, B, C, D, E, N: Potential state
7. Initialise Optimal Paths from 2 // Starting from A to N
8. Initialise C, S_n, d_n, B_{g_i}, L_{nn}, D, τ_0, τ_{ij}, η_{ij}, $P_{i,j}^k$,
9. Initialise α = 3, β = 2, ρ = 0.01, t = 0.005, ʎ= 1,ω=1
10. Compute $\tau_0 = 1/(n * L_{nn})$
11. Calculate $\tau_{ij}(t) = (1-\rho) * \tau_{ij}(t) + \rho * \tau_0$
    Calculate $\eta_{ij} = 1/d_{i,j}$
    Calculate $P_{i,j}^k(t) = ((\tau_{i,j}(t))^{\alpha} * (\eta_{i,j})^{\beta})/(\sum_{i \epsilon J_i^k}[\tau_{i,j}(t)]^{\alpha} * [\eta_{i,j}]^{\beta})$
12. Calculate $P_{i,j}^k$ for potential states
13. For i = 1 to n Do
        Select [Node with highest probability] from $P_{i,j}^k(t)$
    End Do
14. If node with highest Probability= failed node then
        Select node with next highest probability
    End if
15. While the termination condition is not met Do 1 to 16
16. Generate O_{AL} // transmission path

17. Compute C=Sum ($l_1 + l_2 + \cdots + l_n$); g_j=Sum ($g_1 + g_2 + \cdots + g_n$)
18. Compute $D = W / B_{g_i}$
19. Compute a= $\lambda C + \omega\, g_j$
19. Compute $B_{g_i} = {}^{W}/_{(D-a)}$
20. Compute Output: O_{AL}, P_T, B_{g_i}, D, T_t
End While

4.3.5 Numerical computation of multiple failure survivability in capacity efficient ACS model

The alternative path is generated in real time, with the bandwidth required to transmit or reroute a message. Algorithm 2 depicts the procedure for producing an alternate route together with the required bandwidth. This section describes the analytical method for determining an alternate path for rerouting a message. Figure 4.14 depicts the analytical method for generating alternative paths in greater detail. The parameter specifications for the capacity efficient ACS are shown in Table 4.1. For the purposes of this analysis, the majority of the parameter values in Table 4.1 are based on best practices found in the literature. Figure 4.13 depicts a transition diagram of a real-world wireless network setup. The link costs in Figure 4.13 are randomly generated.

This study provides a scenario for the suggested method's simplicity for capacity efficient ACS model as shown in Figures 4.12, 4.13, and 4.14. Figure 4.12 depicts p2p connections in a wireless communication network when multiple subscribers want to send a voice over the network. As shown in Figure 4.12, each piece of network equipment represents a node and a voice message transmitter at point Q. The nodes in the network are represented by the (WiMax: worldwide interoperability for microwave access) TV centers in Figure 4.12. Figure 4.13 depicts the transition diagram from Figure 4.12. The circles represent different network nodes, and transmission lines linking nodes are links. Figure 4.14 depicts the analytical ways of generating the alternative paths.

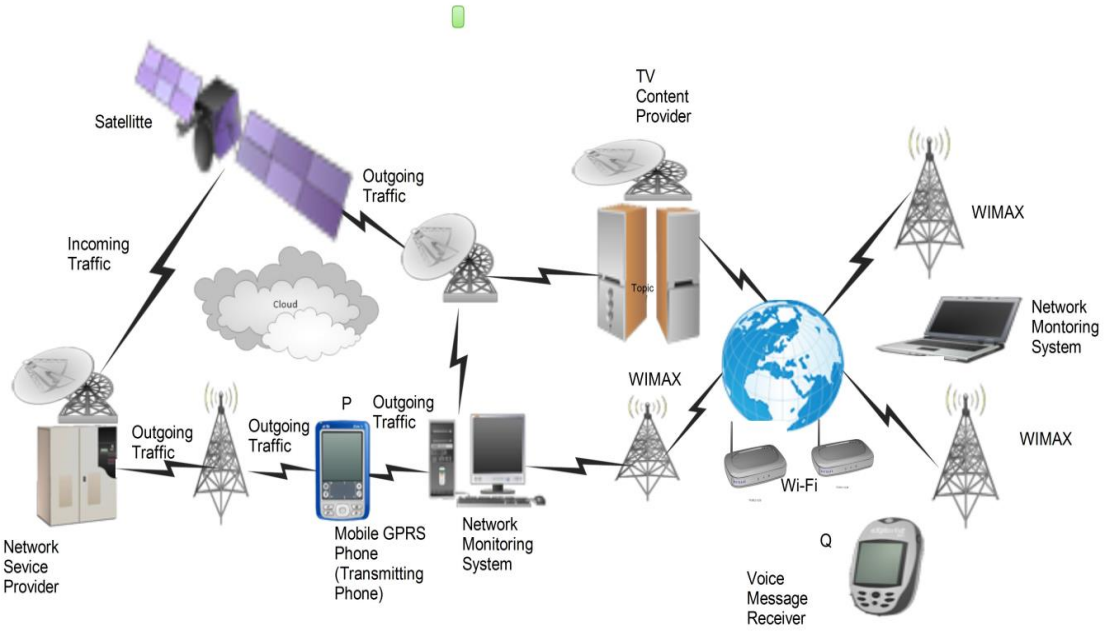

Figure 4.12: Voice transmission node-to-node failure network

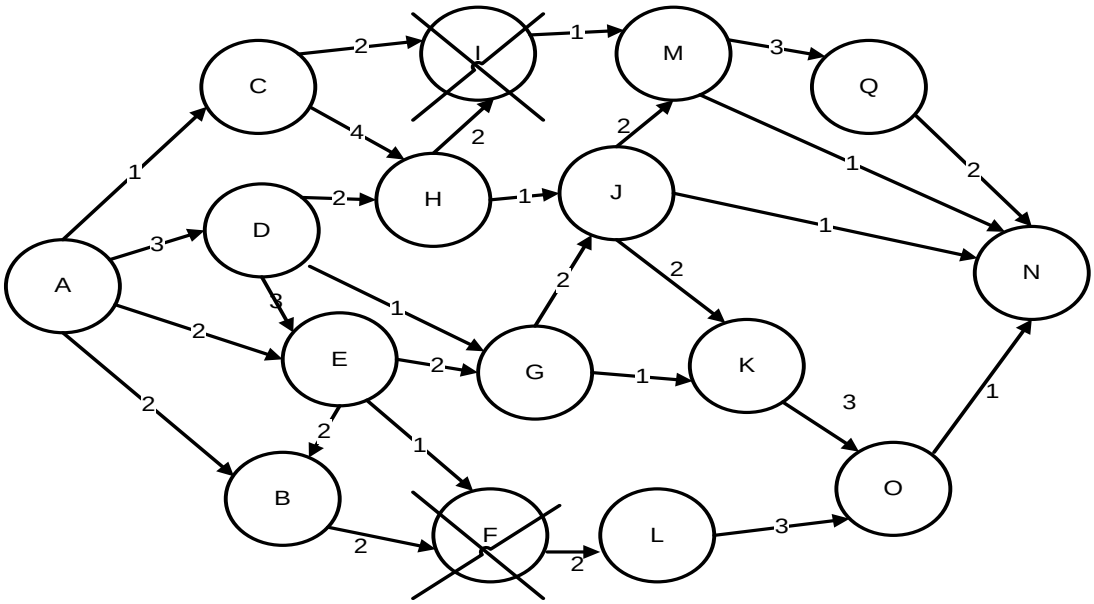

Figure 4.13: A state transition diagram depicting a real-world scenario

Table 4.1: Parameter for capacity efficent ACS model

Characteristics of ACO	ACO Type	Pheromone Coefficient β	Heuristic Coefficient α	Rate of Evaporation ρ	Distanced	1st node Transmission Time	Packet size
Characteristics	ACS	1	2	.10	Varable	.005secs	500-bytes

For a transmission from node A to N

The First Iteration: A: Starting state

Potential State: B, C, D, E. Lengths are determined at random.

Consider equation 1: $\tau_0 = \frac{1}{n\,L_{nn}}$. For length AB, $\tau_0 = \frac{1}{16*2} = 0.03125$

Consider Local update

Consider equation 2: $\tau_{ij}(t) = (1.0 - \rho).\tau_{ij}(t) + \rho.\tau_0$, $\tau_{AB} = (1.0 - 0.10) * 0.03 + 0.10 * 0.03 = 0.90 * 0.03 + 0.003 = 0.03$

For distance AE, $\tau_0 = \frac{1}{16*2}$=0.03125, $\tau_{AE} = (1.0 - 0.10) * 0.03 + 0.10 * 0.03 = 0.9 * 0.03 + 0.003 = 0.03$

For distance AD, $\tau_0 = \frac{1}{16*3}$=0.02083, $\tau_{AD} = (1 - 0.1) * 0.02 + 0.1 * 0.02 = 0.9 * 0.02 + 0.002 = 0.02$

For distance AC, $\tau_0 = \frac{1}{16*1}$=0.0625, $\tau_{AC} = (1 - 0.1) * 0.06 + 0.1 * 0.06 = 0.9 * 0.06 + 0.006 = 0.06$

Equations 3 and 4 apply the global updating rule only to edges which belong to the best ant route.

From equation 5

$\eta_{AB} = \frac{1}{2} = 0.5$, $\eta_{AE} = \frac{1}{2} = 0.5, \eta_{AD} = \frac{1}{3} = 0.33, \eta_{AC} = \frac{1}{1} = 1$

Consider equation 6:

$w(A,B) = [\tau_{A,B}]^{\alpha}[\eta_{A,B}]^{\beta} = (0.03)^2(0.5)^1 = 0.00045$, $w(A,E) = [\tau_{A,E}]^{\alpha}[\eta_{A,E}]^{\beta} = (0.03)^2(0.5)^1 = 0.00045$ $w(A,D) = [\tau_{A,D}]^{\alpha}[\eta_{A,D}]^{\beta} = (0.02)^2(0.33)^1 = 0.000132$

$w(A,C) = [\tau_{A,C}]^{\alpha}[\eta_{A,C}]^{\beta} = (0.06)^2(1)^1 = 0.0036$

Sum=0.00045+0.00045+0.000132+0.0036=0.0046

Probabilities: $P_{AB}^{k} = \frac{0.00045}{0.004632} = 0.097 \approx 0.10$, $P_{AE}^{k} = \frac{0.00045}{0.004632} \approx 0.10, P_{AD}^{k} = \frac{0.000132}{0.004632} = 0.028 \approx 0.03, P_{AC}^{k} = \frac{0.0036}{0.004632} = 0.778 \approx 0.78$

Node C is selected as next node; it is the most probable node.

2ND Iteration, Current state: C.

Potential State: I, H. $:L_k = (C - I) = 2, L_k = (C - H) = 4$

Consider equation 1: $\tau_0 = \frac{1}{n\,L_{nn}}$, Length CI, $\tau_0 = \frac{1}{16*2}$=0.03125

Consider local update, $\tau_{ij}(t) = (1.0 - \rho).\tau_{ij}(t) + \rho.\tau_0$,$\tau_{CI} = (1.0 - 0.10) *$

Figure 4.14: Analytical method of generating the alternative path

$0.03 + 0.10 * 0.03 = 0.9 * 0.03 + 0.003 = 0.03$

for distance CH, $\tau_0 = \frac{1}{16*4}$=0.0156

$\tau_{CH} = (1 - 0.1) * 0.0156 + 0.1 * 0.0156 = 0.9 * 0.0156 + 0.00156$=0.0156

Using equation 5: $\eta_{CI} = \frac{1}{2} = 0.5, \eta_{CH} = \frac{1}{4} = 0.25$

Using equation 6: $w(C, I) = [\tau_{CI}]^{\alpha}[\eta_{CI}]^{\beta} = (0.03)^2(0.5)^1 = 0.00045$, $w(C, H) = [\tau_{CH}]^{\alpha}[\eta_{CH}]^{\beta} = (0.0156)^2(0.25)^1 = 0.000064$

Sum=0.00045+0.000064=0.00051

$P_{CI}^{k} = \frac{0.00045}{0.00051} = 0.88$, $P_{CH}^{k} = \frac{0.000064}{0.00051} = 0.125 \approx 0.13$.

Node I is the most probable node, but I cannot be chosen because failure occurred here. H is chosen. The only available device where traffic can flow through is Node J. Node J is the current state.

3rd Calculation (Iteration)

J: Current State and N, M: Potential State

For distance JN, Using Equation 1, $\tau_0 = \frac{1}{16*1}$=0.0625

Local update, Using equation 2: $\tau_{ij}(t) = (1 - \rho).\tau_{ij}(t) + \rho.\tau_0$, $\tau_{JN} = (1 - 0.1) * 0.0625 + 0.1 * 0.0625 = 0.9 * 0.0625 + 0.00625$ $\tau_{JN} = 0.0625$

For distance JM, $\tau_0 = \frac{1}{16*2}$=0.03125,

Local Update, $\tau_{JM} = (1 - 0.1) * 0.03125 + 0.1 * 0.03125 = 0.9 * 0.0315 + 0.003125$ $\tau_{JM} = 0.03125$

From equation 5, $\eta_{JN} = \frac{1}{1} = 1$, $\eta_{JM} = \frac{1}{2} = 0.5$

Using equation 6:

$w(J, N) = [\tau_{JN}]^{\alpha}[\eta_{JN}]^{\beta} = (0.0625)^2(1)^1 = 0.0039$, $w(J, M) = [\tau_{JM}]^{\alpha}[\eta_{JM}]^{\beta} = (0.03125)^2(0.5)^1 = 0.0005$

Sum=0.0039+0.0005=0.0044, $P_{JN}^{k} = \frac{0.0039}{0.0044} = 0.886 \approx 0.89$, $P_{JM}^{k} = \frac{0.0005}{0.0044} = 0.114 \approx 0.11$. Node N is selected since it is the most probable node. From Node J, the message will move to Node N. In this analytical scenario, the generated path is A– C – H – J – N which is alternative path and is the near optimal path because it has a low path cost of 7. The needed bandwidth to send the packet from transmitter to receiver is calculated in subsection 4.2.7.

Figure 4.14: Analytical method of generating the alternative path continues

4.3.6 Spare capacity allocation (SCA) for voice message

The equations 9 – 11 of subsection 4.1.8 are used in calculating the spare capacity to reroute the voice message.

4.3.7 The bandwidth needed for rerouting the voice message

Using equations 10-11, this subsection in Figure 4.15 calculates the bandwidth required for rerouting the voice message on the path generated in subsection 4.2.5. For example, for a given 500-bytes of a voice message and 20-bytes of an IP header, the real message weight is (500.00-20.00) =480-bytes. Delay is determined by dividing the link length by speed of propagation. The initial time is 5ms (0.0050s), and 5 nodes exist in the path, it takes the message to travel from the transmitter to the receiver: 5 multiply by 5=25milliseconds from the direction of A – C – H – J – N.

Sum of Lengths =1 + 4 + 1 + 1= 7 metres, $\text{Time} = 25\text{ms} = \frac{25}{1000}\text{s} = 0.025\text{second}$

$$\text{Transmission Speed} = \frac{7\text{m}}{0.025\text{s}} = 280\text{m/s},$$

$$\text{Delay} = \frac{7\text{m}}{280\text{m/s}} = 0.025\text{s}.$$

From equation 9 :$a = 7 + 5 = 12$, α and β are taken to be 1

$$\text{B}_{\text{Req}} = \frac{\text{W}}{\text{D}-\text{a}} = \frac{480}{25-12} = \frac{480}{13\text{ms}} = \frac{480}{0.013} = 36923.08\text{bytes/sec} = 36.92\text{ Kbytes/s}.$$

Figure 4.15: Bandwidth required for transmitting the message

4.4 EVALUATION AND VALIDATION MECHANISMS

The measurements listed are used to evaluate and validate the effectiveness of the suggested model:

- **Measuring throughput:** Throughput refers to the number of units of digital data that a system can process in a given length of time [92]. It can be applied to a wide range of systems, including network systems.

$$Throughput = \frac{Message\ Size}{Transmission\ Time} \quad \text{(Bits/Seconds)} \qquad (12)$$

- **Measuring path cost:** To make path cost more precise, recall that a path in a graph G = (N, E) is a sequence of nodes $(x_1, x_2, \ldots, x_p)$ such that each of the pairs $(x_1, x_2), (x_2, x_3), \ldots, (x_{p-1}, x_p)$ are edges in E.

  The cost of a path is simply the sum of all the edge costs along the path, that is

$$Path_{cost} = c(x_1, x_2) + c(x_2, x_3) + \ldots + c(x_{p-1}, x_p). \quad (13)$$

Given any two nodes *x* and *y*, there are typically many paths between the two nodes, with each path having a cost.

- **Transmission time:** It is the time taken a packet to move from source to destination.

$$Transmission\ Time = \frac{Packet\ Size}{Bit\ Rate} \quad (14)$$

- **Complexity:** is the length of time it takes an algorithm to run as a function of the input length. It calculates how long each statement of code in an algorithm takes to execute. Running time for different algorithms falls into different complexity classes. Big O notation describes the complexity of the algorithm. Algorithm with smaller growth characteristics will on average, take less time to complete than those with larger growth characteristics (for large problems). A constant algorithm O (1) will take the same amount of time to be completed no matter how large. Linear algorithm O (n) increases steadily with the data size. A quadratic or exponential grows much faster than *n* as *n* increases.
- **Packet drop:** Some packets must be lost by routers due to congestion. Previously, this was done at random, resulting in inefficient multimedia traffic performance.
- **Bandwidth usage:** Bandwidth refers to a network's capacity to transfer data between devices or the internet within a particular span of time. Higher bandwidth allows data to be transferred at a faster rate. As stated in equation 9 of subsection 4.1.8,

$$\text{Bandwidth Usage is } B_{usage} = \frac{W}{D}$$

where W is the message size and D is transmission delay is millisecond

- **Transmission delay time measurement:**

$$\text{Transmission Delay Time is } D_t = \frac{W}{B_{usage}} \quad (15)$$

where D_t is the transmission delay time, W is the message size and B_{usage} is the bandwidth usage.

- **Rate of packet delivery (PDR):** Is determined as the percentage of the total number of packets delivered successfully to the target to the number of packets transmitted by the transmitter [23].

$$PDR = \frac{P_{Recieved} * 100}{\sum_{i=1}^{n} P_{Generated}} \quad (16)$$

$P_{Recieved}$: Means, the number of packets received whereas $P_{Generated}$ is the number of packets generated by the transmitter and *shows* the node count in the network.

4.5 CHAPTER SUMMARY

This chapter describes the research design and methodology used for this study. The proposed capacity efficient evolutionary and swarm models are developed in detail in sections 4.1 and 4.2. Mathematical demonstrations of the goal functions and analytical statements applied throughout this chapter were provided. The purpose of this study was to look at how capacity efficient EGA and ACS models were used to solve the listed research problems. The capacity-efficient EGA model framework is made available. Sections 4.2.3 and 4.3.3, respectively, described the mathematical justification of capacity efficient EGA and ACS, illustrating all of the procedures required to build an alternative path in the event of a failure. The methods for assessing and validating the research study are also discussed. This study proposes a novel approach to dealing with the problem of traffic flows in wireless networks caused by repeated failures and attacks.

CHAPTER 5: INVESTIGATIONAL ANALYSIS AND OUTCOMES

5.1 INVESTIGATION 1: ANT COLONY SYSTEM SURVIVING ATM NODE-NODE NETWORK FAILURES.

5.1.1 Introduction

This section uses ACS intelligent modeling to overcome failures in an ATM network. In the literature, various methods for failure restoration have been proposed. They vary in the routing protocol being used, and while there has not been sufficient research on multiple failures of communication systems, the use of ACS is fairly recent in connectivity failures recovery. This aspect inspires this study. The gaps listed have really been identified as the foundation for improving existing survivability strategies: (i) there are a number of failures in traffic flow that require additional consideration. (ii) In order to maintain a stable network, spare capacity allocation issues in WATM networks with multiple failures must be addressed more thoroughly.

Swarm Intelligence is used in the proposed model to accomplish WATM network resilience. The suggested work is designed to be proactive in the face of multiple failures. Based on projected findings, this method is used to estimate data traffic and communication systems flow, but there is a need to recognise failure vulnerable network cases. This means that failure prediction must be performed in situations where a failure is likely. Failure tracking could be done based on the proactive approach to facilitate network recovery.

The goal of this research section is to use an intelligent swarm model to create a system which can withstand the consequences of numerous failures on WATM network. This study's major contributions are as follows: (i) Creation of a new suggested capacity efficient and quick recovery ACS, which can help communication network survive node-node failures. (ii) Knowledge creation and thorough illustrations of task scenarios as a standard guideline for telecom professionals to know network failure survivability rate. This research tends to be among the first to illustrate how a swarm intelligent application can be effectively used and applied to ATM network survivability rate, to the best of the authors' knowledge and awareness.

5.1.2 Investigational setup

Figure 5.1 depicts a WATM network interconnected by different network nodes that are linked together communication links. A through L indicates the nodes existing on the network, while

C and F representing failed nodes. Between two mobile system subscribers P and Q, an WATM network is established. Transmitter P in access point A initiates the packet communication, and reader Q in vertices E receives the information. Using a smart phone, the transmitter P sends a voice packet from the router A to a transceiver Q located at the router E. Once Client P transmits a voice packet to consumer Q, the message is forwarded through the nodes depicted in the scenario of Figure 5.1. The downtime is recorded as a result of node failure at nodes C and F. Later, the transmitting node realised there was no response from the receiving node, at which point the swarm model generated an alternate path to avoid the failure, and the network was revived using the remaining nodes. The message was received by User Q. This is accomplished by forwarding a voice message from node A through the system to produce an alternative route. The scenario is depicted diagrammatically in Figure 5.1 while Figure 5.2 is a depiction of the transition diagram from Figure 5.1. The outcomes of these experiments clarify sub-objective 1.

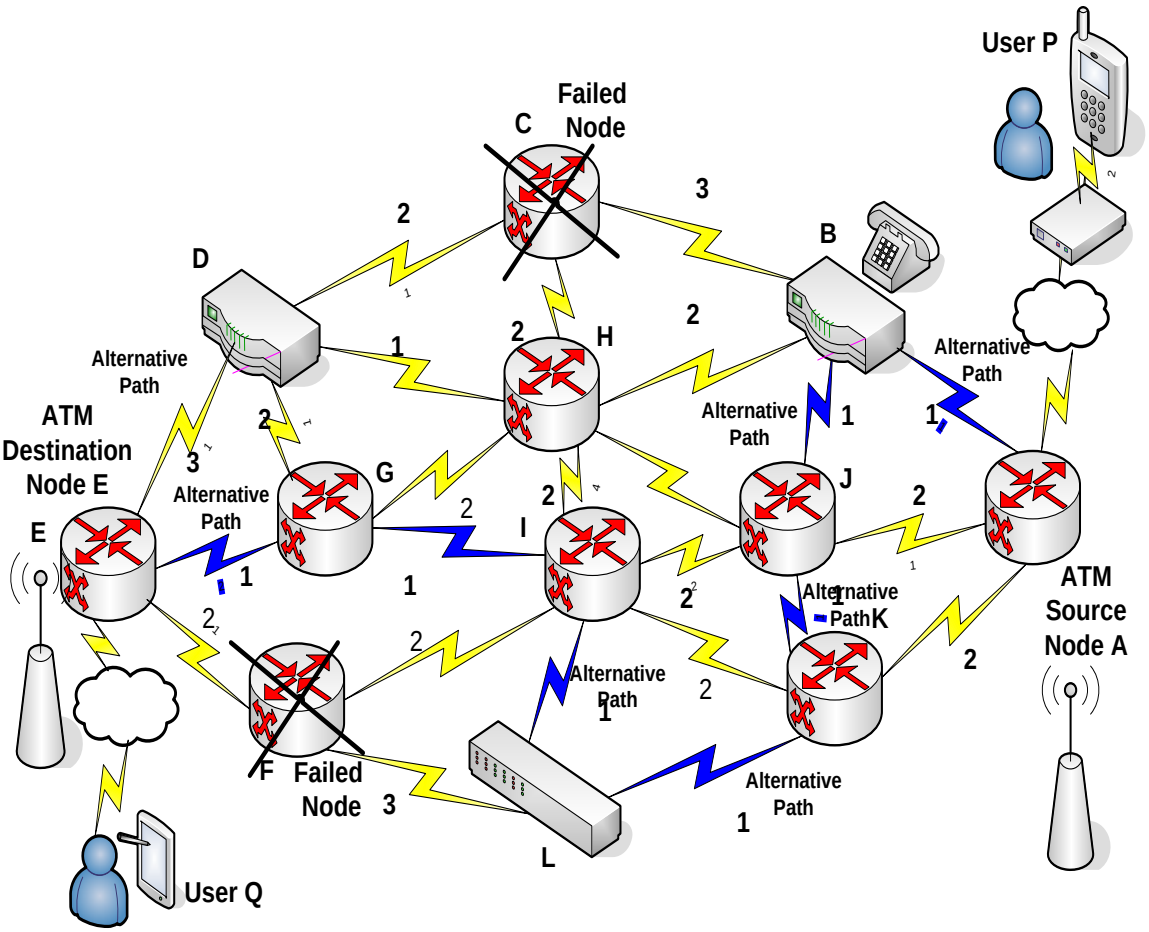

Figure 5.1: Node-node failure on voice transmission.

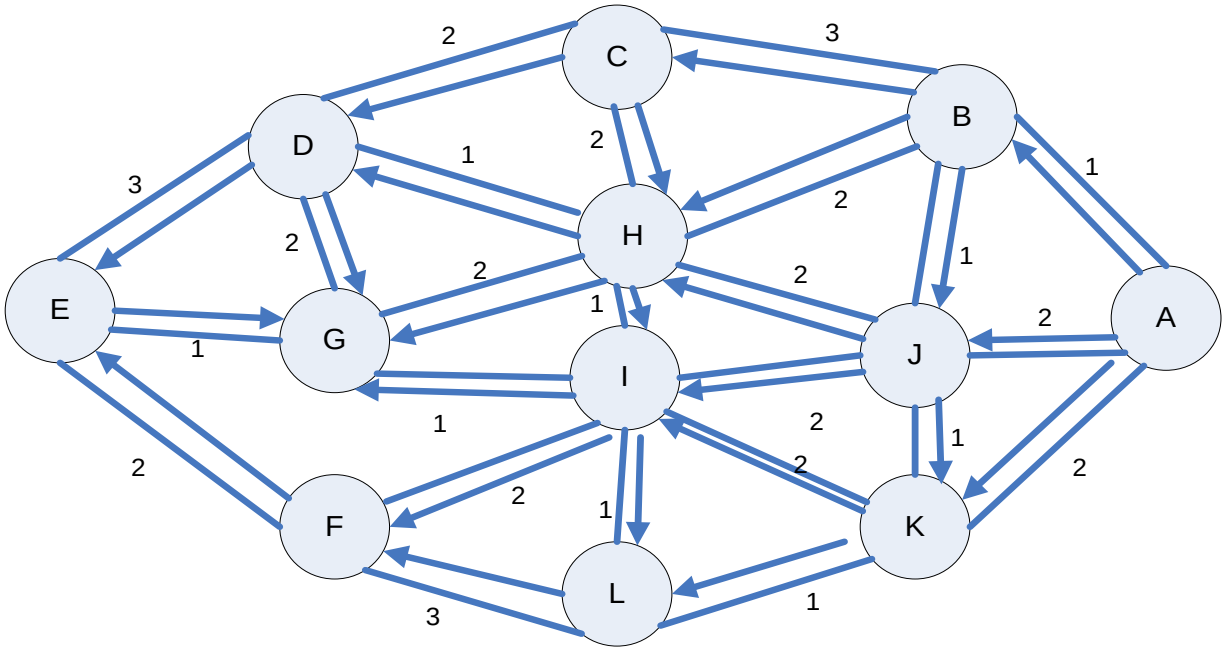

Figure 5.2: A state transition diagram depiction from Figure 5.1

Figure 5.2 depicts a transition diagram of circles indicating node and communication lines indicating links, respectively. The nodes are shown on devices from A to L and Links have been defined as the distance between two network nodes. The link costs in Figures 5.2 and 5.4 are randomly generated. Figure 5.4 depicts the same scenario as Figure 5.1, except that the node failures have been relocated to the network's centre. J and H are failed nodes. Figure 5.4 depicts the transition diagram in Figure 5.3.

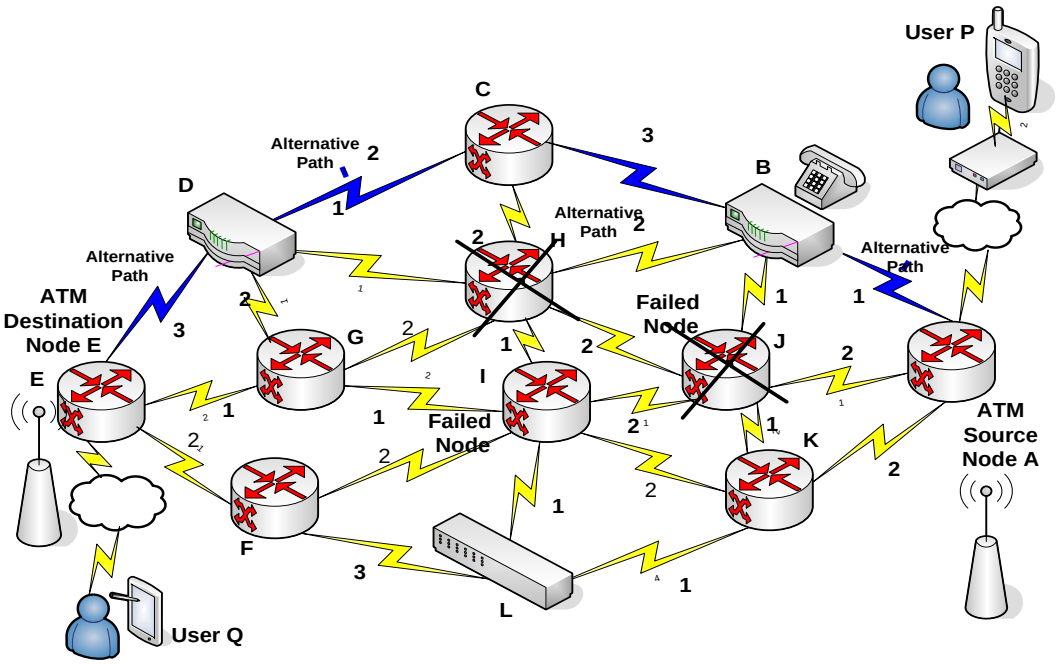

Figure 5.3: Node-node failure on voice transmission at centre.

