RESILIENCY MECHANISM

IN WIRELESS MESH NETWORKS

Enrolment no - 122206

Name of Student - GEETANJALI

Name of Supervisor - Prof. Dr. S.P. GHRERA

May- 2014

Submitted in partial fulfilment of the Degree of

Masters of Technology

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT, DIST. SOLAN, (H.P.), INDIA

TABLE OF CONTENTS

CERTIFICATE

This is to certify that the work titled "**RESILIENCY MECHANISM FOR WIRELESS MESH NETWORK**" submitted by "**GEETANJALI**" in partial fulfilment for the award of degree of M.Tech of Jaypee University of Information Technology, Waknaghat has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor ……..

Name of Supervisor Prof. Dr. S.P. Ghrera

Designation HOD (CSE)

Date

ACKNOWLEDGEMENT

This may seen long but the task of my thesis work both theoretically and practically may not have been completed without the help, guidance and mental support of the following persons. Firstly I would like to thank my guide Head of Department (HOD) of CSE and ICT, Jaypee University of Information Technology, Waknaghat, **Prof. Dr. S.P. Ghrera** sir who provided me the related material and idea for the project proposal. He indeed guided me to do the task for my thesis in such a way that it seems to be research work. His continuous monitoring to support me and my research work encouraged me a lot for doing my thesis in very smooth manner. Even if I made the mistake sometime he always tried to correct those mistakes and endeavour always to take me in the right direction. Further, I would like to extend my thanks to **Dr. Nitin Rakesh**- my previous guide who is currently the HOD in Chandigarh University. He always supports me and keeps my moral high. I will always be grateful to him for giving me the clear vision regarding my career.

Secondly, I would like to thank **My Parents** and **Family** who has always been with me for inspiring me that I can do the good research task with the hard work. He always helped me to grow my mind focused towards the hard work for implementation of thesis with having the research work in the mind.

Thirdly, I would like to thank **God** for keeping me enthusiastic, energetic and healthy every time due to which I could complete my thesis work successfully.

Once again thanks a lot to all mentioned people in my life.

Signature of the Student .....

Name of the Student GEETANJALI

Date .....

SUMMARY

Today, network services (like email, World Wide Web etc) [1-2] have become a basic need in day-to-day communication. For providing these network services more effectively, WMN (Wireless Mesh Network) [3-6] has turned into a popular topology which builds high performance infrastructure. Since, the possibilities of numerous failures always exist during communication; resiliency has been proved to be an important aspect for WMN to recover from these failures. Resiliency in general is the diligence of reliability and availability in network. Several types of resiliency based routing algorithms have been proposed i.e. Resilient Multicast, ROMER *etc*. Resilient Multicast establishes two-node disjoint path and ROMER uses credit based approach to provide resiliency in the network. However these proposed approaches have some disadvantages in terms of network throughput and network congestion.

We have proposed Buffer Based Routing method in which instead of maintaining routing table at each node we provide buffering at each node which reduces routing cost. At specific interval of time (after specified communication steps) it clears the buffer to increase performance and prevent overhead in network. Using this approach we effectively perform resiliency and exploits advantages of WMN. Further we have shown the comparative performance analysis of previous approaches with our proposed approach. Network throughput, network congestion and resilience against node/link failure, Packet Loss Ratio(PLR) and End-to-End Delay are particular performance metrics which are examined over different sized WMN.

LIST OF FIGURES

LIST OF TABLES

CHAPTER #1

INTRODUCTION

- *Problem Statement*
- *Motivation*
- *Objective*
- *Organization of thesis*

CHAPTER 1

INTRODUCTION

Problem Statement

Today, network services (like email, World Wide Web etc) [1-2] have become a basic need in day-to-day communication. For providing these network services more effectively, WMN (Wireless Mesh Network) [3-6] has turned into a popular topology which builds high performance infrastructure. With the growth of network services, several types of network communication threats (node/link failure) are moreover coming into existence.

Let us take an example: In a network of 10 nodes, suppose S is the source node and J is the destination node and remaining eight nodes are the intermediate nodes through which data will be send from source node to destination node. If some intermediate nodes/links are failed (as shown in figure 1) then in that case how to send the data from source to destination.

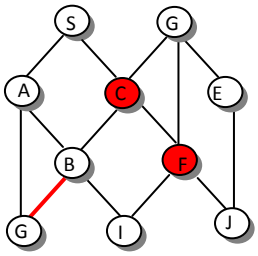


Figure 1: Node/Link Failure

To resist these communication threats, resiliency [7-13] is a significant approach for WMN.

Basically resiliency is the capability to provide services in the face of failure. As number of nodes are destroyed then what will be the effect of metric (i.e. throughput, network congestion, and resiliency) in the network i.e.

How to Increase network Throughput: Throughput is defined in terms of cost i.e. total amount of delay occurs during transmission of packets from source to destination even though number of nodes is destroyed.

How to reduce traffic congestion from network: It is defined in terms of rate of packet transmission i.e. total numbers of packets transmitted at a unit of time in a network .If number of nodes in the network are more than the possibility of network congestion increases in the network.

Several resilient based algorithms have been proposed to provide effective communication in network during the existing failures but building up an efficient resilient algorithm which can keep track of network parameter is still a challenge. Our main goal is to focus on these problems:

- How to provide effective communication in case of failures exist in network
- How to Measure different metric as number of links removed
- How to Increase throughput of network
- How to Reduce network congestion from network
- How to Implement resiliency in network

Motivation

Wireless Mesh Networks have seen an increased interest lately because of increasing applications they find in today's world. A question that comes intertwined with wireless mesh network is how to provide communication in the network during failures (node/link). There are many existing algorithms that have been developed after many years of research and each one has its own pros and cons. Using simulation, we have studied Resilient Multicast and ROMER approaches deeply to understand its finger points and then suggest improvements.

Objective

The project has following objectives:

- To study about resilient WMN and algorithms for resilient implementation in WMN.
- To simulate Resilient Multicast and ROMER and study the impact of results over different network parameters.
- To suggest an improvement in Resilient Multicast and ROMER to further increase the resiliency in WMN.

Organization of thesis

This section discusses the framework of this thesis which is organized as follows:

Chapter 1 Introduction: This chapter introduces the problem statement, motivation, objective of thesis.

Chapter 2 About the Network: It introduces the basics of computer network, its need, types, wireless mesh network, causes and types of failures inside the network and resiliency.

Chapter3 Preliminaries and Background: Reviews the preliminaries and background of this thesis.

Chapter 4 Proposed Approach: Describes the proposed resilient algorithm i.e. BBR (Buffer Based Routing Algorithm) which provides efficient communication in case of multiple failures.

Chapter 5 Performance Analysis: Shows the performance analysis of BBR algorithm in comparison of previous approaches i.e. RM and ROMER with results.

Chapter 6 Implementation Results: Shows the implementation of all three approaches i.e. Resilient Multicast, ROMER and BBR Approach.

Chapter 7 Conclusion: Presents the conclusion of the thesis and highlights the future research direction based on results obtained.

CHAPTER #2

ABOUT NETWORK

- *What is network?*
- *Need of network*
- *Types of network*
- *Failures in network*
- *Resiliency*

CHAPTER 2

ABOUT NETWORKS

2.1 What is a Network?

A network consists of two or more computers that are linked in order to share resources, exchange files, or allow electronic communications [14]. The computers on a network might be linked through cables, telephone lines, radio waves, satellites, or infrared light beams [14-15].

In computers, networking is the linking of two or more computing devices for the purpose of sharing the data/information. Basically network consists of the computers, wiring and other devices, such as hubs, switches and routers that make up the network infrastructure (see figure 2). Devices such as switches and routers provide traffic control strategies for the network. All sorts of different technologies can actually be employed to move data from one place to another, including wires, radio waves, and even microwave technology [15-17].

2.2 Need of Network in Computer?

Figure 2: Network [18]

There are some persuasive reasons about the need of network for e.g. If your business has more than one computer, then you can get several benefits from networking. A local area network (LAN) connects your company's computers, allowing them to share

and exchange a variety of information [19]. While one computer can be useful on its own, several networked computers can be much more useful [19].
Here are several reasons where a computer network can help your business:

- **File sharing:** Through networking several user access the same file and preventing the people from creating different versions accidently.
- **Printer sharing:** Several computers can be shared the same printer by using the networking. For example in colleges it's still cheaper to use a network printer than to connect a separate printer to every computer.
- **Communication and collaboration:** People working on a same company or in offices, networking allows employees to share files, view other people's work, and exchange ideas more efficiently. In a larger office, to communicate quickly and to store messages you can use e-mail and instant messaging.
- **Data protection:** A network makes it easier to back up all of your company's data on an offsite server, a set of tapes, CDs, or other backup systems [19].

2.3 Types of Network

When an organization comes to setting up an organization, it has two options: i) wired ii) Wireless network. Wired uses networking cable to connect computers and wireless uses radio frequencies to connect computer. Each type of networking has its own advantages and disadvantages like wired networking have different hardware requirements, range and benefits while wireless networking takes into consideration the range and mobility.

2.3.1 Wired Networking

Wired networks are the most common type of local area network (LAN) technology. It is simply a collection of two or more computers, and other devices linked by Ethernet cables. The computer must have an Ethernet adapter to connect a computer to a network with an Ethernet cable [20].

There are three basic network topologies that are most commonly used today:

a) **Star Network**

The star network is a general naive type of network which has one central hub that connects to three or more computers and has the ability to network printers [20] (see figure 3). This type of networks can be used for small businesses and home networks [20].

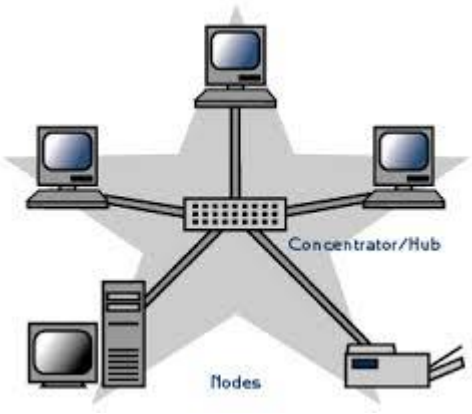


Figure 3: Star Network [20]

Advantages of Star Network

- Star network is easy to wire and install.
- During network connections or removing devices no disruptions.
- It is easy to remove parts and detect faults.

The main advantage of Star Network is that any non-centralised failure will have very slight effect on the network.

Disadvantages of Star Network

- Star network require more cable length.
- Nodes attached are disabled, if hub, switch fails.
- Star network is more expensive than bus topology because of the cost of the hubs is high.

The main disadvantage of Star Network is that it requires extra hardware.

Application of Star Network

The star network is very useful where some processing have to be centralized and some should be performed locally.

b) **Bus Network**

To identify the signals bus networking uses special type of software and broadcasts this signal to all directions (see figure 4).

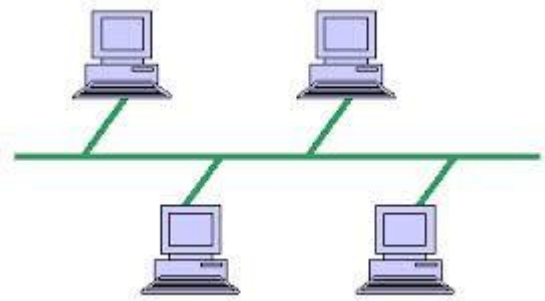


Figure 4: Bus Network [20]

Advantages of Bus Network

- Implementation and extension is easy in bus network
- Bus network is mostly used for temporary networks

The main advantage of bus network is that failure of one computer does not affect another computer.

Disadvantages of Bus Network

- Bus network has limited cable length
- Any fault in cable can cause the destruction of whole network

Sending of only one signal at a time has been proved to be major disadvantage of bus networking.

Application of Bus Network

It is mainly used for industrial applications.

c) **Ring Network**

Ring network is somewhat similar to bus network because it has no central host computer. Each computer in the network has two neighbouring nodes, and each node has its own applications independently (see figure 5). The data transmission is limited to one direction only. Ring network is in closed loop where each node can transmit the data by consuming the token.

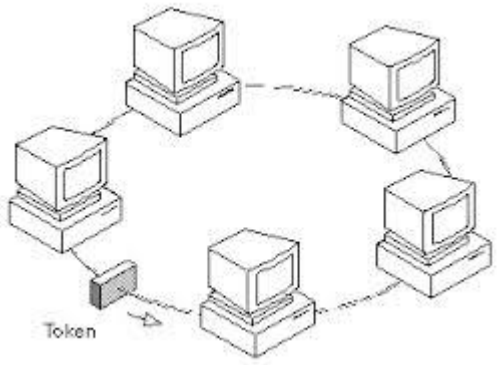


Figure 5: Ring Network [20]

Advantages of Ring Network

- Transferring of data is quickly.
- As packets travel in one direction only, so data transmission is very simple

The main advantage of Ring Network is that it prevents network collisions.

Disadvantages of Ring Network

- Transmission is very slow because data packets must pass through every computer between source and destination.
- Data cannot be transmitted successfully if any node fails in the network.
- It is difficult to troubleshoot the ring

The main disadvantage of Ring Network is that all computers must be turned on even if only two nodes want to transmit the data packets.

So far we have discussed about wired network and its various types, but wired networks have its own disadvantages.

Disadvantages of Wired Networking

- Non Portable
- Cost of fibre optics+ copper+ coaxial cable
- Static in nature
- Bandwidth fixed in advance
- Difficult to find path break if any

2.3.2 Wireless Network

A wireless network is another option for business networking which provides communication between nodes by using high frequency radio waves [20].

Wireless allows sharing between devices which increases mobility and decreases range.

. There are two main types of wireless networking [20]:

a) Peer to Peer or Ad-Hoc
b) Infrastructure

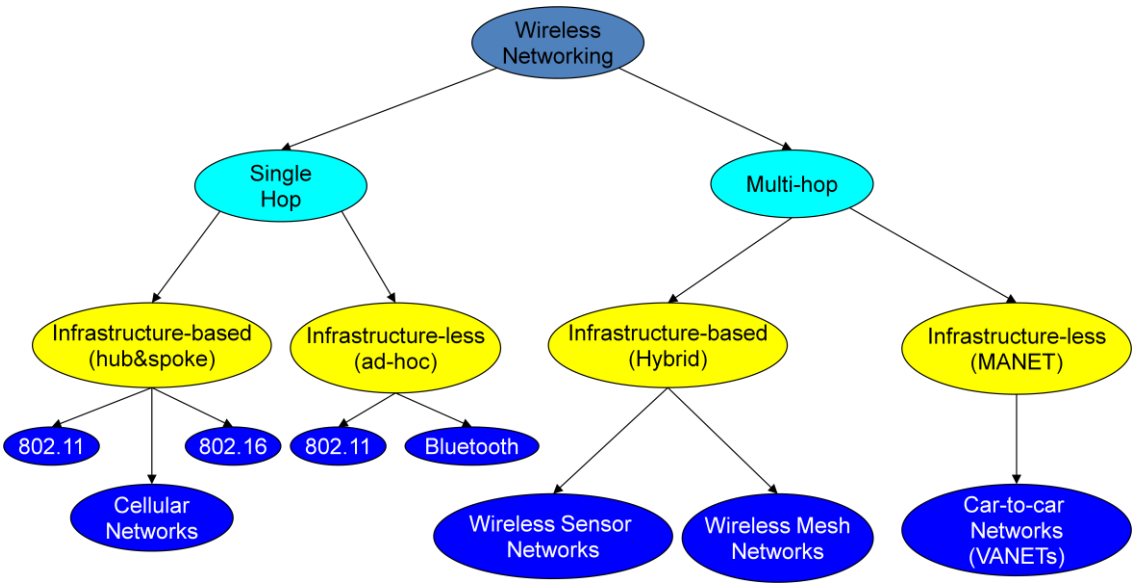


Figure 6: Wireless Network [21]

a) An **Ad-hoc or peer-to-peer** wireless network consists of various computers equipped with NIC. Each computer can directly communicate with any other computer. (See figure 7). Computers are able to share files but cannot able to access wire LAN [22].

Figure 7: Ad-Hoc Network [20]

b) An **Infrastructure Based** Network

An infrastructure wireless network has an access point. To provide the connectivity between wireless computers access points (like hub) is used. Infrastructure network provide a bridge between wires and wireless LAN and allow computer access to LAN resources [22].

Advantages of Wireless Network

- Portable
- Cost is less
- Dynamic in nature
- No path breaks

2.3.2.1 Wireless Mesh Network

Wireless mesh network is a combination of:

- Ad-hoc and Mesh Network
- Self configured

Ad-hoc network happens at OSI Layer 1 (Physical Layer) where all the devices can communicate directly to any other device i.e. with in radio ranges.

Mesh Network happens at OSI Layer 3(Network Layer) where each device on network acts as router and re-transmit packet on behalf of any other devices.

Self configured means a network should not need a system administrator to tell it how to get a message to its destination.

2.4 Wireless Mesh Network

Wireless mesh networks (WMNs) are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity [23].

2.4.1 Architecture of Wireless Mesh Network

WMNs consists of two types of nodes i) Mesh Routers, ii) Mesh Clients.

Mesh Router is the backbone of WMNs. It has minimal mobility. Mesh router provide the access for mesh and conventional clients (see figure 8). Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16 and sensor networks are the integration of WMN which can be accomplished through the gateway and bridging functions in the mesh routers [23].

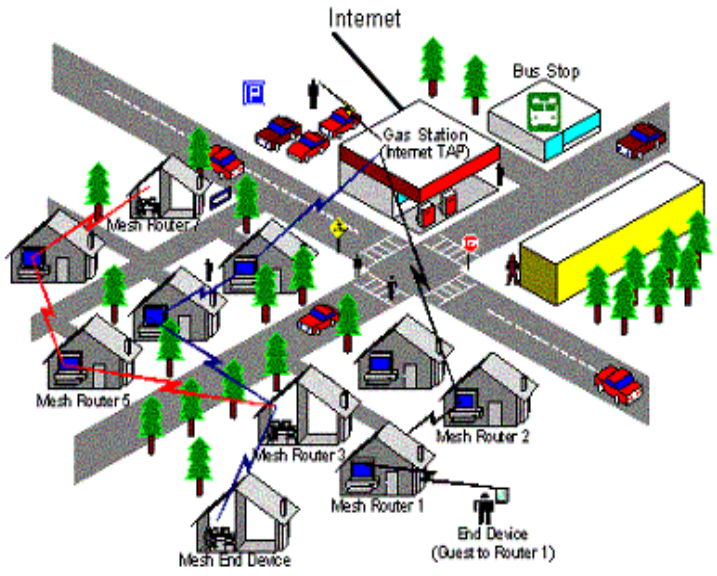


Figure 8: Wireless Mesh Network [21]

Mesh clients can be stationary or mobile. Mesh clients can form a mesh network among them and form a mesh router among mesh router.

Mesh router provides same coverage area through multi-hop communications with much lower transmission power. Mesh router is equipped with multiple interfaces for improving the flexibility of mesh networking [23]. A similar hardware platform is used for both mesh and conventional routers. The backbone of mesh clients is the mesh routers and they have the minimal mobility. Mesh clients and Mesh Routers have simpler hardware and software and mesh clients can be work as mesh routers. For example, for mesh clients has a light-weight communication protocols, mesh clients has no gateways and bridges functions and mesh client has a single wireless interface [23]. The integration of WMNs is provided by mesh routers using gateways/bridge in addition with mesh networking between mesh clients and routers. Using mesh routers conventional nodes can directly connect with WMNs. Through mesh routers customers can access WMNs like Ethernet. So, WMNs help users to be always-on-line anywhere, anytime.

2.4.2 Benefits of Wireless Mesh Network (WMN)[24]

1) Less Expensive than Traditional Networks

Wireless mesh network requires less cost to set up. For large areas of coverage, WMNs are used. Using wireless mesh networks, as there is no physical linking between the nodes, for this WMNs are less expensive than wired networking.

2) Wireless Mesh is extremely adaptable and expandable

Wireless mesh nodes can be extended or removed depending on large or small coverage area. Wireless mesh networks are used for blocked network configurations and for lack of sight. An example of blocked configuration is Ferris wheel where a wheel may block the signal.

3) Wireless Mesh Networks Support High Demand

Wireless Mesh Network supports large coverage area with high speed, quality video surveillance. Wireless Mesh Network provides high throughput and highly reliable connectivity.

Wireless Mesh Network is a complete solution for larger areas and delivers the connectivity for both indoors and outdoors. Wireless Mesh Networks are a reliable for a variety of public safety applications, parking garages, campus grounds, schools, business parks, and other large outdoor facilities wireless connectivity.

