IMPROVEMENT OF QUALITY OF SERVICES (QoS) IN INTERNET OF THINGS (IoT)

THESIS

submitted in fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Faculty of Informatics and Computing

by

Gyanendra Kumar
(Regn. No.: YMCAUST/PH04/2K16)

Under the Supervision of

Dr. Parul Tomar

Department of Computer Engineering
J.C. Bose University of Science and Technology,YMCA,
Faridabad-121006, (Haryana), INDIA

December 2022

DECLARATION

I hereby declare that the work presented in the thesis entitled **"IMPROVEMENT OF QUALITY OF SERVICES (QoS) IN INTERNET OF THINGS (IoT)"** by **GYANENDRA KUMAR,** being submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy in the Department of Computer Engineering under Faculty of Informatics and Computing of J.C. Bose University of Science and Technology YMCA, Faridabad, during the academic year 2022-2023, is a bonafide record of my original work carried out under the guidance and supervision of **Dr. PARUL TOMAR, ASSOCIATE PROFESSOR, DEPARTMENT OF COMPUTER ENGINEERING,** and has not been presented elsewhere.

I further declare that the thesis does not contain any part of any work which has been submitted for the award of any degree either in this university or in any other university.

(GYANENDRA KUMAR)
Registration No. YMCAUST/PH04/2K16

CERTIFICATE

This is to certify that this thesis entitled **"IMPROVEMENT OF QUALITY OF SERVICES (QoS) IN INTERNET OF THINGS (IoT)"** by **GYANENDRA KUMAR**, submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy in Department of Computer Engineering under Faculty of Informatics and Computing of J.C. Bose University of Science and Technology, YMCA, Faridabad, during the academic year 2022-2023, is a bonafide record of work carried out under my guidance and supervision.

I further declare that to the best of my knowledge, the thesis does not contain any part of any work which has been submitted for the award of any degree either in this university or in any other university.

Dr. Parul Tomar
Associate Professor
Department of Computer Engineering
Faculty of Engineering and Technology
J.C. Bose University of Science and Technology,
YMCA, Faridabad

Dated:

ACKNOWLEDGMENT

First and foremost, I express my sincere gratitude to my supervisor Dr Parul Tomar, Associate Professor, Department of Computer Engineering, J.C. Bose University of Science and Technology, YMCA, Faridabad, for her mentoring and guidance during this research work. Her profound knowledge, generous guidance, timely advice, insightful criticisms and encouragement made it possible for me to carry out the research work successfully.

I would like to extend my heartful thanks to Prof. C.K. Nagpal, Dean faculty of Informatics and Computing for his motivation. I would like to concede my special thanks to Prof. Atul Mishra, Chairman, Department of Computer Engineering, J.C. Bose University of Science and Technology, YMCA, for his constant support and encouragement over the period of my research work. I sincerely thank Prof. Komal Bhatia, Prof. Manjeet Tomar, Dr Neelam Duhan, and Dr Sapana Gambhir for their critical comments and valuable suggestions rendered throughout my research work.

I would like to thank from the bottom of my heart to my friend Dr Lal Pratap Verma and Mr Anubhav Kumar for helping me to understand the concept of research, publications and other technicalities. It's fortunate to acknowledge the support of my friends, Mr Sur Singh Rawat, Mr Mahesh Singh and Ms Pragya, for their motivation and generous care in all ups and downs throughout the research tenure.

I am immensely indebted to my parents, Sh. Jagadeesh Prasad and Smt. Pushpa Maurya, for their motivation and persistent belief in me, towing me out from the stress. I would also like to thank, Mr Narendra Kumar, Mr Bhupendra Kumar and Mr Shailesh Maurya, for their tremendous understanding and continuous support. I convey my gratitude and love to my dear wife, Shalini Maurya, for inspiring me and being the best critic. Above all, I would like to express my love to my son and daughter, Aarav Maurya and Anvesha Maurya, who, at such a tender age, understand me and give me strength by saying, "Papa, Go-ahead". I also thank to all my well-wishers who helped me directly or indirectly during this research work.

(Gyanendra Kumar)
Registration No. YMCAUST/PH04/2K16

ABSTRACT

With time and demand, technology will undoubtedly advance. This idea may be applied to current communication networks as well. As a result, network technology is evolving in new directions, such as the Internet of Things (IoT), M2M communication, and so on. When it comes to the IoT, its diversity and complexity increase because, to fulfil its defined vision of ”Things Will Be Alive and Intelligent,” various types of technology have to be improved or developed to provide a common interaction platform for heterogeneous devices. As in the IoT environment, network and device resources may be limited, so offering satisfactory quality of services (QoS) is inevitable and challenging. The QoS of any network is improved by optimizing an existing system or developing a new one by increasing the metrics that measure its performance, such as throughput, latency, energy consumption, message overhead, etc. From the literature study, it is found that to provide desired IoT infrastructure, there exist numerous technical challenges apart from social and economic. In this thesis, two key technical challenges: deployment of IPv6 and optimal utilization of resources, are studied in detail.

In IPv6 protocol suit, much of the functionalities are inherited from the legacy IPv4 with added stateless addressing capability, which makes it suitable in the resource-constrained network environment. But it requires an efficient self-address generation scheme and duplicate address detection (DAD) protocol to achieve optimal performance. In this thesis, a survey of IPv6 addressing strategy in an IoT environment is performed and identified that existing schemes suffer from high duplicate address generation, high energy consumption, and adds high message overhead during DAD. It is also found that existing DAD solutions suffer from denial of services (DoS) attacks in the presence of malicious nodes in the network. This thesis proposed a stateless spatiotemporal IPv6 addressing scheme and a secured duplicate address detection protocol to address these issues. Extensive experimental evaluation is performed, and observed results show that the proposed work minimises duplicate address generation, energy consumption, and overhead.

Many multi-homing devices in modern networks are now equipped with multiple network interfaces to provide seamless connectivity. Advances in transport layer protocols for multi-path transmission of multi-house devices are essential to maximizing the exploitation of multiple network interfaces. Hence, this thesis presents a literature review of different challenges and solutions of multipath communication along with the recent development in CMT and MPTCP transport layer protocol. According to the literature review, CMT still has several significant issues, including spurious retransmission, receiver buffer blocking (RBB), congestion window (cwnd) expansion, re-ordering, and long round trip time (RTT), all of which result in poor performance. To mitigate these issues, this thesis presents a path rank-based CMT (R-CMT), which calculates the rank of each path according to its successful transmission capability and accordingly schedules data chunks. Experimental results indicate that R-CMT scheduling achieves better network latency, throughput, and cwnd growth. Apart from these key contributions, this thesis also presents a new paging technique to maximize the utilization of cache memory of devices and a cost-effective, efficient, and accurate mine monitoring system, SENSEnuts IoT platform and Bayes decision theorem-based mine control system.

The significance of this thesis study is that it performs a literature survey to understand the different technological advancements and challenges in the IoT environment. This thesis further proposed different solutions and experimentally validated that the work done in the thesis improves the QoS metrics such as throughput, energy consumption, latency, and communication overhead.

TABLE OF CONTENTS

List of Tables

List of Figures

LIST OF ABBREVIATIONS

6LoWPAN	IPv6 over low- power wireless personal area network
A-CMT	Adaptive data packet scheduling for CMT
ADC	Analog to digital converter
AMQP	Advanced Message Queuing Protocol
AOPS	Adaptive ordering predicting scheduling
AQI	Air quality index
ASR	Address success rate
BALIA	Balanced link adaptation
BS	Base station
CMT	Concurrent multipath transmission
CMT-CA	Content-aware CMT
CMT-DA	Distortion-aware CMT
CMT-LA	Loss-Aware CMT
CMT-NC	Network coding based CMT
CMT-QA	Quality-aware adaptive CMT
CoAP	Constrained Application Protocol
CUMACK	Cumulative acknowledgement
CWND	Congestion window growth
DAC	Delayed acknowledgment
DAD	Duplicate address detection
DDS	Data Distribution Service
DHCP	Dynamic host configuration protocol
DoS	Denial of service
DSIPA	Distributed Spatial IP Address Assignment
EPOC	Energy and Goodput Optimized CMT
EXI	Efficient XML Interchange
FDIPA	Four dimensional IP addressing

FDPS	Forward delay-based packet scheduling
FEC	Forward Error Correction
FIFO	First in first out
FMTCP	Fountain code-based Multipath TCP
GND	Ground
GPS	Global positioning system
GRP	Global routing prefix
HOL	Head of Line
HTML	Hyper Text Mark-up Language
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IID	Interface identifiers
IoT	Internet of things
IP	Internet protocol
IPCC-SCTP	Path Congestion Control SCTP
ITS	Intelligent transport system
LDF	Longest distance first
LIA	Linked increases algorithm
LRU	Least recently used
LS-SCTP	Load Sharing SCTP
LTE	Long term evolution
M2M	Machine to machine
MAC	Media access control
MPIPA	Multi-Projection IP address Assignment
MPTCP	Multipath transmission control protocol
MQTT	Message Queue Telemetry Transport
NA	Neighbour advertisement
NDP	Neighbour Discovery Protocol
NR-SACK	Non-renegable selective acknowledgment
NS	Neighbour solicitation

OCPS	Offset compensation-based packet scheduling
OLIA	Opportunistic linked algorithm
PF	Potentially-Failed
PR-SCTP	Partially Reliable SCTP
PSN	Path sequence number
QoS	Quality of Service
RA	Router advertisement
RBB	Receiver buffer blocking
R-CMT	Rank based concurrent multipath transmission
RFC	Request for comment
RFID	Radio frequency identification
RTT	Round trip time
SACK	Selective acknowledgement
SBD	Shared bottleneck detection
SCTP	Stream Control Transmission Protocol
SFR	Split Fast Retransmit
SIPA	Spatial IP Address Assignment
SLAAC	Stateless auto configuration
SLIPA	Scan-line IP Assignment
SLIPA-Q	Scan-line IP Assignment with equal Quantity
SRMT	Selective-Redundancy Multipath Transfer
ssthresh	Slow Start Threshold
SYN	Synchronize
TCP	Transmission Control Protocol
UART	Universal asynchronous receiver transmitter
UDP	User datagram protocol
UM	Underground mines
WIFI	Wireless fidelity
W-SCTP	Westwood SCTP
WSN	Wireless sensor networks

XML	eXtensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Chapter I

INTRODUCTION

1.1 INTRODUCTION

The Internet of things (IoT) is a network of billions of self-communication devices connected to the Internet. The devices in this network are equipped with the necessary hardware and software that have the ability to process and transfer data with each other. These devices can be deployed in applications such as supply chain, logistics, smart environment, agriculture, social life, entertainment, health, and fitness, producing a huge amount of data to service applications' needs. To fulfil modern needs, the number of Internet-connected devices is exploding day by day. It was more than 8.7 billion in 2012 [1], increased up to 31 billion by 2020 [2], and is expected to be 125 billion by 2030 [3]. According to the claim made by manufacturers, over one trillion microchips will be manufactured for IoT devices by 2040. These sensing and actuating devices connect via the Internet using technologies such as fixed Ethernet, cellular, Wi-Fi, Bluetooth, ZigBee, 802.15.4, Lora and PLC etc. In IoT terminology, devices are called nodes, which can be resourceful or constrained [4]. As per the requirements of IoT, end nodes should be dynamic, self-adapting, self-configuring, and with a unique identity. They must support interoperable communication protocols so that the data produced by the node can be integrated into the information network to service IoT applications.

1.2 IoT TERMINOLOGY AND RELATED WORK

In literature, there exists a large number of definitions for IoT. This section presents key definitions which are commonly accepted across the research community.

According to RFID group, IoT can be defined as, *"The global network of* *interconnected things uniquely addressable depend on defined communication protocols"*.

Sundmaeker et al. [5] define IoT as, *"Objects' are active participants in information, social and business processes where objects are enabled to interact and exchange information among themselves and with the environment by communicating data and information sensed about the surrounding environment, while reacting independently to the physical events and affecting it by running processes that cause actions and create services with or without human involvement"*.

Gubbi et al. [6] present a user-centric definition of IoT as, *"Interconnection of actuating and sensing devices as long as the ability to exchange information across different platforms through a combined framework, developing a general operating image for enabling innovative applications. This is accomplished by seamless, ubiquitous sensing, information representation and data analytics with Cloud computing as the framework"*.

Kumar et al. [7] defines IoT by considering the future development of technology and things as,*"IoT is a network of uniquely identified things that are connected to the Internet. These things can be living, dead, subs, nano things or unknown things. It may have the ability to process, transmit and store data in any known or unknown form such as electrical, magnetic, optical and chemical"*.

1.2.1 IoT Architecture

Different architectures are available in the literature based on different aspects of requirements. These aspects of requirement can be on the basis of various web services of the network [8], on the basis of modern Internet network structure [9], on the consideration of security aspects of the network [10], and many more. Figure 1.1 presents a general architecture with basic building blocks. Different components of the architecture are as follows:

Node: Nodes are things in IoT, which are connected to Intranet/Internet, gateway, router, and communication media, via IoT local area network or wide area network as shown in Figure 1.1. Based on the various characteristics, IoT nodes can be divided into various classes, such as relay nodes, sensors/actuators, powering devices, and connecting devices.

IoT LAN: It is a network of IoT nodes within the control of a single entity or administrator. IoT LAN uses short-range connecting devices to connect different nodes and can be configured by using different network technologies

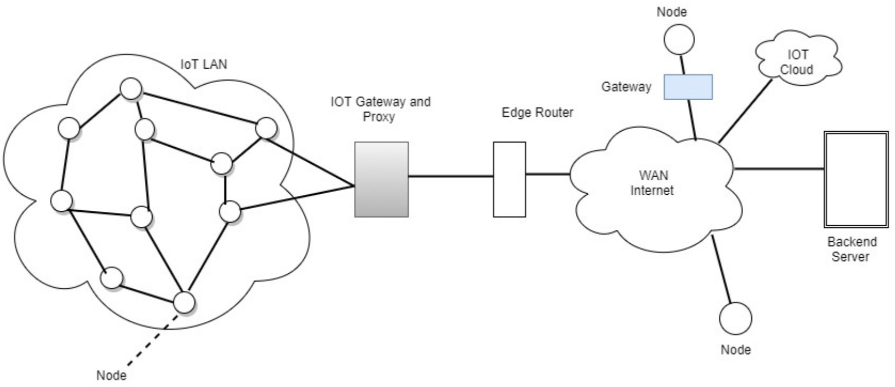


Figure 1.1: General Architecture of IoT

and topologies. IoT LAN may be connected to the internet through an IoT gateway or IoT proxy to provide global connectivity to IoT nodes. Nodes in IoT LAN can be connected via electric, radio wave, sound wave, magnetic wave, optical signals, chemical signals and so on.

IoT WAN/Internet: IoT LAN or node may be directly connected to the internet or WANs, which are further connected to the Internet and usually managed by different administrators and sub-network. IoT WAN/Internet cover a very large geographical area.

IoT Gateway and Proxy: IoT gateway is a device which connects the IoT node and LAN with the Internet. It is an interface between the Internet and an IoT node or LAN. It is a network layer device which transfers IP packets between the Internet and IoT LAN. IoT proxy performs application layer functions between different entities and IoT nodes. Sometimes IoT proxy can be connected directly with an IoT gateway to minimize complexity overhead.

Communication Media: The main function of communication media is to transfer information in the form of signals from one node to another node or network. Signals, like electrical, radio, magnetic, sound, chemical, etc., may be in any form. This can be done in the modern network through wired and wireless media.

Edge Router: Edge router is used to transform the IP address from one form to another, like IPv4 to IPv6, and forward received data packets to the destination.

1.2.2 Layered Protocol Stack

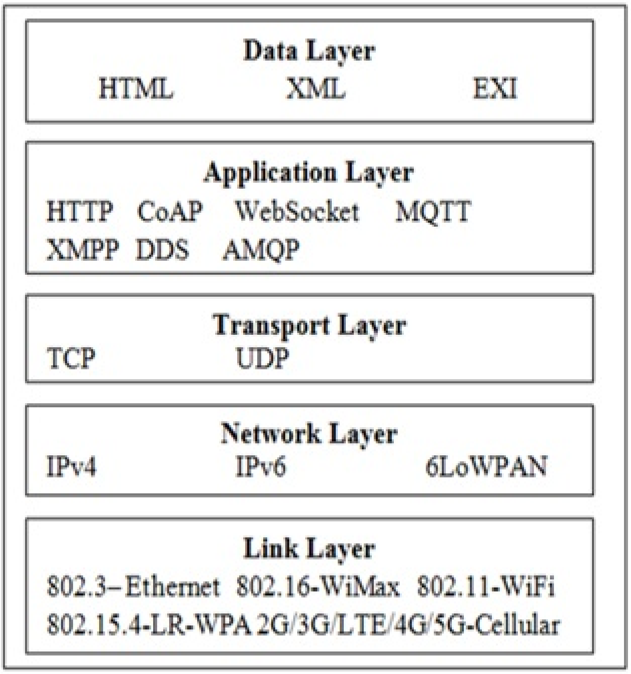
IoT has many requirements, such as a large number of heterogeneous devices, which can be deployed in resource constraints environments, and nodes need to provide reliable services. They should be able to communicate via the Internet.

To fulfil these requirements, a general protocol stack for IoT devices Figure 1.2 is provided, which has five distinct functional layers, named (i) Data, (ii) Application, (iii) Transport, (iv) Network, and (v) Link Layer.

Data Layer: The primary requirement of nodes in the Internet of Things is data exchange, which is accomplished by encoding transferred contents in semantic representation languages such as eXtensible Markup Language (XML), Hyper Text Mark-up Language (HTML) for unconstrained nodes, and Efficient XML Interchange (EXI) for constrained nodes.

Application Layer: This layer provides an application interface with a transport layer to transfer data to the Internet. The HTTP protocol is commonly used to encode application layer data but is inappropriate in a constrained environment. Constrained Application Protocol (CoAP) is suitable in constrained environments to transfer data and uses lightweight UDP rather than TCP. Other application layer protocols like WebSocket, Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), Data Distribution Service (DDS), and Advanced Message Queuing Protocol (AMQP) are also available. Still, these protocols are specific for a particular type of application.

Transport Layer: The primary function of the transport layer is to offer end-to-end data delivery without considering the network. Transmission Control Protocol (TCP), Stream Control Transmission Protocol (SCTP), and



Data Layer
HTML XML EXI

Application Layer
HTTP CoAP WebSocket MQTT
XMPP DDS AMQP

Transport Layer
TCP UDP

Network Layer
IPv4 IPv6 6LoWPAN

Link Layer
802.3–Ethernet 802.16-WiMax 802.11-WiFi
802.15.4-LR-WPA 2G/3G/LTE/4G/5G-Cellular

Figure 1.2: IoT Protocol Stack

UDP are used to deliver data from one end to the other.

Network Layer: The network layer is responsible for delivering the data from the source node to the destination node. The addressing and routing protocols and other supporting protocols route the data from source to destination. Initially, IPv4 was used to address devices, but due to limitations, IANA has already announced the exhaustion of IPv4 addresses. As per the study, trillions of IoT devices are expected and will require a unique address. To solve the problems of IPv4, IPv6 standards have been proposed, which can address almost all objects available on the planet. IPv6 address is represented using 128 bits. Thus, it can assign a unique address to billions of IoT nodes.

Link Layer: The link layer is responsible for sending data over the network's physical medium. Protocols of link layer in IoT environment can be 802.3 Ethernet, 802.11 WiFi, 802.16- WiMax, 802.15.4 low rate wireless personal area network (LR-WPANs), and 2G/3G/LTE/4G/5G cellular connection etc.

1.2.3 Applications of IoT

With the advancement of IoT technologies, a large number of IoT-based applications are being developed, which are making our lives comfortable. These applications can be inculcated in our daily routines in many ways, such as healthcare, smart city, personal and social, smart homes, intelligent transport systems (ITS), and smart environment. The functioning environment of these applications must be equipped with smart devices and objects that have the self-communicating ability with each other. IoT applications should be capable of sensing the surrounding environment and location, sharing, remote controlling, ad hoc networking, and secure communication [11]. Some key application domains with required capabilities and related applications are summarized in Table 1.1.

1.2.4 IPv6 Addressing

In IoT networks, massive scaling of end nodes can be supported by deploying IPv6 addressing protocol suit as IPv4 has less space and functionality. In the resource constraint IoT network, each end node should have self-configuration capability and a unique identity, which can be provided by IPv6. The unique identity of end nodes is primarily maintained by employing the stateless auto-configuration (SLAAC) method. In SLAAC, each node generates its identity by itself, and this newly generated unique identity can be verified by using the duplicate address detection (DAD) protocol. The procedure used for assigning unique addresses through IPv6 addressing scheme is as follows:

Table 1.1: Key IoT application domains, capabilities, and deployment

Application Domain	**Sub Categories**	**Capabilities**	**Scenarios of Application**
Healthcare	Monitoring	Location sensing and sharing	Tracking, Identification
	Home Care	Environment sensing	Authentication, Sensing
	Fitness	Ad hoc networking	Smart diagnostic, Assistance
		Secure communication	Smart hospital services
Smart City	Waste Management	Location sensing and sharing	Logistic, Safety
	Traffic Congestion	Environment sensing	Augmented maps
	Noise Monitoring	Remote controlling	Environment Monitoring
	Energy Management	Ad hoc networking	Automated ticketing
	Pollution Control	Secure communication	Mobile ticketing, Tracing
	Smart lighting and parking		Smart metering
Personal and Social	Social services	Location sensing and sharing	Historical records
	Privacy management	Ad hoc networking	Social networking
	Entertainment	Secure communication	Tracking, Identification
Industry	Process control	Location sensing and sharing	Environment Monitoring
	Logistic Management	Environment sensing	Tracking, Identification
	Supply Chain	Remote controlling	Sensing, logistic
		Secure communication	Safety, Automation
Smart Home	Security	Location sensing and sharing	Comfortable home,
	Energy control	Environment sensing	Automatic Operation
	Entertainment	Remote controlling	Intelligent Monitoring
	Lifestyle	Ad hoc networking	Smart metering, kids protection
		Secure communication	Plant management
ITS	Smart fleet	Location sensing and sharing	Robot Taxi
	Automotive	Environment sensing	Enhance living
		Secure communication	City information model
Smart Environments	Industrial operation	Location sensing and sharing	Smart workplace
	Smart Agriculture	Remote controlling	Irrigation, Emergency site
	Air quality	Secure communication	Quality environment
		Environment sensing	Rescue personal tracking

- In the SLAAC mechanism, 128 bits IPv6 address is formed by combining 64 bits global routing prefix (GRP) and 64 bits interface identifiers (IID).

- In SLAAC, the IPv6 uniqueness of nodes is maintained by the DAD protocol. DAD protocol uses neighbour discovery protocol (NDP) to detect address duplication.

- In the NDP, duplicate address detection is performed using neighbour advertisement (NA) and neighbour solicitation (NS) messages.

- To detect duplication, when a new node creates a target IPv6 address, it broadcasts a full or partial target address across the network to verify uniqueness.

- If no node claims the target address, then it will be assigned to the node otherwise it will be declared invalid, and the whole process starts again. This repetition of the process will cause an increase in energy consumption and network overhead.

1.2.5 DAD Security

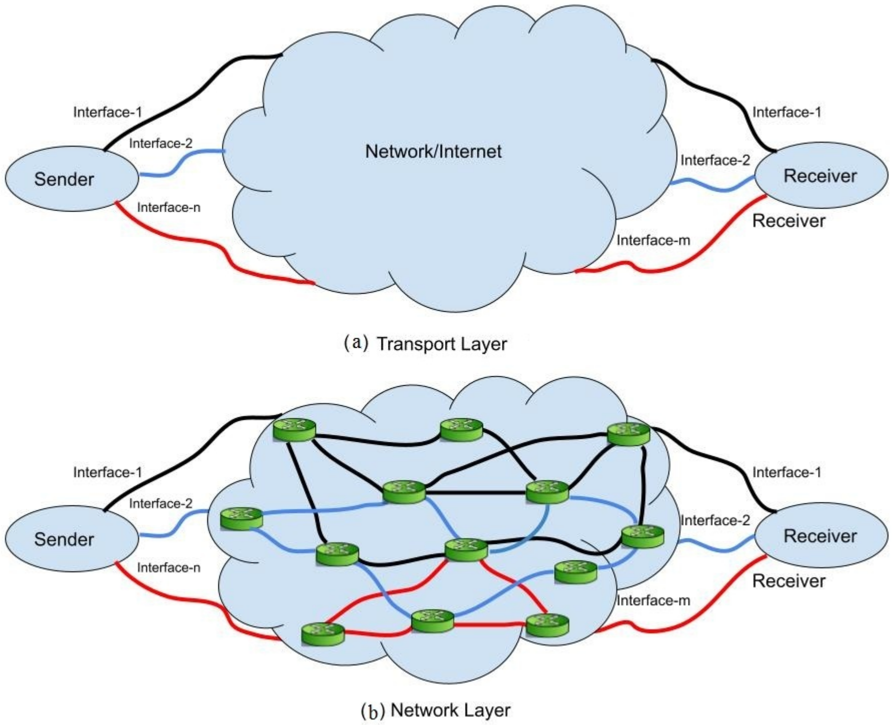
The SLAAC-based addressing scheme uses the DAD process of Neighbour Discovery Protocol (NDP), which allows the node to configure a unique IP after verifying it with an existing host on the same link. Once the node generates the address, it uses an NS message to broadcast the address or part of it into the network. Existing network nodes with similar addresses have to reply using an NA message. If the new node does not receive replies within the stipulated time, it will assign the generated IP address; otherwise, it will regenerate a new address. The NDP has limitations on securing NS and NA messages whereby any node acting as a single link in the conventional DAD approach can respond to each NS message transmitted from the target host, exposing the DAD process to a denial of service (DoS) attack. An old or new malicious node might take advantage of this flaw in DAD solutions by continually replying to all target addresses or assigning existing assigned addresses, preventing a node from entering the network or causing network disruption and misusing a large number of network resources [12]. A malicious node, whether new or old, can attack in three methods [13-14]: Privacy of address, address spoofing, and address conflict.

Apart from these assaults, the authors of [15] identified privacy and security risks such as time correlation, node position monitoring, address scanning, and exploitation of device-specific vulnerabilities. As a result, it is necessary to improve the DAD protocol by considering these risks and constraints.

1.2.6 Multipath Routing and Provisioning

Recently, proposals for multipath routing provision at the transport layer have opened up another research dimension to meet the requirements. These proposals emphasize establishing multiple concurrent paths end-to-end between hosts so as to make maximum use of path diversity [16].

From Figures 1.3 (a) and (b), the idea of multipath routing on the transport and network layers can be understood. To take advantage of multipath routing, the transport layer must facilitate the end hosts to establish concurrent paths for data routing. Most modern devices use Multihoming technology to establish multiple paths between end hosts. There exist several multipath routing concepts at different layers. A layer wise classification of multipath routing protocols based on different parameters is available in [16]. Multipath communication is gaining momentum to become an emerging choice of technology, which has many advantages and challenges [17].



(a) Transport Layer

(b) Network Layer

Figure 1.3: Illustration of Multipath Routing

The multipath routing protocol at the transport layer provides improved load balancing, resource pooling, diversity, security, and throughput and can accommodate future internet architecture. But it still suffers from many challenges, such as improper data chunk scheduling, receiver buffer blocking, spurious retransmission, congestion window (cwnd) growth, and unordered delivery of data chunks, which affect the performance. So it is mandated to improve the existing solutions for multipath routing at the transport layer.

1.2.7 QoS and QoS Parameters

The Quality of Service as a non-functional component provides satisfactory service by different service providers and systems. Due to the heterogeneous nature of IoT, the overall QoS in IoT is the capability of providing services like sensing service, network service, cloud service and services by various enabling technologies and components.

QoS parameters of IoT services apart from basic parameters like bandwidth, delay, packet loss rate, jitter, and throughput are as follows: *System Lifetime*: A measure of the longevity of the nodes.

Latency: The time delay experienced in a system.

Quality: The quality of a sensor network is determined by the quality of data provided in response to a query.

Delay and Delay Variation: Refer to delay and delay variation in data collection from nodes.

Bandwidth, Capacity and Throughput: Indicate the capacity of a sensor network to send data over a link within a given time.

Energy consumption: Calculated based on a specified energy model (e.g., considering the total number/volume of packets/data sent). In particular, in the case of wireless sensor networks (WSN), energy consumption is directly associated with the lifetime of the sensor network.

Resource Optimization and Cost Efficiency: Measures the ability of the system to maximize social welfare, defined as an efficient allocation of limited resources in society to optimize resource utilization. Thus, the social welfare of a system is equal to the difference between the system‘s benefit and cost.

The applicability of a set of QoS parameters depends on the specific IoT application domain in combination with enabling technologies and service providers. Numerous challenges exist in deploying an IoT framework, one of these being meeting the quality requirements of IoT-based applications in terms of energy efficiency, sensing data quality, network resource consumption, and latency.

1.3 CHALLENGES IN IoT SCENARIO

The enormous growth of IoT and the development of various applications have to be faced with a variety of challenges such as the demand for higher data rates, low network latency, high reliability, unique identification, the better quality of services (QoS), and efficient IoT applications. There are a large number of technical barriers that exist but in the area of IoT three biggest challenges identified [1, 18] are energy constraint environment, heterogeneous common protocols, and deployment of IoT devices with a unique identification or IP address. The QoS is another major requirement of users in IoT-based services. It is not only dependent on developed applications but also on deployed network technologies. Hence it becomes a mandate to develop efficient IoT-based applications as well as technologies that can help in the provisioning of better QoS. The research community is working in the direction of designing and developing innovative technologies which can resolve the above-said challenges. Summarized information on the challenges in the IoT environment is given below in Table 1.2. The next sub-section presents various key technological challenges reported in the literature.

Table 1.2: Open research challenges in IoT

Technical challenges of IoT	**Description**
Common Standards	There is a need for common standards among the participating players.
Scalability	To support massive and heterogeneous devices, it requires scalable management protocols, architectures, and communication networks.
Energy Consumption	Mostly IoT devices are battery operated, hence needs energy efficient functionalities and alternate energy sources.
Security & Privacy	Machine to machine communication perspective, Lightweight, and self healing capabilities. Ensure data confidentiality, identity management, authentication, trust, access control, and encryption.
Deployment of IPv6	Address generation, assigning, self-configuration, and management, uniqueness, security, and privacy provisioning in IPv6 assignment
QoS Support	Defining new QoS requirements, support, and fulfilment in shared and resource constraint environment.
Openness	Opening boundaries of existing system considering security, standards, tools, and interfaces.
Applications	Designing and development of IoT-based solutions.
Self Adaption	Configuration, updation, detection, healing, reporting, data collection by devices independently
Resource Utilization	Optimal utilization of available resources in resource constrained environment.

Scalability: With the technological advancement in IoT, the number of devices connected to the internet is increasing and will eventually reach a number in the trillions in the near future. Some questions like identification, naming, authentications, security, privacy, maintainability, and other supports in such massive scaling of things are inevitable. It will be challenging to develop protocols, standards, architectures, real-time solutions, utility models, and data management for massive scaling of heterogeneous devices and applications [19, 20]. Thus, scalability will become a significant issue in the area of IoT.

Deployment of IPv6: Many barriers can slow the progress of IoT development. According to CISCO [1], the deployment of IPv6 is the significant barrier that slows down IoT deployment progress. Moreover, IoT networks deploy low-power operated devices and protocols; here, IETF 6LoWPAN can be used to identify attached devices. The IPv6 protocol supports a stateless auto-configuration mechanism but needs efficient address generation and configuration mechanisms to avoid conflict and misuse of network resources. With the large number of devices connecting to the Internet space, IPv6 is likely to have an essential role in handling the scalability at the network layer. IPv6 also supports security provisioning, making it a secure communications enabler in the IoT [21]. As supported by the IoT6 project, IPv6 is suitable for IoT, and IoT is suitable for IPv6 [19].

QoS support: Most IoT communication occurs in the wireless environment. In such a situation, it is tough to provide QoS requirements; moreover, high data congestion with growing IoT make it even more difficult [6]. Thus, to support QoS in IoT, there is a need for different solutions for different requirements. The WSN research community has already proposed some solutions, but extensive research work is still required to be incorporated into IoT. QoS solutions for M2M communication can be the starting point, but they still need specific solutions in future IoT networks [4].

Energy consumption: The energy consumption in IoT networks is still in the incubation state. Most of the functions of IoT devices support low-power communication like 6Lowpan, but they are still in the early stage of development. Energy-efficient heterogeneous sensing is primarily required in IoT applications because it directly affects network traffic, energy consumption and data storage [6]. Battery replacement of billions of devices in a fully functional IoT environment is very difficult. Therefore, optimization of existing protocols and green energy concepts can be deployed with IoT devices to make them power-efficient [19]. There is a need for some mechanism for devices to generate energy from stimuli like vibrations, heat, light, body movement, airflow, etc. [1] through which the issue of energy consumption can be minimised.

Security and Privacy: Security provision is imminent due to the heterogeneous nature of IoT networks and the massive scaling of devices and applications. The security system of IoT networks needs to cover more levels and objects than a normal network. IoT security architecture should be designed considering the device-to-device communication perspective rather than human-to-human communications [11]. As IoT devices are resource constrained to communicate wirelessly, this makes them prone to fail and more vulnerable to security attacks. To counter security attacks, IoT systems and devices must be strong enough to detect, diagnose, deploy countermeasures, and repair independently with lightweight protocols [20].

IoT makes life easy but may compromise the privacy of individual users. So there must be some mechanism to deal with data confidentiality, Identity management, authentication, trust, access control, and encryption [19-20].

Common standards: In forming an IoT network, common standard plays an important role. It allows different players to come across and collaborate with each other in technology development. Many globally accepted organizations, such as IEEE, CISCO, ITU-T, 3GPP, ISO etc., are participating to standardise architecture, communication, security, identification, information processing, platform, and application requirements [1, 11].

Openness: Most sensor-based systems operating within boundaries will require openness to serve remote centres or users in the coming days. However, it requires many research challenges like modification of existing security standards, data analysis techniques and tools, new communication interfaces, new information exchange policies etc. [20].

Self Adaption: Unlike regular IoT networks, most devices are resource constrained; hence, they need to adapt to the environment without any external support. Given the heterogeneity and scalability of the IoT, it is extremely important that the devices manage themselves on their own. Self Adapting capabilities may include identity management, service discovery, device discovery, tuning with external protocols, and fault tolerance [22].

Applications: With the global reachability and adaptability IoT based applications has high priorities over traditional such as WSN and M2M. But designing and developing efficient IoT-based applications such as smart cities, smart homes, environment monitoring, and intelligent farming is still a challenge. However, developing applications requires a smart management system, well structure network, and a smart architecture to support IoT applications [6, 19].

1.4 RESEARCH OBJECTIVES

This section presents the key problems identified from the literature and based on these problems the research objectives are framed. To accomplish the set objectives, work carried out is also outlined along with its scope.

1.4.1 Problem Identification

From the study of literature following problem areas have been identified to get better solutions in the development of IoT infrastructure.

- Large number of devices will be deployed in IoT. Thus, better IPv6 deployment strategies and schemes will be required.

- Optimal utilization of available network resources is also one of the key requirements, it is more reasonable in a constrained environment.

- Providing better QoS to users by different service providers is also challenging, hence needs optimization in existing IoT solutions keeping in mind the QoS requirements.

- As there is an increase in the number of heterogeneous devices and applications, thus ensuring security and privacy also require better standards and solutions.

- Designing and developing novel applications for better utilization of IoT technologies to improve the quality of the working environment and lifestyle.

1.4.2 Research Objectives of Proposed Thesis Work

The main objective of this study is to improve the QoS parameters like energy consumption, delay, bandwidth, throughput, etc, along with security and privacy for IoT.

- Designing of new address assignment method with minimum probability of duplication.
- To secure duplicate address detection (DAD) process from the attack of the malicious IoT nodes.
- Maximum exploitation of available multiple network interfaces by designing novel multipath routing protocol considering QoS parameters.
- Optimization of device resources by designing novel methods.

1.4.3 Work Carried Out

To achieve set objectives, the following research work has been carried out during my PhD.

- Perform a literature review of various IP addressing schemes.
- Proposed a new stateless spatial IPv6 addressing scheme.
- Proposed new IPv6 addressing with Secure DAD.
- Perform a regressive literature review of multipath transport layer protocols.
- Proposed path rank-based concurrent multipath transmission (R-CMT), a transport layer multipath routing protocol.
- Proposed a novel page replacement algorithm to maximize cache memory utilization of devices.
- Developed underground mine monitoring system based on SENSEnuts IoT platform.

1.4.4 Scope of Work

In location-aware IoT applications where large numbers of sensor nodes are required, the proposed spatial IPv6 and secure DAD scheme can provide seamless integration to the internet and provide each node with a unique IP address. Since the IP address of sensor nodes maintain location and time information, hence management of deployed network will be very easy. Even geographic routing can be deployed in the network by using location and time information. With the advancement of technologies, many devices are coming with Multihoming capabilities equipped with multiple network interfaces such as Wi-Fi, LTE, Ethernet, and other heterogeneous radio links. Thus, the realization of a transport layer design for multi-homed devices like CMT and MPTCP is inevitable. The proposed R-CMT variants can be deployed in such an environment to better utilise multiple network interfaces.

1.5 CONTRIBUTIONS TOWARDS OBJECTIVES

This PhD research work has focused to develop efficient communication mechanisms and applications for IoT environments. In this direction following main contributions have been outlined to achieve the research objectives of the thesis.

1.5.1 A Stateless Spatial IPv6 Address Configuration Scheme

The motivation of this research work is to bridge the gap in the growth of IoT technology reported by CISCO [1]. Potential solutions presented in different scenarios and circumstances in the allocation of IPv6 also prompted to contribute in this direction [9]. The advantage of a location-based addressing scheme is that there is no need to maintain logical as well as physical location information. Moreover, location is encoded in IPv6 address, so it can be handy in geographical routing. There are many location-aware IPv6 addressing schemes available in the literature [23-29]. Most of the schemes do not follow the self-configuration standard of IoT. Also, the performance of these schemes is limited when applied in an IoT environment. To enhance the performance while keeping the shortcomings in mind, a new efficient stateless spatial

IPv6 address assignment scheme is proposed with the aim of increased address success rate (ASR), less communication overhead, and energy consumption to achieve the first objective of the research.

1.5.2 IPv6 Addressing Scheme with a Secured Duplicate Address Detection

The uniqueness of generated IPv6 from the stateless addressing scheme is maintained by the DAD protocols. In the Internet Engineering Task Force (IETF) DAD standard [30] and optimised DAD solutions [13, 31–33], a new node joining the network broadcasts the complete target address in the network using an NS message. If any node claims the target address, then it will become invalid, and the whole process starts again, which will cause an increase in energy consumption and network overhead. The above solution, which exposes the complete target address in the network, is prone to different attacks. In order to solve these problems, another method for DAD is available in [34], which is dividing the IID of the target address into two parts DAD ID and Node ID. In this scheme, instead of the complete target address, only the DAD ID part is broadcasted in the network and nodes with matching DAD ID will reply with their Node ID using NA. This solution is not a complete solution as the new node address is hidden from the existing malicious node but in case of the new node is malicious, then this scheme fails, because the complete address of the replying node is exposed to the new malicious node. To mitigate this problem, this work of the thesis proposed a secured DAD for IoT networks which mitigates DoS attacks from the malicious node by minimising communication overhead and energy consumption to achieve the second objective of the research.

1.5.3 A Survey of CMT and MPTCP Multi-Path Transport Layer Protocols

The objective of this survey work is to categorize and investigate the salient features of available multipath approaches with their applicability along with performance in different scenarios of deployment. This work adds the following contributions.

- Core issues that arise and their handling in multipath transmission.

- A comprehensive study of the existing MPTCP and CMT-based multipath transport layer approaches.

- A comprehensive evaluation of CMT and MPTCP approaches in terms of working principles, operating environment, path characteristics, and handling of the core issues of multipath communication.

- Comparative study of CMT and MPTCP transport layer protocol.

- Highlight the development of future research directions of CMT and MPTCP transport layer protocols.

1.5.4 Path Rank Based Data Chunk Scheduling for CMT

The optimization and advancement in CMT scheduling policy improve throughput, robustness, bandwidth utilization, and reliability. However, it still suffers from unwanted retransmissions, improper congestion window (cwnd) growth, receiver buffer blocking, out-of-order chunk delivery, and improper data scheduling as a result of degradation of performance. In addition to these, it is still challenging to achieve desired performance in heterogeneous wireless environments [17, 35-36]. Learning from the existing CMT scheduling policies, this research advances state-of-the-art by proposing a new R-CMT solution by considering the ratio of successfully received and transmitted chunks by the path. A new SCTP-based R-CMT solution is proposed with the aim to improve throughput, cwnd growth and file transfer time to achieve the third objective of the research.

1.5.5 A New Paging Technique to Maximise Cache Memory Utilization of Device

As IoT devices are resource-constrained, optimal utilization of available resources is necessary. In this direction, this thesis proposed a novel longest-distance first (LDF) page replacement algorithm with the aim to achieve the fourth objective by maximizing the utilization of cache memory. The simulation results show that the proposed method optimally utilizes cache memory to minimise the cache miss rate and improve the CPU performance.

1.5.6 SENSEnuts IoT Platform and Bayes Decision Theorem Based Mine Control System

With the advancement of IoT technologies, developing new and efficient IoT-based applications is inevitable to smooth human life. In this direction, this thesis proposed a novel underground mine monitoring and information sharing system. This proposed system is based on SENSEnuts IoT platform and Bayes decision theorem to predict the threats in underground mines. The literature indicates that the existing underground mines monitoring systems are expensive and need accurate monitoring, flexible hardware and software, and an information sharing system. To overcome the above-said shortcomings, this thesis proposed a system that is intended for underground mines to monitor gas levels, smoke levels, air quality levels, and the temperature of underground mines (UM). It aims to develop an enhanced underground mine safety system based on IoT, cloud-enabled, cost-effective, efficient mine monitoring and intelligent controlling systems.

1.6 ORGANIZATION OF THESIS

The rest of the thesis is organized as follows.

i) **Chapter 2** presents the literature survey of the state-of-the-art spatial IPv6 addressing schemes with its comparative analysis.

ii) **Chapter 3** presents a proposed stateless spatial-temporal IPv6 addressing scheme called four-dimensional IP addressing (FDIPA). It is based on the principle that two things cannot be placed at the same location simultaneously. It uses the time and location of devices to generate the target IPv6 address and assigns it to the device after verifying the uniqueness with the duplicate address detection (DAD) protocol.

iii) **Chapter 4** provides the protection of the DAD process from DoS attack. This chapter proposes a better and more secure DAD process for the IoT environment. The proposed DAD process performs address verification in such a way that nodes on the network do not obtain a complete IPv6 address. Hence, it become difficult to perform a DoS attack to disrupt the DAD.

iv) **Chapter 5** presents different challenges of multi-path transmission with possible handling strategies. It also surveyed innovation related to concurrent multi-path transmission (CMT) and multi-path transmission control protocol (MPTCP) transport layer protocols with their working principles, path characteristics, network environment, and handling of challenges. Furthermore, this chapter identifies the future research trend and open problems of multipath communication protocols at the transport layer.

v) **Chapter 6** it has been identified that CMT still suffers from many serious problems such as spurious retransmission, receiver buffer blocking (RBB), congestion window (cwnd) growth, re-ordering, and long round trip time (RTT), in result performance is degraded. Thus, this chapter introduces a path rank-based CMT (R-CMT) which schedule data chunk according to the rank of the path. This scheduling criterion calculates the rank of each network path based on the ratio of successfully received and transmitted chunks.

vi) **Chapter 7** presents a new paging technique to maximize the utilization of cash and flash memory of computing devices deployed in IoT networks. The proposed method is based on the longest distance first (LDF) page replacement policy and produces better results than referenced policies.

vii) **Chapter 8** presents an automated real-time monitoring, alarming, and information sharing system that will help to avoid accidents in underground mines. This system generates alerts and shares information with the concerned official to take immediate preventive measures.

viii) **Chapter 9** summarizes the conclusions drawn from the intensive experimentation carried out in our present research work on “Improving the quality of services for IoT”. This chapter also incorporates the future research directions in which this work can be further extended.

1.7 SUMMARY

This chapter of the thesis presents an introduction to IoT terminologies, applications, and key research work areas. It further describes the different technological challenges in developing IoT infrastructure, identified problems, and research objectives. In the last, it also presents motivations and contributions toward the achievement of set objectives. The next chapter presents the literature survey and highlights the limitations and future research directions of the IPv6 addressing scheme for the IoT environment.

Chapter II

LITERATURE REVIEW OF IP ADDRESSING SCHEMES

As the IPv4 address was already exhausted before the beginning of the Internet of Things (IoT) so IPv6 is widely used to assign a unique identity to IoT nodes. This chapter analyses different components required in assigning IPv6 addresses to IoT nodes, along with a detailed survey of IPv6 address assignment schemes. This chapter also highlights the architectural complexity, limitations of IoT nodes, renumbering, multihoming, merging of IoT networks and other challenges towards assigning IPv6 addresses to IoT nodes. A comprehensive survey on recent addressing schemes with classification based on allocation table and spatial information is presented. This chapter also compares the performance of various addressing schemes based on metrics such as area of applicability, energy consumption, overhead etc. It also describes future research options for addressing IoT networks.

2.1 IPv6 ADDRESSING CHALLENGES IN IoT

The number of connected things to the Internet is exponentially increasing day by day. The number of connected things to the Internet is 25 billion, expected to increase to 76 billion by 2025 [2] and 125 billion by 2030 [3]. Such a heterogeneous network requires smart, scalable, interoperable, efficient protocols with a unique identity for every device to maintain trust and security. To meet the above requirement there is a need of the development of innovative technology, applications, and services. This development should be capable of powering the connectivity of heterogeneous IoT networks. Various studies by the IoT Research Community, such as architecture, protocols, schemes, applications, open challenges, future research trends, etc., are detailed in the literature [6-7, 19, 58-66].

