Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Kufa
Faculty of Computer Science and Mathematics
Department of Computer Science

Enhanced Security and Performance in MANETs with Blockchain and Deep Learning

A Thesis

Submitted to the Council of College of Computer Science and Mathematics / University of Kufa in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Computer Science

By

Huda Abdulraheem Ahmed

Supervised by

Prof. Dr. Hamid Ali Abed Al-Asadi

2024 A.D 1446 A.H

﴿وَقُل رَّبِّ أَدْخِلْنِي مُدْخَلَ صِدْقٍ وَأَخْرِجْنِي مُخْرَجَ صِدْقٍ وَاجْعَل لِّي مِن لَّدُنكَ سُلْطَانًا نَّصِيرًا﴾

صدقَ اللهُ العليُّ العظيم

﴿ سورة الاسراء: الآية 80 ﴾

Declaration

Aware of legal liability I hereby declare that I have written this dissertation myself and all the contents of the dissertation have been obtained by legal means.

Signature:

Date: / /2024

Name: Huda Abdulraheem Ahmed

Approval of Scientific Supervisor

I certify that this dissertation, **"Enhanced Security and Performance in MANETs with Blockchain and Deep Learning"** was prepared under my supervision at the University of Kufa, Faculty of Computer Science and Mathematics, in a partial fulfillment of the requirement for the degree of Doctor of Philosophy in Computer Science.

Signature:

Supervisor's Name: **Prof. Dr. Hamid Ali Abed Al-Asadi**

Degree: Prof. Dr.

Date: / /2024

In view of the available recommendations, I forward this dissertation for debate by the examining committee.

Signature:

Name: **Prof. Dr. Furkan Hassan Saleh**

Head of Computer Science Department, Faculty of Computer science and Mathematics, University of Kufa.

Date: / /2024

Certification of Linguistic Expert

I certify that I have read this dissertation, **" Enhanced Security and Performance in MANETs with Blockchain and Deep Learning"** and corrected its grammatical mistakes; therefore, it has become qualified for debate.

Signature:

Name:

Degree:

Address:

Date: / /2024

Certification of Scientific Expert

I certify that I have corrected the scientific content of this dissertation, **" Enhanced Security and Performance in MANETs with Blockchain and Deep Learning",** therefore, it has become qualified for debate.

.

Signature:

Name:

Degree:

Address:

Date: / /2024

Certification of Scientific Expert

I certify that I have corrected the scientific content of this dissertation, **" Enhanced Security and Performance in MANETs with Blockchain and Deep Learning",** therefore, it has become qualified for debate.

.

Signature:

Name:

Degree:

Address:

Date: / /2024

Committee's Report

We are the chairman and members of the examination committee; we certify that we have read this dissertation **" Enhanced Security and Performance in MANETs with Blockchain and Deep Learning"** as the examining committee, examined the student (Ahmed Raheem Kadhim) in its content and it is qualified as a dissertation for the degree of Doctor of Philosophy in Computer Science.

Signature:
Name:
Title:
Date: / /2024
(Member)

Signature:
Name:
Title:
Date: / /2024
(Member)

Signature:
Name:
Title:
Date: / /2024
(Member)

Signature:
Name:
Title:
Date: / /2024
(Member)

Signature:
Name: Furkan Hassan Saleh
Title: Professor
Date: / /2024
(Member & Supervisor)

Signature:
Name:
Title:
Date: / /2024
(Chairman)

Approved for the Council of the Faculty of Computer Science and Mathematics, University of Kufa.
Signature:
Name: **Assist. Prof. Dr. Salam Hassan Mhesn Al-Augby**
Dean of the Faculty of Computer Science and Mathematics
Date: / /2024

DEDICATION

To my father & Mother souls

To my family with love

To

Everyone who encourages and helps me with Gratitude

Huda Abdulraheem Ahmed

ACKNOWLEDGEMENTS

Sincerely and greatly, I feel urged to praise almightily "**ALLAH**" the most gracious and most merciful, and his prophet **"MOHAMMED"** and his kinsfolk because this research has been completed under their benedictions.

This dissertation would not have been possibly written without the help, support, advice, and patience of my supervisor, **Prof. Dr. Hamid Ali Abed Al-Asadi,** His expertise, insightful comments, and useful advice have decisively contributed to this work. The words are not enough to express my gratitude for all that they have done for me.

I would also like to thank my family and friends for their support, as always, for which my mere expression of thanks likewise does not suffice. Finally, my sincere thanks to everyone who helped me to complete this work.

Abstract

Mobile Ad Hoc Networks (MANETs) face critical challenges, including non-optimal routing, security vulnerabilities during data transmission, and performance degradation due to unicasting, multicasting, and geo-casting demands. These issues are further exacerbated by the dynamic nature of MANETs, characterized by frequent topology changes and varying node mobility speeds. Addressing these challenges requires an efficient routing strategy that can ensure both security and optimal data delivery across the network.

To tackle these problems, this research introduces an Optimized Link State Routing (OLSR) protocol enhanced with a deep learning model and blockchain technology. A novel Twin-Attention based Dense Convolutional Bidirectional Gated Network (SA_DCBiGNet) is developed to detect black hole nodes, while the Extended Osprey-aided Optimized Link State Routing Protocol (EO_OLSRP) and Extended Osprey Optimization Algorithm (EOOA) are employed to select optimal routes based on node and link stability. The model also integrates blockchain storage using the Interplanetary File System (IPFS) to secure data, with validation performed through a Delegated Proof of Stake (DPoS) consensus mechanism. This approach ensures both high security and efficiency in routing and data transmission.

The proposed model is evaluated using multiple mobile simulation models in conjunction with the NS3 simulator and achieves superior results compared to

existing methods. The model delivers a packet delivery ratio (PDR) of 99.8%, with throughput reaching 2900 Kb/s, and reduces routing overhead to 41.7% and end-to-end delay to 19.1 ms. Compared to conventional approaches like SRABC, HEDAR, and SETORD, the proposed model demonstrates significant improvements in key performance metrics, proving its effectiveness in enhancing both the security and performance of MANETs for video transmission.