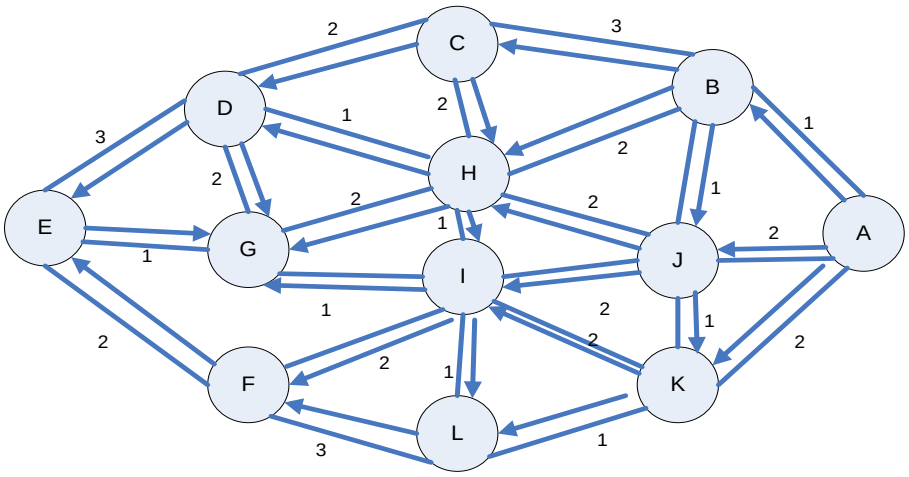

Figure 5.4: A state transition diagram depicts Figure 5.3

5.1.3 Investigation 1.1: multiple nodes failure at the network's edges.

This section discusses the analytical method of determining an alternate path to the node failures in Figure 5.5.

1ST Iteration: Starting state: A, B, J, and K: Potential State, Distances are generated at randomly

Consider equation 1:$\tau_0 = \frac{1}{n\,L_{nn}}$

Length AB, $\tau_0 = \frac{1}{12*1}$=0.080

Local update: Consider equation 2: $\tau_{ij}(t) = (1-\rho).\tau_{ij}(t) + \rho.\tau_0$; $\tau_{AB} = (1-0.1)*0.080 + 0.10*0.080 = 0.080$

Length AJ, $\tau_0 = \frac{1.0}{12*2}$=0.040; $\tau_{AJ} = (1.0-0.10)*0.040 + 0.10*0.040 = 0.040$

Length AK, $\tau_0 = \frac{1.0}{12*2}$=0.040; $\tau_{AK} = (1.0-0.10)*0.040 + 0.10*0.040 = 0.040$

Consider equation 3: $\eta_{AB} = \frac{1.0}{1.0} = 1.00,\ \eta_{AJ} = \frac{1.0}{2.0} = 0.50, \eta_{AK} = \frac{1.0}{2.0} = 0.50$

Consider equation 4: $w(A,B) = [\tau_{A,B}]^{\alpha}[\eta_{A,B}]^{\beta} = (0.08)^2(1)^1 = 0.0064$

$w(A,J)=[\tau_{A,J}]^{\alpha}[\eta_{A,J}]^{\beta}=(0.040)^2(0.50)^1=0.00080$

$w(A,K)=[\tau_{A,K}]^{\alpha}[\eta_{A,K}]^{\beta}=(0.040)^2(0.50)^1=0.00080$

Sum=0.00640+0.00080+0.00080=0.0180,

Probabilities: $P^k_{AB}=\frac{0.00640}{0.0080}$=0.80, $P^k_{AJ}=\frac{0.00080}{0.0080}$=0.10, $P^k_{AK}=\frac{0.0080}{0.00840}$=0.10

B is picked as probable device, the probability is the highest.

Next Iteration 2ND: B: Current state, C, H, J: Potential State

$L_k=(B\text{-}C)=3.0$, $L_k=(B\text{-}H)=2.0$, $L_k=(B\text{-}J)=1.0$

Consider equation 1: $\tau_0=\frac{1}{n\,L_{nn}}$: BC, $\tau_0=\frac{1}{12*3}$=0.030, Length= $\frac{1}{12*2}$=0.040

Length BJ, $\tau_0=\frac{1}{12*1}$=0.080

Local update: Consider equation 2: $\tau_{ij}(t)=(1-\rho).\tau_{ij}(t)+\rho.\tau_0$

$\tau_{BC}=(1.0-0.10)*0.030+0.10*0.030=0.030$;

Figure 5.5: Calculation of the ACS for the generation of alternate route

$\tau_{BH}=(1.0-0.10)*0.040+0.10*0.040=0.040;$
$\tau_{BJ}=(1.0-0.10)*0.080+0.10*0.080=0.080$
Consider equation 3:
$\eta_{BC}=\frac{1}{3}=0.30$ $\eta_{BH}=\frac{1}{2}=0.50$, $\eta_{BJ}=\frac{1}{1}=1.0$
Consider equation 4: $w(B,C)=[\tau_{BC}]^{\alpha}[\eta_{BC}]^{\beta}=(0.03)^2(0.3)^1=0.00027$
$w(B,H)=[\tau_{BH}]^{\alpha}[\eta_{BH}]^{\beta}=(0.04)^2(0.5)^1=0.0008;$
$w(B,J)=[\tau_{BJ}]^{\alpha}[\eta_{BJ}]^{\beta}=(0.08)^2(1)^1=0.0064$
Sum=0.00027+0.0008+0.0064=0.00747
Probabilities: $P_{BC}^{k}=\frac{0.00027}{0.00747}=0.36$, $P_{BH}^{k}=\frac{0.0008}{0.00747}=0.11$, $P_{BJ}^{k}=\frac{0.0064}{0.00747}=0.86$
J is probable, its probability is the highest.
3RD Iteration: J: Current state, H, I, K: Potential State
$L_k=(J-H)=2, L_k=(J-I)=2$, $L_k=(J-K)=1$
Using equation 1: $\tau_0=\frac{1}{n\,L_{nn}}$: Length JH, $\tau_0=\frac{1}{12*2}=0.040$, Length JI, $\tau_0=\frac{1}{12*2}=0.040$,
$For\ distance\ JK,\ \tau_0=\frac{1}{12*1}=0.080$
Local update
Consider equation 2: $\tau_{ij}(t)=(1.0-\rho).\tau_{ij}(t)+\rho.\tau_0$
$\tau_{JH}=(1.0-0.10)*0.04+0.10*0.04=0.04;$ $\tau_{JI}=(1.0-0.10)*0.040+0.10*0.040=0.040$
$\tau_{JK}=(1.0-0.10)*0.080+0.10*0.080=0.080$
Consider equation 3: $\eta_{JH}=\frac{1}{2}=0.5$ $\eta_{JI}=\frac{1}{2}=0.50$, $\eta_{JK}=\frac{1}{1}=1.0$
Consider equation 4: $w(J,H)=[\tau_{JH}]^{\alpha}[\eta_{JH}]^{\beta}=(0.04)^2(0.5)^1=0.0008$
$w(J,I)=[\tau_{JI}]^{\alpha}[\eta_{JI}]^{\beta}=(0.04)^2(0.5)^1=0.0008;$
$w(J,K)=[\tau_{J,K}]^{\alpha}[\eta_{J,K}]^{\beta}=(0.08)^2(1)^1=0.0064$
Sum=0.0008+0.0008+0.0064=0.008
Probabilities: $P_{JH}^{k}=\frac{0.0008}{0.008}=0.1$, $P_{JI}^{k}=\frac{0.0008}{0.008}=0.1$, $P_{JK}^{k}=\frac{0.0064}{0.008}=0.8$
Node K is selected as next node
4th Iteration: Current state: K
Potential State: L, I: $L_k=(K-L)=1$, $L_k=(K-I)=2$
Using equation 1: $\tau_0=\frac{1}{n\,L_{nn}}$: $For\ distance\ KL,\ \tau_0=\frac{1}{12*1}=0.08$,
distance KI, $\tau_0=\frac{1}{12*2}=0.04$
Local update
Consider equation 2: $\tau_{ij}(t)=(1-\rho).\tau_{ij}(t)+\rho.\tau_0$: $\tau_{KL}=(1.0-0.10)*0.080+0.10*0.08=0.08$
$\tau_{KI}=(1-0.1)*0.04+0.1*0.04=0.04$
Using equation 3: $\eta_{KL}=\frac{1}{1}=1$, $\eta_{KI}=\frac{1}{2}=0.5$
Using equation 4: $w(K,L)=[\tau_{KL}]^{\alpha}[\eta_{KL}]^{\beta}=(0.08)^2(1)^1=0.0064$
$w(K,I)=[\tau_{KI}]^{\alpha}[\eta_{KI}]^{\beta}=(0.04)^2(0.5)^1=0.0008$
Sum=0.0064+0.0008=0.0072;
Probabilities: $P_{KL}^{k}=\frac{0.0064}{0.0072}=0.89$, $P_{KI}^{k}=\frac{0.0008}{0.0072}=0.1$; Node L is selected as next node.

Figure 5.5: The ACS calculation for producing alternate route is still ongoing

5^{th} Iteration Current state: L

Potential State: F, I

$L_k=(L\text{-}F)=3$, $L_k=(L\text{-}I)=1$

Using equation 1: $\tau_0=\frac{1}{n\,L_{nn}}$: For distance LF, $\tau_0=\frac{1}{12*3}=0.03$, distance LI, $\tau_0=\frac{1}{12*1}=0.08$

Local update

Consider = equation 2: $\tau_{ij}(t)=(1\text{-}\rho).\tau_{ij}(t)+\rho.\tau_0$: $\tau_{LF}=(1.0\text{-}0.10)*0.030+0.10*0.030=0.030$

$\tau_{LI}=(1.0\text{-}0.10)*0.080+0.1*0.08=0.08$

Using equation 3: $\eta_{LF}=\frac{1}{3}=0.3$, $\eta_{LI}=\frac{1}{1}=1.0$

Consider equation 4:

$w(L,F)=[\tau_{LF}]^{\alpha}[\eta_{LF}]^{\beta}=(0.03)^2(0.3)^1=0.00027$;

$w(L,I)=[\tau_{LI}]^{\alpha}[\eta_{LI}]^{\beta}=(0.08)^2(1)^1=0.0064$

Sum=0.00027+0.0064=0.00667

$P^k_{LF}=\frac{0.00027}{0.00667}=0.04$, $P^k_{LI}=\frac{0.0064}{0.00667}=0.96$

I is chosen, its probability is the highest and F is a failed device.

Current state: I, Potential State: F, G

$L_k=(I\text{-}F)=2$, $L_k=(I\text{-}G)=1$

Consider equation 1: Length IF, $\tau_0=\frac{1}{12*2}=0.08$, Length IH, $\tau_0=\frac{1}{12*1}=0.08$

Local update

Consider equation 2: $\tau_{IF}=(1.0.0\text{-}0.10)*0.08+0.10*0.03=0.08$

$\tau_{IG}=(1.0\text{-}0.10)*0.040+0.10*0.040=0.040$

Consider equation 3:

$\eta_{IF}=\frac{1}{2}=0.50$ $\eta_{IG}=\frac{1}{1}=1$

Using equation 4:

$w(I,F)=[\tau_{LF}]^{\alpha}[\eta_{LF}]^{\beta}=(0.08)^2(0.5)^1=0.0032$

$w(I,G)=[\tau_{LI}]^{\alpha}[\eta_{LI}]^{\beta}=(0.04)^2(1)^1=0.0016$

Sum=0.0032+0.0016=0.0048

$P^k_{IF}=\frac{0.0032}{0.0048}=0.67$, $P^k_{IG}=\frac{0.0016}{0.0048}=0.33$

F is a failed node, G is selected as next node and the destination node is E

Update Trail: A, B, J, K, L, I, G, E

$P^k_{LF}=\frac{0.00027}{0.00667}=0.04$, $P^k_{LI}=\frac{0.0064}{0.00667}=0.96$

'I' has the highest probability and it is selected as next node and F is a failed node.

I: Current state, F, G: Potential State

$L_k=(I\text{-}F)=2$, $L_k=(I\text{-}G)=1$

Consider equation 1: Length IF, $\tau_0=\frac{1}{12*2}=0.080$, Length IH, $\tau_0=\frac{1}{12*1}=0.080$

Local update: Consider equation 2: $\tau_{ij}(t)=(1\text{-}\rho).\tau_{ij}(t)+\rho.\tau_0$

$\tau_{IF}=(1.0\text{-}0.10)*0.080+0.10*0.030=0.080$

$\tau_{IG}=(1.0\text{-}0.10)*0.040+0.10*0.040=0.040$

Consider equation 3:

$\eta_{IF}=\frac{1}{2}=0.50$ $\eta_{IG}=\frac{1.0}{1.0}=1.0$

Figure 5.5: The ACS Calculation for Generating Alternative paths is still ongoing.

Consider equation 4:

$w(I,F)=[\tau_{LF}]^{\alpha}[\eta_{LF}]^{\beta}=(0.08)^2(0.5)^1=0.0032$

$w(I,G)=[\tau_{LI}]^{\alpha}[\eta_{LI}]^{\beta}=(0.04)^2(1)^1=0.0016$

Sum=0.0032+0.0016=0.0048

$P_{IF}^{k}=\frac{0.0032}{0.0048}=0.67$, $P_{IG}^{k}=\frac{0.0016}{0.0048}=0.33$

F is a failed node, G is selected as next node and destination is E

Updated Trail: A, B, J, K, L, I, G, E

Current state: I, Potential State: F, G

$L_k=(I\text{-}F)=2$, $L_k=(I\text{-}G)=1$

Consider equation 1: Length IF, $\tau_0=\frac{1}{12*2}=0.08$, Length IH, $\tau_0=\frac{1}{12*1}=0.08$

Local update

Consider equation 2: $\tau_{IF}=(1.0.0\text{-}0.10)*0.08+0.10*0.03=0.08$

$\tau_{IG}=(1.0\text{-}0.10)*0.040+0.10*0.040=0.040$

Consider equation 3:

$\eta_{IF}=\frac{1}{2}=0.50$ $\eta_{IG}=\frac{1}{1}=1$

Using equation 4:

$w(I,F)=[\tau_{LF}]^{\alpha}[\eta_{LF}]^{\beta}=(0.08)^2(0.5)^1=0.0032$

$w(I,G)=[\tau_{LI}]^{\alpha}[\eta_{LI}]^{\beta}=(0.04)^2(1)^1=0.0016$

Sum=0.0032+0.0016=0.0048

$P_{IF}^{k}=\frac{0.0032}{0.0048}=0.67$, $P_{IG}^{k}=\frac{0.0016}{0.0048}=0.33$

F is a failed node, G is selected as next node and the destination node is E

Update Trail: A, B, J, K, L, I, G, E

$P_{LF}^{k}=\frac{0.00027}{0.00667}=0.04$, $P_{LI}^{k}=\frac{0.0064}{0.00667}=0.96$

I has the highest probability and it is selected as next node and F is a failed node.

I: Current state, F, G: Potential State

$L_k=(I\text{-}F)=2$, $L_k=(I\text{-}G)=1$

Consider equation 1: Length IF, $\tau_0=\frac{1}{12*2}=0.080$, Length IH, $\tau_0=\frac{1}{12*1}=0.080$

Local update

Consider equation 2: $\tau_{ij}(t)=(1\text{-}\rho).\tau_{ij}(t)+\rho.\tau_0$

$\tau_{IF}=(1.0\text{-}0.10)*0.080+0.10*0.030=0.080$

$\tau_{IG}=(1.0\text{-}0.10)*0.040+0.10*0.040=0.040$

Consider equation 3:

$\eta_{IF}=\frac{1}{2}=0.50$ $\eta_{IG}=\frac{1.0}{1.0}=1.0$

Consider equation 4:

$w(I,F)=[\tau_{LF}]^{\alpha}[\eta_{LF}]^{\beta}=(0.08)^2(0.5)^1=0.0032$

$w(I,G)=[\tau_{LI}]^{\alpha}[\eta_{LI}]^{\beta}=(0.04)^2(1)^1=0.0016$

Sum=0.0032+0.0016=0.0048

$P_{IF}^{k}=\frac{0.0032}{0.0048}=0.67$, $P_{IG}^{k}=\frac{0.0016}{0.0048}=0.33$

F is a failed node, G is selected as next node and destination is E

Updated Trail: A, B, J, K, L, I, G, E

Figure 5.5: The ACS Calculation for Generating Alternative paths is still ongoing

Table 5.1: A full cycle probability update.

Current state	A	B	C	J	K	L	I	G	H	F	E
A	0.80	0.62	0.00	0.08	0.31	0.00	0.00	0.00	0.00	0.00	0.00
B	0.00	0.00	0.36	0.86	0.00	0.00	0.00	0.00	0.11	0.00	0.00
J	0.00	0.00	0.00	0.00	0.80	0.00	0.1.	0.00	0.10	0.00	0.00
K	0.00	0.00	0.00	0.00	0.00	0.89	0.11	0.00	0.00	0.00	0.00
L	0.00	0.00	0.00	0.00	0.00	0.00	0.96	0.00	0.00	0.04	0.00
I	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.33	0.00	0.67	0.33

Terminating state, and ant has traversed all states=E

5.1.4 The bandwidth needed for transferring the packet in Figure 5.5

Consider equations 10 and 11: the size of voice message is 500-bytes and IP header is 20bytes, the real message size$= 500\text{Bytes} - 20\text{ Bytes} = 480\text{ Bytes}$. It will take the packet to be transmitted from transmitter to receiver $= 5 \times 8 = 40$ sec. With the path A-B-J-K-L-I-G-E, The length= 7m.

$$\text{Speed} = \frac{7\text{ meters}}{40\text{ seconds}} = 0.1750\text{ meters/seconds}$$

$$\text{Delay} = \frac{7\text{ meters}}{0.1750\text{meters/seconds}} = 40\text{ seconds.}$$

Consider equation 7, $a = 8 + 7 = 15$, α and β are assumed to be 1

$$B_{Req} = \frac{W}{D-a} = \frac{480}{40-15} = \frac{480}{25} = 19.2\text{Bytes/s.}$$

5.1.5 Investigation 1.2: Multiple node failures at WATM networks centre

Figure 5.6 presents the analysis of finding the alternative path to the failed nodes in Figure 5.4

1st Iteration:
A: Starting State
B, J, K: Potential state
The starting state and possibilities state of Figures 5.2 and 5.4 are the same; the same computation as in Figure 5.2's first iteration is applicable for Figure 5.8. Node B is chosen as another node because it is the most probable.
Last Iteration
3rd Iteration: C: Current State
Potential State: D, H
$L_k=(C\text{-}D)=2$, $L_k=(C\text{-}H)=2$
Consider equation 1: Length CD, $\tau_0=\frac{1}{12*2}=0.040$, Length CH, $\tau_0=\frac{1}{12*2}=0.040$
Local update
Consider equation 2: $\tau_{ij}(t)=(1\text{-}\rho).\tau_{ij}(t)+\rho.\tau_0$
$\tau_{CD}=(1.0-0.10)*0.040+0.10*0.040=0.040$
$\tau_{CH}=(1.0\text{-}0.10)*0.040+0.10*0.040=0.040$
Consider equation 3:
$\eta_{CD}=\frac{1}{2}=0.50$, $\eta_{CH}=\frac{1}{2}=0.50$,
Consider equation 4:
$w(C,D)=[\tau_{KL}]^{\alpha}[\eta_{KL}]^{\beta}=(0.04)^2(1)^1=0.0008$
$w(C,H)=[\tau_{KI}]^{\alpha}[\eta_{KI}]^{\beta}=(0.04)^2(0.5)^1=0.0008$
Total=0.00080+0.00080=0.00160
$P^k_{CD}=\frac{0.00080}{0.00160}=0.50$, $P^k_{CH}=\frac{0.00080}{0.00160}=0.50$
Failed node is H, H cannot be chosen.
The next node to be selected is node D.
Updated Trail: A, B, C, D, and E.

Figure 5.6: ACS calculation for generating alternative path

The routing path produced is A–B–C–D–E. Table illustrates the probability distribution of various nodes chosen.

Table 5.2: A full cycle probability update

Current state	A	B	C	D	E	J	K	H
A	0.00	0.62	0.00	0.00	0.00	0.08	0.31	0.11
B	0.00	0.00	0.36	0.00	0.00	0.86	0.00	0.00
C	0.00	0.00	0.00	0.50	0.00	0.00	0.00	0.50
D	0.00	0.00	0.00	0.00	0.89	0.00	0.00	0.00

The state is being terminated, and the ant has passed through all of them=E

5.1.6 The bandwidth needed for transferring the packet in Figure 5.6

$$B_{Req} = \frac{W}{D-a} = \frac{480}{25-14} = \frac{480}{11} = 43.64 \text{Bytes/s}.$$

5.1.7 Section summary

This study demonstrates how an ACS procedure is investigated in order to accomplish WATM network resilience. The goal of this study is to identify existing multiple failure systems in order to identify gaps and address those gaps by suggesting a WATM resilience concept swarm - Based. The new model's analytical solutions were made clear in Figures 5.5 and 5.6. The Investigational procedure outlines the various failure locations in WATM networks (e.g. Failures at the edges and at the center of networks). The suggested resilience method, depicted in Figures 5.1 and 5.3, could be used by any telecoms setup that relies on WATM networks as its spine to resolve both single and multiple failures. At the conclusion of the study, the analytical solution of the ACS concept was being used to produce the alternate route whenever the main route failed. Whenever the failure was moved to the network's edge, as seen in Figure 5.1, the alternate solution path A –B – J –K – L – I – G – E was produced, while when these were moved to the network's center, as seen in Figure 5.3, the alternate solution path A –B – C – D – E was obtained. For every flow path, the bandwidth needed to submit a packet was determined. With such a system already in place, the platform will continue to function even if a node fails. Scientific investigations should concentrate on additional multiple failures which are not considered in the study. The model used in this work can be improved further by expanding the state space.

5.2 INVESTIGATION 2: ACS ON THE SURVIVAL OF WIRELESS NETWORKS NODE-NODE FAILURES FOR NEAR OPTIMAL MESSAGE ROUTING

5.2.1 Introduction

This study creates a capacity efficient ACS survivability model based on fast restoration to quickly resolve node-node failures issue and improve service.

A wireless telecommunications network is an intricate system of transmitting hubs. There is no such thing as a single network; rather, there is a hierarchy of networks [95]. In the event that a node or a link fails, it is recommended that connectivity in a wireless network be rerouted on an alternate route. The resilience issue is exceedingly complicated in the perspective of this hierarchy.

Wireless networks that span the globe are prone to a variety of failures, including component failures and connectivity failure. Failures prompted by a catastrophic event are those that can cause a wide-area outage and impair network efficiency [94]. A wireless network failure can occur for a variety of factors, such as the loss of a node or a connection. Unintentional connector breaks, node glitches, design flaws, natural catastrophes (e.g., burn), and mishandling are all common causes of failure. Wireless network is vulnerable to numerous of failures, from fibre slashing and synchronous equipments failure to simultaneous failures that can hinder a massive component [96].

In the literature, various methods for failure restoration have been proposed, with differences in the network models used. The following gaps listed have been identified as the basis for motivation/improvement of emerging survivability techniques:

- Node-node failures in wireless network traffic-flows that require extra consideration.
- Spare capacity distribution issues with node-node failures that need to be addressed quite thoroughly to maintain a stable network.

In an attempt to settle failures of motivating properties such as foraging and self-organisation, it was revealed that the capacity efficient ACS approach meets the route discovery specifications of wireless networks. With the help of a proposed ant-based method, optimised paths can be suggested with reduced latency, and the problem of stagnant growth can be solved. These will be the pillars of motivation. Several aspects of ant colony behaviour, namely, job scheduling, classification of its most suitable, and collaborative mobility, motivated scholars to use the capacity efficient ACS. Despite the fact that only one and multi

failures are the most common forms of failings in a wireless network, protecting against these two types of failures should not be overlooked. Failure of a node for a particular network involves both the failure of the source or recipient of the message and the failure of an access point. A link will be isolated if its transmitter/receiver node fails, however, an interference in system caused by a failed desired location cell can be recovered through possessing redundancy at a distant location. The application of a capacity-efficient Ant Colony System (ACS) model in network failure revival is a relatively new development.

The purpose of this section is to establish a capacity-efficient ACS resilience method for resolving wireless network node-node failures. The following points are the major contributions of this section:

- The establishment of a new suggested capacity efficient ACS system which could help wireless network clients in surviving multiple node-node failures.
- In terms of bandwidth requirement to reroute packets, investigations conducted in finding optimised routes together generated knowledge in instances spanning from no failure to multiple failures.

5.2.2 Investigational setup

The following tools are used in developing the proposed model: Java, NS-2 and Matlab.
Java is used in analytical scenario simulation for the following reasons:

- Java programming language is an object-oriented programming language that uses bytecode instructions executed by a stack-based virtual machine and is one of the most popular programming languages used in enterprise development. Since Java is built on bytecode rather than assembly language, it has several advantages. For example, code written once can be executed on multiple platforms, assuming a virtual machine implementation. Java is very portable. As long as a computer has a Java interpreter, the same Java application will run identically on any computer, regardless of hardware or operating system [97].
- Aside from portability, another significant advantage of Java is its set of security features, which protect a PC running a Java program not only from problems caused by erroneous code but also from malicious programs such as viruses.

NS-2 (Network Simulator Version-2) is a free and open-source discrete event simulator designed specifically for network simulation. NS-2 was developed and licensed for use under the General Public License in 1996-97. (GNU) [98].

- It supports both wired and wireless simulation of functions and protocols such as TCP, UDP, and others. The REAL simulator ideology inspired the development of NS-2.
- NS-2 is a popular simulator because of its flexibility and modularity. It is written in two major programming languages: C++ and Object-Oriented Tool Command Language.

It is believed that Matrix laboratory (MATLAB) supports a variety of data link layer simulation controls,

- It can provide users with modeling tools that can be customised.
- It is highly adaptable and can take full advantage of MATLAB's powerful programming capabilities to improve simulation performance [99].

Investigations 2.1–2.6 show nodes labeled A through to T and they conducted at various locations of varying numbers of node failures. In these investigations, the nodes representing network devices, the line connecting one node to another symbolises a link, and the failed vertices, as well as the generated optimal alternatives route, are stated in the figure labels. The vast majority of investigations have been run of varying numbers of node failure. The most commonly used investigation instances are instances A and B. In investigations 2.1 and 2.5, results, tables and figures are displayed, whereas only the narrative investigational tests 2.2–2.4 and 2.6 are shown. The outcomes of these experiments clarify sub-objective 2

In every experiment, the network is setup and the simulation experiments generate prototypes of experiments where results are generated

The motivating factors for selecting a specific number of nodes in a network are as follows:

- Throughput is one of the determinants for selecting the number of nodes in a network. If the network's throughput is low, more nodes will be required to increase the percentage of throughput. Low throughput lowers network efficiency.
- Node life span is another consideration when determining the number of nodes in a network. If there are a limited number of nodes in a densely populated area, the network's life span will be reduced, causing network malfunctioning and increasing transmission delay.
- Another factor to consider when determining the number of nodes in a network is the subscriber base. The size of coverage also influences the number of nodes in a

network. Congestion occurs when there are fewer nodes in a network in a densely populated area.

5.2.3 Rerouting with 20 nodes network

Voice packets are transferred from node A to E. The transition diagram for the investigational setup's twenty-node network is shown in Figure 5.7. Link costs are generated randomly.

Paths are computed in a randomised manner each time an information packet needs to be sent in the randomised path routing method, so that the set of routes taken by various shares of different packets changes over time. As a result, a large number of routes for each sender and receiver can potentially be generated [100],[101]. However, the algorithm ensures that the randomly generated routes are as dispersed as possible, i.e., the routes are geographically separated as far as possible so that they are unlikely to pass through a black hole at the same time. Since selecting a sample requires the use of randomly generated numbers, simple random sampling is used in this study. More specifically, it necessitates the creation of a sampling frame, which is a list or database of all members of a population.

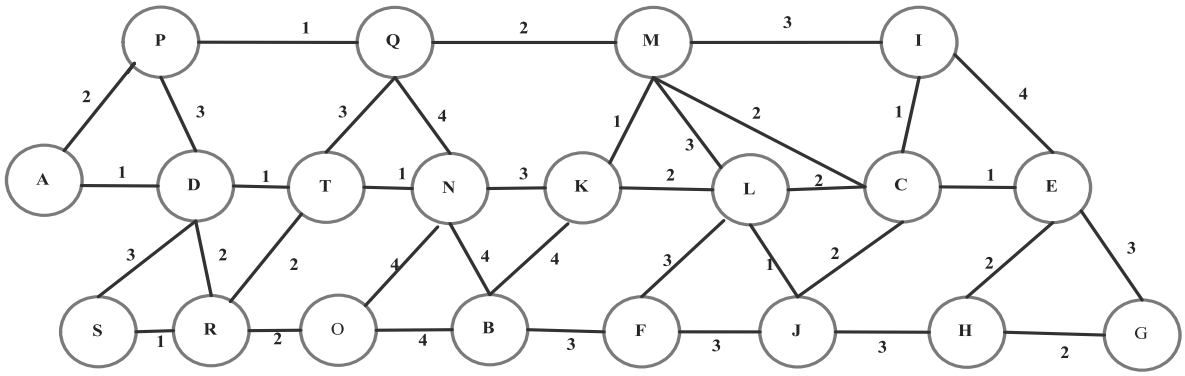

Figure 5.7: A twenty-node (20) network is represented by a transition diagram

Table 5.3 shows the parametric requirements for the proposed system throughout investigations 2.1–2.21.

Table 5.3: ACS parametric specification

ACO Properties	Type of ACO	Pheromone Coefficient β	Heuristic Coefficient α	Rate of Evaporation ρ	Distance d (m)	Transmission Time to 1st node(seconds)	Message size (Bytes)
Characteristics	ACS	2	3	0.010	Variable	0.0050	Range variability

5.2.4 Investigation 2.1: Routing in the absence of a node failure

Figure 5.8 depicts a 750-byte voice packet sent from transmitting node A to recieving node E.