It is a primary requirement to assign a unique address to each and every node in the IoT environment. Using an assigned address, one can uniquely identify and issue commands from a remote location to individual devices connected to the IoT. IPv4 is one of the addressing protocols used to assign unique addresses on the traditional Internet. Still, due to its limited address space and functionality, it is unsuitable in an IoT environment. IPv6 is the solution that can address the scalability problem in the IoT environment. IPv6 provides self-auto configuration functionality to a node. Assigning unique addresses in an IoT environment using IPv6 addressing schemes or extended schemes has the following technical challenges:

Constraint Node: In an IoT environment, a constrained node may not able to generate a unique IPv6 address and does not support manual configuration due to many limitations like the absence of input/output interface, limited processing, and unidirectional communication and so on. There may be nodes with extremely limited capabilities, such as nanodevices [37] linked to the Internet, which must be addressed in the future.

Renumbering Challenges: In IoT, environment devices can move from one network to another while connected to the Internet. There should be a provision to regenerate unique addresses without affecting ongoing operations.

Multihoming Challenges: IoT nodes may be accessed from a different network or Internet connection. Multihoming may occur when nodes move back from the IPv6 networks to non-IPv6 networks.

Proxying and Tracking non-IP nodes: IoT nodes may work as bridges or proxies for non-IP networks. A unique ID, such as a MAC address associated with these nodes, may be used to generate an IPv6 address. The unique ID associated with these nodes may change according to their use. So there must be provided to handle it because IPv6 addresses may not be permanent for such nodes.

Duplicate Address Detection: As the nodes generate their address themselves so generated address by nodes may not be unique locally or globally. An efficient DAD protocol must be used to check the uniqueness of the generated address.

Unique Address Generation: Each node in IoT uses IPv6 address configuration schemes to generate an IPv6 address using the addressing scheme and checks its uniqueness which is later assigned to the node if successful. So it requires an efficient addressing scheme that should always generate a unique address or one with a minimal probability of conflict with existing addresses in the network.

Energy Consumption: There should be an efficient addressing scheme to generate addresses with minimum energy consumption.

Auto configuration: As devices in IoT environments are limited in resources, auto-configuration must be provided to generate unique IPv6 addresses.

Communication Overhead: Each node sends a request and replies to messages during the IP address generation. An efficient address configuration scheme should generate an IP address with minimum message transmission into the network.

The absence of Global Prefix: If a network of IoT nodes is disconnected from the internet, then the node may not get information on the global prefixes. Hence it will not be possible for a node to generate an IPv6 address [9].

Unidirectional IoT node: It is impossible to assign an IPv6 address to the unidirectional node by existing addressing schemes. All schemes assume there is bidirectional communication with nodes for DAD.

Directly Connected node: In an IoT network, a few nodes may be connected to the internet directly with a different global prefix.

Interconnected Network: when two or more IoT networks are connected via shared links, it is impossible to configure the local prefix in existing IPv6 schemes. As they perform DAD within the local network.

2.2 IPv6 ADDRESSING ARCHITECTURE

An IoT device has self-configuration capabilities, operates in constrained environments, and uses low-power transmission media. Since Autoconfiguration and 802.15.4 are defined in IPv6 or its extension protocol, hence IPv6 protocol or its extension is logically compatible in IoT environments. That is why IPv6 is used to assign unique addresses to billions of heterogeneous nodes in IoT networks, 128 bits of fixed length consisting of a global prefix and a local prefix part, as shown in Figure 2.1. The number of bits in the global and local prefix varies depending on the link type and deployment scenario, but 64-bit global and local prefixes are generally used. Local prefixes are further divided into groups depending on the technology used and the deployment scenario.

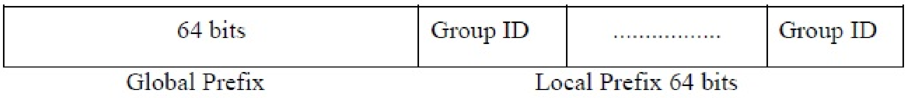


Figure 2.1: IPv6 address structure

The IPv6 addressing architecture supports two types of addressing for unicast addresses: Unique Local Address (ULA) [38] and Globally Unique Address (GUA). ULA IPv6 packets cannot be forwarded by the router as it is not guaranteed to be unique across other networks. ULA allows the network administrator to assign addresses to devices for local network communication. On the other hand, GUA is globally unique and is provided by the Internet Assigned Numbers Authority (IANA).

IPv6 protocol suits define manual and auto address configuration schemes to attached devices. In the case of IoT, devices may not be able to provide input and output interfaces, so manual configuration is not suitable. In IPv6 stateless auto-configuration devices generate their address without interacting with other network entities. IPv6 addresses can be classified into different classes based on the data used, state, and computation to generate addresses, as shown in Figure 2.2.

Based on computation: In this method, classification is based on whether centralised or distributed computation is used to generate an IPv6 address. A central system takes responsibility for the IP assignment process in a centralised scheme. While in the distributed system, multiple network systems participate in IP assignment.

Based on State: This classification is based on whether any repository is used on not during the generation of address and is classified into stateful addressing and stateless addressing. Stateful Address Autoconfiguration: In this method, devices assign IPv6 addresses with the help of a dynamic host configuration protocol (DHCP). A DHCP server is used to maintain a table to monitor the addressing of network devices. It is not suitable in an IoT environment as devices or networks may not be able to support the maintenance of tables or DHCP servers. Stateless Address Autoconfiguration (SLAAC): SLAAC provides a dynamic and scalable mechanism to configure IPv6 addresses independently. In IPv6 or extended networks, devices generate their IPv6 address by themselves with the help of SLAAC. As devices generate their address independently, duplicate address detection (DAD) protocol is used to avoid address conflict.

Based on Data: In this classification is based on the type of data or information used to generate an address and is classified into two classes: spatial and non-spatial. Spatial Addressing: in this class, addresses are generated by the algorithms which use spatial information available with devices. Non-Spatial Addressing: in this class, addresses are generated by the algorithms which use non-spatial data available with devices.

2.3 IPv6 ADDRESSING SCHEME

IPv6 addressing schemes developed for Wireless Sensor Networks (WSN) and MANETs can be employed in IoT to assign unique addresses to devices. Research on IPv6 addressing schemes for constraint and the unconstrained node has been carried out extensively by the community of WSN and MANETs, which is almost similar to the IoT environment. This section presents a survey of commonly used stateless IPv6 addressing schemes with their classification, configuration details, merits and demerits.

Classification: Figure 2.2 shows the classification of addressing schemes as per their working methods. The description of key classes is presented below.

Stateful auto address configuration: Stateful protocols can be further divided into distributed and central management. Since address details for all IoT nodes in the network are stored in one or more than one IoT node, which results in a unique address, so there is no requirement for duplicate address detection (DAD) mechanisms. Central addressing uses the same concept of the DHCP protocol by using a centralized allocation table. Distributed addressing allows many nodes to keep a record of the allocation table independently and to allocate addresses to requesting nodes using the exchange of messages with neighbour nodes.

Stateless auto address configuration: Stateless auto-configuration is the method where IoT nodes within the IPv6 or 6LoWPAN network automatically generate their own IPv6 address. These schemes can be classified into two categories.

Non-Spatial addressing Schemes: This type of addressing scheme does not consider about spatial information of nodes in generating of address [39]. Listed below are some of the Non-spatial addressing methods designed by the research

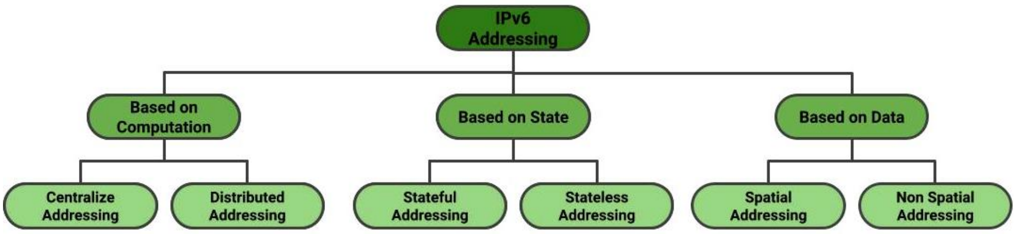


Figure 2.2: IPv6 address classification

community. EUI-64: A globally unique IPv6 address generated from the network interface's globally unique identifier, such as IEEE 802 48-bit MAC addresses [40]. The last 64-bit local prefix is generated by using the 48-bit MAC address of the network interface identifier and 16 bits IEEE reserved value FFFE. Other methods are used to generate the IPv6 address if a network identifier is unavailable.

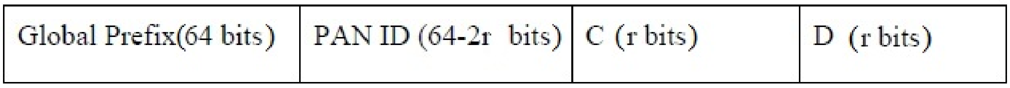
Privacy Addresses: An IPv6 address is generated using pseudorandom algorithms if a globally unique identifier is unavailable or if a host wishes to improve privacy by making IP-based tracking impossible [41]. In this scheme, an MD5 message digest of a random or previously saved history value is used to generate the last 64-bits of the IPv6 address. Left most 64 bits of the message digest are used as an identifier, and the rightmost 64 bits are saved for historical value.

Cryptographically Generated Addresses: For securing IPv6 Neighbour Discovery procedures, IPv6 addresses may be generated from public keys and signed by private keys. These are seldom used.

Spatial addressing Schemes: In this type of addressing scheme, each node uses its spatial location information to generate the related IP address. Listed below are some of the key spatial addressing methods presented.

Spatial IP Address Assignment (SIPA) [23]: For any IP-based network, SIPA IP addresses assignment schemes can be used to solve the address assignment problem. With SIPA, each node independently generates its IP address using spatial information. Since SIPA assumes that each node is aware of its spatial location [42], the address assignment takes place independently. In SIPA, each IoT node generates its IP address by taking the (x; y) coordinates of the node as the two least significant octets in the IPv4 address and 64 least significant bits in the case of the IPv6 address. This method is successfully implemented in Contiki IoT operating system [43]. Figure 2.3 shows the IPv6 address structure used in SIPA. C and D are calculated using Equation (1).

$$C = [x * (2^{\mathrm{r}} - 1)/Max(x)] \; and \; D = [y * (2^{\mathrm{r}} - 1)/Max(y)] \tag{1}$$



Global Prefix(64 bits)	PAN ID (64-2r bits)	C (r bits)	D (r bits)

Figure 2.3: SIPA IPv6 address structure

SIPA is simple to implement but its Address Success Rate (ASR) is never reach 50% when number of nodes more than 300 when r=8 bits.

Advantages: (1) SIPA takes (x, y) coordinates of the node to generate the least significant bits in the IP address. (2) SIPA takes advantage of the relation between spatial locations in routing, and it neither needs a central server nor communication between nodes to generate IP address.

Disadvantages: (1) In this mechanism, there is no guarantee that each node will have its own unique address, since two or more adjacent nodes may generate the same IP address. (2) Success rate of SIPA can never to be 100% with more than one node.

Scan-line IP Assignment (SLIPA) [24]: The scan-line IP assignment (SLIPA), a method which will assign every node with its own unique address. SLIPA method scans every node with the same least y-coordinate value from left to right and then scans the nodes with the succeeding y-coordinate value. Repeat the procedure until all nodes have been scanned. If two or more adjacent nodes generating the same IP address were found, SLIPA would "move up" the adjacent nodes to ensure one address belongs to only one node without ruining the spatial relation between nodes. The assignment is unsuccessful if two or more nodes are assigned to the same IP address. The experiment shows that SLIPA performs better in the maximum number of nodes that can be successfully assigned under different distribution patterns.

SLIPA address structure is the same as shown in Figure 2.3, but the calculation of C and D by Equation (2) and (3) is different.

D is calculated based on sorting nodes in the y-coordinate and assigning a line sequence number to nodes having the same value [24].

$$C = [(x - Min(x))/Q] \tag{2}$$

Where Q = [Max(x)-Min(x)]/(2^r-1).

$$D = D(k, SN) = SN \ if \ k = 1 \ else \ D = D(k, SN) = D(k-1, SN) + 1 \ if k > 1 \tag{3}$$

Where SN is the scan line number starting from 0, and k denotes kth node having the same y-coordinate value.
The detailed description of these equations are available in [24]. Simulation results show that SLIPA's ASR is 100% when the network nodes are between 700 to 1250 if r=8 bits.

Advantages: (1) SLIPA algorithm improves the assignment success rate (ASR) more than SIPA. (2) SLIPA can attain a good ASR when nodes are regularly distributed.

Disadvantages: (1) If nodes are deployed by random distributions, the improvements would be limited. (2) Scan-line fails when the line number reaches 256 since the last octet in IP address can't exceed 255 in the case of IPv4.

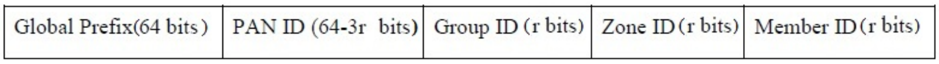
Scan-line IP Assignment with equal Quantity Partitioning (SLIPA-Q) [25]: SLIPA-Q uses the equal-quantity partition instead of the equal-distance partition of SLIPA. SLIPA-Q is based on the scan-line concept, and an optimised form of the SLIPA IP address assignment scheme. SLIPA-Q IPv6 address structure is the same as SLIPA, and the value of C and D is calculated based on the below method.
Q = t/(2^r-1), where t is the total number of nodes in the network.
Z = int(i/Q), where i is the order value assigned to the node when shorted in the x direction and starts from 0.
C = ((i - i^l)mod(Z^h-Z^l+1))+ (Z^h-Z^l+1)
if Q >= max_node(Z)
C = ((Z+1)mod(Z^h-Z^l+1))+ (Z^h-Z^l+1)
if Q<max_node(Z) where i^l denotes lowest order value, Z^h highest zone value and Z^l lowest zone value.
D = D(k,SN) = SN if k=1
D = D(k,SN) = D(k-1,SN)+1 if k>1

Experiment shows that SLIPA-Q performs better than SLIPA and SIPA for IP assignment of different distributions and different numbers of nodes. SLIPA-Q has been tested 1,000 times with 1,000 randomly deployed nodes; the average ASR obtained by SLIPA-Q is double that of SLIPA. Under the same 88% ASR, the average numbers of nodes that can be successfully assigned by SLIPA-Q, SLIPA, and SIPA are 950, 850, and 135, respectively. Compared to previous spatial IP assignment schemes, SLIPA-Q can significantly improve ASR for allocating IP addresses to a huge set of nodes.

Advantages: (1) SLIPA-Q replaces the equal-distance partition with an equal quantity partition and uses ASR as the key performance indicator to represent the ability to assign a unique IP address. (2) This scheme maintains spatial relations among nodes.

Disadvantages: (1) This scheme is limited to two-dimensional space and doesn't mention how to deal with the mobility of nodes in the network. (2) This scheme does not guarantee unique IP addressing as well.

Multi-Projection IP address Assignment(MPIPA) [26]: The basic concept of MPIPA is applying a projection scheme to represent nodes from three-dimensional space to two-dimensional space and then applying the equal-quantity partition and scan-line scheme used in SLIPA-Q to calculate zone ID and member ID of each node by their x coordinates and y coordinates. In MPIPA, nodes report their three-dimensional location information to the base station (BS) to request IP addresses once deployed in the network. The BS will perform MPIPA to determine the node's IP address by utilizing the node's location information. Figure 2.4 shows the IPV6 address structure used by MPIPA. Zone ID and Member ID is determined similarly to SLIPA-Q C and D field. The group ID is determined by partitioning z-coordinates into 2^r groups (from 0 to 2^r-1). MPIPA uses two kinds of grouping methods.
Distance Based Grouping (MPIPA-D)
$G = (\max(z)-\min(z))/(2^r-1)$
$G_{id} = \text{int}\ ((\text{node}(z)-\min(z))/G)$
Quantity Based Grouping (MPIPA-Q)
G = order number of nodes when sorted in z-direction.
$Q=t/(2^r-1)$
$G_{id} = \text{int}(G/Q)$



Global Prefix(64 bits)	PAN ID (64-3r bits)	Group ID (r bits)	Zone ID (r bits)	Member ID (r bits)

Figure 2.4: MPIPA IPv6 address structure

Simulation results show that when r=9 bits in SIPA and r=6 bits in MPIPA are used, ASR of SIPA drops to zero while MPIPA-D and MPIPA-Q still maintain 100% when the number of nodes is above 6000. MPIPA-Q (ASR 90%) performs better than MPIPA-D (ASR 45%) when the number of nodes is approximately 80,000.

Advantages: (1) MPIPA extends two-dimensional spaces to three dimensional spaces to assign IP addresses in the network. (2) MPIPA can also be applied in an IPv6-based network by defining the interface ID in standard IPv6 address format. (3) MPIPA can achieve higher ASR than randomly selected addressing methods.

Disadvantages: (1) MPIPA can be used only when nodes are fixed. (2) MPIPA does not guarantee to generate node's unique IP addresses.

Distributed Spatial IP Address Assignment (DSIPA) [44]: The basic concept behind DSIPA is to assign an IP address to the node based on neighbour discovery. In DSIPA, nodes with IP addresses are responsible to assign an IP address to their neighbour by using their location coordinates. Each node generates its IPv6 address by transferring its physical location into logical location coordinates; therefore, every node maintains spatial relations with each other. Spatial information can be used to perform geographical routing.

Advantages: (1) Relationships between nodes can be identified based on their IP addresses. (2) Less energy consumption in IP addresses generation.

Disadvantages: (1) Duplicate address can be generated. (2) DSIPA can be used only when nodes are fixed.

In [27], the authors proposed an IPv6 addressing scheme based on node location information and passive DAD for 6LoWPAN-based networks and claimed improved delay and overhead. Abdullah et al. [28-29] proposed a novel GPS location-based IPv6 addressing scheme for WSN and used it to predict the node's location from its address, but it does not consider ASR and overhead. In [44], another IP assignment scheme was presented named DSIPA. In DSIPA, an IP-assigned node is responsible for assigning an address to the neighbour node based on its location. In a paper [45], authors have proposed a scheme based on the IoT network's hierarchal structure. In [46], another scheme uses node clock skews to generate the unique IPv6 address for IoT nodes. A new stateless IPv6 address Autoconfiguration scheme for the 6LoWPAN network using colour coordinates is outlined in [47]. Another work [48] proposed a dynamic IPv6 address allocation scheme for applications with massive nodes and indefinite topology, such as smart cities. Abdulha et al. [55] proposed an IPv6 addressing scheme to mitigate reconnaissance attacks, which generates addresses using device coordinates, random numbers and MAC of the coordinator node. Xu et al. [56] proposed location-based addressing in the 6LoWPAN network. The node's location is projected based on the coordinator or edge router. Hussain et al. [57] proposed demand-based location-aware proxy mobile IPv6 addressing, which improves the signalling cost and load of the network.

2.4 COMPARISON OF STATELESS IPv6 ADDRESSING

Addressing IoT is one of the biggest challenges in recent years, and many schemes, as discussed in the previous section, have been developed. A comparative summary of key IPv6 configuration schemes based on addressing overhead, energy consumption, ASR, and location awareness is presented in Table 2.1. This work compares the essential performance metrics like the uniqueness of generated address, energy consumption, communication overhead and embedded location information in the address. These Addressing schemes are classified into two categories non-spatial and spatial. Most non-spatial addressing schemes guarantee to generate unique addresses within specified constraints, while spatial techniques generate IPv6 addresses with embedded spatial information but do not guarantee uniqueness. Although the performance of these IPv6 addressing schemes is promising, optimise schemes would be required to address the issues like Quality of service (QoS) aware IPv6 addressing scheme to ensure the QoS requirements of IoT environment, network security, scalability, and adaptability of harsh environment.

Table 2.1: Comparison of IPv6 Addressing Schemes in IoT

Scheme	**Year**	**Stateless**	**Distributed**	**Energy**	**Overhead**	**Location**
IPv6 Auto [40]	1998	✓	✓	High	High	×
SIPA [23,49]	2004	✓	✓	High	High	✓
Color-Coordinate [47]	2009	✓	✓	High	High	✓
SLIPA[24]	2009	×	×	High	High	✓
Wang et al. [50]	2010	×	×	High	High	×
SLIPA-Q [25]	2011	×	×	Low	Low	✓
MPIPA [26]	2012	✓	×	Low	Low	✓
DSIPA [44]	2012	✓	×	High	High	✓
Xiaonan et al. [51]	2013	✓	×	Low	Low	✓
Wang et al. [27]	2014	✓	✓	High	High	✓
Chakraborty et al. [45]	2015	×	✓	Low	Low	✓
Clock-Skew[46]	2015	✓	✓	Low	Low	×
Wang et al. [52]	2016	×	✓	Low	Low	✓
Mavani et al. [53]	2018	✓	×	High	High	×
Wang et al. [54]	2018	✓	✓	Low	Low	✓
O'Daniel et al. [28,29]	2019	✓	✓	High	High	✓
Mishra et al. [48]	2019	✓	×	Low	Low	×
SEUI-64 [55]	2019	✓	×	High	High	×
Xu et al. [56]	2021	✓	×	Low	Low	✓
Hussain et al. [57]	2021	✓	✓	Low	Low	✓

Most of the schemes are centralized and do not follow the self-configuration standard of IoT. The performance of these schemes is also limited when applied in an IoT environment. From this study, the following shortcomings have

been identified.
1) Available existing schemes do not guarantee the generation of unique IPv6 addresses; hence they need optimization.
2) Most of these existing schemes are centralized and stateful, therefore not compatible with the IoT environment.
3) The ASR of location-based schemes is limited, so it adds more overhead and energy consumption during the addressing process.
4) It is also identified that optimization is required to minimize energy consumption and overhead of the addressing process.
5) Enhancement is also required to secure duplicate address detection process in IPv6 address assignment as it suffers from many issues.

2.5 SUMMARY

This chapter presents the survey of IoT basic building blocks, IPv6 addressing architecture, IoT protocol stack, IPv6 addressing schemes and IPv6 addressing challenges in detail. The work of this chapter presents a detailed description of IoT architecture with fundamental building blocks considering the deployment scenarios of hardware components of IoT networks. This work also describes the layered stack protocols considering the deployment and services offered by software components. Finally, a comparison between addressing schemes are presented based on the different performance metric. As IPv6 addressing in IoT has been a promising area of research in recent years, this chapter has surveyed and presented all-important IPv6 addressing schemes with their advantages and disadvantages. The number of IoT devices will increase exponentially to 125 billion by 2030. So it requires a scalable, secure, and interoperable IPv6 addressing scheme for such a heterogeneous network. Keeping in mind the addressing requirements of the IoT network, the next chapter presents a new stateless spatial IPv6 addressing scheme based on the location and time of the IoT device.

Chapter III

A STATELESS SPATIAL IPv6 ADDRESS CONFIGURATION SCHEME FOR IoT

The Internet of Things (IoT) is going to create a heterogeneous network of billions or trillions of connected things with self-aware, self-configuration capabilities that will exchange data with each other. This heterogeneous IoT network requires standard protocols, secure and energy-efficient wireless communication, and the allocation of unique identities such as IPv6 addresses. One of the key challenges in such a heterogeneous network is the maintenance of device location and unique identity to ensure the smooth functioning of location-aware applications. Hence, this thesis chapter presents a stateless spatial temporal IPv6 addressing scheme called four-dimensional IP addressing (FDIPA). It is based on the idea that two objects can not simultaneously be in the same place. It uses the time and location information of the device to generate the target IPv6 address. After verifying its uniqueness with the duplicate address detection (DAD) protocol, it assigns the generated address to the device. It maintains spatial and temporal information and guarantees a unique identity for a large-sized network. Analytically, it is proved that FDIPA will always generate a unique identity if there is no technological limitation. However, the performance of FDIPA is evaluated based on metrics such as Assignment Success Rate (ASR), communication overhead, and total energy consumption in the assignment of a unique IPv6 address. The experimental results show that FDIPA achieves good ASR while keeping low energy consumption and less overhead in the network.

3.1 INTRODUCTION

In the literature study, it has been identified that there are three main barriers to the slow growth of IoT: a) the assignment of IPv6 addresses, b) the energy source of IoT nodes, and c) the agreement on standards [1]. All things connected to the Internet must be assigned a unique IP address, accomplished either by IPv4 or IPv6. Because of the limited addressing space, IPv4 cannot be used in the IoT; the solution to this problem may be IPv6, which has a huge address space. It could accommodate all devices connecting to the Internet in the next century. The IPv6 protocol suite defines manual, stateful, and stateless auto address (SLAAC) configuration. By considering the self-configurable characteristics of devices, SLAAC is widely accepted in the IoT environment.

SLAAC is simple, dynamic, and scalable and provides a way for IoT nodes to self-configure IPv6 addresses [9]. The IPv6 address is represented by a 128-bit fixed size numerical value and is generally divided into two parts; the leftmost 64-bit prefix and the rightmost 64-bit Interface Identifier (IID) [67]. The number of bits in the prefix and IID can vary depending on the IoT node's link type and deployment scenario. An IoT node creates a 128-bit IPv6 address by combining the prefix and IID. The first part prefix is extracted from the network router's router advertisement (RA) message. The second part generates the IID by the node using any addressing scheme. The uniqueness of a generated address is verified using the duplicate address detection (DAD) protocol. A verified unique IPv6 address is assigned to the new node's interface. If a duplicate address is found during the DAD process, a second IID is generated, and the entire process is repeated, leading to delays and energy consumption [30, 40].

The IID is generated by various schemes depending on the deployment scenario and device capability [9,68-69]. These schemes are classified into two classes: spatial and non-spatial. A non-spatial scheme generates IID using stored numerical or any randomly generated values of an IoT node. While the spatial scheme uses spatial information of nodes like location [70-72] and time to generate bits of IID. The performance of addressing schemes is evaluated using different metrics, like assignment success rate (ASR), total energy consumption, communication overhead, average delay time, etc.

According to CISCO [1], the deployment of IPv6 is a significant obstacle in developing IoT technology as existing networks are based on IPv4. In addition, there are already existing methods to overcome the various barriers to IPv6 allocation [9], encouraging anyone to contribute towards this. A location-based addressing method eliminates the requirement to maintain track of both logical and physical location data. Furthermore, because the location is encoded in IPv6 addresses, it might be helpful for geographical routing. The first step toward location-based IP addressing was coined by Adam Dunkel, named spatial IP address assignment (SIPA) and successfully implemented in the Contiki IoT operating system [23]. SIPA is pretty simple and generates IP using two-dimensional location information. However, its performance is low. Later, scan line IP assignment (SLIPA), another version of SIPA, was proposed with improved ASR. However, its performance is also limited [24]. SLIPA-Q [25] was also proposed, which improves SLIPA's performance but requires a centralized system to detect duplication, making it unsuitable for IoT. A three-dimension location-based scheme, MPIPA [26], is proposed, improving ASR but still suffers when many nodes are deployed. In [27], the authors proposed an IPv6 addressing scheme based on node location information and passive DAD for 6LoWPAN-based networks and claimed improved delay and overhead. Abdullah et al. [28-29] proposed a novel GPS location-based IPv6 addressing scheme for WSN and used it to predict the node's location from its address, but it does not consider ASR and overhead. A study of recent spatial IPv6 addressing schemes is summarized in Table 2.1. Most schemes are centralized and do not follow the self-configuration standard of IoT. The performance of these schemes is also limited when applied in an IoT environment. From this study, the following shortcomings have been identified.

- Existing schemes do not guarantee the generation of unique addresses; hence they need optimization.

- Most of these are centralized and stateful, therefore not compatible with the IoT environment.

- The ASR of location-based schemes is limited, so it adds more overhead and energy consumption during the addressing process.

- Optimization is required to minimize energy consumption and overhead of the addressing process.

To enhance the performance keeping the above shortcomings in mind, this thesis chapter proposes a new efficient stateless spatial IPv6 address assignment scheme with the aim of increased ASR, less communication overhead, and energy consumption. The essential contributions of this chapter of the thesis are as follows:

- A four-dimensional IPv6 address format is proposed. The address generation scheme FDIPA is presented based on the proposed address format.

- The proposed FDIPA scheme generates IPv6 addresses by using the time and location information of the IoT node. As two things can not be put together simultaneously, IPv6 generated by FDIPA will always be unique.

- An analysis of unique IPv6 address generation, energy consumption, and communication overhead is presented.

- A thorough evaluation was conducted. The results indicate that the suggested method provides a unique identity for many nodes and enhances ASR while reducing communication overhead and energy usage.

FDIPA uses IoT devices' location and time information to generate the last 64-bit IID according to the defined IPv6 format. As two different devices can not be placed in the same location simultaneously, FDIPA generates IID with a minimum probability of duplicacy. Further, based on generated IID and extracted GRP from RA, FDIPA forms a 128-bit unique IPv6 address. A mathematical and experimental analysis is presented, which reveals how FDIPA generates a unique identity for a large number of devices. Moreover, simulation results reveal that FDIPA achieves better performance in terms of ASR, communication overhead, and energy consumption.

3.2 PROPOSED FDIPA SCHEME

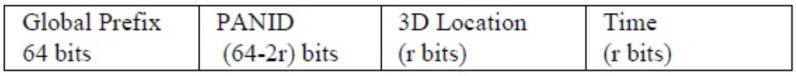
The conditions and assumptions of the proposed addressing scheme will be described in this section. The proposed network concept is presented first, followed by a description of the FDIPA IPv6 address format. Finally, the proposed FDIPA technique is outlined for assigning a unique IPv6 address to each node based on the nodes' three-dimensional position and synchronized time.

3.2.1 Network Model

The random network model is considered to be based on IPv6, and connected devices are mobile and fixed. Edge routers or Gateways can connect devices or nodes to the Internet directly or indirectly. It is also expected in this model that all nodes can determine their three-dimensional location utilizing available methodologies [72] or GPS to determine three-dimensional quadratic (x, y, z) location.

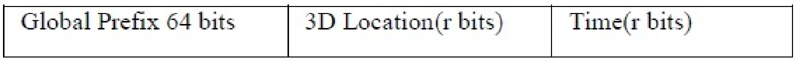
3.2.2 IPv6 Address Format

The proposed method is based on the IPv6 address format depicted in Figures 3.1, 3.2, and 3.3. Figures 3.1 and 3.2 are for IoT devices that are part of a local network, whereas Figure 3.3 is for independent nodes directly connected to the Internet.



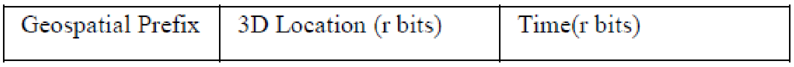
Global Prefix 64 bits	PANID (64-2r) bits	3D Location (r bits)	Time (r bits)

Figure 3.1: IPv6 address format inside sub-network of a local network



Global Prefix 64 bits	3D Location(r bits)	Time(r bits)

Figure 3.2: IPv6 address format inside a local network



Geospatial Prefix	3D Location (r bits)	Time(r bits)

Figure 3.3: IPv6 address format of independent node

3.2.3 FDIPA

The main principle of FDIPA is that two objects cannot simultaneously be placed at the same place. FDIPA presupposes that things are placed in four-dimensional space in the IoT environment. The first three dimensions, x, y, and z, will represent location, while the fourth dimension, t, will represent time. FDIPA generates IPv6 addresses by considering the x, y, and z information of the IoT node and t the gateway or network's synchronized time. When a node generates an IPv6 address, it uses the duplicate address detection (DAD) protocol to ensure that it is unique. If the address is unique, it will be assigned to the node; otherwise, the process will be repeated. To generate IPv6 addresses, nodes perform the following three phases in FDIPA: (a) Time Synchronization, (b) Three Dimension Location Calculation (c) IPv6 address generation utilizing FDIPA. Before the detailed description of FDIPA, the different parameters used are defined as follows:

x- the x-coordinate value of the IoT node.

y- the y-coordinate value of the IoT node.

z- the z-coordinate value of the IoT node.

t- Synchronized system time of the IoT node.
n- Number of nodes in the IoT network.
Time Synchronization: In spatiotemporal-based IoT applications, sensing devices must synchronize their system time with any reference time. There are many clock synchronization mechanisms available in the literature. Most of these methods used gateway clock g(t) to maintain a standard clock among the devices connecting to the network. A device can synchronize its clock t using Equation (1).

$$t = \theta + f * g(t) \tag{1}$$

Where θ clock offset and f is clock skew.
The sender-initiated synchronization between gateway-node pairs is achieved through handshaking. At t_1, a node sends a synchronization pulse packet to the gateway. Gateway receives this packet at t_2= t_1 + pd + θ (here, pd is propagation delay). The gateway sends an acknowledgement back to the node at t_3, and the node receives an acknowledgement at t_4. From Equations (2) and (3), clock offset and propagation delay values can be calculated.

$$\theta = ((t_2 - t_1) - (t_4 - t_3))/2 \tag{2}$$

$$pd = ((t_2 - t_1) + (t_4 - t_3))/2 \tag{3}$$

From the Equations (1), (2), and (3), a node can synchronize the clock t with the gateway, assuming that no clock skew is present.

Three dimension location calculation: In location-aware IoT applications, devices can identify their location. Many well-defined methods are available in the literature to estimate location. If the IoT node cannot determine its location, it will use the location information of the gateway or any other device. In this proposed scheme, the location coordinate (x, y, z) of the IoT node is identified concerning the gateway node (x_c, y_c, z_c), and the relative location is estimated according to the Equations (4) [72].

$$location(x,y,z) = \begin{cases} x = \frac{\sum_{i=1}^{k} x_{ci} A_i}{\sum_{i=1}^{k} A_i} \\ y = \frac{\sum_{i=1}^{k} y_{ci} A_i}{\sum_{i=1}^{k} A_i} \\ z = m_{L1} y + b_{L1} \end{cases} \tag{4}$$

Here A is an area of a triangular patch, m denotes the slope of the patch, and b denotes the intersection with axis z.

However, it is assumed that all nodes or sensor nodes in the IoT network are location-aware. But in some specific situations, such as when two or more sensors can be housed in a device, thus have duplicate spatiotemporal characteristics. The following three cases may be considered to deal with this situation. 1- Multiple sensors without a microcontroller – Sensors without a microcontroller, such as a temperature, proximity, and other environmental sensors, just perceive ambient stimuli and report them to the device or gateway; they do not require an IP address. For internet connectivity, only the gateway or device requires an IP address.

2- Multiple sensor nodes with microcontroller and without location awareness. In this case, the device will act as the gateway or coordinator, and the sensors housed in the device will act as the sensor nodes. These sensor nodes will derive their location from the device's relative position. Several well-developed mechanisms are available to estimate the relative position of the known location of another device based on the angle of arrival and the signal strength indicator [54, 72].

3- Multiple sensor nodes with microcontroller and location-aware–In this case, sensor nodes will identify their location independently.

IPv6 Address generation: The main principle behind FDIPA for the unique identity (IP) generation of an individual node is by concatenation of location and time as per Equation (5) and it works on two rules.

Rule 1- Two different things can't occupy the same location simultaneously.

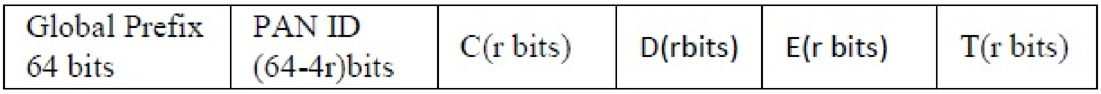
Rule 2 – Two different things can occupy the same location at different times.

$$IP_i = location(x.y.z)_i.time(t)_i \tag{5}$$

If there are n nodes in a network, then n identities (IP_1, IP_2...IP_i...IP_n) will be generated. It can be proved that all these identities are unique.

Algorithm 1 IPv6 Generation

```
Result: IPv6 Address
Input: GRP, Node_Type, time, Max_DAD
Node_Type=Semiconfigured
P:
Loc=GetNodeLocation()
r=GetIIDFormat()
IID=FDIPA(Loc,r,time)
Broadcast NS    //DAD for Duplicacy
while (Timeout==False) do
    Receive NA
    $DAD\_count^{++}$
    if ($DAD\_count < MaxDAD$) then
        Goto P;
    end
    else
        Log System Management Error
    end
end
IP=concatenate(GRP, IID)
Node_Type=configured
Return (IP)
```



Global Prefix 64 bits	PAN ID (64-4r)bits	C(r bits)	D(rbits)	E(r bits)	T(r bits)

Figure 3.4: FDIPA IPv6 Address Format

Proof of unique identities

Let the identity of ith node is IP$_i$ and its value will be (x.y.z)$_i$.t$_i$ as per Equation (5). So identity of all n nodes in network will be (x.y.z)$_1$.t$_1$, (x.y.z)$_2$.t$_2$ .....(x.y.z)$_i$.t$_i$,...........(x.y.z)$_{n-1}$.t$_{n-1}$, (x.y.z)$_n$.t$_n$.

Suppose there are two different nodes numbered with i and j with their identity IP$_i$ and IP$_j$ where i≠j and 1≤ i, j≥n. IP$_i$ ≠ IP$_j$ or (x.y.z)$_i$.t$_i$ ≠ (x.y.z)$_j$.t$_j$ for all value of i and j. It can be proved with the following cases.

Case 1

if t$_i$ = t$_j$ then (x.y.z)$_i$ $\neq (x.y.z)_j$ according to Rule 1.

Case 2

If (x.y.z)$_i$ = (x.y.z)$_j$ then t$_i$ $\neq t_j$ according to Rule 2.

So (x.y.z)$_i$$.t_i \neq (x.y.z)_j.t_j$ or IP$_i$ $\neq IP_j$ is true for all i, j.

From the above cases, it is clear that the identity generated by FDIPA will always be unique if there is no technological limitation.

But the IPv6 address is represented with 128 fixed bits, so the location and time cannot be encoded in a certain number of bits. Here IPv6 address is generated according to the address format shown in Figure 3.4, and values are calculated using Equations (6), (7), (8), and (9).

$$C = [x * (2^{\mathrm{r}} - 1)/Max(x)] \tag{6}$$

$$D = [y * (2^{\mathrm{r}} - 1)/Max(y)] \tag{7}$$

$$E = [z * (2^{r} - 1)/Max(z)] \tag{8}$$

$$T = [t * (2^{r} - 1)/Max(t)] \tag{9}$$

Algorithm 2 Verification of Received NS

```
Result: NA
Input: NS
while (IP address is not empty) do
    IPx = Extract IP from addresses
    IIDx=substring(IPx,64,127)
    if ($DADIDx == DADID\_F$) then
        Sendout NA
    end
end
Discard NS  Return ()
```

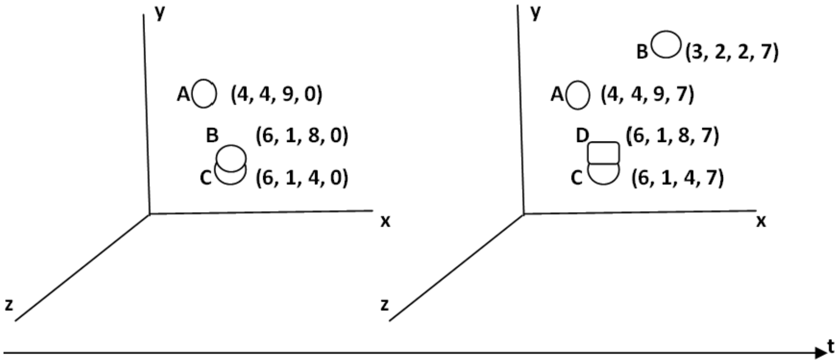


Figure 3.5: Example Network with coordinate values of 4 nodes

The proposed scheme is described using pseudo-code Algorithm 1, Algorithm 2, and Algorithm 3. Uniqueness is maintained using the DAD protocol, which uses neighbour discovery protocol (NDP) to detect duplication. In the NDP uniqueness is ensured using neighbour advertisement (NA) and neighbour solicitation (NS) messages [73].

Spatial IPv6 Assignment Example: Figure 3.5 is an example of a network with four deployed nodes: A, B, C, and D. When a node is deployed in the network, it first gets its location coordinates (x, y, z) and then synchronizes the system time (t) with the router or gateway. The node also extracts the global routing prefix from the RA message sent by the network router. After receiving the values of x, y, z, and t, the node uses the spatial addressing scheme to generate the IPv6 address.

Algorithm 3 FDIPA IID Generation

```
Result: IID
1  Input: Loc, r, time, PANID
2  x=getX(Loc)
3  y=getY(Loc)
4  z=getZ(Loc)
5  t=time
6  C= x*($2^r$-1)/Max(x)
7  D= y*($2^r$-1)/Max(y)
8  E= z*($2^r$-1)/Max(z)
9  T= t*($2^r$-1)/Max(t)
10 IID=concatenate(PANID,C,D,E,T)
11 Return(IID)
```

In Figure 3.5, initially, at time t=0, three nodes, A, B, and C, are deployed in the network with their coordinates (4,4,9,0), (6,1,8,0), and (6,1,4,0). Further, at time t=7, another node, D joins the network at coordinate position (6,1,8,7), and B moves to (3,2,2,7). At time t=0, nodes A, B, and C generate their IPv6 addresses; at time t=7, node D will generate its IP address according to the location and time values (Coordinates). In this example, FDIPA uses the IPv6 format of Figure 3.4 with r = 4 bits, 64 bit global prefix = FE80::0001, 48 bit pan id = F000..0001 and Max (x, y, z, and t) = 32. Generated IPv6 addresses of nodes A, B, C, and D by FDIPA are shown in Table 3.1, along with SIPA and MPIPA (SIPA3D). The hexadecimal digit values of IPv6 are generated according to Equations (6), (7), (8), and (9).

In this example, SIPA uses the address format shown in Figure 2.3 with r = 8 bits and MPIPA 3D uses the format shown in Figure 2.4 with r = 8 bits for field C and r = 4 bits for fields D and E. From the generated IPv6 shown in

Table 3.1: Generated IPv6 address of node A, B, C, and D

Node	Generated IPv6 address by the different scheme		
	SIPA	**MPIPA**	**FDIPA**
A	FE80::0001:F000..0001:1F1F	FE80::0001:F000..0001:1F24	FE80::0001:F000..0001:1140
B	FE80::0001:F000..0001:2F07	FE80::0001:F000..0001:2F03	FE80::0001:F000..0001:2030
C	FE80::0001:F000..0001:2F07	FE80::0001:F000..0001:2F01	FE80::0001:F000..0001:2010
D	FE80::0001:F000..0001:2F07	FE80::0001:F000..0001:2F03	FE80::0001:F000..0001:2033

Table 3.1, it is clear that FDIPA generates unique IPs for all four nodes, while SIPA and MPIPA generate similar IPs for B, C, D, and B, D respectively.

3.3 ANALYSIS

This section presents an analytical model for evaluating the proposed scheme's performance. Because time and location synchronization is a prerequisite in spatiotemporal-based IoT applications, it is not included in the analysis. The analysis considers ASR, communication overhead, and energy consumption. The rest of the section goes through the modelling that was used to assess the various schemes' performance.

3.3.1 ASR

The success of any IPv6 addressing scheme depends on the ability to generate a unique address for each node available in the IoT network. The performance of the address generation scheme is measured in terms of ASR [25]. It is defined as the percentage of successful unique IPv6 address generation to each node in the network without conflict against the total number of execution of the IP addressing scheme. It is calculated with the help of Equation (10).

$$ASR = s/t \tag{10}$$

s: number of successful unique addresses assigned to each node in the network without address conflict.
t: total number of execution of the scheme.

3.3.2 Communication overhead

Once a node is deployed in the network, it quickly generates its IPv6 address and verifies its uniqueness by DAD. In DAD node broadcast an NS message into the network and waits for a response to the NA message. The process is repeated if DAD detects a conflict; otherwise, the address is allocated to the node. Communication overhead represents the total number of messages a node adds to a fixed network during addressing. Total communication overhead added (C_{Total}) in the network during the DAD process of the proposed scheme includes a new address broadcast cost (C_B) and response cost (C_R) as per Equation (11).

$$C_{Total} = D_n * (C_B + C_R) \tag{11}$$

Where D_n represents the total number of times, the DAD process is repeated to generate unique IP,
and C_B = (N-1)*(p_1), C_R=m*(p_2). Here N is the total number of nodes in the network, p_1 is the broadcast payload, p_2 is the response payload, and m is the number of responses.

3.3.3 Energy

This subsection analyzes energy consumption for SIPA, MPIPA, and FDIPA schemes. Analysis of energy consumption has been done under the random distribution of nodes.

Energy model This proposed work uses the energy model, which is commonly used by the researcher. The three kinds of the energy model are described below:
a) The energy consumption for transmitting the l-bits over a distance d is calculated using Equation (12).

$$E_{Tx}(l, d) = l * E_{elec} + l * \epsilon_{amp} * d^2 \tag{12}$$

b) The energy consumption for receiving the l-bits data packet is evaluated using Equation(13).

$$E_{Rx}(l) = l * E_{elec} \tag{13}$$

c) Energy consumption for forwarding l-bits data packet over a distance d is evaluated using Equation (14).

$$E_{Fx}(l) = E_{Tx}(l, d) + E_{Rx}(l) \tag{14}$$

There are three main phases in these schemes. Firstly, each node generates its spatial IP address by using physical location and time, second, the DAD protocol is performed for detecting duplicate IP addresses, and third is conflict resolution of IP. The DAD process and conflict resolution mainly consume energy, and the whole consumption model is as follows:

Computing energy consumption: In these schemes, each node computes its physical location (from GPS or other ways) to a logical location; the computing values are C, D, E, and T. Energy consumption by a node for computing these values is evaluated using Equations (15),(16) and (17) for SIPA, MPIPA, and FDIPA respectively.

$$E_{compute} = (2 * r * (E_{mul} + E_{sht})) \quad r = 12 \tag{15}$$

$$E_{compute} = (3 * r * (E_{mul} + E_{sht})) \quad r = 8 \tag{16}$$

$$E_{compute} = (4 * r * (E_{mul} + E_{sht})) \quad r = 6 \tag{17}$$

Duplicate address detection: The energy consumption of DAD for single IP is calculated using Equation (18).

$$E_{DAD} = \sum_{i=1}^{N} (E_{Tx}(l,d) + NB_i * E_{Rx}(l)) \tag{18}$$

E$_{DAD}$ is the energy consumption of duplicate address detection; NB$_i$ is the average number of neighbours.