List of Abbreviations

Abbreviation	Description
AEACO	Adaptive Elite Ant Colony Optimization
AI	Artificial intelligence
AODV	Ad hoc On-Demand Distance Vector
AQOR	Ad hoc Qos on-demand routing
ARF	Auto Rate Fallback
AVC	Advance Video Coding
BANs	Body Area Networks
BGP	Border Gateway Protocol
BLTM	Blockchain-Based Lightweight Trust Management
BS	Base Station
CARA	Collision-Aware Rate Adaptation
CBMANET	Control Based Mobile Ad hoc Networking
CCA	Clear Channel Assessment
CEDAR	Core-Extraction Dis- tributed Ad hoc Routing
CNN	Convolutional Neural Network
CPM	Critical Path Method
CSGR	Cluster-head Switch Gateway Routing
DARPA	Defense Advanced Research Projects Agency
DAGs	Directed Acyclic Graphs
DCFM	Denial Contradictions with a Fictitious node Mechanism
DLCP	Dynamic Load balancing Cluster based Protocol
DoS	Denail of Service
DNN-DoS	Deep Neural Networks based DoS
DPoS	Delegated Proof of Stake
DPoT	Delegated Proof of Trust

DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
DWT	Discrete Wavelet Transform
ECS	Enhanced Cuckoo Search
EDCA	Enhanced Distributed Channel Access
EDCF	Enhanced Distributed Coordination Function
EDCF-DM	EDCF with Dual Measurment
EFCM	Enhanced Fuzzy C-Means Algorithm
EO_OLSRP	Extended Osprey-Assisted Optimized Link State Routing Protocol
ETSI	European Telecommunications Standards Institute
FDMA	Frequency-Division Multiple Access
FEC	Forward Error Correction
FSR	Fisheye State Routing
GAHC	Genetic Algorithm with Hill Climbing
GPSR	Greedy Perimeter Stateless Routing
GSR	Dynamic Source Routing
HAS	Http Adaptive Streaming
HCPSO	Hybrid Cat-Particle Swarm Optimization
HDTC	High-Definition TV Content
HDWSNs	High Density Wireless Sensor Networks
HEDAR	Highly Efficient Dual Authenticated Routing
HWMP	Hybrid Wireless Mesh Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
LANMAR	Landmark Routing Protocol
LAR	Location-Aided Routing

LMR	Land Mobile Radio
LRT	Link Residual Time
LSTM	Long Short-Term Memory
MAC	Medium Access Control
MANETs	Mobile Ad hoc Networks
MDC	Multiple Description Coding
MDSQ	Multiple Description Scalar Quantizers
MIO	Maritime Interdiction Operations
MMEE	Multi-path Multi-Channel Energy Eficient
MPR	Multi-Protocol Router
MSLD	MANET Service Location and Discovery
NCW	Network-Centric Warfare
NS3	Network Simulator 3
OLSP	Optimized Link State Protocol
OLSR	Optimized Link State Routing
OOA	Osprey Optimization Algorithm
OSI	Open Systems Interconnection
OSI	Open Systems Interconnection
PANs	Personal Area Networks
PAMAS	Power Aware Multi-Access with Signaling
PISVT	Protocol Independent Secure Video Transmission
PBFT	Practical Byzantine Fault Tolerance
QoE	Quality of Experience
QoS	Quality of Service
RAS-HO	Resource Allocation theme for wireless video Sending with Hybrid Optimization
RBAR	Receiver-Based Auto Rate
RODQL	Reward Optimized Deep Q Learning

RTS/CT	Request to Send/Clear to Send
SA_DCBiGNet	Twin-Attention-Based Dense Convolutional Bidi-Rectional Gated Network
SCTP	Stream Control Transmission Protocol
SETORD	Secured Encryption Technique with Optimum Route Discovery
SPAN	Switched Port Analyzer
SRA	Secure Routing Algorithm
SRABC	SRA Blockchain
SVM-DoS	Suppose Vector Machine based DoS
TCP	Transmission Control Protocol
TDMA	Time-Division Multiple Access
TMS	Trust Management System
TORA	Temporary Ordered Routing Algorithm
UAVs	Unmanned Aerial Vehicles
USSOCOM	United States Special Operations Command
VoD	Video-On-Demand
WRP	Wireless Routing Protocol
WSN	Wireless Sensor Networks
XML	Extensible Markup Language
ZHLS	Zone-Based Hierarchical Link State
ZRP	Zone Routing Protocol

List of Symbols

Symbol	Meaning
$\vec{h}_t^1 \in N^H$ **and** $\vec{h}_t^2 \in N^H$	Output of the hidden layer in the forward direction
H	Number of elements
t	Time
$\overleftarrow{h}_t^1 \in N^H$ **and** $\overleftarrow{h}_t^2 \in N^H$	Output of the hidden layer in the reverse direction
$x_t \in N^T$	Each label value for the merging term at the instant
T	Number of labels
y_t	Input time
$f(.)$	Activation function
a **and** w	Weight matrices
$g(.)$	GRU processing network
c	Total number of modules
N_t	Total number of samples
E_c	True vector
E_c^k	Label matrix
n	Node
y	Independent node
$T_y(n)$	Likelihood of performing a given predicted action
$0 < \varepsilon < 1$	Weighting factor
$T_x(n; j)$	Dependability of node n
$Y \in R^{C \times C}$	Channel's attention architecture

y_{ji}	Outcome of i^{th} channel
$F \in R^{C \times H \times W}$	End result
β	Scale parameter
$N = H \times W$	Total amount of pixels
s_{ij}	i^{th} Position is influenced by the j^{th} position
$K_{s \to y}$	collection of paths that starts at a font node s and end at an end node y
$T_x(k; j)$	Trustworthiness of the path itemized by the node y
C_{ij}	Link stability from i and j
X_{ij}	Safety degree
$\lambda_1, \lambda_2, \lambda_3$	Weighting vectors
LQ_{ij}	Link quality
S_{ij}	Factor for forecasting mobility
$V(Y)$	Variance
h	Total number of nodes
Y_h	Message level attained from each adjacent node
p	Position of the search agents
p_i	i^{th} search agents
$p_{i,j}$	j^{th} dimension
N	Total number of search agents
M	Problem variable
r_{ij}	Random variable in the range between [0,1]
lb_j	Lower bound
ub_j	Upper bound

G_i	Objective function of i^{th} search agents
G	Choice of the objective function
GL_i	Feature positions of i^{th} search agents
P_{best}	Finest search agents' locations
$P_i^{L_1}$	New position of i^{th} search agents in the preliminary point
$p_{i,j}^{L_1}$	j^{th} vector
$G_i^{L_1}$	Objective function rate
$R_{i,j}$	Random variable in the range of [0,1]
$P_i^{L_2}$	Second sage location of i^{th} search agents
$P_{i,j}^{L_2}$	j^{th} vector
$G_i^{L_2}$	Objective function value
K	Number of iterations
$p \in R^n$	Real vector
$\overline{p} \in R^n$	Opposite vector

List of Figures

List of Tables

Table of Contents

Bundesrepublik Deutschland

Urkunde

über die Eintragung des
Gebrauchsmusters Nr. 20 2024 101 651

Bezeichnung:

Ein neuartiges optimiertes Link State Routing Protokoll für effiziente Videopaketübertragung und Blockchain-System für verbesserte Sicherheit in MANETS

IPC:

H04L 47/2491

Inhaber/Inhaberin:

Ahmed, Huda Abdulraheem, Basrah, IQ
AL-Asadi, Hamid Ali Abed, Prof. Dr., Basrah, IQ

Tag der Anmeldung:

05.04.2024

Tag der Eintragung:

29.04.2024

Die Präsidentin des Deutschen Patent- und Markenamts

Eva Schewior

Eva Schewior

München, 29.04.2024

Die Voraussetzungen der Schutzfähigkeit werden bei der Eintragung eines Gebrauchsmusters nicht geprüft.
Den aktuellen Rechtsstand und Schutzumfang entnehmen Sie bitte dem DPMAregister unter www.dpma.de.