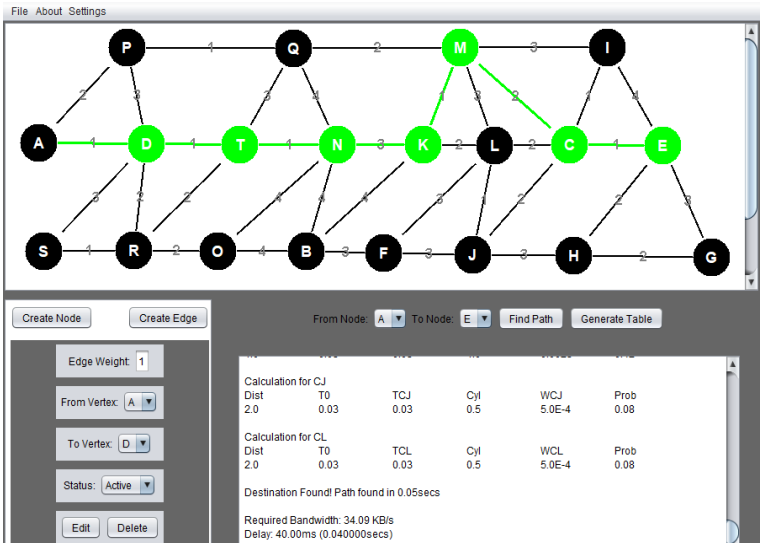

Figure 5.8: Wireless network without node failure

Figure 5.8 shows a voice message that takes 0.050s to get to its target. The bandwidth required to transfer data from transmitter to receiver is 34.10-Kbytes/s. The transmission delay is 0.04s. A–D–T–N–K–M–C–E is the produced optimal route. Table 5.4 depicts the probability distributions of chosen nodes in Figure 5.8 that are on the near optimal path. Table 5.5 displays the pheromone concentration at each node along the optimal path depicted in Figure 5.8.

Table 5.4: The ACS routing probability distributions

Current State	D	P	T	S	N	Q	B	M	L	C	I	K	E
A	0.831	0.173	0	0	0	0	0	0	0	0	0	0	0
D	0	0.03	0.78	0.03	0	0	0	0	0	0	0	0	0
T	0	0	0	0	0.81	0.03	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0	0	0	0	1.00	0
K	0	0	0	0	0	0	0.03	0.81	0	0	0	0	0
M	0	0	0	0	0	0.42	0	0	0	0.42	0.08	0	0
C	0	0	0	0	0	0	0	0	0.08	0	0	0	0.42

Table 5.5: A full cycle pheromone update

Current State	D	P	T	S	N	Q	B	M	L	C	I	K	E
A	0.050	0.030	0	0	0	0	0	0	0	0	0	0	0
D	0	0.02	0.05	0.02	0	0	0	0	0	0	0	0	0
T	0	0	0	0	0.05	0.02	0	0	0	0	0	0	0
N	0	0	0	0	0	0	0	0	0	0	0	0.02	0
K	0	0	0	0	0	0	0.02	0.05	0.16	0	0	0	0
M	0	0	0	0	0	0.03	0	0	0	0.03	0.02	0	0
C	0	0	0	0	0	0	0	0	0.03	0	0	0	0.05

5.2.5 Investigation 2.2: Rerouting due to a node failure (Failed Node: D)

Investigation 2.2 depicts an investigation in which a packet is rerouted over a telecommunications network after a node fails at the network's edge (Failed node: D).

A 550-byte voice message has been configured for rerouting from transmitting node A to receiving node E. The voice packet gets to the receiver node in 0.060s. The needed bandwidth to transfer data from transmitter to receiver is 25.00 Kbytes/s. There is a transmission delay of 0.0454s. A–P–Q–M–K–L–J– C–E is the generated path.

In investigation 2.1, there is no node failure, so adequate bandwidth is made available to transfer message, as opposed to investigation 2.2, which has a failure. Transmission is also quicker in investigation 2.1 than in investigation 2.2 due to the lower network latency in investigation 2.1 due to the increased path cost value. Table 5.8 displays the full results.

5.2.6 Investigation 2.3: Rerouting with 2-node failure at the network's edge and center (Failed Nodes: M and D)

A 600-byte voice packet is scheduled to be rerouted from transmitter node A to receiver node E for the packet to reach its destination. The bandwidth expected to transfer from sender to the receiver equals 27.271Kbytes/s.. The transmission delay is 0.0502 s. A–P–Q–T–N–K–L–J–C–E is the generated path. The failed nodes are M and D.

Rerouting is observed to be quicker in investigation 2.2 than investigation 2.3 due to the obvious low transmission delay. The large voice message necessitated the use of more bandwidth in investigation 2.3. Table 5.8 displays the comprehensive data.

5.2.7 Investigation 2.4: Rerouting when 3-nodes fail

Investigation 2.4 depicts the design to simulate outcome of rerouting a voice packet on the network with the failed 3-node at the network's edge and centre.

(A) Instance A: 3-Node failures at random (Node Failures: M, O and K)

A 350-byte voice message is configured in investigation 2.4 for rerouting from transmitter node A to receiver node E. The message got to receiver at 0.071s. The bandwidth needed to send from transmitter to receiver equals 15.222 Kbytes/s. There is a 0.0509s delay. The alternate route produced equals A–D–T – N – B – F – L – J – C – E.

The path cost of the alternative path created in investigation 2.4(A) is higher than that of investigation 2.3, which contributes to the longer transmission delay in investigation 2.4. (A). As a result, rerouting in investigation 2.4(A) is slower than in investigation 2.3; comprehensive results are shown in Table 5.8.

(B) Instance B: The result of 3-node failures in the network's centre (Failed Node: N, K and L)

In investigation 2.4(B), a 650-byte voice message is sent from transmitting node A to receiving node E for rerouting. The packet got to its target node in 0.0742s. The bandwidth needed to transfer data from transmitter to receiver is 27.082 Kbytes/s. There is a 0.0502 second delay. The alternate route found is A–D–T–R–O–B–F–J–H–E.

Rerouting time is longer in investigation 2.4(B) whereas it is lower in investigation 2.4(A) because the path cost in investigation 2.4(B) is higher, which keeps increasing transmission delay (refer Table 5.8 for such trend).

5.2.8 Investigation 2.5: Rerouting with randomised 4-node failures (Failed Nodes: D, M, K, and H)

Figure 5.9 depicts the network rerouting of a voice packet with four randomised node failures. A 480-byte packet is set for rerouting from transmitting node A to receiving node E.

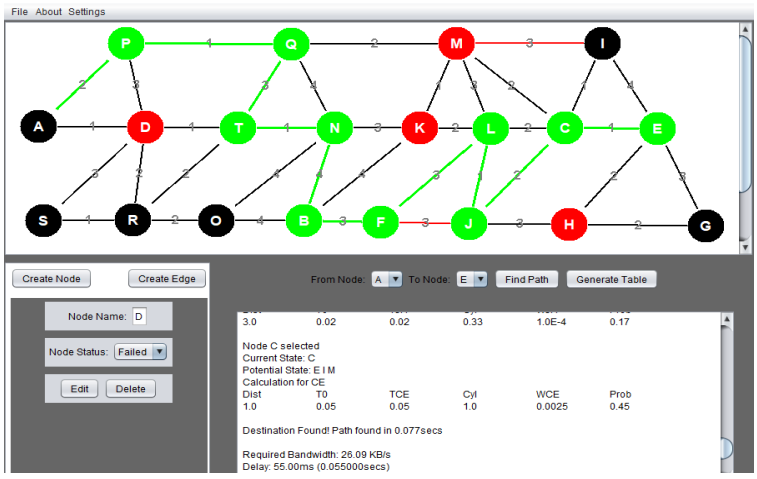

Figure 5.9: Wireless network with 4-node failures at random

Figure 5.9 shows a voice message that takes 0.077s to get to its target node. The bandwidth needed to route on the transmitter to receiver is 26.091Kbytes/s. There is a 0.0550s delay. The generated path: A–P–Q–T–N–B–F–L–J–C–E. Table 5.6 shows the ACS routing probability distributions of selected nodes in Figure 5.9 that are on the optimal path. Table 5.7 shows the pheromone concentration at each node along the optimal path depicted in Figure 5.9.

Table 5.6: The ACS routing probability distribution

Current State	P	Q	T	N	B	F	L	J	C	E
A	0.17	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P	0.00	0.96	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Q	0.00	0.00	0.17	0.00	0.00	0.00	0.00	0.00	0.00	0.00
T	0.00	0.00	0.00	0.45	0.00	0.00	0.00	0.00	0.00	0.00
N	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
B	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
F	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
L	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.69	0.00	0.00
J	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.83	0.00
C	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.45

Table 5.7: A full cycle pheromone update

Current State	P	Q	T	N	B	F	L	J	C	E
A	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P	0.00	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Q	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00
T	0.00	0.00	0.00	0.05	0.00	0.00	0.00	0.00	0.00	0.00
N	0.00	0.00	0.00	0.00	0.05	0.00	0.00	0.00	0.00	0.00
B	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00
F	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00
L	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.05	0.00	0.00
J	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00
C	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.05

Rerouting is slower in investigation 2.5 due to the higher delay value generated 2.4(B). Nevertheless, due to the various sizes of voice packets that are transferred, varying bandwidths are used.

5.2.9 Investigation 2.6: Rerouting with randomised 5-node failures (Failed Nodes: D, R, O, K, and M)

A 500-byte voice message is configured for rerouting from transmitting node A to receiving node E in investigation 2.6. The packet gets to its target node in 0.081s. The bandwidth needed to transmit on transmitter to receiver equals 21.741Kbytes/s. There is a 0.06 second delay. The alternate route: A–P– Q–T–N–B–F–L–J– C–I–E.

The path cost of investigation 2.6's alternate route is greater than that of investigation 2.5, contributing to the longer transmission delay in investigation 2.6. As a result, rerouting in investigation 2.6 is slower than in investigation 2.5. The detailed results are shown in Table 5.8.

5.2.10 Measuring the proposed model's performance in investigations (2.1–2.6)

Table 5.8 summarises the results of various investigations conducted in different sized of voice packets transferred over the network with varying numbers of node failures.

Table 5.8: Performance analysis of the investigations (2.1 – 2.6)

Investigational Number	Packet Size(Bytes)	Failed Node number	Transmission Time (seconds)	The Bandwidth Required (Kbytes)	Delay (seconds)	Path Generated	Path cost
2.1	750	0	0.050	34.09	0.040	A – D – T – N – K – M – C – E	10
2.2	550	1	0.060	25.00	0.045	A – P – Q – M – K – L – J – C – E	12
2.3	600	2	0.064	27.27	0.050	A – P – Q – T – N – K – L – J – C – E	16
2.4A	350	3	0.070	15.22	0.050	A – D – T – N – B – F – L – J – C – E	17
2.4B	650	3	0.074	27.08	0.050	A – D – T – R – O – B – F – J – H – E	21
2.5	480	4	0.077	26.09	0.055	A–P– Q– T – N – B –F – L – J – C – E	21
2.6	500	5	0.080	21.74	0.060	A–P– Q– T– N – B –F– L– J – C– I –E	25

The solution to the optimization issue is depicted in Table 5.8. Investigations 2.1–2.2, show the outcomes of reduced path-cost obtained from the best alternative path produced, that reduces transmission time and delay values, resulting in rapid voice packet rerouting. The graphical patterns in Table 5.8 reveal the inherent knowledge in subsections 5.2.11–5.2.12.

5.2.11 Delay and transmission time in relation to failed node

The packet movement time and delay needed to send a packet across a network with multiple node failures is depicted in Figure 5.10 which depicts that whenever there is no vertices failure, the packet is delivered quickly and the propagation delay is very minimal. When 2-nodes fail, the transmission time increases, and thus the delay time increases due to the increasing size of the rerouted message. Transmission time and delay increase after 3-node failures due to the rising prevalence of node failure; rerouting becomes more difficult. Apart from 2-node and 3-node failures, in which the same time lag values were produced, transmission time and delay increase as node failure increases, such that the concentration of node failures is at the edge and centre in 2-node failures, thereby contributing to a longer delay.

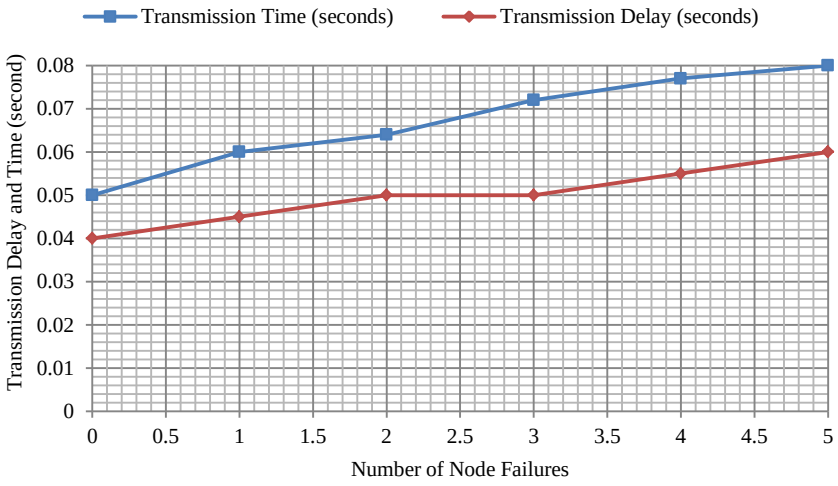

Figure 5.10: Delay & transmission time in relation to the number of node Failures.

Transmission delay is the amount of time required to push the entire packet's bits into the transmission line in a packet switching network, whereas transmission time is the amount of time from the beginning to the end of a message transmission in a telecommunications network. In the case of a digital message, it is the time between the first and last bits of the message leaving the transmitting node.

5.2.12 The needed bandwidth & path cost versus node failures.

When a network node fails, the required bandwidth to transfer the packet to its target node is adequate at 0-node failure, and the transmission path cost is smaller (because the path cost is lower, limited bandwidth will be used to transmit messages). Figure 5.11 depicts a path cost of a transmission path and the bandwidth needed to transfer a voice message. From 1-node failure to 5-node failures, the path cost and bandwidth rise, slowing down packet rerouting. As two investigations instances are run, the mean is obtained by plotting in investigation 2.4.

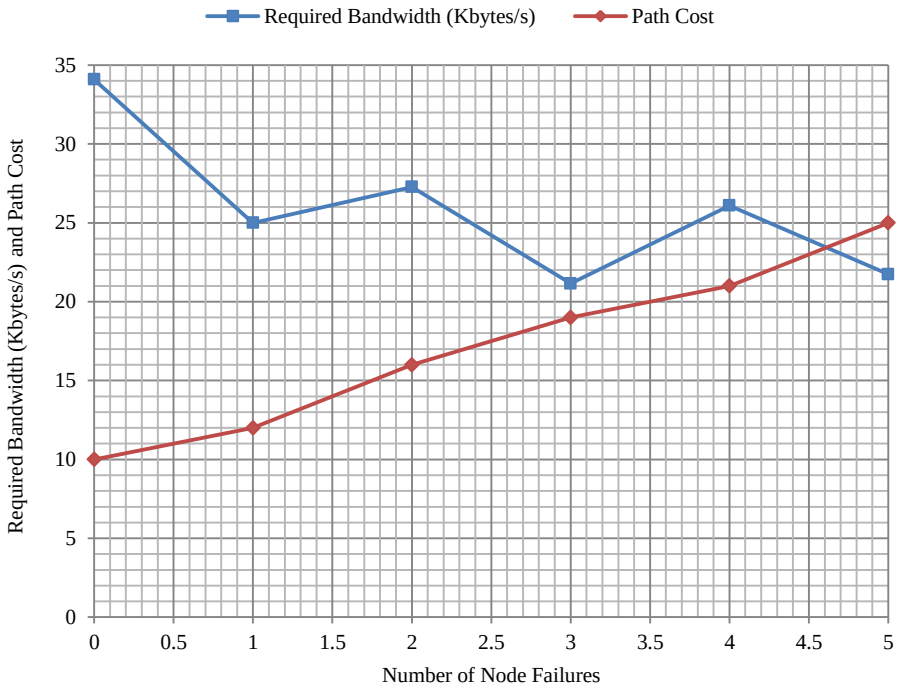

Figure 5.11: The needed bandwidth & path cost are weighed against node failure

5.2.13 Rerouting with a network of twenty-six nodes

As shown in investigations 2.7–2.13, nodes are labeled A through Z, & investigational studies are conducted at various positions of differing quantities of node failures. In these tests, the circles indicate network nodes, lines linking one node to the next depicting links, the failed nodes have been stated in the figure labels, as well as the generated alternate optimised

routes are indicated.. The vast majority of investigations are carried out for varying numbers of node failures. Investigation 2.9 includes two investigation instances: Instances A and B. Investigations 2.7 and 2.11 show figures, tables, and results, whereas investigations 2.8–2.10 and 2.12–2.13 only show descriptive results. Figure 5.12 depicts a transition diagram of a twenty-six node network of investigations 2.7–2.13. Link costs are generated randomly.

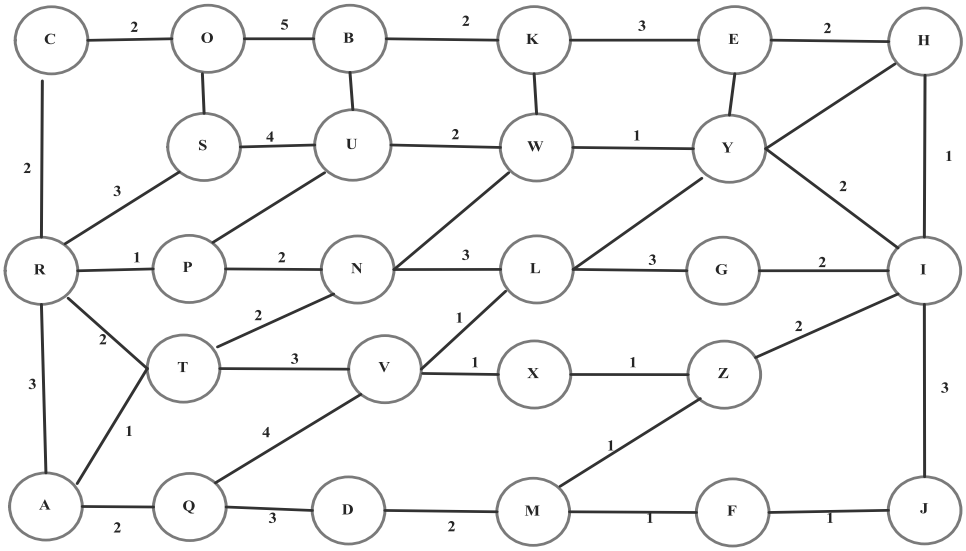

Figure 5.12: A wireless network with twenty-six nodes is represented by a transition diagram.

5.2.14 Investigation 2.7: Routing in the absence of a failed node

Figure 5.13 shows a 500-byte voice packet being sent from transmitter node A to receiver node E.

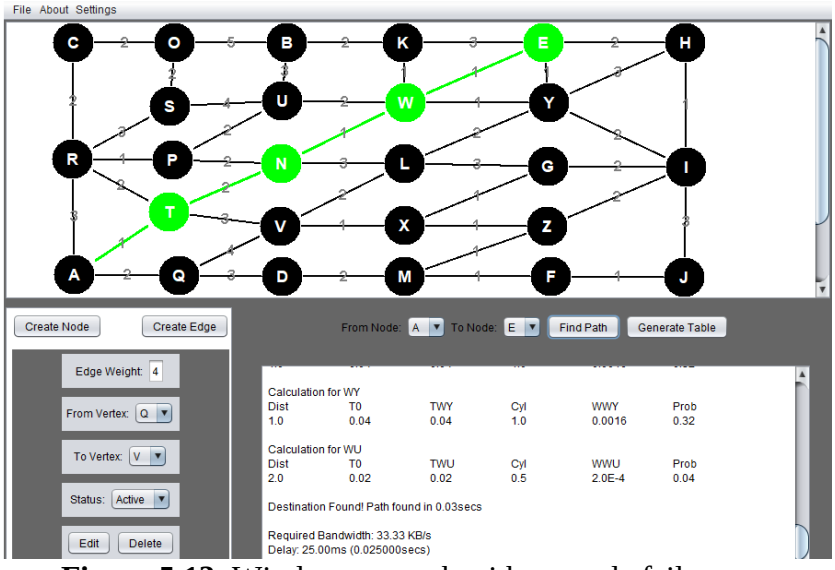

Figure 5.13: Wireless network without node failure

Figure 5.13 depicts the primary path generated when no nodes fail. The voice message takes 0.03 seconds to get to its target node using this routing. The needed bandwidth to transfer data from transmitter to receiver equals 33.33 Kbytes/s. It takes 0.0250 seconds to send a message. The best path produced to transfer the packet is A – T – N – W – E. Table 5.9 depicts the probability estimation of each node in Figure 5.13 that was chosen to produce best path. The content of Table 5.10 depicts the pheromone concentrations at each node along the rerouting passage as depicted in Figure 5.13. For inclusion in the routing path, nodes with higher pheromone concentrations are chosen.

Table 5.9: The ACS routing probability distribution

Current State	T	Q	N	W	P	E	K	Y	U
A	0.89	0.11	0.00	0.00	0.00	0.00	0.00	0.00	0.00
T	0.00	0.00	0.50	0.00	0.00	0.00	0.00	0.00	0.00
N	0.00	0.00	0.00	0.89	0.11	0.00	0.00	0.00	0.00
W	0.00	0.00	0.00	0.00	0.00	0.32	0.32	0.32	0.04

Table 5.10: A full cycle pheromone update

Current State	T	Q	N	W	P	E	K	Y	U
A	0.04	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00
T	0.00	0.00	0.04	0.00	0.00	0.00	0.00	0.00	0.00
N	0.00	0.00	0.00	0.04	0.02	0.00	0.00	0.00	0.00
W	0.00	0.00	0.00	0.00	0.00	0.04	0.04	0.04	0.02

5.2.15 Investigation 2.8: Rerouting due to a node failure (Node that failed: L)

Investigation 2.8 depicts the outcome of rerouting a packet through a wireless network with one node failure at the network's edge. A 550-byte voice packet has been configured for rerouting from transmitter node A to receiver node E. The packet gets to its target node at 0.0361 seconds. The needed bandwidth to push packet is 34.381Kbytes/s. There is a 0.0301 second delay. The generated path is A – T – N – W – K – E. In investigation 2.7, there is no node failure, so enough capacity is assigned for packet transfer, as opposed to investigation 2.8, which has a failure. Because of the shorter transmission delay in investigation 2.7, routing is also quicker than in investigation 2.8. Table 5.13 displays the detailed results.

5.2.16 Investigation 2.9: Rerouting with 2-node failures at the edge and centre of the network

Investigation 2.9 depicts the simulated outcome of rerouting a voice packet with 2-node failures at the network's edges and centre.

(A) Instance A: Failure at the edge and centre (Failed nodes: 'B' and 'N')

A packet of 450 Bytes has been configured to reroute from transmitting device A to receiver node E. The message takes 0.04s to reach its destination after this rerouting. The required bandwidth to retransmit to receiver is 23.68 Kbytes/s. 0.0351 seconds is the transferring time. A–T–R–P–U–W– E is the produced altermate route.

When investigation 2.9(A) and investigation 2.8 are compared, we discovered that the transferring delay of investigation 2.9(A) is greater transferring delay of investigation 2.8 as a result of node failures of investigation 2.9(A), making rerouting slower in investigation 2.9 (A). Furthermore, in investigation 2.8, there's really only 1-node failure; the transmission time is shorter than in investigation 2.9(A) (see Table 5.13 for more information).

(B) Instance B: As a result of 2-node failures in the centre (Failed nodes: N and W)

A 480-byte voice message is configured to be rerouted through a transmitting node A to receiving node E in investigation 2.9(B). Following this rerouting, the voice packet requires 0.046 seconds to get to its target node. The needed capacity to reroute to receiver is 26.674 Kbytes/s. It took 0.0401 seconds to send the message. A – T – R – P – U – B – K – E is the generated alternative path.

When investigation 2.9(B) is compared to investigation 2.9(A), it is discovered that the bandwidth used in investigation 2.9(A) to retransmit the packet is less than that of investigation 2.9(B). This is because the voice message rerouted in investigation 2.9 was larger in size. The transferring delay of investigation 2.9(B) is greater than the transmission delay in investigation 2.9(A), implying that the network's node failure intensity at the center does indeed have a significant impact on transmitting outage than failure concentration at the network's edge.

5.2.17 Investigation 2.10: Rerouting with 3-node failures (Failed nodes: P, B and N)

Investigation 2.10 dipicts the outcome of rerouting a packet with node failure at the network's edge and center. A 700-byte voice message is scheduled to be rerouted from transmitter node A to receiver node E.

The packet gets to its target node at 0.0521seconds. The needed bandwidth to transfer it to receiver is 35.00 Kbytes/s. There is a delay of 0.0454 seconds. A – T – R – C – O – S – U – W – E is the generated path. The delay in investigation 2.10 is greater than delay in

investigation 2.9(B), implying that rerouting is slower in investigation 2.10. The detailed results are shown in Table 5.13.

5.2.18 Investigation 2.11: Randomised 4-node failures (Failed nodes: C, O, L, and W)

Figure 5.14 depicts the outcome of rerouting a packet with randomised 4-node failures. A packet with a capacity of 800-bytes is rerouted from transmitting node A to receiving node E.

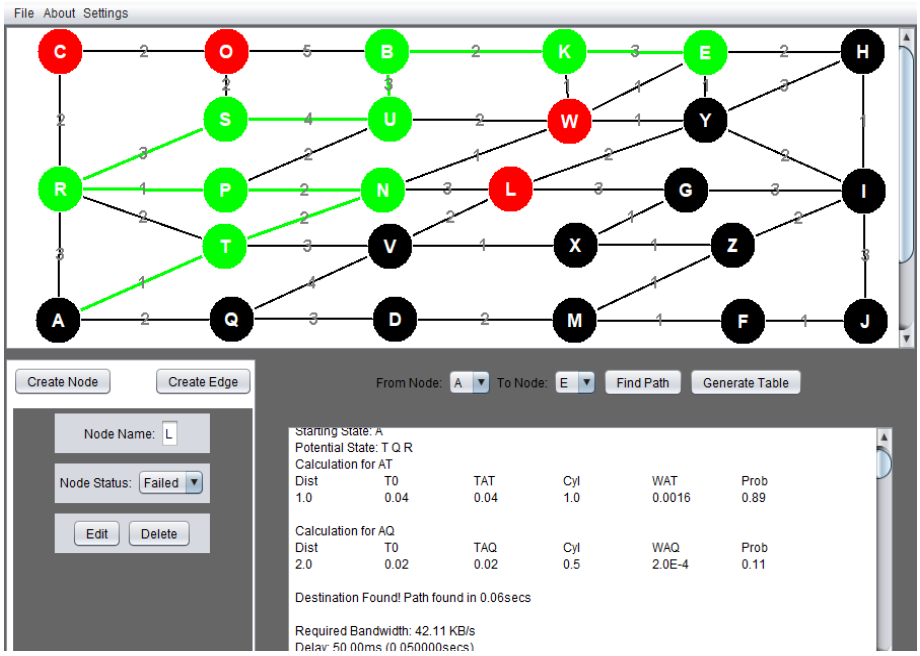

Figure 5.14: 4-nodes failure on a network

Figure 5.14 depicts the primary path generated when four nodes fail. The voice message takes 0.06 seconds to get to its target node using this routing. The required bandwidth to retransmit from transmitter to receiver is 42.111 Kbytes/s. The transferring time is 0.0501 seconds. The best path produced is A–T–N–P–R–S–U–B–K–E. Table 5.11 depicts the probability estimation of each node in Figure 5.14 that was chosen to produce a path. Table 5.12 depicts the pheromone intensity at each node along the routing path shown in Figure 5.14.

Table 5.11: The ACS routing probability distribution

Current State	T	N	P	R	S	U	B	K	E
A	0.89	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
T’	0.00	0.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00
N	0.00	0.00	0.11	0.00	0.00	0.00	0.00	0.00	0.00
P	0.00	0.00	0.00	0.89	0.00	0.00	0.00	0.00	0.00
R	0.00	0.00	0.00	0.00	0.50	0.00	0.00	0.00	0.00
S	0.00	0.00	0.00	0.00	0.00	0.11	0.00	0.00	0.00
U	0.00	0.00	0.00	0.00	0.00	0.00	0.50	0.00	0.00
B	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
K	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

Table 5.12: A full cycle pheromone update

Current State	T	N	P	R	S	U	B	K	E
A	0.04	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
T	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00
N	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00
P	0.00	0.00	0.00	0.04	0.00	0.00	0.00	0.00	0.00
R	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00
S	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00
U	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.00
B	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00
K	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02

Since investigation 2.11 does indeed have a relatively high path cost than investigation 2.10, rerouting in investigation 2.10 is faster than in investigation 2.11. In investigation 2.11, a higher transmission delay value indicates slow rerouting.

5.2.19 Investigation 2.12: Rerouting with randomised 5-node failures (Failed node: C, V, L, W and O)

Investigation 2.12 depicts outcome of rerouting a voice packet across the network with 5-node failures. In this investigation, a 650-byte packet is rerouted from transmitter node A to receiver node E.

The voice message takes 0.068 seconds to reach its destination in investigation 2.12. The capacity needed to transfer from transmitter to receiver equals 36.111Kbytes/s. There is a 0.0553second delay. A – T – N – P – R – S – U – B – K – E is the generated alternative path.

The path cost of the produced path in investigation 2.12 is greater compared to investigation 2.11, contributing to the longer transmission delay in investigation 2.12. As a result, rerouting in investigation 2.12 is slower than in investigation 2.11: The detailed results are shown in Table 5.13.

5.2.20 Investigation 2.13: Rerouting with randomised 6-node failures (Failed nodes: L, W, Y, V, H and X)

Consider investigation 2.13, a 300-byte voice message is rerouting from transmitter node A to receiver node E. The voice message uses 0.08 seconds to get to its destination. The required bandwidth for transmission from transmitter to receiver is 14.292Kbytes/s. The delay is 0.0602 seconds. A – T – N – P – R – C – O – S – U – B – K – E is the alternative path generated.

Due to greater intensity of node failure of investigation 2.13 than in investigation 2.12, as well as a higher transmission delay in investigation 2.13 than in investigation 2.12, rerouting is faster in investigation 2.12. Table 5.13 displays the detailed results.

5.2.21 Performance measurement of the suggested approach

Table 5.13 summarises the results of various investigations performed while different sizes of voice packets are rerouted with varying numbers of nodes failure.