Conflict and regeneration: If there is an IP conflict occurs in the network, then the node will change its state and restart the IP assignment process. This process will be repeated till unique IP is generated or reached the maximum allowed DAD process (MAXDAD). The total energy consumption during this process will be (denoted by E$_{conflict}$) and calculated using Equation (19).

$$E_{conflict} = D_n * (E_{compute} + E_{DAD} + E_{Tx} + E_{Fx}(l,d) * Avg_{hop}) \tag{19}$$

Where D$_n$ denotes the number of DAD process repeated to generate unique IP.

Total energy consumption Total energy consumption (E$_{Total}$) in these schemes can be calculated using Equation (20).

$$E_{Total} = E_{compute} + E_{DAD} + E_{conflict} \tag{20}$$

3.4 EVALUATION

This section presents the comparative analysis between 2D SIPA, 3D MPIPA, and FDIPA. Performance is evaluated based on three parameters. The first parameter is the ASR which assesses the probability of each scheme providing a unique IPv6 address to all IoT nodes, the added communication overhead and the third parameter is the energy consumed to assign the IP address to all IoT nodes in the network.

Table 3.2: Simulation Environment Setting of ASR

Four-Dimensional Simulation Environment Parameters	
Distribution of Nodes	**Range of x, y, z, and t**
Random	x:0∼63; y: 0∼63; z: 0∼63; t:0∼63
x –direction	x: 17∼47; y: 0∼63; z:0∼63; t:0∼63
y –direction	x: 0∼63; y:17∼47; z: 0∼63; t:0∼63
z -direction	x:0∼63; y:0∼63; z: 17∼47; t:0∼63
t -direction	x:0∼63; y:0∼63; z: 0∼63; t:17∼47
Oblique	x:0∼45;y:x∼(x+18);z:0∼63; t:0∼63

3.4.1 ASR

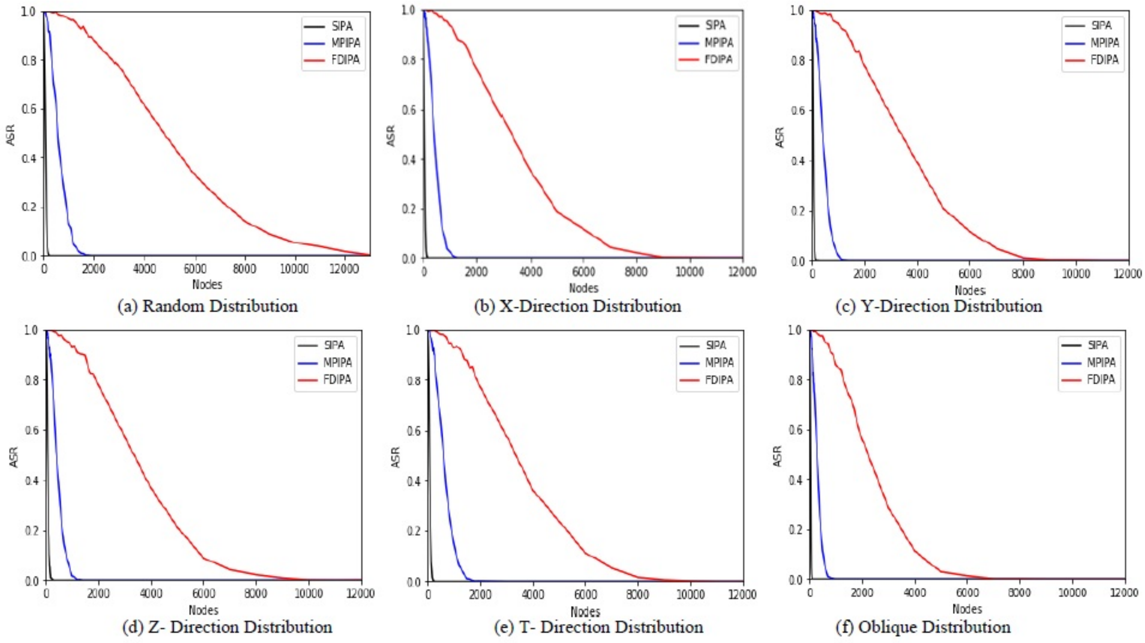
The evaluation is performed in simulation environment set according to Table 3.2. To evaluate the performance in ASR, the 64-bit global prefix and 40-bit pan are considered constant values, and the last 24 bits are set by the addressing scheme when deployed in the network, and the number of IoT nodes increases until ASR falls to zero. To calculate the average ASR, each algorithm runs 1,000 times. The ASR evaluation outcome of six different distributions is elaborated on below.

Random distribution : In this case, nodes in the network are randomly deployed. Hence the range of x, y, z, and t is set from 0 to 63. Figure 3.6 (a) shows the curve of the ASR, in FDIPA it falls to 0% when the number of nodes exceeds 13000, while it falls to 0% in 2D SIPA and 3D MPIPA when the number of nodes is respectively turned out to be 220 and 1800. In this case, the

ASR of FDIPA is 100% as long as the number of nodes does not exceed 250. On the contrary, SIPA and MPIPA's ASR at such nodes are approximately 0% and 75%, respectively. This suggests that SIPA and MPIPA generate more duplicate IP addresses than FDIPA.

x and y-Direction distribution:The range of x, y, z, and t is set from 17-47, 0-63, 0-63, and 0-63 respectively in the X distribution. Figure 3.6 (b) shows the curve of ASR, and in FDIPA, it falls to zero when the number of nodes increases to 10000, while in SIPA and MPIPA, it falls to 0% when nodes exceed only 160 and 1500. In this case, the ASR of FDIPA is 100% as long as the number of nodes does not exceed 180. On the contrary, SIPA and MPIPA's ASR at such nodes are approximately 0% and 75%, respectively. In this distribution, ASR performance is slightly less than the random distribution. The reason is that X distribution supplies less space as the X range is limited between 17 to 47. But the performance of FDIPA is still much better than SIPA and MPIPA. The Y-direction distribution ASR curve is similar to the X-direction, as shown in Figure 3.6 (c), with a difference in the Y limit instead of X.

z-Direction distribution: x, y, z, and t range is set in the z direction distribution from 0-63, 0- 63, 17-47, and 0-63, respectively. Figure 3.6 (d) shows the curve of the ASR, in FDIPA it falls to 0% when the number of nodes exceeds 10000, while it falls to 0% in 2D SIPA and 3D MPIPA when the number of nodes is respectively turned out to be 220 and 1200. SIPA's performance in this distribution is similar to random distribution because it does not consider



(a) Random Distribution

(b) X-Direction Distribution

(c) Y-Direction Distribution

(d) Z- Direction Distribution

(e) T- Direction Distribution

(f) Oblique Distribution

Figure 3.6: The ASR comparison graph under six different node distributions

Table 3.3: The obtained ASR for different distributions of nodes

ASR	**100%**			**75%**			**50%**			**25%**			**0%**		
	SIPA	**MPIPA**	**FDIPA**	**SIPA**	**MPIPA**	**FDIPA**	**SIPA**	**MPIPA**	**FDIPA**	**SIPA**	**MPIPA**	**FDIPA**	**SIPA**	**MPIPA**	**FDIPA**
Random	1	30	250	50	350	2500	75	600	4800	115	875	6800	220	1800	13000
x-Direction	1	25	180	37	275	2200	55	450	3300	75	600	4800	160	1200	10000
y-Direction	1	25	180	37	275	2200	50	400	3800	75	600	4800	160	1200	10000
z-Direction	1	25	180	50	275	2200	75	400	3800	105	600	4800	220	1200	10000
t-Direction	1	30	180	50	350	2200	75	600	3800	105	875	4800	220	1800	10000
Oblique	1	15	110	25	180	1450	37	280	2500	50	400	3500	110	900	8000

Z values in the IP assignment. While FDIPA and MPIPA performance are similar to X and Y distribution. In this distribution, FDIPA performance is much better than SIPA and MPIPA.

t-Direction distribution: x, y, z, and t range is set in the z direction distribution from 0-63, 0- 63, 0-63, and 17-47, respectively. Figure 3.6 (e) shows the curve of the ASR, in FDIPA it falls to 0% when the number of nodes exceeds 10000, while it falls to 0% in 2D SIPA and 3D MPIPA when the number of nodes is respectively turned out to be 220 and 1800. Performance SIPA and MPIPA in this distribution is similar to random distribution because it does not consider T values in IP assignment. However, FDIPA still performs much better than SIPA and MPIPA.

Oblique distribution: x, y, z, and t range is set from 0-45, x-x+18, 0-63, and 17-47, respectively, in the Z direction distribution. Figure 3.6 (f) shows the curve of oblique distributions, ASR of FDIPA falls to 0% when the node increases to 8000, while in SIPA and MPIPA, it falls to 0% when the number of nodes exceeds 110 and 900, respectively. In this distribution, ASR performance is less than all other distributions because X and Y range is limited by each other. In this case, FDIPA still performs much better than SIPA and MPIPA.

The simulation results are shown in Figure 3.6, which clarifies the relationship between ASR and the number of nodes in six different types of node distribution. The result shows that the ASR of FDIPA is better than that of 2D SIPA and 3D MPIPA in all six distributions. It can also be seen from this result that the distribution of nodes in the network also affects the ASR. When the nodes are randomly distributed, the ASR of FDIPA falls to 0% on 13000 nodes, while in oblique distribution, it becomes 0% only on 8000 nodes. From the observation of ASR in different distributions, it is clear that FDIPA can assign IPv6 addresses to much larger nodes than SIPA and MPIPA. Table 3.3 shows the obtained ASR in the different distributions of SIPA, MPIPA, and FDIPA of the different number of nodes. With this data, it could be observed how each curve of the graph falls.

3.4.2 Communication Overhead

The evaluation of communication overhead under the different sizes of networks with 24 bits of addressing space is observed. As shown in Figure 3.7, the experimental result reveals that FDIPA adds less communication overhead in the network than MPIPA and SIPA. However, SIPA's overhead increases exponentially when the network size increases by 2000 nodes. FDIPA adds very less message overhead into the network. The main reason for this is that very few duplicate addresses are generated.

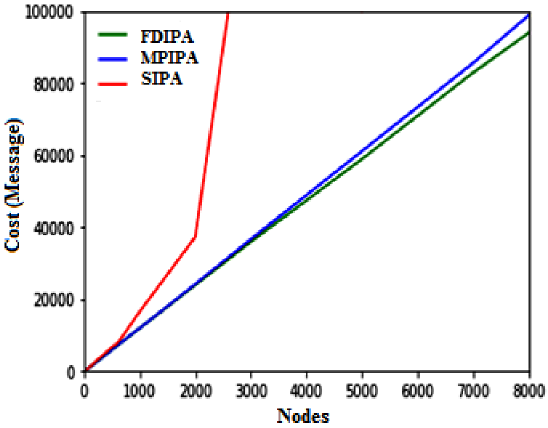


Figure 3.7: Added addressing cost

3.4.3 Energy Consumption Analysis

This section presents the evaluation of the total energy consumption of SIPA, MPIPA, and FDIPA in a Four- dimensional random network under 16 and 24 bits address space. The related network parameters and configuration settings are shown in Table 3.4.

Table 3.4: Simulation environment setting of Energy

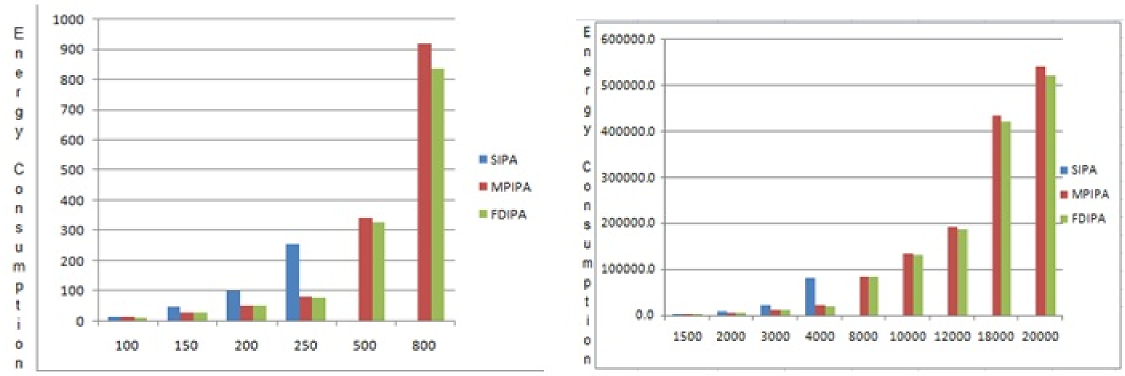
Parameter	**Definition**	**Unit**
[X, Y, Z, T]	Network range	15,15,15,15m3
N	Total number of nodes	5,03,000
R	Transmission range of node	2~3m
d_{ij}	Distance from ni to nj	2~3m
E_{elec}	Energy dissipation rate to run the radio	50nJ / bit
ϵ_{amp}	Energy dissipation rate to transmit amplifier	100pJ /bit/ m2
ϵ_{mul}	The energy consumption of multiply operator	6.39 nJ / bit
ϵ_{sht}	The energy consumption of the shift operator	4.26 nJ / bit
L	Packet length	2,000 bits

The following section shows the comparison of energy consumption when address conflicts among nodes are resolved by the DAD protocol. The X-axis shows the corresponding number of nodes, and the graph's Y-axis shows the energy consumption in jule. In these results, FDIPA outperformed MPIPA and SIPA due to less addressing conflict. In this result, it is also observed that when the number of nodes in the network increases to more than 4000, then SIPA fails to assign IP. The outcomes of the results are as follows:

(1) FDIPA uses space and time to assign unique IPv6 addresses to many nodes without conflict and achieves good ASR. Figure 3.6 and Table 3.3 indicate that the ASR achieved by FDIPA is approximately eight times better than SIPA and MPIPA after running the simulation more than 1000 times for random node placement.

(2) As shown in Figure 3.7, the proposed scheme adds reduced communication overhead during IPv6 address generation. The Reason for less communication overhead is that, FDIPA generates IP with a very high likelihood of uniqueness.

(3) Experimental result in Figures 3.8 (a) and (b) show that FDIPA also reduces energy consumption in IP assignment.



(a) With 16 bits address space

(b) With 24 bits address space

Figure 3.8: Comparison of energy consumption under a random distribution

It is clear from Equation (20) that the maximum energy in an IP assignment would be in resolving the conflict. This is the main reason for low energy consumption in FDIPA as it generates unique IP, minimizing conflict.

3.4.4 Result and Discussion

The results clearly show that the proposed scheme achieves good ASR. As the location is encoded into IP, management of IoT networks and applications will be easy, and even geographical routing can be used. The results shown in Figures 3.7 and 3.8 further reveal that the proposed scheme adds less overhead to the network and consumes less energy during IP assignment. As most IoT networks are resource-constrained and devices are operated by limited energy sources like a battery, hence the proposed scheme is not only efficient, but it will also improve the scalability of the network.

3.5 SUMMARY

This chapter proposed a new SLAAC-based IPv6 addressing scheme, FDIPA, which generates IP using node spatial temporal information. The proposed scheme has been evaluated against metrics such as ASR, added communication overhead, and energy consumption in assigning IP. The results confirmed that FDIPA achieves better ASR while keeping low communication overhead and energy consumption. It also associates location and time with IPv6 addresses to fulfil application requirements. The uniqueness of generated IPv6 in stateless addressing is ensured with the help of the DAD protocol. Due to poor design, the DAD protocol is vulnerable to different types of DoS attacks. In the next chapter of this thesis, a secure DAD protocol is proposed, which not only makes the DAD protocol immune from DoS attacks but also minimises addressing overhead and energy consumption.

Chapter IV

IPv6 ADDRESSING SCHEME WITH SECURED DUPLICATE ADDRESS DETECTION

In the resource constraint IoT network, each end node should have self configuration capability and a unique identifier such as IPv6. The unique identity of end nodes is primarily maintained by employing the stateless autoconfiguration method. In the stateless configuration method, each node generates its identity itself and the Duplicate Address Detection (DAD) protocol is used to verify the unique identity of the node. In existing DAD solutions, when a new node creates a target address, it broadcasts a full or partial target address across the network to verify uniqueness. In the case of complete address broadcasting, the target address is exposed to all the network nodes, whereas in partial broadcasts, the address of some network nodes is exposed to the new node. A malicious node can take advantage of this feature and can disrupt the DAD process by claiming the target address or by making the existing address assigned. This chapter presents a better and more secure DAD process for the Internet of Things (IoT) environment to protect the DAD process from such attacks. In the proposed work, the new node and the existing node transmit only a partial address, and both nodes preserve a portion of the address. In this way, neither the existing nor the new node is able to know the full address of each other, and thus they cannot disrupt the DAD process. Experimental results indicate that the proposed scheme's address success rate (ASR) outperformed existing DAD solutions in the presence of malicious nodes. Also, because of the partial address transmitted by nodes in the network, addressing cost and energy consumption also get reduced.

4.1 INTRODUCTION

On Internet, it is a prerequisite that each device must have a globally unique IP such as IPv4 or IPv6 address to communicate. As IPv4 provides only a limited number of addressing spaces hence in the IoT network IPv6 is suitable. One of the main barriers identified by the CISCO system [1] is the deployment of IPv6 addresses in IoT; hence need to address the IPv6 allocation issues [7], and privacy and security considerations [15] of the address generation mechanism. The IPv6 address generation in resource-constrained IoT networks such as 6LoWPAN and Zigbee is mainly achieved by employing the stateless auto address configuration (SLAAC) [9,69] mechanism. SLAAC is designed to provide the simplest, most scalable, and dynamic way by which nodes can themselves configure IPv6 addresses. In the SLAAC mechanism, the IPv6 address is formed by combining 64 bits global routing prefix (GRP) and 64 bits interface identifiers (IID). The GRP of all the nodes in a network is the same and is delivered by the network's Edge Router or Access Router (AR). The second part IID is generated by the node using any addressing scheme. In SLAAC, the IPv6 uniqueness of nodes is maintained by the DAD protocol. DAD protocol uses neighbour discovery protocol (NDP) to detect address duplication. In NDP, duplicate address detection is performed using neighbour advertisement (NA) and neighbour solicitation (NS) messages [73].

The depleting IPv4 address space opens the door to developing an efficient IPv6 addressing scheme, as it is compatible in an IoT environment. Many schemes for IPv6 address allocation to constrained nodes have been covered extensively by the wireless sensor network (WSN) research community, especially in the academic literature. Requirements for addressing schemes in an IoT environment are almost similar to WSN. Over the years, many SLAAC-based IID generating techniques have been developed. A standardized method for Generating Semantically Opaque IID is outlined in [68] without compromising the security and privacy of users. Abdullah S. A. [55] highlights the present addressing scheme and security concerns and presents a new IPv6 addressing strategy to mitigate reconnaissance attacks by maximizing search space from the malicious node. Song G. et al. [74] outlined a hash scheme for DAD in which the target address is encrypted, which prevents attackers from launching a destination attack.

In the Internet Engineering Task Force (IETF) DAD standard [30] and optimized DAD solutions[31-33,75], a new node joining the network broadcasts the complete target address in the network using an NS message. If any node claims the target address, then it will become invalid, and the whole process starts again, which will cause an increase in energy consumption and network overhead. The above solutions expose the complete target address in the network, which is prone to different attacks. To solve these problems, another method for DAD is available in [34], which is dividing the IID of the target address into two parts DAD ID and Node ID. In this scheme, instead of the complete target address, only the DAD ID part is broadcasted in the network and nodes with matching DAD ID will reply with their Node ID using NA. This solution is not a complete solution as the new node address is hidden from the existing malicious node, but in case of the new node is malicious, then this scheme fails because the complete address of the replying node is exposed to the new malicious node.

An existing or new malicious node can take advantage of this shortcoming of DAD solutions and can repeatedly reply to all target addresses or assign an existing assigned address; this way, a node can be prevented from joining the network or malicious node join with the conflicting address to disrupts network and also a lot of network resources are misused [12]. A new or existing malicious node can attack in the following three ways [14, 75].

Privacy of Address: By getting the address, a malicious node can track node activity and behaviour and poses a threat to data generated by the node.

Address Spoofing: A malicious node spoofs a good node to mislead in the DAD process and can disrupt the normal service of the network.

Address Conflict: A new malicious node may join the network with the existing address to generate address conflict and consume network resources.

Besides these threats, authors of [15] identified privacy and security threats such as the correlation of activities of the time, location tracking of nodes, address scanning, and device-specific vulnerability exploitation. The motivation of this work is to develop an efficient IPv6 addressing scheme to enhance security and privacy and increase the ASR of the DAD process keeping in mind other network performance parameters such as overhead, energy consumption, delay etc. To secure the DAD process and avoid such attack by improving address assignment success rate (ASR) and lower communication overhead, this work proposed a secure DAD for IoT network which perform the following task.

1. In the secure DAD, only part of the target address is broadcast, and part of the assigned address is unicast. In this process, a new or existing malicious node cannot know the complete target address and the assigned address. As a result, the DAD process is secured from the attack by a malicious node, and ASR is increased.

2. Only part of the target and assigned address are used instead of the com-

plete address hence lowering the addressing cost and energy consumption.
3. Secrete portion of the address is not shared across the network; hence privacy of nodes is preserved.

4.2 IPv6 ADDRESSING SCHEME WITH SECURED DAD

This section provides a detailed outline of the proposed IPv6 addressing scheme with secure DAD. This scheme's IPv6 address assignment process is explained with the example at the end of the section.

4.2.1 Network Model

The network of the proposed secure DAD scheme is based on the network architecture described in [34]. There are three types of nodes in the IoT networks: new nodes, configured nodes, and semi-configured nodes. These nodes are connected to the IPv6 internet via the AR. The configured node is one whose DAD process has been completed, where a semi-configured node has just launched the DAD process, and a new node is yet to start the DAD process. To provide security proposed IPv6 address format, as shown in Figure 4.1, is divided into two major parts, 64 bits of GRP and 64 bits of IID. In the first part, GRP identifies a specific local IoT network, such as 6LoWPAN or Zigbee, and it is delivered by AR. The second part (IID) is divided into three parts DAD ID, Secret ID and Node ID. The IID is self-generated by node using any addressing scheme or form by combining randomly generated three parts. In this scheme, the DAD ID and Node ID part are used in the DAD process to ensure uniqueness, while the Secret ID is kept secret by the node. This scheme uses expanded beacon and command frames specified in [34], as shown in Table 4.1 and Table 4.2, and a new node uses the Media Access Control (MAC) address to generate a temporary link address (TLA) during DAD.

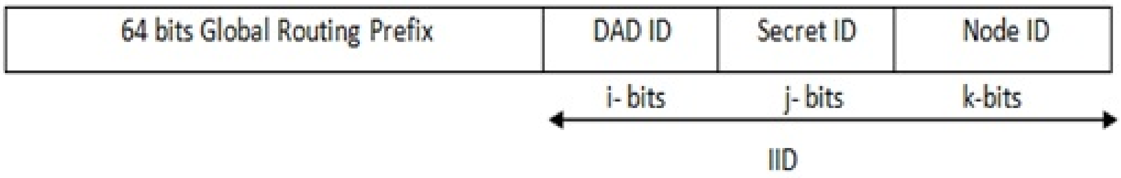


Figure 4.1: IPv6 Address Format Used in IoT Network

Table 4.1: Expanded beacon frame

Type	Communication Mode	Payload
0	Broadcasted by an AR or a Configured Node	GRP
1	Broadcasted by a Half-Configured Node	DAD ID

Table 4.2: Expanded command frames

Type	Communication Mode	Payload
0xA	Unicasted by a Configured Node	Node ID
0xB	Unicasted by a Semi-Configured Node	Node ID

4.2.2 Secure DAD

When node A wants to connect to an existing network, it obtains GRP from Type -0 beacons of AR, generates IID, and configures a unique address according to the following DAD process.

1). A new node generates 64 bits of IID [76] using any scheme and divides it into three parts or generates IID by randomly generating three different parts, 16 bits DAD ID, 16 bits Secret ID and 32 bits Node ID [77]. It broadcasts DAD ID as payload in the type-1 frame, TLA as the source address and marks itself as a semi-configured node. Before broadcasting a type-1 frame following conditions must be satisfied:

- Condition 1: DAD ID must differ from the DAD IDs received by the new node in type-1 beacon frames.

- Condition 2: A node can only repeat up to the maximum number of allowed DAD processes; otherwise, a log is created with a system management error.

2). If the DAD ID of the configured and semi-configured node is equal to the DAD ID of the received Type-1 frame broadcast by the new node, then configure and semi-configured nodes unicast its Node ID back to the new node using Type-0xA frame.

3). If the new node does not receive any type-0xA or 0xB frame in the specified time, then it goes into step 4; otherwise, it acts as per the following rules:

- Rule 1: If the Node ID of the new node is not equal to any Node ID of the received Type-0xA frames, then the new node goes to step 4.

- Rule 2: If the Node ID of the new node is not equal to the Node ID of any semi-configured node and is equal to the Node ID of a configured node, then the new node creates a new Node ID which is different from the Node ID of any configured node and goes to step 4.

- Rule 3: If the Node ID of the new node is equal to any semi-configured node, then it goes to step 1.

4). The new node marks itself as configured and forms a unique IPv6 address by combining GRP with Random ID or IID.

The above proposed IPv6 addressing scheme with secure DAD can be represented using two pseudo codes. The first one is IPv6 address generation which is used by a new node to form an IPv6 address, its pseudo code is described in Algorithm 1. When a configured/semi-configured node receives the broadcast NS frame from a new node, then the second pseudo-code described in Algorithm 2 is used to verify the conflict of the IPv6 address of the new node.

The proposed IPv6 address assignment process with secure DAD is shown with the help of an example in Figure 4.2. Four semi-configured nodes, A, B, C, and D. They randomly make three parts DAD ID, Secret ID and Node ID and broadcast type-1 frames simultaneously. After A receives the Type-0xA frame from configured node 4FFF:6:F32A:8:74:2C:: B3, it finds that its

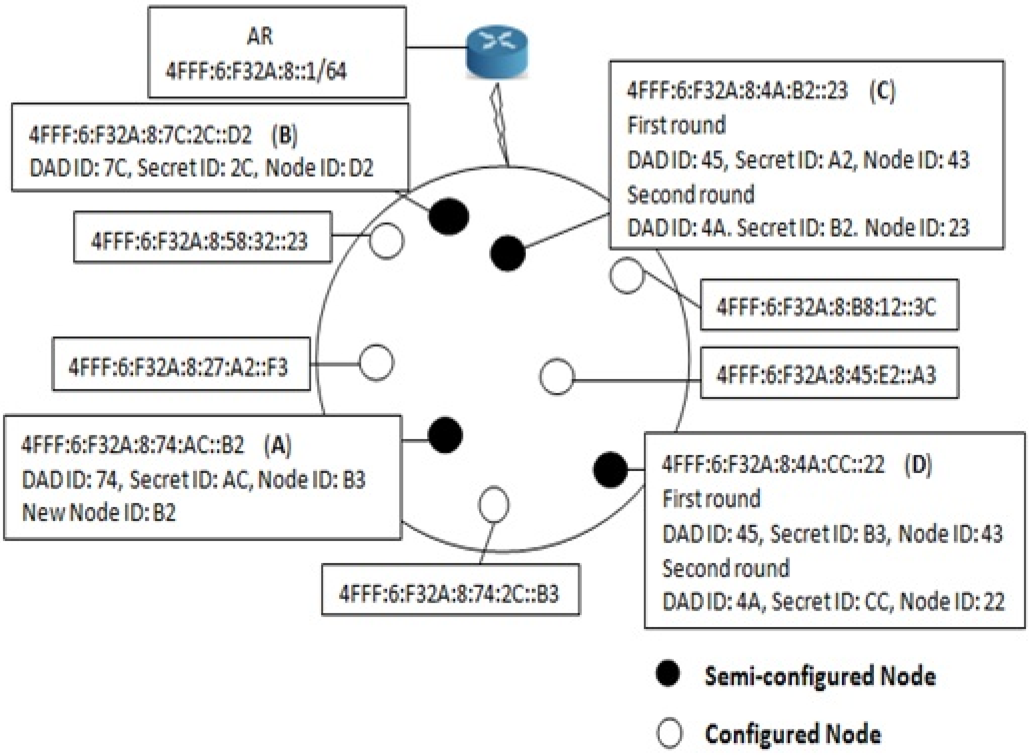

AR
4FFF:6:F32A:8::1/64
4FFF:6:F32A:8:7C:2C::D2 (B)
DAD ID: 7C, Secret ID: 2C, Node ID: D2
4FFF:6:F32A:8:4A:B2::23 (C)
First round
DAD ID: 45, Secret ID: A2, Node ID: 43
Second round
DAD ID: 4A. Secret ID: B2. Node ID: 23
4FFF:6:F32A:8:58:32::23
4FFF:6:F32A:8:B8:12::3C
4FFF:6:F32A:8:27:A2::F3
4FFF:6:F32A:8:45:E2::A3
4FFF:6:F32A:8:74:AC::B2 (A)
DAD ID: 74, Secret ID: AC, Node ID: B3
New Node ID: B2
4FFF:6:F32A:8:4A:CC::22 (D)
First round
DAD ID: 45, Secret ID: B3, Node ID: 43
Second round
DAD ID: 4A, Secret ID: CC, Node ID: 22
4FFF:6:F32A:8:74:2C::B3
● Semi-configured Node
○ Configured Node

Figure 4.2: Example of Secure DAD

Algorithm 1 IPv6 Generation

```
Result: IPv6
Input:GRP, Type, Node_Type, Rec_DADID[ ],Max_DAD
Node_Type= Semiconfigured
P:
if (Type=0) then
    U:
    DADID=random(0x0000,0xffff)
    if (Compare(DADID, Rec_DADID)) then
        Goto U;
    end
    SecreteID=random(0x0000,0xffff)
    NodeID=random(0x00000000,0xffffffff)
    Node IID= concatenate(DADID, SecreteID, NodeID)
end
else
    V:
    IID=IIDScheme()
    DADID=substring(IID,0,15)
    if (Compare(DADID, Rec_DADID)) then
        Goto V;
    end
    SecreteID= substring(IID,16,31)
    NodeID= substring(IID,32,63)
end
Broadcast NS Frame Type 1
while (Timeout=false) do
    Receive NA Frame
    if (Frame Type==0xA and NodeID==NodeID_F) then
        NodeID=Diff_Random(NodeID_F)
    end
    if (Frame_Type==0xB and NodeID==NodeID_F) then
        DAD_count++
        if (DAD_count<MaxDAD) then
            Goto P;
        end
        else
            Log System Management Error
        end
    end
end
IPv6==concatenate(GRP, DADID, SecreteID, NodeID)
Node_Type=configured
```

Node ID 0xB3 is the same as a configured node. So, according to case 3, A selects a different New Node ID 0xB2 and combines DAD ID 0x74, Secrete ID 0xAC, and Node ID 0xB2 with GRP to generate a unique IPv6 address. Node B does not receive any type-0xA frame because its DAD ID does not match with any node. So it forms its IPv6 address in the first round with DAD ID, Secretes ID and Node ID. Node C and D find that their DAD IDs and Node IDs are identical, so they generate new DAD IDs, Secrete IDs and Node IDs in the second round, and broadcast type-1 frames. Since their DAD ID's in the second round differ from any configured and semi-configured node. When they do not get the response in the prescribed time, both nodes make their unique IPv6 address with available DAD ID, Secret ID and Node ID.

Algorithm 2 Verification of Received NS Frame

```
Result: NA Frame
Input:NS Frame
Receive NS Frame Type 1
while (IP addresses is Not Empty) do
    IPx=Extract IP from addresses
    DADIDx=substring(IPx,64,79)
    NodeID=substring(IPx,96,127)
    if (DADIDx==DADID_F) then
        NodeID=Diff_Random(NodeID_F)
        if (Node_Type==configured) then
            Sendout NA Frame Type 0xA
        end
        else
            Sendout NA Frame Type 0xB
        end
    end
end
Discard NS
```

4.3 DAD SECURITY

This section verifies the security threats of the proposed scheme in the presence of malicious nodes in the network.

4.3.1 Privacy of Address

In this DAD process, a new node A randomly generates three parts, DAD ID, Secrete ID and Node ID and broadcasts a type-1 frame. If already configured node X receives a type-1 frame and finds that its DAD ID is the same, then it replies to A by unicasting type-0xA. If A's node ID is not equal to X's node ID, then the IPv6 address is acquired in Case 1; otherwise, it is acquired in Case 2. If X is a semi-configured node then responds to A by Type-0xB frame, and A finds that its node ID is different, then it acquires an IPv6 address in Case 1 or else launches a new IPv6 addressing process. In this way, neither A nor X share the secret ID of their address and still get a unique IPv6 address. Since the Secret ID is not shared by the new node or the existing node, it can be said that the privacy of the IPv6 address is preserved in the proposed scheme.

4.3.2 Address Spoofing Attack

If existing node X is malicious and spoofs node A by returning the Type-0xA frame. Node A will acquire its IPv6 address in Case 1 or Case 2. If attacker X spoofs as a Semi-configured node, then Node A will acquire the address in Case 1 or launches a new addressing process. In this new DAD process, the probability of generating two identical Node IDs and Secrete IDs is approximately zero and equal to $1/2^j$.

Proof of zero probability of identical Node ID

If an f-number of malicious nodes exists, those have the same DAD ID as new Node A.

Then the probability (Ps) of generating identical Node ID by new node A = Existing Node IDs of attacker nodes(f)/Total available Node Ids.

Ps=$f/2^j$

If f=1 then (there is only one malicious node) Ps=$1/2^j$

Here j=32, so P=$1/2^{32}$ and Ps are near zero.

4.3.3 False Address Conflict Attack

In this proposed DAD process, neither a new node A nor an existing Node X can cause a false address conflict because only the DAD ID and the Node ID are shared between A and X. Secrete ID part is kept hidden by both nodes. The new node A cannot incorrectly assign itself the address of the existing node X to cause a false address conflict because X sends a Type-0xA frame in the reply that contains only the Node ID. However, the probability of a false address conflict is almost zero and equal to $1/2^k$.

Proof of zero probability of conflict attack

The probability (Pc) of false address conflict by new node=1/Total number of Secrete Ids

Pc=1/2^k
Here k=16 bits; hence Pc=1/2^{16} and Pc is near zero. Therefore, even despite the false reply of X or the attempt of A for the conflict of false address, this DAD process successfully provides a unique IPv6 address, still preserving the privacy of the address.

Hence despite the spoofing attack, a new node will successfully assign a unique IPv6 address in this new DAD process.

4.4 EVALUATION

Evaluation of the proposed scheme is performed on three metrics 1) ASR, 2) total added communication overhead, and 3) energy consumption.

ASR is defined according to [74] when a node uses addressing scheme S to assign an IP address in the existence of an attack. If the addressing scheme run n times and m times has succeeded, then the ASR of S is:

ASR=m/n

Total Network Communication overhead (C_{DAD}) added by the proposed DAD process includes the response cost (C$_R$) and broadcast cost (C$_B$), as shown in the Equation (1) where D$_n$ is the number of DAD process repeated for address assignment by a new node. In Case 1 and Case 2, D$_n$ will equal 1, but in Case 3, D$_n$ is greater than 1. C$_B$ and CR are evaluated using Equations (2) and (3), respectively, where N is the total number of nodes, p1 is the payload size in the Type-1 frame, p2 is the payload size in the Type-0xA frame, m1 and m2 is the number of configured and semi-configured nodes returning Type-0xA frame respectively.

$$C_{DAD} = D_n * (C_B + C_R) \tag{1}$$

$$C_B = (N - 1) * (p_1) \tag{2}$$

$$C_R = (N - 1) * (p_2) \tag{3}$$

Total energy consumption (E$_{TOTAL}$) is evaluated using Equation (4).

$$E_{TOTAL} = E_{compute} + E_{DAD} + E_{conflict} \tag{4}$$

where E$_{compute}$ is the energy consumption in generating IID bits, E$_{DAD}$ is the energy consumption in duplicate address detection and E$_{conflict}$ is the energy consumption to resolve the duplicate address. E$_{compute}$, E$_{DAD}$, and E$_{conflict}$ are evaluated by Equations (5), (6), and (7), respectively.

$$E_{compute} = (64 * (E_{mul} + E_{sht})) \tag{5}$$

$$E_{DAD} = \sum_{i=1}^{N-1} (E_{Tx}(l,d) + NB_i * E_{Rx}(l,d)) \tag{6}$$

$$E_{conflict} = D_n * (E_{compute} + E_{DAD} + E_R) \tag{7}$$

where NB$_i$ is the average number of neighbour nodes each node has. The energy consume in sending response by existing node is E$_R$ and calculated using Equation (8). E$_{Tx}(l,d), E_{Rx}(l), andE_Fx$ (l,d) are the transmitting, receiving and forwarding energy consumption and evaluated using Equations (9), (10), and (11), respectively.

$$E_R = (m_1 + m_2) * p_2 * (E_{Tx}(l,d) + E_{Fx}(l,d) * Avg_{hop}) \tag{8}$$

$$E_{Tx}(l,d) = l * E_{elec} + l * \epsilon_{amp} * d^2 \tag{9}$$

$$E_{Rx}(l) = l * E_{elec} \tag{10}$$

$$E_{Fx}(l,d) = E_{Tx}(l,d) + E_{Rx} \tag{11}$$

Table 4.3 shows the rest of the constant parameters for evaluating energy consumption in first-order radio networks.

Table 4.3: Parameters of the first order radio model

Parameters	**Definition**	**Unit**
Eelec	Energy dissipation rate to run the radio	nJ/bit
ϵ_{amp}	Energy dissipation rate to transmit amplifier	pJ/bit/m2
l	Data length	bits
d	Transmission range	m
E$_{mul}$	The energy consumption of multiply operator	nJ/bit
E$_{sht}$	The energy consumption of shift operator	nJ/bit

This work evaluates the performance based on the ASR, total overhead cost added by a new node in the network and total energy consumption during IP assignment. Assessment parameters are shown in Table 4.4, and the ASR, overhead and energy consumption comparison of the proposed scheme is made with the standard [69] and improved DAD [34], as shown in Figure 4.3, Figure 4.4 and Figure 4.5, respectively.

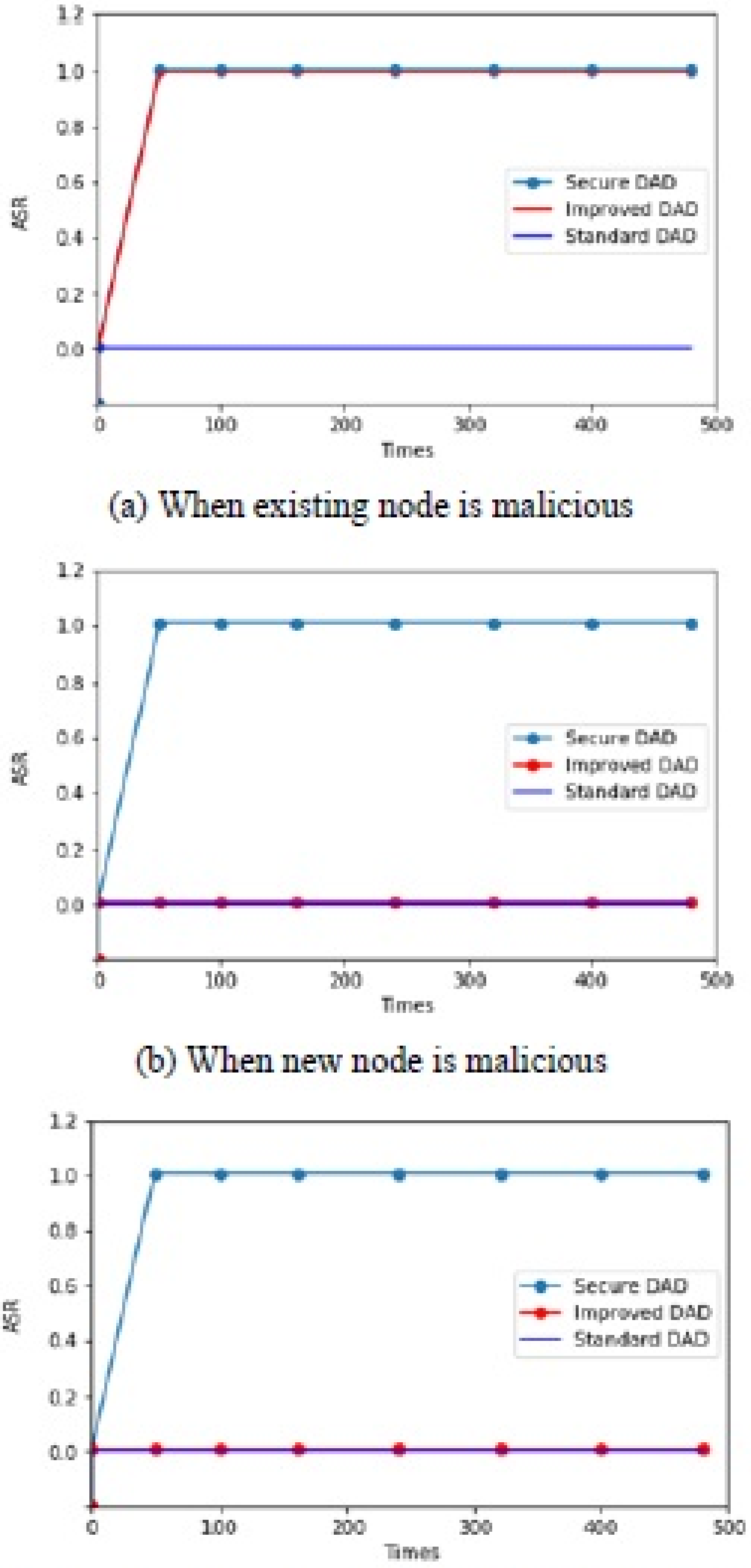
Table 4.4: Simulation environment setting

Parameter	**Definition**	**Unit**
[X, Y]	Network range	[400*400]m2
N	Total number of nodes	[50,500]
d	Transmission range of each node	2∼3m
i, j, k	Size of DAD ID, Secrete ID, and Node ID	6, 16, 32 bits
l	Packet length	320 bits

ASR is evaluated by running the DAD process many times at different intervals under the malicious node attack. The attacking node uses the following method in three different scenarios. In scenario 1, to reply, an existing malicious node spoofs an NA frame to the new node according to the target address of the NS frame. In scenario 2, a new node joining the network is malicious; when the existing node responds NA frame of NS, the malicious node assigns itself an existing address. In scenario 3, when existing and new nodes are malicious, use the above method to attack the DAD process.

From the definition of ASR, it can conclude that if ASR is 0, then the attack is entirely functional, and if ASR is one, then the attack is wholly prevented during DAD.

The experimental results of ASR are shown in Figure 4.3 when DAD is under attack in three different scenarios. The result shown in Figure 4.3(a) depicts scenario 1, indicating that standard DAD cannot handle false replies



(a) When existing node is malicious

(b) When new node is malicious

(c) When new and existing node both are malicious

Figure 4.3: ASR under the different scenario of attack

by malicious. This type of attack causes the DAD process to fail. Thus the ASR of standard DAD is zero, while in the case of secure DAD and improved DAD, only a partial address is available, so the malicious node can not figure out the actual target address. The probability of random spoofing causing conflict is nearly zero. Thus the ASR of secure and improved DAD is nearly 100%. The result shown in Figure 4.3(b) depicts scenario 2, indicating that standard and improved DAD both fail because a new malicious node joining the network always gets the address of the existing node. Thus the ASR of standard and improved DAD falls to zero. While in the case of secure DAD secret ID part is hidden, so the new malicious node can not figure out the existing address. The probability of generating an existing address to cause DAD to fail is nearly zero. Thus the ASR of secure DAD is almost 100%. The result shown in Figure 4.3(c) depicts scenario 3, and it is clear that only a secure DAD process succeeds with ASR near 100%. While standard and improved DAD fails because of malicious nodes.

Above mentioned results indicates that secure DAD has the following advantages over standard and improved DAD.

1- The secure DAD does not share Secrete ID parts; hence it preserves the privacy of nodes.

2- The secure DAD effectively prevents the DAD process from attacking malicious nodes.

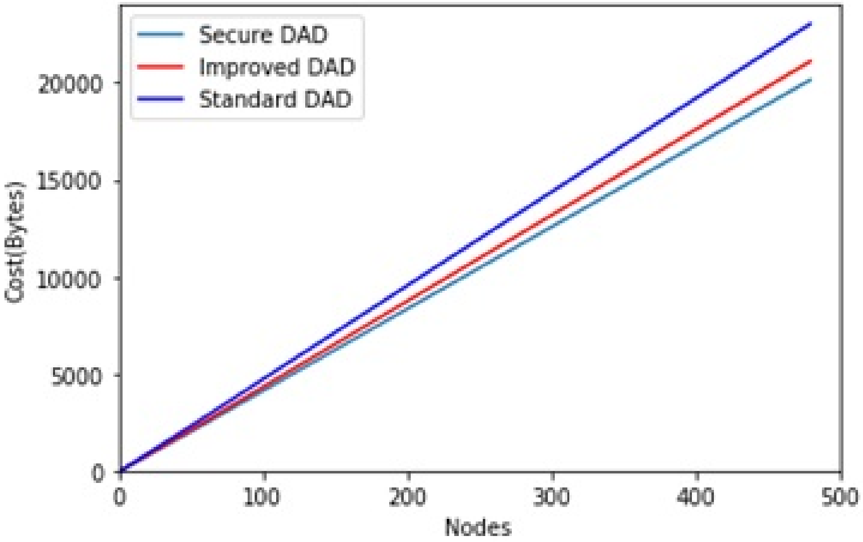


Figure 4.4: Added addressing cost

From Figure 4.4, it can be seen that the proposed secure DAD resulted better than the standard and improved DAD based on total added overhead

addressing cost. The reasons behind the low overhead cost are as follows:
1) Instead of the full IID, only the DAD ID and Node ID parts are used.
2) DAD process is repeated only when the same DAD ID and the Node ID of semi-configured nodes are generated.