Chapter One

General Introduction

Chapter 1: General Introduction

1.1 Preface

Advancements related to computers and communications have come a long way during the last several decades. Mobile phone users may communicate with one another and share information quickly and efficiently because of quicker, smaller, as well as more dependable gadgets [1]. Units in a mobile setting require an infrastructure that facilitates the exchange of information and communication while they are on the go [2]. Strategic networks have many difficulties because of the severe geographical characteristics and conditions of the operational environment, such as limited bandwidth, excessive latency, and inadequate reliability [3].

In general, the connectivity architecture of battlefield networks is not static. Since mobile ad hoc networks (MANETs) do not rely on any form of pre-existing infrastructures they may be used in strategic contexts that are both energetic and inspiring. Because of its adaptability, MANETs are a desirable network choice for tactical tasks. Comparing MANETs to standard wireless connections reveals a number of benefits [4]. The prominent advantages include reliability, enhanced node mobility, self-organizing interaction, scalable ad hoc network routing, adaptability, and self-management. When a quick communication system installation is required for tactical operations like Maritime Interdiction Operations (MIO) and United States Special Operations Command (USSOCOM) tasks, MANETs come in convenient, in addition to other applications of MANETs such as, extended networks connectivity, service of emergency, vehicular networks, smart cities, and IoT.

MANETs are often used in practical situations as necessary [5]. Because of the constantly changing nature of the links and lack of a fixed configuration

are referred to on-demand technologies. No new infrastructure is needed since the wireless network has previously been set up. An automatic network is created among MANET terminals as they are self-configured. Furthermore, due to node is movable, its setup is dynamic. Because nodes in a network are used regardless of uses, their resources are restricted. Due to capacity improvements and current technical developments, they are additionally employed for video streaming. Services for live streaming of videos are becoming more and more common in human life. People started using cellular phones and other handheld gadgets everywhere in the globe and in all spheres of life. A further application for the MANET devices in this scenario is video streaming [6]. A schematic depiction of a MANET is shown in Figure 1.1.

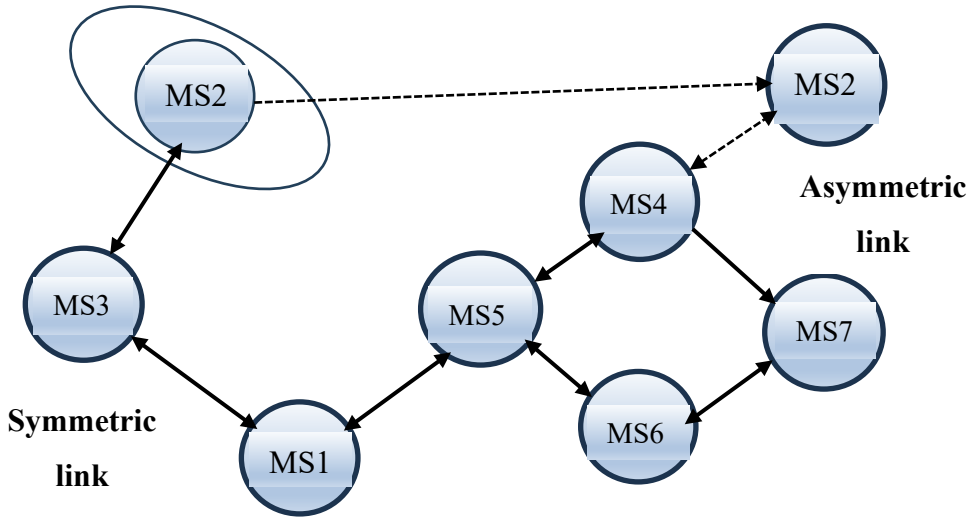


Figure 1.1. Typical illustration of a MANET

The principal problem is the limited resources of the MANET systems. It is challenging to utilize video streaming due to limitations in resources. In light of this, it is now crucial to research modifying the Open Systems Interconnection (OSI) model's layering to include video streaming. The model used for reference has many levels, such as the data link and physical layers. Video quality while streaming may be increased by making enhancements to the aforementioned layers. A number of investigators made

contributions in this direction. Particularly, more studies concentrated on implementing a cross-layered strategy that shall assist in improving the quality of video streaming in MANETs [15]. Figure 1.2 represents the conceptual architecture of MANETs.

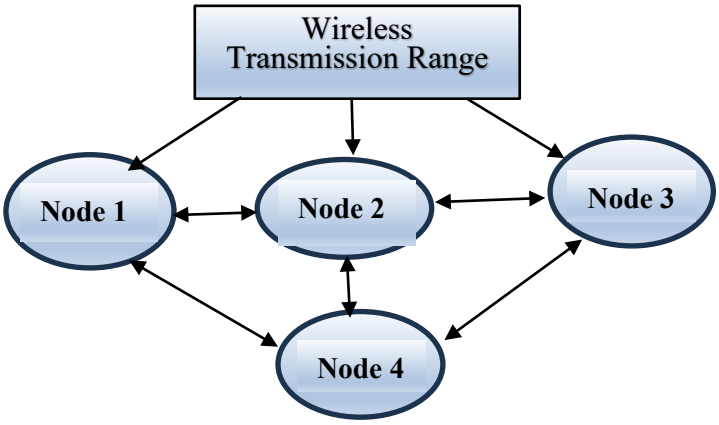


Figure 1.2. Architecture of MANETs

MANETs possess self-configuration capabilities, self-organization abilities, dynamic network configuration, resource constrained, limited link capacity and security, as well as operate without any fixed infrastructure. MANETs function in a multi hop fashion, enabling mobile nodes not only to transmit their own packets but also to forward packets to additional mobile nodes. Furthermore, the prominence of internet-based video streaming has developed recently, incorporating various applications such as High-Definition TV content (HDTC), mobile TV, video chats on mobile devices, and surveillance systems.