Table 5.13: Performance analysis of the investigations (2.7 – 2.13)

Investigation Number	Message Size (Byte/s)	Number of node failures	Transmission Time (Seconds)	The Bandwidth required (Kbytes)	Delay (Seconds)	Path generated	Path cost
2.7	500	0	0.030	33.33	0.025	A – T – N – W – E	5
2.8	550	1	0.036	34.38	0.030	A – T – N – W – K – E	8
2.9(A)	450	2	0.040	23.68	0.035	A – T – R – P – U – W – E	9
2.9(B)	480	2	0.046	26.67	0.040	A – T – R – P – U – B – K – E	14
2.10	700	3	0.052	35.00	0.045	A – T – R – C – O – S – U – W – E	16
2.11	800	4	0.060	42.11	0.050	A – T – N – P – R – S – U – B – K –E	21
2.12	650	5	0.068	36.11	0.050	A – T – N – P – R – S – U – B – K – E	21
2.13	300	6	0.080	14.29	0.060	A –T – N – P – R – C – O – S – U – B – K – E	25

It was deduced from Table 5.13 that adequate capacity is needed to transfer a message in order to achieve a best path. Whenever an adequate bandwidth is utilized, transmitting delay is reduced, as demonstrated in investigations 2.7–2.9. (A). It was observed that the location of failure influences message delivery time, and that message delivery is determined by how quickly the system can generate the shortest alternative path. Similarly, high rerouting delay is observed when inadequate bandwidth is utilized as demonstrated in investigations 2.9(B) – 2.13.

Table 5.13 also shows that Investigations 2.7–2.9(A) achieve rerouting path optimization. This is due to the lower path cost value observed from the path generated, which minimises rerouting time and delay values, allowing voice packet rerouting to be completed more quickly. The graphical patterns of Table 5.13 are displayed in subsections 5.2.22–5.2.23, showing the inherent information.

5.2.22 Delay & routing time versus node failure

The amount of time needed for a message to be delivered when there is no vertices failure is relatively low (in Figure 5.15) due to the obvious lower transmission delay. It was noticed that when the quantity of failed nodes rises, transmission time increases since recomputing

the alternative path and rerouting the voice message takes more time. From 2-node failures to 6-node failures, the transferring time and delay rise, making rerouting slower. Since two investigation instances are performed, the average is plotted in investigation 2.9. The rerouting delay and time needed to send a packet with a certain quantity of node failures is depicted in Figure 5.15.

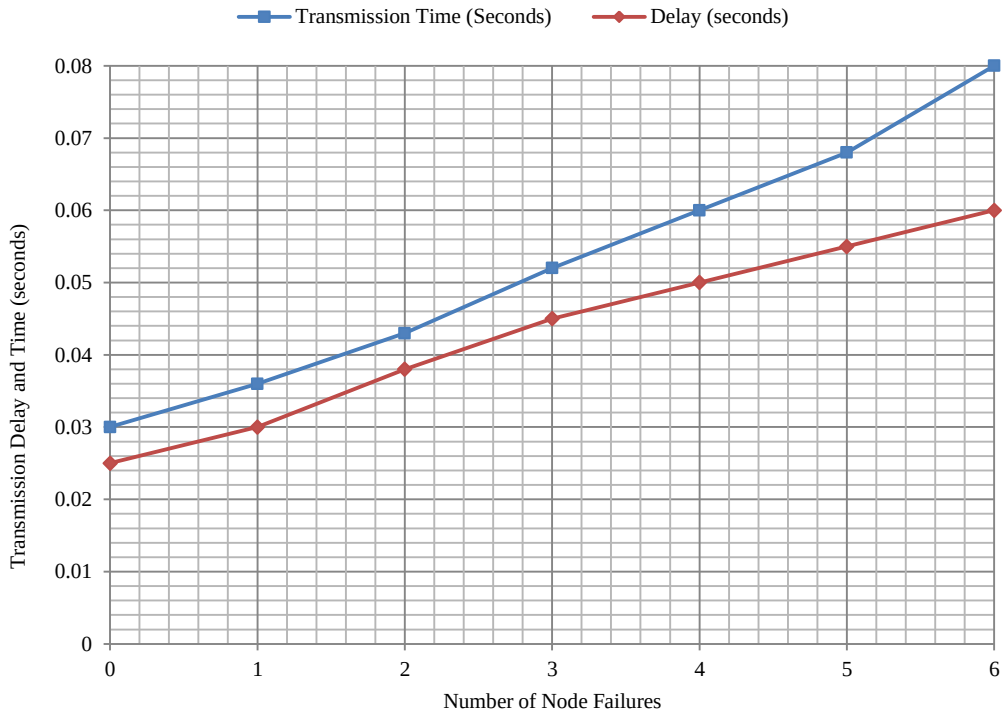

Figure 5.15: Delay & routing time versus failed nodes

5.2.23 The needed bandwidth and packet capacity versus node failures

When there is no node failure, the bandwidth used to transfer the message to its target node is adequate, and transferring rate is quicker because the transferring delay is kept to minimum at one node failure, as shown in Figure 5.16. The bandwidth needed to retransmit a packet rises whenever the quantity of node failures rises up to 4-node failures at 2-node failures. It has been discovered whenever bigger volume of message is retransmitted, the more bandwidth is needed to reroute the voice message. The bandwidth begins to dwindle whenever the quantity of node failures rises from four to six. Since there is a greater amount of node failure and the dwindling impact of channel capacity on packet rerouting, rerouting is extremely slow at the 6-node failures. The bandwidth and message size begin to increase up to node 4 at node 3. As node failures increase from node 4 to node 6, bandwidth and message size drop significantly. Two instances of the investigation were run, and the mean is charted in investigation 2.9. Figure 5.16 depicts the capacity needed to convey a packet when a network node fails.

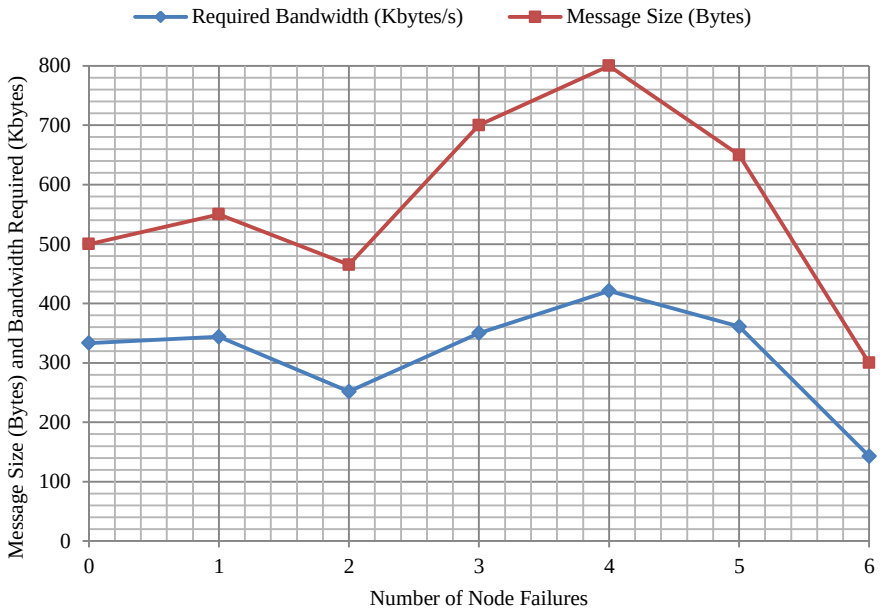

Figure 5.16: Message size & bandwidth required versus failed nodes

5.2.24 Rerouting with a network of thirty (30) nodes

NODEThe node labels are A through Z and A1 through D. Investigations 2.14–2.21 demonstrate how the investigations are conducted with varying number of nodes failure at various positions. Here, the circles indicate network nodes, and the connector that connects one device to the next indicates a link. The node failures in the figure are labeled, and the generated alternatives near best path are indicated. The majority of the investigations were carried out with a variable quantity of failures. Investigation 2.16 contains two investigation instances: instances A and B. Investigations 2.14 and 2.18 contain figures, tables, and results, whereas investigations 2.15–2.17 and 2.19–2.21 only contain descriptive results. Packets are transferred from transmitter node L to receiver node B. The transition diagram for the investigational setup's thirty-node network is shown in Figure 5.17. Link costs are generated randomly.

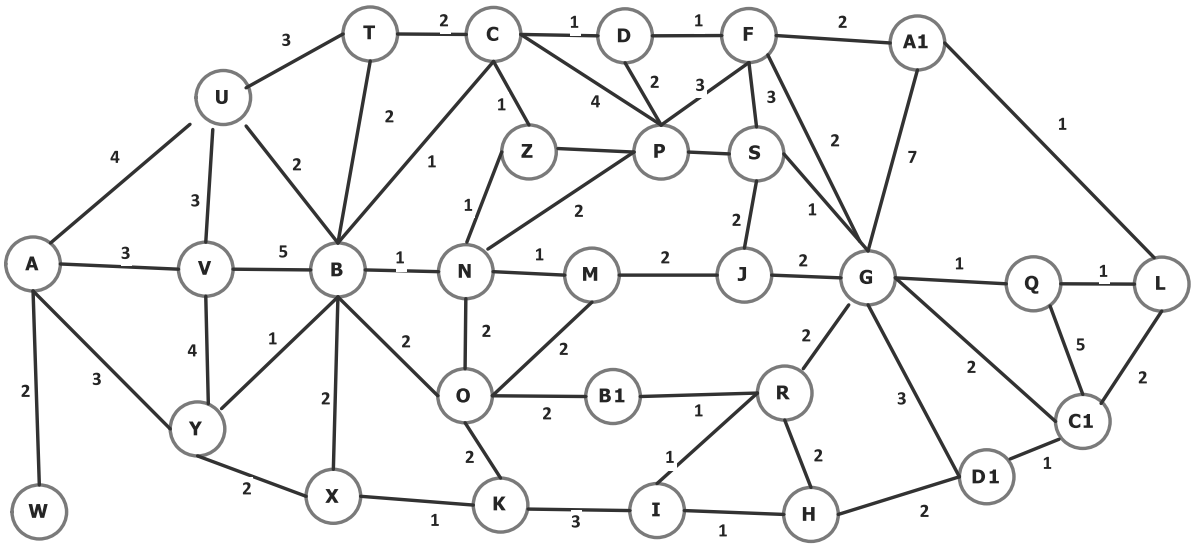

Figure 5.17: A transition diagram showing a network of thirty nodes

5.2.25 Investigation 2.14: routing in the absence of a failed node

Figure 5.18 shows a voice packet of 500-bytes being sent from transmitter node L to receiver node B.

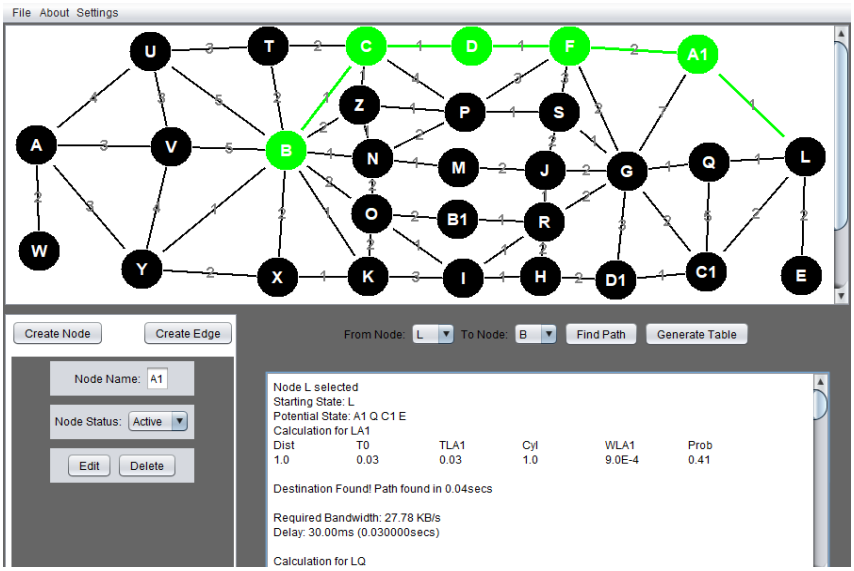

Figure 5.18: Telecom network without node failure

The packet takes 0.04 seconds to reach its destination, as shown in Figure 5.18. The bandwidth needed to transport from transmitter to the receiver is 27.781Kbytes/s. There is a 0.0300 seconds delay. L –A1 – F – D – C – B is the generated near optimal path. Table 5.14 depicts the probability estimation of chosen nodes in Figure 5.18 that are on the near optimal path. Table 5.15 shows the pheromone accumulation at each node along the best optimum path depicted in Figure 5.18.

Table 5.14: The ACS routing probability distribution

Current State	A1	F	G	D	P	C	B	Z
L	0.42	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A1	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
F	0.00	0.00	0.15	0.69	0.00	0.00	0.00	0.00
D	0.00	0.00	0.00	0.00	0.15	0.69	0.00	0.00
C	0.00	0.00	0.00	0.00	0.00	0.00	0.45	0.45

Table 5.15: A full cycle's pheromone update

Current State	A1	F	G	D	P	C	B	Z
L	0.03	0	0	0	0	0	0	0
A1	0	0.02	0	0	0	0	0	0
F	0	0	0.02	0.03	0	0	0	0
D	0	0	0	0	0.02	0.03	0	0
C	0	0	0	0	0	0	0.03	0.03

5.2.26 Investigation 2.15: rerouting due to a node failure (failed node: E)

Investigation 2.15 depicts the outcome of rerouting a voice packet with a node failure at the network's edge. A 500-byte voice message has been configured for rerouting from transmitter node L to receiver node B. The packet gets to its target node at 0.0401seconds. The needed capacity to transfer packet to the receiver is 27.781Kbytes/s. There is a 0.0300 second delay. L – A1 – F – D – C – B. is the generated near optimal path.

The same parameters were used in investigations 2.14 and 2.15 to determine the impact of a failure on a system connected wirelessly via the network structure. Node E's failure has no

impact on rerouting because it is connected outside the network structure. As a result, the same rerouting parameters were generated in investigation 2.15 and investigation 2.14. The detailed results are shown in Table 5.18.

5.2.27 Investigation 2.16: rerouting with 2-node failures (network's edge and centre)

Investigation 2.16 depicts the simulated outcome of rerouting a voice packet with 2-node failures on network's edge & centre.

Instance A: Two network edge node failures (failed node: A1 and X)

A 480-byte packet has been configured for rerouting from transmitter node L to receiver node B. The voice message gets to its target node in 0.050 seconds. The capacity needed to transfer data to its receiver is 21.821Kbytes/s. There is a 0.035-second delay. L – Q – G – F – D – C – B is the near optimal path generated.

For the realisation that in the investigation 2.15, the packet weight is larger than the packet weight in investigation 2.16(A), transmission in investigation 2.15 is faster. Since the quantity of node failures is lower in investigation 2.15 than in investigation 2.16(A). The packet size is chosen at random; it could be larger or smaller. The detailed results are shown in Table 5.18.

Instance B: The end result of 2-node failures at the network's center (failed node: J and N)

Through investigation 2.16(B), a 450-byte voice message is sent from transmitter node L to receiver node B for rerouting. Investigation 2.16(B) depicts the alternate route produced whenever 2-nodes in the network's center fail. After this rerouting, the voice message arrives at its destination in 0.056 seconds. The capacity needed to reroute to receiver is 20.45 Kbytes/s. It takes 0.0351seconds to send a message. The alternative path that was produced is L – Q – G – F – D – C – B.

When investigation 2.16(B) and investigation 2.16(A) are compared, we discovered that the bandwidth needed to transfer the voice message in investigation 2.16(B) is less than that used in investigation 2.16(A). This is because the packet transferred in investigation 2.16(B) is smaller than the packet retransmitted in investigation 2.16(A). Furthermore, the rerouting paths and transmission delay values produced by the two investigations were identical. The

time transferring in investigation 2.16(B) is shorter due to varying weight of messages retransmitted: The comprehensive outcomes are depicted in Table 5.18.

5.2.28 Investigation 2.17: Rerouting with randomised 3-node failures (Node failure: A1, G and R)

Investigation 2.17 depicts the outcome of rerouting a voice packet with 3-node failures at the network's edge and centre. Since it is a random selection, the nodes chosen could be located anywhere on the network.

Randomised 3-node Failures (Node failure: A1, G and R).

Through investigation 2.17, a 600-byte voice message is sent from transmitter node L to receiver node B for rerouting. The packet gets to its target node in 0.06s. The required capacity to transfer to receiver is 26.091Kbytes/s. There is a 0.040 second delay. L – Q – C1 – D1 – H – I – O – B is the alternative path generated.

When investigation 2.17 is compared to investigation 2.16(B), it is discovered that rerouting is dragging in investigation 2.17 than in investigation 2.16(B) due to a significant increase of node outages in investigation 2.17, which contributes to an increase in the value of delay time. Furthermore, because the rerouted voice message is larger in size, the bandwidth needed to transfer is greater in investigation 2.17. Table 5.18 displays the detailed results.

5.2.29 Investigation 2.18: rerouting with randomised 4-node outages (failed nodes: A1, I, J and G)

Figure 5.19 depicts a 550-byte voice packet sent from transmitter node L to receiver node B.

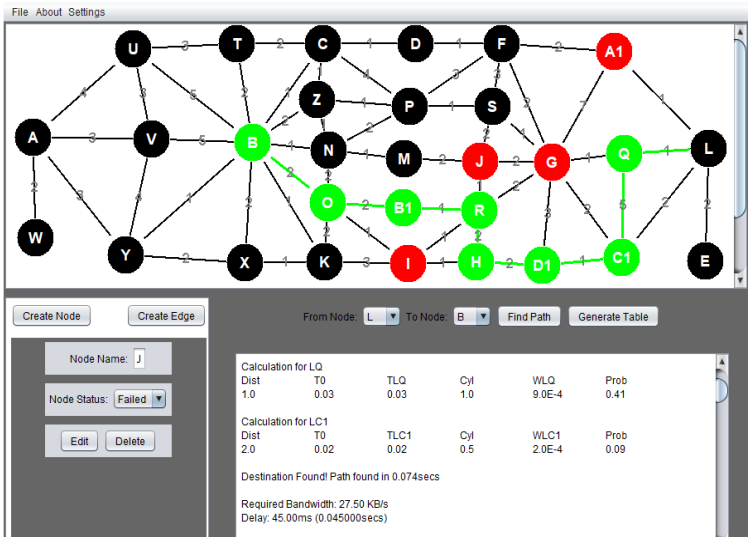

Figure 5.19: 4-Node outages in wireless network

The voice message takes 0.074 seconds to arrive at the destination, as shown in Figure 5.19. The capacity needed to transfer packet to the receiver is 27.5 Kbytes/s. There is a 0.0450-second delay. The best route path produced is L – Q – C1– D1 – H – R – B1 – O – B. Table 5.16 depicts the probability estimation of various nodes in Figure 5.19 that are on the near optimal path. Table 5.17 shows the pheromone concentration at each node along the best optimum path depicted in Figure 5.19.

Table 5.16: The ACS routing probability distribution

Current State	Q1	C1	D1	H	R	B1	O	B
L	0.41	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Q	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
C1	0.00	0.00	0.82	0.00	0.00	0.00	0.00	0.00
D1	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
H	0.00	0.00	0.00	0.00	0.18	0.00	0.00	0.00
R	0.00	0.00	0.00	0.00	0.00	0.31	0.00	0.00
B1	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00
O	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.13

Table 5.17: A full cycle's pheromone update

Current State	Q1	C1	D1	H	R	B1	O	B
L	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Q	0.00	0.05	0.00	0.00	0.00	0.00	0.00	0.00
C1	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00
D1	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00
H	0.00	0.00	0.00	0.00	0.02	0.00	0.00	0.00
R	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00
B1	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00
O	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02

As there are more node failures in investigation 2.18, rerouting takes longer than in investigation 2.17.

5.2.30 Investigation 2.19: Rerouting with randomised 5-node outages (Failed nodes: A, A1, I, T and G)

Investigation 2.19 depicts the outcome of rerouting a packet with randomly selected 5-node outages. From investigation 2.19, a 700-byte voice packet is configured for rerouting from transmitting node L to receiving node B. The packet gets to its target node in 0.0780 seconds. The capacity needed for transfering from transmitter to receiver is 29.171 Kbytes/s. There is a 0.05 second delay. L – Q – C1 – D1 – H – R – B1 – O – K – B is the alternative path generated.

When comparing investigation 2.19 to investigation 2.18, we discovered that the capacity utilized in investigation 2.18 is less than that of investigation 2.19 because the message rerouted in investigation 2.18 is smaller in size. Because the transferring delay in investigation 2.19 is greater, transmission is faster in investigation 2.18. The comparisons are shown in Table 5.18.

5.2.31 Investigation 2.20: Rerouting with randomised 6-node outages (Failed nodes: A1, Q, H, R, M & Z)

Investigation 2.20 depicts the simulated outcome of rerouting a packet with six randomised node outages. A packet of 450-bytes has been configured to rerouting from transmitting node L to receiving node B. The voice message takes 0.0851 seconds to get to its target node. The required bandwidth to transfer from transmitter to receiver is 18 Kbytes/s. The transferring delay is 0.0550 seconds. L–CI–D1–G–J–S–F–P–N–O–B is the alternative path generated.

When comparing investigation 2.20 to investigation 2.19, it revealed that the capacity needed in investigation 2.20 is less than the capacity needed in investigation 2.19 because the packet retransmitted in investigation 2.20 is less than that of the investigation 2.19. Since the rerouting delay in investigation 2.20 is greater than in the investigation 2.19, transmission is speedy in investigation 2.19. The comparisons are depicted in Table 5.18.

5.2.32 Investigation 2.21: Rerouting randomised 7-node outages (Failed nodes: A1, Q, I, B1, M, D and F)

Investigation 2.21 depicts the outcome of rerouting a packet with the 7-node outages randomly distributed. A 650-bytes of packet has been configured to rerouting from transmitting node L to receiving node B. In this investigation, the voice message uses 0.0900 s to get to its target node. The required capacity to transfer to receiver euals 21.671 Kbytes/s.

The transfer delay equal 0.060 seconds. L–Q–C1–D1–H–R–J–S –P–Z–C–B is the near optimal path generated.

Due to the increasing amount of node failure in investigation 2.21, rerouting is sluggish than in investigation 2.20, resulting in a higher value of packet delay. The comprehensive outcomes are depicted in Table 5.18.

5.2.33 Performance measurement of the suggested model (investigations 2.14–2.21)

Table 5.18 summarises the results of several investigations in which different weights of packets are sent with varying numbers of node outages.

Table 5.18: Performance analysis of the investigations (2.14 – 2.21)

Investigation Number	Message Size(Bytes)	Number of Failed Node	Transmission Time (seconds)	The Bandwidth Required (Kbytes)	Delay (seconds)	Path Generated	Path cost
2.14	500	0	0.040	27.78	0.030	L – A1 – F – D – C – B	6
2.15	500	1	0.040	27.78	0.030	L – A1 – F – D – C – B	6
2.16(A)	480	2	0.050	21.82	0.035	L – Q – G – F – D – C – B	7
2.16(B)	450	2	0.056	20.45	0.035	L – Q – G – F – D – C – B	7
2.17	600	3	0.060	26.09	0.040	L – Q – C1 – D1 – H – I – O – K – B	12
2.18	550	4	0.074	27.50	0.045	L – Q – C1 – D1– H – R– B1– O – B	16
2.19	700	5	0.078	27.17	0.050	L – Q – C1 – D1 – H – R – B1 – O – K – B	17
2.20	450	6	0.085	18.00	0.055	L – CI – D1 – G – J – S – F – P – N – O – B	22
2.21	650	7	0.09	21.67	0.060	L – CI – D1 – G – J – S – F – P – N – O – K – B	23

Investigations 2.14–2.16(B) achieve transmission path optimization, as shown in Table 5.18. This is because the lowered path cost generated from the best alternate route reduces transmission time and packet delay, making voice message rerouting speedy. Table 5.18's graphical patterns are shown in subsections 5.2.34–5.2.35, revealing the inherent knowledge.

5.2.34 Packet delay & transmission time versus node failure

The packet delay and transferring time needed to send a packet are shown in Figure 5.20 when the number of failed nodes increases. When only 1-node fails, the time it requires for a voice packet to arrive is reduced, as is the packet delay, resulting in faster message transmission. From 1 to 7-node outages, transferring time and packet delay begin to increase. This is because the amount of node outages has risen.

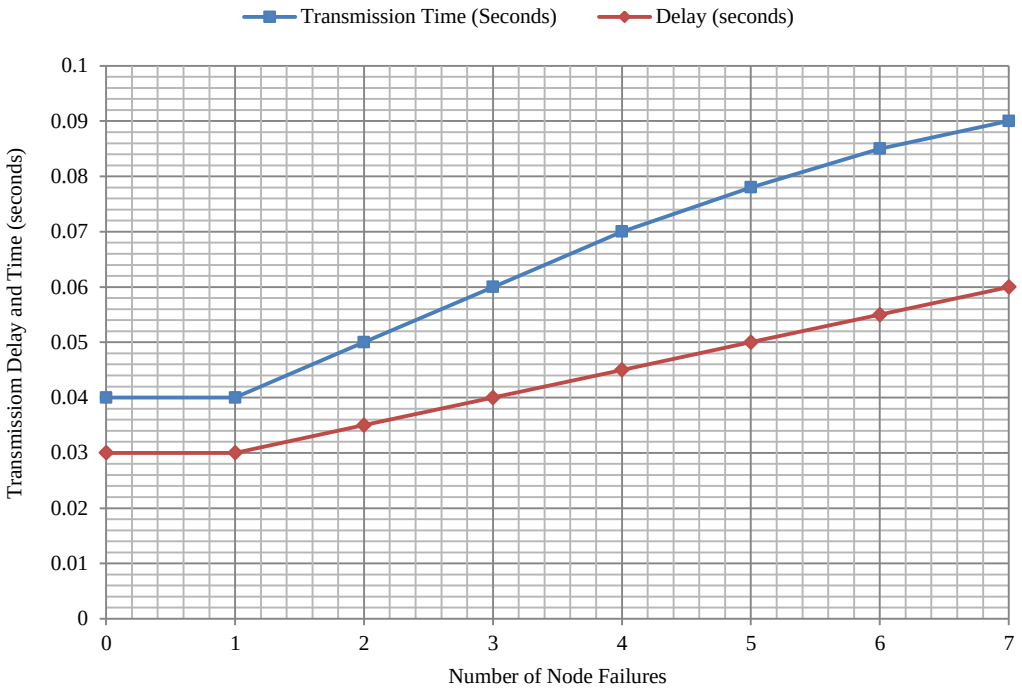

Figure 5.20: Packet delay & transmission time in relation to node failure

5.2.35 The required bandwidth & path cost versus node failures

When a network node goes down, Figure 5.21 depicts the path-cost of a rerouting path as well as the network capacity needed to transfer a voice packet. The capacity utilized to transfer the packet to its target node is adequate from no node to 1-node outage, and the transferring path cost is relatively low. From 1 to 7-node outages, the capacity utilized to retransfer packets is risen, as did the path-cost, making rerouting slower. The path-cost rises with rising node outages, resulting in capacity depletion with 3-node failures. In investigation 2.16, the mean capacity and path-cost are charted because there are two investigation instances.

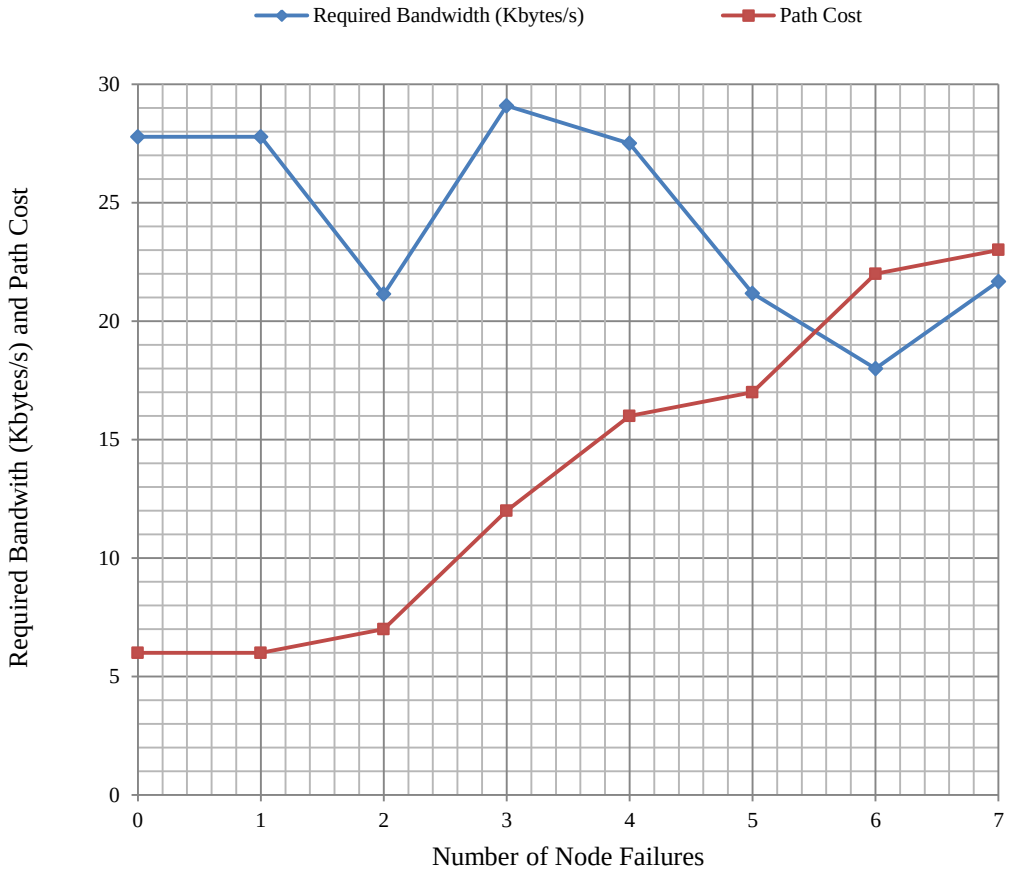

Figure 5.21: Required bandwidth & path cost versus failed nodes

5.2.36 Comparison between the suggested model to other routing protocol

Investigations 2.1, 2.7, and 2.14, which accomplished voice routings in the absence of node outage, are compared with the effectiveness of the suggested scheme and Dijkstra. MATLAB is used to implement the Dijkstra algorithm. The results and figure from investigation 2.1 are depicted, but the outcomes from investigations 2.7 and 2.14 are displayed. Figure 5.22 depicts the MATLAB code of the investigation 2.1.