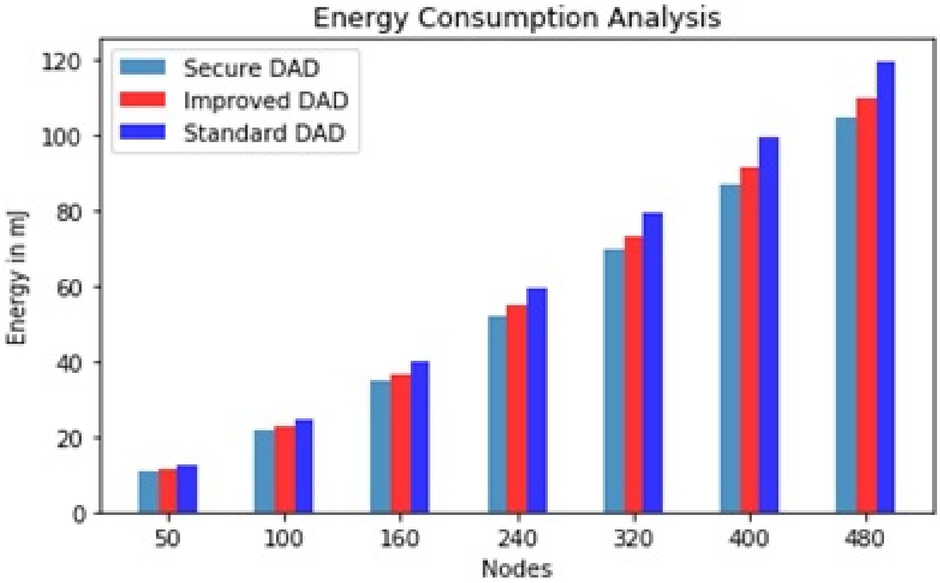


Figure 4.5: Energy consumption

Result shown in Figure 4.5 indicates that the energy consumption of the proposed scheme is less than standard and improved DAD. The main reason behind it is to add less overhead and minimize repetition of the DAD process.

4.5 SUMMARY

With the advancement of IoT technology number of nodes is increasing exponentially, and the use of SLAAC-based IPv6 addressing poses a serious threat to the DAD process and network security. In existing DAD, a new node broadcasts the target address into the network, which allows a malicious node to mislead and disrupt network services. This chapter proposes an IPV6 address scheme with secure DAD to protect the DAD process from the malicious node. In the secure DAD, secrete ID portion of the IID is not shared while the existing DAD broadcasts full IID. This scheme uses the concept of Secret ID, which is hidden during the DAD process. This will help secure nodes' identity from a malicious node and will result in less overhead compared to the existing DAD methodology. In addition, the uniqueness of the IPv6 address of the nodes is also guaranteed in the proposed scheme. Compared with other existing DAD schemes, Secure DAD has an advantage in terms of ASR, added overhead in the network and energy consumption. Using the proposed scheme, higher scalability can be achieved as it costs less overhead in the network.

Most devices and IoT networks have limited resources, such as limited device energy source, memory, processing power, network bandwidth, and so on. In such circumstances, making the best use of limited resources is critical. Hence, in this direction, the next chapter of the thesis presents the literature survey of multipath transport layer protocols, which reveals how to maximise the exploitation of multiple network interfaces available with devices.

Chapter V

A LITERATURE SURVEY OF CMT AND MPTCP MULTI-PATH TRANSPORT LAYER PROTOCOLS

To fulfil the current needs, a large amount of generated data explodes into the network not only by humans but also by self-configured devices such as the Internet of Things (IoT) and machine-to-machine (M2M) communication. It mandates effective QoS services such as throughput, latency, bandwidth and reliability in the network. Currently, many multi-homing devices are equipped with many network interfaces with heterogeneous environment adaptability. Thus, the enhancement of transport layer protocols for multi-path transmission of multi-homed devices is inevitable to fulfil the required QoS services by maximising the exploitation of multiple network interfaces. Hence, this chapter presents different challenges of multi-path transmission with possible handling strategies. It also surveyed innovation related to concurrent multi-path transmission (CMT) and multi-path transmission control protocol (MPTCP) transport layer protocols with its working principles, path characteristics, network environment, and handling of challenges. Furthermore, this work of thesis identifies the future research trend and open problems of multipath communication protocols at the transport layer.

5.1 INTRODUCTION

Nowadays, the support of high-quality video streaming services in a wireless mobile network is very demanding as throughput can be degraded along with the traffic load, attenuation loss, fading, and signal-to-noise ratio. Meanwhile, current mobile devices have a large storage size, high computing power, high-resolution display capability, and multiple sophisticated networking interfaces. We expect these mobile devices to improve the Quality-of-Service (QoS) by simultaneously using multiple networking interfaces. A multi-homed user device such as a smart phone, laptop, tablet, or Internet-of-Things (IoT) device can

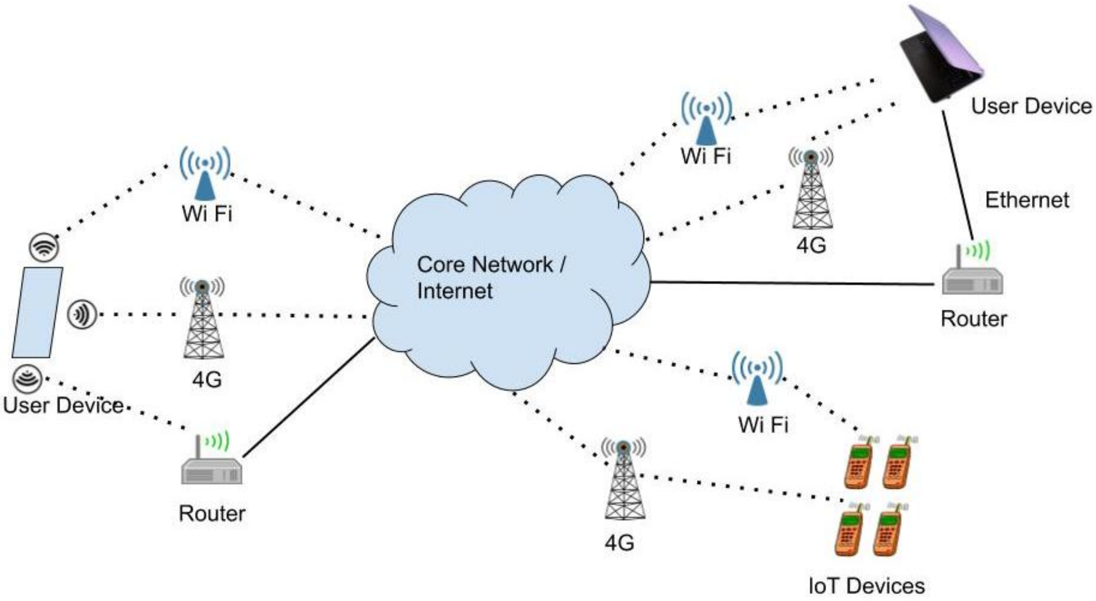


Figure 5.1: Multihoming devices

support multiple networking interfaces such as Wi-Fi (IEEE 802.11), cellular (3G/4G/LTE), and Ethernet. As shown in Figure 5.1, it can be connected simultaneously using numerous network access technologies through different pathways (disjoint paths).

The device's multi-homing feature [78-80]can improve the network's reliability, resilience, load balancing, and fault tolerance to the network. Multi-homing is a cost-effective, technically feasible, and widely accepted capability of user devices. The plethora of multi-homed devices and the advances of the fifth-generation (5G) cellular networks have efficiently utilized the available resources of multi-communication interfaces. The diversity of machine-to-machine (M2M) and IoT-based applications mainly operate in resource-constrained wireless communication environments such as Wi-Fi, radio links, 4G/Long Term Evolution (LTE) networks, etc. In such network environments, multipath transport protocols exploit multiple available network paths and struggle to fulfill the strict QoS requirements for providing higher data rates, low network latency, and high reliability. A solution is the optimal use of the available multiple networking interfaces of multi-homed user devices.

The Transmission Control Protocol (TCP) does not provide multi-homing. In particular, an application can only bind a single IP address to one specific TCP connection with another host. If the TCP sockets-based Application Programming Interface associated with that IP address goes down, the TCP connection is lost and must be reestablished. For this reason, the Internet Engineering Task Force (IETF) standardized the Stream Control Transmission

Protocol (SCTP) [82] to integrate the multi-homing feature into its specification. Then, Iyengar et al. [81] designed the Concurrent Multipath Transfer (CMT) approach for multi-network interface devices to utilize such a feature of SCTP. CMT is based on SCTP and improves throughput, resource utilization, latency, and network reliability (stated as CMT-SCTP). However, CMT-SCTP suffers from severe drawbacks: improper packet scheduling, unnecessary packet retransmission, unnecessary reduction of the Congestion Window (CWND), receiver buffer blocking [17, 85], and so on.

The Multipath TCP working group of IETF introduced the Multipath TCP (MPTCP) [83-84],which allows a TCP connection to use multiple paths to exploit resource usage and increase redundancy. In MPTCP, a multipath connection that contains multiple flows can dynamically be established. The MPTCP transfers data simultaneously over different available sub flows, including IPv4 and IPv6. It has two main functions: (1) path management; and (2) multipath packet scheduling.

The primary task of path management is to establish, remove, and manage those sub flows that can play a part in the end-to-end data transmission. The path management algorithm can dynamically add or delete sub flows to participate in the concurrent transmission. Path management initiates and manages the sub flows, which are part of the same multipath connection. On the other hand, a multipath packet scheduler distributes packets over different paths according to a particular policy. For example, the packet scheduler can aggregate throughput by utilizing all available capacity. Moreover, packet scheduler can reduce latency by choosing low latency paths or can enhance reliability (duplicate packets). Apart from the multipath scheduler, MPTCP has an additional flow management mechanism, namely, Congestion Control (CC), that controls induced network load and avoids congestion.

In a wireless network, the performance of MPTCP is mainly limited due to the long Round-Trip-Time (RTT) and the frequent loss of data packets. For this reason, various multipath transport protocols have been suggested. CMT-SCTP [81-82] and MPTCP [83-84] protocols constitute a boon for multipath data transmission devices. Multipathing solves the problem of single-path insufficiency by combining multiple available pathways to increase bandwidth and throughput.

Over time different multipath approaches has been designed for Transport Layer. The objective of this survey work is to categorize and investigate the salient features of available multipath approaches with their applicability along with performance in different scenarios of deployment. This work adds the following contributions.

- Core issues that arise and their handling in multipath transmission.
- A comprehensive study of the existing MPTCP and CMT-based multipath transport layer approaches.
- A comprehensive evaluation of CMT and MPTCP approaches in terms of working principles, operating environment, path characteristics, and handling of the core issues of multipath communication.
- Comparative study of CMT and MPTCP transport layer protocol.
- Highlight the development of future research directions of CMT and MPTCP transport layer protocols.

The rest of the chapter is arranged as follows. Section 5.2 highlights the core issues and their handling by multi-path protocols. Section 5.3 presents the key MP-TCP and CMT-SCTP multi-path transport layer protocols with their comparative performances in different deployment scenarios. Section 5.4 presents the finding of the survey works. Section 5.5 provides the future research directions, and finally, section 5.6 summarise the chapter.

5.2 CHALLENGES AND HANDLING

It seems warranted that multipath communication will increase applications throughput by taking advantage of additional network resources. Unfortunately, it did not work efficiently in the case of multi-path transmission due to several challenges. This section presents the primary performance affecting challenges and their handling by MP-TCP and CMT-SCTP developed in recent years.

5.2.1 Scheduling

Concurrent data transmission over available multiple interfaces does not necessarily meet the expectations. Different paths with varying properties, such as the heterogeneous nature of transmission delay and bandwidth, cause out-of-order delivery of data packets, reducing the network's required performance. In multipath transmission, intelligent scheduling of data packets over available multiple interfaces is necessary to improve the overall throughput as well as the

Table 5.1: Summary of Scheduling Schemes in Multipath Transmission

Scheme	Year	Scheduling Policy	Description
Xu et al. [86]	2013	Quality Aware	More traffic amount is scheduled to a path in which the quality coefficient is higher and it is calculated based on parameters of each path such as loss rate, transmission rate, congestion, etc.
Deng et al. [132]	2015		
Cao et al. [136]	2017		
Wallace et al. [127]	2012	Delay Based	Scheduling of data is carefully decided based on the data transmission delay of each path and the most widely used scheduling policy.
Sarwar et al. [125]	2013		
Kuhn et al. [124]	2014		
Yang et al. [108]	2014		
Le et al. [109]	2017		
Saavedra et al. [119]	2017		
Sou et al. [141]	2017		
Sharma et al. [128]	2019		
Ni et al. [110]	2015	Feedback	Scheduling of data is based on feedback information from SACK to future scheduling options.
Cao et al. [137]	2016		
Huang et al. [116]	2015	Packet Order Prediction	Scheduling is based on a prediction of packets arrival order.
Ferlin et al. [118]	2017	Load Balancing	The scheduler maintains Data packets flow load balance between each sub-flow of multipath transmission.
Delgado et al. [142]	2017		
Lee et al. [140]	2019		
Oh et al. [87]	2015	Queuing Status	Scheduler decides data scheduling based on queuing delay of individual sub-flow.
Pokhrel et al. [143]	2017		
Eklund et al. [126]	2018		
Shailendra et al. [95]	2013	Bandwidth Aware	Data packets scheduling is decided based on the available bandwidth of each path.
Jiyan et al. [133]	2016		
Zhu et al. [115]	2017		
Wu et al. [139]	2014	Loss Aware	Schedule data packets according to packet loss and variations in loss across available multiple paths.
Ni et al. [165]	2014		
Jiyan et al. [134]	2015		
Dong et al. [121]	2017		
Liu et al. [138]	2019		
Deng et al. [131]	2016	Energy Aware	Data packets are scheduled according to the energy consumption of available multiple paths.
Wu et al. [130]	2017		
Wu et al. [135]	2017		
Kimura et al. [117]	2017	Hybrid	Adopts multiple scheduling criteria.
Verma et al. [129]	2017		
Lu et al. [146]	2018	Priorities Aware	Data packets are scheduled for high-quality interface links.

performance of the network. One of the critical challenges of packet scheduling and path selections has the most considerable effect on system performance [106]. Over a period of time, a lot of multipath transmission methods have been developed to maximize the optimality of the network by using different scheduling policies. These key scheduling policies are summarized in Table 5.1 with their scheduling type and description.

5.2.2 Loss and Retransmission

When multi-homed devices transmit generated data over the different multiple paths, data may be lost for many reasons (network error, path disconnection, channel error, etc.) Iyengar et al. rectified the retransmission issue in CMT and proposed a Split Fast Retransmit (SFR) scheme. However, Iyengar et al. [82] suggested another solution for the congestion window update problem. Xu et al. [86] suggested a path quality-based data transfer approach transmit data packets over multipath and minimize retransmission. Cue et al. [100] identified the loss problem and path delay and suggested Fountain code-based

Multipath TCP (FMTCP), which minimizes the effect of different path delays and losses. However, Peng et al. [101] proposed a fluid concept for a large group of MP-TCP schemes which improve TCP-friendliness, responsiveness, and window growth.

5.2.3 Congestion Window Growth

Transport Layer uses two state variables to keep up the transmission between the sender and receiver. The first one is the Congestion Window (cwnd), and the second one is the Slow Start Threshold (ssthresh). The sender starts sending data with the initial cwnd value and keeps on increasing exponentially until it reaches up-to ssthresh. The main objective of cwnd is to limit the sender to sending more than the network capacity in the current load condition. The objective of modifying the cwnd is to adopt the current network status. Various authors have suggested different types of cwnd growth policies to adapt network congestion status. Shailendra et al. [94] suggested an MPSCTP method to simultaneously transmit data packets over multiple paths. However, Shailendra et al. [95] proposed a bandwidth estimation-based resource pooling (BERP) congestion control (CC) algorithm to enhance the throughput and performance of multipath communication. Xu et al. [96] suggested that cross-layer fairness-driven SCTP-based CMT improve video data transmission and maintains fairness with competing flows. However, Peng et al. [101] identified the fairness problem of multipath transmission and suggested a fluid concept for MP-TCP algorithms to improve the stability, and uniqueness of the system. Xu et al. [114] studied networking problems and presented a new design of a deep reinforcement learning-based control framework which realizes network experience-to-control congestion on multi-path TCP. Zhu et al. [115] suggested a new cwnd growth policy that uses a bandwidth estimation approach based link increase algorithm to enhance the throughput of multi-path communication. However, Huang et al.[116] identified the three multipath problems unordered data delivery at the receiver side, the importance of packets being different, and the utilization of available multipath bandwidth. To overcome the above problem, the author suggested an adaptive ordering predicting scheduling (AOPS) scheme to minimize the first two problems. It uses the packet arrival order at the receiver side to adapt the transmission area of each path.

5.2.4 Receiver Buffer Blocking (RBB)

In multipath communication, a sender transmits data concurrently over multiple paths to utilize the available network resources. However, each available path has different transmission latency and bandwidth. Therefore, the receiver receives out-of-order data. The destination has a limited size receiver buffer to reorder the received data. As the frequency of unordered data increases, the receiver buffer gets blocked. This type of problem is known as the RBB problem. Various authors have suggested different techniques to alleviate the RBB problem for multipath communication.

Iyengar et al. analyzed the retransmission issue in CMT and proposed the SFR scheme to improve the performance. However, CMT uses the equal data distribution policy to transfer data packets over the multiple available paths. It creates an RBB problem due to dissimilar transmission latency and bandwidth of different paths. Abdrabou and Prakash [89] analyzed the MPTCP multihomed wireless interfaces, where one interface is connected to a WiFi network and the second interface emulates a 3G or 4G link. The authors suggested that the MPTCP coupled CC algorithm can transfer more data on the WiFi link than the dedicated link at a limited receiver buffer. The CMT suffers from the buffer blocking problem, while every path has a different transmission rate and delay. Yilmaz et al. [190] proposed a non-renewable selective acknowledgement (NR-SACKs) to free the receiver-side buffer. The acknowledgement strategy simply deletes the segment from the receiver buffer without considering the cwnd growth and reordering. Natarajan et al. [193] suggested a new state named Potentially-Failed (PF) to mitigate the RBB due to path failure. This state shows whether the destination is reachable or not. Thus, all available new data will be forwarded to another alternative path. However, in [90], Xu et al. suggested the network coding-based CMT (CMT-NC) minimize the RBB problem in CMT-SCTP in the heterogeneous network environment.

5.2.5 Excessive Network Congestion

: One of the inefficiencies of multipath communication is excess data transmission due to multiple sub-flow management [104], increased acknowledgement packets [17], and frequent retransmission [157-158]. It mandates multipath protocols to double ensure before generating any data packets into the network to avoid excessive congestion.

5.2.6 Long Round Trip Time (RTT)

Variations in RTT of the different paths may increase out of the ordered arrival of the data packet at the receiver; hence sender pour more duplicate data packets into the system. More duplicate packets in the network system increase congestion and longer RTT and lead to the system's poor performance. A longer RTT path must be taken care of while transferring data to mitigate expired and unordered packets' arrival.

5.2.7 Communication Channel Impairment

Most communication interfaces in multi-homed devices are wireless and prone to error from external interferences. Examples of such interfaces are IEEE802.11 (Wi-Fi), IEEE802.15.1 (Bluetooth), Zigbee, LTE, etc [148]. The presence of external interference, interruption, path loss, and multipath fading may force the device to delay the transmission due to the wrong detection of the busy interface, packet loss, and jitter and consequently degrade the performance of the multipath protocol.

5.2.8 Heterogeneous Communication Standards

Standards for heterogeneous networks vary according to the adopted strategies of network carriers; for instance, retransmission policy and packet loss handling in the 3G network is different from 4G [149]. Also, when 4G is compared to Wi-Fi, there is a difference in loss rate, RTT, and bandwidth due to different standards adopted by network carriers. Designing generic multipath protocols in such an environment is difficult without modifying existing standards. Many organizations, such as IEEE and IETF, are working to provide common standards for security, privacy, communication, and architecture; still, more effort is needed.

5.2.9 Packet Reordering

Packet reordering at the receiver end is one of the major issues in communication. It rarely occurs in single-path transmission but frequently occurs in multipath transmission. Reordering in multipath transmission occurs due to packet loss and different delays of the different paths. There are many solutions that exist to handle it; in [88] author discussed four packet reordering solutions for MPTCP protocols. A packet reordering solution for the wireless environment is discussed in [93]. In [94-95], the authors presented reordering solutions for SCTP-based protocols.

5.2.10 Fairness

Another concern in multipath communication is fairness among multiple traffic flows. Multipath-based data transmission may acquire high bandwidth share than other competing data transmission flows [96-97]. So it is required to design a friendly flow control mechanism among multiple data flows to ensure proper sharing of network resources. Multipath implementation based on the estimation of bandwidth utilization, data rate and implementation guidelines [98] can minimize fairness issues.

5.2.11 Stream Handling

The single data stream is transmitted via multiple sub-flows or interfaces in multipath communication. But intermediary devices (Middlebox) consider each sub-flow single connection. A gateway may change the stream by adding or removing bytes to payloads and in a result, changes the boundaries of the data stream [105]. The multipath protocol should have provisions to detect these changes and fallbacks. A solution to this problem is an additional checksum on a payload with every segment of multipath communication [103]. This checksum allows for detecting any possible modification to the data stream.

5.2.12 Head of Line (HOL) Blocking Problem

To ensure ordered delivery of data packets receiver held packets in the buffer until lost packets were received. This situation is called Head of Line Blocking (HOL) [111-112]. Due to multiple sub-flow in multipath communication, HOL blocking worsens, thus reducing performance. This issue can be minimized by carefully monitoring buffers occurring at different layers [144] and RTTs of each sub-flow [145]. A forward Error Correction (FEC) coding scheme has been proposed to handle the HOL blocking problem to recover from the loss of data packets at the receiver end [161-164]. Other solutions to avoid HOL blocking by sending lost packets via faster sub-flow.

5.2.13 Pareto-optimality

Upgrading existing single-path communicating devices to multipath may degrade the performance of other devices without any performance improvement; this is reported in [99,113, 154] as not the Pareto-optimality issue in multipath communication. It is a challenging task to design multipath communication as Pareto-optimal. One such example, [152] is not Pareto optimal while [153] is Pareto optimal.

5.2.14 Security

With the invention of multipath communication number of new security threats arisen. From the threats identified in [150], a multipath communication mechanism should provide secure handshaking, secure addition and removal of multiple sub-flows, and prevention from flooding and hijacking attacks. An additional mechanism should be placed to tackle denial-of-service (DoS) attacks, such as reset attacks and SYN cookie misuse. Applications also suffer from multiple IPs during multipath communication; a guideline is given in [149,151] to deal with such problems. Another security breach that may arise from traffic splitting is the broken trust model. For example, analyzing intrusion detection and data leak prevention by the sniffer, firewall, or gateway may become problematic in multipath transmission [160].

5.3 MULTIPATH TRANSPORT LAYER PROTOCOL

This section presents the state-of-the-art multipath approaches of CMT-SCTP, MP-TCP, and various Internet engineering task forces to handle multi-homing, multipath scenarios, their applications, issues, and solutions. This section begins with the basic concept of multi-homing, its applications, and its major advantages.

5.3.1 Multi-homing and Multipath approaches

Multi-homing and multipath approaches are receiving more research attention due to exponential growth in devices with multiple network interfaces (examples: IoT devices, smartphones, laptops, tablets, etc.). Multi-homing is on the rise as it is economically, and technically feasible. It is globally accepted when reliability, fault tolerance, and load balancing are the major requirements of the network. A multi-home device can be connected simultaneously through multiple network access technology along with multiple paths (disjoint paths) to increase reliability and fault tolerance. However, multi-pathing provides a solution to single-path deficiency by exploiting available multiple paths to aggregate bandwidth and increase throughput [167,168,169].

The use of multiple paths in mobile devices not only enhances the reliability and fault tolerance of the network but the user may also be benefited from economical service plans (e.g. when 3G and Wi-Fi services are available then the user can choose the best cheapest plan). The recent implementation of the multipath transport protocol by SAMSUNG GALAXY S7 and Apple iOS7 (https://support.apple.com/ en-us/HT201373) further encouraged the multipath protocol optimization at the transport layer. The data centre is another important application of a multipath transport protocol. Multipath transport protocol enables numerous connection architectures in the data centre, that could not be supported by single-path transport protocols. For example, Amazon EC2 gets three times better throughput than single-path by utilizing different bandwidth paths [170,171]. Apart from these applications, the major advantages of multipath transport protocols are as follows.

Load balancing: Load balancing is usually done by the network layer where a network operator routes the data according to different path load statuses. However, network layer load balancing approaches leads to network unstable [172]. On the other hand, transport-layer load balancing gradually increases the traffic rate on each available path over a period of several RTT and balances the traffic on each path in more stable fission.

Resource pooling: Resource pooling of different multiple paths at the transport layer eases better utilization of path characteristics (bandwidth, delay, and RTT) than a single path [173]. Transport layer resource pooling allows the network to dynamically allocate available resources to fulfil the current traffic requirement. In single-path applications, when a primary path fails, it causes an interruption in application traffic. On the other hand, multipath may shift faulty path traffic to other available paths.

Diversity: Network diversity is a technique; deployed in the data centre network, wireless network, and the Internet to get better resource utilization. A study [174] shows that in 30-80% cases, a different path with better bandwidth and transmission delay is available as compared to the default path. Therefore, reliability and bandwidth aggregation can be achieved by utilising the diversity of the multipath. The path diversity is very supportive in reducing packet loss [175] and multimedia applications' end-to-end delay [176].

Role in the future Internet architectures: The application of multipath at the transport layer enables to switch from one access technology to another (3G to Wi-Fi) [177] and have planned to play a crucial role in the advancement of future Internet technology and Cloud Computing. Apart from that, the 5G technology vision is to use concurrent multipath data transfer technology to fulfil high bandwidth and fewer delay requirements. Moreover, using different multiple paths achieves better throughput to fulfil the need for Cloud.

Security: In multipath transmission, data is transmitted via multiple independent sub-flow, making it difficult for intruders or malicious entities to intercept or monitor the data as individual path carries only part of the whole data [16].

High Throughput: By exploiting multiple network paths, a high data transmission rate is achieved, hence increasing the throughput of the system, which is essential in many critical applications [166].

5.3.2 Multipath Transport Layer Protocols

Transport layer protocols generally categorize into connection oriented and connectionless protocols. In this work, the main focus is on the study of connection oriented transport layer protocol. The multipath connection-oriented transport protocols can further classify into two categories, one is CMT based on SCTP and another one is MP-TCP based on TCP.

SCTP and CMT: The SCTP specification was the first multipath transport protocol proposed in the RFC 2960 [178] in 2000 (now obsolete), and then it was later updated in RFC 3309 [183] and RFC 4460 [184]. The present SCTP protocol description is in RFC 4960 [81] and was adopted by IETF in 2007. The SCTP is message-oriented, multi-streaming, and multi-homing including, a reliable, connection-oriented, window-based congestion control (CC) service. The SCTP allows a device to create a logical connection establishment over the different multiple interfaces having a unique IP address. The SCTP also offers ordering and reliability in a stream, mitigate SYN attacks and the use of SACK is compulsory. Initially, SCTP was designed to uses the multistreaming and multi-homing characteristics to enhance the reliability of the communication network when the main path is unreachable because of congestion or connection failure. Later, load balancing and bandwidth aggregation become the primary objective of SCTP. Thus, several efforts made by various researchers to enhance the performance of the SCTP in terms of load balancing and bandwidth aggregation. A modified version of SCTP named BA-SCTP [179] was presented to aggregate the existing bandwidth over the multiple interfaces. However, in Westwood SCTP (W-SCTP) [180], enhancement of the SCTP protocol is proposed that aims load balancing across multiple interfaces using bandwidth-aware scheduling. An extended SCTP, named Load Sharing SCTP (LS-SCTP) [181-182] was proposed which is capable to aggregate the bandwidth and maintain load balancing among multiple active transmission paths. Another extension of SCTP was proposed in [185] to mitigate the effect of packet loss in the lossy environment and it also limits the redundant data transmission over a different path to minimize the congestion in the network. In [186] Selective-Redundancy Multipath Transfer (SRMT) scheme is proposed, which uses the primary path to send data and the secondary path to transmit redundant data to mitigate the degradation of video data quality. In order to make reliable SCTP flexible for video streaming, in [187] the Partially Reliable SCTP (PR-SCTP) and in [188] additional rules are specified. Ye et al. [192] proposed an autonomous per Path Congestion Control SCTP (IPCC-SCTP) scheme which reduces the false retransmission. It applies the concept of a unique path sequence number (PSN) for every path; it decides the unordered or ordered delivery of data packets for each receiver. In [196] author proposed Wireless Multi-Path SCTP (WiMP-SCTP), which uses data-stripping and data-duplicating mode for transmission in the wireless environment to aggregate bandwidth.

Another milestone in the development of SCTP is CMT proposed by Iyengar et al. to transfer the data packets simultaneously over the different multiple paths. Most CMT solution enhances the bandwidth utilization, robustness, throughput, and resiliency of the network. The CMT uses a round-robin policy to schedule data chunks over multiple paths. However, each path has a dissimilar network characteristic (bandwidth and delay) and the CMT data scheduling policy does not include path delay and bandwidth. As a result, the destination receives unordered data. CMT uses the limited-sized receiver buffer to re-ordering of the received data packet.

However, as the unordered data packet increases, the receiver buffer gets blocked because the destination does not pass the data packet to the upper layer until it received the missing packet.

Later, Iyengar et al. identified the retransmission issue of CMT and proposed a solution called the SFR algorithm. The SFR maintains the records of the highest TNS Ack by the receiver. It improves the performance of the CMT in terms of retransmission of data packets. Iyengar et al. also suggested another algorithm, which maintains the separate cwnd, for each destination to grow separately. It uses the independent CUMACK for each destination and adjusts the cwnd according to the received CUMACK. CMT also decreases the acknowledgement traffic by delaying acknowledgement until at least two can be sent collectively. However, CMT sends an immediate acknowledgement, when it receives unordered data packets. Because of frequent un-order data delivery, the reordering acknowledgement increases regularly.

To reduce the acknowledgement traffic, Delayed acknowledgement for CMT (DAC) was also incorporated into SFR. Yilmaz et al. [190] proposed the NR-SACK scheme to the free receiver-side buffer to mitigate the RBB problem because of unordered data packet delivery. The acknowledgement scheme simply omits the segment without considering the reordering and cwnd growth. Most of the concurrent schemes such as CMT-DA [134], CMT-QA, and CMT-CA [189] are based on basic CMT. These CMT-based schemes use round-robin scheduling for data transmission among multiple paths. However, each path has a different transmission delay and bandwidth. Hence, the data packet received unordered at the receiver. Due to unordered data packet delivery, CMT faces SACK overhead, unwanted retransmission, receiver buffer blocking, unnecessary cwnd reduction, and improper data chunk scheduling.

Xu et al. suggested a path and Quality-aware adaptive CMT (CMT-QA) scheduling approach for heterogeneous wireless networks. The main goal of this scheme was to reduce out-of-order delivery of data packets by reducing the reordering delay and unnecessary fast retransmissions. The authors state that CMT-QA achieves enhanced performance when multimedia data is transmitted over the different multiple paths. However, it suffers from fairness [96] issues towards other TCP flows. In [90], the authors further improved CMT-SCTP in a heterogeneous network and outlined CMT-NC. Arianpoo et al. [91] suggested another improved network coding-based CMT protocol (coded SCTP-CMT) which utilizes Q-learning approaches [191]. Wu et al. [134] proposed a new distortion-aware CMT (CMT-DA) approach to enhance the streaming of video quality in the wireless environment. This approach mitigates the distortion by reducing the data packet loss rate of video streaming. In another work, Wu et al. [189] outlined a content-aware CMT (CMT-CA) approach, which includes the analysis of video contents to schedule the data for enhancing the quality. Dreibholz et al. [104] introduced a sender buffer splitting approach that divides the sender buffer based on the number of multiple paths. The author claims that this scheme improved the receiver's buffer blocking, but still suffers from the local blocking because of path inequality.

Natarajan et al. identified the receiver buffer problem arising because of path failure and described a new condition called potential failure (PF) state [193] for its solution. This state shows that the destination cannot be reached by this path due to network congestion or connection link failure so all new data packet is transmitted to the available alternate path. Shailendra et al. outlined an MPSCTP [94] as a solution for reordering and crippled cwnd growth and claims for better throughput and retransmissions compared to basic CMT. The authors later optimized MPSCTP [194] to incorporate the data transmission rate on every path based on the total latency of the path. This scheme reduces the average chunk delay on different paths but still suffers from problems of available bandwidth usage due to its uniform bandwidth sharing policy. Shailendra et al. further introduced the Tx-CWND retransmission destination selection scheme [195] to mitigate the RBB of MPSCTP.

Jiyan W. et al. proposed Energy and Goodput Optimized CMT (EPOC) [197] solution to deliver video streaming over different multiple wireless paths. It proposed two models, the first one is an analytical framework to establish a relationship between energy consumption and goodput and the second is a joint rate allocation scheme and forward error correction coding to reduce energy consumption with required goodput. The author claims that EPOC achieves better goodput, energy consumption, and distortion. In [138] author presents Loss-Aware CMT (CMT-LA) which schedules packets according to packet loss and loss rate of every path to aggregate bandwidth and parallel transmission. In the result, the author claims CMT-LA reduces reordering delay and unnecessary retransmission more than classical CMT. Shaowei L. et al. proposed a selective retransmission-based CMT mechanism (CMT-SR) [198] to improve retransmission. CMT-SR monitors and analyzed the delay and bandwidth of each path and estimates the arrival time of packets. CMT-SR uses a pull-based and push-based mechanism to identify packet loss on time and it prioritizes the retransmission of important parts of data. The experimental result shows that CMT-SR achieves better quality and delivery of data. Verma L.P. et al. [129] proposed an adaptive data packet scheduling for CMT (A-CMT), it uses path delay and bandwidth to identify path conditions and schedule data chunks accordingly. This method improves average performance in terms of throughput of the network system up to 13%. In [199] author pro-

Table 5.2: SCTP and CMT Transport Protocols

Transport Protocol	**Year**	**Based on**	**Network**	**Path**	**Problem to Address**
SCTP [81,178,183]	2000, 2002, 2007	Multihoming	General	General	Fault tolerance and resource aggregation
PR-SCTP [187]	2004	bandwidth aggregation	General	General	Spurious retransmission
BA-SCTP [179]	2004	bandwidth estimation	General	General	Scheduling, Fairness
W-SCTP [180]	2004	bandwidth estimation	General	Disjoint	balancing load
LS-SCTP [181-182]	2004	path quality	General	General	Spurious retransmission
m-SCTP [202-203]	2005, 2007	Soft handover	Mobile	General	Resource Pooling
CMT-SCTP [82]	2006	Retransmission policies, Cwnd Updates	General	Independent	Cnwd Growth, Retransmission
WiMP-SCTP [196]	2007	aggressive failure detection	Wireless	Independent	Packet reordering
DAR-SCTP [204]	2007	aggressive failure detection	General	Independent	Fault tolerance
cmpSCTP [205]	2008	path quality	General	General	Packet reordering
mSCTP-CMT [206]	2009	dwelling time, available bandwidth ratio and round-trip time	Wireless	Disjoint	Packet reordering
CMT-PF[193]	2009	aggressive failure detection	General	General	Retransmission, Cnwd Growth
FPS-SCTP [207]	2010	estimation of arrival times	Mobile	Disjoint	Packet reordering
WM2-SCTP [208]	2010	QoS of each sub-flow	Wireless	Disjoint	Resource Pooling
Yilmaz et al. [190]	2010	NR-SACKs, Delay	General	General	Throughput
Dreibholz et al. [104]	2010	buffer size and splitting	General	Asymmetric	Packet reordering, Receiver Buffer Blocking
CMT-SCTP[212]	2011	optimized buffer handling	General	General	Packet reordering
CMT-SCTP[213]	2011	bandwidth estimation	General	Asymmetric	Resource Pooling
CMT-SCTP[214]	2011	bandwidth estimation	Wireless	Asymmetric	Resource Pooling
CMT-QA [86]	2013	path's data handling capability	Wireless	Independent	Packet reordering, Spurious retransmission
Cao et al.,[209]	2014	cwnd, load sharing	Wireless	Asymmetric	Fairness, Load Sharing
DAPS[124]	2014	round-trip time	Wireless	Asymmetric	Receiver Buffer Blocking
Cao et al.[210]	2014	receiver-based sending rate estimator	Wireless	Independent	Fault Tolerance
Okamoto et [185]	2014	Bi-casting only important packets	Wireless	General	Spurious retransmission
CMT-DA [134]	2015	utility maximization theory, path status estimation	Wireless	Independent	Throughput
Xu et al.[96]	2015	path quality, window-based mechanism	Wireless	General	Fairness, Reordering
Cao et al.[211]	2015	cognitive approach	Wireless	General	Fairness, Cnwd Growth
MPSCTP [94,194-195]	2011, 2013, 2015	additional sequence number, bandwidth estimation	General	Independent	Reordering
CMT-CQA[136]	2015	QoE path history information	Wireless	Asymmetric	Cnwd Growth, Fault Tolerance
CMT-CA [189]	2016	Markov decision process, feedback channel status	Wireless	Independent	Cnwd Growth
DaSilva et al.[186]	2016	Secondary path used to send redundant data	General	General	Spurious retransmission
CMT-NC [90]	2016	network coding, group-based transmission	Wireless	disjoint	Spurious retransmission, Receiver Buffer Blocking
Arianpoo et [91]	2016	Q-learning and logistic regression	Wireless	Disjoint	packet reordering, receiver buffer blocking
A-CMT [129]	2017	path delay and bandwidth	General	General	Cnwd Growth
CMT-EA[197]	2017	forward error correction coding and rate allocation	Wireless	General	energy conservation
CMT-SR[198]	2017	bandwidth and delay	General	General	Spurious retransmission
Arianpoo et [199]	2017	distributed Q-learning mechanism	Wireless	General	Fairness
Eklund et [126]	2018	path characteristics, queuing status, and data flows	General	Independent	queuing status and data flows
CMT-VR[215]	2018	packet priority and rate less Raptor coding	Wireless	General	Spurious retransmission
CMT-LA[138]	2019	packet loss and loss variation	Wireless	General	Packet reordering, Spurious retransmission
BRCPD [216]	2019	buffer awareness, frame-level rate control	Wireless	General	Loss Rate
CL-SCTP [217]	2019	Overdue Messages, Redundant Frames	Wireless	General	Spurious retransmission

posed Reinforcement learning (RL) based CMT to improve the fairness issue towards other sub-flow. Table 5.2 summarizes the key SCTP-based algorithms and approaches to multipath transmission.

Multipath TCP (MP-TCP)

MP-TCP is another main connection-oriented protocol that supports multihoming, similar to SCTP. MP-TCP mainly serves to distribute traffic on multiple routes. MP-TCP provides transparency between the top layer (application) for multiple connections. Furthermore, MP-TCP fully supports middle-boxes integration in today's Internet architecture [97-98,168, 218-219]. MP-TCP provides better performance than traditional TCP and SCTP, with data segments tearing mid-segments in the modern architecture of the Internet. As a result, MP-TCP provides better deployment capabilities and performance. In MPTCP, a single tokenized session is divided into multiple sub-flow with an option to differentiate between PMTCP and TCP connections. Data packets use two different sequence numbers for lost detection and packet reordering at the receiver end. In Table 5.3 a summary of key MPTCP algorithms is presented. In recent years, many of the uncoupled (independent CC between sub-flows) multipath transmission strategies [196,221-222] were introduced. On the other hand, the policy of controlling congestion independently leads to unfairness issues during transmission. To overcome this problem, MP-TCP uses an adaptive coupled CC policy by appropriately modifying the congestion window growth policy with respect to the network state of each sub-flow [152,170]. Additionally, Linear Systematic Coding Based MPTCP (SC-MPTCP) [222] infers the characteristics of coupled CC policy that outperforms MP-TCP. Nevertheless, these advanced coupled algorithms did not consider the actual state of the network (loss of packets either due to congestion or due to noisy wireless channels [223-225]) hence leading to performance degradation. Khalili et al. [99] suggested that MP-TCP does not care about the optimal Pareto allocation policy, and resolved the issue through a linked increases algorithm (LIA). The authors also identified the fairness issue and lower channel usage associated with the MP-TCP protocol and structured an opportunistic linked algorithm (OLIA) with respect to the window growth adjustment strategy. Their approach provides both the best resource pooling and responsiveness that traditional LIA policy could not fulfil. Peng et al. [226] recommended an effective fluid-based model for a large class of MP-TCP algorithms that alleviates the problems such as uniqueness, existence, and stability associated with the designing part of the CC algorithm concerning MP-TCP. Their approach is concerned with performance metrics such as TCP-friendliness, receptiveness, and window (congestion) variations. Moreover in [101], the authors further claim to optimize the performance of MP-TCP CC strategies by designing a new Balanced link adaptation (Balia) scheme. This scheme asserts to manage a good balance between TCP-friendliness, window oscillations, and receptiveness performance metrics. Whereas, these schemes did not consider the nature of the wireless channel and visually halved the size of the congestion window, which greatly affects their performance in the wireless environment.

Ferlin et al. [227] proposed shared bottleneck detection (SBD) scheme for MPTCP, called MPTCP-SBD. MPTCP-SBD dynamically coupled/decoupled sub-flows based on the shared/non-shared bottleneck link detection strategy. Additionally, authors in [228] extensively investigated the effects of multipath scheduling over delay-susceptible applications (e.g., live-streaming, gaming, and video conferencing). The authors in [17] surveyed insight into the details of routing over multiple paths and traffic splitting problems. Moreover, they present in-depth details of improving the network's performance by organizing multipath technology across networks. However, in [160], the authors present a holistic view of the issues of multipath traffic splitting concerning aspects of layers. Cao et al. [229] identified that the existing multipath algorithms gain only coarse-grained load balancing of congestion status using packet losses and propose an algorithm based on the congestion equality principle to handle it. They develop a queuing delay parameter-based algorithm that uses packet queuing delay to manage congestion and achieve fine-grained load balancing. Oh, and Lee [87] suggested a novel MP-TCP scheduling policy concerning path delay and receiver buffer. This scheme estimates unordered packets based on performance differences of individual sub-flow and accordingly schedules packets to each sub-flow. This policy efficiently adjusts the trade-off between network throughput and delay performance. Xu et al. [232] proposed pipeline network coding-based MPTCP (MPTCP-PNC) to reduce unnecessary coding-encoding delays and bandwidth misuse in the existing coding-based system. The MPTCP-PNC uses innovative, economic coding, quality-based delivery planning and related data transmission policy to improve overall system performance. Cui et al. [100] presented FMTCP to mitigate the dependency between the individual sub-flow and neglect the effect of a bad-performing sub-flow on other sub-flow in multipath transmission. The FMTCP uses fountain codes to efficiently manage the variable characteristics of different multiple paths.

Table 5.3: MPTCP Transport Layer Protocols

Transport Protocol	**Year**	**Based**	**Network**	**Path**	**Problem to Address**
MPTCP [97]	2011-2013	Simultaneous transmission over multiple sub-flow	General	Disjoint	Bandwidth aggregation
NC-MPTCP [111]	2012	network coding, compensating the lost packets	General	General	receive buffer
Hassayoun et al. [243]	2012	Retransmission	General	General	Packet reordering
QoS-MPTCP [236]	2012	partial reliability	General	General	network availability and QoS
Peng et al. [226]	2013	fairly allocation of bandwidth	General	General	Fairness, RP
Khalili et al. [99]	2013	optimal resource pooling and responsiveness	General	General	Pareto-optimality
Coudron et al. [244]	2013	opportunistic linked-increases	Cloud	Independent	Pareto-optimality
Van der Pol et al. [240]	2013	Simultaneous use of multiple paths	Open Flow	General	Link Failure
A-MPTCP [241]	2013	Additional sub-flow creation mechanism	CloudNet	General	Transmission Delay
CWA-MPTCP [233]	2013	end-to-end path delay	Wireless	Independent	receive buffer

SC-MPTCP [222]	2013-2014	linear systematic coding	General	General	retransmissions, receive buffers
Yang and Amer [108]	2014	in order arrival scheduling	General	General	receive buffer
FMTCP [100]	2015	Fountain code-based	General	Disjoint	higher total goodput, lower delay
Ni et al. [110]	2015	feedback information from SACK	General	Independent	receive buffer, enhanced throughput
Le and Bui [109]	2015	forward-delay-based packet scheduling	General	General	receive buffer, enhanced throughput
AMTCP [242]	2015	addition of a dynamic number of the sub-flows	datacenter	General	Throughput
Ferlin et al. [227]	2016	shared bottleneck detection	General	General	Fairness, Throughput
Jiyan et al. [131]	2016	Energy-aware and Prioritise frame Scheduling	Wireless	Independent	Goodput, Delay, Energy Consumption
C. Xu et al. [102]	2016	pipeline network coding	Wireless	General	Delay, Bandwidth utilization
Oh et al. [245]	2016	feedback-based path failure detection	General	General	retransmissions, receive buffers

Jiyan et al. [133]	2016	priority-aware scheduling and forward error correction	Wireless	General	end-to-end delay, bandwidth utilization, and goodput
Cao et al. [246]	2016	receiver-centric buffer blocking-aware data scheduling	Wireless	Asymmetric	reordering, receive buffers
Mmptcp[247]	2016	randomizing of a flow's packets	datacenter	Independent	Loss rate, Throughput
Cui et al.[248]	2016	end-to-end coding	General	General	throughput and latency
Kaiping et al. [92]	2016	network coding, end-to-end congestion control	Wired, Wireless	General	Fairness
Choi et al[249]	2017	optimal load balancing scheduler	Wireless	General	HOL blocking, Throughput
Wang et al. [250]	2017	genetic algorithm, a rate distribution vector, Energy-aware Scheduling	Wireless	General	Throughput, Energy Consumption

Kimura et al. [251]	2017	Highest Sending Rate, Largest Window Space, and Lowest Time/ Space-based scheduling	General	General	Throughput
Lim et al. [252]	2017	Earliest Completion First Scheduling	General	Asymmetric	Bandwidth aggregation
BELIA[115]	2017	estimation of the real bandwidth of the link	General	General	Throughput
LDDoS [268]	2017	low-rate distributed denial-of-service attack-aware energy-efficient	Mobile Cloud	General	energy usage, DoS attack
Lin et al.[253]	2018	packets retransmission	General	General	data latency
Le et al. [254]	2018	Forward delay-based packet scheduling	General	Asymmetric	reordering
Ferlin et al.[255]	2018	forward error correction	General	Asymmetric	retransmissions, HOL
Jiyan et al. [256]	2018	Delay-Energy-quality-aware	Wireless	Asymmetric	throughput
Mena et al.[257]	2018	capacity estimation of path	Wireless	Independent	Handover
Ting et al. [258]	2018	bottleneck bandwidth and round-trip propagation time	Wireless	General	Fairness

Morawski et al. [269]	2018	optimal load distribution	Wireless	General	Energy Consumption
Elgabli et al.[263]	2018	Scalable Video Coding	Wireless	Independent	Fairness
Jia et al. [259]	2019	minimizing the flow completion time	datacenter	General	energy consumption
Trinh et al.[260]	2019	low energy consumption paths to deliver data	Wireless	General	throughput and energy efficiency
Könsgen et al. [261]	2019	allocation of link capacity using mixed linear programming	General	General	throughput and fairness

Thomas et al. [231] proposed a hybrid CC policy for multipath and multi-source transmission that leads to higher bandwidth aggregation than normal MPTCP. This scheme employs multi-flow CC, network assistance (MFCCNA) policy, and an in-network module for network topological information; this scheme dynamically explores the obtainable topological information about the network. MFCCNA's ultimate objective is to enhance resource utilization in the network without compromising the friendliness issue. Still, MFCCNA works without considering aggressiveness with reference to the window growth policy. Hence, leads to data packet losses and performance degradation.