High bandwidth demands and strict delay limitations is increased in video streaming since rapid delivery of packets is necessary to ensure uninterrupted multimedia transmissions. The image resolution deteriorates if packets are dropped or arrived slowly because decoding problems often spread to other parts of the stream. Owing to video's enormous bit rate demands, a multimedia stream can trigger major congestion in the network [8]. Therefore, it is critical to consider the prospective influence of every

single video user on the network's characteristics and ensure the underlying network does not consume more resources than it can handle. However, many network architectures lack the processes necessary for the protocol layers to adjust appropriately to bottom channel situations and particular requirements of applications. Although protocol layering is a useful concept for simplifying network architecture, its use in wireless systems is limited by the inability to easily separate the levels due to the characteristics of the medium of wireless communication [9]. Furthermore, it is challenging to achieve the overall performances desired by complex applications in the absence of protocol layer interactions.

1.1.1Video Transmission over MANETs

the system needs to have a suitable capacity as well as an acceptable delay and jitter limit. Furthermore, the video codec needs to have enough flexibility to adjust a video stream to the specific network settings at any time. Therefore, a codec needs to be capable of lowering stream bitrates yet preserving a suitable level of clarity. HTTP Adaptive Streaming (HAS) has become the most popular way to distribute commercial video, such as movies and TV shows, in standard VoD providers [10]. The video material is codec-independently split into short-duration chunks and encoded at various encoding speeds (quality levels). The end user will alternate among the segments of varying specifications instead of the content server, depending on several factors such as projected bandwidth availability, CPU capability, and screen resolution. Providing error-free content is one of HAS's advantages from the perspective of the content supplier. This is because HTTP is based on a dependable Transmission control protocol (TCP). However, there are a number of drawbacks to the HAS streaming technique for MANETs and the programs that are running on it.

- The extra delay added to interactive videos will end up resulting in an absence of synchronization between sender and receiver, especially in a wireless setting where failures lead to TCP re-transmissions.

- Since multi-hop routing requires transmitters-receivers to be continuously on, the necessity of continually producing numerous versions of a video may result in shorter battery lifespans, which might compromise the task of a rescue team. The only exception to this rule is if the MANET is truly a VANET, in which instance the alternator of the car might provide power by way of the battery.

- User datagram protocol (UDP) is an increasingly practical transport protocol since it allows for continued streaming regardless of the event of a packet being lost and node-controlled rerouting in the event that a node moves beyond the range and renders a wireless link inoperable.

Large buffers and a considerable start-up time are used in TCP-based streaming to offset the trade-off between error-free transmission as well as delay. Because of the complexity of dynamic memory refresh as well as memory access, bigger buffers can deplete the battery [11]. Figure 1.3 displays the overall routing mechanism types in MANETs.

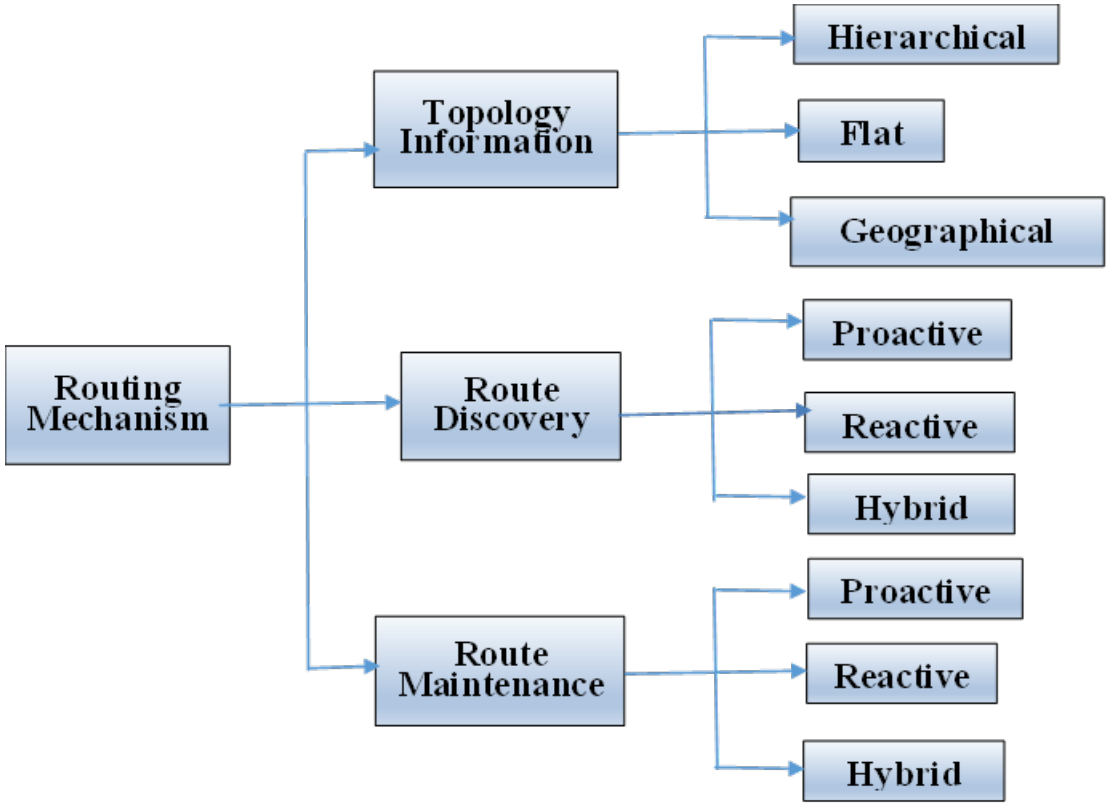


Figure 1.3. Submodules of routing mechanisms in the MANET

The acronym for Optimized Link State Routing Protocol is OLSR [12]. In this method, every single node routinely broadcasts the state of its links. Each node broadcasts link state data that it has obtained from neighbours in its vicinity. Each node keeps track of the link state information it gets from other nodes. Each node uses the information mentioned earlier to calculate the next hop for each destination. Tables have an impact on it and make it proactive. Below are some advantages of the OLSR approach [13].

- Because OLSR possesses a low average E2E latency, it is utilized for operations that require the least amount of latency.
- OLSR execution is easier to make use of and less expensive to work with compared to other methods. Furthermore, the routing method is flat.

- Its routing procedure can be handled without the use of the central management system.
- Because both the source and the destination pairings can vary quickly, the protocol is more appropriate for MANETs.
- Since the communications are delivered asynchronously and are transmitted on a regular basis, a dependable message control connection is not necessary.
- By only communicating topological data contained in response to an alteration in the network topology, OLSR lowers the volume of network overhead. This lessens congestion and conserves network resources.
- OLSR can manage big networks with lots of nodes without seeing a noticeable increase in overhead or latency because of its flexible architecture. It can therefore be used in sizable MANETs.
- The network's robustness and dependability may be improved by using OLSR's capability to identify various routes connecting source and DNs.
- Because of its power-efficient architecture, OLSR can be used in wireless networks with low battery capacity. Lowering the overall amount of broadcast messages and streamlining the routing procedure accomplish this.
- OLSR may be used in dynamic circumstances like MANETs since it can swiftly adjust to alterations in the configuration of the network.