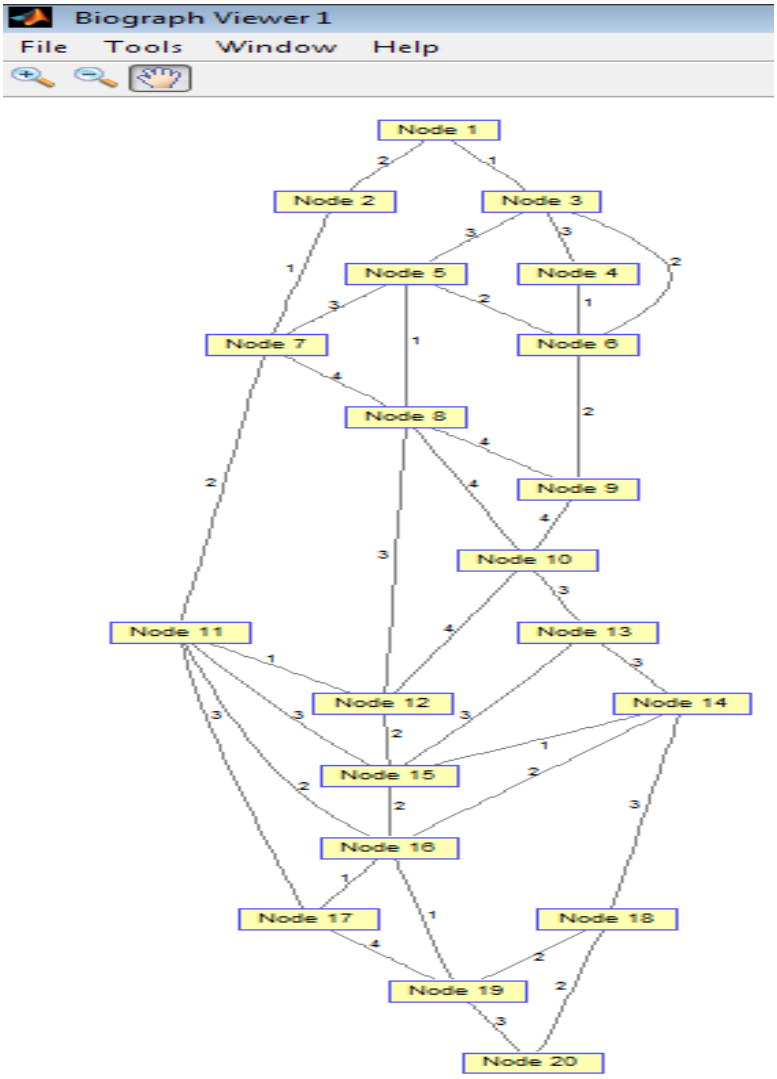

Figure 5.22: Representation of Figure 5.8 in Dijkstra model

Figure 5.23 depicts the MATLAB codes used in investigation 2.1 to generate the alternative transmission path.

>> net = sparse([1 1 2 3 3 3 4 5 5 5 6 7 7 8 8 8 9 10 10 11 11 11 11 12 13 13 14 14 14 15 16 16 17 18 18 19],[2 3 7 5 4 6 6 6 7 8 9 8 11 9 10 12 10 12 13 12 15 16 17 15 14 15 15 16 18 16 17 19 19 19 20 20], [2 1 1 3 3 2 1 2 3 1 2 4 2 4 4 3 4 4 3 1 3 2 3 2 3 3 1 2 3 2 1 1 4 2 2 3], 20, 20) >>[minimum_cost,shortest_path,predicted_paths]=graphshortestpath(net,1,19) minimum_cost = 10 shortest_path = 1 2 7 11 16 19 predicted_paths = Columns 1 through 13 0 1 1 3 3 3 2 5 6 8 7 11 10 Columns 14 through 20 13 11 11 11 14 16 19 >>view(biograph(net,[],'ShowArrows','off','ShowWeights', 'on'))	Output Net = (1, 2) 2, (1, 3) 1, (3, 4) 3, (3, 5) 3, (3, 6) 2, (4, 6) 1, (5, 6) 2, (2, 7) 1, (5, 7) 3, (5, 8) 1, (7, 8) 4, (6, 9) 2, (8, 9) 4, (8, 10) 4, (9, 10) 4, (7, 11) 2, (8, 12) 3, (10, 12) 4, (11, 12) 1, (10, 13) 3, (13, 14) 3, (11, 15) 3, (12, 15) 2, (13, 15) 3, (14, 15) 1, (11, 16) 2, (14, 16) 2, (15, 16) 2, (11, 17) 3, (16, 17) 1, (14, 18) 3, (16, 19) 1, (17, 19) 4, (18, 19) 2, (18, 20) 2, (19, 20) 3 Biograph object with 20 nodes, path = 1–3–5–8–12–11–16–19 = A–D–T–N–K–M– C–E, Path cost = 10.

Figure 5.23: Alternative transmission path of investigation 2.1 with MATLAB code

The Outcomes of Simulation

(i) In investigation 2.1, the Dijkstra technique together with the suggested method produced the same path: A–D–T–N–K–M–C–E. Both methods produced the same path cost, which is ten implying that the packet delay for both techniques is the same.

(ii) In investigation 2.7, Dijkstra produced the rerouting path A – T – N – W – Y – W – E of the (6) path-cost, whereas the suggested model produced the path A – T – N – W – E of the (5) path cost. The suggested model clearly outperforms the Dijkstra technique due to these outcomes

(iii) From investigation 2.14, the suggested method produced path L – A1 – F – D – C – B and (6) path-cost, whereas the Dijkstra algorithm produced path L – Q – G – S –P – Z – B of the (7) path cost, implying communication with the suggested system is faster but slower with Dijkstra.

From the outcomes produced in (i)–(iii), the suggested method outperforms a Dijkstra technique at each and every stage of node failure, with the exception of outcome number (i) in which the same outcomes were produced.

5.2.37 Suggested Technique with Related Routing Methods

Using the NS-2 simulator, the suggested method packet delivery ratio is compared to certain other routing strategies in this section. The following NS-2 simulation claims were established in the investigation conducted.

- The nodes that exist in the wireless network are all the same. It implies a node could be either a transmitter or a receiver, and that each node can route signal from a node to the other if it is not destined for itself.
- The data communication spectrum of the network's nodes is the same. In this simulation, the highest communication range is set to 20 m.
- Data packets are transmitted bidirectionally (communication can occur in either direction). This applies to data packet routing based on ACS-inspired swarm - based approaches.
- There is a common medium of transfer of data. In this case, it is the radio connection which occurs between nodes which are 20 m away.

The supremacy of the suggested system was validated using the parameters in Table 5.19.

A number of routing algorithms are available to assist in determining the path and distance of network traffic. Dijkstra's algorithm is one of the best shortest path search algorithms. The Dijkstra algorithm is used as the basis for comparison because it finds the shortest path. This algorithm employs the connection matrix and weight matrix. Thus, a matrix consisting of paths from the source node to each node is formed; allowing us to choose a column of destination from the path matrix formed and finds the shortest path. Similarly, a column from a matrix is selected to find the shortest distance between the source and destination nodes. The Dijkstra algorithm has been used in computer networking for system routing and in Google Maps to find the shortest path from one location to another [102]. For these reasons, Dijkstra is one of the most widely used routing algorithms.

The parameters used here are based on best practices from the existing literature, but they are verified and tested on various simulation results generated from these investigations before being applied to our work. Figure 5.24 depicts the generated results.

Table 5.19: Environments for simulation

Environments	**Value**
Coverage area	500m * 500m
Investigational time	200 sec.
Communication range	20m
MAC protocol	IEEE 802.15.4
Transmission speed	5 m/s
Packet size	512 Bytes
Nodes count	10~100
UDP connection count	5~20
Communication transfer rate	4 kBps

The percentage of incoming signals at the desired location terminal is the metric that measures effectiveness. The simulation outcomes explain the Dijkstra technique, the (AODV) which is Reactive and (ADPV) which is Adaptive and (DSDV) which is Proactive strategies, as well as the suggested model's packet delivery ratios. The simulation accounts for packet transfer at a rate of 5 meter/seconds. The packet delivery ratio decreases as the packet count increases, as illustrated in Figure 5.24. All protocols have a packet delivery ratio greater than 75% when there are 50 nodes in the network. As the number of nodes increases, their success ratios change. Despite this, the proposed scheme achieves a packet delivery ratio of 72% even with 100 nodes because each node effectively saves the routing details of its neighbors. By comparison, the effectiveness of AODV, DSDV and ADPV deteriorates significantly as the number of nodes rises. Whenever network size is small, the suggested technique and Dijkstra function properly and produce good delivery ratios, whereas the AODV delivery ratio completely fell under 70%. When there are many nodes in a large network, the ADPV routing protocol is inefficient. Table 5.20 shows the packet delivery ratio of evaluated routing models.

Table 5. 20: Packet Delivery Ratio of evaluated model with ACS

Number of nodes	ACS model	Dijkstra model	Reactive model (AODV)	Proactive model (DSDV)	Adaptive model (ADPV)
10	0.94	0.92	0.85	0.84	0.84
20	0.92	0.88	0.84	0.83	0.82
30	0.89	0.86	0.83	0.83	0.81
40	0.86	0.85	0.82	0.82	0.78
50	0.86	0.84	0.80	0.81	0.78
60	0.84	0.84	0.79	0.78	0.76
70	0.84	0.83	0.78	0.78	0.76
80	0.83	0.80	0.76	0.75	0.75
90	0.82	0.78	0.75	0.74	0.75
100	0.82	0.78	0.75	0.74	0.74

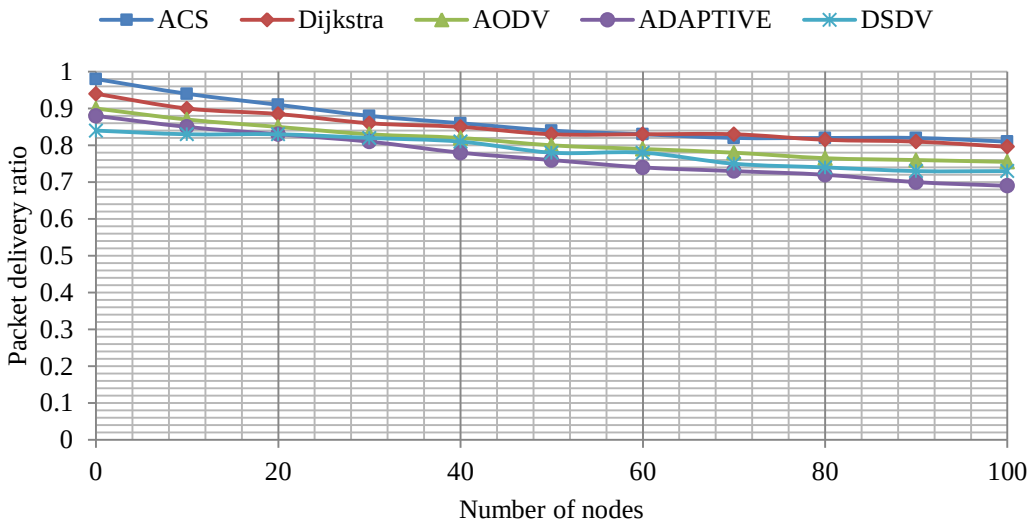

Figure 5.24: Packet delivery ratio at 5 m/s

5.2.38 Analysis of the suggested model's complexity and related work

Using complexity analysis approach, Table 5.21 compares the performance of the suggested model of investigations 2.1–2.6 to that of an adaptive method.

Table 5.21: Assessment of the proposed model's and adaptive recovery model's performance

Investigational No.	No. of Node Failures	Variables	Suggested Model Complexity $O(m+\frac{nlogn}{\rho})$	Adaptive Restoration Model $O\left(lm+\frac{n}{\rho}\right)$.
2.1	0	n=8, l=10, m=7, $\rho = 0.1$	78.25	150.00
2.2	1	n=9, l=12, m=8, $\rho = 0.1$	93.88	186.00
2.3	2	n=10, l=16, m=9, $\rho = 0.1$	109.00	244.00
2.4A	3	n=10, l=17, m=9, $\rho = 0.1$	109.00	253.00
2.4B	3	n=10, l=21, m=9, $\rho = 0.1$	109.00	289.00
2.5	4	n=11, l=21, m=10, $\rho = 0.1$	124.55	320.00
2.6	5	n=12, l=25, m=11, $\rho = 0.1$	140.50	395.00
Average			764.18	1837.00

Figure 5.25 depicts the effectiveness of the suggested scheme of investigations 2.9-2.12 and the adaptive recovery versus the node outages and runtime complexity using Big O notation.

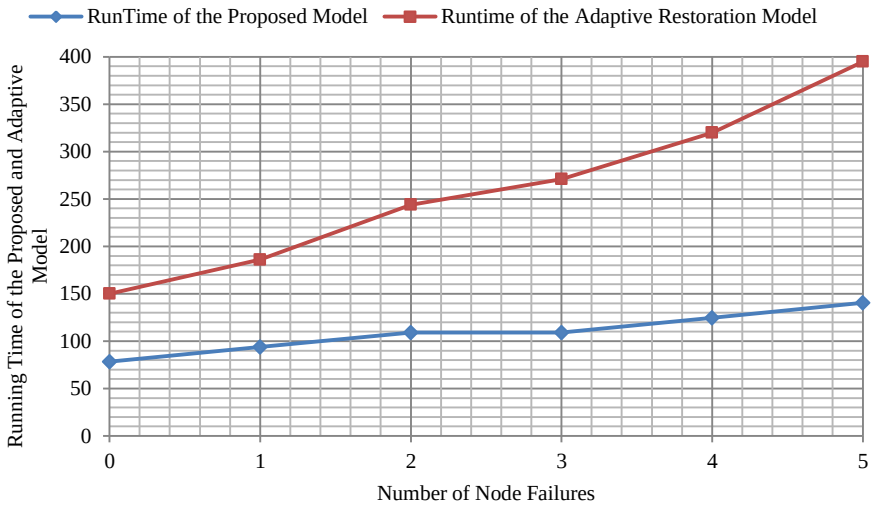

Figure 5.25: Time complexity against failed nodes

In terms of computational time, Figure 5.25 demonstrates that the new model performs better than adaptive recovery model. The number of runs required to produce the best path by the proposed model is less than that required by the adaptive recovery model. As a result, the suggested model is able to produce an effective alternative path faster than the adaptive recovery mode.

5.2.39 The suggested model with Dijkstra technique

Table 5.22 compares the execution efficiency in the suggested system and the Dijkstra algorithm. The Dijkstra algorithm's computation cost is used to validate the number of iterations of the simulated results. Dijkstra's runtime is given in [103]: O (|M||N|+|N|2 log|N|), |M| is the amount of links (edges) and |N| is the amount of vertices (nodes). The algebraic affirmation is implemented in Table 5.22 to measure the runtime of Dijkstra's produced paths.

Table 5.22: Capacity efficient ACS and Dijkstra algorithm runtime efficiency

Communication Links Produced by ACS	Communication Links Produced by Dijkstra	ACS-System $O(M+\frac{nlogn}{\rho})$	Dijkstra Algorithm $O(\|M\|\|N\|+\|N\|^2 log\|N\|)$
(i) A – D – T – N – K – M – C – E	A – D – T – N – K – M – C – E	79.25	113.80
(ii) A – T – N – W – E	A – T – N – W – Y – W – E	38.95	83.41
(iii) L – A1 – F – D – C – B	L – Q – G – S –P – Z – B	51.69	83.41
Sum of run time		169.89	280.62

Figure 5.26 compares the runtime of the suggested model and the Dijkstra algorithm.

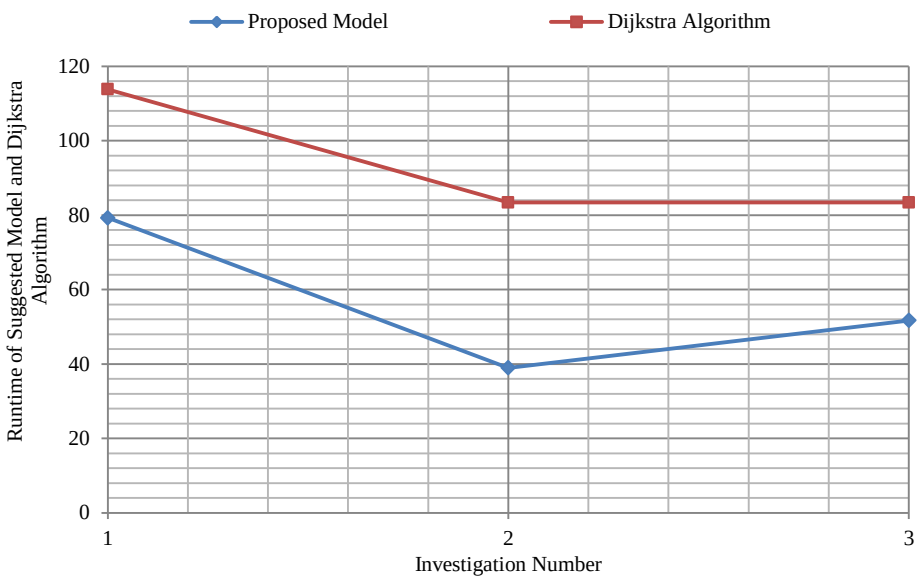

Figure 5.26: Runtime efficiency of suggested model versus Dijkstra

In terms of runtime computation, Table 5.22 demonstrates that the new system performs better the Dijkstra model since the suggested model's overall running time is less than the Dijkstra model.

5.2.40 Section summary

This study suggests a capacity efficient ACS system for telecoms resilience of failure that produces a nearly best alternate route to redirect packets for every outage stage. According to Tables 5.8, 5.13, and 5.18, the network with a longer alternate route, it takes more time for a packet to reach its target. Since the data gets to its target node within a short period, communication with a reduced path cost is thought to be close to optimal. A sufficient bandwidth for transmitting is produced, and a shorter delay captured. It was observed that the placement of a node outage influences the size of path cost, which is a factor in communication speed. It has been demonstrated that the more nodes in a communication path, the more bandwidth is required to effectively communicate a message.

The optimization problem is solved in investigations 2.1–2.2 (Table 5.8), 2.7–2.9 (A) (Table 5.13), and 2.14–2.16 (B) (Table 5.18). This is due to the reduced path cost value obtained through the optimum solution alternate routes obtained, that reduces transmitting time and delay time, allowing voice message rerouting to occur more quickly.

The similarity was based on the assessment of other similar data transfer models, as shown in sections 5.2.36-5.2.39. The proposed system performs better than adaptive recovery, Dijkstra algorithm, and reactive model in terms of runtime, packet delivery, rerouting speed, and communication delay. In contrast to the adaptive recovery system, that adds duplication and squanders network resources by retaining the fallback route in storage for recovery, the suggested model reroutes voice packets in near real time, as demonstrated in investigations 2.1–2.6, 2.7–2.13, and 2.14–2.21. As demonstrated in investigations 2.1–2.6, 2.7–2.13, and 2.14–2.21, the suggested system retransmits packets with the needed capacity for capacity efficiency. This expedites the process and ensures that the output at the receiving node is of high quality. In investigations 2.1–2.6, 2.7–2.13, and 2.14–2.21, alternate solution paths that are automatically produced.

To remotely resolve telecom network failures, the prototype presented is suggested as a pilot for Africa's telecoms for example Globalcom, MTN, and others. The authors intend to broaden the method's coverage in the future by combining the ACS and other protocols to improve efficiency. The suggested capacity efficient ACS is also planned for use in telecoms to resolve link–link outages.

5.3 INVESTIGATION 3: REROUTING RESILIENCE DURING IOT OPERATIONS WITH GENETIC ALGORITHM COMPUTING

5.3.1 Introduction

When a node (node) and a connector (link) fail during an Internet of Things operation, restoration has to be done immediately. This section uses an enhanced genetic algorithm to generate an alternate path.

The goal of this study is to resolve multiple transmission failures in an IoT network. IoT network problems include actions taken against network systems to disturb node activities, alter principle works, or corrupt stored information [104].

Initially, the Internet has been used to transmit datagrams with a unique Identifier between users and information sources. The Internet has been used to exchange information by many of modest, asset-restricted objects linked in millions made up of the Internet of Things as technology advances (IoT). A huge number of information from such equipment burdens the IoT network. As a result, to make very good use of the network resources available, it is necessary to offer a solution to a variety network interrelated issues in IoT, such as data transfer, sustainable energy, congestion, homogeneity, expandability, durability, service quality (QoS), and confidentiality [105].

The IoT networks can be seen in many critical areas of our society, including commercial activity, financial services, and task services. The IoT core network is vulnerable to multiple related failures affected by external anomalies, malware, upgrades to compiled code, residual faults, and targeted attacks. These occurrences have a potential to degrade IoT network services for a long duration. A survivability plan to maintain network integrity in the event of a failure is obviously critical [106]. The Internet of Things systems are extensively used for high-speed information transmission. Time division and trying to switch operations are built into the Internet of Things network, allowing connectivity between nodes that occur at higher velocities.

Several network failures have occurred in IoT networks and connected nodes, providing good drive for this research [107]. These occurrences have frequently created severe breakdowns, and its influence in aspects of potential operations, lost revenue, and people's perceptions, including assurance in advancement, has been aggravated due to its sluggish identification and treatment. There are numerous reasons for IoT network outages, with the most common being unexpected cable breaks, hardware glitches, software issues, natural catastrophes, and mishandling, and

malicious attack (both hardware and software). All potential causes of IoT failures usually result in link-link outages. Individual link failure and shared link failure are the two broad types of link failure. The ability to differentiate between collective and individual link failures is dependent on whether each or much more links fail at the same time. Collective failures show that the involved links have a failing features of the product in common [108].

5.3.2 Contributions and research questions

In the literature, numerous strategies for failure recovery have been proposed, and they vary depending on the system designs used [109]. The identified gaps influenced the following research questions investigated in this research work:

- How can capacity efficient evolutionary algorithm system be successfully developed to withstand multiple node-link failures that disrupt traffic flow in IoT networks?
- In the event of multiple node-link failures, how resilient is flow traffic in IoT networks?

The following are the primary contributions of this research:

- Evaluating a newly suggested on-demand recovery and capacity efficient EGA model to help IoT network subscribers in surviving multiple node-link failures; and
- Extensive investigations were carried out in order to identify optimal paths for rerouting multimedia packet on IoT large networks, varying from zero failure to multiple node-link outages with the required capacity (bandwidth).

5.3.3 Investigational setup

Nodes are labeled from A, B, ……Z and from A1, B1, C1,….. D1 in investigations 3.1-3.8, and investigations are run at various places with different amount of failed nodes and links. The circles in the simulated investigation represents network nodes, the line that connects one node to the other indicates a link, and the failed nodes and failed links, as well as optimal alternative paths generated, are indicated in the figure labels. Results, tables, and figures are depicted in investigations conducted in 3.1, 3.3 3.5, and 3.7, but only results from investigations 3.2, 3.4, 3.6 &3.8 are shown in Table 5.24. The link costs are generated at random. Source node ‘A’ sends multimedia traffic to destination node X. Figure 5.27 depicts a thirty-node IoT network in the system setup. Owing to its suitability for network programming, the investigation is carried out using the Java language. Link costs are generated randomly.

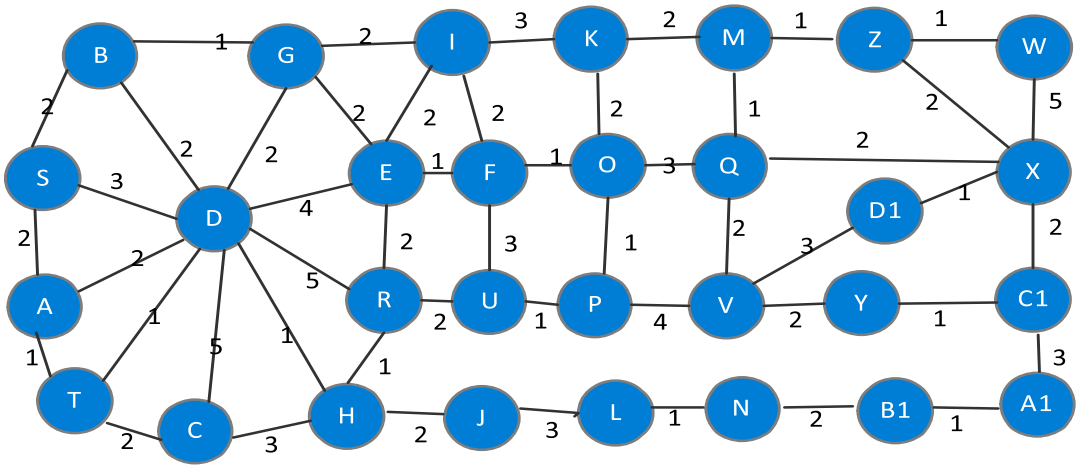

Figure 5.27: A 30-node network is represented by a transition diagram.

Throughout investigations 3.1-3.8, the parametric configuration for the capacity efficient EGA model is shown in Table 5.23.

Table 5.23: Parameters specification

EGA Properties	Number of Node	Probability for Crossover	Capacity for Multimedia (Bytes)	Initial Time(s)	IP Header	Failure in Node-Link
Characteristics	variable	0.500	Variable	0.005	20-Bytes	variable

The aforementioned tests are performed:

In Investigation 3.1, an IoT network with 0-node and 0-link failure is considered.

Investigation 3.2 considers an IoT network with a single node and a single link failure.

Investigation 3.3: failure of a single node and 2-links is considered.

Investigation 3.4: failure of 2-nodes and 3-links is considered.

Investigation 3.5: 2-node and 4-link failure is considered.

Investigation 3.6: failure of 3-nodes and 5-links is considered.

Investigation 3.7: failure of 3-nodes and 6-links is considered, and

Investigation 3.8: failure of 4-nodes and 7-links is considered. (The results are shown in Table 5.24).

5.3.4 Performance evaluation of a network of 30-nodes with a various numbers of device and link failures

Table 5.24 depicts the effectiveness evaluation of 30-nodes with varying numbers of node-link failures.

Table 5.24: Performance comparison of investigations 3.1–3.8

Investigation Number	Number of (node, link) failure	Transmission Time (seconds)	Required Bandwidth (Kbytes/s)	Fitness	Delay (ms)	Path Cost	Multimedia Size (Bytes)	Path Generated
3.1	(0,0)	0.7370	33.33	0.0026	40	14	600	A–D–G–I– F– O – Q–X
3.2	(1,1)	0.7820	50.00	0.0023	40	15	700	A–D–R–U –P–V– Q –X
3.3	(1,2)	0.8280	46.43	0.0019	40	18	650	A –D –R –U –F– O – Q –X
3.4	(2,3)	0.8900	18.75	0.0029	45	20	300	A–S–D –E –I –K –M –Z –X
3.5	(2,4)	1.1560	30.00	0.0027	40	16	480	A–D–R–U– P –O –Q – X
3.6	(3,5)	1.1700	22.22	0.0028	45	18	400	A– D– E– F– I– K–M–Z –X
3.7	(3,6)	1.1850	23.81	0.0029	45	15	500	A–D–E– F– O–K–M–Q –X
3.8	(4,7)	1.2030	28.95	0.0004	45	17	550	A–D– E–F–O –P–V–D1–X

The solution to the optimisation issue is depicted in Table 5.24. This is demonstrated in investigations 3.1–3.2 and 3.7, where the outcomes of the least path cost values are indicated in the optimum solution alternate routes obtained reduce runtime and thus speed up multimedia traffic rerouting. The results of investigations 3.1, 3.5, and 3.7 are shown in the following sections.

5.3.5 Investigation 3.1: A node-link failure-free IoT network is considered

Figure 5.28 depicts a 600-byte multimedia traffic configured to communication from transmitter node A to receiver node X.

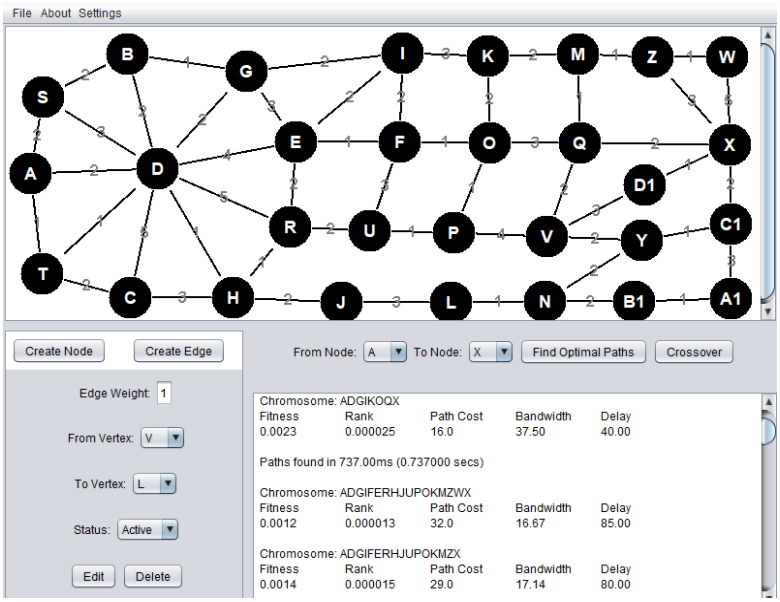

Figure 5.28: A node-link failure-free IoT network.

Table 5.25 displays the paths produced by Figure 5.28.

Table 5.25: Paths that were initially generated (first generation)

Paths (Seria No.)	Paths (Chromosomes)	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay (s)
1	A – D – G – I – F – O – Q – X	0.0026	0.000028	14	33.33	40
2	A – D – G – E – I – F – O – K – M – Q - X	0.0021	0.000023	19	24.00	55
3	A – D – G – E – I – F – O – Q – V – D1 – X	0.0019	0.000021	21	26.09	55
4	A – D – G – E – I – F – O – Q – X	0.0023	0.000025	17	31.58	45
5	A – D – G – I – E – R – U – P – O – Q – X	0.0021	0.000023	19	24.00	55
6	A – D – G – I – E – R – U – P – V – D1 - X	0.0019	0.000021	21	26.09	55
7	A – D – G – I – E – F – O – K – M – Q – X	0.0023	0.000025	17	22.22	55
8	A – D – G – I – E – F – O – Q – X	0.0026	0.000027	15	28.57	45
9	A – D – G – I – K – M – Z – W – X	0.0022	0.000023	18	33.33	45
10	A – D – G – I – K – M – X	0.0026	0.000027	15	35.29	40
11	A – D – C – H – R– E – F – O – Q – X	0.0020	0.000021	20	30.00	50
12	A – D – H – R– U – P – V – Q – X	0.0026	0.000027	15	28.57	45
13	A – D – H – R– U – F – I – K – M – Q – X	0.0021	0.000023	19	24.00	55
14	A – D – H – R– U – F – 0 – K – M – Z – X	0.0022	0.000024	18	23.08	55
15	A – D – H – R– U – F – O – K – M – Q – X	0.0023	0.000025	17	22.22	55
16	A – D – H – R– U – F – O – P – V – Q – X	0.0021	0.000023	19	24.00	55
17	A – D – H – R– U – F – O – Q – X	0.0026	0.000027	15	28.57	45
18	A – D – E – G– I – F – O – K – M – Q – X	0.0019	0.000021	21	26.09	55
19	A – D – E – F– U – P – O – Q – X	0.0023	0.000025	17	31.58	45
20	A – D – E – F– U– P – V – Y – C1 – X	0.0020	0.000021	20	30.00	50
21	A – D – R – U– P – O – K – M – Z– X	0.0021	0.000023	19	28.57	50
22	A– D – R – U– P – O – Q – X	0.0020	0.000025	15	37.50	40

New Population

The various iterations generated by the evolutionary cycle of investigation 3.1 are depicted in Table 5.26.