2.4.3 Applications of Wireless Mesh Network[21]

- Broadband Internet Access

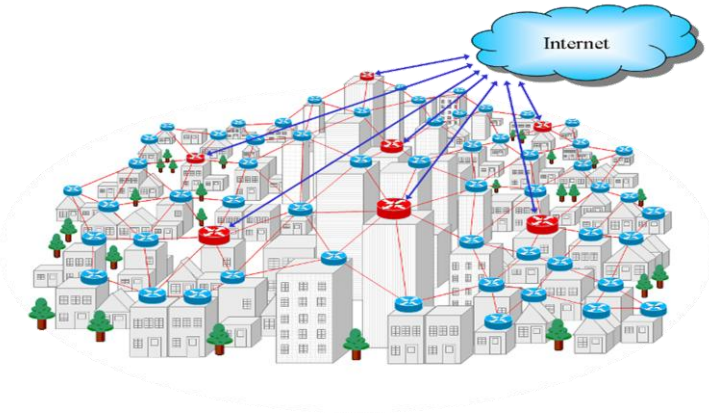


Figure 9: Broadband Access [21]

- Mobile Internet Access

In Mobile internet access it has a direct competition with G2.5 and G3 cellular systems. Mobile internet access is used in different areas:

a) Law enforcement

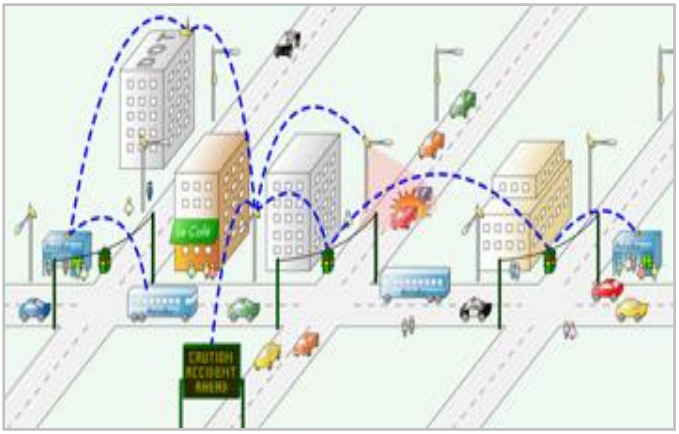


Figure 10: Law Enforcement [21]

b) Intelligent Transportation

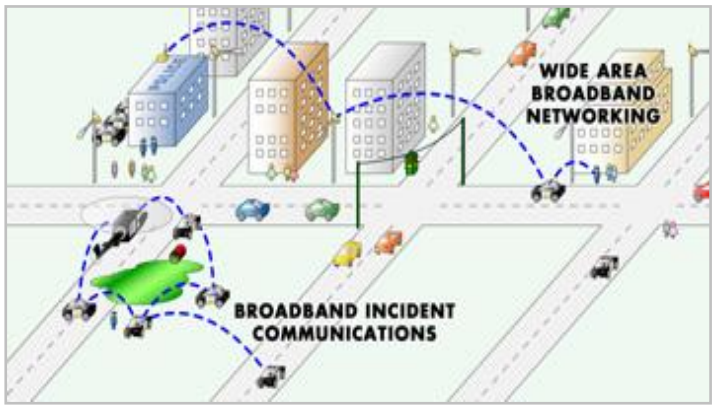


Figure 11: Intelligent Transportation [21]

2.5 Causes of communication failures in Network

Failures can be caused in networks by many reasons. Let us take an example: a hardware component of the network, failure from denial of service Attacks, and failures due to catastrophic events Kyas has identified five categories of errors that can lead to general system failure [23]. These errors are:

- Software Problem
- Hardware Problem
- Network Problem
- Denial of Service Attack
- Operator Error

2.5.1 Software Problem

Network software failures can be caused by faulty device drivers, operating system faults and anomalies.

Failures can arise from insufficient capacity, excessive delays during peak demands well as a catastrophic failure arising from the loss of a vital component or resource [25-28]. Software problem also arises due to IP miss-configuration, heavy loads etc.

2.5.2 Hardware Problem

In the actual deployment of the networks there are variations in more than just the hardware components that are selected. These variations include the quality of equipment, the quality of network planning and design, the complexity of implementation, the interaction and interoperability of components [29].

A network designer can select and deploy equipment with a wide range of redundancy options ranging from having no redundancy to the complete duplication of equipment and links.

2.5.3 Network Problem

Causes of failures within the lower layers of the model are often defective NIC cards, defective cables and connections, failures in interface cards in bridges routers and switches, beacon failure, checksum errors, and packet size errors [25-26].

Many of the errors and failures as described here are often localized and not catastrophic in nature. In understanding the contribution of localized failure to network reliability, it is important to consider the scale and size of the failures that are caused by individual network components.

For example, the failures of a NIC card will not likely results in a single point of failure of the enterprise network. However, a core Router failure without appropriate redundancy and switchovers can incapacitate an entire network.

2.5.4 Denial of Service Attack

An example of the impact of denial of service attacks is the code Red virus and a more recent variation, slammer worm, disrupted millions of computers by unleashing a well coordinated distributed Denial of Service Attack. These attacks resulted in a sufficient loss of corporate revenues worldwide [29].

The increased frequency of occurrence or threat, and the impact of this type of network failure on network disruption are considerable and therefore the Denial of Service Attack category must be included in any valid failure analysis model of an internet connected enterprise network.

Worms such as Code Red and Slammer are probably authored and unleashed by an individual or a small number of individuals. Predicting the percentage of network failures caused by this type of error is difficult because it is such a recent phenomenon with random occurrence. However, the potential impact of this failure is enormous and widespread and cannot be discounted.

2.5.5 Operator Error

Operator Error as defined by kyas et al. as those failures caused directly by human actions. Operator error is further subdivided into intentional or unintentional mistakes and as errors that do or do not cause consequential damage. Kyas suggests that Operator Error is responsible for over 5% of all system failures [25-29].

2.6 Types of Failure in Network

Many types of Physical failures are occurred due to above reasons for e.g. networking device failure and communication link failure.

2.6.1 Networking Device or Router Failure

In any model if any routing device becomes faulty then it stops forwarding of messages to next level device. In below diagram (see figure 12) networking device at level 2 is failed then all the communication towards this node will get interrupted.

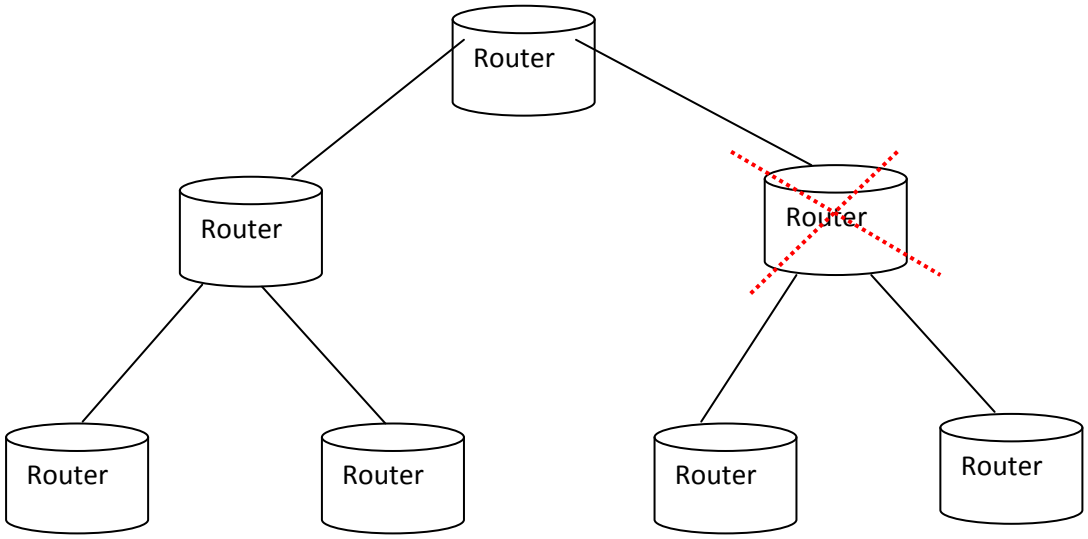


Figure 12: Networking Device Failure

2.6.2. Communication Link Failure

Due to above explain faults in any model if any communication link failed. Devices which are connected to this link will not communicate to each other (see figure 13).

In the below figure two of communication link failed, the communication that will flow using this link is interrupted. Here cross mark shows that link is not working

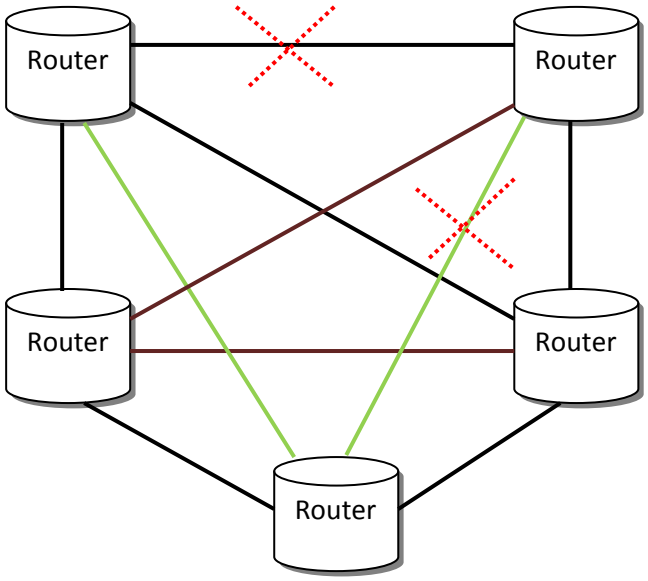


Figure 13: Communication Link Failure

2.7 Fundamental challenges in Routing over Wireless Mesh Network

There are two fundamental challenges in routing over wireless mesh network.

First, routing design has to address issues in both short and long-time scales. Similar to wired routing, coarse-grained routing maintains stable routes in the long term (e.g., tens of seconds or more) [21]. In the meantime, the fine-grained operation has to adapt to the instantaneous wireless channel variations (e.g., the channel coherence time is typically at the scale of a few milliseconds) in order to achieve high throughput [21]. A good wireless mesh routing algorithm has to both ensure long-term route stability and achieve short-term opportunistic performance.

Second, wireless routing has to ensure robustness against a wide spectrum of soft and hard failures, ranging from transient channel outages, links with intermediate loss rates, and failing nodes [29]. Possibility of failures always exists during communication.

2.8 Recovery from the above Failures

There exist different strategies to provide effective communication during failure in the network. One of the solutions to provide communication in the network even though failure exists inside our network is Resiliency [30].

Resiliency is defined as the capability to provide service in the face of failures.

2.9 Resiliency

Origin of resiliency is from Latin verb: "resilire" ~ jump back [31]

Resilience definition in different fields [31]

- In Physics Resiliency is defined as: After a deformation resulting from external forces if a material is able to recover its original state.
- In Ecology Resiliency is defined as in ecology resiliency is moving from stable to disturbance state.
- In Psychology and psychiatry Resiliency is defined as: when facing misfortunate resilience is able to live and develop successfully.

"Resilience is the persistence of *dependability* when facing *changes*."

Changes can be particular attacks:

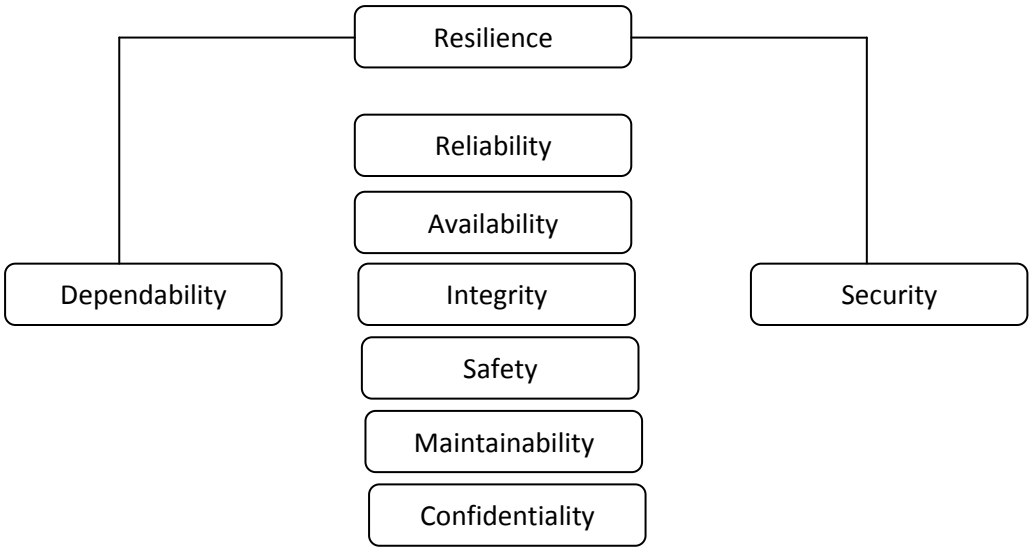


Figure 14: Resilience Types

Computer and communication networks are increasingly critical in supporting business, leisure and daily life in general (see figure 14). There is also an evident increase in cyber attacks on networked systems. Thus, there is a compelling need for resilience to be a key property of networks. Resilience is the ability of the network to maintain acceptable levels of operation in the face of challenges, such as malicious attacks, operational overload, mis-configurations, or equipment failures.

The first phase comprises the use of defensive measures to protect the network from foreseeable challenges, the ability to detect in real-time challenges that have not been anticipated and subsequently remediate their effects before the network operation is compromised, and finally disengage possibly sub-optimal via specific recovery procedures [32].

The second phase caters for the longer-term evolution of the system, through the diagnosis of the causes of the challenge and the refinement of the system operation [32].

2.9.1 Network Resilient Process

The basic idea of network resilient process is that one must be able to (1) perform an offline evaluation of resilience strategies to combat specific types of challenges, then (2) generalise successful solutions into reusable patterns of resilience mechanisms, and finally be able to (3) select and deploy appropriate patterns to address these challenges when they are observed during run-time [32].

The network resilient process is shown in below diagram which consists of three phases (see figure 15).

- Challenge Analysis
- Resilience Patterns
- Resilience Simulation

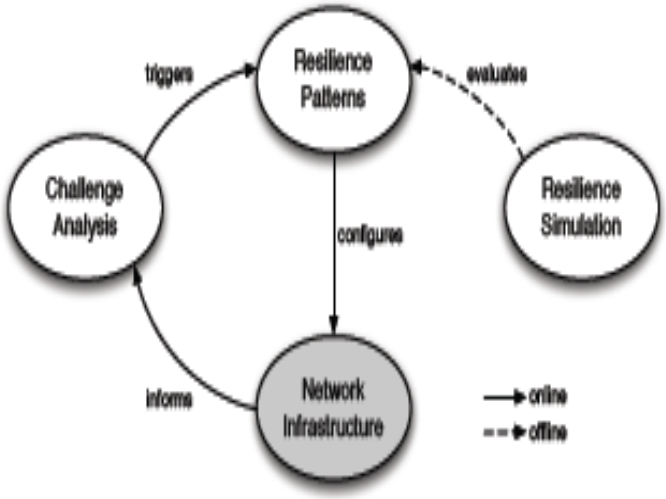


Figure 15: Process for the design and evaluation of network resilient [32]

Challenge Analysis: To gather and store the current state of the network, challenge analysis use online monitoring infrastructure. Metrics of the challenge analysis may produce higher level information or trigger the reconfiguration of the network.

Resilience Simulation: To contest the challenges resilience simulation may use different scenarios and evaluate these scenarios using policy based configurations.

Resilience Patterns: Resilience configurations that perform well against specific challenges in the simulation environment are promoted to reusable patterns [32].

2.10 Motivation

As we march into age of networking communication, the problem of network failure are moreover increases day by day.

To provide effective communication in Wireless Mesh Network, several algorithms have been researched but the possibilities of numerous failures always exist during communication.

Resiliency has been proved to be an important aspect for WMN to recover from these failures or resiliency is the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges [33].

There exist certain perspectives of resiliency [33]:

1. What are the main Future Internet elements
2. What are the main tussles in the Internet
3. Approaches to measuring the validity of Future Internet architectures?

For resilience, a Future Internet should include the following elements, which form a resilience control loop (see figure 16).

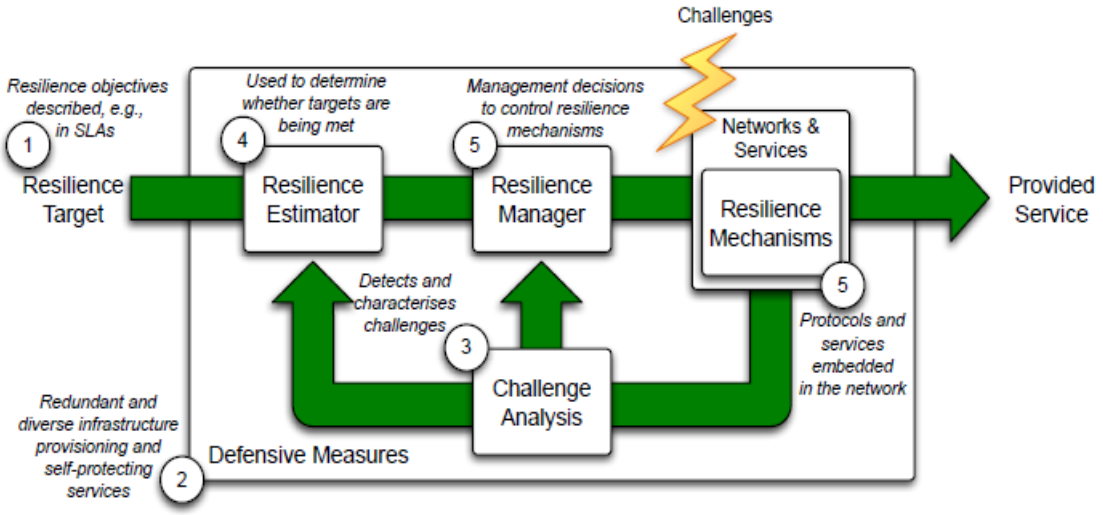


Figure 16: Resiliency control loop Mechanism [33]

Several approaches to effectively perform communication in Wireless Mesh Network (WMN) have been proposed. Further communication failures and possibilities of minimum services during such failures are very hard to maintain. Building up an efficient resilient algorithm which can keep track of network parameter is still a challenge. To understand it in a better way let us take an example:

- **Single failure**: If only single failure arise inside network.

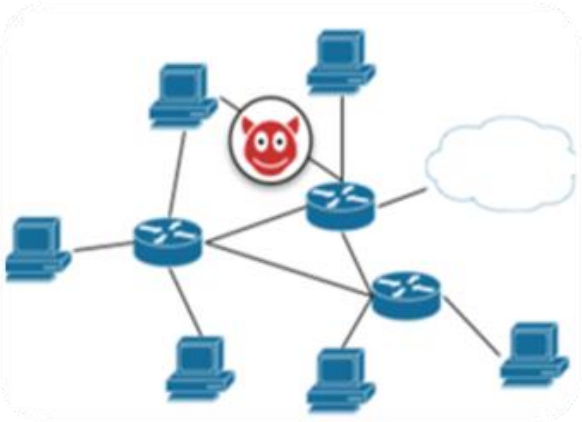


Figure 17: Resilience Measure during single failure [33]

What will be effect of metric (i.e. throughput, network congestion, and resiliency) in the network?

- **Two failures**: If more than one failure arises in the network.

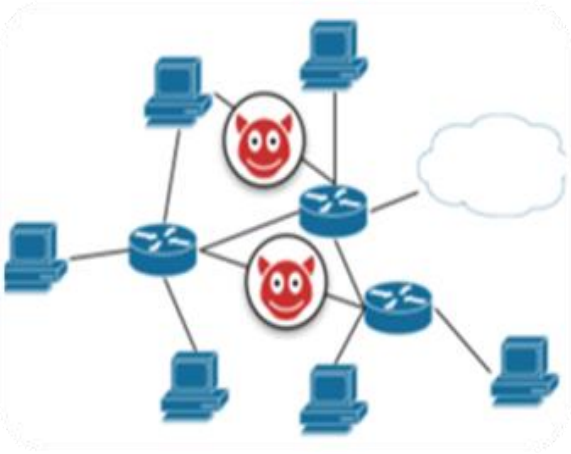


Figure 18: Resilience Measure during two failures[33]

What will be effect of metric (i.e. throughput, network congestion, and resiliency) in the network?

- **Multiple Failures:** if three failures arise in the network.

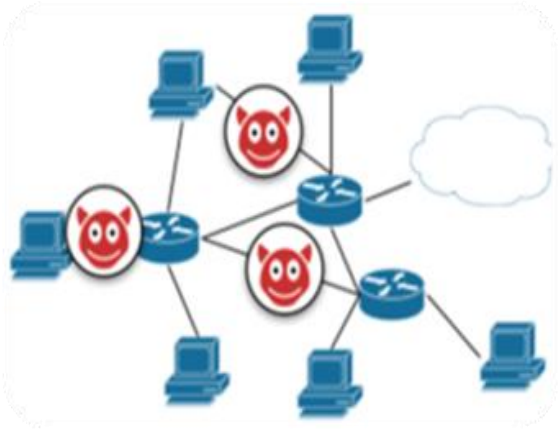


Figure 19: Resilience Measure during three failures [33]

What will be effect of metric (throughput, network congestion, resiliency) in the network?

On considering number of failures in the network what will be the effect of metrics (i.e. throughput, network congestion, resiliency) inside the network. How the resiliency will be affected in that case. There exist three different cases to measure resiliency (see figure 20).

Best case: when in a network of ten nodes only one or two node/link fails and resilient matrices are not affected too much.

Average case: when in a network of ten nodes maximum three or four node/link fails and it will little more affect our resilient metrics.

Worst case: when in a network of ten nodes half of the network gets failed and it will drastically affect our network metrics.

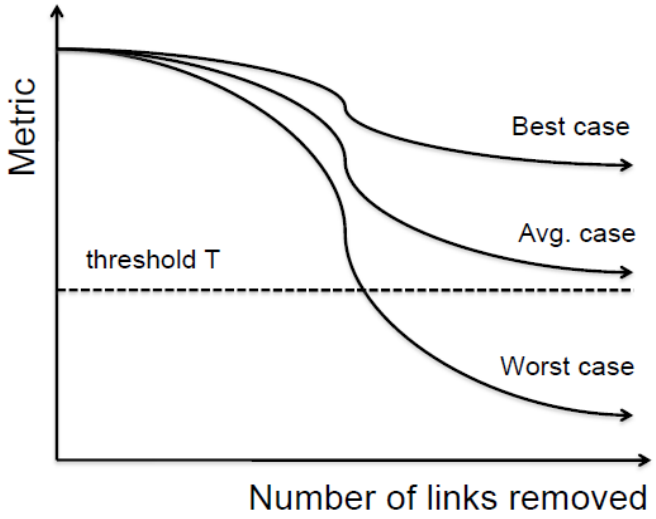


Figure 20: Resilience Measure Graph [33]

2.11 Conventional Approach of Resiliency

In the conventional approaches of Resiliency, they suggest multiple path selection and broadcasting method to send the messages. Means to provide resiliency in network, messages are sent through alternate path at the same time, when one of the node/link fails, sender sends the messages through alternate path to destination node. While in other method resiliency is provided by broadcasting the packets to the entire network. At each node value of R (credit cost) and T (threshold value) will be calculated; only if the value of R is greater than T, packet will be forwarded by the next node. Otherwise (if value of R is less than T) it will be simply discarded by the node without giving the warning signal to source node.