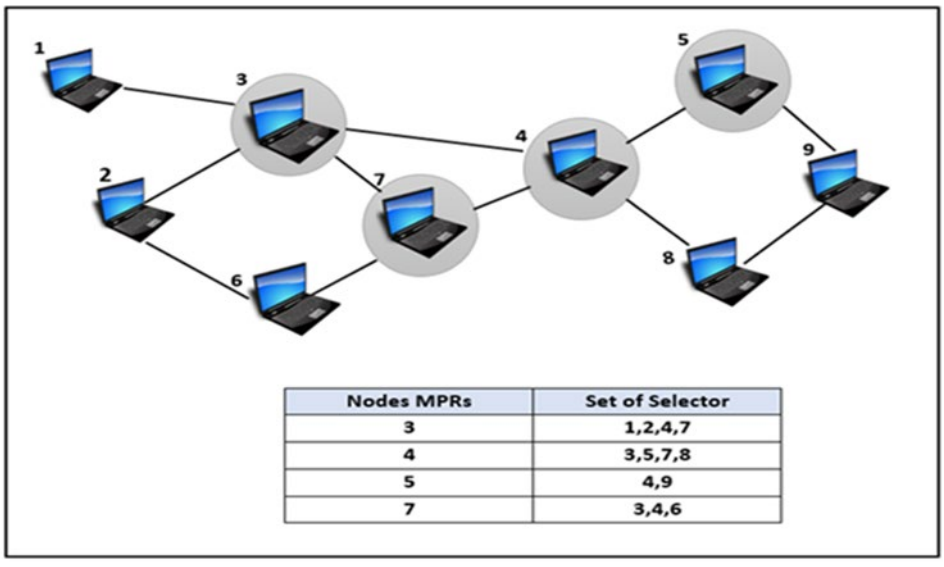
MultiPoint Relaying is a technique used by OLSR to lessen message flooding. In this model, every node (n) selects a set of neighbouring nodes to serve as

multipoint relays (MPR(n)). These nodes then deliver control packets about n-neighbours that are not in MPR(n) and analyse control packets from n, whereas they advance the packets. MPR(n) is nominated such that MPR's single-hop neighbours (n) include each of N's two-hop neighbours [14].

The most utilized ad-hoc routing protocol is OLSR. The most important node that stands out is the critical path method (CPM), which is the best position to get across in a flooding process so as to reach every node without extending out in every direction. All supervisory roles are decreased when the MPR delivers a connection status.

OLSR needs to provide the shortest path routes is incomplete link state flooding, as seen in Figure 1.4. OLSR is intended to function entirely autonomously, without depending on any one source.

The procedure can tolerate an equitable loss of some control messages since every single node provides them on a frequent basis, negating the need for dependable control message transmission [15].



Nodes MPRs	Set of Selector
3	1,2,4,7
4	3,5,7,8
5	4,9
7	3,4,6

Figure 1.4. Example network of OLSR

1.1.2. Blockchain with MANETs

Blockchain is a scattered ledger system it enables one to store transactions or information records that can be considered safe, clear, and impervious to tampering [16]. It first came to light in 2008 as the basic technology behind Bitcoin, a system of decentralised digital currency. Today, however, it is used in many other domains wherein the goal is to do away with the middleman. A blockchain is essentially a digital ledger that chronologically but irrevocably preserves a sequence of operations or blocks of information. The sequence of blocks that are referred to as a "blockchain" created when every block has hashes of the one before it. A block is immune to manipulation and deception when it has been included in the chain since it is unable to be removed or changed without destroying all blocks that come after it. The foundation of the blockchain system is a distributed system of nodes, each of which contributes to the verification of fresh activities or blocks and keeps an archive of the ledger. Whenever a transaction gets uploaded to the blockchain, it is tested by nodes on the network using a process known as consensus that guarantees agreement among all nodes regarding its authenticity. The blockchain's basic principles are depicted in Figure 1.5.

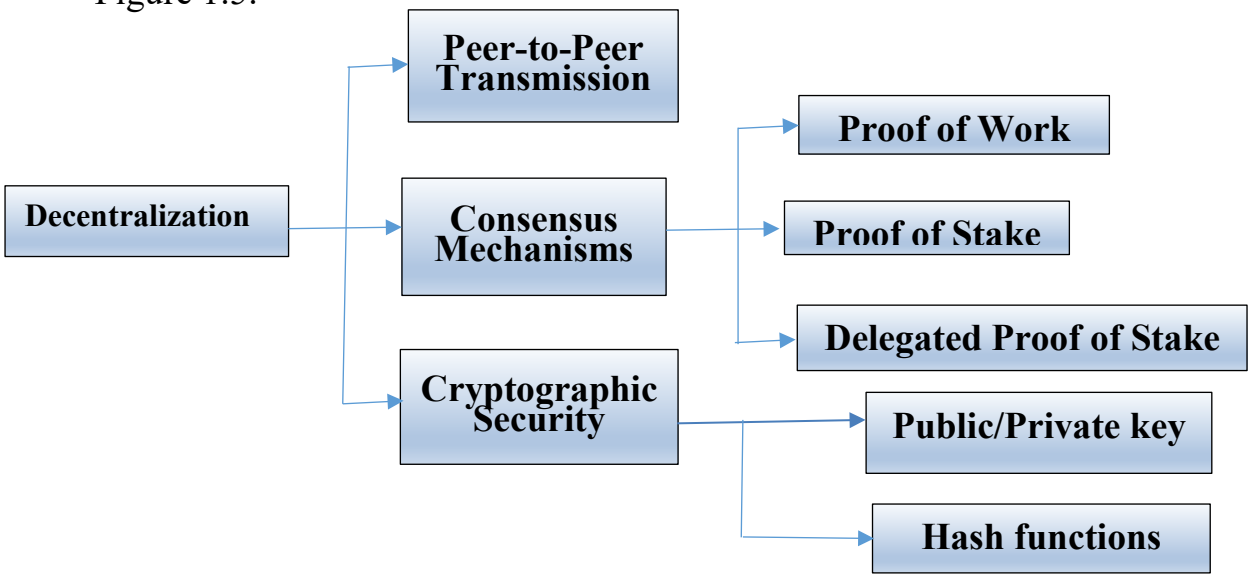


Figure 1.5. Blockchain Principles

Blockchain is being used in a number of industries, including logistics, supply chain management, medical services, and academic validity authentication. Practical Byzantine Fault Tolerance (PBFT), is used by certain blockchain platforms, such as Hyperledger. For the above technique to work, two of the three nodes must concur on their agreement. Scalability with MANETs can prove problematic because of frequent connection failures. Thus, PBFT might not work.