Table 5.26: Investigation 3.1's evolutionary cycle

2nd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A –D–G – I – F– O– Q – X	0.0026	0.000028	14	33.33	40
A–D – H – R– U – P – V – Q – X	0.0026	0.000027	15	28.57	45
A –D – H – R– U – F – O – Q – X	0.0026	0.000027	15	28.57	45
A – D – G – I – K – M – X	0.0026	0.000027	15	35.29	40
A – D – G – E – I – F – O – Q – X	0.0023	0.000025	17	31.58	45
A – D – G – I – E – F – O – K – M – Q – X	0.0023	0.000025	17	22.22	55
A – D – H – R– U – F – O – K – M – Q – X	0.0023	0.000025	17	22.22	55
A – D – E – F – U – P – O – Q – X	0.0023	0.000025	17	31.58	45
A – D – H – R – U – F – O – K – M – Z – X	0.0022	0.000024	18	23.08	55
3rd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A – D – G – I – F – O – Q – X	0.0026	0.000028	14	33.33	40
A – D – H – R– U – P – V – Q – X	0.0026	0.000027	15	28.57	45
A – D – H – R– U – F – O – Q – X	0.0026	0.000027	15	28.57	45
A – D – G – I – K – M – X	0.0026	0.000027	15	35.29	40
4th Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A – D – G – I – F – O – Q – X	0.0026	0.000028	14	33.33	40
A – D – G – I – K – M – X	0.0026	0.000027	15	35.29	40

The transferring path is chosen among the most recently produced population, with the transferring path with the highest ranking and lowest path cost taken into account; the path is A–D–G–I–F–O–Q–X, with a transmission capacity of 33.33 Kbytes/s. The optimal alternative path uses 0.7370 seconds to produce.

5.3.6 Investigation 3.2: An IoT network with 1-node and 1-link failure is considered (Failed Node: H, failed link: H – J)

In investigation 3.2, a multimedia packet of weigth 700-bytes is sent for rerouting from transmitting node A to receiving node X.

The transferring path is obtained in the most recently produced population, with the route with the highest ranking and minimum path cost being A – D – R– U – P – V – Q – X, and it utilizes a capacity of 50 Kbytes/s. The optimal alternative path uses 0.7820 seconds in producing a path.

Routing in investigation 3.1 is faster than rerouting in investigation 3.2 because there is 0-node and 0-link failure in investigation 3.1 whereas there is 1-node and 1-link failure in investigation 3.2. Table 5.24 describes the detailed results.

5.3.7 Investigation 3.3: An IoT network with 1-node and 2-link failures (Failed node: H and failed links: H – J and G – I)

In Figure 5.29, a multimedia packet of weigth 650-bytes is sent for rerouting from transmitting node A to receiving node X.

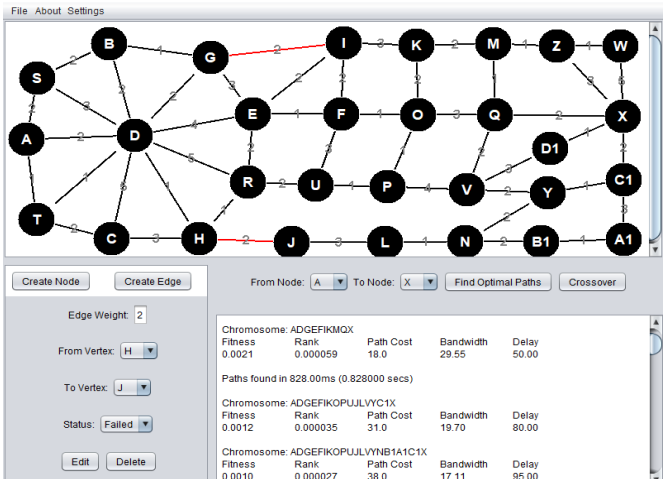

Figure 5.29: Network with two link failures at H – J and G – I

Table 5.27 displays the routes produced by Figure 5.29.

Table 5.27: Paths that were initially generated (1st generation)

Serial No.	Routes (Chromosomes)	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay (s)
1	A – D – G – E – F – I – K – M – Q – X	0.0021	0.000059	18	29.55	50
2	A – D – G – E – F – I – K – O – Q – X	0.0019	0.000054	20	32.50	50
3	A – D – G – E – F – U – P – O – Q – X	0.0021	0.000059	18	29.55	50
4	A – D – G – E – F – O – K – M – Q – X	0.0023	0.000066	16	27.08	50
5	A – D – G – E – F – P – V – Y – C1 – X	0.0020	0.000057	19	26.00	55
6	A – D – G – E – F – O – P – V – D1 – X	0.0021	0.000059	18	29.55	50
7	A – D – G – E – F – O – Q – X	0.0025	0.000071	14	36.11	40
8	A – D – G – E – I – K – M – Z – X	0.0021	0.000058	18	36.11	45
9	A – D – H – R – U – P – O – K – M – Z – X	0.0023	0.000066	16	23.21	55
10	A – D – H – R – U – P – O – Q – V – D1 – X	0.0022	0.000063	17	20.07	55
11	A – D – H – R – U– P – V – D1 – X	0.0024	0.000068	15	30.95	45
12	A – D – E – F – U– P – V – D1 – X	0.0019	0.000055	19	38.24	45
13	A – D – E – F – U– P – V – Q – X	0.0019	0.000055	19	38.24	45
14	A – D – E – F – O – Q – X	0.0025	0.000072	13	43.33	35
15	A – D – E – I – K– M – Q – X	0.0022	0.000062	16	40.63	40
16	A – D – R – E – F– O – Q – X	0.0022	0.000062	16	40.63	40

New Population

Table 5.28 displays the various generations obtained during the evolutionary cycle of investigation 3.3.

Table 5.28: Investigation 3.3's evolutionary cycle

2nd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A –D – G – E – F – O – Q – X	0.0025	0.000071	14	36.11	40
A –D – H – R – U– P – V – D1 – X	0.0024	0.000068	15	30.95	45
A – D – H – R – U – P – O – K – M – Z –X	0.0023	0.000066	16	23.21	55
A – D – E – F – O– Q – X	0.0025	0.000072	13	43.33	35
A – D – H – R– U – P – O – Q–V– D1 –X	0.0022	0.000063	16	20.07	55
A – D – E – I – K– M – Q – X	0.0022	0.000062	16	40.63	40
A – D – R – E – F– O – Q – X	0.0022	0.000062	16	40.63	40
A – D – G – E – I – K – M –Z – X	0.0021	0.000058	18	36.11	45
3rd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A –D – G – E – F – O – Q – X	0.0025	0.000071	14	36.11	40
A –D – E – F – O– Q– X	0.0025	0.000072	13	43.33	35
A –D – H – R – U– P–V–D1 – X	0.0024	0.000068	15	30.95	45
A –D – H – R– U– P– O – K– M – Z – X	0.0023	0.000066	16	23.21	55
4th Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A –D – G – E – F – O – Q – X	0.0025	0.000071	14	36.11	40
A –D – E – F – O – Q – X	0.0025	0.000072	13	43.33	35

The rerouting path is chosen in the most recently produced chromosomes, with the path with the top ranking and lowest path cost, which is A–D–E–F–O–Q–X, and it uses a capacity of 43.333 Kbytes/s. The optimal alternative path used 0.8280 seconds to produce. The iteration stops here because new path with better fitness will not be produced with further iteration.

When investigations 3.3 and 3.2 are compared, it is shown that rerouting is quicker in investigation 3.2 than that in investigation 3.3 because the amount of node to link outages in investigation 3.3 is greater than the amount of node to link outages in investigation 3.2.

5.3.8 Investigation 3.4: An IoT network with 2-node and 3-link failures is considered (Failed node: H and G; failed links: H–J, G–I and D–H)

In investigation 3.4, a multimedia packet of weigth 300-bytes is sent for rerouting from transmitting node A to receiving node X.

The transferring route is obtained in the most recently produced population, with the route with the highest ranking and minimum path cost being A–S–D–E–I–K–M–Z–X, and it uses a capacity of 18.75 Kbytes/s. The optimal alternative path uses 0.8280 seconds to generate.

When comparing investigations 3.4 and 3.3, it is shown that rerouting is quicker in investigation 3.3 than in investigation 3.4 because the rerouting duration in investigation 3.3 is less than that of investigation 3.4. The in-depth outcomes are shown in Table 5.24.

5.3.9 Investigation 3.5: Failure of an IoT network with two nodes and four links is considered (Failed nodes: H and G, Failed links: H-J, G–I, D–H, and D–G)

In Figure 5.30, 480-bytes of multimedia traffic is configured to retransmit from transmitting node A to receiving node X.

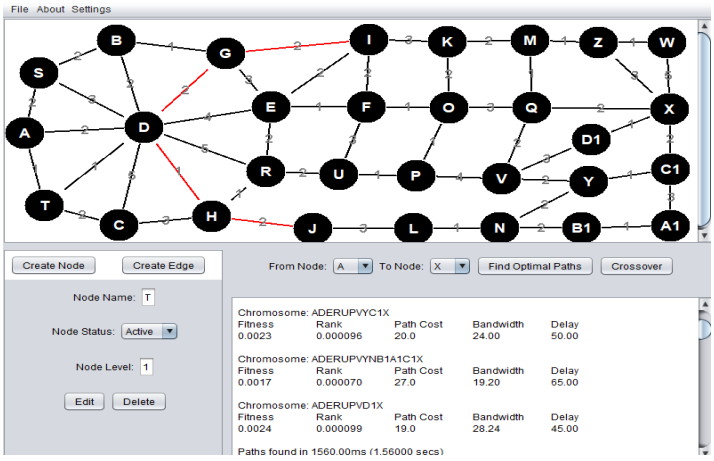

Figure 5.30: Failure of a network with 2-nodes and 4-links

Initial-Population: Figure 5.30 generates two chromosomes (routes), which comprise the population at the start

New-Population

Table 5.29 displays the various generations obtained during the evolutionary cycle of investigation 3.5.

Table 5.29: Investigation 3.5's evolutionary cycle

2nd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A–D–E–F –O– K–M –Z – X	0.0028	0.000117	16	24	45
A –D –R – E– F– O – Q – X	0.0027	0.000114	16	30	40
3rd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A–D–R –E – F – O –Q–X	0.0027	0.000114	16	30	40

The retransmitting route is chosen in the most recently produced chromosomes, with the path with the lowest path cost and delay being A–D–R–E–F–O–Q–X, with a transmission capacity of 30 Kbytes/s. It requires 1.1560 seconds to produce the best possible alternative path.

5.3.10 Investigation 3.6: An IoT network with 3-node and 5-link failures (Node failures: H, C and G; Link failures: H–J, G–I, C–H, B–G and I–E)

In investigation 3.6, a 400-byte multimedia message is configured to rerouting from transmitting node A to receiving node X. The transferring route is obtained in the most recently produceded population, and the path with the best ranking and lowest path cost is taken into account, which is A – D – E – F – I – K – M – Z – X, with a transmission bandwidth of 22.22 Kbytes/s. The alternative path requires 1.1700 seconds to generate.

Rerouting is slower in investigation 3.6 than investigation 3.5 owing to higher number of node and link failures and higher rerouting time generated in investigation 3.6, (see Table 5.24 for the pattern).

5.3.11 Investigation 3.7: Failure is considered for an IoT network with 6-nodes and 6-links (Node failures: H, G, and I, Failed links: H–J, G–I, D–H, D–G, I–E, and H–R)

Figure 5.31 shows a multimedia traffic of 500 Bytes being rerouted from transmitting node A to receiving node X.

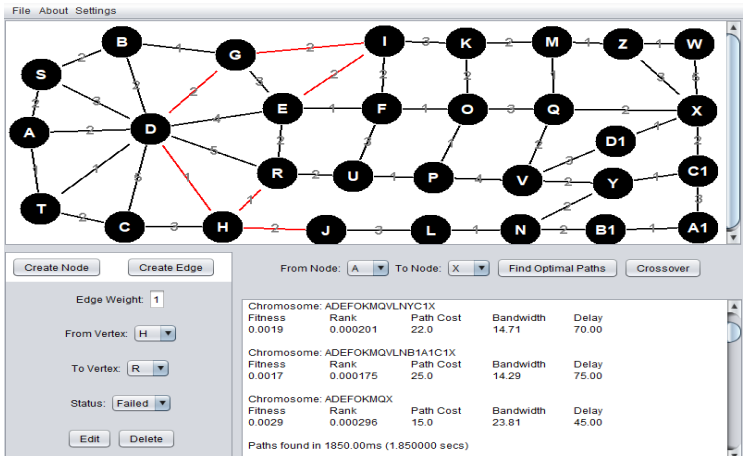

Figure 5.31: Failure of a network with 4-nodes and 6-links

Initial Population: Figure 5.31 generates 6 chromosomes (paths), which comprise the population at the start.

New Population

Table 5.30 displays the various generations obtained during evolutionary iterations of investigation 3.7.

Table 5.30: Investigation 3.7's evolutionary cycle

2nd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A – D – E – F – O – K – M – Q – X	0.0029	0.000296	15	23.81	45
A – D – E – F – O – K – M – Z – X	0.0027	0.000280	16	25.00	45
A – D – R – U – P – O – Q – X	0.0026	0.000274	16	31.25	40
3rd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A – D – E – F – O – K – M – Q – X	0.0029	0.000296	15	23.81	45
A – D – E – F – O – K – M – Z – X	0.0027	0.000280	16	25.00	45
4th Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
A – D – E – F – O – K – M – Q – X	0.0029	0.000296	15	23.81	45

The rerouting route is A–D–E–F–O–K–M–Q–X, and the rerouting capacity is 23.811 Kbytes/s. The best possible alternative path takes 1.18500 seconds to generate. Figure 5.31 depicts a typical prototype developed in this study. Despite the occurrence of 6-node and 6-link failures in this experiment, the system was able to generate an alternative path. The system is capacity efficient and reroutes messages in real time despite multiple failures. It is worth noting to say that the experiment performed here serves as a follow up on objectives 1 and 2.

5.3.12 Investigation 3.8: Consider an IoT network with four node and seven link failures (Failed node: H, G, C and I; Failed links: H – J, G – I, C – H, B – G, I – K, H – R and G – I)

In investigation 3.8, a 550-byte multimedia message is sent for rerouting from transmitting node A to receiving node X. The transferring route is chosen in the most recently produced chromosomes, with the route with the highest ranking and lowest path cost being: A–D–E–F–O–P– V–D1–X, and it utilizes a capacity of 28.95 Kbytes/s for rerouting. The optimal alternative path utilizes 1.2030 seconds to produce. The iteration ends in third generation since only one path survives to this generation.

Since the larger weight of the packet retransmitted in investigation 3.8, the bandwidth utilized is greater than that used in investigation 3.7. The rerouting time generated in investigation 3.8 is higher which also contributed to slower rerouting; Table 5.24 shows the detailed results.

5.3.13 Comparing the suggested approach to common routing protocols

The metric used to measure performance is mean throughput, which is calculated as the proportion of the total number of data that a sender sends to a receiver to the time it takes the receiver to obtain the last packet [110]. NS2 undertaken a comparative and performance assessment of three protocol: Dijkstra, reactive (AODV), and proactive (DSDV) [111] and the suggested technique. The following parameters were used in the simulation investigation to determine the mean throughput (see Table 5.31). As shown in Table 5.32, the simulation outcomes explain the mean throughput of the Dijkstra, (AODV), (DSDV), and proposed model.

Table 5.31: Environment for simulation

Environment	**Value**
Coverage area	550m * 550m
Investigational time	100 - 500 sec.
Transfer distance	20m
Media access control protocol	802.15.4 IEEE
Transfer velocity	5 m/s
Message weight	512 Bytes
The nodes quantity	100
The User Datagram Protocol connection	5~20
Transfer rate	4 kBps

Table 5.32: Mean network throughput for 30-nodes

Mean Throughput (Kbps)	100	200	300	400	500
Enhance Genetic Algorithm	621.6	618.5	610.6	607.2	590.0
Dijkstra	619.3	617.4	608.5	605.7	588.0
Destination Sequenced Distance Vector	555.9	543.0	540.7	532.4	515.6
Ad-hoc On-Demand Distance Vector	501.0	480.2	475.3	468.6	460.3

Figure 5.32 represents the graphical interpretation of Table 5.32.

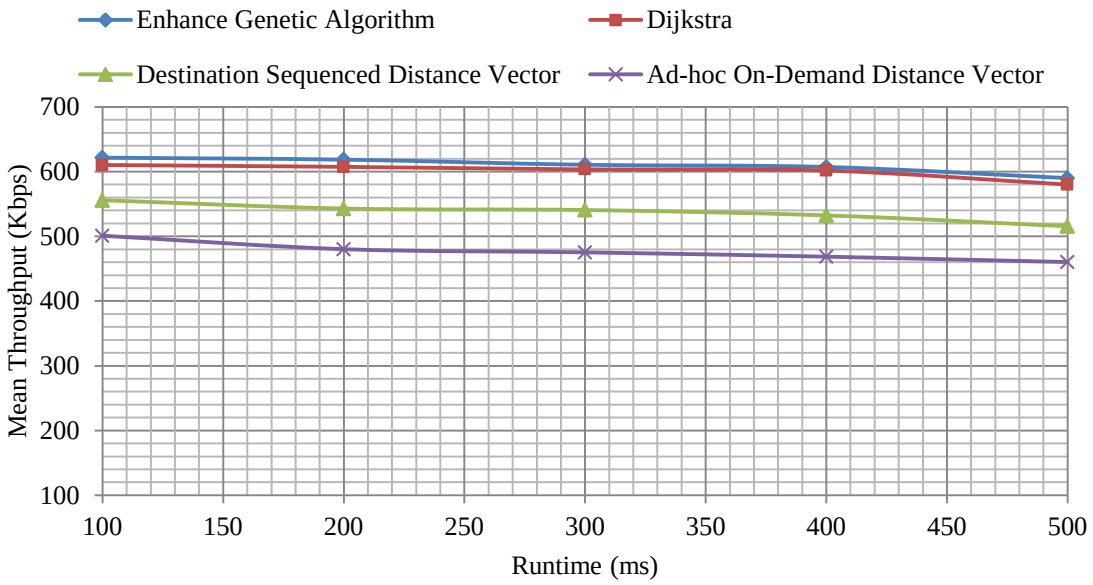

Figure 5.32: Mean throughputs vs. runtime of routing models

According to the simulation results depicted in Figure 5.32, the EGA model's mean throughput value significantly outperformed the other three routing algorithms in terms of throughput. Since there is no node or link outage in this case, the highest mean throughput is achieved at time 100ms, and it is noticed that as rerouting time increases, node-link failures increase while mean throughput value decreases, thereby leading to poorer connectivity. As a result, routes take 500 ms longer due to increasing node-link failure, lowering mean throughput.

5.3.14 IoT Network scalability

A scalable network must be able to adapt when failures occur, it should continue to function until the problem is resolved. It does not require full deployment to function, allowing for gradual rollout and tweaks along the way. It is also used in wireless networks that employ various access technologies [112]. This network system uses a horizontal scaling approach for scaling. This scaling is used because it can increase capacity by connecting multiple hardware or software entities so that they can work as a single unit. This research increased the number of nodes as a result of the networks' scalability:

- At 20 nodes network, the network is scalable because the network can still accommodate more nodes and at this time memory is expanded since required bandwidth is calculated to transmit the traffic. Transmission time is not increasing unless there is node failure on the network. Increase node failures increase the memory usage and transmission time also increases. (See Table 5.8 for performance analysis of the investigations (2.1 – 2.6)).

- At 26 nodes network, increasing number of nodes in this network will not affect the transmission time and memory usage since the required bandwidth calculated will not affect the memory usage and transmission time. (See Table 5.13 for performance analysis of the investigations (2.7–2.13) and Table 5.34 for performance analysis of investigations 4.1–4.7).
- At 30 nodes network, the network is scalable as the increase number of node in the network will not increase memory usage and transmission time thereby (see Tables 5.18 for performance analysis of the investigations (2.14 – 2.21), Table 5.24 for performance comparison of investigations (3.1–3.8).

It can be seen from these tables that as node failures increase so also transmission time also increases and the failure increases that means memory usage will also increases meanwhile if there is no node failure the memory usage and transmission time will remain minimal.

Since node and link failures are the most common types of failures in IoT networks, the different failure in IoT network (node-link) is considered [113] [114].

5.3.15 Suggested IoT network infrastructure

Increased speed and bandwidth are the most talked-about 5G features. This is applicable to the experiments performed in sections 5.1, 5.2, 5.3, and 5.4 because the rerouting paths are generated in real time, as is the bandwidth required to reroute messages. With data rates of up to 10 Gbps, 5G will be 10 to 100 times faster than current 4G LTE technology [115]. Using 5G as a backbone for IoT network transmission will improve performance and yield better results due to its capabilities.

5G density allows for up to 100 times the number of connected devices in the same physical area as 4G LTE today, while maintaining 99.999 percent availability. These are the scalability and availability features of 5G that allow message rerouting when there are network failures, bringing business advantages for mobile workforces; the real benefit is expanding the mobile customer market. These characteristics demonstrate the benefits of the experiments performed in sections 5.1, 5.2, 5.3, and 5.4 in that the rerouting is done in real-time and the number of nodes can be increased.

The new 5G system must adapt and enable devices and network components to make proactive smart decisions. To provide the best user experience and create a path for both network and

device power efficiency, the network should decide whether to use data using 4G or 5G technology for specific services or applications, using metrics such as remaining battery level, RF strength, network load, and resource availability. Power performance and efficiency have always been considered critical 5G features for optimisation by network operators and device manufacturers, and they have continued to drive energy-efficiency network ideas into 3GPP standards [116]. Since nodes in every wireless network have limited battery power, computational power, and memory, they must conserve energy while routing in order to extend their usefulness and network lifetime. This fact applies to the experiments in sections 5.1, 5.2, 5.3, and 5.4.

5.3.16 Section summary

This research work provided a capacity efficient EGA) that is resistant to multiple IoT node-link failures by producing an optimum solution alternate route with sufficient capacity to reroute multimedia traffic when a connection path fails. For example, connection failure has been shown in simulation investigations 3.1-3.8 to increase the use of bandwidth and cause communication delays, which slows multimedia traffic rerouting. According to research, the bigger the network, the more bandwidth is required to successfully reroute traffic and prolong the rerouting time. The focus of the comparison in section 5.3.13 was the evaluation of other similar routing techniques. In terms of runtime and mean throughput, the proposed model outperformed the AODV and DSDV recovery techniques. In contrast to other evaluated rerouting models, the suggested model reroutes multimedia traffic in real time, as demonstrated in investigations 3.1-3.8.

The prototype is intended to be used as a testing ground for IoT service providers. The suggested capacity efficient EGA model is highly suggested for addressing node-link failures in IoT networks in addition to making IoT networks stable during this pandemic period in which urgent communications are unavoidable. This researcher intends to examine the proposed for high-performance computing (HPC) in order to increase effectiveness.

5.4 INVESTIGATION 4: VIDEO TRAFFIC IS FAULT-TOLERANT TO CASCADED LINK FAILURES CAUSED BY A WIRELESS NETWORK ATTACK

5.4.1 Introduction

The section resolves multiple link failures that occur as a result of a wireless network attack that impeded video traffic on the network. Many network failures have been reported by wireless network service providers, and most research has focused on single failures. This provides a strong impetus for this research. Since most of these attacks result in cascaded link failures in wireless networks, an enhanced genetic algorithm (EGA)-based model is designed to resolve such link-link failures to achieve a fault-tolerant network system during failure occurrences.

The goal of this study was to look into the effectiveness of a capacity-efficient EGA-based model in addressing the impact of cascaded link failures in wireless networks. The study's main contributions are as follows:

(i) The design of a new suggested capacity efficient enhanced genetic algorithm (EGA) model to help wireless network providers survive cascaded link failures caused by fraudulent attacks.

(ii) An analytical scenario for practitioners and detailed investigations to generate alternative paths that reroute video traffic on a sampled complex network of cascaded link failures with the required bandwidth.

5.4.2 Investigational setup: Twenty-six (26) nodes network

As shown in investigations 4.1- 4.7, nodes are labeled from A through to Z, and investigations are conducted at various places of various numbers of link failures. The circles in the simulations represent nodes, the line linking one node to the other indicates a connector called a link, and the link failures are depicted in the labeled figures, as are the optimum solution alternate paths generated. Tables, figures, and outcomes are shown in investigation 4.5, while Table 5.34 displays outcomes from investigations 4.1-4.4 and 4.6-4.7. The link costs are generated at random. Source node B sends video traffic to destination node Z. Figure 5.33 depicts the transition diagram for the twenty-six node network. The investigation is carried out using Java language programming owing to its capability in network restoration programming. Link costs are generated randomly.

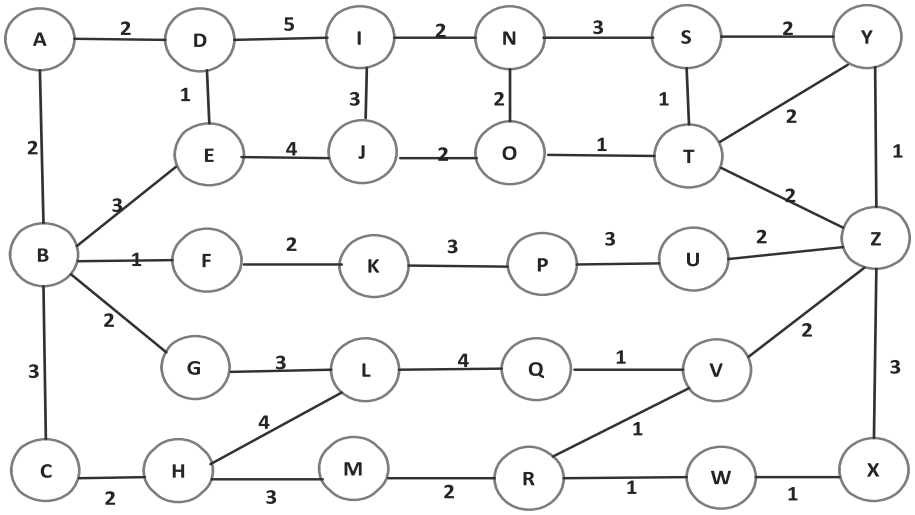

Figure 5.33: A transition illustration indicating a network of twenty-six nodes

Table 5.33 depicts the parameters for the capacity efficient EGA in investigations 4.1-4.7.

Table 5.33: Specification of parameters

EGA Properties	Number of Node	Crossover Probability	Video Size (Bytes)	Starting (Initial) Time(s)	IP-Header	Failed Link
Characteristics	variable	0.50	Varied	0.005	20-bytes	variable

The mentioned tests are performed:

In investigation 4.1, a wireless network with no link failure is considered;

Investigation 4.2 considers a wireless network with one link failure;

Investigation 4.3 considers a wireless network with two links failure;

Investigation 4.4 considers a wireless network with three links failure;

Investigation 4.5 considers a wireless network with four links failure;

Investigation 4.6 considers a wireless network with five links failure, and

Investigation 4.7 considers a wireless network with six links failure. (See Table 5.33 for the results).

5.4.3 Summarized investigations: Performance analysis of a twenty-six (26) node network with a varying number of link failures

The effectiveness of a network of twenty-six nodes with varying numbers of link failures is seen in Table 5.34.

Table 5.34: Performance analysis of investigations 4.1–4.7

Exp. No.	Number of link failure	Transmission Time/s	Bandwidth /Kbytes/s	Fitness	Path Cost	Video Size/ Bytes	Path Generated
4.1	0	0.088	37.50	0.0039	9	500	B – G – L – Q – V – Z
4.2	1	0.098	42.31	0.0034	9	600	B – G – L – Q – V – Z
4.3	2	0.162	40.00	0.0031	11	550	B – F – K – P – U – Z
4.4	3	0.170	53.85	0.0026	11	700	B – F – K – P – U – Z
4.5	4	0.218	25.00	0.0045	12	300	B – E – J – O – T – Z
4.6	5	0.234	33.33	0.0036	13	400	B – C –H– M– R – V – Z
4.7	6	0.256	36.67	0.0037	12	450	B – G – K – P – U – Z

As shown in Table 5.34, the lower the number of network link failures, the shorter the rerouting time and the faster the speed of video traffic rerouting. The larger the video traffic, the more bandwidth is required to reroute it over the wireless network. Owing to space limitations, only investigation 4.5 is detailed.

5.4.4 Investigation 4.1: Consider a wireless network with no link failure

In Figure 5.34, a 500-byte video message is scheduled for communication from transmitting node B to receiving node Z.

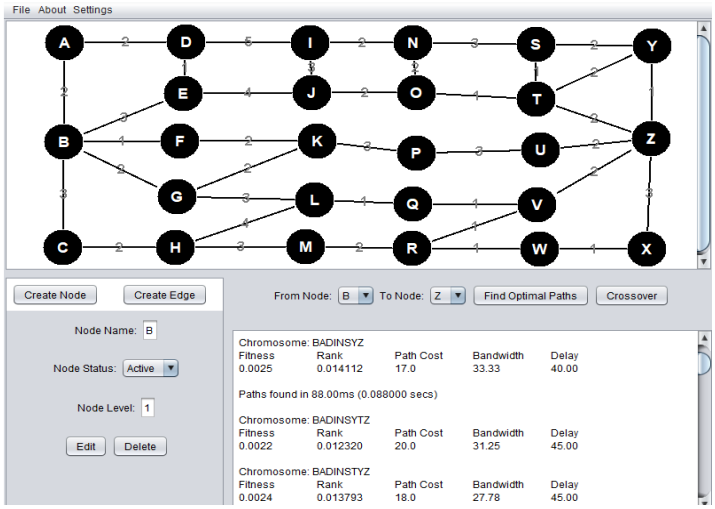

Figure 5.34: Network with no link failures

Table 5.35 displays the paths produced by Figure 5.34.