Each conventional approach has its own advantages and disadvantages. For e.g. multicast packet transmission causes traffic overhead, random path selection, resist resilient during multiple failures. While in broadcasting approach delay in packet transmission, high bandwidth consumption, provide fault tolerant with redundancy, credit cost assumption problems are there.

Network during any type of fault happening. We consider a scenario, which shows if any fault occurs in a network device then it will tend all the network devices become either inactive for a specific time or permanently stopped working. The first issue is fault recover and second is redundancy issue.

In order to provide an efficient solution over these drawbacks, we have proposed Buffer Based Routing (BBR) approach which adopts routing technique based on buffer allocation. The routing approach starts with the selection of the route with minimum number of buffered nodes. The proposed approach consists of three steps: i) buffer allocation to the network nodes; ii) selecting optimum path for routing; and iii) resilient packet transmission.

2.12 Basic Overview of BBR (Buffer Based Routing approach)

In order to provide an efficient solution over drawbacks discussed in previous section, we have proposed Buffer Based Routing (BBR) approach which adopts routing technique based on buffer allocation. The routing approach starts with the selection of the route with minimum number of buffered nodes. The proposed approach consists of three steps: i) buffer allocation to the network nodes; ii) selecting optimum path for routing; and iii) resilient packet transmission.
In first step i.e. buffer allocation, according to BBR least cost path selection, buffers are placed at alternate positions in the network.

In the second step i.e. Selection of optimum path for routing, the routing table consist of seven parts i.e. 1) node; 2) node address; 3) next hop; 4) next hop buffered 5) next hop address; 6) cost; and 7) buffered node. Initially buffer space will not be allocated next hop and next hop buffered field. These fields are updated when buffer allocation algorithm is executed. When buffer allocation algorithm is terminated, last visited node consists of the updated which it broadcasts to entire nodes of the network. Thus Routing Table (RT) of each node of the network is updated.

In third step i.e. resilient packet transmission, Aim of RPT is to successfully transfer information from source to destination node of a network even during failures. For this purpose, routing path from source to destination in RPT must have following characteristics [49]:

a) The route must contain minimum number of buffered node.

b) If more than one path has same number of buffered nodes then it will select least cost.

Initially BBR approach allocates buffers to the entire network (as described in part (i)) and after that packet transmission starts. In the network less than or equal to $n/2$ nodes are buffered. During packet transmission, the non buffered node forwards packet to next node and send acknowledgement (ACK) to its preceding node. The preceding buffered node will store packet until ACK is received from next buffered node. When the ACK is received from next buffered node, the preceding buffered node deletes the packet from the buffer.

CHAPTER #3

PREMELARIES AND BACKGROUND

CHAPTER 3

PREMILINARIES AND BACKGROUND

When considering a Wireless Mesh Network (WMN) [23], resiliency [34] is becoming a key requirement and service primitive for various applications. Several algorithms [35-43] based on resiliency for WMN have been proposed. We have considered four of these recently proposed approaches;

1) Resilient Multicasting in WMN [44]

2) Resilient Opportunistic Mesh Routing for Wireless Mesh Networks (ROMER) [45]

3) Resilience in Computer systems and networks [34]

4) An Adaptive Approach to Network Resilient [37]

To examine resilient multicasting approach [44] over WMN, we consider a WMN (figure 21) with source node 'S' and multiple destination nodes D = $\{d1, d2, d3 \ldots . dn\}$ to reach from source to destination. Resilient multicast [45] will select at least two disjoint-node path for each {S, D} pair. In case of failure, traffic will switch to another path to reach the destination. But one of the major drawbacks of resilient multicast is that it increases the network congestion and can immune from any single node/link failure in network. While ROMER [45] define credit based forwarding approach to transmit data from source 'S' to destination 'D'. Source node will forward the packet by taking maximum credit cost. At each node, value of R and T will be calculated; where R is the credit cost to reach from one node to its sink node and T is the threshold value. Source node will forward data with maximum credit to its sink node. As the sink node will get the data it will calculate value of T and compare value of R and T. If $R > T$ then only node will forward the packet, otherwise it will simply discard the packet. The drawback of this algorithm is that if node cost is higher, there is a possibility to discard the packet even at initial stage.

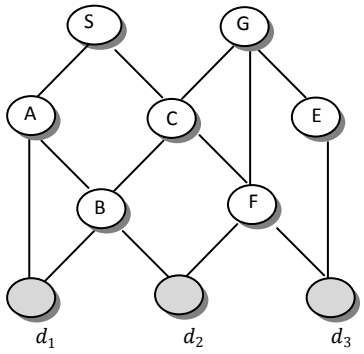


Figure 21: Wireless Mesh Network [49]

We have compared the performance of previous approaches (Resilient Multicasting in WMN [44] and ROMER [45]). This comparative study evaluates disadvantage of these popular approaches to communicate data in WMN. For this study we have considered a WMN as shown in figure 21. Network consists of one source (S) node and three destination ($\mathfrak{D} = \{d_1, d_2, d_3\}$) nodes. Remaining nodes of this network are intermediate nodes. We have firstly evaluated [44] and then [45].

1) Resilient Multicasting in WMN:

Resilient multicast [44] proposed resiliency based routing approach with two node disjoint-paths for each $\{S, \mathfrak{D}\}$ pairs. Let us examine this approach using WMN as in figure 21 where $\{s - d_1\ , s - d_2\ , s - d_3\}$ are three disjoint-paths between$\{S, \mathfrak{D}\}$. The possible steps to communicate data between $\{S, \mathfrak{D}\}$ in WMN using [44] are path estimation and failure recovery.

Step 1: Path Estimation

This step calculates two node disjoint-paths for each$\{S, \mathfrak{D}\}$. *Output:* possible disjoint-paths for figure 21 are as in Table 1:

Path\ $\{S, \mathfrak{D}\}$	**Source−Destination Pair**		
	$\{s - d_1\}$	$\{s - d_2\}$	$\{s - d_3\}$
1	$\{s - A - d_1\}$	$\{s - A - B - d_2\}$	$\{s - C - F - d_3\}$

2	$\{s - C - B - d_1\}$	$\{s - C - F - d_2\}$	$\{s - A - B - d_2 - F - d_3\}$

Table 1: Path Estimation

According to Table1 from $\{s - d_1\}$ there exist two paths $[s - A - d_1]$ and $[s - C - B - d_1]$ and packets will be flooded over both paths concurrently. This approach will increase traffic over two node disjoint path to send packet to a destination. The major drawback of this approach is increase in network congestion. Another drawback with this approach is that it estimates only first two disjoint paths even if other shortest paths exist.

Step 2: Failure Recovery

In previous step two distinct paths are generated to communicate from source S to all three destinations ($\mathfrak{D} = \{d_1, d_2, d_3\}$ (as shown in Table1). Failures may always exist in network during communication. Resilient multicast considers two types of failures in network i.e. node failure and link failure. To explain node/link failure and its recovery let us consider an example where source is S and destination is d_1. Now according to step1 there exist two disjoint paths $[s - A - d_1]$ and$[s - C - B - d_1]$.

The below given cases show the consequences of node/link failure and its recovery using resilient multicast approach [44] (see figure 22).

Case 1: (Node Failure) initially both $[s - A - d_1]$ and $[s - C - B - d_1]$ paths were followed concurrently to communicate the data between $\{s - d_1\}$. If node 'A' fails, destination node d_1 switches to the unaffected path i.e. $[s - C - B - d_1]$.Similarly $\{s - d_2\}$ will follow $[s - C - F - d_2]$ and $\{s - d_3\}$ will follow $[s - C - F - d_3]$ path. Thus even during failure of node 'A', data communication from source S to destination $\{d_1, d_2, d_3\}$ can be achieved (see figure 22).

Case 2: (Node Failure) if node 'C' fails, in case of $\{s - d_1\}$, traffic will switch to the path that excludes node 'C' i.e. it will follow $[s - A - d_1]$ path to reach d_1. Similarly $\{s - d_2\}$ will follow $[s - A - B - d_2]$ and $\{s - d_3\}$ will follow $[s - A - B - d_2 - F - d_3]$ path.

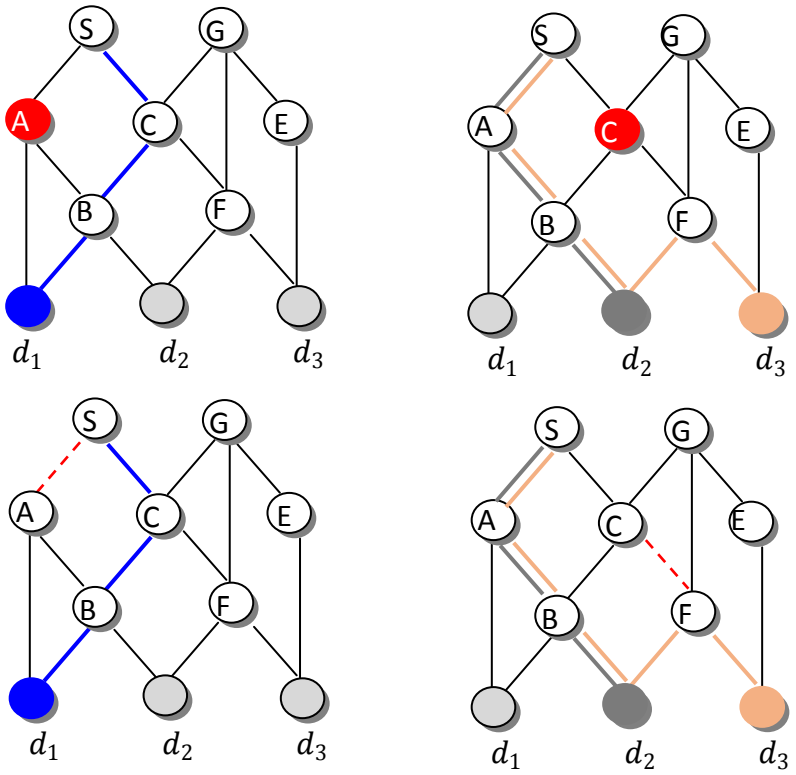


Figure 22: Failure cases in Wireless Mesh Network

Therefore during node failure the approach will switch to another path (as evaluated in step1) which excludes the failure node to communicate between sources to destination (figure 22).

Case 3: (Link Failure) if link between $'s - A'$ fails, then it will affect$\{s - d_1\}$, $\{s - d_2\}$ and $\{s - d_3\}$. Traffic will automatically switch to unaffected path i.e. $[s - C - B - d_1]$ to reach d_1. $[s - C - F - d_2]$ is the path for $\{s - d_2\}$ while $[s - C - F - d_3]$ is the path for $\{s - d_3\}$.

Case 4: (Link Failure) if link $'s - C'$ fails, then $\{s - d_1\}$ path will switch to$[s - A - d_1]$, $\{s - d_2\}$ will follow$[s - A - B - d_2]$ and $\{s - d_3\}$ will follow$[s - A - B - d_2 - F - d_3]$.

If both links $'s - C'$ and$'s - A'$ fails then there is no path available to communicate between $\{s - d_1\}$, $\{s - d_2\}$, $\{s - d_3\}$ and network communication will fail. Similarly if nodes A and C fails (in case 1 and 2) then entire communication fails. Furthermore,

there will be no possible path available to reach to destination except nodes A and C which means it can immune at most one node/link failure in the network.

Key Features of Resilient Multicast Approach

- Packets are forward concurrently on both paths to reach the destination.
- Resilient Multicast do not care about minimum cost between {S, D}.
- In case of node/link failure, traffic on unaffected path reaches the destination.

Disadvantages of Resilient Multicast

- Traffic Overhead
- Resist Resilience during multiple failures
- Random path selection

2) ROMER[13]

ROMER [45] which is another routing approach for WMN. It describes credit based forwarding approach to reach from $\{S, \mathfrak{D}\}$(see figure 23).Where S is the source node and M_2, M_3 and M_5 are intermediate nodes and D is $destination$ node (see figure 24).

In ROMER [45] at each node value of R(credit cost) and T(threshold value) is calculated. If value of R (credit cost) is greater than T(threshold value), then only a node will forward the packet to its destination node. If value of R (credit cost) is less than T (threshold value), packet will be simply discarded by the node. Packets reach to its destination node by consuming a cost present at each node.

Now let us evaluate ROMER [45] which is another routing approach for WMN. It describes credit based forwarding approach to reach from $\{S, \mathfrak{D}\}$ .Where S is the source node and M_2, M_3 and M_5 are intermediate nodes and D is $destination$ node (see figure 24).

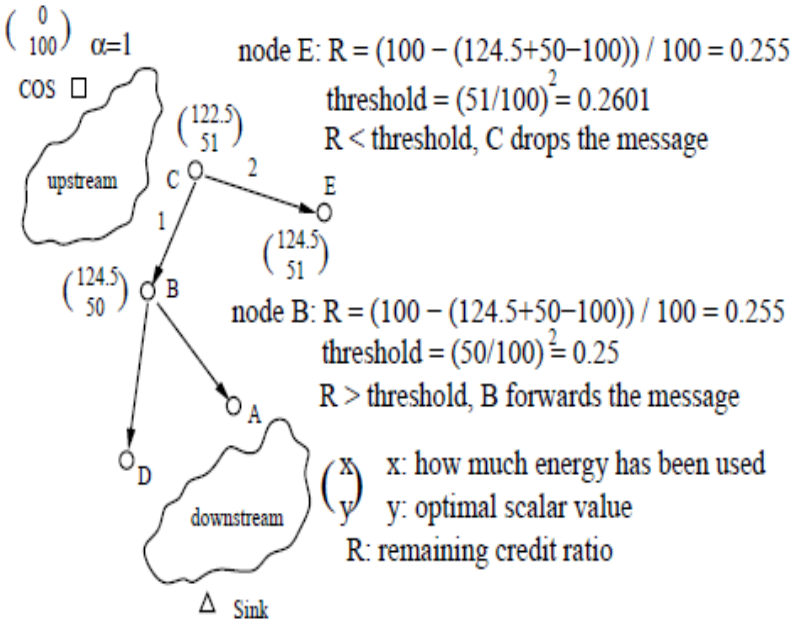


Figure 23: Mesh Based Forwarding [45]

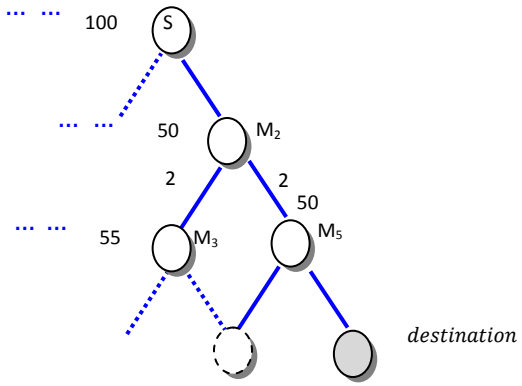


Figure 24: Resilient Opportunistic Mesh Routing for Wireless Mesh Network (ROMER).

Each node is assigned some cost and the packet traverses from one node to another by consuming this cost. To explain this approach let us assume that cost of source node is 100 units and credit limit is also 100 units. Now packet may consume 200 units of cost to reach from$\{S\ to\ \mathfrak{D}\}$.

The possible steps to communicate data between $\{S, \mathfrak{D}\}$ in WMN using [44] are as follows:

Step 1: Let us assume that to reach from node S to M_2 (intermediate node), packet has consumed 120.5 units. Node M_2 broadcasts packet by consuming 2 unit of cost to its next node i.e. M_3 and M_5. At each node the value of remaining credit ratio (R) and threshold (T) are computed and compared. Let us discuss cases of computation at node M_2 which means that there exist two paths i.e. M_2 M_3 and M_2 M_5.

We have shown it using two cases:

Case 1: when credit cost (R) is less than threshold value (T)

Case 2: when credit cost (R) is greater than threshold value (T)

Case 1: (when $R < T$) i.e. discard the packet .The cost of M_2 is 50 units, M_3 has 55 units. In this case it will follow M_2, M_3 path. So, M_2 will forward packet consuming 2 unit of cost to M_3. After receiving the packet, M_3 will calculate R and T. See detail as below:

At M_3, $R = (100 - (120.5 + 2 + 55 - 100))/100$ (1)

$= (100 - (177.5 - 100))/100$ (2)

$= (100 - (77.5))/100$

$= 22.5/100$

$= .225$

Where (122.5+55-100) =77.5 is the amount of credit needed; (100-(77.5)) =22.5 is the remaining credit available for M_3 and 22.5/100 is the ratio of remaining credit to initial credit.

Further threshold value is calculated as T = $(55/100)^2$ =.3025, where 55 is M_3 cost and 100 is the cost of the source.

Case 2: (when R>=T) i.e. packet will be forwarded to next node. The cost of M_2 is 50 units, M_5 has 50 units. In this case it will follow M_2M_5 path. So, M_2 will forward the packet by consuming 2 unit of cost to M_5 .After receiving the packet, M_5 will calculate R and T.

At M_5 R= (100-(120.5+2+50-100))/100 (3)

$$= (100 - (172.5 - 100))/100$$

$$= (100 - (72.5))/100$$

$$= 27.5/100$$

$$= .275$$

Where $(120.5 + 2 + 50 - 100) = 72.5$ is the amount of credit needed. (122.5 is the cost consumed by packet by reaching from source node to intermediate node (M_2) ;50 is the cost of node M_5 and 100 is the source cost (1)) ; $(100 - (72.5)) = 27.5$ is the remaining credit available for M_5 and $27.5/100 = .275$ is the ratio of remaining credit to initial credit. The threshold value T= $(50/100)^2$ =.2500, where 50 is M_5 cost and 100 is the cost of the source. Now, here $R > T$, so packet will be forwarded to next node.

The major drawback of ROMER[45] approach are;1) discarding the packet (when the node cost becomes higher, see figure 23); 2)during node or link failure the possibility of successful packet delivery till the destination node reduces based on the predefined credit cost; comparative study of resilient multicast [44] and ROMER [45] in WMN is shown in table 2. In section 3 we have proposed Buffer Based Routing (BBR) as a solution to overcome these disadvantages.

Key feature of ROMER [45]:

- Source node forwards the packet by taking minimum credit cost.
- Packet reached to destination by consuming credit cost
- At each node credit cost R and threshold value T is calculated
- It broadcast the packet to entire network to avoid node/link failure

Drawbacks of ROMER [45]:

- Delay in packet transmission
- High bandwidth consumption
- Provide fault tolerance with redundancy
- Assume credit cost initially

Resilient Multicast Routing [44] and ROMER [45] are the popular resilient routing algorithms for WMN. Both these approaches are having problems of restricted network throughput, network congestion, and successful packet delivery against node/link failure. Let us introduce both these approaches to classify these problems.

Resilient Multicast Routing Protocol [44] establishes two-node disjoint path to communicate between each $[source, destination]$ pair. In case of node/link failure, traffic on unaffected path reaches the destination. This will increase network communication cost (reduces throughput).

Another drawback of this approach is increased network congestion due to failure of a node/link but multiple failures will further restrict resiliency in the network.

While in ROMER [45], source node forwards the packet by taking maximum credit cost. At each node credit cost R and threshold value T is calculated to reach from source to destination. The major drawback of ROMER is that, if cost at each node is higher then there is possibility to discard the packet. ROMER broadcasts the packets in the network and this will result increased network communication cost (reduces throughput) and increased network congestion due to multiple packet delivery in the network.

Table 2 shows a comparison between ROMER and Resilient Multicast approach:

S.No.	**Resilient Multicasting in WMN**	**ROMER**
1.	It follows two node disjoint-path approach , in which packet forwards concurrently on both paths to reach the destination.	It follows credit based forwarding approach in which packets reached to destination by consuming credit cost.
2.	Resilient multicast can tolerate maximum of 1 node/link failure in network.	During node or link failure the possibility of successful packet delivery till the destination node reduces based on the predefined credit cost.

3.	Network congestion problem occurs as it broadcasts data concurrently on both paths.	Discarding the packet when the node cost becomes higher.

Table 2: Comparison between Resilient Multicast and ROMER

3) Resilience in Computer systems and networks[34]

In this paper the authors describe resiliency in terms of network and systems. Resiliency is one of the important aspects for various systems and networks.

Hutchison et al [46] define resilience is a combination of two things:

- Truth worthiness which is a combination of dependability, security, per formability.
- Tolerance which includes survivability, disruption and traffic tolerance.

The authors describe resiliency metrics with dependability metrics which includes availability, performance, per formability and survivability.

In general, resiliency is the ability to recover from failures [47].

Resiliency is a term which is used in many different fields like dearnley [48] used the resilience term in database systems which is the ability to return to its previous state after performing same action.

More detailed classification of resilience in computer networks and systems is shown in figure 25.