A multitude of severe problems arising from the constantly changing architecture, node movement, restricted processing power, constrained bandwidth capability, restricted battery power, and safety features of MANETs pose a danger to their survival and rate of acceptance. There are several problems with security. The largest is the absence of trust amongst nodes, which underlies the majority of additional safety issues, including MANET routing stability [17].

Consequently, implementing a strong trust system will automatically make the system secure. Finding the nodes that are acting improperly and do not merit the confidence of their fellow nodes is the difficult part of maintaining a stable and accessible connection that performs as intended. By resolving this problem, all of the network's nodes will behave properly and operate according to plan, which will enhance the protection of the MANETs. The primary issue with how packets is routed in MANETs is that uneven transmission of packets is often caused by the participant nodes' lack of reliability and credibility. Routing, identifying malicious nodes, time synchronization, safety levels, reliability, and nodes' ability to perform a certain type of observing duty are only a few of the scenarios where trust is helpful [18].

Blockchain is an innovation that facilitates transparent, safe, decentralized data storage and transmission. It functions as an enormous

repository that maintains a record of every communication among participants from the time the blockchain was established. The decentralized design of blockchain, meaning it's essentially maintained by a select group of individuals rather than an individual server, is one of its best features. Blockchain technologies contain safety features to safeguard the infrastructure and do not require a middleman to confirm that the data and chain are legitimate. A "blockchain" is a hash chain that is ultimately formed by every single block holding hash of the preceding block[19].

PBFT, is used in certain blockchain platforms, such as Hyperledger. For the above technique to work, two of the three nodes must concur on their agreement. Scalability with MANETs can prove problematic because of frequent link failures. Thus, PBFT could not work. The application of blockchain-based principles to trust management was additionally investigated by the researchers; this is covered in the section that follows.

A randomized distributed method for establishing trust among nodes in MANETs is called Blockchain-Based Lightweight Trust Management (BLTM). Trust management plays a critical role in maintaining reliable interaction between nodes in MANETs [20]. Because they need an authoritative source to maintain trust, which would be unfeasible in a distributed network, typical central trust management approaches may not be suitable for MANETs. Consequently, managing confidence in MANETS necessitates a distributed strategy.

MANETs utilize BLTM technology to enhance both the safety and reliability of node-to-node transmission. BLTM creates an accessible and safe trust architecture between nodes by fusing the blockchain platform with the trust management approach.

BLTM protocol for MANETs, which, as Figure 1.6 illustrates, is divided into four stages. They involve the stages of block maintenance, blockchain-based consensus, trust assessment, and block creation [21]. Every node assesses the reliability of its adjacent nodes during the trust assessment stage using a variety of factors, including the packet forward rate, reply time, and packet loss rates. In accordance with the assessment, the node subsequently allocates a trust level to every one of its neighbours.

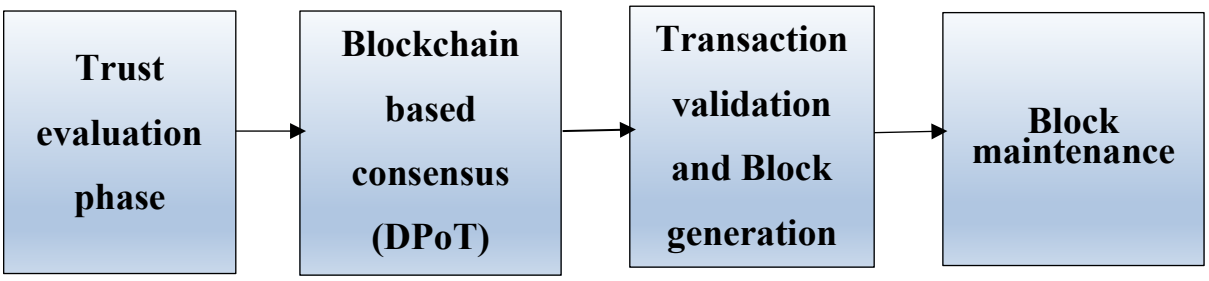


Figure 1.6. Phases of BLTM Protocol

In order to minimize the cost of computation and guarantee that agreement is obtained promptly, BLTM employs a lightweight consensus method. The method is referred to as Delegated Proof of Trust (DPoT). It is OLSR procedure compatible. To create DPoT, they embraced the DCFM plan. To reach a consensus, DPoT makes use of the delegator and validator nodes [22].

To construct a block in the framework of a blockchain, the delegate node must decide what data should be contained within the block in order to manage it during the block creation stage. After the pool's activities are gathered into a block, the blockchain network uses the SHA-256 method to generate a hash value that is appended to the block. This hash value is derived entirely from the information contained in the transactions. To link the blocks and form a chain, the hash from the one before it is additionally included as information in the present block. The block hash only supports a particular

structure, which consists of a hash signature that begins with ten consecutive zeros [23].

To ensure node confidence in a secure mobile ad hoc network, a blockchain could be used. Every blockchain block contains transaction-related data and accompanying metadata, such as a timestamp, transaction hash, delegate ID, and nonce. The hashed session contains the transaction generator ID, related transaction data, and the delegate ID. By doing this, it is made possible for block operations to be reliable and unreliable from none of the nodes that are involved [24]. Whenever the network is initially founded, the genesis block, which is the primary block in the blockchain, is produced containing a blank list of operations [25].

1.2 Related works

Malik et al. [26] describes the man-in-the-middle attack as a type of network safety assault that entails modifying and stopping network communication between two entities. This can be accomplished regarding routing protocols by faking routing packets, which leads to routers directing traffic via the attacker's computer. Afterwards, the attacker alters and disrupts the traffic before sending it to its intended location. Passwords and corporate data are examples of sophisticated information that can be obtained by man-in-the-middle attacks.

Intending to provide soft QoS assistance for MANETs that are severely burdened with each optimal transmission and demand considerably less latency than, for example, a data transfer application, the recommended design makes use of the IEEE 802.11e standard. Setting traffic priorities and modifying routing protocols based on application demands might help reduce latency. Using the IEEE 802.11e procedure, the researchers distinguish among various applications' accessibility at the MAC layer according to QoS

demands. Compared to wired networks having static infrastructures where there may be several regulatory zones in the route connecting the video transmitter utilizing MANETs, where all the nodes serve as a gateway. The Enhanced distributed coordination function (EDCF) is the primary functionality in the IEEE 802.11e standard that offers QoS [27].

Since the Ad hoc system has restricted resources, power becomes a crucial problem that needs to be handled. Multiple investigations have put forward various approaches [28] to manage scarce resources in an effective way. The two main kinds of power-efficient protocol specifications for MANET routing are primarily load transfer and distribution management, which depend on the route to effectively decrease the power used in the communication procedure.