Table 5.35: Paths that were initially generated

Serial No.	Rerouting Paths	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay (s)
1	B – A – D – I – N – S – Y – Z	0.0025	0.0141	17	33.33	40
2	B – E – D – I – N – S – Y – Z	0.0025	0.0141	17	33.33	40
3	B – E – J – I – N – O – T – Z	0.0025	0.0141	17	33.33	40
4	B – F – K – P – U – Z	0.0034	0.0191	11	38.46	30
5	B – G – L – Q – V – Z	0.0039	0.0224	9	37.50	30
6	B – G – L – Q – V – R – W – X – Z	0.0032	0.0182	13	21.74	45
7	B – G – L – H – M – R – V – Z	0.0025	0.0141	17	33.33	40
8	B – C – H – L – Q – V -- Z	0.0031	0.0175	13	33.33	35
9	B – C – H – M – R – V – Z	0.0031	0.0175	13	33.33	35
10	B – C – H – M – R – W – X – Z	0.0028	0.0160	15	29.41	40

New population

The different generations obtained in the developmental cycle of investigation 4.1 are shown in Table 5.36.

Table 5.36: Investigation 4.1's evolutionary cycle

2nd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(ms)
B – F – K – P – U – Z	0.0034	0.0191	11	38.46	30
B – G – L – Q – V – Z	0.0039	0.0224	9	37.50	30
B – C – H – L – Q – V -- Z	0.0031	0.0175	13	33.33	35
B – C – H – M – R – V – Z	0.0031	0.0175	13	33.33	35
B – C – H – M – R – W – X – Z	0.0028	0.0160	15	29.41	40
3rd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(ms)
B – F – K – P – U – Z	0.0034	0.0191	11	38.46	30
B – G – L – Q – V – Z	0.0039	0.0224	9	37.50	30
B – C – H – M – R – V – Z	0.0031	0.0175	13	33.33	35
4th Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(ms)
B – G – L – Q – V – Z	0.0039	0.0224	9	37.50	30

The best alternative path found is B – G – L – Q – V – Z. The message requires 37.50 Kbytes/s of bandwidth to be routed. Since only one chromosome is generated here, the iteration ends at the fourth generation. The time required to generate the best alternative path is 0.0880 seconds.

5.4.5 Investigation 4.2: Wireless network with one link failure (Failed link: H – L)

In investigation 4.2, a 600-byte video message is configured for rerouting from transmitting node B to receiving node Z. The best alternative path found is B – G – L – Q – V – Z, which has a bandwidth of 40 Kbytes/s. The best alternative path takes 0.0980 seconds to generate.

When comparing routing in investigation 4.1 to rerouting in investigation 4.2, it is discovered that the same transmission paths are generated in both investigations 4.1 and 4.2, but transmission in investigation 4.1 is still faster than rerouting in investigation 4.2 due to link failure in investigation 4.2. The detailed results are shown in Table 5.34.

5.4.6 Investigation 4.3: Consider a wireless network with two link failures (Failed links: H–L and G–L)

In figure 5.35, a 550-byte video message is configured for rerouting from transmitting node B to receiving node Z.

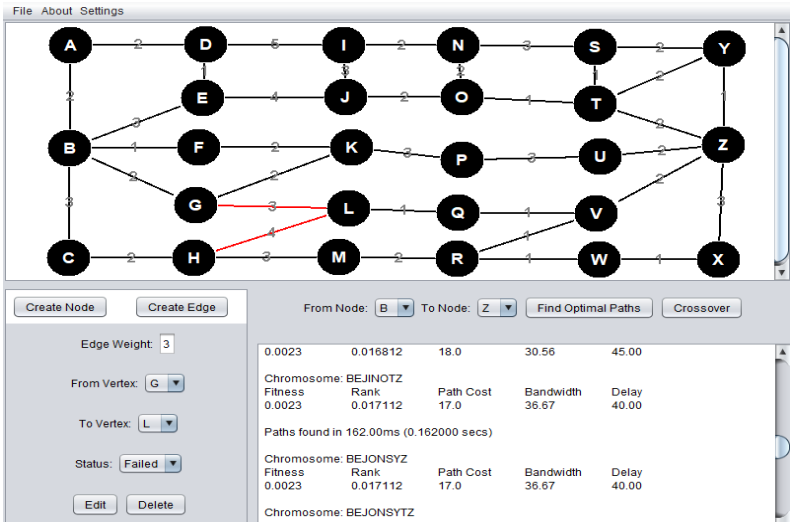

Figure 5.35: Two link failures in the network at H – L and G – L

Table 5.37, shows the initial generated paths from Figure 5.35

Table 5.37: Paths that were initially generated (1st generation)

Serial No.	Rerouting Paths (Chromosomes)	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay (s)
1	B – A – D – I – N – S – Y – Z	0.0023	0.0171	17	36.67	40
2	B – E – D – I – N – S – Y – Z	0.0023	0.0171	17	36.67	40
3	B – E – J – I – N – O – T – Z	0.0023	0.0171	17	36.67	40
4	B – F – K – P – U – Z	0.0031	0.0230	11	42.31	30
5	B – C – H – M – R – V – Z	0.0029	0.0211	13	36.67	35
6	B – C – H – M – R – W – X – Z	0.0026	0.0194	15	32.35	40

New population

The various iterations obtained by the developmental cycle of investigation 4.3 are shown in Table 5.38.

Table 5.38: Investigation 4.3's evolutionary cycle

Second Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
B – F – K – P – U – Z	0.0031	0.0230	11	42.31	30
B – C – H – M – R – V – Z	0.0029	0.0211	13	36.67	35
B – C – H – M – R – W – X – Z	0.0026	0.0194	15	32.35	40
Third Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
B – F – K – P – U – Z	0.0031	0.0230	11	42.31	30
B – C – H – M – R – V – Z	0.0029	0.0211	13	36.67	35
Fourth Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
B – F – K – P – U – Z	0.0031	0.0230	11	42.31	30

B – F – K – P – U – Z is the best alternative path. The bandwidth needed to retransmit the packet is 42.31 Kbytes/s. The optimal alternative path takes 0.1620 seconds to generate. The iteration ends at the fourth generation because only one chromosome crossover occurred in the previous generation.

Owing to the higher link failures of investigation 4.3, the rerouting process in investigation 4.2 is faster in investigation 4.3, and transfer time is longer in investigation 4.3 than in investigation

4.2. The slower rerouting in investigation 4.3 can also be attributed to the higher path cost (11) generated, whereas investigation 4.2 generates a lower path cost (9).

5.4.7 Investigation 4.4: Consider a wireless network with three link failures (Failed links: H –L, G – L and D – I)

In investigation 4.4, a 700-byte video message is configured to transfer from transmitting node B to receiving node Z. The best alternative path found is B – F – K – P – U – Z, which has a capacity of 53.85 Kbytes/s. The required time to produce the best alternate route is 0.1700 seconds.

By comparing rerouting in investigations 4.3 and 4.4, it was discovered that the same rerouting path generated in investigation 4.3 is also generated in investigation 4.4. Since this is the smaller size of the rerouted video message and the lower number of link failures in investigation 4.3, rerouting is faster than in investigation 4.4 (see transmission time). The two investigations have the same path cost and transmission delay value, but due to the different sizes of video messages, they were not rerouted on the same bandwidth. (The pattern can be found in Table 5.34).

The best alternative path found is B – G – L – Q – V – Z. The message requires 37.50 Kbytes/s of bandwidth to be routed. Because only one chromosome is generated here, the iteration ends at the fourth generation. The best alternative path takes 0.0880 seconds to generate.

5.4.8 Investigation 4.5: Consider a wireless network with 4-failed links (Failed links: H - L, G – L, D – I and F – K)

Figure 5.36 shows a video traffic of 300 Bytes being rerouted from transmitting node B to receiving node Z.

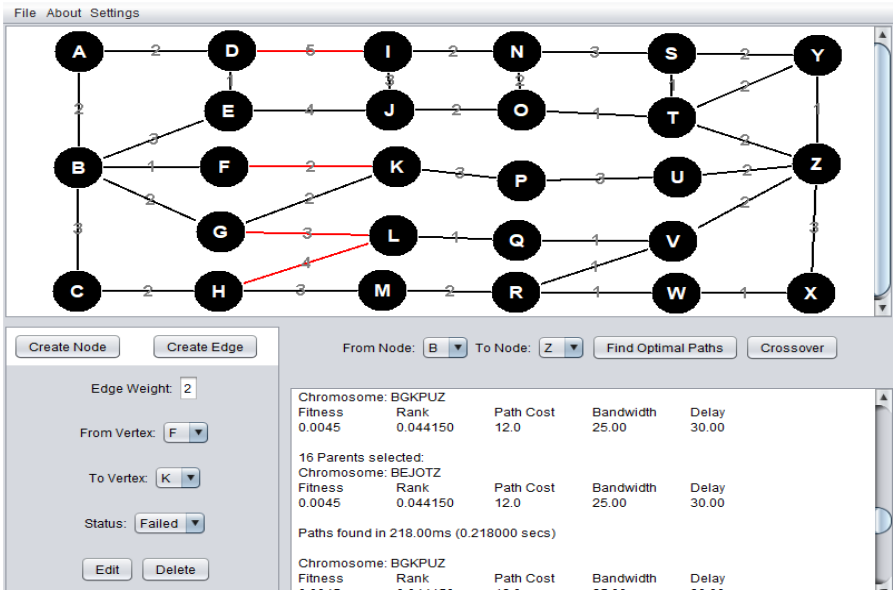

Figure 5.36: Link failure at H – L, G – L, D – I and F – K

Figure 5.36 generates 4 chromosomes (routes), which constitute the candidate solution.

Table 5.39 depicts the developmental cycle of investigation 4.5.

Table 5.39: Investigation 4.5's evolutionary cycle

2nd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
B– E – J – O – T – Z	0.0045	0.0442	12	25.00	30
B–C–H–M –R–V– Z	0.0043	0.0424	13	20.00	35
3rd Generation	Fitness	Rank	Path Cost	Bandwidth (Kbytes/s)	Delay(s)
B – E – J – O – T – Z	0.0045	0.0442	12	25.00	30

The best alternative path found is: B – E – J – O – T – Z. To perform rerouting, it consumes 25 Kbytes/s of bandwidth. It takes 0.2180 seconds to find the best path.

When rerouting in investigation 4.5 is compared to rerouting in investigation 4.4, it is discovered that the greater the number of link failures, the greater the bandwidth used in rerouting in investigation 4.5. It is stated that amount of failed links rises, so does the rerouting period. Owing to higher link failure recorded in investigation 4.5, the path cost is higher than in investigation 4.4, making rerouting faster in investigation 4.4 than in investigation 4.5.

5.4.9 Investigation 4.6: Consider a wireless network with five links failure (Failed links: H – L, G – L, D – I, F – K and E – J)

In investigation 4.6, a 400-byte video message is configured for rerouting from transmitter node B to receiver node Z. The best alternative path found is B – C – H – M – R – V – Z, which has a

bandwidth of 26.67 Kbytes/s. The time required to generate the best alternative path is 0.2340 seconds.

Since the path fitness and path cost values in investigation 4.5 are higher than those in investigation 4.6, the rerouting path obtained in investigation 4.5 is of best quality than that of investigation 4.6. As a result, rerouting in investigation 4.5 is faster than rerouting in investigation 4.6. (The pattern can be found in Table 5.34).

5.4.10 Investigation 4.7: Consider a wireless network with six links failure (Failed links: H – L, G – L, D – I, F – K, E – J and H – M

In Figure 5.37, a 450-byte video message is configured for rerouting from transmitting node B to receiving node Z.

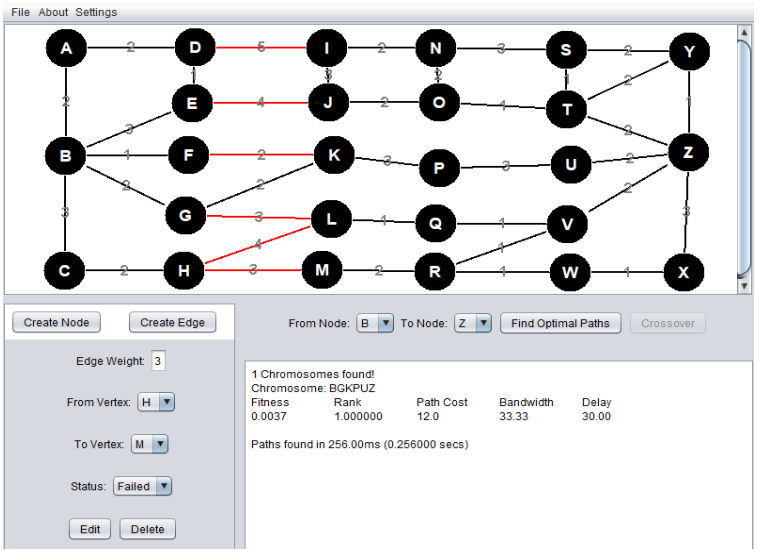

Figure 5.37: Link failure at H – L, G – L, D – I, F – K, E – J and H – M

The best alternative path generated is B – G – K – P – U – Z. This is the only surviving rerouting path. The bandwidth used in rerouting is 33.333 Kbytes/s, and it requires 0.256 seconds to produce the optimal alternative path. As a result of the increased link failures and longer rerouting time in investigation 4.7, rerouting is slower than in investigation 4.6.

5.4.11 Comparing the suggested model to the well-known Dijkstra model

The runtime of capacity efficient EGA is $O\left(\frac{2kln2}{2^k-1}N\right)$, K indicates the amount of iteration performed to get the optimal alternative path, N indicates the initial population capacity. The runtime of Dijkstra model is also shown by [71] to be O(mlogn), n indicates the amount of nodes inside optimal alternative path, m indicates the amount of connectors [71]. Table 5.40

compares the efficiency of the proposed method of investigations 4.1–4.7 with the Dijkstra model.

Table 5.40: Comparative analysis of capacity efficient EGA and Dijkstra model

Investigation Number	Failed Links	Variables	EGA Model $O\left(\frac{2kln2}{2^k-1}\mathrm{N}\right)$	Dijkstra Model $O(mlogn)$.
1	0	N=10, k=4, n=6, l=9, m=5, $\rho = 0.1$	3.6968	3.8908
2	1	N=8, k=3, n=6, l=9, m=5, $\rho = 0.1$	4.7530	3.8908
3	2	N=6, k=3, n=6, l=11, m=5, $\rho = 0.1$	3.5648	3.8908
4	3	N=6, k=3, n=6, l=11, m=5, $\rho = 0.1$	3.5648	3.8908
5	4	N=4, k=2, n=6, l=12, m=5, $\rho = 0.1$	3.6968	3.8908
6	5	N=2, k=1, n=7, l=13, m=6, $\rho = 0.1$	2.7726	5.0706
7	6	N=1, k=1, n=6, l=12, m=5, $\rho = 0.1$	1.3863	3.8908

For example, the running time of EGA model of investigation 4.1 in Table 40 is calculated as: $T(k) = \frac{2kln2}{2^k-1}\mathrm{N}$, $T(k) = \frac{2*4\ln 2}{2^4-1} * 10 = \frac{80(0.6932)}{15} = 3.6968$. For the Dijkstra model, the running time: $D(t) = (mlog\ n) = 5\log 6 = 4.6689 = 3.8908$. As indicated in Table 5.40, the lower runtime of the suggested technique shows rerouting is more effective and profitable in the suggested technique than the well-known Dijkstra.

5.5 CHAPTER SUMMARY

This study proposes a capacity efficient EGA for wireless network survivability by producing an optimum solution alternate path to reroute video traffic at every failure stage. Table 5.34 simulation investigations show, among other things, that link failure increases bandwidth usage and causes transmission delay, which slows down video traffic rerouting. It has been observed that the wider the connectivity, the bigger bandwidth is required to adequately reroute a message and the higher the rerouting time. The section 5.4.11 comparison focuses on the evaluation of other similar routing models. For runtime, the suggested model performs better than Dijkstra's models.

The prototype is suggested as a pilot for African telecom service vendors, particularly as a response to making wireless networks fault-tolerant during this global epidemic era, when urgent transmissions are required. The suggested capacity efficient EGA is intended to be used in the resolution of cascaded link failures caused by fraudulent attacks in wireless networks. In order to improve efficiency, this researcher intends to examine the suggested technique on computing with high performance platforms.

Section 3 discusses how this chapter investigated various wireless network survivability issues on existing wireless network survivability models. The various survivability strategies were also explained to understand the performance of different wireless network survivability models. Frameworks for wireless network survivability, known as the capacity efficient EGA and ACS models, were proposed in response to the shortcomings of existing wireless network survivability models.

Capacity efficient EGA and ACS were tested on various wireless network failures in a variety of investigations, and rerouting paths within the networks were generated. A variety of wireless networks of varying sizes are used to demonstrate the resilience of these models. As discussed in section 5.2, a general wireless network investigation was carried out with a focus on wireless networks. According to the findings of the evaluation, capacity efficient EGA and ACS are both durable and dependable.

The EGA was used for additional investigations on IoT and general wireless network environments, as explained in sections 5.3 and 5.4. The most recent EGA investigation was carried out on the N2L and L2L wireless network environments, and the results demonstrate that capacity efficient EGA is a procedure of offering that is continually dependable, strong, and safe wireless network survivability.

Future studies should concentrate on a wide range of wireless network survivability issues. These have been categorised based on the year they were published as well as the type of wireless topic which can assist future researchers to decide what topic to investigate.

Based on the implementations of capacity efficient EGA and ACS in various investigations involving various wireless network survivability usages, it is clear that capacity efficient EGA and ACS are models that can be used in a variety of wireless network areas, irrespective of the length and width, type, or surroundings of the wireless network setup. Capacity efficient EGA and ACS produced similar and dependable outcomes when evaluated on N2N, N2L, and L2L wireless models, demonstrating the model's dependability.

CHAPTER 6: CONCLUSION AND FUTURE WORK

6.1 DISCUSSION OF THE RESEARCH STUDY

In telecom businesses where it is being used, wireless network survivability has made a significant contribution to service quality. However, there are some requirements that must be followed for adoption to be simple. Adoption is heavily influenced by system specification. Chapter 1 focused on wireless network survivability, showing some of the real-world issues faced by wireless network failures caused by hurricanes in some industrialised countries, as depicted in Figures 1.1, 1.2, and 1.3, and how this impacts the telecommunications industry. The research objectives are specified to focus on the topics to be covered and the goals to be achieved. The research questions that are relevant to the research objectives are also developed. The focus of the study is explicitly stated in the contexts of how the research questions are posed and this is addressed at the end. The study's shortcomings are addressed to shed more light on the areas that were left out. This chapter also includes a chapter plan for the rest of the research.

Chapter 2 begins with a comprehensive overview of wireless network survivability, including recovery strategies and challenges that contribute to recovery strategy issues. The gaps that future wireless network optimisation researchers will need to fill are also addressed. The chapter also includes discussion of the structure of wireless network messages, such as voice, video, and multimedia messages. This chapter ends with survivability of wireless networks prone to failures: based on the reviewed literature. An open research structure covering various wireless network challenges such as single link failure, single node failure, multiple link failure, multiple node failure, and multiple node-links failure has also been mapped out. The failures are also explored, as are the optimisation options for resolving them. This open research framework will serve as a guide for future researchers looking into various concerns of wireless network optimisations model.

The purpose of chapter 3 is to examine various survivability solutions to failures in wireless networks in order to discover gaps that future wireless researchers may use as a starting point for their research. The failures of a single link, a single node, multiple links, multiple nodes, and multiple node-links were discovered and divided into sub-themes. The sub-themes were used to construct a wireless network routing system. In Figures 3.4-3.10, it can be seen that ADPV and TORA optimisation techniques addressing failures have received

little attention in the literature. Multiple node failures, as well as failures of multiple nodes to link have also rarely been studied, and should be studied, especially with potential ADPV techniques. Future studies could look at designing resilient, efficient, and accessible routing protocols that take into account all quality-of-service criteria. It is expected that this study will encourage wireless network designers and academics to investigate the proposed research questions in subsection 3.17.1 and other survivability approaches that consider message, voice and video transmissions.

Chapter 4 describes the research design and methodology used for this study. The proposed capacity efficient evolutionary and swarm models are developed in detail in sections 4.1 and 4.2. Mathematical demonstrations of the goal functions and analytical statements applied throughout this chapter were provided. The purpose of this study was to look at how capacity efficient EGA and ACS models were used to solve the listed research problems. The capacity-efficient EGA model framework is made available. Sections 4.2.3 and 4.3.3, respectively, described the mathematical justification of capacity efficient EGA and ACS, illustrating all of the procedures required to build an alternative path in the event of a failure. The methods for assessing and validating the research study are also discussed. This study proposes a novel approach to dealing with the problem of traffic flows in wireless networks caused by repeated failures and attacks.

Chapter 5 proposes a capacity efficient EGA and ACS for wireless network survivability by producing an optimum solution alternate path to reroute voice, video and multimedia traffic at every failure stage. Simulation investigations, as shown in Tables 5.8, 5.13, 5.18, 5.24, and 5.34, show that node-node, link-link, and node-link failures increase bandwidth usage and cause transmission delay, slowing down voice, video, and multimedia traffic rerouting. It has been discovered that the greater the connectivity, the greater the bandwidth required to adequately reroute a message and the longer the rerouting time. The comparison in sections 5.2.36, 5.2.37, 5.2.38, 5.2.39, 5.3.13, and 5.4.11 focuses on the evaluation of other similar routing models. The proposed model outperforms Dijkstra's models in terms of runtime. The suggested framework performs better than the popular Dijkstra algorithm, proactive, adaptive and reactive models, in terms of throughput, packet delivery ratio, speed of transmission, transmission delay and running time. The simulation result of experiments performed on Dijkstra, reactive, proactive, adaptive, and proposed models was determined to back up these claims about the proposed model's performance. The simulation results show that the

proposed model outperforms others, as shown in Table 5.20 of section 5.2.37, with capacity efficient ACS having a PDR of 0.89, Dijkstra having a PDR of 0.086, reactive model having a PDR of 0.83, proactive model having a PDR of 0.83, and adaptive model having a PDR of 0.81. In sections 5.2.38 and 5.2.39, another simulation experiment was carried out to compare the running time of the proposed model with that of other routing models. According to Tables 5.21 and 5.22, the capacity efficient ACS model has an average running time of 169.89ms, while the adaptive model has an average running time of 1837ms and Dijkstra has a running time of 280.62ms. In terms of mean throughput, the capacity efficient EGA model was compared to other routing models. The capacity efficient EGA model has a mean throughput of 621.6, Dijkstra has a mean throughput of 619.3, proactive (DSDV) model has a mean throughput of 555.9, and reactive (AODV) model has a mean throughput of 501.0. Dijkstra is used as a comparison because its mean throughput is closer to that of EGA. According to Table 5.40 of section 5.4.11, capacity efficient EGA has a running time of 3.6968 and Dijkstra has a running time of 3.8908. Based on this analysis, the capacity efficient ACS and EGA outperform the other listed routing algorithms in terms of running time.

The prototype is suggested as a pilot for African telecom service vendors, particularly as a response to making wireless networks fault-tolerant during this global epidemic era, when urgent transmissions are required. The suggested capacity efficient EGA and ACS are intended to be used in the resolution of node-link, cascaded link and node-link failures caused by fraudulent attacks in wireless networks. In order to improve efficiency, this researcher intends to examine the suggested technique on computing with high performance platforms.

6.2 RESOLUTIONS TO RESEARCH OBJECTIVES

The main research objective of this study is to establish a framework for traffic flow survivability in wireless networks with multiple failures. This is accomplished in sections 4.1.2, 4.2, and 4.3. This research goal is met by developing a capacity efficient evolutionary swarm survivability framework based on capacity efficient EGA and ACS models. The model's design takes into account the strengths of the two models, capacity efficient EGA and ACS, which are used to resolve failures while also validating the system. Investigations are carried out in different wireless network failure scenarios, namely N2N, L2L, and L2L of various network sizes, to validate the suggested model's dependability. The investigations, as described in Chapter 5, demonstrated that this model can resolve network failures in wireless

network contexts. The following five study sub-objectives supported the main research objective. These are as follows:

(i) **To design a swarm intelligence system that resolves multiple failures in WATM networks in order to survive node-node failures.** Section 5.1 achieves this goal by conducting investigations to solve multiple WATM network failures.

(ii) **To design a swarm intelligence resilience system based on resource effectiveness and rapid recovery in order to manage node-node failure problems rapidly and improve wireless network service quality.** Section 5.2 achieves this goal by conducting investigations to solve node-node failures in wireless network.

(iii) **To investigate the resilience of an evolutionary computing paradigm focused on resource effectiveness and on-demand recovery in IoT networks to quickly handle node-link failures.** This is achieved in section 5.3.

(iv) **To develop an enhanced genetic algorithm (EGA) that focuses on capacity efficiency and fast restoration in order to quickly handle link-link failures on a large node network.** This is also achieved in section 5.3.

(v) **To develop methods for creating a comprehensive blueprint for wireless network failure survivability research designs that academics and practitioners can use in the future. This is intended to make it easier to identify additional key wireless network survivability issues that are not covered in this study but which must be addressed.** This is accomplished through the research conducted in Section 3.

6.3 SUMMARY OF CONTRIBUTIONS

6.3.1 Intellectual merit/contributions

This research investigation has contributed significantly by identifying the failures that occur in wireless networks that are worth resolving with a wireless survivability model using findings in the existing literature. Sections 3.5.1-3.5.5 identified and discussed these failures.

An adequate investigation was also carried out to confirm the choice of such failures, to demonstrate the researcher's objective opinion in the selection of such failures. This contributes significantly to the investigation of future researchers that may wish to expand on what already exists on wireless network failures uncovered for the purposes of this research.

Furthermore, the review of the available literature assisted in the identification and categorisation of existing wireless network failures that had to be dealt with. This enables any prospective researcher to address these flaws in their pursuit of a discrepancy in the field of wireless network survivability.

The methodology used in this research study is systematic in the sense that a structured approach to identifying issues in the form of failures was used from the beginning. This is covered in the intelligence gathering findings, which show the failures of the wireless network, as shown in sections 5.1.1 – 5.4.10.

This study's methodology includes the use of various mathematical and analytical strategies, such as the EGA and ACS approaches. This is backed by system test cases that provide a strong and reliable performance analysis of the method, which has passed the reliability test by adapting the network's links and nodes.

The inclusion of mathematical computations in the methodology, supported with real-life scenarios, makes it strong and smart in providing the required information for wireless network providers in making decision appropriately.

The model's capacity to develop a newly suggested model is a significant contribution to capacity efficient EGA and ACS model and fast restoration that could assist wireless network users to survive multiple network outages includes: node-node, link-link and node-link failures.

Another contribution of this model is that extensive studies are conducted to determine appropriate paths with the requisite bandwidth for rerouting packets that ranged from no failure to numerous failure scenarios.

One of the major novelties that make this study applicable around the world is an effort to answer wireless network failures, which are one of the global wireless survivability issues.

The study's methodological contributions include the following:

(i) The researcher's view on the wireless network survivability literature that reveals network survivability topics is an open research structure on wireless network survivability owing to failures. These have had little attention in research, resulting concerns to establish a blueprint for a wireless network failure survivability study.

The goal of this study was to look at different optimization routing algorithms in wireless networks in order to identify gaps that future wireless researchers might use as a starting point for their research

(ii) Data from simulation trials is used to undertake investigational assessments of the suggested model. These tests indicate that the ACS model is reliable for rerouting voice messages, whereas the EGA model is reliable for sending video and multimedia communications.

6.3.2 Broader impact/contributions

Telecom network subscribers and Telecom vendors can use the capacity-efficient EGA and ACS framework, as shown in **Figure 4.1 of subsection 4.1.2**, to resolve network failures. As illustrated in **Figure 4.1**, the model will assist wireless network users in making informed decisions about network restoration.

Specifically, video transmission on the iPad, iPod, and phones (Android and iPhone) is now possible without delay caused by link–link failures. Failures on handheld nodes are resolved by incorporating capacity efficient EGA, as shown in Figure 4.2. The majority of handheld nodes have inbuilt video message rerouting algorithms.

In addition, voice message transmission failures on hand held nodes are also easily resolved without delay since failures are resolved in real time owing to rerouting model built on them. (See Figure 4.1 of section 4.1.2). The majority of handheld nodes have inbuilt voice message rerouting models.

Some of the advantages of the suggested model are as follows:

(i) It resolves any type of wireless network failure in the literature.

(ii) It provides directions to telecom network providers to resolve any kind of wireless network failure.

The survivability solution path from varied wireless network location scenarios shows that the suggested capacity efficient EGA and ACS are feasible for current business applications such as high speed broadband networks.

6.4 LIMITATIONS

6.4.1 Theoretical limitations

The scientific literature is one of the major issues affecting research in wireless network survivability. Journals are not readily available when it comes to recent publications on wireless network survivability model development. Due to the language barrier, however, this research is only to streamline access to journals that are published in the English language.

6.4.2 Methodological limitations

The model is been developed with Java programing language, the application can only work on a wireless network environment when the application is compiled. In addition, the application performs better on network operating systems in the background; for example sun solaris, novel netware and UNIX operating system. At the user's end (fore ground) the operating system could be Windows operating system. Network configuration parameters must be well structured in such a way to give the expected result.

6.5 PRACTICAL IMPLICATIONS AND RECOMMENDATIONS ON THE PROPOSED EVOLUTIONARY AND SWAM MODELS

The contributions resulting from the research study are discussed in Section 1.6 of Chapter 1. The emphasis in this section is primarily on the practical implications and recommendations that arise from the implementation of the proposed capacity efficient EGA and ACS framework. The thesis has the following notable practical significance, contributions, and suggestions.

(i) A properly functioning capacity efficient EGA and ACS framework for addressing most of the wireless network failure issues faced in current wireless network survivability models.

(ii) Knowledge development for system engineers, professionals, and academic researchers as a standard guideline to understand alternative path generation in wireless networks and wireless network survivability.