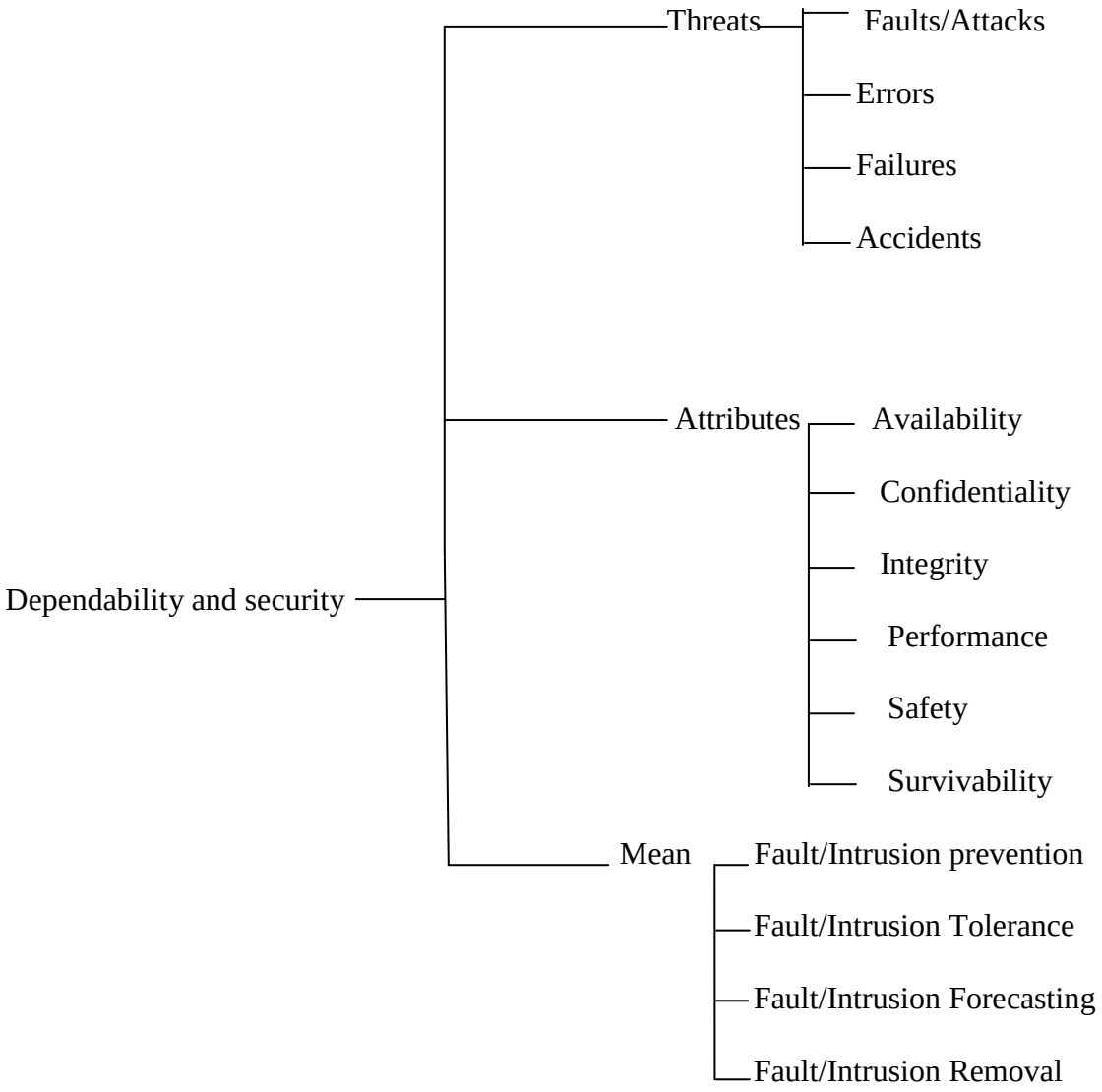


Figure 25: Classification of threats [34]

The authors describe four types of resiliency models:

i) Resiliency of Availability model

ii) Resiliency of Performance model

iii) Resiliency of Per formability model

iv) Resiliency of Survivability model

i) Resiliency of Availability Model

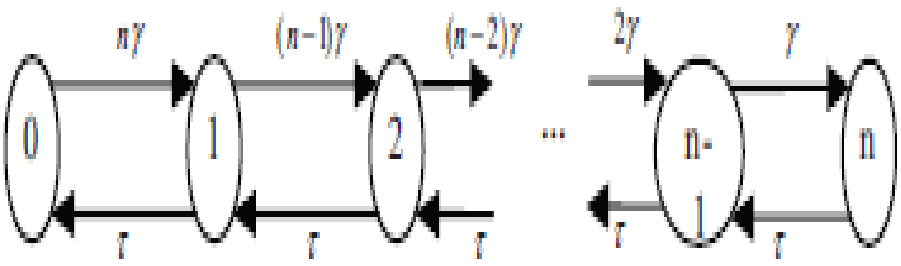


Figure 26: Telephone Switching System Availability Model [34]

Consider there is n number of channels in a telephone switching system (see figure 26). The channel failure and repair time is distributed exponentionally with a mean of 1/n and 1/n respectively.

The author computes two types of unavailability:

- Steady state unavailability UA
- Instantaneous unavailability UA(t)

Let in a state i, u(i) is the steady state probability then

Steady state unavailability = U(A)

U(A) = 0

Here failure rates vary over certain period of time.

There are several ways to integrate time dependent failure with availability models and one of the easiest way is approximation continuous function which is a constant function for computing the network resilience.

ii) Resiliency of Performance Model

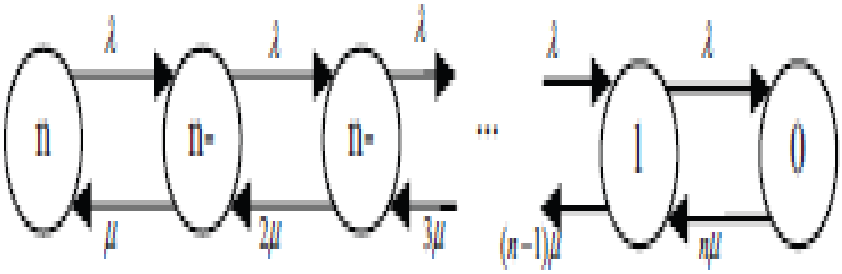


Figure 27: Telephone Switching System Performance Model [34]

The author considers the same telephone switching systems for performance model as shown in figure 27. In figure 27, steady index (j) defines number of channels in use, poision with rate u(x) defines call arrival process and distribution rate u(t) indicates the call holding time.

For a continuous time markov chain (CTMC), let u(x) be a steady state probability in a state i. Then, steady state blocking probability

Pb= u(n)

iii) Resiliency of Per formability Model

To define the per formability of model the authors construct a composite telephone switching system model having n channels. Poison with rate u(x) define call arrival process, distribution rate u(t) indicates call holding time and channel failure and repair time is defined with an exponentionally mean of 1/u(x) and 1/u(t) (see figure 28).
In per formability model, resilience is computed by varying both arrival rate and failure rate after a system comes in steady state.

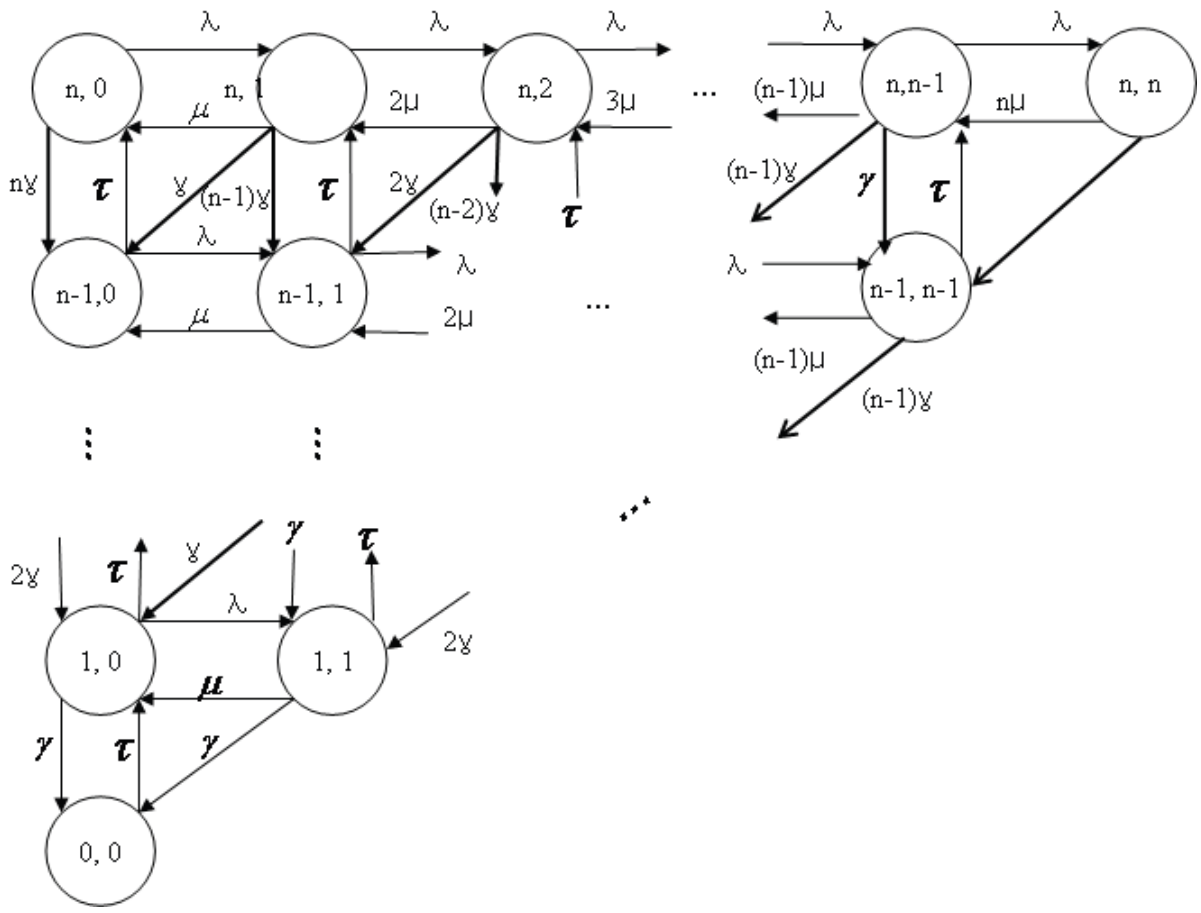


Figure 28: Telecom Switching System Per formability Model[34]

iv) Survivability Model

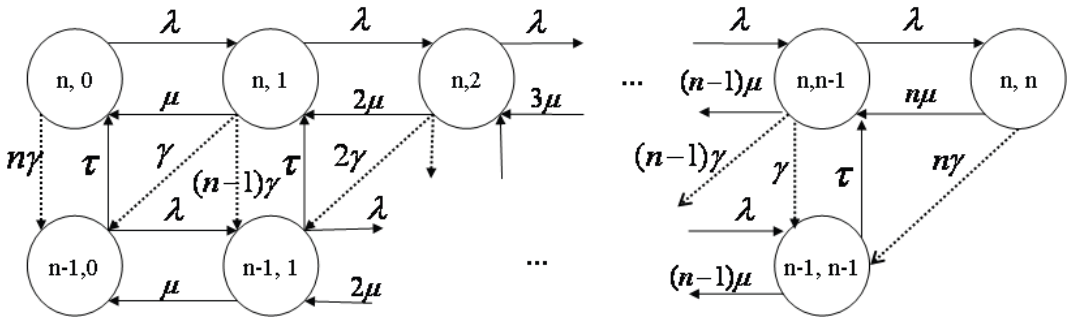


Figure 29: Switching System Survivability Model[34]

In survivability model, instantaneous transitions have taken place which is represented by dotted arcs.

The survivability model is a new composite model which is shown in figure 29.

In this paper, the author constructed a dependable resilience model and varies from performance model to dependable/performance model by applying several changes i.e. failures/overload/increase in arrival rate etc.

Features of resilience in computer systems and networks [34]

- Computer system and network resilience enforce changes in both type of models i.e. availability model and performance model.

- To compute the resilience availability and performance model, failure rate changes over the time.

4) An Adaptive Approach to Network Resilient[37]

A number of mechanism i.e. monitoring system, IP Flow information tool used in intrusion detection and classification system are needed to provide resilience in network.
However, it is very difficult to describe these mechanisms working in a complex multi service network means how the configuration changes over the time when facing new type of challenges, how context changes.

The configuration of resiliency mechanism is done by policy based management framework.

In adaptive approach for network resilient, authors discuss 4 types of approaches:

1) Identification and remediation of fine grain challenge (figure 30).
2) Detection of volume based anomaly technique.
3) Strategies of policy based management.
4) Resiliency of DDOS attacks.

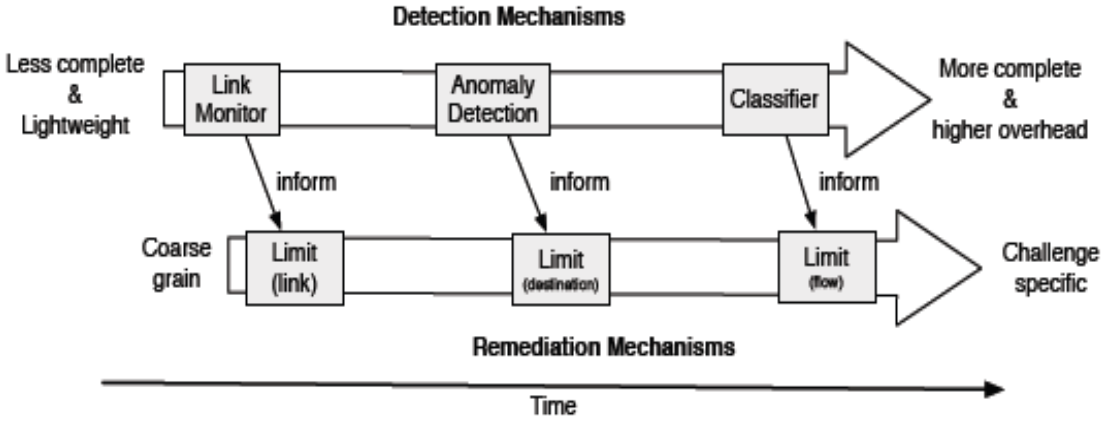


Figure 30: Coarse to fine grain challenge identification and remediation [37]

Policy based management Strategy [37]:

To decouple the hard wired implementation of resilience, policy based mechanisms are used.

For example: rum time management strategy define resilience strategy rule.

Policy based mechanism also discuss the network configuration and resilience mechanism which releases the strategy of resilience without interrupting service operation. For progressive multi stage resilience approach policy based management framework is one of the necessary features.

To configure the resiliency mechanism operation at run time, several policies are used as shown in figure 31.

Here events represents challenges occurrence i.e. DDOS attack, context change i.e. resource availability.

In a policy repository, policies are represented by reconfiguration strategies which define how several component operations in a network should be modified.

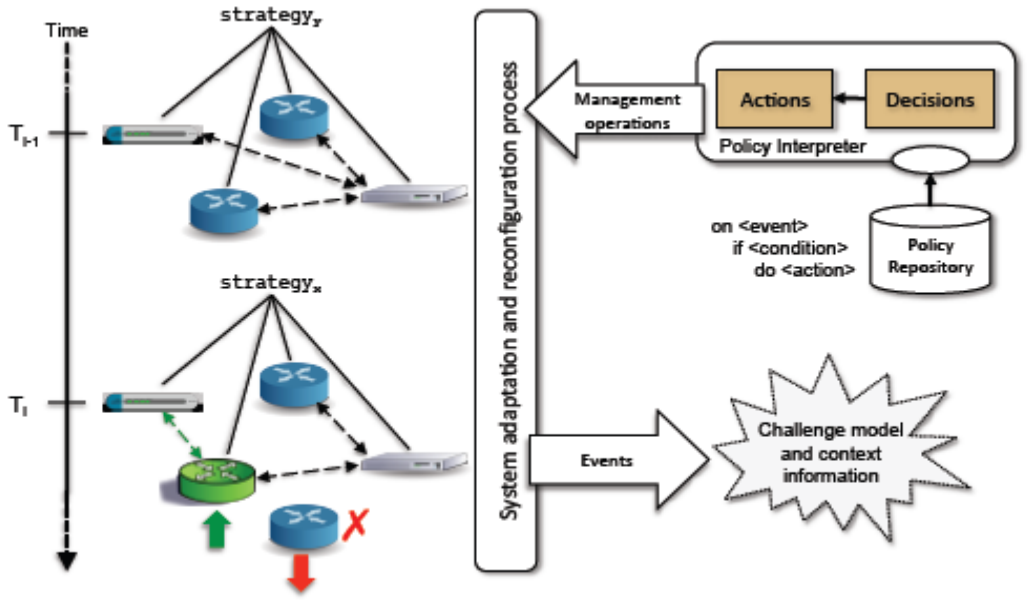


Figure 31: Policy-based reconfiguration of mechanisms during run-time [37]

The subject based decisions and events of policies are evaluated by policy interpreter. These policies determine number of actions to be performed under different circumstances.

The policy may include mechanisms of parameter tuning, interconnection re-wiring and diabling and enabling of dynamic mechanisms which are currently deployed in a particular strategy.

Policy based configuration consider 2 cases:

a) To ensure resilience, it shows the network mechanism to a high traffic volume.

b) Resiliency mechanism shows the schematic representation of enhanced router.

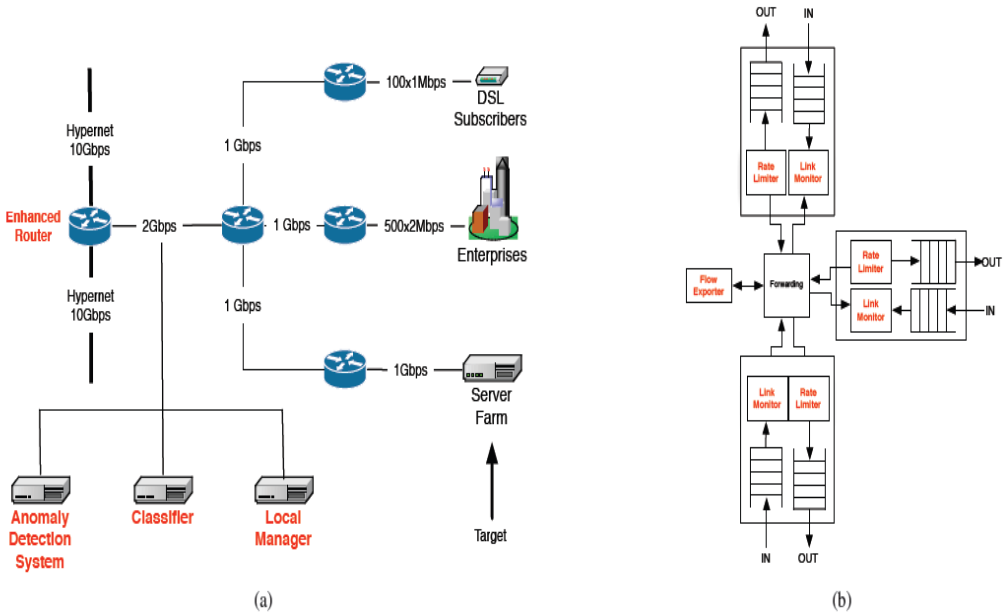


Figure 32: a) Showing the mechanisms used to ensure resilience of the network to high-traffic volume challenges [37]; b) A schematic representation of the enhanced router showing the resilience mechanisms used [37].

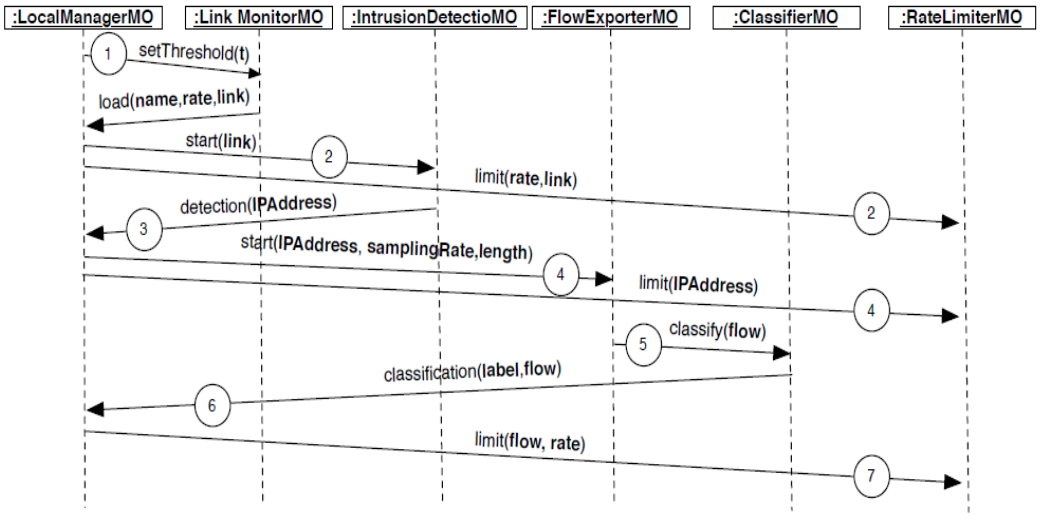


Figure 33: Algorithm for incremental challenge identification and remediation for high-volume traffic challenges [37]

The following steps include the algorithm for incremental challenge identification and remediation [37] as shown in figure 33:

(1) LinkMonitorMO at a given period of time link monitor MO evaluates the utilization of link with threshold rate which is set by localmanager MO.

(2) LocalManagerMO configures the subnetwork components like high utilization of link, MO rate limiter etc. MO rate limiter notified the starting limit of traffic on a link at a given rate. MO rate limiter is coarse grained first remediated action which reduces the overall impact of the attack.