MP-TCP provides bandwidth aggregation and flexibility during data transmission in the network. However, it does not consider the path attribute (delay and bandwidth) significant in data transmission over multiple paths [97,232]. Because of this, the destination receives uncontrolled data packets that cause congestion window reduction and unnecessary retransmission. To overcome unordered packet delivery, Le and Bui proposed an MPTCP forward delay-based packet scheduling (FDPS) [109], while Yang and Amer proposed a one-way delay-based MPTCP scheduling [108]. Both of these policy schedule packets over the multiple sub-flow based on the estimated path delay of each path by source. On Conversely, Ni et al. proposed an offset compensation-based packet scheduling (OCPS) [110] that performs scheduling based on feedback received from SACKs.

Multi-streaming is one more idea initially employed by SCTP-based CMT to manage different network conditions. MP-TCP directly inherits this feature from SCTP-CMT. Li et al. suggested NC-MPTCP [111] minimize retransmission in case of delay. Systematic coding MPTCP (SC-MPTCP) applies redundant code [222] to mitigate unnecessary fast retransmission. Cui et al. suggested another improved version of MP-TCP using foundation-code [100], while Zhou and Shi proposed congestion window adaptation MPTCP (CWA-MPTCP) [233] to regulate the transmission rate in such a way so that each sub-flow has a similar end-to-end delay. The initial implementation of MP-TCP support fully ordered and fully reliable connection-oriented services. Still, this property makes MP-TCP unstable in real-time applications. Therefore, Xu et al. proposed a partially reliable MP-TCP (PR-MPTCP) [234] to sustain real-time applications, for example, a multimedia stream.

With the advent of resource constraint devices, the requirement of energy-efficient multipath communication becomes necessary; hence Jiyan et al. [131, 256] proposed energy-aware and priority frame-based packet scheduling for the heterogeneous wireless environment to enhance the goodput, delay, and energy consumption in multipath transmission. Further, Wang et al. [250] present MPTCP based on a genetic algorithm, a rate distribution vector, and Energy-aware scheduling to optimize the throughput and Energy Consumption of devices in a heterogeneous wireless network. In another survey work, Jia et al. [259] proposed an MPTCP algorithm by minimizing the flow completion time of transmission to minimize the energy consumption of the system in the cloud-based data centre. Trinh et al.[260] proposed low energy consumption path-based scheduling to enhance the throughput and energy consumption of the system in the wireless environment. To mitigate the DoS attack during multipath communication, a low-rate distributed denial-of-service (LDDoS) attack-aware energy-efficient MPTCP [268] was proposed for a cloud-based system to optimize energy usage.

Li et al. [265] proposed reinforcement learning-based MPTCP to identify the best sub-flow for packet transmission in the heterogeneous wireless environment to aggregate the throughput of the system. In [261], Könsgen et al. proposed MPTCP to allocate estimated path capacity using mixed linear programming to aggregate the throughput of the system. Several other researchers have also contributed to MP-TCP optimization in real-time applications, such as QoS-MPTCP [235-236], message-oriented MPTCP (MO-MPTCP) [238], quality-driven multipath TCP (ADMIT) [237], and cross-layer scheduler [239].

5.3.3 CMT versus MPTCP

The objective of CMT and MPTCP is to maximize the exploitation of available multipath resources but their working principles differ from each other. A listing of major differences is outlined in Table 5.4.

Table 5.4: Comparison of CMT and MPTCP

Parameter	**CMT**	**MPTCP**
Connection Establishment	4-Way Handshaking	3-Way Handshaking
Congestion Control	Uncoupled	Coupled
ACK Mechanism	SACK and Delay SACK	Cumulative ACK, SACK and Delay SACK
Compatibility of Middle Boxes	Not Compatible	Compatible
Performance	High Throughput with excessive CPU utilization	Limited Throughput
Fairness	Limited	Maximum possible

5.4 FINDINGS

With the development of Multihoming devices and loaded end-to-end multipath communication capability, this survey finds that the popularity of multipath transport layer protocols CMT and MPTCP is increasing daily. From the survey work of these protocols presented in Table 5.2 and Table 5.3, it has been found that most of the challenges mentioned in Section 2 have been resolved to a large extent. It is believed that this survey outlined almost all the potential challenges in Section 2 and their possible solutions by CMT and MPTCP in Table 5.2 and Table 5.3. This survey allows a reader to easily recognize recent developments in multipath transmission and make their proposal feasible. In this survey, it is also found that most CMT and MPTCP solutions share common problems and algorithms but use different approaches such as fairness, path diversity, Pareto-optimality, and receiver buffer impact. Limited acceptance of CMT by middleboxes like port address translation, firewalls, network address translation, etc., makes MPTCP more popular for Internet networks. Both protocols use different control signals for establishing multipath connections and CC mechanisms. Several works have been undertaken to promote multi-path communication in resource constraints and heterogeneous networks, such as IoT and M2M communication [270]. In addition to the technical aspects, it has been found that the following major efforts have also led to the optimized development of multipath communication: experience, rigorous testing, fault identification and resolution, government and industry support for the research community, and standardization. Although the development of multipath transmission is growing at a rapid pace, it still requires more marketing support to engage industries and users. Currently, only a few companies are making multipath-equipped smartphones. Apple has deployed multi-path TCP on iPhones; any iOS12 or more application can use multipath TCP. LG and Samsung are developing smartphones in South Korea to use cellular and Wi-Fi interfaces to achieve bandwidths of up to 1Gbps [271].

5.5 FUTURE RESEARCH DIRECTIONS AND CHALLENGES

This survey shows that many research avenues around multipath transmission are open or need improvement. Next, make some relevant observations to develop aspects and present opportunities for future work.

Standardization is required for the rapid development of multipath communication. Only a few basic multipath protocols are standardized [96,97,183, 187,193,196,204], and it seems it requires great work.

Energy Consumption during transmission is also one of the requirements in the resource constraint environment such as M2M/IoT communication. In survey work [131,197,250,256,259-260], energy consumption is taken into consideration during multipath data transmission. Still, it requires an energy-efficient algorithm to full fill the future needs of battery-operated multi-home devices.

Security in multipath is discussed in Section II. Still, in the survey, it was hard to find any promising work to deal with security issues only [268] authors have presented limited work on DoS attack handling. Security threats such as handshaking, multiple sub-flow, flooding, hijacking, and DoS attacks arising due to multipath transmission are promising research challenges.

IoT adds more difficulty in communication due to its heterogeneous nature, resource constraint devices, mobility, dynamic nature, etc., and they are merely considered in the literature. Multipath communication will undoubtedly contribute significantly to the development of IoT, so its impact cannot be ignored.

Deep-Learning and Artificial Intelligence are increasingly becoming essential technique to solve problems [272] and can be used to solve the issues that arise in multipath transmission. Several works based on artificial intelligence have been performed to measure the QoS [273-274] to solve the optimization in single-path transmission. Hence, a better solution could be possible using deep learning, machine learning, or other artificial intelligence-based methods to solve multipath issues.

Wireless Technology and enabled devices are rapidly evolving, such as Wi-Fi, Zigbee, Bluetooth, LORA, etc. Therefore, exploring the impact and resolution of these new technologies in the multipath transmission is necessary.

Fifth Generation communication requirements, such as extremely high bandwidth and ultra-low latency, mandate the deployment of multipath transmission [275]. Furthermore, some studies have been made to incorporate multipath in 5G [276-277]. Therefore, multipath transmission over the 5G network is a key promising research area to innovate solutions required in handling issues of multi-home technologies.

Scheduling is one of the key factors behind the success of multipath transmission. As shown in Table 5.1, several scheduling criteria are adopted by multipath algorithms. The performance of scheduling algorithms depends on the compatibility of network conditions and applications. It is found that most of the algorithms use single scheduling criteria and perform better in favourable conditions and poor when conditions change. Therefore, there is a requirement for context-aware scheduling so that the multipath algorithm adopts the best scheduling policy when the network context changes. Some initial works available in the literature use two scheduling policies [196, 278]. Overhead is increasing in multipath transmission than a single path hence reducing scalability. Therefore an optimal solution is required to minimize the computation power, complexity, and memory use in multipath transmission. Packet Reordering, Spurious Retransmission, and Buffering issues are studied in literature but still pose a great challenge. These are the key factors affecting the performance of multipath communication and hence need extra attention in the future design of algorithms.

The cross-Layer designing approach can be a boon for multipath communication. It is clear that data traffic routing performs at the network and data link layer while QoS parameters (such as RTT, Bandwidth, congestions, and delay) are available at a higher layer. Therefore to obtain the best results, parameters across layers should be visible to the multipath algorithm; hence cross-layer provisioning of multipath transmission can be promising research in the future.

5.6 SUMMARY

Multipath communication has become the de facto protocol to meet the growing demand for optimal performance in many scenarios and usages. Therefore, it has become inevitable to research multipath transport layer protocols. This work surveyed the development of CMT and MPTCP transport layer protocols. It examines three major research works: key challenges of multipath communication, a survey of CMT and MPTCP transport layer protocols, and future research directions.

From the learning of this literature survey, it has been identified that scheduling data chunks are key to maximising the exploitation of available network interfaces. Hence, the next chapter proposed a novel data chunk scheduling algorithm based on CMT in the multihoming environment.

Chapter VI

PATH RANK BASED DATA CHUNK SCHEDULING FOR CMT

In modern communications networks such as the Internet of Things (IoT) and machine-to-machine communication, the device equipped with a multi-homing feature optimally exploits multiple network interfaces using the concurrent multipath transfer (CMT). This enhances system performance by concurrently scheduling data chunks on multiple network paths. Over a period of time, several scheduling criteria have been developed to optimize performance. However, from the literature survey of the previous chapter, it has been identified that CMT still suffers from many serious problems such as spurious retransmission, receiver buffer blocking (RBB), congestion window (cwnd) growth, re-ordering, and long round trip time (RTT), resulting in poor performance. These problems occur due to the asymmetric nature of path characteristics. Thus, this chapter introduces a path rank-based CMT (R-CMT) which schedule data chunk according to the rank of the path. The proposed scheduling method calculates the rank of each network path based on the ratio of successfully received and transmitted chunks. The simulation results indicate that the proposed R-CMT scheduling achieves higher performance in terms of network latency, throughput, and cwnd growth.

6.1 INTRODUCTION

The experience of past decades reveals that the growth rate of technological advancement is an incomparable height. The achievement in technology adds a tremendous number of heterogeneous devices to communication networks. Moreover, the diversity of M2M and IoT-based applications which heavily rely on resource-constrained wireless communication environments such as WIFI, radio links, LTE many more also makes it more complex. Nevertheless, to fulfil the growing demand for higher data rates, low network latency, and high reliability, the researcher should find innovative ways of communication. A solution to compensate for demands is the optimal use of available multiple network interfaces with devices [78-80]. With increasing Multihoming devices and advancement of fifth-generation communication (5G) system, it mandates the efficient utilization of available multi-communication interface resources. Hence multi-path data transmission introduced by Internet Engineering Task Force (IETF) can be a boon for Multihoming devices as shown in Figure 5.1.

Unfortunately, legacy transport layer protocol transmission control protocol (TCP) and user datagram protocol (UDP) does not support Multihoming capability. Later IETF standardizes stream control transmission protocol (SCTP) [82], to integrate Multihoming communication into its specification. To utilize the Multihoming capability of SCTP, Iyengar, et al. [81] designed CMT for multi-network interface devices. CMT improves the throughput, resource utilization, latency, and reliability of the network. On the other side CMT suffers from a number of challenges such as improper packet scheduling, unnecessary retransmission, congestion window (cwnd) reduction, receiver buffer blocking [17, 85], and many more. Further to incorporate the guaranteed reliability with quality control communication capabilities of TCP, the multi-path TCP (MP-TCP) was also introduced in [83-84] which is primarily proposed for a wired network. Hence its performance is limited in the wireless environment due to long RTT, and frequent loss of data packets.

Hence CMT is proposed to increase network performance by the concurrent transmission of data chunks in multipath communication [81]. To meet the many challenges of multipath transmission, the Data Chunk Scheduler chooses critical paths from the many paths that allow greater performance for multipath communication. According to the scheduling policy, whenever the application has to send data, the scheduler distributes the data simultaneously over multiple paths [35, 85]. In the last decades, many scheduling policies have been developed to mitigate the challenges. However basic CMT and CMT-potentially failed (CMT-PF) [193] schedulers use a round-robin scheduling policy to transmit an equal amount of data chunks without considering path characteristics such as delay, bandwidth, and cwnd hence inevitably suffering RBB. To mitigate RBB, Dreibholz et al. [104] proposed a sender buffer splitting approach to schedule data chunks according to the blocking of a fraction of the path but it suffers from local blocking. Shailendra et al. [95] implemented a scheduling policy based on the total delay of the path to reduce average data chunk delay but suffer from improper bandwidth utilization. Xu et al. [86, 90] proposed a quality-aware adaptive and network coding-based scheduling policy for the wireless environment to improve throughput but this approach did not remove RBB completely. Wallace et al. [279] present two techniques, renewable and Markov, to enhance the throughput of a CMT session by handling RBB and cwnd on the cost of accuracy and scalability. Jiyan et al. [134] advance CMT scheduling policy based on the distortion level of each path to mitigate delay and retransmission issues. Jiyan et al. [189] further outlined a content-aware CMT scheduling policy based on the feedback of path status and estimated contents of data to be transmitted in a multipath heterogeneous wireless environment. Another class of CMT scheduling policy based on network coding is developed which uses a Q-learning approach to minimize RBB problems up to a certain extent [91]. Verma et al. [129] proposed path delay and bandwidth awareness based on an adaptive data chunk scheduling policy for CMT (A-CMT) and claim better throughput, cwnd growth, and transmission time. They further optimize multipath transmission by developing a cross-layer-based adaptive data chunk scheduling policy. It uses medium access control-layer data to identify congestion in advance and regulate the cwnd of the path [128]. A raptor code-aware CMT which utilizes the Markov Decision process to schedule packets is also available in literature and claims improvements in goodput and delay [215]. In another work, Jiyan et al. [197] again developed a CMT scheduling policy based on the energy consumption of different paths as it is necessary for the resource constraint environment. Liu et al. [138] suggested loss aware CMT scheduling policy based on packet loss and loss variation of paths and claims improved reordering delay and unnecessary fast retransmission.

While optimization and advancement in CMT scheduling policy improve throughput, robustness, bandwidth utilization, and reliability but still suffer many challenges as result it causes degradation of performance. In addition to these, it is still challenging to achieve desired performance in heterogeneous wireless environments [35-36, 85]. The main reason behind the challenges of multipath communication is the asymmetric nature of different paths. When the data chunk scheduler does not intelligently distribute the chunks it causes a serious problem i.e. unordered delivery of the chunks to the receiver. To deliver the chunk in sequence, the receiver stores it in the receiver buffer and generates the missing Selective Acknowledgment (SACK) and delayed the delivery of chunks to the application. Due to this the receiver buffer blocks and unnecessary retransmissions, as well as reduction in cwnd occurs which affect the performance.

Learning from the existing CMT scheduling policies, this chapter advances the state of the art by proposing a new R-CMT solution by considering the ratio of successful received and transmitted chunks by the path. The important contribution of this research work is as follows.
1) A new SCTP-based R-CMT solution is proposed with the following features.

- Rank evaluation of each active path based on the ratio of successfully received and transmitted data.
- In the congestion avoidance (CA) phase, the growth of the cwnd is adapted according to the rank of the path.
- Maximize ordered delivery of data to mitigate RBB problem and improves different latency.
- Enhancing throughput from aggregating multiple paths to achieve the main objective of CMT.

2) Developed fast retransmission mechanism to identify the highest rank path for retransmission of missing data chunks. 3) Performed extensive simulation of proposed scheduling algorithms in the asymmetric network environment. Simulation results reveal the following facts.

- R-CMT improves the throughput up by 6%, 13% and 17% from A-CMT, CMT-PF, and CMT, respectively.
- Better cwnd growth is achieved compared to referenced schemes.
- Average file transfer time is also improved.

The remainder of this chapter describes the proposed R-CMT scheduling policy in section II; mathematical and experimental analysis in sections III and IV; and the conclusion in section V.

6.2 PROPOSED R-CMT SCHEDULING POLICY

In multipath communications, sending device schedules data chucks over the available multiple paths to maximize the network performance. But due to the asymmetric nature of each path, the receiver node receives data chunks in an unordered manner. Therefore scheduling of data chunks over multiple paths plays an important role. If data chunks are equally distributed over multiple paths, then due to different characteristics (bandwidth, delay, transmission rate, error rate, etc.), path capacity is not fully utilized. To maximize the available path utilization R-CMT is proposed.

The design architecture of R-CMT is shown in Figure 6.1, the whole system consists of a sender, N numbers of paths, and a receiver. At the sender, R-CMT consists of three main components, which are a path rank calculator, data chunk scheduler, and fast retransmitter. Whenever application data is available for transmission at the transport layer, data chunks are formed and entered into the sender buffer. The scheduler picks data chunks from the buffer and distributes them across multiple paths according to rank. The rank of the path is calculated by the path rank calculator. At receive end data chunks may arrive out of order, to ensure the ordered delivery to the application a limited size receiver buffer is used.

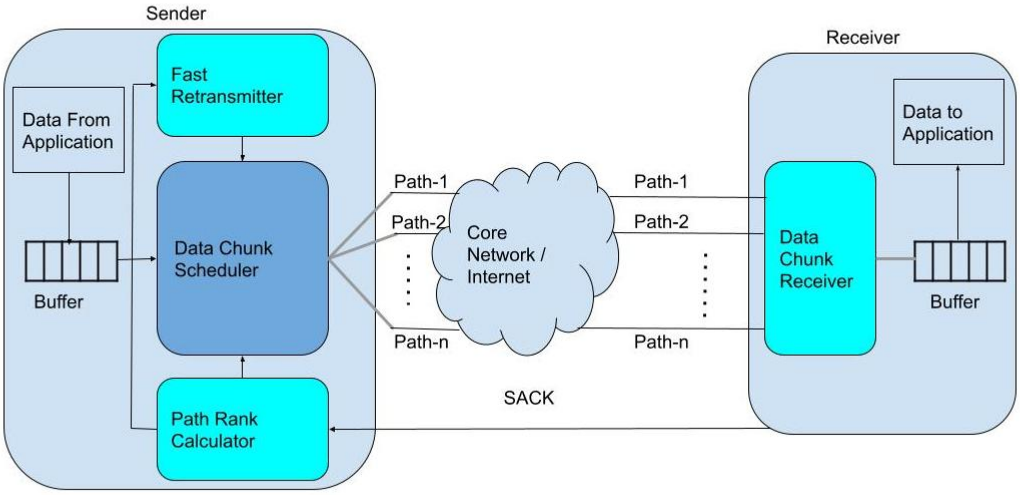


Figure 6.1: R-CMT architecture

After the reception of data chunks, the receiver sends a gap report to the sender by SACK message. From the two consecutive SACKs reports, the sender can identify how many data chucks were successfully delivered and outstanding.

R-CMT includes three phases; 1) Rank evaluation of each path when SACK is received. 2) Adjust the data transmission rate of each path according to its rank. 3) Identification of the best path for fast retransmission. The complete description is presented in the following subsections.

Algorithm 1 Path Rank Calculation

```
Result: $R_k$
Input: P, $T_{nk}$ , $R_{nk}$ , k, $R_{k-1}$
$TR_k$=Null
while (p ϵ P and status p==active) do
    $TR_k = Rn_k/Tn_k$
    $R_k(p) = R_{k-1}(p) + (TR_k - R_{k-1}(p))/k$
end
```

6.2.1 Path Rank Calculator

After receiving successfully delivered and outstanding data chunks R-CMT calculates the rank of each individual path using the Algorithm 1. The complete procedure is explain as follows.

Suppose P is a set of N paths in a given CMT association, $p_i \epsilon P$ is the ith path and R is the set of the rank of paths. Tn$_k$ denotes the number of data chunks successfully transmitted by the sender using p_i during $\triangle t_k$. Rn_k denotes the number of successfully received data chunks by a receiver using p_i during $\triangle t_k$. St$_k$ is k^{th} SACK receive time stamp at sender from the receiver and $\triangle t_k$ is the kth time interval of two consecutive SACKs time stamp.

$$\triangle \, t_k = St_k - St_{k-1}$$

The successful transmission rate (TR_k) of path p_i at St_{k+1} is calculated using Equation (1).

$$TR_k = Rn_k/Tn_k \tag{1}$$

The rank of p_i during $\triangle t_{k+1}$ ($R_k(p_i)$) is calculated using Equation (2).

$$R_k(p_i) = R_{k-1}(p_i) + (TR_k - R_{k-1}(p_i))/k \tag{2}$$

6.2.2 Data Chunk Scheduler

Once the rank of each path is calculated, the data chunk scheduler will adjust the congestion window of each path accordingly. The procedure for data chunk scheduling is described in Algorithm 2.

6.2.3 Fast Retransmitter

To mitigate delay constraints in case of loss and timeout, this work also proposed fast retransmission policy. It selects the highest rank path using Algo-

Algorithm 2 Path Rank Data Chunk Scheduling Policy

```
Result: cwnd$_{k-1}$
Input: $P, R_k, SSTHRSH, k, cwnd_{k-1}$
for (p $\epsilon$ P and status p==active) do
    if ($cwnd_{k-1} < SSTHRSH(p)$) then
        cwnd$_k$(p) = min (NEWACK$_{k-1}$(p), MTU)
    end
    else
        if ($cwnd_{k-1}(p) \geq SSTHRSH(p)$) then
            cwnd$_k$(p) = cwnd$_{k-1}$(p) + MTU * R$_k$(p)
        end
    end
end
Return (cwnd$_k$)
```

rithm 3 to send lost data chunks. After receiving three consecutive missing SACK reports for a particular data chunk, the sender assumes that the data chunk has been lost. Therefore sender needs to immediately retransmit the missing data chunk. For retransmission, the sender selects the highest rank path as described in Algorithm 3.

Most of the scheduling policies consider some of the performance-affecting factors such as RTT, bandwidth, cwnd, loss, buffer blocking, etc. But R-CMT considers successful chunk transmission rate to calculate the rank of a path using Algorithm 1 and regulates data transmission by adjusting cwnd using Algorithm 2. Here successful data chunk transmission or rank of a path not only depends on some of the affecting parameters rather considers all.

Algorithm 3 Fast Retransmission

```
Result: P$_f$
Input:P, R$_k$, SSTHRSH, cwnd$_{k-1}$
if (RTO$_p$ expire) then
    SSTHRSH (p) = max (cwnd$_{k-1}$(p)/2, 3*MTU)
    cwnd$_k$ = MTU
end
if (Receive 3-SACKs (duplicate)) then
    SSTHRSH (p) = max (cwnd$_{k-1}$(p)/2, 3*MTU)
    cwnd$_k$ = SSTHRSH (p)
end
Temp=0
for (p $\epsilon$ P and status p==active) do
    if (Temp<R(p)) then
        Temp=R(p) and P$_f$ = p
    end
end
Return(P$_f$)
```

6.3 ANALYSIS

The main objective of this section is to analyze the performance of R-CMT in terms of ordered delivery, RBB, throughput and effect of fast retransmission on the system. These parameters are analyzed in a different number of discrete rounds. A round starts with the transmission of the data chunk and ends with the reception of a SACK. The length of the round can be a minimum as one RTT, RTO, or RTO$_{max}$. These rounds can fall in one of three states: Slow start (SS), Congestion avoidance (CA), and exponential back-off (EB).

The cwnd of a path during CA in R-CMT is adjusted according to equation (3) when the next round starts.

$$cwnd_k = \begin{cases} min(NEWACK_k, MTU) \ when \ SS \\ cwnd_k + MTU * R_k(p)) \ when \ CA \\ cwnd_k/2 \ when \ EB \end{cases} \tag{3}$$

A path transmits maximum data at a particular moment according to Equation (4).

$$DATA_k = min(cwnd_k - OUT_k, RWND_k) \tag{4}$$

R-CMT updates cwnd according to the rank of a path R(p) as shown in Algorithm 2, hence Equation (4) can be written as (5).

$$DATA_k(p) \propto R_k(p) \tag{5}$$

6.3.1 RBB and Ordered Delivery of Data Chunks

The ordered delivery of data chunks at the receiver end can be maximized when different data chunks sent from different paths reach the receiver at a certain time. A sender transmits data through a path in the following three ways, less than, the greater, or equal transmission capacity of a path at a particular moment. The first case ensures ordered delivery but on the cost of throughput, the second case does not ensure ordered delivery as well as throughput because in this case congestion will increase. The third case ensures ordered delivery as well as maximizes throughput, here R-CMT comes into the picture. R-CMT scheduling ensures the sender sends data almost equal to the capacity of a path by adjusting the cwnd according to the rank of the path. From Equations (3) and (5) the data that can be transmitted through a path at a particular moment, k is $DATA_k \propto R_k$. From Equation (2).

$$DATA_k \propto R_{k-1} + (TR_k - R_{k-1})/k$$

$$DATA_k \propto (R_0 + TR_1/k + ...TR_k/K)$$

It further implies $DATA_k \propto Avg(TR)$ of the path. Hence R-CMT ensures data transmission through a path in proportion to its successful transmission capacity. As result ordered data delivery is ensured to the recipient. It is already reported that due to different delay and bandwidth, data scheduling cause a problem with out-of-ordered delivery due to this CMT suffers from the RBB problem. But R-CMT minimizes the out-of-order delivery of data, hence a reduction in RBB.

6.3.2 Throughput

The throughput (η) of a path during a session can be estimated using Equation (6).

$$\eta(p) \propto E(Tr)/E(t) \tag{6}$$

Where E(Tr) expected number of data chunks sent successfully in expected session E(t). In R-CMT data is transmitted in rounds and each k^{th} round lasts $\triangle t_k$ time. So throughput of a round can be calculated.

$$\eta(p) \propto E(Tr)_k/\triangle t_k \tag{7}$$

Here $E(Tr)_k$ depend on how much data is transmitted during a round and it will be.

$$E(Tr)_k \propto DATA_k$$

$$E(Tr)_k \propto cwnd_k \text{ From Equation(5)}$$

$$E(Tr)_k \propto R_k \text{ From Equation(3)}$$

So from here, Equation (7) can be written as.

$$\eta(p) \propto R_k/\triangle t_k \tag{8}$$

Hence the overall throughput of path will be.

$$\eta(p) \propto \sum_{k=0}^{k_max} R_k/\triangle t_k \tag{9}$$

From Equation (9), it is clear that the throughput of the system depends on the rank of the individual path. Here R-CMT maximizes the throughput because it exploits the available multiple paths with its available capacity by regulating transmission through the rank of the path.

6.3.3 Effect of Fast Retransmission

When three consecutive duplicate acknowledgements are received at the sender then it concludes that the packet has been lost due to any reason. Therefore source needs to retransmit the lost data chunks. In R-CMT retransmission will take place via the highest rank path. It seems that overhead on the highest rank path may increase in some situations which will affect the overall performance. But R-CMT smartly manages this situation by reducing the rank of the path because when overhead increases it reduces the successful delivery rate of the path. So in the next round path rank also changes and fast retransmission will be via any other highest rank path, simultaneously it will also reduce normal data chunk transmission along with the previous highest rank path.

6.4 EVALUATION

The throughput, congestion window growth, and transmission time of proposed R-CMT are evaluated in an asymmetric environment under different circumstances and compared with CMT and CMT-PF along with A-CMT. The performance of these schemes is evaluated using the NS-2.35 simulation tool on commonly adopted network topology as shown in Figure 6.2. It consists of one CMT source and one destination with two network interfaces. As most modern devices are connected with at least two network interfaces [270], hence two bottlenecks are taken. The bandwidth and transmission time of each link is shown in Figure 6.2. During simulation, the path loss rate varies according to the scenario otherwise fixed as Path1 5% and Path2 10%. UDP traffic generator is used to add background traffic. The setup is configured with 50 packets queue size along with a drop tail queuing policy. The network configuration of both links is asymmetric as interfaces follow different standards. The simulation settings are summarized in Table 6.1.

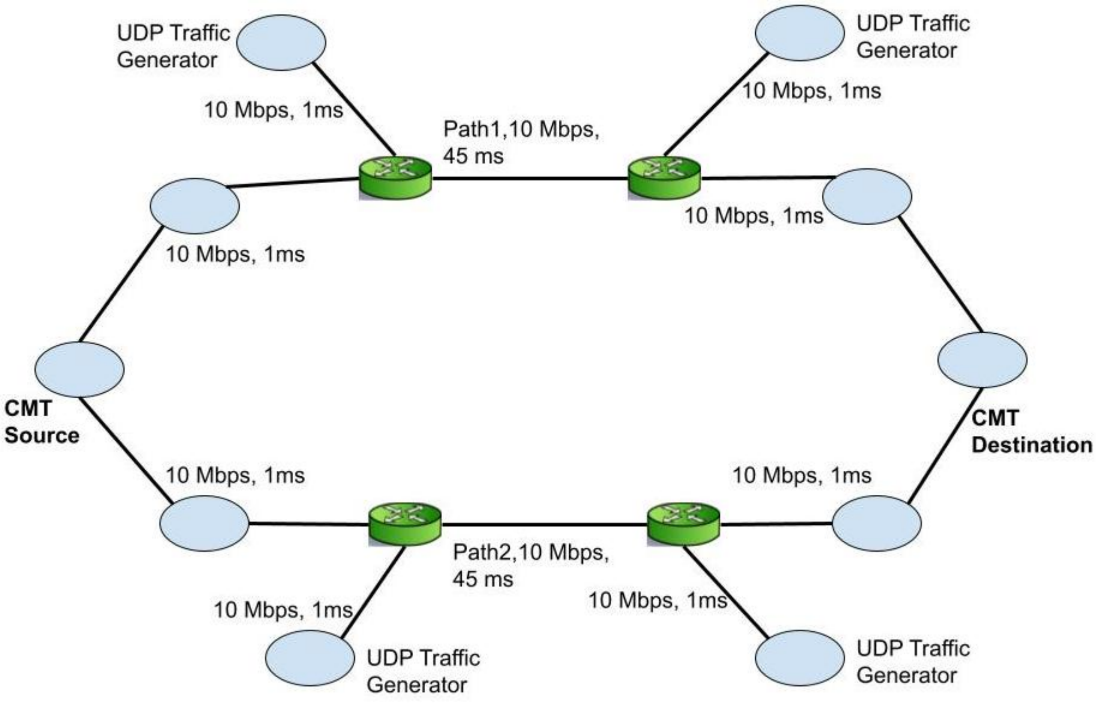


Figure 6.2: Simulation topology

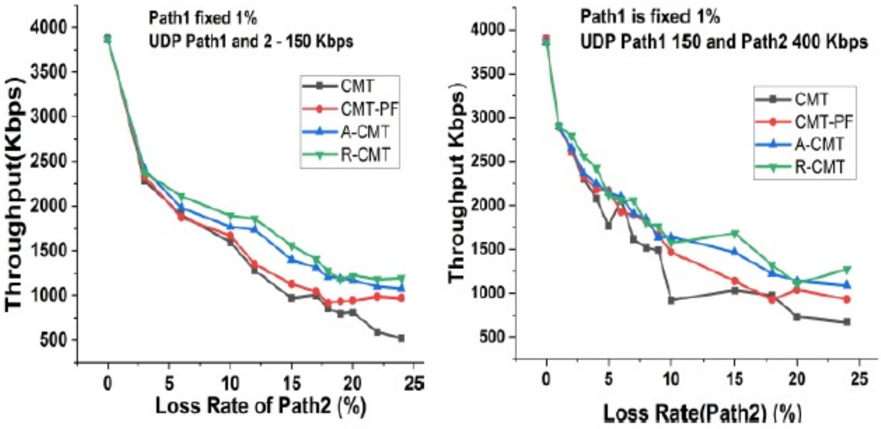
Table 6.1: Network simulation parameters

Network Parameters	Values
CMT MTU	1500 bytes
CMT Data Chunk Size	1468 bytes
CMT RBB size	64 KB
Sender Buffer Size	64 KB
CMT Application	FTP
CMT RTX Policy	RTX-CWND
Queuing Policy	Drop-tail
Queue Size	50 Packets
Path Packet Loss Rate	Path-1: 5%, Path-2: 10%
Bottleneck Bandwidth	10Mbps
Path Propagation delay	47 ms
Simulation Time	200 s
Background Traffic	UDP
UDP Application	CBR, Path-1:150, Path-2:400 Kbps

6.4.1 Throughput with variable packet loss rate

The first evaluation of the throughput is under packet loss rate of Path1 fixed 1% and Path2 varies from 1% to 25% in two different scenarios of setup. Initially, background traffic by UDP application of Path1 and Path2 is set to 150

Kbps. Later background traffic of Path2 is set at 400 Kbps. The observed throughput is plotted in Figures 6.3 (a) and (b) respectively. From the figure, it is clear that as the packet loss rate increases the throughput of each variant decreases. CMT shows the least throughput among all variants due to its equal data chunk distribution policy and not considering any path characteristics.



(a) First scenario

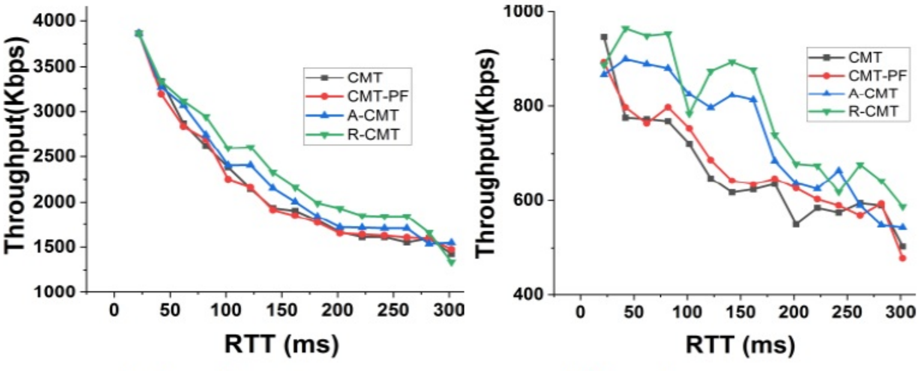
(b) Second scenario

Figure 6.3: Throughput under packet loss rate

CMT-PF considers the path failure characteristic which is why it performs better than CMT when the loss rate increases. A-CMT uses a delay based data distribution policy; therefore it performs better than CMT and CMT-PF. However, R-CMT achieves better throughput than CMT, CMT-PF and A-CMT because it uses a path rank-based data distribution policy.

6.4.2 Throughput with variable path delay

The second evaluation of the throughput is under variation of RTT of Path2 from 20 ms to 400 ms while Path1 is set on 94 ms and observed throughput is plotted in Figures 6.4 (a) and (b). Observation is performed under two different scenarios normal loss rate (i.e. Path1 1% and Path2 2%) and heavy loss rate (i.e. Path1 5% and Path2 10%) while background traffic of Path2 is set at 400 kbps. From Figures 6.4 (a) and (b) it is clear that as delay increases the throughput of each variant decreases. In this scenario, CMT and CMT-PF performance is almost similar because they are not utilizing any path characteristics. However, A-CMT uses delay as a path characteristic to schedule data chunks over multiple paths. Therefore A-CMT achieves better throughput as compared to CMT and CMT-PF in a variable delay environment. While R-CMT considers the successful data delivery rate to schedule chunks. Thus, R-CMT achieves better throughput in the variable path delay situation.



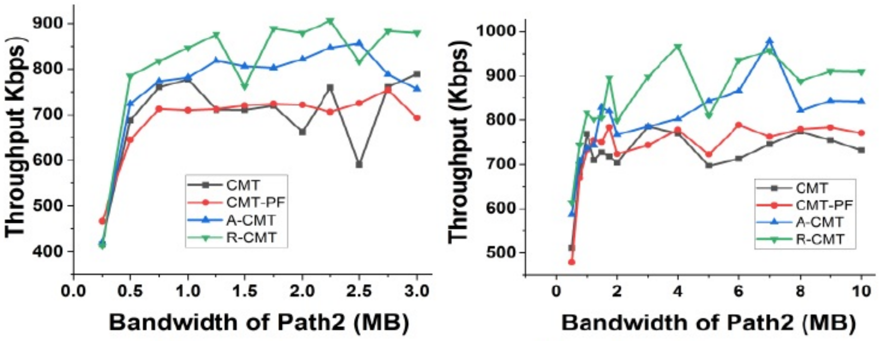
(a) Normal loss rate

(b) Heavy loss rate

Figure 6.4: Throughput vs RTT

6.4.3 Throughput with variable bandwidth

The third evaluation of throughput is under variation of path bandwidth i.e. Path2 is set to vary between 0.25 Mbps to 10 Mbps while Path1 is fixed at 10 Mbps, in two different scenarios. In the first scenario, the normal UDP traffic rate is set at 150 kbps in both the paths and in the second scenario, Path1 150 kbps and Path2 400 kbps. The observed results are plotted in Figures 6.5 (a) and (b). From the figures, it is clearly shown that CMT and CMT-PF achieve almost similar performance because they do not consider bandwidth in data chunk scheduling. However, A-CMT uses delay which is directly related to bandwidth and hence gives better throughput than CMT and CMT-PF. While R-CMT uses rank which considers bandwidth and other factors also that is why it achieves the best throughput.



(a) First scenario

(b) Second scenario

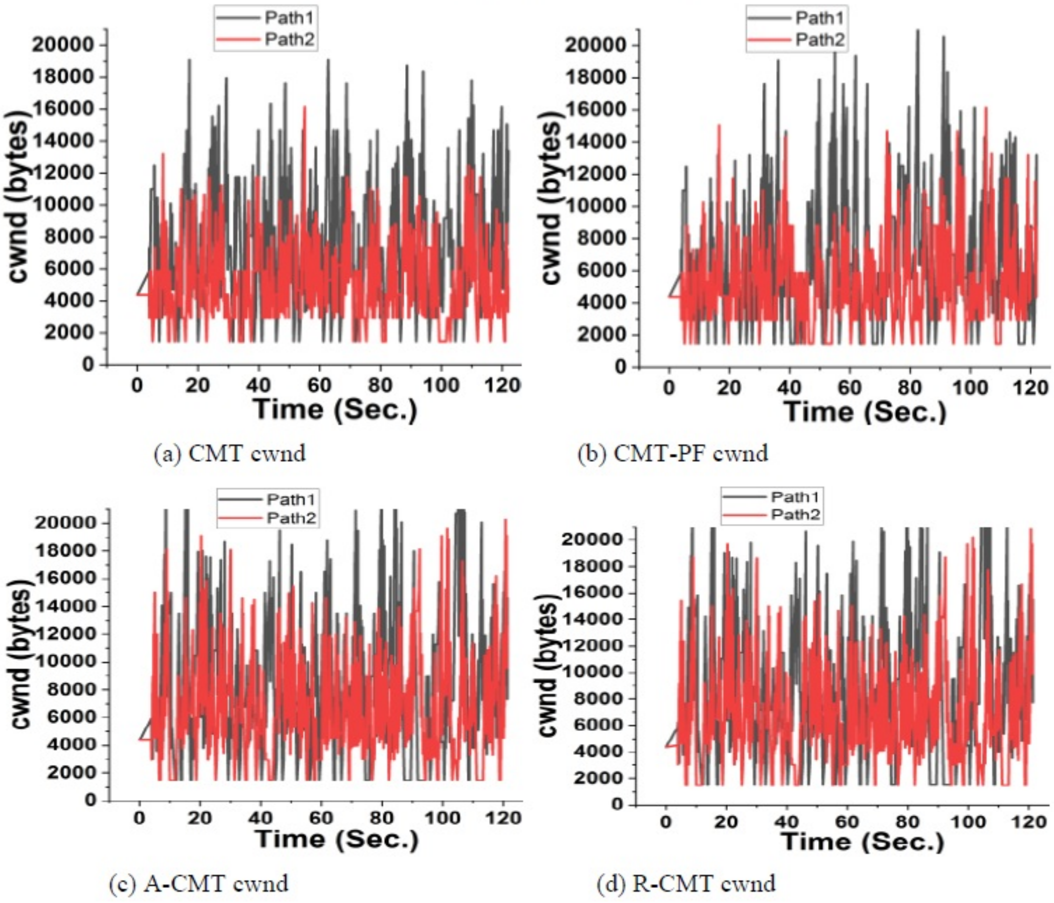
Figure 6.5: Throughput against variable path bandwidth

The simulation results in all circumstances reveal that R-CMT achieves approximately 6%, 13%, and 17% better throughput than A-CMT, CMT-PF, and CMT respectively. It is possible because R-CMT schedules data chunks according to the rank of the individual path, which is directly proportional to the successful transmission rate of the path in other words it can be concluded that R-CMT considers all performance affecting parameters which is the reason behind better throughput.

6.4.4 Congestion window growth and file transfer time

Figures 6.6 (a)–(d) presents the cwnd growth of CMT, CMT-PF, A-CMT, and proposed R-CMT respectively. In this simulation, the Path1 and Path2 loss rates are set 5% and 10% respectively and the simulation time is 120 seconds. The rest of the settings are according to Table 6.1. Since R-CMT controls the cwnd growth based on the path dynamic factor rank which varies according to the successful transmission rate of the path that is why it achieves better cwnd growth.

Figure 6.7 shows another evaluation of R-CMT i.e. average file transfer time of different sizes. The observed result shows that R-CMT takes less time



(a) CMT cwnd

(b) CMT-PF cwnd

(c) A-CMT cwnd

(d) R-CMT cwnd

Figure 6.6: cwnd growths in different time stamp

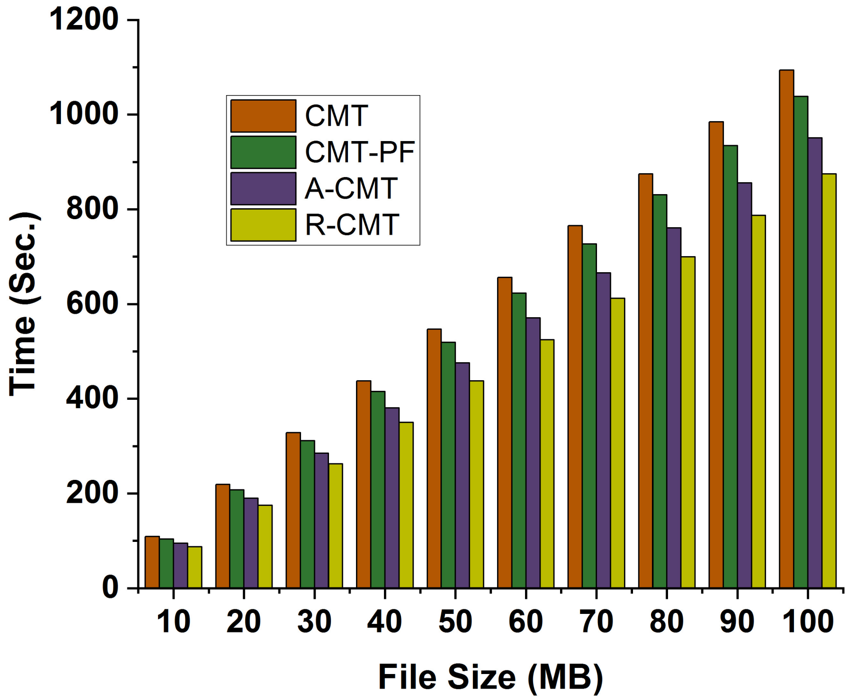


Figure 6.7: File transfer time of different sizes

to successfully transmit the file.

6.5 SUMMARY

This chapter proposed a path rank-based data chunk scheduling scheme called R-CMT. This scheme calculates the rank of each path according to its immediate successful transmission rate and schedules data chunks accordingly. The rank of the path ensures the transmission of the data chunks as per the path maximum capacity making R-CMT achieve better performance. This chapter also proposed fast retransmission policy to select the highest rank path in case of lost data chunks. Regressive simulation has been performed in the different asymmetric scenarios and results reveal that R-CMT achieves better throughput, cwnd growth, and file transfer time.

The R-CMT data chunks scheduling system was suggested in this part of the thesis to maximise network interface use. The next chapter proposes a new efficient memory page replacement technique to maximise the utilization of device memory and CPU.