Black and Grey Hole Attack Detection in MANETs Using a Hybrid Cat and a PSO-based deep learning procedure was first presented by Venkata subramanian et al. [29]. MANET solution uses deep learning algorithms to recognise both blackhole and greyhole attacks. The forwarding ratio measure is utilised in each attack detection block to determine the difference between the faulty and normal nodes. In order to evade discovery, maladaptive nodes altered the collected records. Convolutional neural networks (CNNs) and long short-term memory (LSTM) networks were used to stop this. Hybrid cat-particle swarm optimisation (HCPSO) algorithm is applied to adjust the parameters. The computational cost and effectiveness of this proposed method are constrained.

A Secure Routing Procedure was presented by Ghodichor et al. [19] to mitigate threats using the blockchain frameworks in MANET. Multiple nodes are linked together in a network during MANET communication, making it vulnerable to many types of assaults. As a result, this approach uses a Safe routing algorithm (SRA) that makes use of blockchain to explain a variety of

threats that impact MANETs Secure routing algorithm blockchain technology (SRABC). By applying a hash function to each data transmission, the SRA defends data flow and control against intrusions. Furthermore, examined is the function of blockchain in MANET security, and the relationship between SRA and blockchain is explained. Lastly, the SRABC technique is used to analyse the throughput and PDR and compare it with different routing protocols.

With the assistance of the Highly Efficient Dual Authenticated Routing (HEDAR) protocol, an extremely effective routing technique for dual authentication is presented that integrates To secure data dissemination between the source and destination, cypher text policy-attribute-based encryption (CP-ABE) is combined with a jammer attack detection model based on game theory. Fuzzy logic prediction rules are used by the method to identify the most likely path. The purpose of this is to improve network security and protect nodes from vulnerabilities. The suggested scheme's performance is evaluated in relation to several assessment measures at varying node density levels. The results produced provide a clear description of the proposed system and offer a practical and adaptable way to choose a route that satisfies the security requirements for transmitting data packets in a MANET environment [30].

The next generation of wireless networking has been seen to benefit greatly from the deployment of wireless mesh networks (WMNs), which can be applied to last-mile wireless internet access, home networking, transportation systems, wireless community networks, and wireless enterprise networks. Numerous vendors created their own proprietary mesh systems, but IEEE established a task force known as IEEE 802.11s to build an integrated mesh networking solution in order to achieve interoperability. The work group has established the Hybrid Wireless Mesh protocol (HWMP)

and airtime measurements as the default routing protocol and metrics. A limited number of test beds and several simulation studies have been conducted to assess the HWMP protocol's performance under the presumption of a distinct type of flow with fixed packet size and rate. Real networks, on the other hand, provide a wide range of applications (phone, video, FTP, email, etc.) and differ in terms of packet size and data rate. This article examines and evaluates the HWMP protocol's performance in such a diverse range of application scenarios [31].

Lwin et al. presented lightweight trust management in MANETs using blockchain technology [20]. These days, blockchain is commonly used in MANETs because of its properties such as provenance, consensus, and immutability. The blockchain is used for trustless data exchange between end nodes in addition to safe storage. The kinds of nodes used in the verification procedure and strategies for overcoming computational complexity are the issues in ad-hoc networks. The Optimised Link State Protocol (OLSP), a consensus algorithm and trust management system, are provided by this study to integrate the blockchain idea into MANET. As a result, blockchain resolves the OSLR problems since every node repeatedly carries out the security procedures. Using the current rules also keeps attackers away from the network. The findings demonstrated that this consensus approach, when applied to resource-hungry MANETs, lowers overhead and validation times.

To enable secure video transmission, Sharma et al. [32] combined DYDOG and an optimised Multi-Protocol Router (MPR) with adapted OSLR. Here, the hybrid approach that has been developed can guarantee safe video streaming in MANETs by optimising elements such as OLSR delay and energy consumption. The developed protocol analysed various malevolent attack nodes, such as wormholes, blackholes, and packet replication, to increase the node's mobility and promote security. This work

protected the frames from harmful assaults by encrypting them using techniques like digital signatures and AES. The results from the simulation are validated the effectiveness of the advanced methods. Table 1.1 summarises the body of current literature.

Table 1.1: Comparison of existing works

Ref.no. & year	Method Name	Routing Protocol	Compare With	Simulator Used	Simulation area/ No. of nodes	Result	Performance Metrics	limitations
[4], 2023	AODV and DSR	ADOV	DSR routing protocols	NS2	20	OLSR routing appears to be a good fit for military MANETs.	Routing maintenance and routing transparency	Number of nodes and pause time is reduced
[19], 2023	SRABC	SRA	Q-AODV and DSR	NS2	70	Better performance than compared methods	PDR, throughput, ROH, E2E	---
[33], 2022	high-quality video transmission	EVQDMBRM	State of art	NS2	60	Improved performance like packet loss reduction	Flow rate, video frame reliability, PSNR, Packet loss	Energy consumption in mobile devices is more
[32], 2022	MANET	PISVT	TORA, OLSR, AODV, DSDV	NS2	50	Better performance in QoS parameters	Packet delivery, delay, overhead, energy consumption, throughput	--
[29], 2022	MANETs	HCPSO	IDBA, ICCSO, ANN-FF	NS2	500	Better accuracy	Accuracy, PDR, Throuput, Energy Consumption	--

[27], 2022	MANETs	MSLD	Dir-based Dir-Less PDP	NS-3	50	Better performance	Overhead message, service availability, latency	Other performance metrics
[28], 2022	MANET	MMEE	PRMMAC, QoS-AOMDV, (QMR	NS2	10,30,50	Good performance	Load balancing, network reliability	--
[20], 2020	MANET	OLSR	DCFM	NS3	30	Scalability, reliability, availability	Attack detection overhead, Detection overhead time	Other performance metrics
[30], 2018	HEDAR	SDAR	Basic AOMDV	NS2	100	Satisfactory performance in different metrics	average detection time, network throughput, average end to end delay etc.	Processing time is little bit more,
[34], 2012	SETORD	WEP	AOMDV	NS2	60	Reduce Replay attack, and avoid authentication spoofing	Replay attack, authentication spoofing, node life time	Encounters a greater number of attacks

1.3 Dissertation Motivation

In this research, a Mobile Ad Hoc Network (MANET) is conceptualized as a dynamic network of mobile nodes interconnected via wireless communication, operating autonomously without centralized infrastructure. MANETs exhibit a range of intriguing characteristics, such as the ability to maintain continuous connectivity and remain flexible and responsive as nodes move from one location to another. A fundamental aspect of mobile-to-mobile communication in MANETs is the routing protocols, which dictate the path data, particularly video transmissions, take from the source to the destination. These routing protocols directly influence the overall performance of the network.