(3) IntrusionDetectionMO for counting the incoming packet link, intrusion detection MO uses threshold based algorithm. Whenever it determine the victim IP address intrusion detection MO raises an event to local manager MO.

(4) As local manager MO receives the event of victim IP from intrusion detection MO, it will limit the traffic for victim IP only.

(5) FlowExporterMO records the IP flow after a specific time out period and send this IP flow record to classifier MO with a given sampling rate.

(6) ClassifierMO, classifier MO identifies the precise nature of flow information by using different machine learning classification algorithms.

(7) LocalManagerMO to permit the non malicious traffic to reach to detection, lacal manager MO limit all the malicious attack flow by notifying the rate limiter MO.

The author represents dynamic deployment of resilience mechanisms by using incremental policy driven approach.

The policy driven process is controlled by policies which relies on context information and in complete challenges.

To identify and remediate the challenges, authors demonstrate the feasibility of policy based approach.
Several case studies have been implemented and deployed to discover the generalization of approach by describing malicious (e.g. worm and bonnets) and non malicious challenges.

CHAPTER # 4

BBR APPROACH FOR WMN

- *Buffer Based Allocation*
- *Buffer Based Routing*
- *Buffer Based Resilient Packet Transmission*

CHAPTER 4

BUFFER BASED ROUTING AND RESILIENCY APPROACH FOR WIRELESS MESH NETWORKING

In previous section we have evaluated several drawbacks allied with both resilient multicasting [44] and ROMER [45] approaches in WMN. In order to provide an efficient solution over these drawbacks, we have proposed a Buffer Based Routing (BBR) approach which adopts routing technique based on buffer allocation. The routing approach starts with the selection of the route with minimum number of buffered nodes. The proposed approach consists of three steps:

i) Buffer Allocation to the network nodes;
ii) Selecting Optimum path for routing; and
iii) Resilient Packet Transmission.

4.1 Buffer Allocation Mechanism using BAA

BBR [49] approach adopts routing technique based on buffer allocation i.e. we provide buffering at each node instead of maintaining routing table. The BBR approach consists of three steps: i) Buffer allocation to the network nodes using BAA; ii) Selection of optimum path for routing; iii) Resilient Packet Transmission.

4.1.1 Buffer Based Allocation

According to BBR [49] least cost path selection, buffers are placed at alternate positions in the network. The buffer allocation is achieved in following steps:

a) Select a node N_i randomly from network in figure 34, where i =1, 2, 3……n number of nodes in this network. Assign buffer to this node and mark it as visited node.

b) Choose least cost path from node N_i to its connected neighbouring node and move to this node, make it as N_i. As buffer allocation process is assigned for alternate nodes. So, skip buffer assignment to this node and just mark as visited.

c) Again choose least cost path from node N_i to its connected neighbouring node. Move to this node and make it as Ni. Assign buffer to this node and mark it as visited node.

d) This step compares whether the next node is visited or not. If node is visited then it rollbacks to its previous node and again search for another node.

e) Repeat steps $a - d$ until total buffer placement in network is performed. The buffering process will stop when the total buffered nodes are $\leq n/2$ where n are number of nodes in the network.

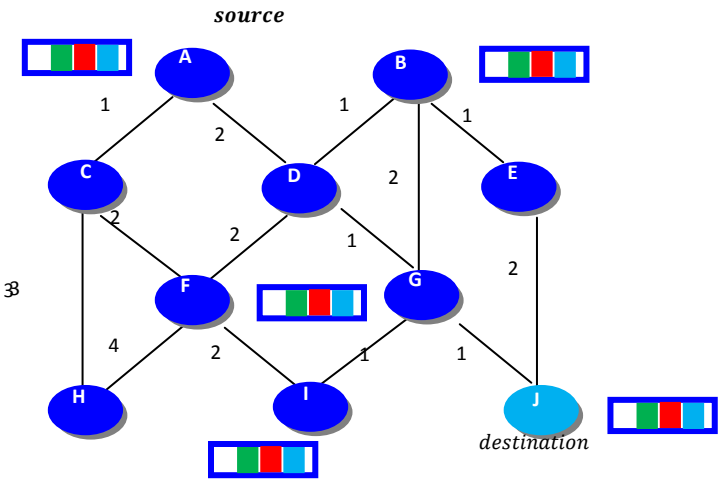


Figure 34: Buffer allocation in the network using BAA (steps $(a - e)$).

Buffers are provided to maintain the resiliency in the network. If we have a network of 10 nodes (figure 34) then total number of buffers allocated in the network are 5. Similarly in a network of 15 nodes, number of buffers allocated in network are 7.

If (n= number of nodes in the network) Then total buffer placement in the network is $\leq n/2$. Minimum and maximum size of buffer is provided to be 5 units of packet i.e. at a

time only 5 packets are stored inside the buffer. To reduce the traffic congestion and increase the speed of data transfer, the minimum and maximum size of buffer is taken to be 5 units. To understand it in a better way let us take an example: figure 34 shows a 10 node network in which source node A and intermediate node F are buffered nodes, let there is only one packet to transmit from source A to destination node J.

Step 1: Node A sends first packet to node C, assuming the transmission of first packet from node A to C is one second.

Step 2: Node C sends an acknowledgement (ack) of packet 1 to node A, assuming ack transmission time is also one second.

Step 3: Further node C transmits the same packet 1 to buffered node F within same time period (i.e. 1 second).

Step 4: Buffered node F sends ack to node C (in 1 sec) and then node C forwards the buffered node F ack to node A (again in 1 sec).

So, total amount of time to transmit the first packet from node A to node F is 5 (1+1+1+1+1) seconds. After 5 seconds first packet will be removed from A buffer node and next packet will arrive. To increase the speed of processing and decrease delay and congestion in the network we take buffer size of 5 units.

The terminologies used in RPT, BBR are shown in table 3.

Terms used in algorithms (table 3,4 and 5)	**Description**
Buffered node Ni	Signifies the node which is a buffered node (i.e. already assigned a buffer)
Next[Ni]	It is used to visit the next node in the network during buffer allocation process
(Node→Node_next)	During allocation of buffers in the network, we maintain a list of nodes that are visited and assigned buffers. So, Node→Node_next which defines: if next node (i.e.

	node→node_next) is present in visited list then rollback to its parent node (i.e. previous→N_i)
Buffer[Ni]	Signifies the array which contains node id of the buffered node
visited list[ ]	It is an array which contains the node id and stores the information of previously visited node in the network
Ni←min_cost_next [N_i]	It is used to select the node which has minimum link cost from the current node and then the node which has less minimum cost will become the next current node
Ni != visited_list[ ]	In our algorithm for each next node N_i we check whether N_i is present in visited list. If N_i is present in visited list array then we go for next node (which has 'next_min_cost(Ni)) otherwise we continue our process from current node
Buffered array[ ]	It is an array which contains node id of the nodes which has already been buffered
visited list[ ] + 1 = Ni	It maintains visited current node N_i into visited_list[]
assign_buffer(Ni)	It is a function used to assign buffer to the node N_i
rollback(previous→Ni)	If node N_i is present in visited list and its next node also present in visited list then we rollback to parent node of N_i
array_buffer[ ]←Ni	It is an array which contains the information about the buffered node, if the node N_i is found eligible to assign then it is added in this array
update_routing_table()	It is a function which is used to update the routing table

Table 3: Terminologies used in BAA and RPT Algorithms

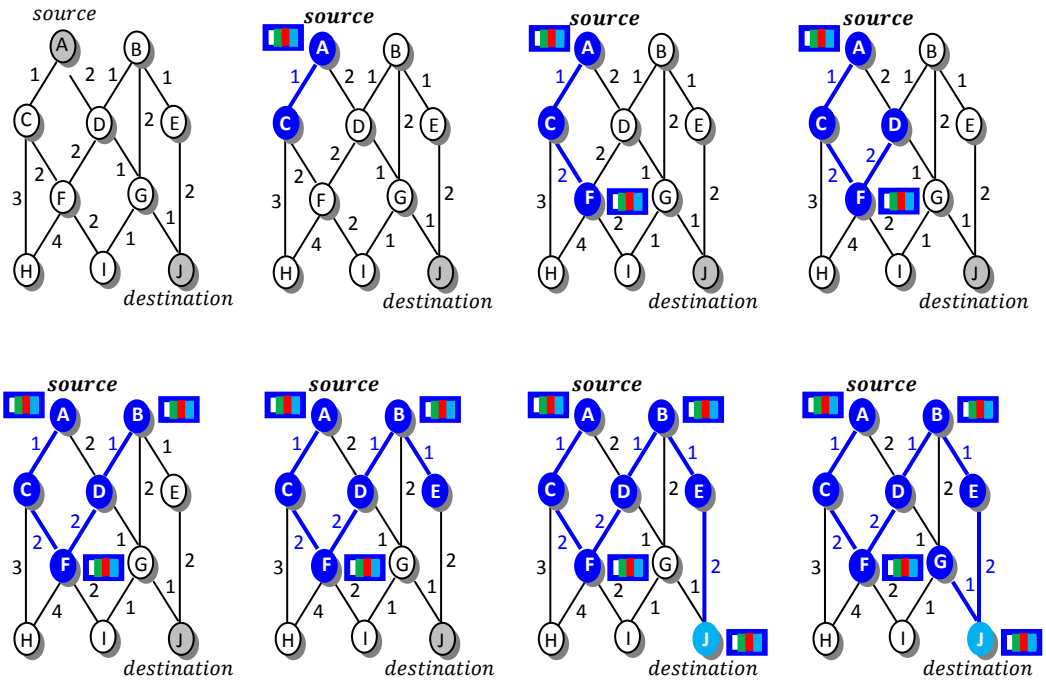


Figure 35: Buffer Allocation Process using BBR

4.1.2 Buffer Based Routing

In BBR approach we have customized the routing table according to include the buffer field with respect to node. The routing table consist of seven parts i.e. 1) node; 2) node address; 3) next hop; 4) next hop buffered?; 5) next hop address; 6) cost; and 7) buffered node? . The construction of routing table involves following steps:

1. Columns node id; node address; next hop id; next hop address; and cost; describe the id of current node, address of the node, id of next hop, address of next hop, cost to the next hop respectively. We do not go in detail of the explanation for updating these fields.
2. Now, the remaining two fields i.e. next hop buffered?; buffered node?; are initialized with the value 'No'. These fields are updating recurrently with the buffer allocation process (shown in Table 4 and Table 5).

3. When the buffer allocation algorithm terminates, the last node broadcast the information of these two fields in the network.
4. All the nodes update their routing table accordingly.

We have shown the routing table of two nodes i.e. source node *A* and destination node d_3. We assume that we start the buffer allocation process form node *A*. The routing tables of each node are updated as the buffer allocation process progresses. For example table 4 shows the routing table of node *A*. Node *A* is the starting node of buffering process so the entries of column Next hop buffered and Buffered node is updated accordingly. Table 5 shows the routing table of node *J*. It is the last buffered node, hence it contain the latest updated routing table. Further, after termination of algorithm node *J* broadcast the routing table information (of two columns i.e. Next hop buffered? and Buffered node?) to entire network. After receiving the updated information each node updates its routing table according to table 5.

As the routing table consist of seven parts i.e. 1) node; 2) node address; 3) next hop; 4) next hop buffered 5) next hop address; 6) cost; and 7) buffered node. Initially buffer space will not be allocated next hop and next hop buffered field. These fields are updated when buffer allocation algorithm is executed. When buffer allocation algorithm is terminated, last visited node consists of the updated which it broadcasts to entire nodes of the network. Thus Routing Table (RT) of each node of the network is updated. Table 5 shows RT of buffered node J which is the last step of BAA algorithm before termination.

Node ID	Node address	Next hop ID	Next hop buffered?	Next hop address	Cost	Buffered node?
A	…	C	No	…	1	Yes
A	…	D	No	…	2	Yes
B	…	D	No	…	1	No

B	…	G	No	…	2	No
B	…	E	No	…	1	No
C	…	F	No/Yes	…	2	No
C	…	H	No	…	3	No
D	…	A	No/Yes	…	2	No
D	…	B	No/Yes	…	1	No
D	…	F	No/Yes	…	2	No
D	…	G	No	…	1	No
E	…	B	No/Yes	…	1	No
E	…	J	No/Yes	…	2	No
F	…	C	No	…	2	No
F	…	D	No	…	2	No
F	…	H	No	…	4	No
F	…	I	No	…	2	No
G	…	D	No	…	1	No
G	…	B	No/Yes	…	2	No
G	…	I	No	…	1	No
G	…	J	No/Yes	…	1	No
H	…	C	No	…	3	No
H	…	F	No/Yes	…	4	No
I	…	F	No/Yes	…	2	No

I	...	G	No	...	1	No
J	...	G	No	...	1	No
J	...	E	No	...	2	No

Table 4: Node A Routing Table

Similarly the routing table of each node have constructed. Here we shown the routing table of last node i.e. J.

Node ID	Node address	Next hop ID	Next hop buffered?	Next hop address	Cost	Buffered node?
A	...	C	No	...	1	Yes
A	...	D	No	...	2	Yes
B	...	D	No	...	1	Yes
B	...	G	No	...	2	Yes
B	...	E	No	...	1	Yes
C	...	F	Yes	...	2	No
C	...	H	No	...	3	No
D	...	A	Yes	...	2	No
D	...	B	Yes	...	1	No
D	...	F	Yes	...	2	No
D	...	G	No	...	1	No
E	...	B	Yes	...	1	No
E	...	J	Yes	...	2	No
F	...	C	No	...	2	Yes
F	...	D	No	...	2	Yes
F	...	H	No	...	4	Yes
F	...	I	No	...	2	Yes
G	...	D	No	...	1	No

G	...	B	Yes	...	2	No
G	...	I	No	...	1	No
G	...	J	Yes	...	1	No
H	...	C	No	...	3	No
H	...	F	Yes	...	4	No
I	...	F	Yes	...	2	No
I	...	G	No	...	1	No
J	...	G	No	...	1	Yes
J	...	E	No	...	2	Yes

Table 5: Node J Routing Table

4.1.3 Buffer Based Resilient Packet Transmission

Aim of RPT is to successfully transfer information from source to destination node of a network even during failures. For this purpose, routing path from source to destination in RPT must have following characteristics [49]:

a) The route must contain minimum number of buffered node
b) If more than one path has same number of buffered nodes then it will select least cost.

Initially BBR approach allocates buffers to the entire network (as described in part (3.1.1)) and after that packet transmission starts. In the network less than or equal to $n/2$ nodes are buffered. During packet transmission, the non buffered node forwards packet to next node and send acknowledgement (ACK) to its preceding node. The preceding buffered node will store packet until ACK is received from next buffered node. When the ACK is received from next buffered node, the preceding buffered node deletes the packet from the buffer. The detailed explanation of packet transmission and failure cases has been already discussed in our previous paper [49]. Table 6 shows the proposed Resilient Packet Transmission (RPT) algorithm.

In our approach we have customized buffer based routing path along with packet content. To understand resilient packet transmission, let us consider a WMN of 10

nodes (figure 33). Here source and destination are randomly selected throughout the network. Our aim is to send data packets from the source node 'A' to destination node 'J'. For packet transmission the routing path need to have following characteristics:

a) The route must contain minimum number of buffered node.
b) If more than one path has same number of buffered node than it will select the least cost path.

The acknowledgement (*ack*) message consist *ack* as well as the id of sender node. Round trip time is defined (RTT) as transmission time of packets from one node to its succeeding node and then receiving acknowledgement back from that succeeding node.

Routing from node A to node J is progressed in following steps:

Step 1: According to buffer allocation process for WMN network as in figure 34 'A' is the buffered node so it store packets until it receive acknowledgement from the next buffer node. By considering its routing table, it will select path $[A - C - F - I - G - J]$ and wait for ack from node C and buffered node F.

Step 2: Node C is the next hop so it receives the packet and lookup the routing table for the next hop which tends towards destination. As it is a non-buffered node it forwards the packet to the next node i.e. F and send *ack* to node A.

Step 3: When node F receives the packet it stores that packet into its buffer. Further it sends *ack* to node C, and forward the packet to next node i.e. I. Meanwhile after receiving the *ack* from node F. Node C will send an *ack* to previous buffered node A. Further node A deallocate packet from its buffer.

Step 4: After receiving the packet, node I forwards this to next hop i.e. node G .

Step 5: Node G forwards the packets to node J which is the destination node.

Note: In our approach the *ack* is send by both buffered and non- buffered nodes. But buffer node stores the data packet until it receives the *ack* of next buffered node. It confirms the delivery of message to the next buffered node.

Let us see following cases: (by considering figure 35)

Case1: Node Failure: if a node fails during communication in network.

Let us suppose node *'I'* fails.

Step 1: As node *'F'* will not able to get ack within its RTT (Round Trip Time) then node *'F'* will send packet one more time, even if it is not able to get an ack then it will assume that node *'I'* has been failed.

Step 2: Node *'F'* will select its next least cost and will send packet to route *'$F-D-G-J$'*.

Further we consider another situation, if node *'G'* fails, node *'I'* will not able to get ack within RTT, then node *'I'* will roll back because there is no other path exist other than node *'G'* to reach to destination. Then node *'F'* will follow *'$F-D-B-E-J$'* path. Advantage of having buffer in network is that in case of node failure there is no need to re-establish the path and can simply access packet from buffers present at intermediate nodes.

Case 2: Link Failure: when a link fails inside a network during communication between source and destination.

Let us take an example when link *'$F-I$'* fails. Link failure case is similar to node failure

Step 1: let *'A'* be source node and *'J'* be the destination node. Node *'A'* will follow its routing table and see that intermediate buffered nodes are in two different paths so it will follow a path with minimum cost path i.e. *'$A-C-F-I-G-J$'* and send packet through this path.

Step 2: As the packet reaches to node *'F'* , there is a link failure *'$F-I$'* so; node *'F'* will not be able to get *ack* within RTT. So node *'F'* will follow another path by seeing its routing table i.e. *'$F-D-G-J$'* which is next highest least cost distance between s, d.

Step 1	a) **select random node N_i from the network.** b) **Assign buffer (N_i);** c) **Visited list [] =N_i;**
Step 2	d) **if (next [Ni]! =null)** e) **Ni←min_cost_next [N_i];** f) **If (Ni=visited list [])**

	g) **Select next_min_cost (N_i);** h) **Go to step (d);** i) **end if;** j) **Else** k) **If (previous [Ni] =buffered array [])** l) **Skip (N_i);** m) **Visited list [] +1=N_i;** n) **Goto step (d);** o) **end if;** p) **Else** q) **Allocation(N_i);** r) **Gotostep(d);** s) **end else;** t) **end else;** u) **end if;** v) **Else** w) **Rollback (N_i);** x) **end else;**
Step 3	**Repeat step 2 until two rollbacks occur at the same node;**
Step 4	**Return;**

***Allocation* (*Ni*)**

begin

if (Ni!=visited_list[])

assign_buffer(N_i);

visited_list [] +1=N_i;

end if;

else

rollback (previous→N_i);

end else;

end;

***assign_buffer* (*Ni*)**

begin

assign buffer to N_i;

array_buffer []←N_i;

update_routing_table();

end;

Table 6: Buffer Allocation Algorithm

1. Source (buffered) node starts transmission through least cost path by considering its routing table (in accordance to section 2.1.3 (a) and (b))
2. Wait for two ack's (buffered node/non buffered node)

3. **If** (next[N_i]!=buffered node N_i)
4. Receive and forward the packets to its downstream node N_i and starts RTT (round trip time).
5. Send ack to its previous node N_i.
6. Go To step(3)
7. **End: if**
8. **Else If** (next[N_i]=buffered [N_i])
9. Store and forward the packet to next N_i and starts RTT
10. Send ack to its previous node N_i
11. Wait for two ack's.
12. **If** (two ack's received within RTT)
13. Go To step(8)
14. **Else**
15. Go To step(22)
16. **End: else if**
17. **Else**
18. **If** (Packet receive within its RTT)
19. Repeat step 3
20. **End: if**
21. **Else**

22. Failure (N_i) **23.** **End: else** **24. End: elseif** **25.** **Else** (destination node) **26.** Receive and store packet **27.** Send ack to its previous node. **28. End: else**
Failure (N_i) 1. **If** (failure N_i=exist) 2. Preceding buffered node select another least cost path to destination node. 3. **End if**

Table 7: Resilient Packet Transmission Algorithm

4.2 Complexity Analysis of BAA and RPT Algorithms

This section shows the time complexity of proposed BAA [49] and RPT approach. BBR approach is previously allocating buffer till the destination but now, we have updated the BBR approach to work for un-traversed link beyond destination. The time complexity of both BAA and RPT is executed as $O(Nlog_2(N)$ using Brute Force method. Table 8 and 9 shows the time complexity of BAA and RPT approaches.