Chapter VII

A NOVEL LONGEST DISTANCE FIRST PAGE REPLACEMENT ALGORITHM

Improvement in the performance of computing devices in program execution can be achieved by employing an efficient page replacement algorithm in memory management. There are many traditional page replacement algorithms used in virtual memory organization like FIFO, LRU, Optimal page replacement, CAR, ARC etc, each of these algorithms tries to reduce the number of page faults in the selection of victim page from the memory frames. This chapter presents all the popular page replacement algorithms and a new approach named as "Longest Distance First (LDF)" page replacement algorithm. From experimental results and analysis, it has been observed that LDF produced better performance in terms of page fault rate and implementation overhead than many traditional page replacement algorithms like FIFO and LRU. The average page fault of LDF is better than the FIFO and LRU of the taken data set. The proposed method can be used in virtual memory management to improve the performance of computer systems by minimising page fault rate.

7.1 INTRODUCTION

The computer is an electronic device which executes the computer program, and the execution of a computer program is managed by the operating system. Almost every computer consists of an operating system which provides all functionality needed in the execution of the program. Functionalities of the operating system can be resource management, process management, memory management etc. When a program executes, it must reside in the main memory of a computer, for that operating system uses different memory management techniques to allocate memory to the program. One of the popular memory allocation techniques is demand paging. In paging programs are divided into pages and memory is divided into fixed-size frames and frame size must be equal to page size. To allocate memory for the execution of programs, pages of programs should be loaded in free frames of memory and to keep track a page table is created.

But in virtual memory only a few pages of programs are allocated in memory frames to start the execution of programs and all pages are kept in the secondary memory of the system. When the central processing unit (CPU) references any instruction of a page, and if that page is available in main memory frames, then that instruction will be executed by the CPU but if the page is unavailable in main memory frames, a page fault will occur. To service page fault, the operating system loads the needed page from secondary memory to the memory frame. If free memory frames are available then the needed page will be allocated in any free frame, if free frames are not available then the operating system selects a victim page from the allocated list. To select the victim page from the memory, the operating system uses page replacement techniques.

Number of page replacement procedures exists like FIFO [280], RAND [280], LRU [281], optimal page replacement [280, 282], ARC [283], CAR [284], and Aging [285], etc. The main criteria used to evaluate the replacement algorithms are their page fault rate and the overhead to implement them.

Commonly accepted algorithm is LRU because of its performance in terms of page fault rate, but it requires high implementation overhead. LDF performs better in terms of page fault rate than LRU over most of the available page reference strings in academics. Its implementation overhead is also less than LRU.

The rest of the chapter is structured as follows: section II discusses popular existing page replacement algorithms. Section III describes the proposed LDF in detail with an example illustration. Section IV describes the results and analysis of taken reference strings. Finally, Section V concludes the chapter.

7.2 PAGE REPLACEMENT ALGORITHMS

When a page fault occurs during the program execution, the operating system uses the memory management algorithm to select the victim page from primary memory and makes room for the required page. Many algorithms have been developed and tested theoretically as well as practically. Some of the popular algorithms are as follows.

FIFO

It is the simplest page replacement algorithm in implementation but it performs poor in terms of page fault rate. The selection of the victim page is based on its arrival in memory. *The oldest page is replaced first.* The running time and implementation of FIFO algorithm is easy but it rarely deployed in any platform. The working principal of this algorithm is explained with the following examples.

From the example as shown in Figure 7.1, the working of FIFO [280] can be understood with reference string 0 1 2 3 0 1 4 0 1 2 3 4. Initially, three empty frames are taken into the memory.

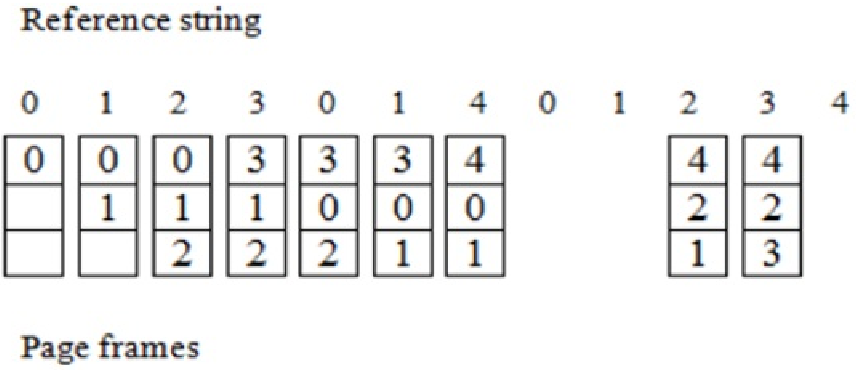


Figure 7.1: Example of FIFO page-replacement algorithm

LRU

The basic idea behind LRU [281] algorithm is that replace the page that will be least recently used. The working can be explain by using the same reference string 0 1 2 3 0 1 4 0 1 2 3 4, shown in Figure 7.2.

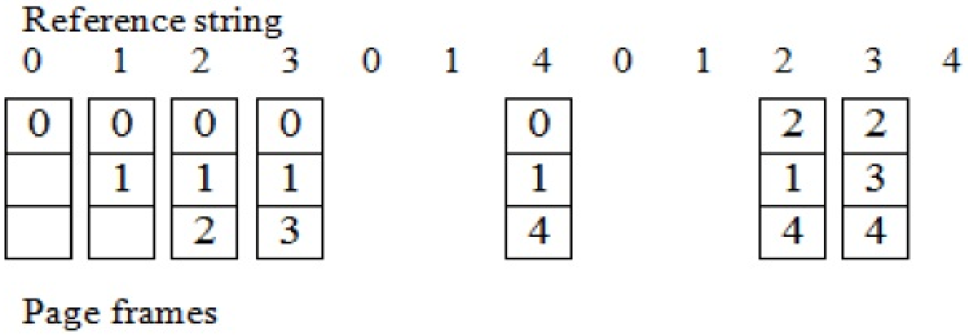


Figure 7.2: Example of LRU page-replacement algorithm

Optimal Page Replacement

The basic idea behind this replacement algorithm is *Replace the page that will not be used for the longest period of time* [286]. It can be understood with the below given example using the reference string 0 1 2 3 0 1 4 0 1 2 3 4, as shown in Figure 7.3 and in case of optimal total page faults are 7.

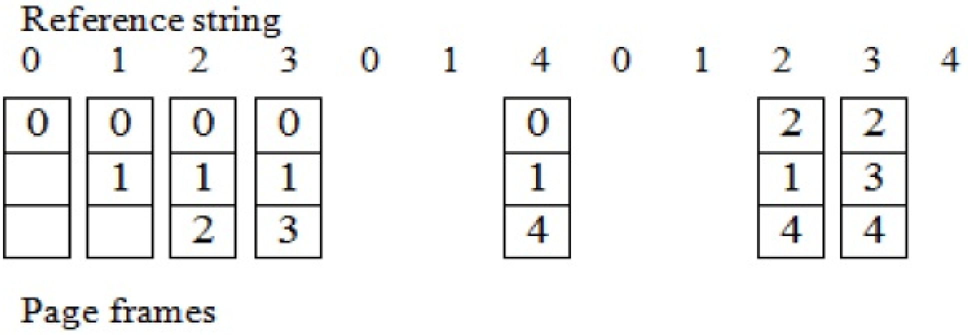


Figure 7.3: Example of optimal page-replacement algorithm

Optimal has the lowest page fault rate than all other algorithms, but it is not possible to implement it, because it requires future knowledge. It never suffers Belady's anomaly problem.

There are many other algorithms available in the literature such as ARC[283], CAR [284], LIRS[287], CLOCK[288], CLOCK-Pro [288], and LRU-K[289] algorithms.

7.3 PROPOSED LDF PAGE REPLACEMENT ALGORITHM

The basic idea behind this algorithm is Locality of Reference [290-291] as used in LRU but the difference is that in LDF, the locality is based on distance, not on the used references. In the LDF, replace the page which is at the longest distance from the current page. If two pages are at the same distance then the page which is next to the current page in the anti-clock rotation will get replaced.

Logic behind the LDF is that most of the program or portion of the program execute sequentially so if the current instruction is n_{th} then the probability of executing the next instruction close to it is more than any other instructions. Similarly probability of executing (n+1), (n+2) ... instructions is more than (n-1), (n-2)....instructions respectively. And by considering locality we can say, the chances of executing instructions close to current instruction are more than other instructions. This is the main reason behind the LDF. In page replacement, if the current page is n_{th} then the probability of executing the next page close to it is more than the other and (n+1), (n+2).. pages probability is more than (n-1), (n-2).. pages.

Calculation of Distance For the calculation of the distance of a page from the current page, arrange page reference numbers in circular form and count how many pages it is away from the current page in both directions, clockwise and anti-clockwise. From these two distances, a minimum distance will be taken.

For example; suppose a page reference string is 0 1 2 3 0 1 4 0 1 2 3 4. The total pages in this reference string are five i.e. 0 1 2 3 4. Now arrange these numbers in circular form as shown in Figure 7.4.

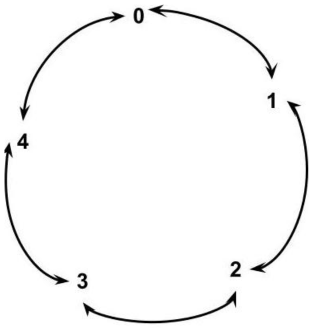


Figure 7.4: Page distance calculation

Now we can calculate the distance of any page from any other page, page numbers 4 and 1 on the distance of one, and 3 and 2 are on the distance of two from page number 0. Similarly, the distance of page number 2 from 0 is 2 clockwise and 3 anti-clockwise so here the smallest distance will be considered as 2.

LDF Page Replacement: This sub-section describes the working of LDF with the help of the following examples.

Example 1: Let us consider page reference string shown in Figure 7.5 i.e. 0 1 2 3 0 1 4 0 1 2 3 4 and number of frames in memory is 3. In the above-given reference string using LDF total page fault is 8. The first three-page reference cause page fault because initially memory frames are free and no page replacement is required. Fourth-page reference i.e. page number 3 will also cause page fault as now memory frames are full, so it requires page replacement, using LDF, page 1 will be replaced with page 3 because the distance of 0 and 1 from 3 is 2 and the distance of page 2 from 3 is 1. Pages 0 and 1 are on the same distance from current page 3 so the page which is next to page 3 will be replaced in anti-clock rotation and it is page number 1. Fifth-page reference 0 will not cause a page fault. Sixth page 1 will cause page fault so page 3 will be replaced because it is on longest distance from 1. The seventh page 4 will

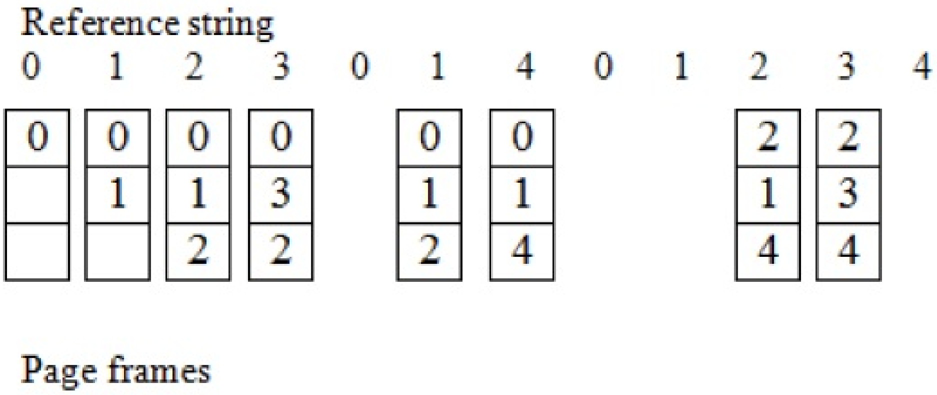


Figure 7.5: Example of LDF page-replacement algorithm with 3 memory frames

also cause page fault so page 2 will be replaced with 4. Page references Eight, Nine and Twelfth will not cause page faults but the tenth and eleventh pages will cause page faults. Total page faults for the above-taken reference string will be 8.

Example 2: Let us consider page reference string 0 2 1 3 5 4 6 3 7 4 7 3 3 5 5 3 1 1 1 7 1 3 4 1 and frames in memory is four, as shown in Figure 7.6. What is the total page fault? The total page fault in this reference string

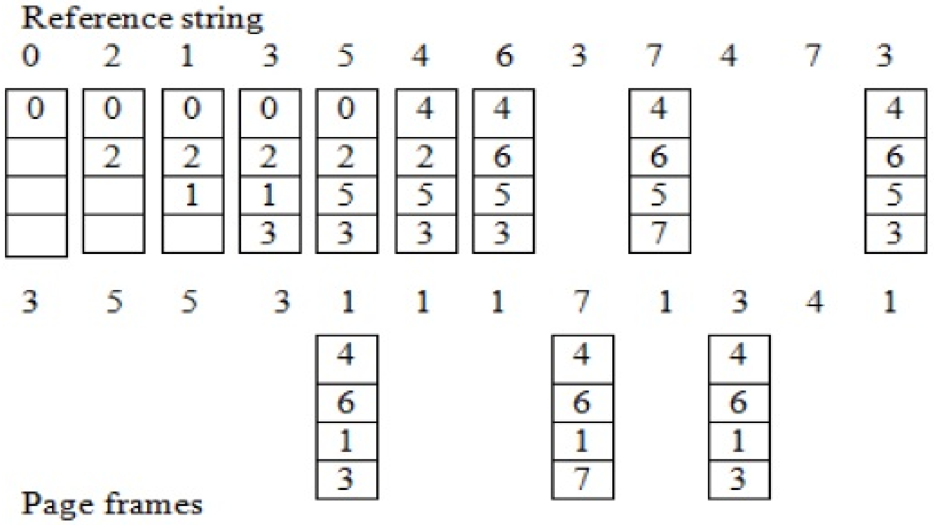


Figure 7.6: Example of LDF page-replacement algorithm with 4 memory frames

is 12. Starting four pages will cause page fault but no page replacement is required as frames are free. Fifth page number 5 will also cause page fault which requires page replacement and page number 1 will be replaced because it is on the longest distance from current page 5. Sixth-page number 4 will also cause page fault and page number 0 will be replaced as it is on the longest distance from current page 4. Seventh-page number 6 will also cause page fault and page number 2 will get replaced, and so on all other references will take place.

Distance Page Fault (Limitation): LDF suffers a problem named Distance Page Fault, when two pages are at the longest distance from each other, they are called distance pages and if they appear in reference string consecutively then they will replace each other and it will cause a page fault. This type of page fault in LDF is known as Distance Page Fault. Let us take reference string 0 1 0 0 2 0 3 3 2 1 1 2 1 3 1 3 1 to illustrate the Distance page fault problem. In this reference string page, 3 and 1 are on the longest distance from each other and appear in the string consecutively so they will replace each other and cause consecutive page faults.

Chance of occurrence of Distance page fault with a program is less because it will happen with only those programs where two jump statement of different page executes by calling each other and pages must be distance pages.

7.4 RESULTS AND ANALYSIS

This section will give a comparative analysis between FIFO, LRU, Optimal, and proposed LDF algorithms. Result analysis has been done using software written in C. Analysis is based on the following set of reference strings listed in Table 7.1. These page reference strings are used in academics to analyse the number of page faults of these algorithms. Initially program checks to page faults of each reference string by considering three memory frames and again

Table 7.1: List of Page Reference Strings

String No.	**Page Reference String**
S1	0 2 1 6 4 0 1 0 3 1 2 1
S2	1 2 3 4 1 2 5 1 2 3 4 5
S3	0 1 2 3 0 1 4 0 1 2 3 4
S4	0 2 1 3 5 4 6 3 7 4 7 3 3 5 5 3 1 1 1 7 1 3 4 1
S5	7 0 1 2 0 3 0 4 2 3 0 3 2 1 2 0 1 7 0 1
S6	5 4 3 2 1 4 3 5 4 3 2 1 5
S7	4 7 0 7 1 0 1 2 1 2 7 1 2
S8	5 0 2 1 0 3 0 2 4 3 0 3 2 1 3 0 1 5
S9	4 3 2 1 4 3 5 4 3 2 1 5
S10	0 2 1 0 3 0 2 3 0 3 2 1 3 0 1
S11	1 0 5 1 1 3 5 1 5 3 4 5 2 1 3 0 1 4 0 5
S12	0 1 0 0 2 0 3 3 2 1 1 2 2 3 2 1 3

it checked page faults by considering four memory frames.

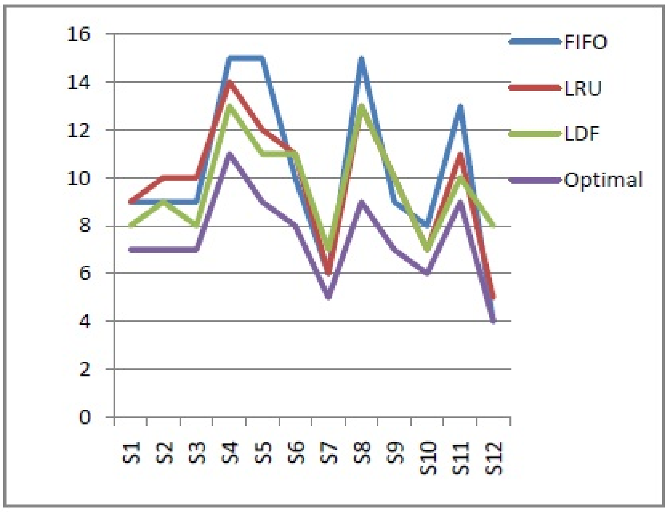


Figure 7.7: Variation of page fault in FIFO, LRU, LDF and Optimal with 3 frame

Figure 7.7 shows the comparison graph between FIFO, LRU, LDF and Optimal page replacement algorithms when three memory frames are considered. It is clear from this graph that LDF outperform FIFO and LRU in terms of page faults.

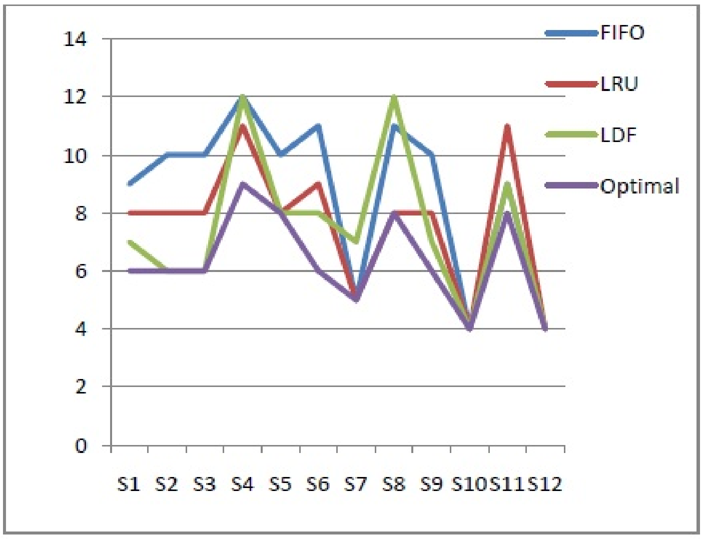


Figure 7.8: Variation of page fault in FIFO, LRU, LDF and Optimal with 4 frames

Figure 7.8 shown the comparison graph between FIFO, LRU, LDF and Optimal page replacement algorithms when four memory frames are considered. In this case, LDF again outperforms FIFO and LRU in terms of page faults.

From the results, it has been clearly shown that the performance of LDF is better than the FIFO and LRU and less than the Optimal algorithm in terms of page faults. The implementation overhead of LDF is less than FIFO, LRU and Optimal because it does not require any extra hardware or support to implement it. From experiments on different page reference strings it is observed that LDF does not suffer Belady's anomaly problem but it needs extra and real experiments to ensure it. Details of the experiment and results are shown in the given below tables and graphs.

Table 7.2: Comparison of page fault between LDF, FIFO, LRU, and Optimal

String	**FIFO**		**LRU**		**LDF**		**Optimal**	
Frames	3	4	3	4	3	4	3	4
S1	9	9	9	8	8	7	7	6
S2	9	10	10	8	9	6	7	6
S3	9	10	10	8	8	6	7	6
S4	15	12	14	11	13	12	11	9
S5	15	10	12	8	11	8	9	8
S6	10	11	11	9	11	8	8	6
S7	6	5	6	5	7	6	5	5
S8	15	11	13	8	13	12	9	8
S9	9	10	10	8	10	7	7	6
S10	8	4	7	4	7	4	6	4
S11	13	9	11	11	10	9	9	8
S12	4	4	5	4	8	4	4	4
Total	122	105	118	92	**115**	**90**	89	76
Average	10.2	8.75	9.83	7.67	**9.58**	**7.5**	7.42	6.33

Table 7.2 shows the page faults with corresponding algorithms as listed, these algorithms have been checked by considering three and four frames. From Table 7.2 it is clear that the total and the average number of page faults occurrence in LDF on taken data is less than LRU and FIFO.

Figure 7.9 shows the comparison of average page faults of all page reference strings listed in Table 7.1. LDF's average page fault is 9.58 and 7.5 when three and four memory frames are considered respectively, it is less than FIFO and LRU.

In strings S7 and S8, LDF suffers from a distance page fault problem because two distance pages are present one after the other.

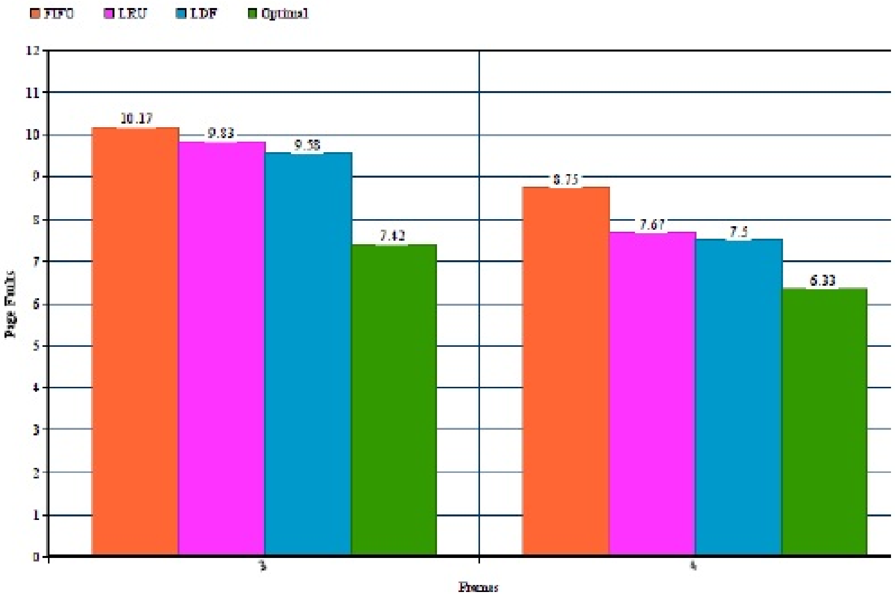


Figure 7.9: Average page faults of taken data set of reference strings

7.5 SUMMARY

This chapter gives a comparative study of commonly used page replacement algorithms such as FIFO, LRU and Optimal. A new approach for page replacement named longest distance first (LDF) has been proposed and compared with existing algorithms. This technique makes use of distance from the current page. From the observation, it has been found that LDF has better performance as compared to FIFO and LRU but lower performance as compared to Optimal. It has also been observed analytically that the implementation overhead of LDF is less than others.

LDF is tested against the page reference strings used which are available in literature but it needs to be tested in the real situation of paging. The distance page fault problem of LDF has already been mentioned. In future, researchers can address the distance page fault problem and perform rigorous testing in real scenarios to make improvements.

The preceding two chapters of this thesis improved existing solutions to better utilise available resources with both devices and networks. There should be an efficient IoT-based application for proper use of the IoT infrastructure. In this direction, the next chapter proposed an IoT-based underground mine monitoring and information sharing application system.

Chapter VIII

SENSEnuts IoT PLATFORM AND BAYES DECISION THEOREM-BASED MINE CONTROL SYSTEM

Life can be saved from the hazardous accidents happening in mines due to firedamp, dust explosion, and gassy environment. Existing mine environment monitoring systems are costly and need optimization for quality of services, real-time monitoring, management, and information sharing. Thus, this chapter presents an automated real-time monitoring, alarming, and information sharing system that will help to avoid such accidents. This system consists of a combined mechanism of SENSEnuts internet of things (IoT) stack platform, cloud server, and data analytics to detect, predict, and monitor real-time dangers of mine. This system generates alerts and shares information with the concerned official to take immediate preventive measures. The proposed system has been tested in simulated coal mine environments, and results show high accuracy, sensitivity, and accurate prediction of hazards due to CO, CO_2, CH_4, dust, and smoke.

8.1 INTRODUCTION

Mining industries have been listed as the most damaging site due to the mines' harsh and limited working conditions [292]. Mine Safety and Health Administration explains the main causes of mine accidents are the use of faulty equipment, explosions caused by the accumulation of gases, and structure failure, which lead to the loss of hundreds of lives every year [293]. In 2014, the accident rate in Punjab's salt range coal mines increased by 35 percent due to the explosions caused by toxic gases [294]. Human and animal life can be put in danger by the leakage of harmful gases in water wells or underground mines (UM). The greenhouse effects of CO_2 and methane (CH_4) gas also disturb the ecosystem [295]. Therefore, continuous and accurate monitoring of the mining environment is inevitable for protecting workers and the environment.

It is estimated that presently, total internet-connected devices are available at approximately 12.2 billion. IoT grew more rapidly than any other technology category on the global level due to the real-time services and applications coined by these high-end technologies [296]. In recent years, the development and growth of IoT can be seen in various areas like e-health services, Smart Grids, home automation, and environment monitoring due to advancements in radio frequency identification (RFID), cloud computing, and wireless sensor network (WSNs) technologies. IoT can enable the enhancement of existing or new information technology services and products to unlock benefits beyond mining automation. Low-cost commercial sensors equipped devices must be devolved for measuring and detecting the concentration of different atmospheric gases. Existing technologies allow monitoring of inaccessible places and assist in automatic event detection, control, and remote information sharing [297]. Zhang et al. tested an integrated WSN and a cable monitoring system for multi-parameter environmental monitoring at Sangwan Coal Mine, Erodes, China. This system requires two operational modes, one of which is periodic inspection and the other is interruption service. These operational modes provide feasibility for real-time monitoring of the mining condition [298].

The generation of toxic gases can be sensed by the integrated WSN with ambient intelligence [299]. This system presents an automated monitoring system that uses theories of situational awareness and spatiotemporal data analysis to make decisions in the UM. Mobile sensing is also introduced in this system for safety purposes in coal mines. Recently, an open-source, cost-effective Arduino-based IoT system has been introduced by Jo et al. [300-301] for early warning, detection and reporting of events in coal mines. Another WSN-based energy-efficient monitoring system has been outlined to enhance safety by early-event detection of the harsh environment of UM [302].

Xiao et al. proposed a multipath communication-based WSN and mine monitoring system to increase reliability [303]. Misra et al. have discussed how cost can be minimized, and power can be reduced in the wireless network for effective informatics in underground mines in harsh environments [304].

A WSN-based fire detection system was presented by [305], which is capable of detecting the location of the fire in coal mines due to the explosion of gases or landslides and controlling such emergencies. Moridi et al. [306] utilized the ZigBee technology to establish a real-time and reliable wireless networking system for the remote information sharing and monitoring of UM and tunnels.

From the literature, it has been identified following shortcomings in existing UM monitoring systems.

- The existing technology cost is more even though it is low power and user-friendly capability.
- Advanced mine management systems can collect a huge amount of data, but accurate monitoring of parameters is limited to using expansive and less flexible hardware and software.
- For underground mine safety systems, many challenges are still open and need an optimized, integrated, comprehensive, and efficient system with efficient monitoring, information sharing and management.

To overcome the above shortcomings, this chapter proposed a system intended for underground mines monitoring gas level, smoke level, air quality level, and the temperature of the UM. It aims to develop enhanced underground mine safety systems based on IoT, cloud-enabled, cost-effective, efficient mine monitoring and intelligent controlling systems. The key contributions of this research work are as follows:

- This chapter proposed a novel SENSEnuts IoT stack platform-based environmental monitoring, analysing, predicting, and information sharing system for UM.
- Use of Thingspeak IoT analytics platform to store sensor data for analysis, management, and information sharing. It also makes whole system implementation easy and cost-effective.
- This system uses a probability-based mathematical model to exploit the historical and real-time monitored data to predict pre-alert danger.
- Comprehensive experimental analysis is performed to evaluate the performance of the proposed system.

The remaining of this chapter's work is organized as follows. In section 8.2, proposed systems are presented, and section 8.3 presents a prototype model and its deployment. Experimental results and their outcome after the analysis are presented in section 8.4. Finally, section 8.5 ends with the conclusion of the proposed work.

8.2 PROPOSED SENSEnuts IoT STACK BASED UNDERGROUND MINE MONITORING SYSTEM

With the advancement and adaptability of IoT technology, it is inevitable to develop IoT based application system. An IoT-based system has the following characteristics:
(1) IoT is an internet-connected network of smart things such as sensors, actuators, smart routers, servers, communicating devices, etc. with self-adapting, dynamic, self-configuring, interoperable protocols, unique identity, and integrated with information network capabilities.
(2) Each smart Thing can be identified by assigning a unique digital name such as IPv4, IPv6, and 6LoWPAN identification. The relationship between these devices can be maintained in the digital domain without any physical connection [307].
(3) Dynamic, self-adapting using an interoperable protocol with a unique identity, devices can communicate information to the other related devices and servers for further processing and application support.

8.2.1 System Architecture

This section proposes a new IoT-based platform for monitoring, data analysis, and information sharing of UM. The functions, as shown in Figure 8.1, of IoT-based platforms are mainly represented by 5-layer architecture [308]. These layers are named Application, Service, Support, Network, and Link Layer. The detailed function of each layer is discussed below.

Link and Network Layer

These layers are responsible for transferring collected data by sensors to remote servers. The proposed system contains SENSEnuts platform-based sensors for data collection and transmission. It contains Wi-Fi, radio, and a USB gateway module.

SENSEnuts microcontroller: SENSEnuts is the most affordable, compact, and advanced IoT-enabled platform for research and development by Eigen Technologies. This platform is useful in various fields, such as industrial applications, academics, and research, to benefit students, faculties, and scientists across various domains. SENSEnuts platform is supported by a user-friendly

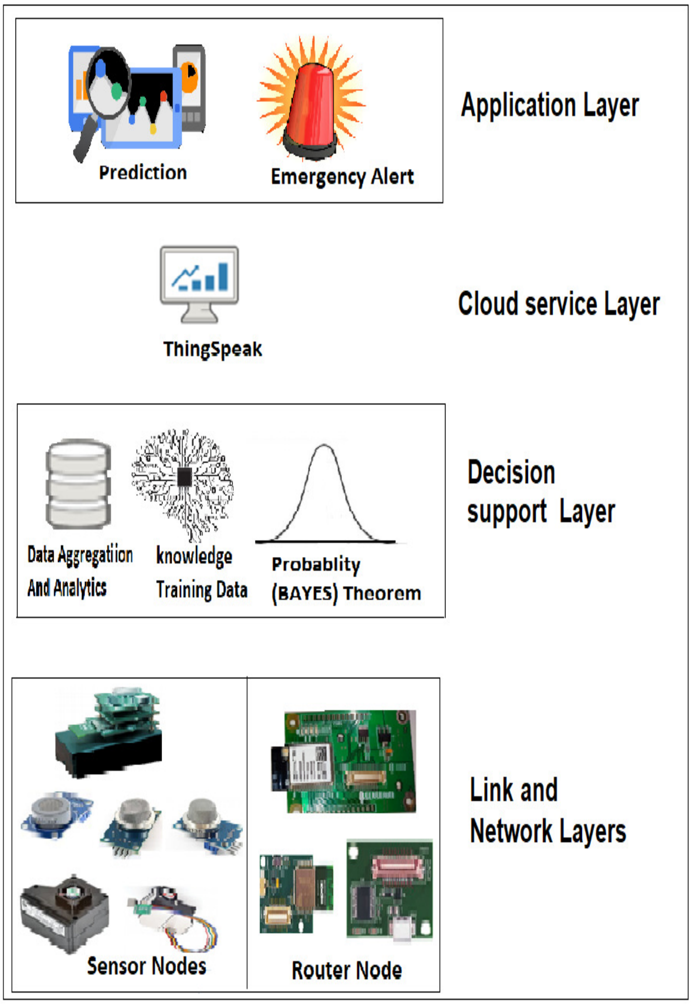


Figure 8.1: The architecture of the proposed SENSEnuts based underground mines monitoring system

GUI and effortlessly integrated with various sensors to monitor stimuli and customize them for various applications, as shown in Figure 8.2(a). It consists of communication modules such as – RADIO, Wi-Fi, and USB GATEWAY module.

Communication module: It may consist of one of the following modules.

Radio Module: It comprises of microcontroller and a transceiver for sending, receiving, and processing the data. It has a 32-bit RISC JN 5168 Microcontroller, 1-32MHz clock speed 256KB flash. Figure 8.2(b) shows the USB Gateway module connected to SENSEnuts.

USB Gateway Module: It is used to load programs into the microcontroller and works as an interface between the device and network gateway for an asynchronous serial data transfer. USB protocols are handled by the device and have the following features, Data Transfer rate of 115200 baud, 128 bytes receive buffer, and 256 bytes transmit buffer. Figure 8.2(c) shows the USB

Gateway module connected with the SENSEnuts module used in the proposed system.

Wi-Fi Gateway Module: SENSEnuts support Low-power Wi-Fi enabled module with a single-band 2.4GHz IEEE 802.11b/g/n 1x1 Wi-Fi transceiver and Integrated with SPI-serial flash memory for software Broadcom BCM43362 chip. It also supports every Wi-Fi security mode with Open, WPA2-PSK, WEP, and WPA. Figure 8.2(d) shows the Wi-Fi module used in our system. It contains 128kB SRAM and integrated 1MB Flash memory which operates in the temperature range from -30°C to +85°C.

Sensors: Following listed below sensors are used in our system to monitor stimuli of the environment.

CO Sensor Module: This sensor is used to sense the presence of CO and CO_2 concentration. Its Concentration detection ranges are 20 to 2000 ppm for CO and 350 to 10000 ppm for CO_2. Figure 8.2(e) shows the CO sensor used in our system, which works on a 6 Volt input power supply. Smoke Sensor Module: A smoke sensor is an electronic fire-detection device that repeatedly senses the existence of smoke, as it is a key indicator of fire, and sends it to the cloud for analysis. Figure 8.2(e) shows the Smoke sensor used in our system.

AQI Sensor module: The AQI is an index for reporting daily air quality. This

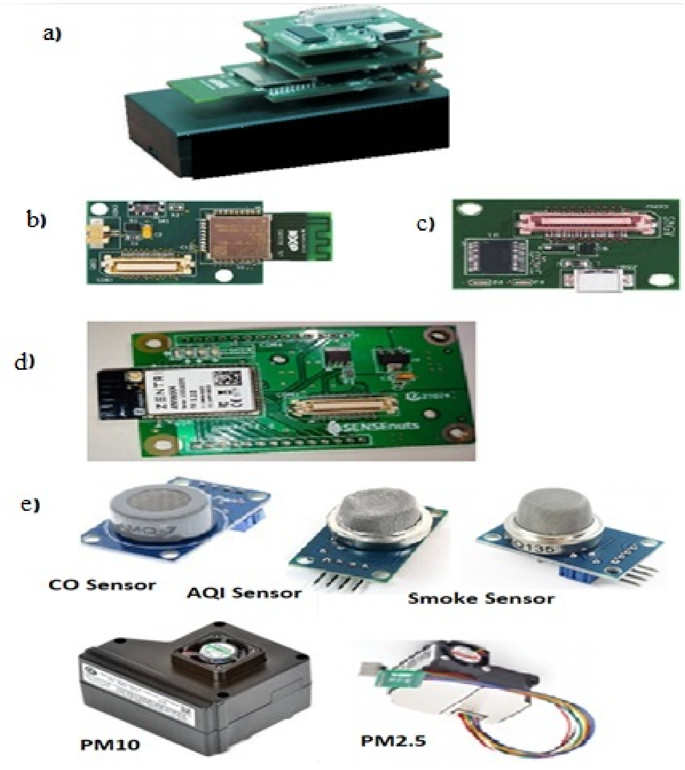


Figure 8.2: System components, (a) SENSEnuts Microcontroller, (b) RADIO module (c) USB gateway, (d) SENSEnuts Wi-Fi module, and (e) sensing nodes

module senses the AQI for five air pollutants recommended by the Clean Air Act: carbon monoxide, ground-level ozone, sulphur dioxide, particle pollution (particulate matter), and nitrogen dioxide. Figure 8.2(e) shows the AQI sensor used in our system.

PM 10 Module: This module is used to sense PM10 particles. PM10 particles include mild dust, spores, pollen, smoke, and dirt from factories, farming, and roads. It is produced by grinding and crushing soil and rocks and then spread to the atmosphere by air. Figure 8.2 (e) shows the PM10 sensor used in our system.

PM2.5 Module: Small particles that are 2.5 micrometres in size are called PM2.5. These consist of heavy metals and toxic organic compounds. They are generated from automobile exhaust, landfill and garbage, processing and smelting of metals. Figure 8.2(e) shows the PM2.5 sensor used in our system.

Networking: The performance of the mine safety systems primarily depends on the deployment and placement of different components in underground mines. In the proposed system, sensing elements are deployed using linear topology along with wireless communication gateways such as radio module and Wi-Fi module.

Decision Support

This layer is responsible for managing the data generated by sensors using the mathematical model, probability theory, statistical analysis, and applications/software. This system has two classes of data: monitored data and historical data. The main issue is how to use both data classes to generate emergency alerts. To address this issue, the system utilizes a Bayesian prediction model. This approach first forms a relation to a response using historical data sets. Then using this relation, it predicts an alert for newly monitored data.

For determining the threat probability, suppose there is N number of sensors (S) deployed, and their readings are observed at time t_1, t_2,...... t_k. Consider p_i(t) as the reading of sensor S_i at a time t, and Mk is the set of all sensor readings at time t_k.

After the complete setup of the mine system and its sensors, Baye's theorem calculates the posterior probability (prediction) of each mine parameter (CN) using Equation (1).

$$P(C_N/M_k) = (P(M_k/C_N) * (P(C_N))/(P(M_k) \tag{1}$$

Where P(M$_k$) is evidence of parameters reading from sensors. P(M$_k$/C$_N$) is a conditional likelihood, and P(C$_N$) is a prior probability, which will be estimated by training historical data. The conditional likelihood P(M$_k$/C$_N$) is calculated using Equation (2) by integrating all parameter likelihood on the whole domain D, using the probability distribution function Pdf($\binom{N}{p}$, C_N).

$$P(M_k/C_N) = \int_a Pdf(M_k/\binom{N}{p}, C_N)).D \tag{2}$$

The likelihood of the whole monitored set M$_k$ of sensors is evaluated using Equation (3).

$$Pdf(M_k/\binom{N}{p}, C_N)) = \prod_{j=1,i=1}^{j=N,i=N} Pdf(p_j(t_i)|N_p, C_N)) \tag{3}$$

The normal distribution of measurement of sensors is evaluated using Equation (4)

$$Pdf(p_j(t_k)|N_P, S_N) = Normal \Big\{ (p_j(t_k); N_{r_j})(N_P t_k), N(\sigma_e)_j \tag{4}$$

Here σ is the standard deviation calculated using the sensor's reading values. The statistical variables mean, standard deviation and normal distribution used in this method are calculated over reading x using Equations (5), (6), and (7).

$$Average(\bar{x}) = \left(\frac{1}{N}\right) * \sum_{i=1}^{N} x_i \tag{5}$$

$$\sigma = \sqrt{\left(\frac{1}{(N-1)}\right) * \sum_{i=1}^{N} (x_i - \bar{x})^2} \tag{6}$$

$$NormalDistributionf\left(x/\bar{x}, \sigma^2\right) = \left(1/\sqrt{2\pi\sigma^2}\right) e^{-(x-\bar{x})^2/2\sigma^2} \tag{7}$$

Cloud Service

In this proposed underground mine safety system, sensors' data are efficiently managed by the IoT analytics platform Thingspeak. The Thingspeak platform allows aggregation, visualization, and analysis of live data and facilitates

collecting data in the cloud. It can instantly visualize sense data using inbuilt tools like Python, MATLAB.
Some of the key functionalities of ThingSpeak include:

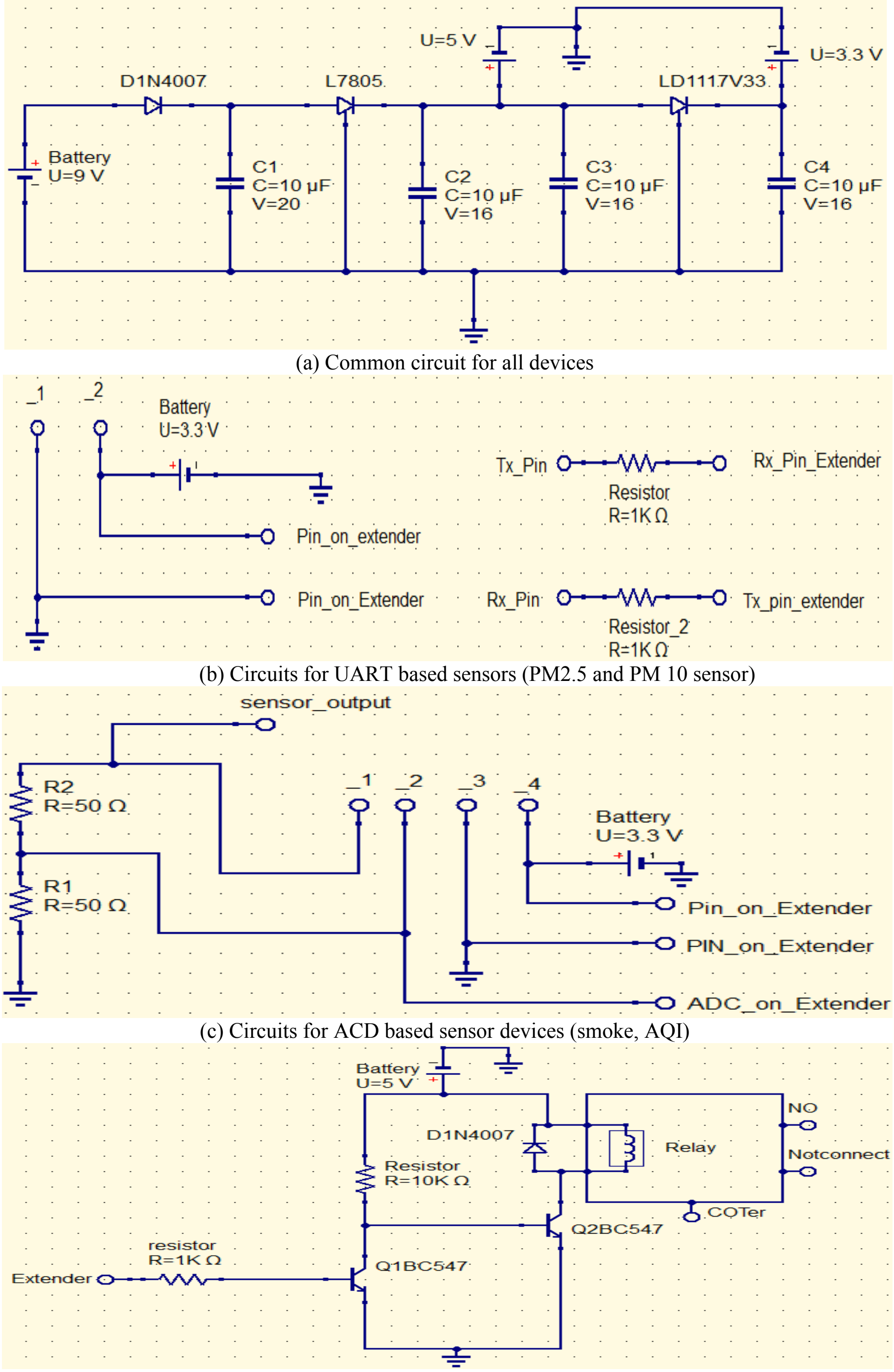
- Easily configured devices that can send their data to the ThingSpeak platform using IoT protocols.
- Real-time data visualization.
- ThingSpeak is an open API for real-time data collection.
- Based on schedule and events, you can run your IoT analytics automatically.
- Easy to build an IoT-based system without setting up local servers and developing web software.
- ThingSpeak allows us to create various applications, such as remote logging applications; locations based applications, and keep the status of the network of things updated.

Application Layer and Information Sharing

This layer comprises components and functions responsible for sharing information and alerts with other applications and controlling authority. The proposed system not only detects abnormalities in mines but is also capable of generating early-warning and remote information sharing in the form of alarms and emergency lights with the help of application layer functionalities. This system is based on the Bayesian prediction model approach, which is why it not only depends on the threshold values but adjusts according to past experiences. The warning signal inside the mine was propagated with alarms and can be shared with any type of IoT-based application and devices such as smartphones, buzzer alarms, laptops, etc. The proposed system has been specifically designed for air quality monitoring, gas monitoring, and smoke monitoring assessment in UM. Figure 8.1 shows the basic architecture of the proposed system. In this system, sensing units are based on the SENSEnuts module, and sensors are attached to the SENSEnuts microcontroller. The sensor nodes capture mine environment parameters-related information and transmit it to the IoT cloud platform Thingspeak. The prediction model extracts parameter types and predicts their value depending on the train data. Thus, this system enables decision-making to detect danger and alert the concerned official to take immediate prevention measures.

8.2.2 Use of Circuits in the System

Sensors used in our system are 3-pin sensors-Vin (input voltage), GND (ground), and DATA (sensed value). These sensors cannot be directly connected with the SENSEnuts module. Thus, the circuit shown in Figure 8.3 (a) connects these sensors with the SENSEnuts. Our system's sensing nodes are either UART-



(a) Common circuit for all devices

(b) Circuits for UART based sensors (PM2.5 and PM 10 sensor)

(c) Circuits for ACD based sensor devices (smoke, AQI)

(d) Circuit to control the relay by SENSEnut

Figure 8.3: Connecting Circuits

based or ADC-based sensors. As the output format of both sensing units is different thus, it requires the different circuits to operate on them simultaneously. Hence, for UART-based sensors, the circuit used to operate is shown in Figures 8.3 (b),(c), and (d). This system uses two UART-based sensors – PM10 and PM 2.5. These circuits are designed by SENSEnuts producer Eigen Technology Pvt. Ltd.