(iii) The requirements and guidelines for designing and developing a unified wireless network survivability framework are crucial.

(iv) A systematic demonstration of a worked scenario on capacity efficient EGA and ACS as applied to various wireless network sizes and topologies serves as a drivetrain components analysis for network engineering practices.

The study's findings also provide a practical and useful framework for wireless network engineers to improve wireless networks' ability to route and reroute messages effectively.

6.6 FUTURE DIRECTIONS

Future scholars should concentrate their efforts on revealing and conducting research in terms of hidden wireless network challenges. Several significant research publications are scattered across various journals.

The findings of 11 years of research on survivability of wireless networks have a lot of ramifications for future researchers. There will be about 20 or more publications in wireless network research between 2012 and 2020 (see Figure 3.2); about 20 or more articles per year. This result offers important insights into the wireless network survivability, but it does not intend to be comprehensive. Figure 3.1 depicts the seven wireless network themes that authors of wireless network survivability must consider when evaluating new wireless network routing protocols, as well as the optimization routing strategies applicable to wireless networks. The findings in Figures 3.4 (Trend of optimization routing technique papers by topic) to 3.10 (Percentage of ADPV routing technique papers) indicate that wireless network survivability is required to address the following:

(i) Sub-topic of ACS routing strategies especially multiple node-links failure.

(ii) Sub-topic of Evolutionary Algorithm routing strategies especially multiple node-links failure.

(iii) Sub-topics of PSO routing strategies especially (a) multiple links failure and (b) multiple node-links failure.

(iv) Sub-topics of AODV routing strategies especially (a) multiple nodes and (b) multiple node-links failure.

(v) Sub-topics of TORA routing strategies especially (a) multiple nodes and (b) multiple node-links failure.

(vi) Sub-topics of ADPV routing strategies especially (a) single link (b) multiple links and (c) multiple node-links failure.

In testing the performance of optimization routing strategies, time complexity is rarely used, as can be seen in Figure 3.11 (Wireless network performance evaluation metrics). Throughput and bandwidth usage take larger percentages.

The following appear as interesting research questions for future academics to investigate in the less explored wireless network survivability techniques where fewer published papers exist:

(i) How can ACS strategies be developed to survive wireless networks subject to multiple node-links failure?

(ii) How can Evolutionary Algorithm strategies be developed to survive wireless networks subject to multiple node-links failure?

(iii) To what extent can PSO strategies be developed to survive IoT wireless networks subject to (a) multiple links failure and (b) multiple node-links failure transmitting messages?

(iv) To what extent can AODV strategies be developed to survive cell phones wireless networks subject to (a) multiple nodes and (b) multiple node-links failure transmitting video data?

(v) To what extent can TORA strategies be developed to survive sensor wireless networks subject to (a) multiple nodes and (b) multiple node-links failure transmitting voice data?

(vi) How can ADPV strategies be developed to survive MANET wireless networks subject to (a) single link (b) multiple links and (c) multiple node-links failure transmitting multimedia data?

Furthermore, future research can look into areas such as measuring packet loss during downtime of links and nodes, as well as how quickly recovery techniques re-transmit lost packets.

REFERENCE

[1] S. Routray, A. M. Sherry, and B. V. R. Reddy, "ATM Network Planning : a Genetic Algorithm," *J. Theor. Appl. Inf. Technol.*, vol. 3, no. 4, pp. 72–79, 2007.

[2] B. S. Awoyemi, A. S. Alfa, and B. T. Maharaj, "Network Restoration for Next-Generation Communication and Computing Networks," vol. 2018, no. 4, pp. 1-13, 2018

[3] W. P. Tay, J. N. Tsitsiklis, and M. Z. Win, "On the Impact of Node Failures and Unreliable Communications in Dense Sensor Networks," vol. 56, no. 6, pp. 2535–2546, 2008.

[4] M. Keshtgary, F. A. Al-zahrani, A. P. Jayasumana, F. Collins, and A. H. Jahangir, "Network Survivability Performance Evaluation with Applications in WDM Networks with Wavelength Conversion ∗." Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04), no. 29, pp. 1-9, 2004.

[5] Y. Zhang and J. Xin, "Survivable Deployments of Optical Sensor Networks against Multiple Failures and Disasters: A Survey," *Sensors (Switzerland)*, vol. 19, no. 21, pp. 1-29, 2019.

[6] R. S. Abujassar, "Restoration of IP Networks by Using a Hybrid Interacting Mechanism Between Layer 2 & 3 in the Networks Over OA&M: Fault Prediction and Mitigation on the IGP Network with Fast Detection by Using the OA&M Ethernet," *Wirel. Pers. Commun.*, vol. 100, no. 3, pp. 819–849, 2018.

[7] D. Wagner, *Lecture Notes in Computer Science: Preface*, vol. 5157 LNCS. 2008.

[8] K. J. S. White, D. P. Pezaros, and C. W. Johnson, "Increasing Resilience of ATM Networks using Traffic Monitoring and Automated Anomaly Analysis," *Int. Conf. Appl. Theory Autom. Command Control Syst.*, no. May, pp. 82–92, 2012.

[9] A. R. of the P. S. and H. S. Bureau and F. C. Commission, "2017 Atlantic Hurricane Season Impact on Communications Report and Recommendations Public Safety Docket No . 17-344 A Report of the Public Safety and Homeland Security Bureau Federal Communications Commission August 2018," no. 17, pp. 1-50, 2018.

[10] R. Katz, "Economic impact of COVID-19 Report of an Economic Experts Roundtable," *Int. Telecommun. Union Place Des Nations CH-1 211 Geneva Switz.*, vol. 3, no. 7, pp. 1–35, 2020.

[11] International Telecommunication Union (ITU), *Economic Impact of COVID-19 on Digital Infrastructure Report of economic experts roundtable organized by ITU*, no. 7. 2020.

[12] R. K and K. Gopal, "A Survey on Cost Effective Survivable Network Design in Wireless Access Network," *Int. J. Comput. Sci. Eng. Surv.*, vol. 5, no. 1, pp. 11–18, 2014.

[13] A. H. Azni, R. Ahmad, Z. A. M. Noh, F. Hazwani, and N. Hayaati, "Systematic Review for Network Survivability Analysis in MANETS," *Procedia - Soc. Behav. Sci.*, vol. 195, pp. 1872–1881, 2015.

[14] R. N. Jadoon, A. A. Awan, M. A. Khan, W. Y. Zhou, A. Shahzad, and S. Hou-Sheng, "An Efficient Nodes Failure Recovery Management Algorithm for Mobile Sensor Networks," *Math. Probl. Eng.*, vol. 2020, no. 9, pp. 1-14, 2020.

[15] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing," *IEEE/ACM Trans. Netw.*, vol. 13, no. 1, pp. 198–211, 2005.

[16] A. R. Hedar, S. N. Abdulaziz, E. Mabrouk, and G. A. El-Sayed, "Wireless Sensor Networks Fault-tolerance Based on Graph Domination with Parallel Scatter Search," *Sensors (Switzerland)*, vol. 20, no. 12, pp. 1–27, 2020.

[17] F. Callegati, D. Careglio, L. H. Bonani, M. Pickavet, and J. Solé-Pareta, "Why Optical Packet Switching failed and can Elastic Optical Networks take its place?," *Opt. Switch. Netw.*, vol. 44, no. 10, pp. 40-62, 2022.

[18] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks," *Int. J. Appl. Graph Theory Wirel. Ad Hoc Networks Sens. Networks*, vol. 3, no. 1, pp. 35–56, 2011.

[19] Y. Zhou and J. Wang, "Efficiency of Complex Networks under Failures and Attacks: A Percolation Approach," *Phys. A Stat. Mech. its Appl.*, vol. 512, no. 10, pp. 658–664, 2018.

[20] Claudio Greco, "Robust Broadcast of Real-time Video over Wireless Network," *Telecom ParisTech*, vol. 2012, no. 7, pp.1-150, 2012.

[21] A. Aliyu *et al.*, "Towards video streaming in IoT Environments: Vehicular communication perspective," *Comput. Commun.*, vol. 118, no. 10, pp. 93–119, 2018.

[22] W. U. Rahman, Y. S. Choi, and K. Chung, "Performance Evaluation of Video Streaming Application over CoAP in IoT," *IEEE Access*, vol. 7, no. 4, pp. 39852–39861, 2019.

[23] U. Jennehag, S. Forsstrom, and F. V. Fiordigigli, "Low Delay Video Streaming on the Internet of Things using Raspberry Pi," *Electron.*, vol. 5, no. 3, pp.1-11, 2016.

[24] A. H. Azni, R. Ahmad, Z. Azri, M. Noh, and F. Hazwani, "Systematic Review for Network Survivability Analysis in MANETS," in *Procedia - Social and Behavioral Sciences*, vol. 195, pp. 1872–1881, 2015.

[25] M. Zhu, F. Song, L. Xu, J. T. Seo, and I. You, "A Dependable Localization Algorithm for Survivable Belt-type Sensor Networks," *Sensors (Switzerland)*, vol. 17, no. 12, 2017.

[26] O. M. Al-Kofahi and A. E. Kamal, "Survivability Strategies in Multihop Wireless Networks," *IEEE Wirel. Commun.*, vol. 17, no. 5, pp. 71–80, 2010.

[27] P. Papanikolaou, K. Christodoulopoulos, and E. Varvarigos, "Joint Multi-layer Survivability Techniques for IP-over-Elastic-Optical- Networks," *J. Opt. Commun. Netw.*, vol. 9, no. 1, pp. A85–A98, 2017.

[28] A. A. Owoade and I. O. Osunmakinde, "Surviving Node-node Failures within Wireless Networks for a Near Optimal Ant Colony System Message Re-routing," *Int. J. Mob.*

Netw. Des. Innov., vol. 9, no. 3–4, pp. 153–182, 2019.

[29] J. P. G. Sterbenz *et al.*, "Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines," *Comput. Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[30] T. Horie, G. Hasegawa, S. Kamei, and M. Murata, "A New Method of Proactive Recovery Mechanism for Large-scale Network Failures," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, no. June, pp. 951–958, 2009.

[31] S. X. Wang, "The Improved Dijkstra's Shortest Path Algorithm and Its Application," *Procedia Eng.*, vol. 29, pp. 1186–1190, 2012.

[32] P. Sharma and A. Planiya, "Shortest Path Finding of Wireless Optical Network using Dijkstra Algorithm and Analysis of Delay and Blocking Probability," vol. 3, no. 4, pp. 77–84, 2016.

[33] A. A. Owoade and I. O. Osunmakinde, "Resilience and Survivability of ATM Node-node Network Failures Using Ant Colony Swarm Intelligent Modelling," in *Proceedings of 2016 SAI Computing Conference, no. 5, pp.1-10,* 2016.

[34] H. Wang, X. Ding, C. Huang, and X. Wu, "Adaptive Connectivity Restoration from Node Failure(s) in Wireless Sensor Networks," *Sensors (Switzerland)*, vol. 16, no. 10, 2016.

[35] S. E. E. Profile, "A Comparison of Existing Routing Algorithms and their Issues : Paving way for Emerging E- AODV," *Proc. 11th INDIACom; INDIACom-2017; IEEE Conf. ID 40353*, vol. 11, no. 6, pp. 2672–2676, 2019.

[36] T. P. Venkatesan, P. Rajakumar, and A. Pitchaikkannu, "Overview of Proactive Routing Protocols in MANET," *Proc. - 2014 4th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2014*, no. May, pp. 173–177, 2014.

[37] S. Saranya and R. M. Chezian, "Comparison of Proactive , Reactive and Hybrid Routing Protocol in MANET," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 7, pp. 775–779, 2016.

[38] R. Zheng, J. Zhang, and Q. Yang, "An ACO-based Cross-layer Routing Algorithm in Space-air-ground Integrated Networks," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 3372–3387, 2021.

[39] Z. Chi, S. Su, and M. A. Khine, "Solving Traveling Salesman Problem by Using Improved Ant Colony Optimization Algorithm," vol. 1, no. 5, pp. 404–409, 2011.

[40] S. K. Gupta, P. Kuila, and P. K. Jana, "Genetic Algorithm Approach for k-coverage and m-connected Node Placement in Target Based Wireless Sensor Networks," *Comput. Electr. Eng.*, vol. 56, pp. 544–556, 2016.

[41] A. A. Mohammed and G. Nagib, "Optimal Routing in Ad-hoc Network using Genetic Algorithm," *Adv. Netw. Appl.*, vol. 3, no. 5, pp. 1323–1328, 2012.

[42] N. M. Razali and J. Geraghty, "Genetic Algorithm Performance with Different Selection Strategiesin Solving TSP," *Proc. World Congr. Eng. 2011, WCE 2011*, vol. 2, no. 1, pp. 1134–1139, 2011.

[43] E. H. Grosse, “Capacity Allocation in a Wireless Communication System,” *Pat. Appl. Publ.*, vol. 1, no. 19, 2007.

[44] B. Chandra Mohan and R. Baskaran, “A survey: Ant Colony Optimization Based Recent Research and Implementation on Several Engineering Domain,” *Expert Syst. Appl.*, vol. 39, no. 4, pp. 4618–4627, 2012.

[45] D. G. Reina, P. Ruiz, R. Ciobanu, S. L. Toral, B. Dorronsoro, and C. Dobre, “A Survey on the Application of Evolutionary Algorithms for Mobile Multihop Ad Hoc Network Optimization Problems,” *Int. J. Distrib. Sens. Networks*, vol. 2016, 2016.

[46] A. Ambhaikar, H. R. Sharma, and V. K. Mohabey, “Improved AODV Protocol For Solving Link Failure In MANET,” *Int. J. Sci. Eng. Res.*, vol. 3, no. 10, pp. 1–6, 2012.

[47] D. IM and E. SM, “Enhanced Algorithms for Fault Nodes Recovery in Wireless Sensors Network,” *Int. J. Sens. Networks Data Commun.*, vol. 06, no. 01, pp. 1–9, 2017.

[48] M. N. Abdulleh, S. Yussof, and H. S. Jassim, “Comparative Study of Proactive, Reactive and Geographical MANET Routing Protocols,” *Commun. Netw.*, vol. 07, no. 02, pp. 125–137, 2015.

[49] M. A. Al-Absi, A. A. Al-Absi, M. Sain, and H. Lee, “Moving Ad hoc Networks-A Comparative Study,” *Sustain.*, vol. 13, no. 11, 2021.

[50] V. Nundloll *et al.*, “The Design and Deployment of an End-to-end IoT Infrastructure for the Natural Environment,” *Futur. Internet*, vol. 11, no. 6, 2019.

[51] S. H. Masood and S. Riza, “Enhancing Fault Tolerance of IoT Networks within Device Layer,” *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 1, pp. 8–11, 2020.

[52] A. P. Singh, A. K. Luhach, X. Z. Gao, S. Kumar, and D. S. Roy, “Evolution of Wireless Sensor Network Design from Technology Centric to User Centric: An Architectural Perspective,” *Int. J. Distrib. Sens. Networks*, vol. 16, no. 8, 2020.

[53] D. T. Do, A. T. Le, R. Kharel, A. Silva, and M. A. Shattal, “Hybrid Satellite-terrestrial Relay Network: Proposed Model and Application of Power Splitting Multiple Access,” *Sensors (Switzerland)*, vol. 20, no. 15, pp. 1–18, 2020.

[54] A. sulaiman A. Okoro Obinnaa, Sellappan Palaniappana, “Overview of Cellular Network : Impact of GSM to the economic Growth in Overview of Cellular Network : Impact of GSM to the economic Growth in Nigeria,” *J. Adv. Appl. Sci.*, vol. 2, no. 6, pp. 192–204, 2014.

[55] S. Moumouni, S. Sr, K. Bm, A. Doumounia, K. Illa, and F. Zougmoré, “Packet Microwave Layer 1 and Layer 2 Throughput in E-band for Mobile Broadband Communications,” *J. Telecommun. Syst. Manag.*, vol. 7, no. 3, pp. 1-8, 2018.

[56] B. Varghese, G. McKee, and V. Alexandrov, “Handling Single Node Failures Using Agents in Computer Clusters,” *Proc. 2010 Int. Symp. Perform. Eval. Comput. Telecommun. Syst. SPECTS’2010*, no. 8, pp. 96–101, 2010.

[57] Q. Xin, E. L. Miller, T. J. E. Schwarz, and D. D. E. Long, “Impact of Failure on Interconnection Networks for Large Storage Systems,” *Proc. - Twenty -second*

IEEE/Thirteenth NASA Goddard Conf. Mass Storage Syst. Technol., no. 4, pp. 189–196, 2005.

[58] L. Wosinska, "Connection Availability in WDM Mesh Networks with Multiple Failures," *2006 Int. Conf. Transparent Opt. Networks*, vol. 3, no. 6, pp. 126–129, 2006.

[59] X. Fu and Y. Yang, "Modeling and Analysis of Cascading Node-link Failures in Multi-sink Wireless Sensor Networks," *Reliab. Eng. Syst. Saf.*, vol. 197, pp. 106815, 2020.

[60] P. Shunmugapriya and S. Kanmani, "A Hybrid Algorithm using Ant and Bee Colony Optimization for Feature Selection and Classification (AC-ABC Hybrid)," *Swarm Evol. Comput.*, vol. 36, no. 10, pp. 27–36, 2017.

[61] G. S. Sharvani and T. M. Rangaswamy, "Efficient Pheromone Adjustment Techniques in ACO for Ad Hoc Wireless Network," *Int. J. Comput. Appl.*, vol. 44, no. 6, pp. 29–32, 2012.

[62] N. Mohan, A. Wason, and P. S. Sandhu, "ACO Based Single Link Failure Recovery in all Optical Networks," *Optik (Stuttg).*, vol. 127, no. 20, pp. 8469–8474, 2016.

[63] R. Yadav and A. Singh, "Performance Comparison of Prim ' s and Ant Colony Optimization Algorithm to Select Shortest Path in Case of Link Failure," vol. 9, no. 6, pp. 1516–1520, 2015.

[64] L. A. De Lima and G. S. Pavani, "Provisioning and Recovery in Flexible Optical Networks using Ant Colony Optimization," vol. IFIP, no. 4, pp.1-5, 2021.

[65] H. Zhang, X. Wang, P. Memarmoshrefi, and D. Hogrefe, "A Survey of Ant Colony Optimization Based Routing Protocols for Mobile Ad Hoc Networks," *IEEE Access*, vol. 5, no. 1, pp. 24139–24161, 2017.

[66] F. Barbosa, A. Agra, and A. de Sousa, "The Minimum cost Network Upgrade Problem with Maximum Robustness to Multiple Node Failures," *Comput. Oper. Res.*, vol. 136, no.12, pp. 1-16, 2021.

[67] U. R. Bhatt, T. Sarsodia, R. Upadhyay, and R. Sharan, "Implementation of Ant Colony Optimization Algorithm for Survivable optical network," *Raghav Sharan Int. J. Eng. Technol. Sci. Res. IJETSR www.ijetsr.com ISSN*, vol. 3, no. 4, pp. 2394–3386, 2016.

[68] Q. Q. Li and Y. Peng, "A Wireless Mesh Multipath Routing Protocol Based on Sorting Ant Colony Algorithm," *Procedia Comput. Sci.*, vol. 166, no. 1, pp. 570–575, 2020.

[69] S. K. Biswas and A. Podder, "Path Restoration Technique of Optical Network with Application of Bit Error Rate (BER) Performance," vol. 9, no. 2, pp. 1736–1743, 2021.

[70] L. B. Bhajantri and N. N, "Genetic Algorithm Based Node Fault Detection and Recovery in Distributed Sensor Networks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 12, pp. 37–46, 2014.

[71] A. A. Owoade and I. O. Osunmakinde, "Fault-tolerance to Cascaded Link Failures of Video Traffic on Attacked Wireless Networks," IEEEXplore, no10, pp. 1–11, 2021.

[72] H. T. Khosrowshahi and M. Shakeri, “Relay Node Placement for Connectivity Restoration in Wireless Sensor Networks Using Genetic Algorithms,” vol. 12, no. 3, pp. 161–170, 2018.

[73] Ayoade Akeem Owoade & Isaac Olusegun Osunmakinde, “Resilient Rerouting in IoT Systems with Evolutionary Computing,” in *Proceedings of 10th Computer Science On-line Conference 2021* Proceeding, vol. 2, no. 229, pp. 194–211, 2021.

[74] K. Vijayalakshmi and S. Radhakrishnan, “Dynamic Routing to Multiple Destinations in IP Networks using Hybrid Genetic Algorithm (DRHGA),” *Engineering*, vol. 2, no. 1, pp. 346–353, 2008.

[75] V. Sarasvathi, N. C. S. N. Iyengar, and S. Saha, “QoS Guaranteed Intelligent Routing using Hybrid PSO-GA in Wireless Mesh Networks,” *Cybern. Inf. Technol.*, vol. 15, no. 1, pp. 69–83, 2015.

[76] V. Anand and S. Pandey, “Particle Swarm Optimization and Harmony Search Based Clustering and Routing in Wireless Sensor Networks,” *Int. J. Comput. Intell. Syst.*, vol. 10, no. 1, p. 1252, 2017.

[77] Y. H. Robinson and M. Rajaram, “Energy-aware Multipath Routing Scheme Based on Particle Swarm Optimization in Mobile Ad hoc Networks,” *Sci. World J.*, vol. 2015, no. 11, pp. 1-9, 2015.

[78] D. Manickavelu and R. U. Vaidyanathan, “Particle Swarm Optimization (PSO)-based Node and Link Lifetime Prediction Algorithm for Route Recovery in MANET,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2014, no. 1, pp. 1–10, 2014.

[79] B. Singh and D. K. Lobiyal, “Energy-aware Cluster Head Selection Using Particle Swarm Optimization and Analysis of Packet Retransmissions in WSN,” *Procedia Technol.*, vol. 4, pp. 171–176, 2012.

[80] Y. Meng, Q. Zhi, Q. Zhang, and N. Yao, “A Two-stage Particle Swarm Optimization Algorithm for Wireless Sensor Nodes Localization in Concave Regions,” *Inf.*, vol. 11, no. 10, pp. 1–16, 2020.

[81] R. F. Abdel-Kader, “Hybrid Discrete PSO with GA Operators for Efficient QoS-Multicast Routing,” *Ain Shams Eng. J.*, vol. 2, no. 1, pp. 21–31, 2011.

[82] M. Sheikhan and E. Hemmati, “PSO-Optimized Hopfield Neural Network-Based Multipath Routing for Mobile Ad-hoc Networks,” *Int. J. Comput. Intell. Syst.*, vol. 5, no. 3, pp. 568–581, 2012.

[83] S. Kumar and P. Negi, “A Link Failure Solution in Mobile Adhoc Network through Backward AODV (B-AODV),” *IJCEM Int. J. Comput. Eng. Manag.*, vol. 11, no. 1, pp. 1–5, 2011.

[84] F. Tong, W. Tang, L. M. Peng, R. Xie, W. H. Yang, and Y. C. Kim, “A Node-grade Based AODV Routing Protocol for Wireless Sensor Network,” *NSWCTC 2010 - 2nd Int. Conf. Networks Secur. Wirel. Commun. Trust. Comput.*, vol. 2, no. 6, pp. 180–183, 2010.

[85] S. R. Azzuhri, M. B. Mhd Noor, J. Jamaludin, I. Ahmedy, and R. Md Noor, “Towards a Better Approach for Link Breaks Detection and Route Repairs Strategy in AODV

Protocol," *Wirel. Commun. Mob. Comput.*, vol. 2018, no. 4, pp. 1-9, 2018.

[86] H. S. H. Jassim, S. K. Tiong, S. Yussof, S. P. Koh, and R. Ismail, "Scenario Based Performance Analysis of Reliant Ad hoc On-demand Distance Vector Routing (R-AODV) for Mobile Ad hoc Network," vol. 2, no. 5, pp. 78–89, 2011.

[87] K. H. Lim and A. Datta, "Enhancing the TORA Protocol Using Network Localization and Selective Node Participation," *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC*, no. 5, pp. 1503–1508, 2012.

[88] A. R. Hilal, A. El Nahas, and A. Bashandy, "RT-TORA: A TORA Modification for Real-time Interactive Applications," *Can. Conf. Electr. Comput. Eng.*, no. 6, pp. 1403–1406, 2008.

[89] S. Liu, D. Zhang, X. Liu, T. Zhang, and H. Wu, "Adaptive Repair Algorithm for TORA Routing Protocol Based on Flood Control Strategy," *Comput. Commun.*, vol. 151, no. 12, pp. 437–448, 2020.

[90] R. Vadivel and V. M. Bhaskaran, "Adaptive Reliable and Congestion Control Routing Protocol for MANET," *Wirel. Networks*, vol. 23, no. 3, pp. 819–829, 2017.

[91] F. Deniz, H. Bagci, I. Korpeoglu, and A. Yazici, "An Adaptive, Energy-aware and Distributed Fault-tolerant Topology-control Algorithm for Heterogeneous Wireless Sensor Networks," *Ad Hoc Networks*, vol. 44, no. 7, pp. 104–117, 2016.

[92] H. Shah and R. Bansode, "Performance Evaluation and Measurement for Energy Efficient Wireless Networks," *Procedia Comput. Sci.*, vol. 79, no. 5, pp. 971–977, 2016.

[93] K. A. Chege and O. C. Otieno, "GSJ : Volume 8 , Issue 5 , May 2020 , Online : ISSN 2320-9186 Research Philosophy Design and Methodologies : A Systematic Review of Research Paradigms in Information Technology," vol. 8, no. 5, pp. 33–38, 2020.

[94] P. E. Heegaard and K. S. Trivedi, "Network Survivability Modeling," *Comput. Networks*, vol. 53, no. 8, pp. 1215–1234, 2009.

[95] O. Kabadurmus and A. E. Smith, "Evaluating Reliability/Survivability of Capacitated Wireless Networks," *IEEE Trans. Reliab.*, vol. 67, no. 1, pp. 26–40, 2018.

[96] P. H. Pathak and R. Dutta, "Designing for Network and Service Continuity in Wireless Mesh Networks," *Springer Sci. Media*, vol. 2, pp. 222, 2013.

[97] K. Gusarovs, "An Analysis on Java Programming Language Decompiler Capabilities," *Appl. Comput. Syst.*, vol. 23, no. 2, pp. 109–117, 2018.

[98] M. Kabir, S. Islam, M. Hossain, and S. Hossain, "Detail Comparison of Network Simulators," *Int. J. Sci. Eng. Res.*, vol. 5, no. 10, pp. 203–218, 2014.

[99] G. F. Tong, J. Li, and H. S. Gao, "Simulation of Time Delay Characteristics of Time Sensitive Networking Based on MATLAB/Simulink," *J. Phys. Conf. Ser.*, vol. 2005, no. 1, pp. 1–9, 2021.

[100] S. Zhao, Z. Lu, and C. Wang, "How Can Randomized Routing Protocols Hide Flow Information in Wireless Networks?," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 11, pp.

7224–7236, 2020.

[101] S. and B. P. S. Ch, “Randomized Routing for Wireless Sensor Networks : Optimized Security and Randomized Routing for Wireless Sensor Networks : Optimized Security and Energy Efficiency,” *Int. J. Electron. Commun. Comput. Eng.*, vol. 3, no. 5, pp. 1–5, 2019.

[102] N. Gupta, K. Mangla, A. Jha, and M. Umar, “Applying Dijkstras Algorithm in Routing Process,” *Int. J. New Technol. Res.*, vol. 2, no. 5, p. 263504, 2016.

[103] D. Sudholt and C. Thyssen, “Running time analysis of Ant Colony Optimization for shortest path,” *J. Discret. Algorithms*, vol. 10, no. 1, pp. 165–180, 2012.

[104] J. Jabez and B. Muthukumar, “Intrusion detection system (ids): Anomaly Detection Using Outlier Detection Approach,” *Procedia Comput. Sci.*, vol. 48, no. 4, pp. 338–346, 2015.

[105] N. N. Srinidhi, S. M. Dilip Kumar, and K. R. Venugopal, “Network Optimizations in the Internet of Things: A review,” *Eng. Sci. Technol. an Int. J.*, vol. 22, no. 1, pp. 1–21, 2019.

[106] L. Xie, P. E. Heegaard, and Y. Jiang, “Modeling and Quantifying the Survivability of Telecommunication Network Systems under Fault Propagation,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8115 LNCS, no. 8, pp. 25–36, 2013.

[107] D. Turner, K. Levchenko, A. C. Snoeren, and S. Savage, “California Fault Lines: Understanding the Causes and Impact of Network Failures,” *Comput. Commun. Rev.*, vol. 40, no. 4, pp. 315–326, 2010.

[108] N. Mohan, “Link Failure Recovery in WDM Networks,” *Int. J. Comput. Sci. Electron. Eng.*, vol. 1, no. 5, pp. 599-602, 2013.

[109] M. K. Saeed, M. Hassan, A. M. Shah, and K. Mahmood, “Connectivity Restoration Techniques for Wireless Sensor and Actor Network (WSAN), A Review,” vol. 9, no. 9, pp. 139–145, 2018.

[110] T. Yashima and K. Takami, “Route Availability as a Communication Quality Metric of a Mobile Ad Hoc Network,” *Futur. Internet*, vol. 10, no. 5, pp. 1-19, 2018.

[111] V. Rajeshkumar and P. Sivakumar, “Comparative Study of AODV , DSDV and DSR Routing Protocols in MANET Using Network Simulator-2,” vol. 1, no. 1, pp. 35–42, 2015.

[112] A. Gupta, R. Christie, and P. R. Manjula, “Scalability in Internet of Things : Features , Techniques and Research Challenges,” *Int. J. Comput. Intell. Res.*, vol. 13, no. 7, pp. 1617–1627, 2017.

[113] M. T. Moghaddam and H. Muccini, *Fault-Tolerant IoT : A Systematic Mapping Study*, no. 9. Springer International Publishing, vol. serene 2019. no.9, pp. 67-84, 2019.

[114] M. Biabani, N. Yazdani, and H. Fotouhi, “REFIT: Robustness Enhancement against Cascading Failure in IoT Networks,” *IEEE Access*, vol. 9, no. 3, pp. 40768–40782, 2021.

[115] R. Y. Yada and A. Foods, “An Overview of Opportunities and Challenges of Food Nanoscience / Technology,” *Int. J. Comput. Sci.*, vol. 9, no. 1, pp. 2612–2618, 2014.

[116] O. Shurdi, L. Ruci, A. Biberaj, and G. Mesi, “5G Energy Efficiency Overview,” *Eur. Sci. J. ESJ*, vol. 17, no. 03, pp. 315–327, 2021.