1. Select random node N_i from the network	$O(1)$
2. Assign buffer (N_i)	$O(1)$
3. Visited list [] =N_i	$O(log_2(N))$
4. **If** (next [Ni]! =null)	$O(1)$
5. Ni←min_cost_next [N_i]	$O(N)$
6. If (Ni=visited list [])	$O(log_2(N))$
7. Select next_min_cost (N_i)	$O(1)$
8. Go To step (4)	$O(Nlog_2(N))$
9. **End if**	

10. Else	
11. If (previous [Ni] =buffered array [])	$O(log_2(N))$
12. Skip (N_i)	$O(1)$
13. Visited list [] +1=N_i	$O(log_2(N))$
14. Go To step (4)	$O(log_2(N))$
15. End if	
16. Else	
17. Allocation(N_i)	$O(Nlog_2(N))$
18. Goto step(4)	$O(Nlog_2(N))$
19. End else	
20. End else	
21. Else	
22. Rollback (N_i);	$O(1)$
23. End else	
24. Repeat step 2 until two rollbacks occur at the same node;	$O(1)$ $\times Nlog_2(N)$
25. Return;	
***Allocation* (*Ni*)**	
Begin	
1. If (Ni!=visited_list[])	$Olog_2(N)$
2. assign_buffer(N_i)	$Olog_2(N)$
3. visited_list [] +1=N_i	$O(1)$
4. End if	
5. Else	
6. rollback (previous→N_i)	$O(1)$
7. End else	
8. End	
***assign_buffer* (*Ni*)**	
Begin	
1. assign buffer to N_i	$O(1)$
2. array_buffer []←N_i	$O(1)$
3. update_routing_table()	$Olog_2(N)$

4. End	
Total complexity of Buffer allocation algorithm:	$O(Nlog_2(N)$

Table 8: Time Complexity of BAA Algorithm

1. Select random node N_i from the new Source (buffered) node starts transmission through least cost path by considering its routing table	$O(log_2(N))$
2. Wait for two ack's (buffered node/non buffered node)	$O(1)$
3. If (next[N_i]!=buffered node N_i	$O(1)$
5 Receive and forward the packets to its downstream node N_i and starts RTT(round trip time)	$O(1)$
6 Send ack to its previous node N_i	$O(1)$
7 GoTo step(3)	$O(N)$
8 End: if	
9 **Else If** (next[N_i]=buffered [N_i])	$O(1)$
10 Store and forward the packet to next N_i and starts RTT	$O(\log(N))$
11 Send ack to its previous node N_i	$O(1)$
12 Wait for two ack's	$O(1)$
13 **If (**packet received within RTT)	
14 Go To step(8)	$O(N)$
15 Else	
16 Go To step(22)	$O(N)$
17 End: elseif	
18 Else	
19 **If** (Packet receive within its RTT)	$O(1)$
20 Repeat step 3	$O(N)$
21 End: if	
22 Else	
23 Failure(N_i)	$O(\log(N))$

24 End: else **25 End: else if**	
26 **Else** (destination node) 27 Receive and store packet 28 Send ack to its previous node **29 End: else**	$O(1)$ $O(1)$ $O(1)$
Failure (N_i) **1. If** (failure N_i=exist) **2.** Preceding buffered node select another least cost path to destination node. **3. End if**	$O(1)$ $Olog_2(N)$
Total complexity of RPT algorithm:	$O(Nlog_2(N)$

Table 9: Time Complexity of RPT Algorithm

The time complexities of Buffer Allocation and RPT algorithms are $O(Nlog_2(N)$.

CHAPTER #5

PERFORMANCE ANALYSIS

- *Resilient Multicast*
- *ROMER*
- *BBR*

CHAPTER 5

PERFORMANCE ANALYSIS

In this chapter we have simulated the performance of BBR approach using MAT LAB. A MAT LAB is a high level language and interactive environment for numerical computation, visualization and programming. We can analyze data, develop algorithm i.e. signal processing, image and video processing control system and communication, computational biology, test and measurement computational.
MAT LAB is a foundation for all products i.e. parallel computing, mathematics, statistics, test and measurement, application development. MAT LAB is a numerical commutating environment and 4G programming language.

We have evaluate performance analysis of BBR (Table 10) in terms of network performance parameters i.e. throughput, resiliency against node/link failure, network congestion and delay. These parameters are defined as:

Throughput*:* throughput is defined as how fast we can actually send data through a network.
Resiliency against node/link failures*:* how resiliency implemented in case of failures.

Network congestion*:* how much load on network exists during transmission of data between source and destination?

Delay: how long it takes for an entire message to completely arrive at destination.

Since Resilient Multicast [44] follows two-node disjoint path, packets broadcast to the network and follows both paths concurrently to reach the destination. In case when any intermediate node/link fails, then packets will automatically switch to unaffected path due to which load on that path increases and throughput decreases. In ROMER [45] throughput is higher than resilient multicast and all packets follow single path. In the proposed approach buffers are placed according to least cost path selection and during packet transferring ,it choose path which has less number of intermediate buffers from {S, D}, so throughput increases because it sends data according to least cost path.

In resilient multicasting packets [44] flows parallel and concurrently through 2-node disjoint path, in case of any node/link failure packets will shift to single path due to which cost of resilient multicast increases. But in ROMER [45] packets follows single path and forward packets according to credit limit. In case when initial credit limit is less, cost at each node is very high and number of failures exists in network, there are more chances of discarding packets by the node. In the proposed approach we employ buffers for storing the packets coming from previous nodes. In case any non-buffered node fails, then we can get data from its preceding buffer and if buffered node fails then. Table 10 shows the theoretical comparison of BBR [49] which shows how BBR [49] approach is advantageous over Resilient Multicast [44] and ROMER [45].

Parameters	Performance	Reasons
Throughput	Increases	Because of least cost buffered path selection during transmission process.
Resiliency against node/link failure	Increases	Because transmission starts from previously buffered node.
Network congestion	Decreases	Due to limited buffer capacity, number of packets in network are less.
Delay	Decreases	Due to transmission of packets (after transmission of first packet)
Reliability and robustness	Increases	Because of implementation of resiliency, network is more reliable, chances of network failure are less.

Table 10: Performance Analysis of BBR

To analyze the performance of BBR [49] approach, let us consider first, a network of five nodes (see Fig. 35(a)) where A is the source node, E is the destination node and compare between these approaches. Now, evaluating the performance of Resilient Multicast [44] ,ROMER [45] and BBR [49] over five different network sizes i.e. $5, 10, 15, 20, 25$

Evaluate network performance using some parameters i.e. throughput (defined in terms of cost), network congestion (in terms of packet transmission) and resiliency against node/link failure (in terms of fault tolerance). We have considered cost as total amount of delay occurs during transmission of packets from source to destination. While packet

transmission is the total number of packets transmitted at a time in network and fault tolerance is possible numbers of paths exist after failure.

5.1 Throughput Analysis of RM, ROMER, BBR

a) Network Throughput: Throughput is defined in terms of cost i.e. total amount of delay occurs during transmission of packets from source to destination. Let us evaluate network throughput of these approaches for network size 5 (Fig. 35(a)).

i) Network throughput of Resilient Multicast [44]: This approach selects at least two node disjoint paths to send data packets. To analyze throughput, we calculate the total amount of cost of selected disjoint paths to reach from $S - D$ (see Fig. 35(a)). Source A selects two disjoint paths i.e. i) $A - B - D - E$ which consumes $1 + 2 + 2 = 5$ units (through $A - B,\ B - D, D - E$) and ii) $A - C - E$ which consumes $2 + 1 = 3$ unit of cost (through $A - C,\ C - E$). So, packet is sent to its destination node by consuming (cost of path 1 + cost of path 2) $5 + 3 = 8$ units.

ii) Network Throughput of ROMER [45]: This approach forwards the packet by taking maximum credit cost (which is assumed at the source node). ROMER states that each node has some cost and packets will be forwarded by every node after calculating the value of credit cost R and threshold value T.

Such that :

If $(R > T)$**)**
Then node forwards the packet;
Else
Discard the packet;

The detail steps of this approach for network size 5 are as:

- Initially 'A' broadcasts data to its downstream nodes i.e. B and C, which

consume total 3 unit of cost to send the packets ($A - C$ = 2 unit) and ($A - B$ = 1 unit).

- Assuming cost of node $B = 55$ and node $C = 50$. Packet will be forwarded by downstream nodes after calculating the value of R and T. At node B if $R < T$ then it discards the packet. At node C, assume $R > T$ then it forwards the packet to its downstream nodes D and E. So the total cost of sending the packets from $C - D$ and $C - E$ is $1 + 1 = 2$ units.

- Further value of R and T are calculated at node D then it forwards the packet to destination E after consuming 2 unit of cost.

- Now cost to send the packets from $A - E$ is (cost in (i) + cost in (ii) + cost in (iii)) i.e.; $3 + 2 + 2 = 7$ units of cost.

iii) Network Throughput of BBR [49]: According to our proposed approach packets are sent through a route which has least number of buffered nodes. In Fig. 35(a), the path $A - C - E$ contains minimum buffered nodes i.e. 2. So it sends the packet using $A - C - E$ path by consuming $2 + 1 = 3$ units (cost of $A - C + C - E$). Hence, BBR approach takes less amount of cost to send data packets from $S - D$.

5.2 Network Congestion of RM, ROMER, BBR

b) Network Congestion: It is defined in terms of rate of packet transmission i.e. total number of packets transmitted at a unit of time in a network. Let us evaluate network congestion on these approaches.

i) Network Congestion on Resilient Multicast: Fig. 36(a) shows that source A has 20 packets to transmit to destination node. Resilient Multicast [44] sends the packets through two-node disjoint paths

i.e. $A-B-D-E$ and $A-C-E$. Twenty packets will be sent through either of these path i.e. $A-C-E$. Resilient Multicast uses redundant copy of these packets to send through other path i.e. $A-B-D-E$. If source node has 20 packets to transmit, [45] will send 40 packets in network.

ii) Network Congestion on ROMER [45]: To provide successful delivery of packets to the destination node. It delivers redundant copy of packets in the network.(see Fig. 36(a)) let source node A has 20 packets to transmit. To calculate the cost consider following steps:

- *'A'* forwards traffic to both nodes i.e. B and C, so total number of packets are $20+20=40$.
- *'B'* discards the packet in case$(R<T)$ and node C forwards redundant copy of packets to D and E. Now, numbers of packets to transmit are $20+20=40$ packets.
- *'D'* forwards the packets through single path i.e. $D-E$ which transmits 20 packets.
- Total number of packets inside the network is $40+40+20=100$ packets (traffic size of ((i) + (ii) + (iii)).

iii) Network congestion on BBR [49]: It forwards the packets according to its buffer capacity as shown in Fig. 36(a). Buffers are placed at alternate positions. Each buffer has size of 4 units. If Source node *'A'* has 20 units to transmit then only 8 packets will be forwarded inside the network at a time.

5.3 Network Resilience of RM, ROMER, BBR

c) Network Resiliency: Resiliency against node/link failure is measured in terms of fault tolerance. Fault tolerance is defined as possible number of paths exists after failure. Let node B has failed.

i. Resiliency in Resilient Multicast [44]: Resiliency achieved in [44] through two-node disjoint path. (See Fig. 36(a)) source 'A' selects two paths $A-$

$B - D - E$ and $A - C - E$. If node 'B' fails, then resiliency is achieved by using second path i.e. $A - C - E$. If node B and C fails, then there is no possible way to reach to destination.

ii. Resiliency in ROMER [45]: Resiliency achieved in [45] by forwarding the redundant copy of packets in the network. Initially [45] forwards the packets through three possible path i.e. $A - B - D - E$, $A - C - D - E$, $A - C - E$. If node B fails then there exist 2 possible paths i.e. $A - C - D - E$ and $A - C - E$.

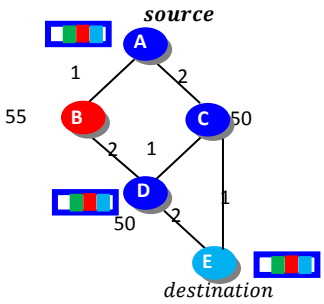
iii. Resiliency in BBR [49]: Resiliency achieved in BBR by storing data packets in buffers placed at alternate positions in the network, when failure occurs in the network during transmission of data packets, the previously buffered node selects another efficient path for packet transmission (see Fig. 36(a)). If node *'B'* fails then there is no effect inside the network because we send the data packets through $A - C - E$ path.

To evaluate the accuracy of performance evaluation of Resilient Multicast, ROMER and BBR we have analyzed the network parameters (throughput, network congestion, resiliency) on $10, 15, 20, 25$ network sizes (see table 11).

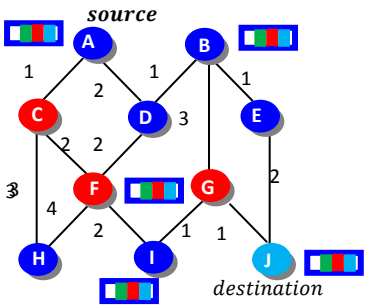
Parameter Metric	**Resilient Multicast**	**ROMER**	**BBR**
Throughput	8	7	3
Network congestion	40	100	8
Resiliency	1	2	1

Table 11: Parameter growth of three approaches in a network of five nodes

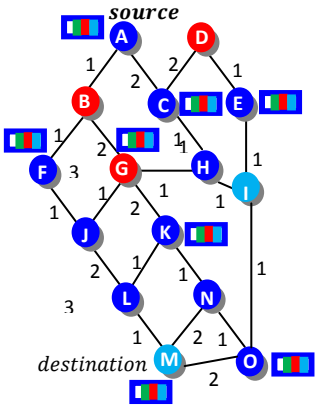
For network size 10: we analyzed network parameters (throughput, network congestion and resiliency against node/link failure) on three approaches i.e. Resilient Multicast [44], ROMER [45] and BBR [49] using a network of 10 nodes.



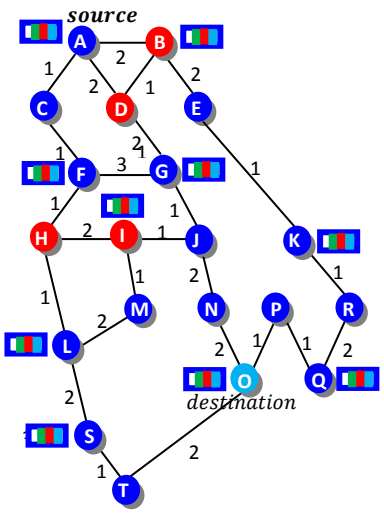
(a)



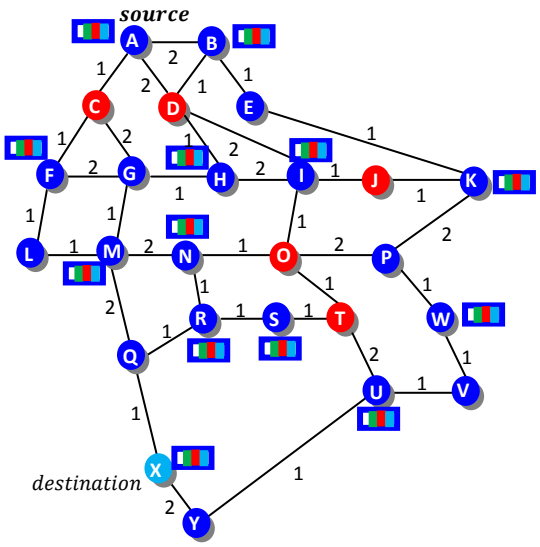
(b)



(c)



(d)



(e)

Figure 36: Network with different sizes ((a), (b), (c), (d), (e) represents $5, 10, 15, 20$ and 25 network sizes).

See Fig. 36(b), As throughput measures in terms of cost. [44] selects two-disjoint paths i.e. $A-C-F-I-G-J$ which consumes 7 units of cost and $A-D-B-E-J$ which consumes 6 units of cost. So, the total amount of cost consumed by Resilient Multicast is 13 unit. In [45] (let node C, F, G discards the packet) so, it consumes 12 units of cost($A-C$, $A-D$, $D-F$, $D-B$, $B-G$, $B-E$, $E-J$) and send packets through $A-D-B-E-J$ path while BBR [49] takes 7 units of cost through $A-D-B-E-J$ path. Network congestion is measured in terms of packet transmission. Suppose source node A has 20 packets to transmit, [44] transmits 40 number of packets using $A-C-F-I-G-J$ and $A-D-B-E-J$ paths inside the network, [45] transmits 140 packets through $A-D-B-E-J$ path (assume node C, F, G discards the packet) while BBR [49] has only 4 packets to transmit through $A-D-B-E-J$ path .While resiliency is measured in terms of possible path exist after failure. In [44], if node D fails then packet will be forwarded through $A-C-F-I-G-J$. In [45] there exist 2 possible paths i.e. $A-C-H-F-I-G-J$ and $A-C-F-I-G-J$. In BBR, packets will be forwarded through $A-C-F-I-G-J$ (Explanation has

been described in 5 nodes of network). Table 12 shows the parameter growth of three approaches in a network of ten nodes.

Parameter Metric	Resilient Multicast	ROMER	BBR
Throughput	13	12	7
Network congestion	40	140	16
Resiliency	1	2	1

Table 12: Parameter growth of three approaches in a network of ten nodes

For network size 15 (see Fig. 36(c)) throughput of Resilient Multicast, ROMER and BBR is 15, 14 and 6, network congestion is 40, 180 and 20 and resilient paths are 1, 8, 1. For network size 20 (see Fig. 36(d)) throughput is 19, 16, 9, network congestion is 40, 200, 24 and resilient paths are 1, 5, 1. For network size 25 (see Fig. 36(e)) throughput is 20, 20, 7, network congestion is 40, 300, 28 and resilient paths are 1, 8, 1 as shown in table 8.

Parameter Metric	Approaches	5-node	10-node	15-node	20-node	25-node	100-node
Throughput (*in terms of cost*)	Resilient Multicast	8	13	15	19	20	89
	ROMER	7	12	14	16	20	76
	BBR	3	7	6	9	7	66
Network Congestion (*in terms of Packet transmission*)	Resilient Multicast	40	40	40	40	40	40
	ROMER	100	140	180	200	300	650
	BBR	8	16	20	24	28	88
Resiliency (*against node/link*	Resilient Multicast	1	1	1	1	1	1

failure)	ROMER	2	2	8	5	8	38
	BBR	1	1	1	1	1	1

Table 13: Network parameters comparison on three approaches ([14], [15], [16])

CHAPTER # 6

IMPLEMENTATION AND RESULTS

- *Implementation Platform*
- *Implementation Details*
- *Simulation*
- *Evaluation criteria*
- *Results*

CHAPTER 6

IMPLEMENTATION AND RESULTS

6.1 Implementation Platform

The Resilient Multicast [44], ROMER [45] and its improvements are implemented on Mat Lab.

Mat Lab is a high level language and interactive environment for numerical computation, visualization and programming.

6.2 Implementation Details

The simulation of all these approaches namely Resilient Multicast [44], ROMER [45] and BBR [49] use the same underlying structure that is described below.

There are two simple modules:

- Path Selection
- Packet Transmission

Since Mat Lab is a numerical based simulator, each module is coded in similar to c language.

6.3 Simulation

The simulation of all the three approaches namely Resilient Multicast [44], ROMER [45] and its improvement carried out in environment mentioned below. The simulation is carried out for 20,25,30,45 nodes with each node having certain links.

6.4 Performance Metrics

To evaluate the performance of network we have considered many of metrics like:

a) Throughput
b) End to End Delay
c) Packet Loss

Parameter	Value
simulator	Mat Lab
Protocols	BBR, ROMER
Number of Nodes	20,25,30,45
Simulation Type	200 sec
Traffic Type	CBR
Transmission Range	250m
Simulation Area	500*400
Interface Type	Queue
Packet Size	512 MB

Table 14: Simulation Parameters

a) Throughput: Throughput is defined as the time taken for a packet to travel form source node to destination node. Figure 43 shows the network throughput of BBR approach of one packet means we have a single packet to transmit from source node to destination node.

$$\textbf{Throughput}: \frac{\text{Total received packets in bytes}}{\text{Time Taken}}$$

b) End to End Delay: It is defined as the average time taken by a data packet to reach its destination. The end-to-end delay graph is shown in figure 48.

$$\textbf{End to End Delay}: \frac{\sum (\text{Received Time- Sent Time})}{\text{Total data packets received}}$$

c) Packet Loss: Packet loss is defined as the number of packets dropped to the number of packets originated by the source node due to traffic congestion.

$$\textbf{Packet Loss: } \frac{(\text{no. of SP- no. of RP})}{\text{no. of SP}}$$

no. of SP = number of Source Packets

no. of RP = number of Received Packets

d) Packet Loss Ratio (PLR): PLR is the ratio of number of packets dropped to the number of packets originated by the source node. The packet loss ratio graph is shown in figure 47.

$$\text{PLR} = \frac{(\text{no. of SP- no. of RP})}{\text{no. of SP}} * 100$$

Figure 44 shows network throughput comparison graph between RM, ROMER and BBR approach and figure 45 shows the network congestion comparison graphs of RM, ROMER and BBR (using table 13). The corresponding values of throughput, PLR and end-to-end delay is shown in table 15.