Figure 8.3(b) is used to operate PM10, PM2.5 and Figure 8.3 (c) for ADC-based Sensor (AQI, SMOKE). Sensors in the system operate at a minimum voltage of 5V, while the SENSEnuts module operates the devices whose Operational voltage is 3.3V. Thus, to use these sensing units with the SENSEnuts device, we need to convert the input 5V of the sensing unit equivalent to 3.3 V of the output supply, which makes the SENSEnuts module compatible with our sensors. This conversion of voltage is done by a relay circuit, as shown in Figure 8.3(d).

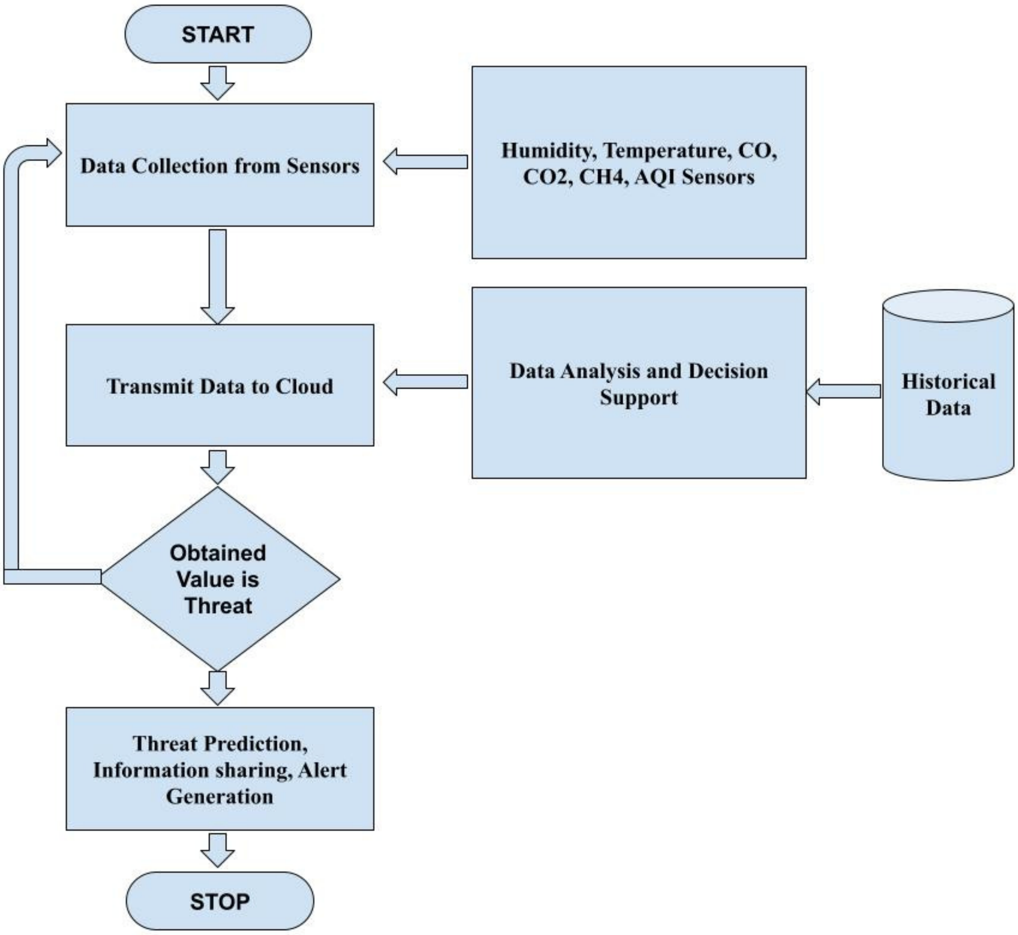

START
Data Collection from Sensors
Humidity, Temperature, CO, CO2, CH4, AQI Sensors
Transmit Data to Cloud
Data Analysis and Decision Support
Historical Data
Obtained Value is Threat
Threat Prediction, Information sharing, Alert Generation
STOP

Figure 8.4: Working flowchart of System

8.2.3 Working Flowchart

Figure 8.4 shows the diagrammatical flow of data from one process to another process involved in our system. This wireless sensor network's application system will measure the concentration of various gases present in the ambient environment of underground mines using various sensors (gases, air quality indices) and send this data to a ThingSpeak IoT platform with the help of a Wi-Fi module. This data is then accessed from ThingSpeak and analyzed to detect danger. This system also stores all the data in the computer for future inspection. The main concern is how to generate a pre-alarm for emergencies. Our system has two sources of information: monitoring data and historical data. By analyzing the historical data, the presumptions are created by visualizing monitored information. Therefore, an alarm triggers when sensor values exceed the threshold level set by monitoring the historical data.

8.3 SYSTEM IMPLEMENTATION

This section describes working along with dependencies between different system components and presents the deployment of a prototype model to check its functioning and performance.

8.3.1 Under Ground Mine Monitoring System

The complete setup and proposed model of the system are shown in Figure 8.5. It is a combination of Smart SENSEnuts-based IoT hardware, data analytics with probability theory, and deployed over the ThingSpeak platform. The system program runs the probability model by obtaining real-time data from sensors and generates threat prediction and alerts, simultaneously updating historical information stored in the database. The system begins by collecting historical mine threat data using low-cost SENSEnuts sensors and ThingSpeak. Next, it analyses historical data from ThingSpeak, where it inspects and cleans the data to fill missing values and remove outliers, noise, or other anomalies. After that, use the analyzed mine data to predict future threats with sophisticated analysis functions available with the ThingSpeak platform. Next, a predictive algorithm is developed using the Bayesian Machine learning model with various input data sets, and training is performed using the time series tool. After evaluating the performance, the predictive algorithm is deployed over ThingSpeak to forecast and display the values of

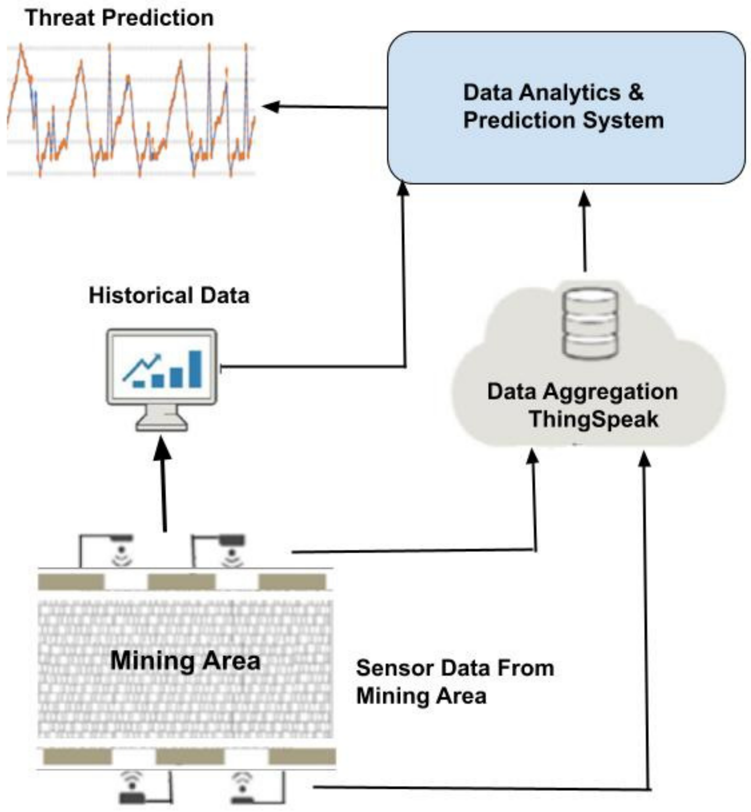

Threat Prediction
Data Analytics & Prediction System
Historical Data
Data Aggregation ThingSpeak
Mining Area
Sensor Data From Mining Area

Figure 8.5: Underground mine monitoring system

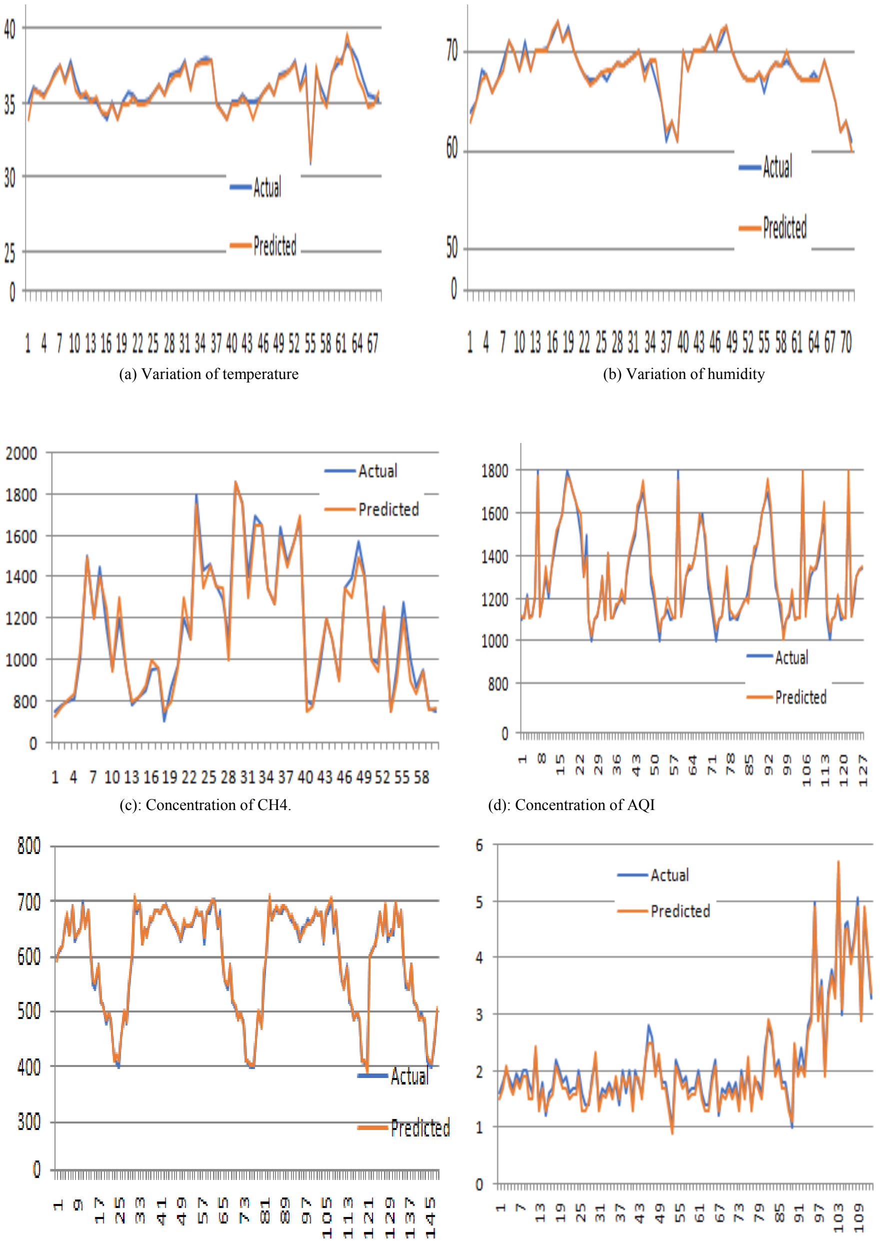
different sensors.

8.3.2 Prototype Deployment

The whole prototype system is deployed in an identical environment to the underground mine in the laboratory. Monitoring sensors are fitted on top of the sidewalls of the laboratory as gases concentrate on the roof. Gases and smoke fumes are randomly generated and installed Wi-Fi-enabled sensors sense them and send these data to the gateway, which is further transmitted to the cloud for monitoring and analysis.

8.4 RESULT AND ANALYSIS

The performance of the UM system towards the monitoring and prediction is evaluated under standards, threshold values of gases, and mine requirements specified in [294].



(a) Variation of temperature

(b) Variation of humidity

(c): Concentration of CH4.

(d): Concentration of AQI

(e): Concentration of CO2.

(f): Concentration of CO.

Figure 8.6: Actual and predicted values of sensors

Figure 8.6(a) and (b) show the variation of measured and predicted values of temperature and humidity of the testing environment. The temperature and humidity of the environment vary between 34-39 ^{0}C and 60-70 %, respectively. The maximum and minimum temperature of the environment was maintained at 40 ^{0}C and 33 ^{0}C, respectively. The minimum and maximum humidity were maintained at 60 and 72 %. Obtained results indicate that the proposed model's predicted and actual measured values are almost identical. To prevent mishaps due to harmful gases and particles, it is inevitable to monitor the real-time concentration of gases. Therefore, the prototype of the proposed system was tested against the real-time monitoring of CH_4, CO_2, CO, and AQI in an identical environment. The concentration of these gases is maintained as per the standards of mine safety. Figure 8.6 shows the variations of actual reading and predicted reading, and it is clearly showing almost identical results. Figure 8.6 (c) shows the concentration of CH_4, which varies between 750 to 1900 ppm. Similarly, Figures 8.6(d), 8.6(e), and 8.6(f) show the concentration of AQI, CO_2, and CO, and their values vary from 1000-1800 ppm, 450-900 ppm, and 1- 6 ppm respectively. The concentrations of these gases are measured against time with a set interval of 2 minutes.

We tested our system several times to check its response. From the response, as shown in Table 8.1, the buzzer was activated whenever threshold limits were reached. Out of 25 observations for true positive, and true negative responses; 21 and 22 times responded in truly positive, and true negative cases respectively. This observation shows that system has sensitivity near 85% in all cases. From the analysis of experimental results, the following outcomes of the system are identified.

- The prediction accuracy of the system is almost identical to actual values.
- Response sensitivity is very high, and it is near 85
- The whole system is deployed over an IoT analytical platform without the deployment of web infrastructure hence reducing the deployment cost of the system.
- The system can perform on-demand visualization, data analysis, and easy sharing of results with other applications.

Table 8.1: Response of Proposed System

Response Type	True	False	Response Sensitivity
Positve	21	4	84
Negative	22	3	88

8.5 SUMMARY

Safety has long been a major concern in the underground mining business. There are many safety gears are available in the market along with an expected increase in mining safety compared to previous decades, but mining accidents still occur. This chapter presents an underground mine safety system based on the SENSEnuts IoT platform with the integration of ThingSpeak IoT analytics and cloud computing. Experimental results of the system indicate an accurate and effective response. Integration of ThingSpeak and Cloud makes it easy for data acquisition, management, analysis, and information sharing. Also, the deployment cost of the whole system is reduced as no web infrastructure and local servers are required.

Chapter IX

CONCLUSIONS AND FUTURE SCOPE

IoT networks and applications are expanding exponentially, requiring many technological enhancements. Due to the resource-constrained nature of IoT devices, optimizing communication protocols, architectures, and hardware to improve QoS parameters like latency, energy consumption, throughput, accuracy, efficiency etc., is imperative. In this direction, this PhD work proposed solutions to above said problems.

This chapter provides the contributions of the research work in achieving the set objectives along with the future scope of the research in the area of IoT.

9.1 CONTRIBUTIONS

To achieve set objectives, this research proposed the following work to improve the QoS parameters of IoT networks, and extensive simulation is performed to verify it.

The first proposed work in this thesis is the FDIPA IPv6 addressing scheme, which generates a large number of unique IPv6 addresses using device location and time. The simulation results reveal that the proposed scheme not only generates a large number of unique addresses but also minimizes communication overhead and energy consumption during the address assignment phase.

The second proposed work in this thesis is the secured DAD process which mitigates the DoS attack from malicious nodes. The proposed method is evaluated under the different attack scenarios, and the result reveals that the proposed method successfully avoided attacks. Simulation results further show that the proposed method adds less communication overhead and energy consumption than existing solutions.

The third proposed work in this thesis is the R-CMT scheduling scheme for multipath data transmission. The proposed method calculates the rank of each independent path based on its successful data chuck transmission rate and accordingly schedules data chunks. From the experimental evaluation, it is observed that R-CMT achieves better performance in terms of throughput, cwnd growth, and file transfer time than referenced schemes.

Apart from the above three key contributions, this thesis work also presents a new paging technique to maximize cache and flash memory utilization, an IoT-based underground mine monitoring and controlling application, a literature survey of IPv6 addressing schemes, and CMT and MP-TCP transport layer multipath protocols.

9.2 SCOPE FOR FUTURE WORK

We accomplished the work in this thesis to meet the defined objectives; however, there are still many study areas in which researchers may strive to improve the present IoT network architecture. The literature review on IPv6 addressing and transport layer multipath routing methods is presented but still needs continuous study to include ongoing research work. In the future, issues like reconnaissance attacks on EUI-64 IPv6 addressing and frequent packet losses in IPv6-based networks should be addressed. During addressing, NDP suffers from the flooding attack of malicious RA and NS messages, which causes congestion and denial of network services. So, in the future, it needs a novel solution to mitigate such issues. Path, rank-based data chunk scheduling of CMT, can be further extended into MP-TCP.

REFERENCES

[1] D. Evans, “The Internet of Things how the next evolution of the Internet is changing everything”, Cisco Systems,2011.

[2] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), 2018. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide.

[3] The Internet of Things is here and growing exponentially, IHS Markit, 2017.Available: https://cdn.ihs.com/www/pdf/IoT-ebook.pdf.

[4] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw., Vol. 54, no. 15, pp. 2787-2805,2010.

[5] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, “Vision and challenges for realising the Internet of Things”, Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): a vision, architectural elements, and future directions,” Future Generation Computer Systems, Vol. 29, pp. 1645–1660, 2013.

[7] G. Kumar, P. Tomar, “A Survey of IPv6 Addressing Schemes for Internet of Things,” International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), Vol. 2, pp. 43-57, 2018.

[8] A. Zanella, N. Bui, A. Castellani, L. Vangelista, “Internet of things for smart cities”, IEEE Internet of Things journal, Vol. 1, no. 1, pp.22-32, 2014.

[9] T. Savolainen, J. Soininen, and B. Silverajan, “IPv6 addressing strategies for IoT,” IEEE Sensor Journal, Vol. 13, no. 10, pp.3511-3519, 2013.

[10] J.A. Vimal, R. S. Albert, P.B. Daisy, “Algorithmic Approach to security Architecture for Integrated IoT Smart Services Environment”, World Congress on Computing and Communication Technologies (WCCCT), 2017.

[11] C. Shanzhi, X. Hui, L. Dake, H. Bo, and W. Hucheng, “A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective”, IEEE Internet of things journal, vol. 1, no. 4, pp. 349-359, 2014.

[12] P. Pandey, “Prevention of ARP spoofing: A probe packet based technique,”in Proc. IEEE 3rd Int. Adv. Comput. Conf. (IACC’13), 2013, pp. 147–153.

[13] M. Mavani, K. Asawa, “Privacy Preserving IPv6 Address Auto-Configuration for Internet of Things”, In: Intelligent Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 19, Springer, Singapore, 2018.

[14] X. Wang and Y. Mu, “A secure IPv6 address configuration scheme for a MANET,” Secur. Commun. Netw., vol. 6, no. 6, pp. 777–789, 2013.

[15] F. Gont, A. Cooper, D. Thaler, “Security and Privacy Considerations for IPv6 Address Generation Mechanisms”, Internet Engineering Task Force, RFC 7721, 2016.

[16] S. K. Singh, T. Das and A. Jukan, ”A Survey on Internet Multipath Routing and Provisioning,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2157-2175, 2015, doi: 10.1109/COMST.2015.2460222.

[17] T.D. Wallace, A. Shami, A review of multihoming issues using streaming control transmission protocol, IEEE Communications Surveys & Tutorials, Vol. 14, pp. 565–578, 2012.

[18] D. Mishra, A. Gunasekaran, S.J. Childe, T. Papadopoulos, R. Dubey, and S. Wamba,”Vision, applications and future challenges of Internet of Things: A bibliometric study of the recent literature ”, Industrial Management & Data Systems, Vol. 116, No. 7, pp. 1331-1355, 2016.

[19] A. Triantafyllou, P. Sarigiannidis, T. Lagkas, “Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends”, Wireless Communications and Mobile Computing, Vol. 2018, Article ID 5349894, 24 pages, 2018.

[20] J. A. Stankovic, ”Research Directions for the Internet of Things,” IEEE Internet of Things, vol. 1, no. 1, pp. 3-9, Feb. 2014, doi: 10.1109/JIOT.2014.2312291.

[21] J. Granjal, E. Monteiro, and J.S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues" IEEE Communications Surveys and Tutorials, Vol. 17, no. 3, pp.1294-1312, 2015.

[22] C.C. Sobin, "A Survey on Architecture, Protocols and Challenges in IoT". Wireless Personal Communications, Vol. 112, pp. 1383–1429, 2020. https://doi.org/10.1007/s11277-020-07108-5

[23] A. Dunkels, T. Voigt, and J. Alonso. "Making TCP/IP Viable for Wireless Sensor Networks," in Proceedings of the First European Workshop on Wireless Sensor Networks (EWSN'04), work-in-progress session, Berlin, Germany, Jan. 2004.

[24] R.I. Chang, C.H. Chang, C.C. Chuang, "Scan-line IP assignment for wireless sensor networks", In 5th International Conference on Wireless Communications, Networking and Mobile Computing, Vol. 24, 2009, pp. 1-5.

[25] R.I. Chang, and C.C. Chuang, "A new spatial IP assignment method for IP-based wireless sensor networks", Personal and Ubiquitous Computing, Vol. 16, pp. 913-928, 2012.

[26] C. Cheng, C. Chuang, and R. Chang, "Three-dimensional location-based IPv6 addressing for wireless sensor networks in smart grid," in Proc. IEEE 26th Int. Conf. Adv. Inf. Netw. Appl., Mar. 2012, pp. 824–831.

[27] X Wang, Y Yang, Y Yao, H Cheng, "An address configuration protocol for 6LoWPAN wireless sensor networks based on PDAD", Computer Standard Interfaces , Vol. 36, no. 6, pp.918-927, 2014.

[28] M.N. Hussein, R. Abdulla,T. O'Daniel, and M. Abbas, "Advanced location-based IPv6 address for the node of wireless sensor network," International Journal of Electrical and Computer Engineering, Vol. 10,no. 3, pp. 2474-2483, 2020.

[29] T. O'Daniel, M.N. Hussein, and R. Abdulla, "Location Determination Using Tesselated Addresses in IPv6 Wireless Sensor Networks," Advanced Science Letters, Vol. 24,no. 3, pp.1723-1726, 2018.

[30] E. Dart, W. Beebee, W. George, R. Asati, C. Pignataro, and H. Singh, “Enhanced duplicate address detection,” Internet Engineering Task Force, Fremont, CA, USA, RFC 7527, 2015.

[31] X. Wang and H. Qian, “Hierarchical and low-power IPv6 address configuration for wireless sensor networks,” Int. J. Commun. Syst., vol. 25, no. 12, pp. 1513–1529, 2012.

[32] S. R. Hussain, S. Saha, and A. Rahman, “SAAMAN: Scalable address autoconfiguration in mobile ad hoc networks,” J. Netw. Syst. Manage., vol. 19, no. 3, pp. 394–426, 2011.

[33] H. Shin, E. Talipov, and H. Cha, “Spectrum: Lightweight hybrid address autoconfiguration protocol based on virtual coordinates for 6LoWPAN,” IEEE Trans. Mobile Comput., vol. 11, no. 11, pp. 1749–1762, 2012.

[34] X. Wang, H. Cheng, and Y. Yao, “Addressing With an Improved DAD for 6LoWPAN”, IEEE Communications Letters, Vol. 20, No. 1, pp. 73-76, 2015.

[35] M. Polese, F. Chiariotti, E. Bonetto, F. Rigotto, A. Zanella and M. Zorzi, ”A Survey on Recent Advances in Transport Layer Protocols,” in IEEE Communications Surveys and Tutorials, vol. 21, no. 4, pp. 3584-3608, 2019, doi: 10.1109/COMST.2019.2932905.

[36] M. Li, A. Lukyanenko, Z. Ou, A. Ylä-Jääski, S. Tarkoma, M. Coudron, and S. Secci,”Multipath transmission for the internet: A survey.”, IEEE Communications Surveys and Tutorials, Vol. 18, no. 4, pp.2887-2925, 2016.

[37] I. F. Akyildiz, and J. M. Jornet, “The Internet of nano-things,” IEEE Wireless Commun., vol. 17, no. 6, pp. 58–63, 2010.

[38] R. Hinden, and B. Haberman, ”Unique local IPv6 unicast addresses.” No. rfc4193. 2005.

[39] F. Ye and R. Peng,“A survey of addressing algorithms for wireless sensor networks”, IEEE the 5th International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, China, 2009, pp. 1-7.

[40] S. Thomson, T. Narten, and T. Jinmei, “IPv6 Stateless Address Auto configuration,” Network Working Group, RFC 4862, Sept. 2007.

[41] T. Narten, R. Draves,“Privacy Extensions for Stateless Address Autoconfiguration in IPv6” RFC 4941, 2007.

[42] A. Savvides, C. Han, M.B. Strivastava, “Dynamic fine-grained localization in ad-hoc networks of sensors”, In: Proceedings of the 5th international conference on mobile computing and networking. Rome, Italy,2001, pp 166–179.

[43] Contiki: The Operating System for Connecting the Next Billion Devices—the Internet of Things. http://www.sics.se/contiki/

[44] C. Y. Cheng, C. C. Chuang, R. I. Chang, “ Lightweight Spatial IP address Configuration for IPv6-based Wireless Sensor Networks in Smart Grid”, SENSORS 2012, IEEE,2012, pp 1-4.

[45] M. Chakraborty, N. Chaki, “An IPv6 based Hierarchical Address Configuration Scheme for Smart Grid”,Applications and Innovations in Mobile Computing (AIMoC), IEEE, 2015, pp. 109-116.

[46] M.M. Kassem, H.S. Hamza, and I.A. Saroit, “A Clock Skew Addressing Scheme for Internet of Things”, PIMRC, 2015, pp. 1553-1557

[47] S. Hyojeong, E. Talipov, and C. Hojung, “IPv6 lightweight stateless address autoconfiguration for 6LoWPAN using color coordinators,” in Proc. IEEE Int. Conf. Pervas. Comput. Commun., 2009, pp. 1–9.

[48] R.K. Mishra, N. Chaki, S. Choudhury, “An Addressing Scheme for Massive Sensor Networks,” In IFIP International Conference on Computer Information Systems and Industrial Management, Springer, Cham, 2019, pp. 481-492.

[49] A. Dunkels, T. Voigt, N. Bergman, and M. Jönsson. “The Design and Implementation of an IP-based Sensor Network for Intrusion Monitoring,” Swedish National Computer Networking Workshop, Karlstad, Sweden, Nov. 2004.

[50] X. Wang, D. Gao, “Research on IPv6 address configuration for wireless sensor networks,” International Journal of Networks Management, Vol. 20, pp. 419–432, Nov. 2010.

[51] W. Xiaonan, Z. Shan, "An IPv6 address configuration scheme for wireless sensor networks based on location information," Telecommunication Systems, Vol. 52, pp. 151-60, Jan. 2013.

[52] X. Wang , D. Le, H. Cheng, "Location-based ipv6 address configuration for vehicular networks," Journal of Network and Systems Management, Vol. 24, pp. 257-84, Apr. 2016.

[53] M. Mavani, K. Asawa, "Privacy enabled disjoint and dynamic address auto-configuration protocol for 6Lowpan", Ad Hoc Networks, Vol. 79, Pages 72-86, 2018.

[54] X. Wang, D. Le, and H. Cheng, "Hierarchical addressing scheme for 6LoWPAN WSN". Wireless Netw, Vol. 24, pp. 1119–1137, 2018. https://doi.org/10.1007/s11276-016-1394-9.

[55] S. A. Abdullah, "SEUI-64, bits an IPv6 addressing strategy to mitigate reconnaissance attacks", Engineering Science and Technology, an International Journal, Vol. 22, no. 2, pp. 667-672, 2019. https://doi.org/10.1016/j.jestch.2018.11.012.

[56] L. Xu, L. Jianwei, J. Hao, L. Dan, C. Han, "IPV6 Address Configuration Method in 6LoWPAN Oriented to the Internet of Power Things", Smart Grid and Innovative Frontiers in Telecommunications. SmartGIFT, vol 373, 2021. https://doi.org/10.1007/978-3-030-73562-3-10.

[57] A. Hussain, S. Nazir, F. Khan, L. Nkenyereye, A. Ullah, S. Khan, and S. Verma,"A Resource-Efficient Hybrid Proxy Mobile IPv6 Extension for Next-Generation IoT Networks," in IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2095-2103, 2023, doi: 10.1109/JIOT.2021.3058982.

[58] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. https://doi.org/10.1155/2017/9324035.

[59] E. Ahmed, A. Gani, I. Hashem,"Internet of things architecture: recent advances, taxonomy, requirements, and open challenges," IEEE Wireless Communications Magazine, Vol. 24, pp. 10–16, 2017.

[60] W. A. Kassab, and K.A. Darabkh, "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions

and recommendations", Journal of Network and Computer Applications, Vol. 163, pp. 102663, 2020.

[61] H. T. Dang, N. Krommenacker, P. Charpentier, D. S. Kim, "The Internet of Things for Logistics: Perspectives, Application Review, and Challenges", IETE Technical Review,Vol. 39, no. 1, pp. 93-121, 2020, DOI: 10.1080/02564602.2020.1827308.

[62] J. Wang, M.K. Lim, C. Wang, and M.L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," Computers and Industrial Engineering, 155, p.107174, 2021.

[63] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," IEEE Software, Vol. 33,no. 1, pp. 112–116, 2016.

[64] A. Whitmore, A. Agarwal, and L.D. Xu, "The internet of things—a survey of topics and trends," Information Systems Frontiers, Vol. 17, pp. 261–274, Apr. 2015.

[65] J. L. Shah and H. F. Bhat, "Towards a Secure IPv6 Autoconfiguration", Information Security Journal: A Global Perspective, vo. 29, no. 1,pp. 14-29,, 2020. DOI: 10.1080/19393555.2020.1716117

[66] A. Anjaiah, A. Govardhan, M. Vazralu, "Internet of Things: Present State of the Art, Applications, Protocols and Enabling Technologies," In: Soft Computing and Signal Processing, Springer, Singapore, 2019, pp. 389-398.

[67] R. Hinden, S. Deering,"IP Version 6 Addressing Architecture," Network Working Group, RFC 4291, Feb. 2006 .

[68] F. Gont, "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Auto configuration (SLAAC)," IETF, RFC 7217, Apr. 2014.

[69] F. Gont, A. Cooper, D. Thaler,W. Liu, "Recommendation on Stable IPv6 Interface Identifiers," IETF, RFC 8064, Feb. 2017.

[70] G. Mao, B. Fidan, B.D.O. Anderson, "Wireless sensor network localization techniques," Computer networks, Vol. 51,no. 10, pp. 2529-2553, Jul. 2007.

[71] N. Patwari, J.N. Ash, S. Kyperountas, A.O. Hero, R.L. Moses, N.S. Correal, “Locating the nodes: cooperative localization in wireless sensor networks,” IEEE Signal Process. Mag. , Vol. 22, no. 4, pp. 54–69, Jun. 2005.

[72] E. Guerrero, J. Alvarez, and L. Rivero,“3D-ADAL: A three dimensional distributed range-free localization algorithm for wireless sensor networks based on unmanned aerial vehicles,” 5th International Conference on Digital Information Management, Thunder Bay, IEEE, Jul. 2010, pp. 332-338.

[73] T. Narten, E. Nordmark, W. Simpson, H. Siliman, “Neighbor Discovery for IP version 6 (IPv6),” Internet Engineering Task Force, RFC 2461, Sep. 2007.

[74] G. Song, Z. Ji, “Novel Duplicate Address Detection with Hash Function”, PLoS ONE, Vol. 11, no. 3, pp. e0151612, March 2016.

[75] M. Mavani, K. Asawa, ”Privacy Preserving IPv6 Address Auto-Configuration for Internet of Things”, In: Hu YC., Tiwari S., Mishra K., Trivedi M. (eds) Intelligent Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 19. Springer, Singapore, 2018.

[76] IEEE Computer Society. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE Standard 802.15.4, Aug. 2006.

[77] B. Carpenter, S. Jiang, “Significance of IPv6 Interface Identifiers”, Internet Engineering Task Force, RFC 7136, 2014.

[78] A. Ravanshid et al., “Multi-connectivity functional architectures in 5G,” in Proc. IEEE Int. Conf. Commun.Workshops (ICC), May 2016, pp. 187-192.

[79] M. Peng, Y. Li, Z. Zhao, and C. Wang, “System architecture and key technologies for 5G heterogeneous cloud radio access networks,” IEEE Netw., vol. 29, no. 2, pp. 6-14, 2015.

[80] J. Moysen and L. Giupponi, “From 4G to 5G: Self-organized network management meets machine learning,” Computer Communications, vol. 129, pp. 248–268, 2018.

[81] J. Iyengar, P. Amer, R. Stewart, Concurrent multipath transfer using SCTP multihoming over independent end-to-end paths, IEEE/ACM Trans. Netw., Vol. 14, pp. 951–964, 2006.

[82] R. Stewart, Ed., Stream Control Transmission Protocol, Standard RFC 4960, Sep. 2007. [Online]. Available: https://rfc-editor.org/rfc/rfc4960.txt

[83] J. Iyengar, C. Raiciu, S. Barre, M. J. Handley, and A. Ford, Architectural Guidelines for Multipath TCP Development, Standard RFC 6182, Mar. 2011. [Online]. Available: https://rfc-editor.org/rfc/rfc6182.txt

[84] A. Ford, C. Raiciu, M. Handley, O. Bonaventure, TCP extensions for multi- path operation with multiple addresses, RFC 6824, IETF, 2013, doi: 10.17487/ RFC6824 . ISSN 2070-1721.

[85] T. Dreibholz, E.P. Rathgeb, I. Rungeler, R. Seggelmann, M. Tuxen, R. Stewartm, ”Stream control transmission protocol: past, current and future standardization activities”, IEEE Commun. Mag., Vol. 49, pp. 82–88, 2011.

[86] C. Xu, T. Liu, J. Guan, H. Zhang, G-M. Muntean, ”CMT-QA: Quality-Aware adaptive concurrent multipath data transfer in heterogeneous wireless networks”, IEEE Trans. Mobile Comput., Vol. 12, No. 11, pp. 2193–2205, 2013. https://doi.org/10.1109/TMC.2012.189.

[87] B. H.Oh, J. Lee, ”Constraint-based proactive scheduling for MP-TCP in wireless networks”, Comput. Netw., Vol. 91, pp. 548-563, 2015. https://doi.org/10.1016/j.comnet.2015.09.002.

[88] A. Alheid, D. Kaleshi, and A. Doufexi, ”Performance evaluation of MPTCP in indoor heterogeneous networks,” in Proc. 1st Int. Conf. Syst. Inform., Modeling Simulation (SIMS), 2014, pp. 213-218. [Online]. Available: http://dx.doi.org/10.1109/SIMS.2014.40

[89] A. Abdrabou and M. Prakash, “Experimental performance study of multi-path TCP over heterogeneous wireless networks,” in Proc. IEEE 41st Conf.Local Comput. Netw. (LCN), Nov. 2016, pp. 172-175.

[90] C. Xu, Z. Li, L. Zhong, H. Zhang, G-M. Muntean, CMT-NC: Improving the Concurrent Multipath Transfer Performance using network coding

in wireless networks, IEEE Trans. Veh. Technol., Vol. 65, no. 3,pp. 1735-1751, 2016. https://doi.org/10.1109/TVT.2015.2409556.

[91] N. Arianpoo, I. Aydin, C.M. Leung Victor, Network Coding as a performance booster for concurrent multi-path transfer of data in multi-hop wireless networks, IEEE Trans. Mobile Comput., Vol 16, no. 4, pp. 1047-1058, 2016. https://doi.org/10.1109/TMC.2016.2585106.

[92] K. Xue, J. Han, H. Zhang, K. Chen, P. Hong, "Migrating unfairness among subflows in MPTCP with network coding for wired-wireless networks", IEEE Trans. Veh. Technol., Vol. 66, no. 1, pp. 798-809, 2016. https://doi.org/10.1109/TVT.2016.2543842.

[93] K. C. Leung, C. Lai, V.O.K. Li, D. Yang, "A packet-reordering solution to wireless losses in transmission control protocol", Vol. 19, no. 7, pp. 1577-1593 2013,. https://doi.org/10.1007/s11276-013-0552-6.

[94] S. Shailendra, R. Bhattacharjee, S.K. Bose, "MPSCTP: A simple and efficient multipath algorithm for SCTP," IEEE Commun. Lett.,Vol. 15, no. 10, pp. 1139-1141, 2011. https://doi.org/10.1109/LCOMM.2011.080811.110866.

[95] S. Shailendra, R. Bhattacharjee, S.K. Bose, "An implementation of Min–Max optimization for multipath SCTP through bandwidth estimation based resource pooling technique," AEU Int J Electron Commun., Vol. 67, no. 3, pp. 246-249, 2013. https://doi.org/10.1016/j.aeue.2012.08.008.

[96] C. Xu, Z. Li, J. Li, H. Zhang, G-M. Muntean, "Cross-layer fairness-driven concurrent multipath video delivery over heterogeneous wireless networks," IEEE T Circ. Syst. Vid., Vol. 25, no. 7, pp. 1175-1189, 2015. https://doi.org/10.1109/TCSVT.2014.2376138.

[97] A. Ford, C. Raiciu, M. Handly, O. Bonaventure, "TCP extensions for multipath operation with multiple addresses," Technical Report, IETF RFC 6824, 2013.

[98] C. Raiciu, C. Paasch, S. Barre, A. Ford, M. Honda, F. Duchene, O. Bonaventure, M.Handley, "How hard can it be? Designing and implementing a deployable multipath TCP," in: Proceedings of 9th USENIX Networked Systems Design and Implementation, 2012 pp. 29-29. https://dl.acm.org/citation.cfm?id=2228338.

[99] R. Khalili, N. Gast, M. Popovic, J-Y. Le Boudec, "MPTCP is not Pareto-optimal: performance issues and a possible solution," IEEE/ACM Trans. Netw., Vol. 21, no. 5, pp. 1651-1665, 2013. https://doi.org/10.1109/TNET.2013.2274462.

[100] Y. Cui, L. Wang, X. Wang, H. Wang, Y. Wang, FMTCP: A fountain code-based multipath transmission control protocol, IEEE ACM T Network., Vol. 23, no. 2, pp. 465-478, 2015. https://doi.org/10.1109/TNET.2014.2300140.

[101] Q. Peng, A. Walid, J. Hwang, S. H. Low, "Multipath TCP: Analysis, design, and implementation", IEEE/ACM Trans. Netw.,Vol. 24, nn. 1, pp. 596-609, 2016. https://doi.org/10.1109/TNET.2014.2379698.

[102] C. Xu, P. Wang, X. Wei, G-M. Muntean, "Pipeline network coding-based multipath data transfer in heterogeneous wireless networks," IEEE Trans. Broadcast., Vol. 63, nn. 2, pp. 376-390, 2016. https://doi.org/10.1109/TBC.2016.2590819.

[103] M. Honda, Y. Nishida, C. Raiciu, A. Greenhalgh, M. Handley, H. Tokuda, "Is it still possible to extend TCP?", In:Proceedings of the 2011 ACMSIGCOMM Con-ference on Internet Measurement Conference. ACM, NewYork, United States, pp. 181–194, 2011.

[104] T. Dreibholz, M. Becke, J. Pulinthanath, E.P. Rathgeb, "On the use of concurrent multipath transfer over asymmetric paths", 3rd IEEE Global Telecommunications Conference (GLOBECOM 2010), 2010, pp. 1 –6.

[105] B.Hesmans, F. Duchene, C. Paasch, G. Detal, O. Bonaventure,"Are TCP ex-tensions middle box-proof?" In:Proceedings of the 2013 Workshop on Hotto- pics in Middleboxes and Network Function Virtualization. ACM, NewYork, United States, 2013, pp.37–42.

[106] B. Arzani, A. Gurney, S. Cheng, R. Guerin,B.T. Loo, "Impact of path char-acteristics and scheduling policies on MPTCP performance," In: 2014 28th In-ternational Conference on Advanced Information Networking and Applications Workshops(WAINA). IEEE, NewYork, United States,pp.743–748, 2014.

[107] D. Zhou, W. Song, P. Wang, W. Zhuang, "Multipath TCP for user cooperation in LTE networks," IEEE Netw., Vol. 29, no. 1, pp. 18–24,2015.

[108] F. Yang, P. Amer, "Using One-way communication delay for in-order arrival MPTCP scheduling," In: Proceedings of the 9th International Conference on Communications and Networkingin China (CHINA-COM),2014, pp.122–125.

[109] T. A. Le, X. L. Bui, "Forward delay-based packet scheduling algorithm for multipath TCP," Mobile Networks and Applications, Vol. 23, no. 1, pp 4-12, 2017.

[110] D. Ni, K. Xue, P. Hong, H. Zhang, H. Lu, "OCPS: Offset compensation based packet scheduling mechanism for multi path TCP", In:2015 IEEE International Conference on Communications(ICC). IEEE, New York, United States, pp.6187–6192, 2015.

[111] M. Li, A. Lukyanenko, Y. Cui, "Network coding based multipath TCP", In:2012 IEEE Conferenceon Computer Communications Workshops (INFOCOM WKSHPS). IEEE, New York, United States,2012, pp.25–30.

[112] M. Scharf and S. Kiesel, "Head-of-line Blocking in TCP and SCTP: Analysis and Measurements," in Proceedings of the IEEE Global Communications Conference (GLOBECOM), 2006.

[113] E. Dong, M. Xu, X. Fu, Y. Cao, "A loss aware MPTCP scheduler for highly lossy networks," Computer Networks, Vol. 157, pp.146-158, 2019.

[114] Z. Xu, J. Tang, C. Yin, Y. Wang, and G. Xue, "Experience-Driven Congestion Control: When Multi-Path TCP Meets Deep Reinforcement Learning," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1325–1336, 2019.

[115] M. Zhu, L. Wang, Z. Qin, N. Ding, J. Fang, T. Liu, and Q. Cui, "BE-LIA: bandwidth estimate-based link increase algorithm for MPTCP," IET Networks, vol. 6, no. 5, pp. 94–101, 2017.

[116] C.M. Huang, Y.C. Chen, and S.Y. Lin, "Packet scheduling and congestion control schemes for Multipath Datagram Congestion Control Protocol," The Computer Journal, vol. 58, no. 2, pp. 188–203, 2015.

[117] B. Y. L. Kimura, D. C. S. F. Lima, and A. A. F. Loureiro, "Alternative scheduling decisions for Multipath TCP," IEEE Communications Letters, vol. 21, no. 11, pp. 2412–2415, 2017.

[118] K. W. Choi, Y. S. Cho, J. W. Lee, S. M. Cho, J. Choi et al., “Optimal load balancing scheduler for MPTCP-based bandwidth aggregation in heterogeneous wireless environments,” Computer Communications, vol. 112, pp. 116–130, 2017.

[119] A. G. Saavedra, M. Karzand, and D. J. Leith, “Low Delay Random Linear Coding and Scheduling Over Multiple Interfaces,” IEEE Transactions on Mobile Computing, vol. 16, no. 11, pp. 3100–3114, 2017.

[120] S. Ferlin, S. Kucera, H. Claussen, and O. Alay, “MPTCP meets FEC: Supporting latency-sensitive applications over Heterogeneous Networks,” IEEE/ACM Transactions on Networking, Vol. 26, no. 5, pp. 1–14, 2018.

[121] E. Dong, M. Xu, X. Fu, and Y. Cao, “LAMPS: A Loss Aware Scheduler for Multipath TCP over Highly Lossy Networks,” in 42nd IEEE Conference on Local Computer Networks (LCN), Singapore, Oct.2017, pp. 1–9.

[122] J. Hwang, A. Walid, and J. Yoo, “Fast coupled retransmission for multipath TCP in data center networks,” IEEE Systems Journal, vol. 12, no. 1, pp. 1056–1059, Mar. 2018.

[123] R. Mittal, V. T. Lam, N. Dukkipati, E. Blem, H. Wassel, M. Ghobadi,A. Vahdat, Y. Wang, D. Wetherall, and D. Zats, “TIMELY: RTT-based congestion control for the datacenter,” ACM Computer Communication Review, vol. 45, no. 4, pp. 537–550, Aug. 2015.

[124] N. Kuhn, E. Lochin, A. Mifdaoui, G. Sarwar, O. Mehani, and R. Boreli, “DAPS: Intelligent delay-aware packet scheduling for multipath transport,” in 2014 IEEE International Conference on Communications (ICC), June 2014, pp. 1222–1227.

[125] G. Sarwar, R. Boreli, E. Lochin, A. Mifdaoui, and G. Smith, “Mitigating Receiver’s Buffer Blocking by Delay Aware Packet Scheduling in Multipath Data Transfer,” in IEEE WAINA, 2013.

[126] J. Eklund, K.J. Grinnemo, A. Brunstrom, ”Using Multiple Paths in SCTP to Reduce Latency for Signaling Traffic,” Computer Communications, Vol. 129, pp.184-196, 2018. doi: 10.1016/j.comcom.2018.07.016

[127] T. D. Wallace, A. Shami, On-demand Scheduling for Concurrent Multipath Transfer under Delay-Based Disparity, in: 8th International Wireless Communications and Mobile Computing Conference (IWCMC), 2012, pp. 833–837.

[128] V.K. Sharma, L.P. Verma and M. Kumar, "CL-ADSP: Cross-Layer Adaptive Data Scheduling Policy in Mobile Ad-hoc Networks," Future Generation Computer Systems,Vol. 97, pp. 530-563, 2019. https://doi.org/10.1016/j.future.2019.03.013.

[129] L.P. Verma, M. Kumar, "An adaptive data chunk scheduling for concurrent multipath transfer," Comp. Stand. Inter.,Vol. 52, pp. 97-104, 2017. https://doi.org/10.1016/j.csi.2017.02.001.

[130] J. Wu, B. Cheng, M. Wang, J. Chen, "Energy-Efficient Bandwidth Aggregation for Delay-Constrained Video Over Heterogeneous Wireless Networks", IEEE Journal on Selected Areas in Communications , vol. 35, no. 1, pp. 30-49, 2017.

[131] J. Wu, C. Yuen, B. Cheng, M. Wang, J. Chen, "Energy-Minimized Multipath Video Transport to Mobile Devices in Heterogeneous Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 34, no. 5, pp. 1160-1178, 2016.

[132] Z. Deng, Y. Liu, J. Liu, X. Zhou, S. Ci, "QoE-Oriented Rate Allocation for Multipath High-Definition Video Streaming Over Heterogeneous Wireless Access Networks", Systems Journal IEEE, vol. 11, no. 4, pp. 2524-2535, 2017.

[133] J. Wu, C. Yuen, B. Cheng, Y. Yang, M. Wang, J. Chen, "Bandwidth-Efficient Multipath Transport Protocol for Quality-Guaranteed Real-Time Video Over Heterogeneous Wireless Networks",IEEE Transactions on Communications , vol. 64, no. 6, pp. 2477-2493, 2016.

[134] J. Wu, B. Cheng, C. Yuen, Y. Shang, J. Chen, "Distortion-Aware Concurrent Multipath Transfer for Mobile Video Streaming in Heterogeneous Wireless Networks", IEEE Transactions on Mobile Computing , vol. 14, no. 4, pp. 688-701, 2015.

[135] W. Wu, Q. Yang, P. Gong, K. S. Kwak, "Energy-Efficient Traffic Splitting for Time-Varying Multi-RAT Wireless Networks", IEEE Transactions on Vehicular Technology , vol. 66, no. 7, pp. 6523-6535, 2017

[136] Y. Cao, C. Xu, J. Guan, H. Zhang, "CMT-CQA: Cross-layer QoS-aware adaptive concurrent multipath data transfer in heterogeneous networks", IEEE Transactions on Electrical and Electronic Engineering, vol. 10, pp. 75, 2015.

[137] Y. Cao, Q. Liu, Y. Zuo, G. Luo, H. Wang, M. Huang, "Receiver-assisted cellular/wifi handover management for efficient multipath multimedia delivery in heterogeneous wireless networks", EURASIP Journal on Wireless Communications and Networking, vol. 2016, pp. 1-13, 2016.

[138] Q. Liu, F. Ke, Z. Liu, and J. Zeng, "Loss-Aware CMT-Based Multipathing Scheme for Efficient Data Delivery to Heterogeneous Wireless Networks", International Journal of Digital Multimedia Broadcasting Vol. 2019, 2019. https://doi.org/10.1155/2019/9474057.

[139] J. Wu et al., "Loss tolerant bandwidth aggregation for multihomed video streaming over heterogeneous wireless networks," Wireless personal communications, vol. 75, no. 2, pp. 1265–1282, 2014.

[140] C. Lee, S. Song, H. Cho, G. Lim, and J. M. Chung," Optimal Multipath TCP Offloading over 5G NR and LTE Networks", IEEE wireless communications letters, vol. 8, no. 1, pp. 293-296, 2019.

[141] S. I. Sou and Y. T. Peng, "Performance modeling for multipath mobile data offloading in cellular/Wi-Fi networks," IEEE Trans. Commun., vol.65, no. 9, pp. 3863-3875, Sep. 2017.

[142] O. Delgado and F. Labeau, "Delay-aware load balancing over multipath wireless networks," IEEE Trans. Veh. Technol., vol. 66, no. 8, Aug. 2017.

[143] S. R. Pokhrel, M. Panda, and H. L. Vu, "Analytical modeling of multipath TCP over last-mile wireless," IEEE/ACM Trans. Netw., vol. 25, no. 3, pp. 1876-1891, Jun. 2017.

[144] X. Corbillon, R. Aparicio-Pardo, N. Kuhn, G. Texier, and G. Simon,"Cross-layer scheduler for video streaming over MPTCP," Proceedings of the 7th International Conference on Multimedia Systems, p. 7, 2016.

[145] S. F. Oliveira, T. Dreibholz, and O. Alay, "Tackling the challenge of buffer bloat in multi-path transport over heterogeneous wireless net-

works," in Quality of Service (IWQoS), 22nd International Symposium of. IEEE, 2014, pp. 123–128.

[146] W. Lu, D. Yu, M. Huang, and B. Guo, "PO-MPTCP: Priorities-Oriented Data Scheduler for Multimedia Multipathing Services", International Journal of Digital Multimedia Broadcasting, Vol. 2018, pp. 1-9, 2018. https://doi.org/10.1155/2018/1413026.

[147] Y. C. Chen, Y. S. Lim, R. J. Gibbens, E. M. Nahum, R. Khalili, and D. Towsley, "A measurement-based study of multipath tcp performance over wireless networks," Proceedings of the 2013 conference on Internet measurement conference, pp. 455–468, 2013.

[148] L. Angrisani, M. Bertocco, G. Gamba, and A. Sona, "Effects of RSSI impairments on IEEE 802.15.4 wireless devices performance susceptibility to interference", 2008 International Symposium on Electromagnetic Compatibility EMC Europe, 2018.

[149] M. Scharf and A. Ford, "Multipath TCP (MPTCP) application interface considerations," IETF, RFC 6897, Mar. 2013. [Online]. Available: https://rfc-editor.org/rfc/rfc6897.txt

[150] M. Bagnulo, "Threat analysis for TCP extensions for multipath operation with multiple addresses," IETF, RFC 6181, Mar. 2011. [Online]. Available: https://rfc-editor.org/rfc/rfc6181.txt

[151] S. Barré, C. Paasch, and O. Bonaventure, "Multipath TCP: From theory to practice," in IEEE/IFIP Networking Conference (IFIP Networking), Valencia, Spain, May 2011, pp. 444–457.

[152] C. Raiciu, M. Handly, and D. Wischik, "Coupled congestion control for multipath transport protocols," RFC 6356 (Experimental), 2011.

[153] R. Khalili, N. Gast, and J.L. Boudec, "Opportunistic Linked-Increases Congestion Control Algorithm for MPTCP," Internet Draft, 2013.

[154] S. Ferlin, T. Dreibholz, O. Alay, Multi-path transport over heterogeneous wireless networks: does it really pay off? in: Proceedings of IEEE GLOBECOM, 2014.

[155] X. Nie, Y. Zhao, Z. Li, G. Chen, K. Sui, J. Zhang, Z. Ye, and D. Pei, "Dynamic TCP Initial Windows and Congestion Control Schemes Through

Reinforcement Learning," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1231–1247, June 2019.

[156] W. Li, F. Zhou, K. R. Chowdhury, and W. M. Meleis, "QTCP: Adaptive Congestion Control with Reinforcement Learning," IEEE Transactions on Network Science and Engineering, Vol. 6, no. 3, pp.445-458, May 2018.

[157] J. Gettys and K. Nichols, "Bufferbloat: Dark buffers in the Internet," ACM Queue, vol. 9, no. 11, pp. 40:40–40:54, Nov. 2011.

[158] M. Polese, F. Chiariotti, E. Bonetto, F. Rigotto, A. Zanella, and M. Zorzi, "A Survey on Recent Advances in Transport Layer Protocols", IEEE Communications Surveys and Tutorials, Vol. 21, no. 4, pp.3584-3608, 2019. DOI 10.1109/COMST.2019.2932905

[159] C. Li, H. Xiong, J. Zou and C. W. Chen, "Distributed Robust Optimization for Scalable Video Multirate Multicast Over Wireless Networks," IEEE Transactions on Circuits and Systems for Video Technology, vol.22, no.6, pp.943-957, Feb. 2012.

[160] M. Li, A. Lukyanenko, Z. Ou, A. Y. Jaaski, S. Tarkoma, M. Coudron, and S. Secci, "Multipath transmission for the internet: A survey," IEEE Communications Surveys Tutorials, vol. 18, no. 4, pp.2887-2925, 2016.

[161] A. G. Saavedra, M. Karzand, and D. J. Leith, "Low Delay Random Linear Coding and Scheduling Over Multiple Interfaces," IEEE Transactions on Mobile Computing, vol. 16, no. 11, pp. 3100–3114, Nov. 2017.

[162] P. Ageneau, N. Boukhatem, and M. Gerla, "Practical random linear coding for MultiPath TCP: MPC-TCP," in 24th IEEE International Conference on Telecommunications (ICT), Limassol, Cyprus, May 2017, pp. 1–6.

[163] Y. Cui, L. Wang, X. Wang, H. Wang, and Y. Wang, "FMTCP: A fountain code-based Multipath Transmission Control Protocol," IEEE/ACM Transactions on Networking, vol. 23, no. 2, pp. 465–478, Apr. 2015.

[164] S. Ferlin, S. Kucera, H. Claussen, and O. Alay, "MPTCP meets FEC: Supporting latency-sensitive applications over Heterogeneous Networks," IEEE/ACM Transactions on Networking, Vol. 26, no. 5, pp.2005-2018, Oct. 2018.

[165] D. Ni, K. Xue, P. Hong, and S. Shen, “Fine-grained forward prediction based dynamic packet scheduling mechanism for multipath TCP in lossy networks,” in 23rd IEEE International Conference on Computer Communication and Networks (ICCCN), Shanghai, China, 2014, pp.1–7.

[166] K. K. Yap, T. Y. Huang, M. Kobayashi, Y. Yiakoumis, N. McKeown, S. Katti, and G. Parulkar, “Making use of all the networks around us: a case study in android,” Proceedings of the 2012 ACM SIGCOMM workshop on Cellular networks: operations, challenges, and future design, pp. 19–24, 2012.

[167] J. Postel, “User datagram protocol (UDP)”, RFC 768, Internet Engineering Task Force, 1980. https://tools.ietf.org/html/rfc768 Accessed 15 January, 2017.

[168] C. Raiciu, J. Iyengar, O. Bonaventure, et al., “Recent advances in reliable transport protocols”, In: SIGCOMM ebook on Recent Advances in Networking, 2013.

[169] T. Ye, D. Veitch, J. Bolot, “Improving wireless security through network diversity”, ACMSIGCOMM Computer Communication Review, Vol. 39, no. 1, pp. 34–44, 2008.

[170] C. Raiciu, S. Barre , C. Pluntke, A. Greenhalgh, D. Wischik, M. Handley,“ Improving datacenter performance and robustness with multipath TCP”, ACM SIGCOMM Computer Communication Review, Vol. 41, no. 4,pp. 266–277, 2011.

[171] C. Raiciu, M. Handly, D. Wischik,“Coupled congestion control for multipath transport protocols”, RFC 6356, Internet Engineering Task Force, 2011. https://tools.ietf.org/html/rfc6356 Accessed 2 December 2016.

[172] B T Innovate, M.H., “The trilogy architecture for the future Internet”, In: To- wards the Future Internet: A European Research Perspective, 79, 2009.

[173] D. Wischik, M. Handley, M.B. Braun, “The resource pooling principle”, ACM SIGCOMM Computer Communication Review, Vol. 38, no. 5, pp. 47–52, 2008.

[174] S. Savage, A. Collins, E. Hoffman, J. Snell, T. Anderson,“The End-to-End Effects of Internet Path Selection”, ACM SIGCOMM Computer Communication Review, Vol. 29, no. 4, pp. 289–299, 1999.

[175] J. G. Apostolopoulos, “Reliable video communication over lossy packet networks using multiple state encoding and path diversity”, In: Photonics West 2001-Electronic Imaging. International Society for Optics and Photonics, Bellingham Washington, United States, pp.392–409, 2000.

[176] Y.J. Liang, E.G. Steinbach, B. Girod, “Real-time voice communication over the internet using packet path diversity”, In: Proceedings of the 9th ACM International Conference on Multimedia ACM, New York, United States, pp.431–440, 2001.

[177] C. Paasch, G. Detal, F. Duchene, C. Raiciu, O. Bonaventure, “Exploring mobile/ Wifi handover with multipath TCP”, In: Proceedings of the 2012 ACMSIGCOMM Workshop on Cellular Networks: Operations, Challenges, and Future Design. ACM, New York, United States, pp.31–36, 2012.

[178] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, V. Paxson, “Stream control transmission protocol”, RFC 2960, Internet Engineering Task Force, 2000. https://tools.ietf.org/html/rfc2960 Accessed Dec 2019.

[179] A. Argyriou, V. Madisetti, “Bandwidth aggregation with SCTP”, In: IEEE Global Telecommunications Conference (GLOBECOM’03), vol.7, IEEE, New York, United States, pp.3716–3721, 2003.

[180] C. Casetti, W. Gaiotto, “Westwood SCTP: load balancing over multipaths using bandwidth-aware source scheduling”, In: 2004 IEEE 60th Vehicular Technology Conference, 2004.VTC2004-Fall, vol. 4. IEEE, New York, United States, pp. 3025–3029, 2004.

[181] A. Abd, T. Saadawi, M. Lee, “LS-SCTP: a bandwidth aggregation technique for stream control transmission protocol”, Computer Communication, Vol. 27, no. 10, pp. 1012–1024, 2004.

[182] A. Abd, T. Saadawi, M. Lee, “Improving throughput and reliability in mobile wireless networks via transport layer bandwidth aggregation”, Computer Network, Vol. 46, no. 5, pp. 635–649, 2004.

[183] J. Stone, R. Stewart, and D. Otis, “Stream Control Transmission Protocol (SCTP) Checksum Change,” RFC 3309, 2002.

[184] R. Stewart, I. Arias-Rodriguez, K. Poon, A. Caro, and M. Tuexen, “Stream Control Transmission Protocol (SCTP) Specification Errata and Issues,” RFC 4460, 2006.

[185] K. Okamoto, N. Yamai, K. Okayama, K. Kawano, M. Nakamura, and T. Yokohira, “Performance improvement of SCTP communication using selective bicasting on lossy multihoming environment,” IEEE 38th Annual Computer Software and Applications Conference (COMPSAC),pp. 551–557, 2014.

[186] C. A. G. da Silva, E. P. Ribeiro, and C. M. Pedroso, “Preventing quality degradation of video streaming using selective redundancy,” Computer Communications, vol. 91, pp. 120–132, 2016.

[187] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen, and P. Conrad, “Stream Control Transmission Protocol (SCTP) Partial Reliability Extension,” RFC 3758, 2004.

[188] M. Tuexen, R. Seggelmann, R. Stewart, and S. Loreto, “Additional Policies for the Partially Reliable Stream Control Transmission Protocol Extension,” RFC 7496, 2015.

[189] J. Wu, C. Yuen, M.Wang, and J. Chen, “Content-aware concurrent multipath transfer for high-definition video streaming over heterogeneous wireless networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 3, pp. 710–723, 2016.

[190] E. Yilmaz, N. Ekiz, P. Natarajan, P. Amer, J. Leighton, F. Baker, R. Stewart, “Throughput analysis of non-renegable selective acknowledgments (NR-SACKs) for SCTP”, Computer Communication, Vol. 33, no. 16, pp. 1982–1991, 2010.

[191] V.K. Sharma, S.S.P. Shukla, V. Singh, “A Tailored Q-Learning for Routing in Wireless Sensor Networks,” In: IEEE International Conference on Parallel Distributed and Grid Computing (PDGC), pp. 663-668, 2012.

[192] G. Ye, T.N. Saadawi, M.J. Lee, “Improving Stream Control Transmission Protocol Performance Over Lossy Links,” IEEE Journal on Selected Area in Communications, Vol. 22, no. 4, pp. 727–736, 2004.

[193] P. Natarajan, N. Ekiz, P. Amer, R. Stewart, ”Concurrent multipath transfer during path failure”, Computer communication, Vol. 32, pp. 1577–1587, 2009.

[194] S. Shailendra, R. Bhattacharjee, S.K. Bose, “An implementation of Min–Max optimization for multipath SCTP through bandwidth estimation based resource pooling technique”, International Journal of Electronics and Communication, Vol. 67, pp. 246-249, 2013.

[195] S. Shailendra, R. Bhattacharjee, S.K. Bose, “A multipath variant of SCTP with optimized flow division extension”, Computer Communication, Vol. 67, pp. 56-65, 2015.

[196] C. M. Huang and C.H. Tsai, ”WiMP-SCTP: Multipath transmission using stream control transmission protocol (SCTP) in wireless networks”, In Proceedings of the 21st IEEE International Conference on Advanced Information Networking and Applications Workshops (AINAW ’07), Vol. 1, pp. 209–214, 2007.

[197] J. Wu, B. Cheng, M. Wang, and J. Chen, “Energy-aware concurrent multipath transfer for real-time video streaming over heterogeneous wireless networks,” IEEE Trans. Circuits Syst. Video Technol., Vol. 28, no. 8, pp.2007-2023, 2017. doi: 10.1109/TCSVT.2017.2695368.

[198] S. Liu, W. Lei, W. Zhang, Y. Guan, “ CMT-SR: A selective retransmission based concurrent multipath transmission mechanism for conversational video”, Computer Networks, Vol. 112, pp. 360–371, 2017.

[199] N. Arianpoo, V.C.M.Leung, “A smart fairness mechanism for Concurrent multipath transfer in SCTP over wireless multi-hop networks”, Ad Hoc Networks, Vol. 55, pp. 40-49, Feb. 2017.

[200] J. Postel, “User datagram protocol (UDP)”, RFC 768, Internet Engineering Task Force, 1980. https://tools.ietf.org/html/rfc768 [

[201] J. Postel “Transmission Control Protocol”, RFC 793, Internet Engineering Task Force, 1981.https://tools.ietf.org/html/rfc793

[202] S.J. Koh, Q. Xie, S.D. Park, “Mobile SCTP (mSCTP) for IP handover support”, Internet Draft https, 2006. https://tools.ietf.org/html/draft-sjkoh-msctp-01.

[203] M. Riegel, M. Tuexen, “Mobile SCTP”, Internet Draft, 2007. https://tools.ietf.org/html/draft-riegel-tuexen-mobile-sctp-09.

[204] S. Maruyama, M. Tuexen, R. Stewart, Q. Xie, M. Kozuka, “Stream control transmission protocol (SCTP) dynamic address reconfiguration”, RFC 5061, Internet Engineering Task Force, 2007. https://tools.ietf.org/html/rfc5061

[205] J. Liao, J. Wang, X. Zhu, “cmpSCTP: an extension of SCTP to support concurrent multi-path transfer”, In: IEEE International Conference on Communications, ICC’08. IEEE, New York, United States, pp. 5762–5766, 2008.

[206] L. Budzisz, R. Ferrús, F. Casadevall, P. Amer, “On concurrent multipath transfer in SCTP-based handover scenarios”, In: IEEE International Conference on Communications, 2009. ICC’09. IEEE, New York, United States, pp.1–6, 2009.

[207] F.H. Mirani, N. Boukhatem, M.A. Tran, “A data-scheduling mechanism for multi-homed mobile terminals with disparate link latencies”, In: 2010 IEEE 72nd Vehicular Technology Conference Fall (VTC2010-Fall). IEEE, New York, United States, pp.1–5, 2010.

[208] Y. Yuan, Z. Zhang, J. Li, J. Shi, J. Zhou, G. Fang, E. Dutkiewicz, “Extension of SCTP for concurrent multi-path transfer with parallel subflows”, In: 2010 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, New York, United States, pp.1–6, 2010.

[209] Y. Cao, C. Xu, J. Guan, H. Zhang, “TCP-friendly CMT-based multimedia distribution over multi-homed wireless networks”, In: 2014 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, New York, United States, pp. 3028–3033, 2014.

[210] Y. Cao, C. Xu, J. Guan, H. Zhang,“Receiver-driven SCTP-based multimedia streaming services in heterogeneous wireless networks”, In: 2014 IEEE International Conference on Multimedia and Expo (ICME). IEEE, New York, United States, pp.1–6, 2014.

[211] Y. Cao, C. Xu, J. Guan, H. Zhang,“CMT-CC: cross- layer cognitive CMT for efficient multimedia distribution over multi-homed wireless networks”, Wireless Personal Communication, Vol. 82, no. 3, pp. 1643–1663, 2015.

[212] H. Adhari, T. Dreibholz, M. Becke, E. P. Rathgeb,and M. T¨uxen, ”Evaluation of concurrent multipath transfer over dissimilar paths”, In IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA ’11), pp. 708– 714, 2011.

[213] T. Dreibholz, M. Becke, H. Adhari, and E. P. Rathgeb,” On the impact of congestion control for Concurrent Multipath Transfer on the transport layer”, In Proceedings of the 11th IEEE International Conference on Telecommunications (ConTEL ’11), pp. 397–404, 2011.

[214] S. Shailendra, R. Bhattacharjee, and S. K. Bose,”Improving congestion control for Concurrent Multipath Transfer through bandwidth estimation based resource pooling”, In Proceedings of the 8th International Conference on Information, Communications and Signal Processing (ICICS ’11), pp. 1–5. IEEE, 2011.

[215] J.Wu, B. Cheng, M. Wang, “Improving Multipath Video Transmission With Raptor Codes in Heterogeneous Wireless Networks”, IEEE Transactions on Multimedia, Vol. 20, no. 2, pp.457-472, Feb. 2018 .

[216] F. Cheng, J.Zhang, Z. Chen, J. Wu, N. Ling, “Buffer-Driven Rate Control and Packet Distribution for Real-Time Videos in Heterogeneous Wireless Networks”, IEEE Access, Vol. 7, pp.27401-27415, Feb 2019.

[217] W.K. Lai, JJ Jhan, JW Li,” A Cross-Layer SCTP Scheme With Redundant Detection for Real-Time Transmissions in IEEE 802.11 Wireless Networks”, IEEE Access Vol. 7, pp.114086-114101, July 2019.

[218] S. Habib, J. Qadir, A. Ali, D. Habib, M. Li, A. Sathiaseelan, “The past, present, and future of transport-layer multipath,” Journal of Network and Computer Applications, Vol. 75, pp. 236-258, 2016.

[219] C. Paasch, O. Bonaventure, “Multipath TCP,” Communications of the ACM, Vol. 57, no. 4, pp. 51-57, 2014.

[220] D. Wischik, C. Raiciu, A. Greenhalgh, M. Handley, “Design, implementation and evaluation of congestion control for multipath TCP,” In: Proceedings of the 8th USENIX conference on Networked systems design and implementation, pp. 99 -112, 2011.

[221] H. Y. Hsieh, R. Sivakumar, "pTCP: an end-to-end transport layer protocol for striped connections," In: Proceedings of the 10th IEEE Conference on Network Protocols (ICNP), pp. 24-33, 2002.

[222] M. Li, A. Lukyanenko, S. Tarkoma, Y. Cu, A. Y. Jaaski, "Tolerating path heterogeneity in multipath TCP with bounded receive buffers," In proceedings of the ACM SIGMETRICS/international conference on Measurement and modeling of computer systems, pp. 375-376, 2014.

[223] P. Dong, J. Wang, J. Huang, H. Wang, G. Min,"Performance Enhancement of Multipath TCP for Wireless Communications with Multiple Radio Interfaces," IEEE Transactions on Communications, Vol. 64, no. 8, pp. 3456-3466, 2016.

[224] J. M. B. Oliveira, H. M. Salgado, M. R. D. Rodrigues,"A new MSE channel estimator optimized for nonlinearly distorted faded OFDM signals with applications to radio over fiber," IEEE Transactions on Communications, Vol. 62, no. 8, pp. 2977-2985, 2014.

[225] V. K. Sharma, M. Kumar, "Adaptive congestion control scheme in mobile ad-hoc networks", Peer-to-Peer Networking and Applications, Vol. 10, no. 3, pp. 633-657, 2017. doi: 10.1007/s12083-016-0507-7.

[226] Q. Peng, A. Walid, S.H. Low, "Multipath TCP Algorithms: Theory and Design," In: Proceedings of the ACM SIGMETRICS/ International conference on measurement and modeling of computer systems, pp. 305-316, 2013.

[227] S. Ferlin, O. Alay, T. Dreibholz, D.A. Hayes, M. Welzl, "Revisiting Congestion Control for Multipath TCP with Shared Bottleneck Detection," In: IEEE INFOCOM, pp. 2419-2427, 2016.

[228] K. Yedugundla, S. Ferlin, T. Dreibholz, O. Alay, N. Kuhn, P. Hurtig, A. Brunstrom "Is multi-path transport suitable for latency sensitive traffic?", Computer Networks, Vol. 105, pp. 1–21, 2016.

[229] Y. Cao, M. Xu, X. Fu, "Delay-based Congestion Control for Multipath TCP," In: Proceedings of the 20th International Conference on Network Protocols (ICNP), pp. 1-10, 2012.

[230] C. Xu, J. Zhao, G.M. Muntean, "Congestion control design for multipath transport protocols: A survey", IEEE Communications

Surveys and Tutorials, Vol. 18, no. 4, pp.2948-2969, 2016. doi: 10.1109/COMST.2016.2558818.

[231] Y. Thomas, G. Xylomenos, C. Tsilopoulos, G. C. Polyzos, “Multi-Flow Congestion Control with Network Assistance”, In: Proceedings of the IFIP Networking Conference (IFIP Networking) and Workshops, pp. 440-448, 2016.

[232] B. Arzani, A. Gurney, S. Cheng, R. Guerin, B.T. Loo, “Impact of Path Characteristics and Scheduling Policies on MPTCP Performance,” In: Proceedings of the 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 743 -748, 2014.

[233] D. Zhou, W. Song, M. Shi, “Goodput improvement for multipath TCP by congestion window adaptation in multi-radio devices,” In: Consumer Communications and Networking Conference (CCNC), pp. 508-514, 2013.

[234] C. Xu, H. Huang, H. Zhang, C. Xiong, L. Zhu, “Multipath transmission control protocol (MPTCP) Partial Reliability Extension”, Internet Draft, 2015. https://tools.ietf.org/html/draft-xu-mptcp-prmp-00

[235] C. Diop, G. Dugué, C. Chassot, E. Exposito, “QoS- aware multipath TCP extensions for mobile and multimedia applications”, In: Proceeding of the 9th International Conference on Advances in Mobile Computing and Multimedia. ACM, New York, United States, pp.139–146, 2011.

[236] C. Diop, G. Dugue, C. Chassot, E. Exposito, “QoS-oriented MPTCP extensions for multimedia multi-homed systems”, In: 2012 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, New York, United States, pp. 1119–1124, 2012.

[237] J. Wu, C. Yuen, B. Cheng, Y. Shang, J. Chen, “Goodput-aware load distribution for real-time traffic over multi path networks”, IEEE Transactions on Parallel Distributed System, Vol. 26, no. 8, pp. 2286–2299, 2015.

[238] C. Xu, H. Zhang, C. Xiong, L. Zhu, “A message-oriented extension to multipath transmission control protocol (MPTCP)”, Internet Draft, 2016. https://tools.ietf.org/html/draft-xu-mptcp-momp-03

[239] X. Corbillon, R. A. Pardo, N. Kuhn, G. Texier, G. Simon, “Cross-layer scheduler for video streams over PTCP”, In: Proceedings of the 7th International Conference on Multimedia Systems. ACM, New York, United States, pp. 7, 2016.

[240] R.V. Pol, M. Bredel, A. Barczyk, B. Overeinder, N. V. Adrichem, F. Kuipers, “Experiences with MPTCP in an intercontinental Open Flow network”, In: Proceedings of the 29th TERENA Network Conference (TNC2013), 2013.

[241] M. Coudron, S. Secci, G. Pujolle, P. Raad, P. Gallard, “Cross-layer cooperation to boost multipath TCP performance in cloud networks”, In: 2013 IEEE2nd International Conference on Cloud Networking (CloudNet). IEEE, New York, United States, pp.58–66, 2013.

[242] L. Li, N. Hu, K. Liu, B. Fu, . Chen, L. Zhang, “AMTCP: an adaptive multi-path transmission control protocol”, In: Proceedings of the 12th ACM International Conference on Computing Frontiers. ACM, New York, United States, pp. 29, 2015.

[243] S. Hassayoun, J. Iyengar, and D. Ros. Dynamic window coupling for multipath congestion control. In Proceedings of the 19th IEEE International Conference on Network Protocols (ICNP ’11), pp. 341–352. IEEE, 2011.

[244] M. Coudron, S. Secci, G. Maier, G. Pujolle, and A. Pattavina. Boosting cloud communications through a crosslayer multipath protocol architecture. In Proceedings of the IEEE SDN for Future Networks and Services (SDN4FNS), pp. 1–8. IEEE, 2013.

[245] B.H. Oh, and J. Lee, “Feedback-based path failure detection and buffer blocking protection for MPTCP”, IEEE/ACM Transactions on Networking, Vol. 24, no. 6, pp.3450-3461, 2016.

[246] Y. Cao, Q. Liu, Y.Zuo, F.Ke, H. Wang, and M. Huang, “Receiver-centric Buffer Blocking-aware Multipath Data Distribution in MPTCP-based Heterogeneous Wireless Networks”, KSII Transactions on Internet and Information Systems, Vol. 10, no. 10, pp. 4462-4660, 2016.

[247] M.K. Sabetghadam, “Mmptcp: a novel transport protocol for data centre networks (Doctoral dissertation, University of Sussex, 2016..

[248] Y. Cui, L. Wang, X. Wang, Y. Wang, F. Ren,and S. Xia, “End-to-end coding for TCP”, IEEE Network, Vol. 30, no. 2, pp.68-73, 2016.

[249] K.W. Choi, Y.S. Cho, J.W. Lee, S.M. Cho, and J. Choi, “Optimal load balancing scheduler for MPTCP-based bandwidth aggregation in heterogeneous wireless environments”, Computer Communications, Vol. 112, pp.116-130, 2017.

[250] W. Wang, X. Wang, and D. Wang, “Energy efficient congestion control for multipath TCP in heterogeneous networks”, IEEE Access, Vol. 6, pp.2889-2898, 2017.

[251] B.Y. Kimura,D. C. Lima, and A.A. Loureiro, “Alternative scheduling decisions for multipath TCP”, IEEE Communications Letters, Vol. 21, no. 11, pp.2412-2415, 2017.

[252] Y.S. Lim, E.M. Nahum, D.Towsley, and R.J.Gibbens, “ECF: An MPTCP path scheduler to manage heterogeneous paths. In Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies”,November, 2017, pp. 147-159.

[253] Y.K. Lin, C.L. Pan, and L.C.L.Yeng, “Network reliability for multipath TCP networks with a retransmission mechanism under the time constraint”, Journal of Statistical Computation and Simulation, Vol. 88, no. 12, pp.2273-2286, 2018.

[254] T.A. Le, and L.X. Bui, “Forward delay-based packet scheduling algorithm for multipath TCP”, Mobile Networks and Applications, Vol. 23, no. 1, pp.4-12, 2018.

[255] S. Ferlin, S. Kucera, H. Claussen, and Ö. Alay, “MPTCP meets FEC: Supporting latency-sensitive applications over heterogeneous networks”, IEEE/ACM Transactions on Networking, Vol. 26, no. 5, pp.2005-2018, 2018.

[256] J. Wu, R. Tan, and M. Wang, “Energy-efficient multipath TCP for quality-guaranteed video over heterogeneous wireless networks”, IEEE Transactions on Multimedia, Vol. 21, no. 6, pp.1593-1608, 2018.

[257] J. Mena, Y. Gao, and M. Gerla, “MPTCP path selection using CapProbe”, 2018 IEEE Wireless Communications and Networking Conference (WCNC), April 2018, pp. 1-6.

[258] T. Zhu, X. Qin, L. Chen, X. Chen, and G. Wei, “wBBR: A Bottleneck Estimation-Based Congestion Control for Multipath TCP”, 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), August, 2018, pp. 1-5.

[259] J. Zhao, J. Liu, H. Wang, C. Xu, W. Gong, and C. Xu, “Measurement, Analysis, and Enhancement of Multipath TCP Energy Efficiency for Datacenters”, IEEE/ACM Transactions on Networking, Vol. 28, no. 1, pp. 57-70, 2019.

[260] B. Trinh, L. Murphy, and G.M. Muntean, “An Energy-efficient Congestion Control Scheme for MPTCP in Wireless Multimedia Sensor Networks”, 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), September, 2019, pp. 1-7.

[261] A.Könsgen, M. Shahabuddin, A. Singh, and A.Förster, “A Mathematical Model for Efficient and Fair Resource Assignment in Multipath Transport”, Future Internet, Vol. 11, no. 2, pp.39, 2019.

[262] Y. Thomas, M. Karaliopoulos, G. Xylomenos, and G.C. Polyzos, “Low Latency Friendliness for Multipath TCP”, IEEE/ACM TRANSACTIONS ON NETWORKING, Vol. 28, no. 1, pp. 248-261, 2020.

[263] A. Elgabli, K. Liu, and V. Aggarwal, “Optimized preference-aware multipath video streaming with scalable video coding”, IEEE Transactions on Mobile Computing, Vol. 19, no. 1, pp.159-172, 2018.

[264] S. Pang, J. Yao, X. Wang, T. Ding, and L. Zhang, “Transmission Control of MPTCP Incast Based on Buffer Balance Factor Allocation in Data Center Networks”, IEEE Access, Vol. 7, pp.183428-183434, 2019.

[265] W. Li, H. Zhang, S. Gao, C.Xue, X. Wang, and S. Lu, “SmartCC: A Reinforcement Learning Approach for Multipath TCP Congestion Control in Heterogeneous Networks”, IEEE Journal on Selected Areas in Communications, Vol. 37, no. 11, pp.2621-2633, 2019.

[266] P. Hurtig, K.J. Grinnemo, A. Brunstrom, S. Ferlin, O. Alay, N. Kuhn, ”Low-latency scheduling in MPTCP”, IEEE/ACM Transactions on Networking,Vol. 27, no.1, pp.302-315,2018.

[267] K. Xue, J. Han, D. Ni, W. Wei, Y. Cai, Q. Xu, P. Hong, "DPSAF: forward prediction based dynamic packet scheduling and adjusting with feedback for multipath TCP in lossy heterogeneous networks", IEEE Transactions on Vehicular Technology, Vol. 67, no. 2, pp.1521-1534, 2017.

[268] Q. Shi, F. Wang, D. Feng, W. Xie, "Adaptive load balancing based on accurate congestion feedback for asymmetric topologies", Computer Networks, Vol. 157, pp.133-145, 2019.

[269] M. Morawski, P. Ignaciuk, "Energy-efficient scheduler for MPTCP data transfer with independent and coupled channels", Computer Communications,Vol. 132, pp.56-64, 2018.

[270] M. Prakash, A. Abdrabou, W. Zhuang, "An Experimental Study on Multipath TCP Congestion Control With Heterogeneous Radio Access Technologies", IEEE Access, Vol. 7, pp.25563-25574, 2019.

[271] O. Bonaventure, The first Multipath TCP enabled smartphones, December 10, 2018. http://blog.multipath-tcp.org/blog/html/2018/12/10/the_first_multipath_tcp_enabled_smartphones.html

[272] M. Latah and L. Toker, "Artificial Intelligence Enabled Software Defined Networking: A Comprehensive Overview," arXiv preprint arXiv:1803.06818, 2018.

[273] A. A. Jawad, P. Shah, O. Gemikonakli, and R. Trestian, "LearnQoS: a learning approach for optimizing QoS over multimedia-based SDNs," in IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2018, pp. 1–6.

[274] I. R. Alzahrani, N. Ramzan, S. Katsigiannis, and A. Amira, "Use of Machine Learning for Rate Adaptation in MPEG-DASH for Quality of Experience Improvement," in 5th International Symposium on Data Mining Applications. Springer, 2018, pp. 3–11.

[275] S. Ibnalfakih, E. Sabir, and M. Sadik, "Multi-homing as an Enabler for 5G Networks: Survey and Open Challenges," in International Symposium on Ubiquitous Networking. Springer, 2016, pp. 347–356.

[276] D. Purkayastha, M. Perras, and A. Rahman, "Considerations for MPTCP operation in 5G," Working Draft, IETF Secretariat, Internet-Draft draft-purkayastha-mptcp-considerations-for-nextgen-00,

October 2017. [Online]. Available: http://www.ietf.org/internet-drafts/draftpurkayastha-mptcp-considerations-for-nextgen-00.txt

[277] K. Lei, S. Zhong, F. Zhu, K. Xu, and H. Zhang, “An NDN IoT Content Distribution Model With Network Coding Enhanced Forwarding Strategy for 5G,” IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2725–2735, 2018.

[278] K. Habak, K. A. Harras, and M. Youssef. OPERETTA: An optimal energy efficient bandwidth aggregation system. In Proceedings of the 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON ’12), pages 121–129. IEEE, 2012.

[279] T. D. Wallace, A. Shami, “Concurrent Multipath Transfer using SCTP: Modelling and Congestion Window Management,” IEEE Trans. Mobile Comput., vol. 13, no. 11, pp. 2510-2521, 2014.

[280] L.A. Belady, ”A Study of Replacement Algorithms for Virtual Storage Computers,” IBM Systems J., Vol.5, No.2, pp. 78-101, 1966.

[281] R. L. Mattson, J. Gecsei, D. R. Slutz, and I. L. Traiger, ”Evaluation techniques for storage hierarchies,” IBM System J., vol. 9, no.2 pp. 78-117, 1970.

[282] A.V. Aho, P.J. Denning, and J.D. Ullman, “Principles of Optimal Page Replacement,” J. ACM, vol. 18, no. 1, pp. 80-93, 1971.

[283] N. Meigiddo, and D. S. Modha, “ARC: A Self-Tuning, Low overhead Replacement Cache”, IEEE Transactions on Computers, pp. 58-65, 2004.

[284] S. Bansal, and D. Modha, “CAR: Clock with Adaptive Replacement”, FAST-’04 Proceedings of the 3rd USENIX Conference on File and Storage Technologies, pp. 187-200, 2004.

[285] A. S. Chavan, K. R. Nayak, K. D. Vora, M. D. Purohit and P. M. Chawan, ”A Comparison of Page Replacement Algorithms”, IACSIT International Journal of Engineering and Technology, Vol.3, No.2, April 2011.

[286] G. Gagne, A. Silberschatz, P. B. Galvin, ”Operating Systems Concepts”, Seventh edition, 2005.

[287] S. Jiang, and X. Zhang, “LIRS: An Efficient Policy to improve Buffer Cache Performance”, IEEE Transactions on Computers, Vol. 54, no. 8, pp. 939-952, 2005.

[288] S. Jiang, X. Zhang, and F. Chen, “CLOCK-Pro: An Effective Improvement of the CLOCK Replacement”, ATEC ’05 Proceedings of the annual conference on USENIX Annual Technical Conference, pp. 35, 2005.

[289] J. E. O’neil, P. E. O’neil and G. Weikum, “An optimality Proof of the LRU-K Page Replacement Algorithm”, Journal of the ACM, Vol 46, no. 1, pp. 92-112, 1999.

[290] P. J. Denning, and K. C. Kahn, ”A Study of Program Locality and Lifetime Functions”, Oper. Sys. Rev., Vol. 9, pp. 207-216, 1975.

[291] P. J. Denning, ”The Working Set Model of Program Behavior,” Comtn. Assoc. Comput. Mach., Vol. 11, pp. 323-333, 1968.

[292] H. Wang, Y. Cheng, and L. Yuan, ”Gas outburst disasters and the mining technology of key protective seam in coal seam group in the Huainan coalfield”, Natural Hazards, Vol. 67, no. 2, pp. 763-782, 2013.

[293] MSHA, Accident/Illness Investigations Procedures, 2011. Available online: https://arlweb.msha.gov/READROOM/HANDBOOK/PH11-I-1.pdf.

[294] CIM, Annual Report of Chief Inspector of Mines, Punjab, 2011. Available online: https://cim.punjab.gov.pk/system/files/Annual%20Report-14.pdf.

[295] M. R. Soltanian, M. A. Amooie, D. R. Cole, T. H. Darrah, D. E. Graham, Pfiffner, S. M. Graham, and J. Moortgat, ”Impacts of methane on carbon dioxide storage in brine formations”, Groundwater, Vol. 56, no. 2, pp. 176-186, 2018.

[296] CISCO, ”Visual Networking Index Conducted by Cisco”, 2020. Available online: https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html.

[297] S. Vural, and E. Ekici, ”Analysis of hop-distance relationship in spatially random sensor networks”, In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, May, 2005, pp. 320-33.

[298] Y. Zhang, W. Yang, D. Han, and Y. I. Kim, "An integrated environment monitoring system for underground coal mines—Wireless sensor network subsystem with multi-parameter monitoring. Sensors", Vol. 14, no. 7, pp. 13149-13170, 2014.

[299] I. O. Osunmakinde, "Towards safety from toxic gases in underground mines using wireless sensor networks and ambient intelligence", International Journal of Distributed Sensor Networks, Vol. 9, no. 2, pp. 159273, 2013.

[300] B. W. Jo, and R. M. A. Khan "An event reporting and early-warning safety system based on the internet of things for underground coal mines: A case study", Applied Sciences, Vol. 7, no. 9, pp. 925, 2017.

[301] B. W. Jo, R. M. A. Khan, and O. Javaid "Arduino-based intelligent gases monitoring and information sharing Internet-of-Things system for underground coal mines", Journal of Ambient Intelligence and Smart Environments, Vol. 11, no. 2, pp. 183-194, 2019.

[302] U. I. Minhas, I. H. Naqvi, S. Qaisar, K. Ali, S. Shahid, and M. A. Aslam, "A WSN for monitoring and event reporting in underground mine environments", IEEE Systems Journal, Vol. 12, no. 1, pp. 485-496, 2017.

[303] X. Shuo, W. E. I. Xueye, and W. A. N. G. Yu, "A multipath routing protocol for wireless sensor network for mine security monitoring", Mining Science and Technology (China), Vol. 20, no. 1, pp. 148-151, 2010.

[304] P. Misra, S. Kanhere, D. Ostry, and S. Jha, "Safety assurance and rescue communication systems in high-stress environments: A mining case study", IEEE Communications Magazine, Vol. 48, no. 4, pp. 66-73, 2010.

[305] S. Bhattacharjee, P. Roy, S. Ghosh, S. Misra, and M. S. Obaidat, "Wireless sensor network-based fire detection, alarming, monitoring and prevention system for Bord-and-Pillar coal mines", Journal of Systems and Software, Vol. 85, no. 3, pp. 571-581, 2012.

[306] M. A. Moridi, Y. Kawamura, M. Sharifzadeh, E. K. Chanda, and H. Jang, "An investigation of underground monitoring and communication system based on radio waves attenuation using ZigBee", Tunnelling and Underground Space Technology, Vol. 43, pp. 362-369, 2014.

[307] G. Kumar, and P. Tomar, ”IPv6 Addressing Scheme with a Secured Duplicate Address Detection”, IETE Journal of Research, Vol. 68, no. 5, pp. 3371-3378, 2022.

[308] G. Kumar, and P. Tomar, ”A survey of IPv6 addressing schemes for internet of things”, International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), Vol. 2, no. 2, pp. 43-57, 2018.

BRIEF BIO DATA

Gyanendra Kumar did his B.Tech. from UPTU Lucknow, India, M.Tech, and PhD (Pursuing) in Computer Engineering from J C Bose University of Science and Technology, YMCA, Faridabad, (Haryana) and working as Assistant Professor with Galgotias University, Greater Noida, UP. His research interests include Adhoc Networks, Operating Systems, Web Mining, Image Processing, and IoT. He has published seven research papers in SCI-indexed journals and 14 papers in Scopus-indexed journals. He has also reviewed many research papers of reputed journals such as Symmetry, Electronics, and Applied Science, Sustainability journals of MDPI, Computer and Electrical Engineering, Internet of Things of Elsevier etc.

LIST OF PUBLICATIONS

Referred journals:

[1] **Gyanendra Kumar** and Parul Tomar, ”A novel longest distance first page replacement algorithm,” ***Indian Journal of Science and Technology***, Vol. 10 (30), 2017 . **(Web of Science)**

[2] **Gyanendra Kumar** and Parul Tomar, ”A Survey of IPv6 Addressing Schemes for Internet of Things,” ***International Journal of Hyper Connectivity and the Internet of Things (IJHIoT)***, Vol. 2 (2), pp. 43-57, Jul. 2018.

[3] **Gyanendra Kumar** and Parul Tomar, ”IPv6 Addressing Scheme with a Secured Duplicate Address Detection,” ***IETE Journal of Research***, Vol. 68 (5), pp. 3371-3378, 2022. **(SCI)**

[4] **Gyanendra Kumar** and Parul Tomar, ”A Stateless Spatial IPv6 Address Configuration Scheme for Internet of Things,” ***IETE Journal of Research***, Oct. 2021. **(SCI)**

[5] **Gyanendra Kumar** and Parul Tomar, ”SENSEnuts IoT Platform and Bayes Decision Theorem Based Mine Control System,” ***MESA Journal***, , Vol. 12(4), pp. 901-914, Nov 2021. **(SCOPUS)**

[6] **Gyanendra Kumar**, Parul Tomar, and Lal Pratap Verma ”Path Rank Based Data Chunk Scheduling for Concurrent Multipath Transmission,” ***The Computer Journal, Oxford***, June. 2022. **(SCI)**

[7] **Gyanendra Kumar**, Parul Tomar, Lal Pratap Verma, Varun Kumar Sharma, Dimitris Kanellopoulos, Sur Singh Rawat, Youseef Alotaibi ”Cmt-sctp and mptcp multipath transport protocols: A comprehensive review,” ***Electronics, MDPI***, July. 2022. **(SCI)**

International conferences:

[1] **Gyanendra Kumar** and Parul Tomar, ”A Review of Concurrent Multi Path Transmission Transport Layer Protocol,” ***TAME 2021***, Faridabad, 2021.

[**2**] **Gyanendra Kumar** and Parul Tomar, "An Experimental Study of Concurrent Multipath Transmission Protocol in Lossy and Asymmetric Network Environment," ***ICICV-2021***, Jaipur, 2021.