PROTOCOLS	MERTICS	20 NODE	30 NODE	45 NODE
	Throughput	455	315.0	227.5
ROMER	End to End Delay	0.4	0.65	0.9
	PLR	2.2%	3.4%	5%
	Throughput	585	341.3	273.06
BBR	End to End Delay	0.23	0.6	0.7
	PLR	0.7%	0.7%	1%

Table 15: BBR and ROMER Results

6.5 Snapshots and Results

We have simulated our algorithm by creating a 25 node network in MAT LAB with random cost and linking is provided on a distance basis. A node which is within 25 meter range of another node then there is direct linking otherwise the node has indirect linking. We have shown the snapshots of following:

1) Snapshot of 25- Node Network
2) Buffer Allocation to the Network
3) Packet Transmission
4) Resilience Implementation

1) Snapshot of 25- Node Network

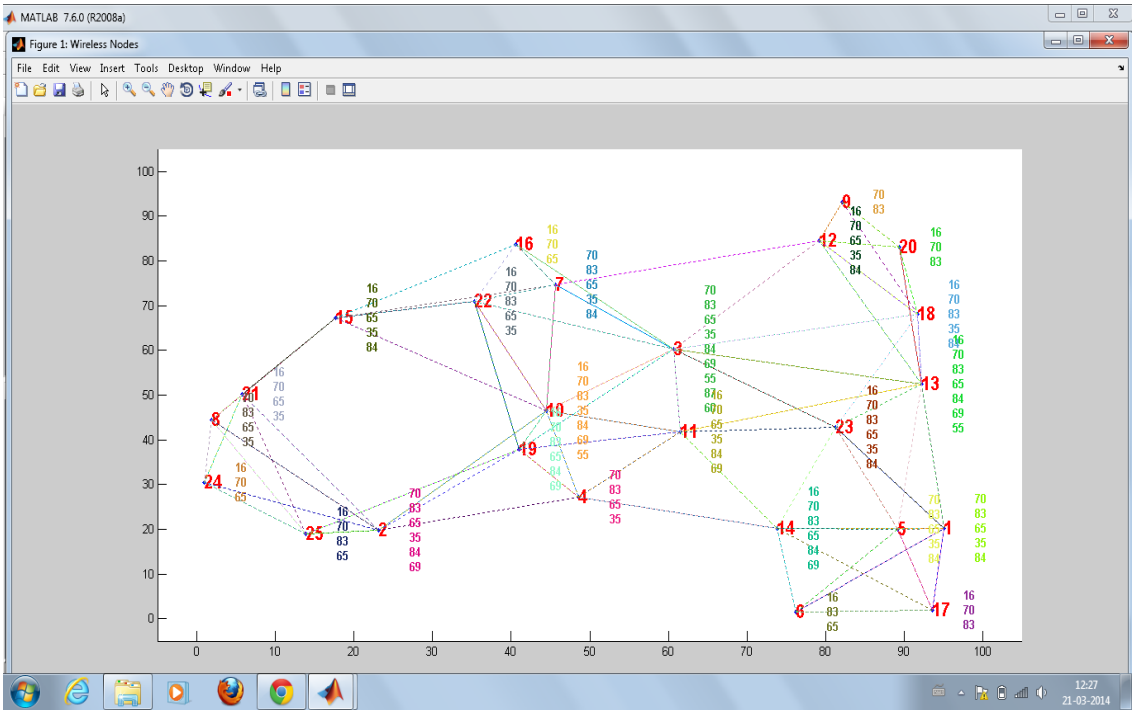


Figure 37: 25- Node Network

2) Buffer Allocation on 25-Node Network

To start buffer allocation process in the network firstly we have to select a source node and a destination node. In this example let us our Source node is 2 and Destination node is 25.

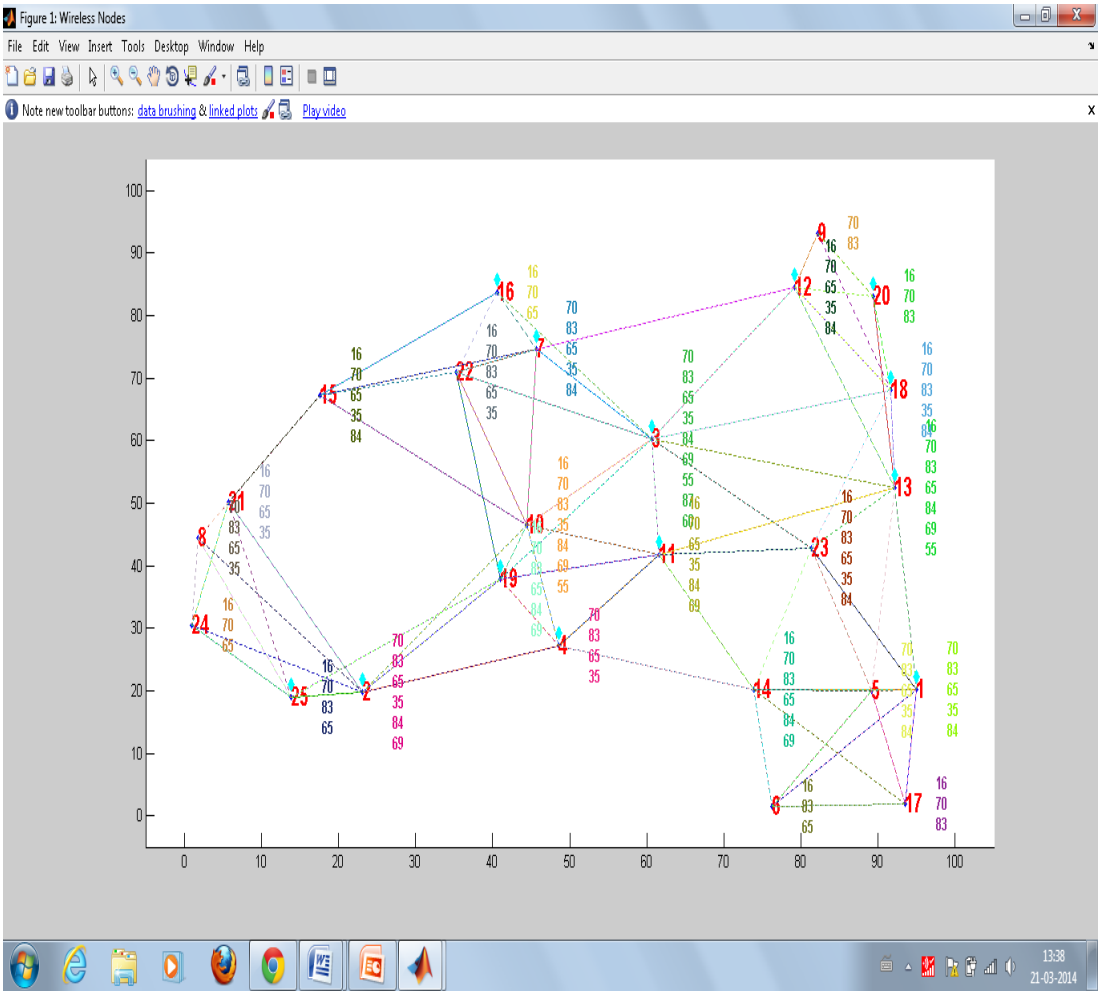


Figure 38: Buffer Allocation to the Network

3) Packet Transmission

Packet Transmission will start after allocating the buffers to the entire network. As shown in figure 39, let node 8 wants to send some data packets to destination node 25. Source node 8 will follow minimum buffered node path 8-2-21-25 and starts the packet transmission through this path.

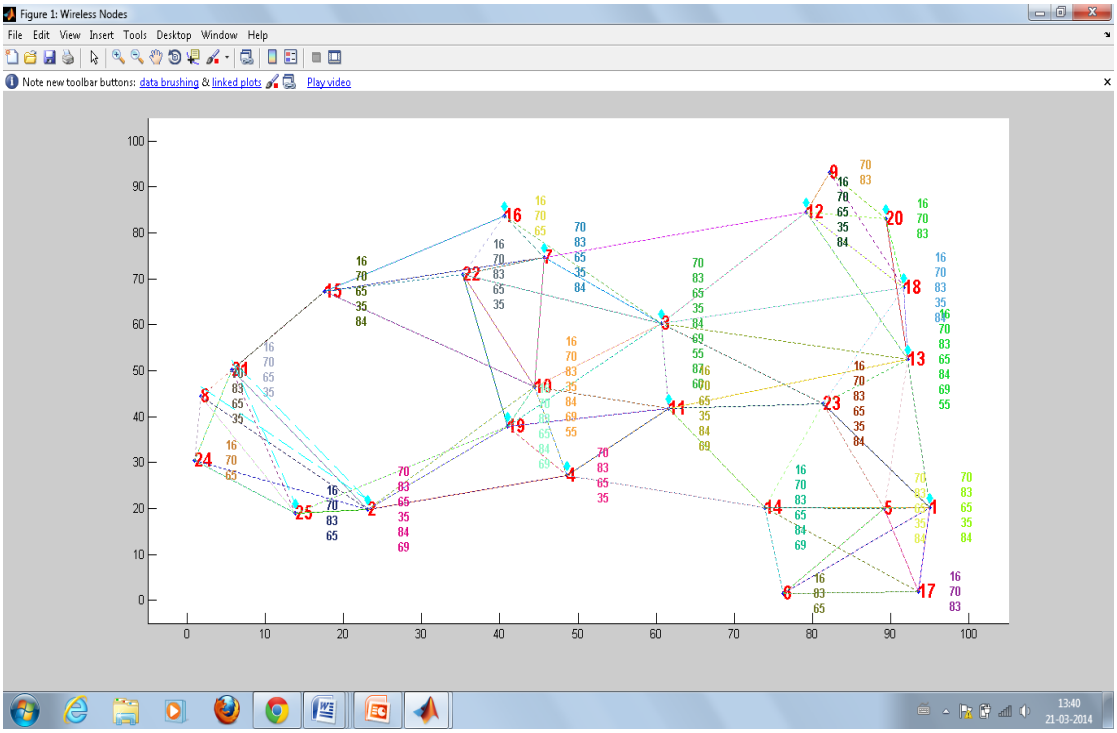


Figure 39: Packet Transmission

4) Resiliency Implementation

Let us understand how resiliency is implemented inside our network. let us consider two cases (without failure and with failure), when there is no failures inside network then path selection loop will terminate after finite number of steps as shown in figure 40.

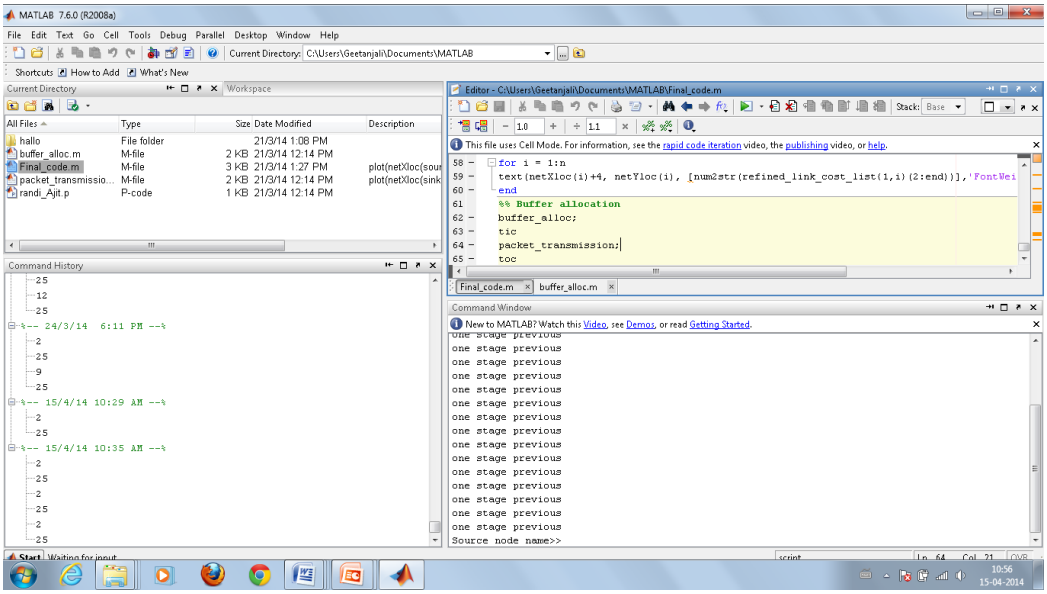


Figure 40: Successful Loop Ending

Another case is when failure exists inside network. After buffer allocation to the entire network let node 20 want to send some data packets to destination node 25 and in between this one of the node has been failed then source node 20 will node be able to find a path to destination node and will stuck into a loop as shown in figure 41.

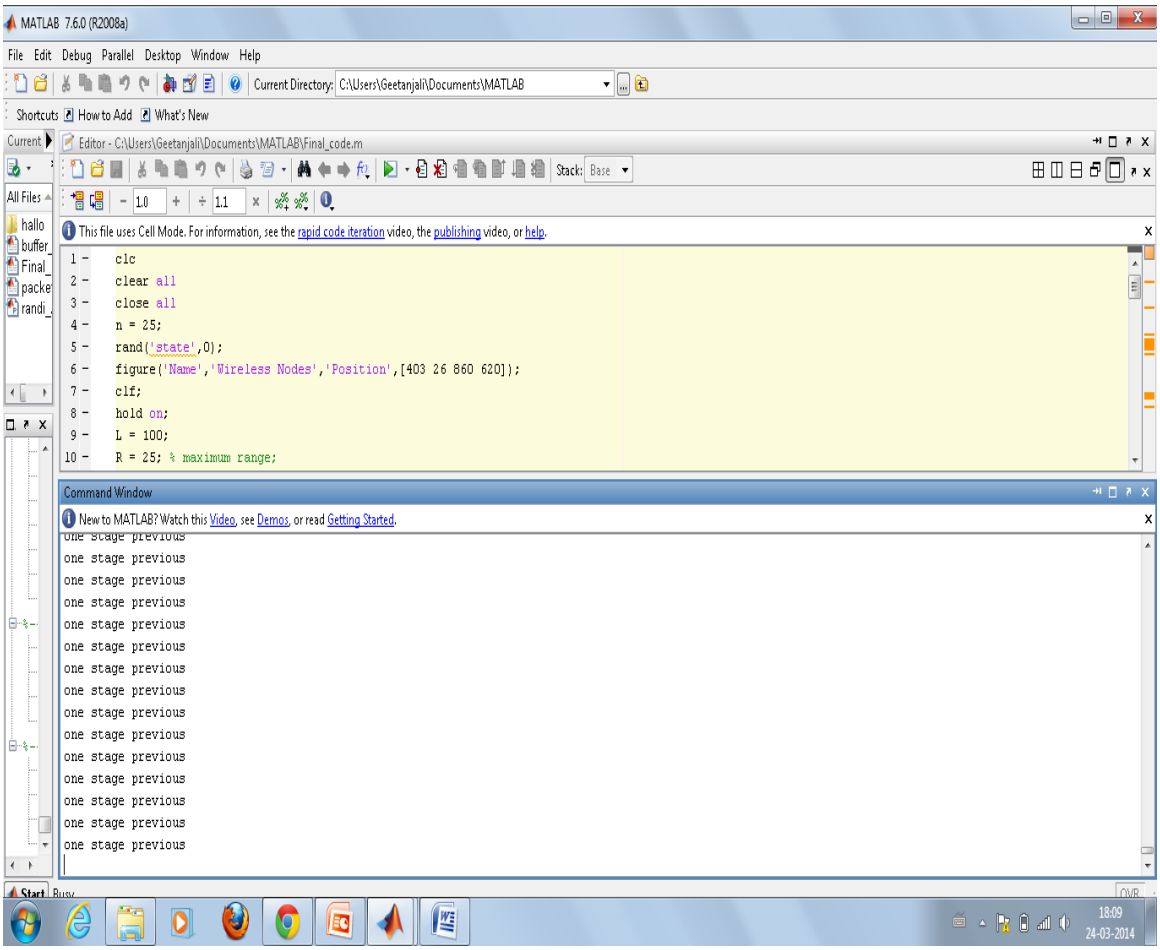


Figure 41: Failure Case

To implement Resiliency BBR approach immediately select previous buffered node i.e. node 12 and send the packet to destination node as shown in figure 42.

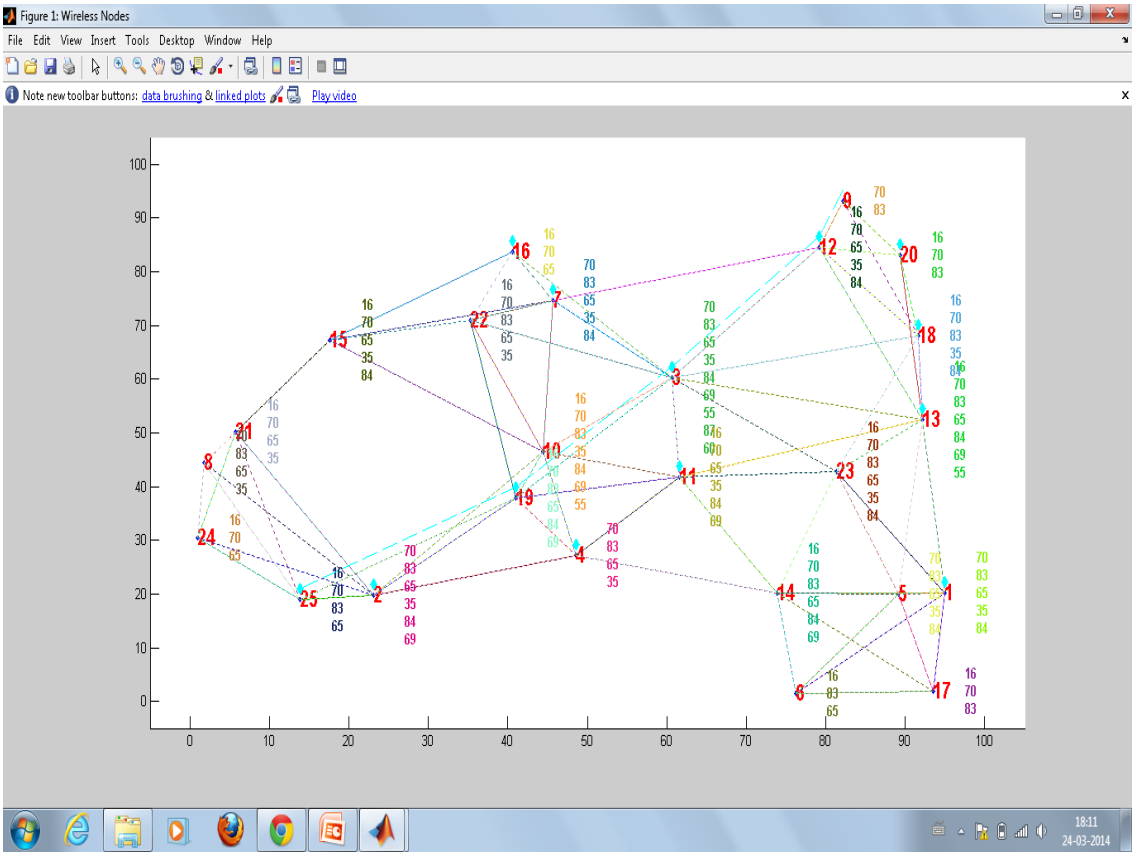


Figure 42: implementation of resiliency

The corresponding throughput, end to end delay and packet loss graphs of ROMER and BBR is shown in figure 43, 44, 45 and 46.Figure 43 shows the network throughput graph of BBR approach.

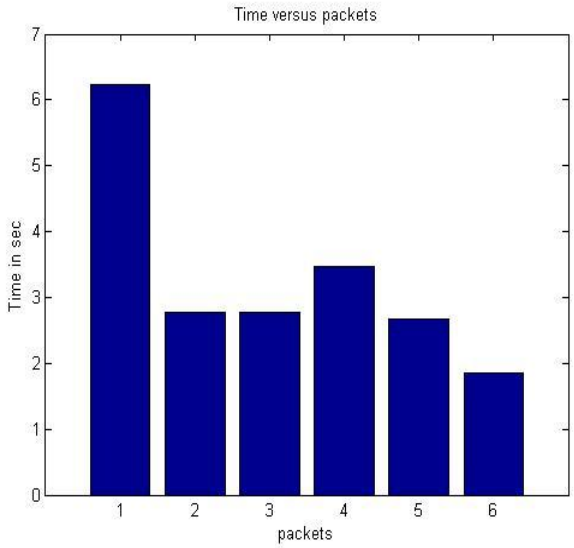


Figure 43: Network Throughput of BBR

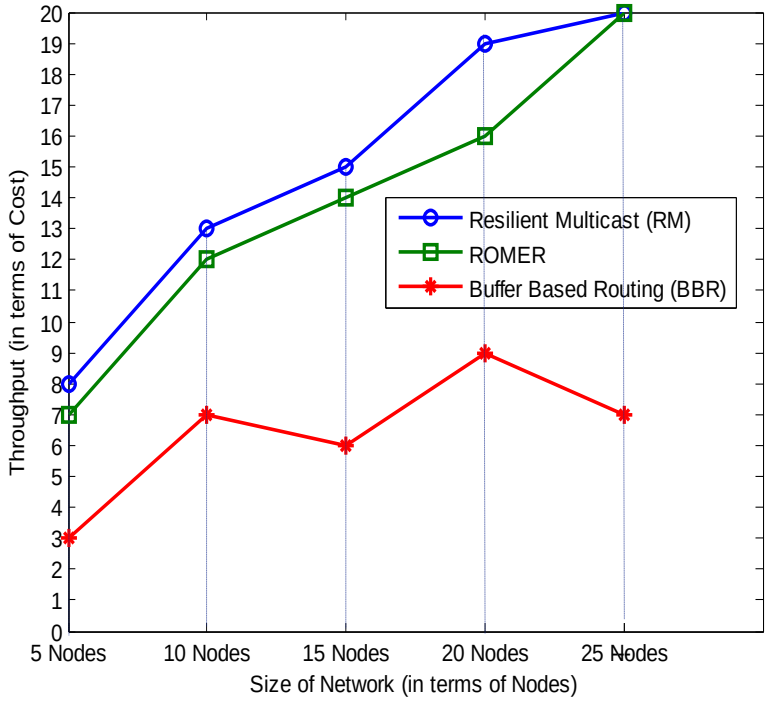


Figure 44: Network throughput of RM, ROMER, BBR

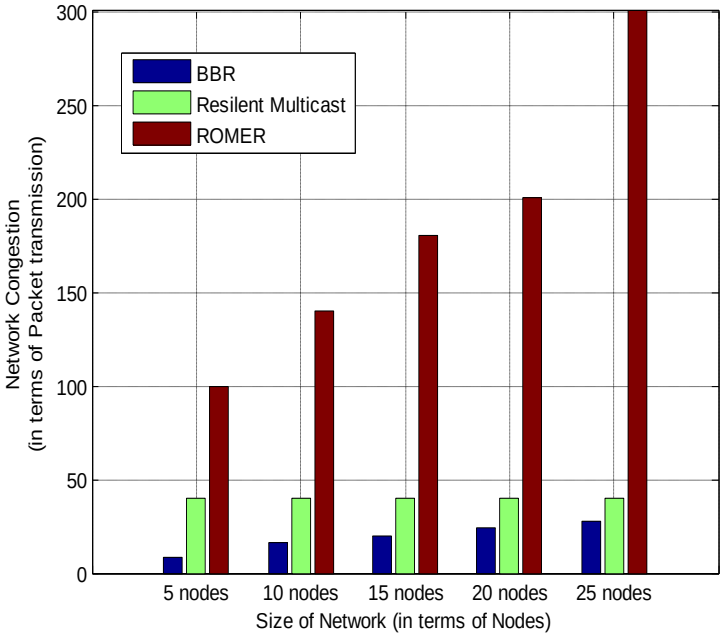


Figure 45: Network Congestion Graph

To provide more accurate results of proposed approach BBR we have evaluated network throughput, packet loss ratio and end to end delay on 20, 25, 30, 45 node networks and correspondingly obtain the results as shown in figure 46, 47, 48 (using table 15). Figure 49 shows the throughput results of resilience implementation in both RM and ROMER.

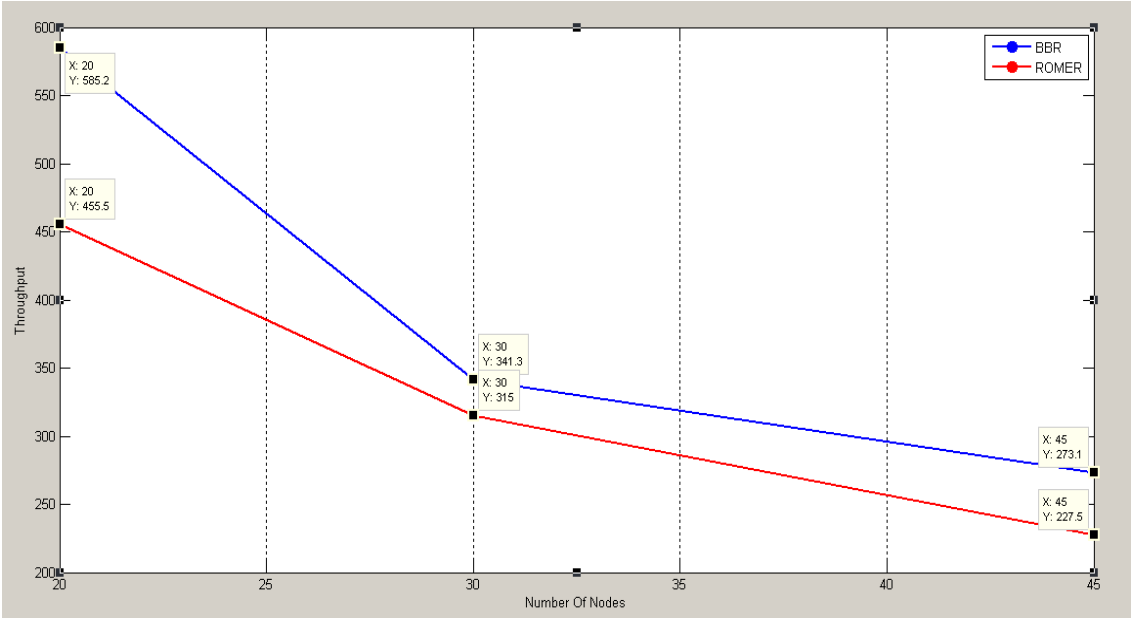


Figure 46 Throughput comparison of RM, ROMER

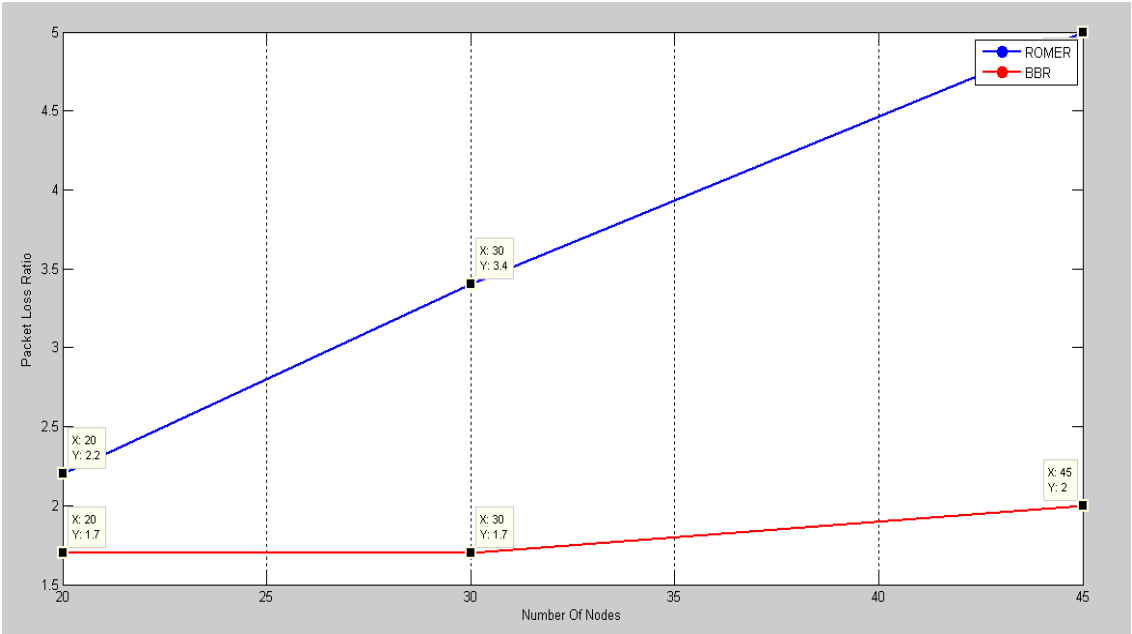


Figure 47: PLR of BBR, ROMER

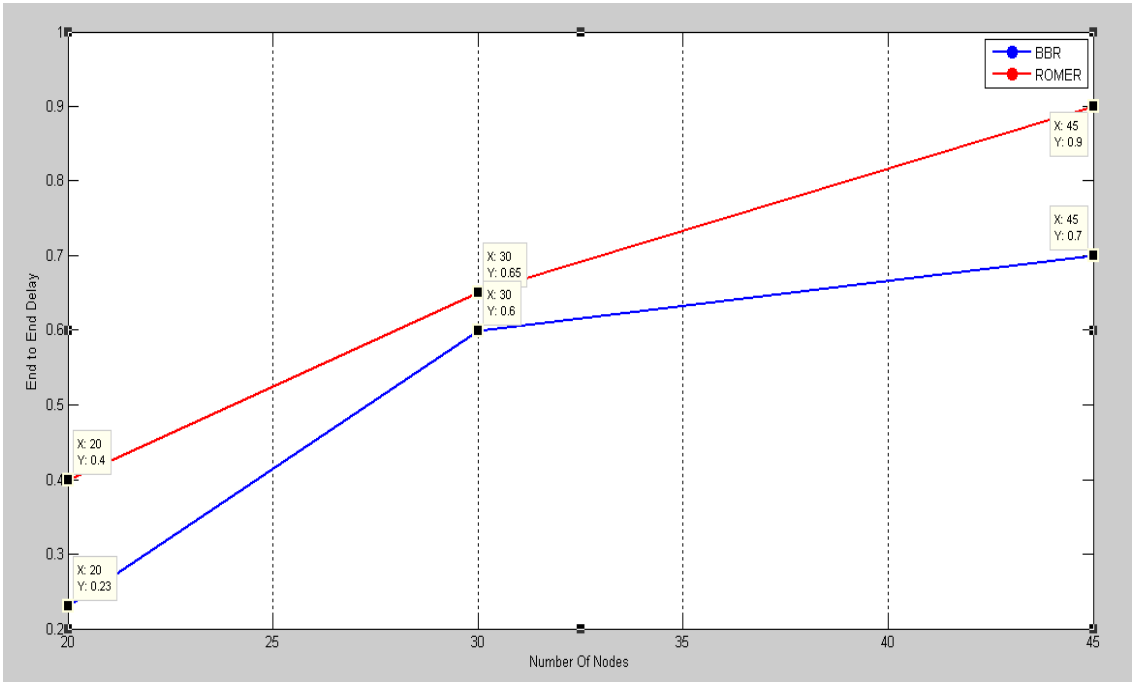


Figure 48: End-to-End Delay of BBR, ROMER

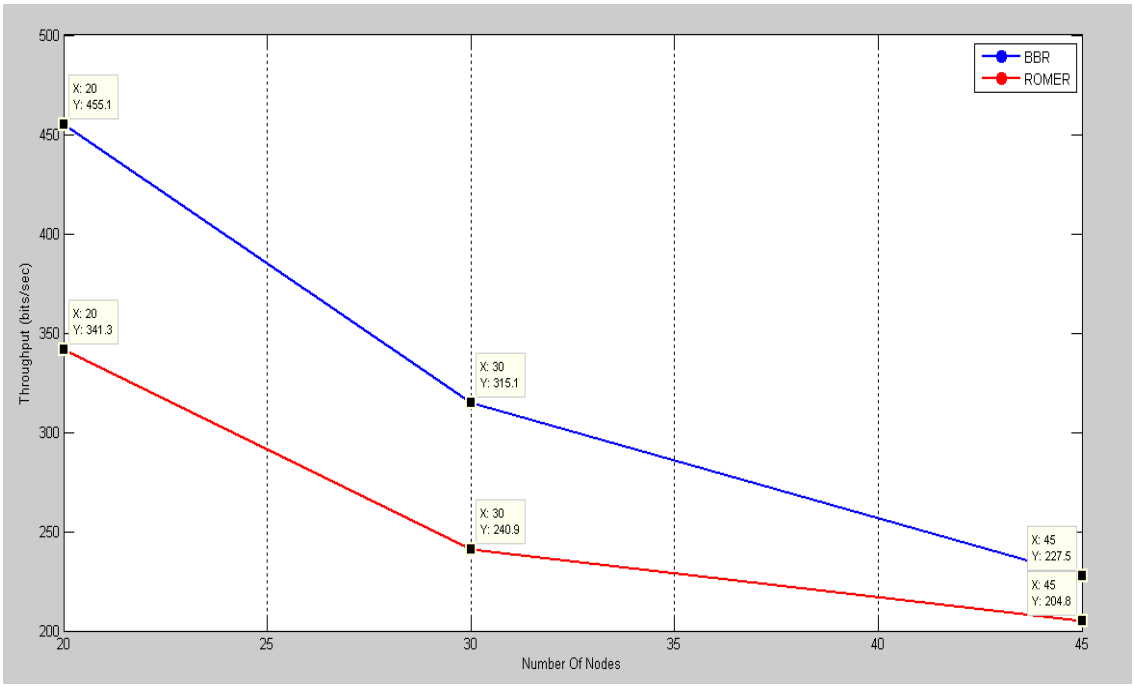


Figure 49: Throughput during Resilience

CHAPTER #7

CONCLUSION AND FUTURE WORK

CHAPTER 7

CONCLUSION AND FUTURE WORK

Conclusion

In this thesis we have proposed an approach to implement resiliency without affecting the network parameters. This approach basically deals with failure cases i.e. node/link failure. We have proposed RPT algorithm as an antidote during such failures. We have evaluated the time complexity of RPT approach as $O(Nlog_2(N)$. Further we have proved that performance of BBR is comparatively improved over previously proposed approaches i.e. Resilient Multicasting and ROMER using network throughput, resiliency against node/link failure, and network congestion as parameters for $5, 10, 15, 20, 25$ nodes network and show the simulation results of 20, 25,30 and 45 node networks.

Future Scope

In future to achieve more accurate results of BBR approach, we will apply it in physical environment and will study the results for any other possible measures.

REFERENCES

[1]. Kwon Ohbyung, and Yixing Wen, "An empirical study of the factors affecting social network service use," *Elsevier Journal of Computers in Human Behavior*, vol. 26, no. 2, 2010, pp. 254–263.

[2]. Hu Tao, Robin S. Poston, and William J. Kettinger, "Nonadopters of Online Social Network Services: Is It Easy to Have Fun Yet ?", *Journal of Communications of the Association for Information Systems*, vol. 29, no. 1, 2011, pp. 441–458.

[3]. Manoufali, Mohamed, et al, "*Technologies and networks supporting maritime wireless mesh communications*", *Proceedings of the IEEE 6th joint Conference on IFIP Wireless and Mobile Networking Conference (WMNC)*, Dubai, 2013, pp. 1–8.

[4]. Won-Suk, kim and Sang-Hwa Chung, "*Design of Optimized AODV Routing Protocol for Multi-Interface Multi-Channel Wireless Mesh Networks*", *Proceedings of the IEEE 27th International Conference on Advanced Information Networking and Applications (AINA),* Barcelona, 2013, pp. 325–332.

[5]. L. Song and Z. Bing Xia, "*An Anycast Routing Protocol for Wireless Mesh Access Network*", *Proceeding of the IEEE WASE International Conference on Information Engineering (ICIE)* , Taiyuan, Shanxi, vol. 2, 2009, pp. 82–85.

[6]. Gupta, Bhupendra Kumar, B. M. Acharya, and Manoj Kumar Mishra, "Optimization of routing algorithm in wireless mesh networks", *Proceedings of the IEEE World Congress on Nature & Biologically Inspired Computing (NaBIC)*, Coimbatore, 2009, pp. 1150–1155.

[7]. Jing Dong, Reza Curtmola, Cristina Nita-Rotaru, "Secure High-Throughput Multicast Routing in Wireless Mesh Networks", *Proceedings of the IEEE Transactions on Mobile Computing*, vol. 10, no. 5, 2011, pp. 653–668.

[8]. Helen Herrman, Donna E Stewart, Natalia Diaz-Granados, Elena L Berger, Beth Jackson, Tracy Yuen, "What is resilience?", *Canadian Journal of Psychiatry, Revue canadienne de psychiatrie*, vol.56, no.5, 2011, pp. 258–265.

[9]. Hossen Mustafa,Xin Zhang,Zhenhua Liu,Wenyuan Xu,Adrian Perrig, "Jamming-Resilient Multipath Routing", *Proceedings of the IEEE Transactionson on Dependable and Secure Computing* vol. 9, no. 6, 2012,pp. 852–864

[10]. Nitin Rakesh and Vipin Tyagi, "*Failure Recovery in XOR'ed Networks*", *Proceeding of the 2012 IEEE International Conference Signal Processing, Computing and Control (ISPCC)*, Waknaghat, India, 2012, pp. 1–6.

[11]. Nitin Rakesh, and Vipin Tyagi. "*Failure Detection using Contour Approach on Network Coded Parallel Networks*", *Proceeding of the International Conference on Modelling Optimization and Computing (ICMOC-2012), Elsevier Procedia Engineering*, Kanyakumari, India, vol. 38, 2012, pp. 763–770.

[12]. Seungjoon Lee, Bobby Bhattacharjee, Aravind Srinivasan, Samir Khuller. "*Efficient and Resilient Backbones for Multihop Wireless Networks*", *Proceeding of the* 2008 *IEEE Transactions on Mobile Computing*, vol.7, no.11, pp. 1349–1362.

[13]. Bu, Tian, Mun Choon Chan, and Ramachandran Ramjee, "Connectivity, performance, and resiliency of IP-based CDMA radio access networks", *Proceeding of the 2006 IEEE Transactions on Mobile Computing*, vol. 5, no. 8, pp. 1103–1118.

[14]. http://en.wikipedia.org/wiki/network_topology

[15]. Roy Winkelman, "an educator's guide to school networks", florida center for instructional Technology college of education, university of south florida 1997-2013, http://fcit.usf.edu/network/

[16]. http:// www.e-network.org/

[17]. Clark, David D., Kenneth T. Pogran, and David P. Reed. "An introduction to local area networks." *Proceedings of the IEEE* 66.11 (1978): 1497-1517.

[18]. https://www.google.co.in/?gws_rd=cr&ei=4U9RUS7KoOJrQfSzQE#q=network+image

[19]. https://smallbusiness.yahoo.com/advisor/why-computer-network

180000942.html

[20]. https://www.iup.edu/WorkArea/DownloadAsset.aspx?id=61283

[21]. Sichitiu, Mihail L. "Wireless mesh networks: opportunities and challenges."*Proceedings of World Wireless Congress*. Vol. 2. 2005.

[22]. https://www.iup.edu/WorkArea/DownloadAsset.aspx

[23]. Akyildiz, Ian F., Xudong Wang, and Weilin Wang. "Wireless mesh networks: a survey." *Computer networks* 47.4 (2005): 445-487.

[24]. http://www.securedgenetworks.com/secure-edge-networks-blog/bid/57702/3-Key-Benefits-of-Wireless-Mesh-Networks

[25]. Kyas, Othmar. *Network troubleshooting*. Palo Alto California: Agilent Technologies, 2001

[26]. Handbook, Military. "Reliability prediction of electronic equipment." *USA Department of Defense, MILHDBK-217F Notice* 2.10.1 (1991).

[27]. Bosworth, Seymour, and Michel E. Kabay, eds. *Computer security handbook*. John Wiley & Sons, 2002

[28]. Cherry, Steven M. "Internet slammed again [hacking]." *Spectrum, IEEE* 40.3 (2003): 59.

[29]. Walter, Chris J. "Identifying the cause of detected errors." *Fault-Tolerant Computing, 1990. FTCS-20. Digest of Papers., 20th International Symposium*. IEEE, 1990.

[30]. Luo, Chao, Hiroyuki Okamura, and Tadashi Dohi. "Characteristic analysis of quantitative definition of resiliency measure." *Software Reliability Engineering Workshops (ISSREW), 2013 IEEE International Symposium on*. IEEE, 2013.

[31]. http://20ebooks.com/read-online/tintroductiont-ef33808057d

[32]. Schaeffer-Filho, Alberto, et al. "A framework for the design and evaluation of network resilience management." *Network Operations and Management Symposium (NOMS), 2012 IEEE*. IEEE, 2012.

[33]. J. P.G. Sterbenz, D. Hutchison, E. K. Cetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines,” Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET), vol. 54, no. 8, pp. 1243–1342, June 2010.

[34]. Trivedi, Kishor S., Dong Seong Kim, and Rahul Ghosh. "Resilience in computer systems and networks." Proceedings of the 2009 International Conference on Computer-Aided Design. ACM, 2009.

[35]. Jaggi, Sidharth, et al. "Resilient network coding in the presence of byzantine adversaries." INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE. IEEE, 2007.

[36]. Schaeffer-Filho, Alberto, et al. "A framework for the design and evaluation of network resilience management." Network Operations and Management Symposium (NOMS), 2012 IEEE. IEEE, 2012.

[37]. Yu, Yue, et al. "An adaptive approach to network resilience: Evolving challenge detection and mitigation." Design of Reliable Communication Networks (DRCN), 2011 8th International Workshop on the. IEEE, 2011.

[38]. Fick, David, et al. "A highly resilient routing algorithm for fault-tolerant NoCs."Proceedings of the Conference on Design, Automation and Test in Europe. European Design and Automation Association, 2009.

[39]. Lee, Sanghwan, et al. "Proactive vs reactive approaches to failure resilient routing." INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. Vol. 1. IEEE, 2004.

[40]. Rao, S. Siva Nageswara, Y K Sundara Krishna, and K. Nageswara Rao. "A Survey: Routing Protocols for Wireless Mesh Networks." International Journal of Research and Reviews in Wireless Sensor Networks (IJRRWSN) 1.3 (2011).

[41]. Rakesh, Nitin, and Vipin Tyagi. "Failure recovery in XOR'ed networks." Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on. IEEE, 2012.

[42]. Gupta, Bhagvan Krishna, Ankit Mundra, and Nitin Rakesh. "Failure Detection and Recovery in Hierarchical Network Using FTN Approach." (2013).

[43]. Rakesh, Nitin, and Vipin Tyagi. "Failure Detection using Contour Approach on Network Coded Parallel Networks." Procedia Engineering 38 (2012): 763-770.

[44]. Zhao, Xin, et al. "Resilient multicasting in wireless mesh networks." Proc. 13th International Conference on Telecommunications. 2006.

[45]. Yuan, Yuan, et al. "ROMER: resilient opportunistic mesh routing for wireless mesh networks." IEEE Workshop on Wireless Mesh Networks (WiMesh). Vol. 12. 2005

[46]. D. Hutchison, J. Sterbenz, Resilinets architecture definitions,Available at: http://wiki.ittc.ku.edu/resilinets wiki/index.php/Definitions.

[47]. Resilience: http://en.wikipedia.org/wiki/Resilience

[48]. P. A. Dearnley, An Investigation Into Database Resilience.*Comput. J.*, 19(2), pp. 117-121, 1976.

[49]. Geetanjali Rathee, Ankit Mundra, Nitin Rakesh, S. P. Ghrera "*Buffered Based Routing Approach for WMN*", *Procceding in IEEE International Conference of Human Computer Interaction*, Chennai, India, 2013 *(accepted in press)*.

[50]. **Geetanjali Rathee**, Nitin Rakesh, " Resilient Packet Transmission for Buffer Base Routing Protocol", accepted in Journal of Information Processing and System (JIPS) (in press), Korea.

Authors Publications

1 **Geetanjali Rathee**, Ankit Mundra, Nitin Rakesh, "Buffered Based Routing and Resiliency Approach for WMN" accepted in IEEE International Conference on Human Computer Interactions – ICHCI-2013 *(in press)*, Chennai, India.

[Indexed: Scopus, DBLP, ISI (Thomas Reuters)

1 **Geetanjali Rathee**, Nitin Rakesh, " Resilient Packet Transmission for Buffer Base Routing Protocol", accepted in Journal of Information Processing and System (JIPS) (in press), Korea.

[Indexed: Scopus, DBLP]