In MANETs, reactive routing protocols, such as the Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), are frequently employed due to their ability to conserve memory by establishing routes only when required. However, despite their utility, existing routing protocols, including SRABC, HEDAR, and SETORD, are vulnerable to various attacks, such as packet dropping and black hole attacks, which can lead to significant issues like network congestion and system failures. These security challenges hinder reliable data transmission, affecting both performance and the user experience.

To address these concerns, this research proposes a novel deep learning-based routing technique aimed at enhancing the efficiency of the Optimized Link State Routing (OLSR) protocol specifically for video transmission in MANETs. Additionally, the integration of blockchain technology strengthens the security of the network by providing decentralized and tamper-resistant storage for data. By leveraging both deep learning and blockchain, the proposed method improves route selection, network performance, and ensures more secure and efficient video data transmission across the network.

The model is further compared with existing approaches like SRABC, HEDAR, and SETORD, demonstrating superior performance in terms of security and efficiency.

1.4 Problem Statement

Delivering high-quality video streaming over Mobile Ad Hoc Networks (MANETs) is challenging due to the limitations of wireless communication. MANETs must handle complex factors such as maintaining network topology amid frequent node mobility. These challenges are magnified when transmitting large multimedia data, leading to unstable connectivity, packet losses, and degraded network performance.

As MANET deployment expands in critical areas like military communications, emergency response, and mobile video streaming, the need to manage data-intensive tasks becomes crucial. MANETs face scalability, security, and performance challenges under dynamic conditions. Node mobility in blockchain-enabled MANETs complicates data transmission as nodes change positions, disrupting block creation and validation. Combined with security issues and fluctuating bandwidth, this hampers high-quality video delivery.

The following points summarize the key issues faced in this research:

1. Inconsistent Connectivity: Node mobility in MANETs disrupts network links, leading to packet loss and unstable video streaming performance.
2. Security Vulnerabilities: MANETs are vulnerable to security attacks like black hole attacks, causing packet drops and compromising data transmission integrity.
3. Insufficient Bandwidth Utilization: Fluctuating bandwidth and high video streaming demands in MANETs lead to performance bottlenecks, reducing transmission efficiency.

4. Multi-hop Communication Issues: Multi-hop routing in MANETs increases latency, lowers throughput, and complicates routing, especially during video streaming.
5. Blockchain Scalability Problems: Frequent node mobility in MANETs disrupts blockchain operations, affecting block creation and data validation scalability.
6. Reactive Routing Limitations: Existing reactive routing protocols are inefficient for video transmission, causing delays and slow route discovery in MANETs.

1.5 The Objectives of the Dissertation

The primary goal of this dissertation is to develop an optimized routing protocol for video streaming over MANETs using advanced deep learning and blockchain technologies. The specific objectives of the research are outlined as follows:

1. **Conduct a Comprehensive Literature Review**

   Investigate the key challenges and complexities involved in developing routing systems for Wireless Multimedia Sensor Networks (WMSNs), with a focus on video streaming over MANETs.

2. **Develop a Novel E-OLSR Protocol**

   Design a scalable, energy-efficient, and reliable Enhanced Optimized Link State Routing (E-OLSR) protocol tailored for video streaming in WMSNs. This includes selecting and refining protocol parameters to optimize Quality of Service (QoS) metrics such as energy consumption, packet delivery ratio (PDR), throughput, and end-to-end (E2E) delay.

3. **Evaluate Protocol Performance in Various Network Scenarios**

   Analyze the performance of the proposed E-OLSR protocol under different network conditions using the NS3 simulator, considering factors such as network size, node mobility, and varying traffic loads.

4. **Compare QoS and Energy Efficiency with Existing Protocols**

   Benchmark the QoS metrics and energy efficiency of the E-OLSR protocol against current WMSN routing protocols, providing a thorough comparison based on simulation results.

5. **Incorporate Blockchain for Enhanced Security**

   Explore the integration of blockchain technology within WMSNs for secure routing decisions. This objective includes the design and implementation of a blockchain-based video routing system and evaluating its impact on QoS metrics.

6. **Develop a Hybrid Deep Learning Model for Blackhole Node Detection**

   Propose a novel hybrid deep learning architecture to identify blackhole nodes and optimize video packet routing in MANET environments, enhancing reliability and security.

7. **Implement Trust-Based Routing for Enhanced Video Continuity**

   Utilize a trust-based routing mechanism to minimize transmission errors and improve PDR, ensuring the continuity of video streams in highly dynamic MANET environments.

8. **Integrate Blockchain with an Optimized Consensus Mechanism**

   Employ blockchain technology with an enhanced consensus algorithm to securely validate and store MANET data, increasing overall security and data integrity.

9. **Comprehensive Protocol Testing and Comparative Analysis**

   Test the proposed protocol across various network parameters and compare its performance with established routing protocols such as SRABC, DSR, AODV, SETORD, HEDAR, DSDV, and OLSR. The comparison will focus on metrics like PDR, latency, throughput, and security.

1.6 Dissertation Contributions

This dissertation presents a significant advancement in the field of Mobile Ad Hoc Networks (MANETs) by proposing a novel routing protocol optimized for video streaming, incorporating cutting-edge deep learning and blockchain technologies. The contributions of this research are detailed as follows:

1. **Development of a Novel Enhanced OLSR (E-OLSR) Protocol**

   This work introduces a scalable, energy-efficient, and reliable Enhanced Optimized Link State Routing (E-OLSR) protocol. The protocol is specifically designed for video streaming in Wireless Multimedia Sensor Networks (WMSNs) and optimizes key Quality of Service (QoS) parameters such as energy consumption, packet delivery ratio (PDR), throughput, and end-to-end (E2E) delay.

2. **Integration of Blockchain for Enhanced Security**

   A key contribution is the integration of blockchain technology to

secure routing decisions within MANETs. The blockchain provides decentralized and tamper-resistant data storage, ensuring enhanced security in data transmission. This system is further validated using an optimized consensus mechanism to safeguard MANET data integrity.

3. **Introduction of a Hybrid Deep Learning Model for Blackhole Detection**

   A novel hybrid deep learning architecture is developed to identify blackhole nodes, which are notorious for disrupting data transmission in MANETs. This model significantly improves the reliability and security of video packet routing by detecting and preventing attacks that compromise data flow.

4. **Implementation of a Trust-Based Routing Mechanism**

   To ensure the continuity of video streams and minimize transmission errors, the research incorporates a trust-based routing mechanism. This approach enhances the packet delivery ratio and ensures reliable data transmission in highly dynamic MANET environments, especially in scenarios with frequent node mobility.

5. **Comprehensive Performance Evaluation under Diverse Network Conditions**

   The E-OLSR protocol is rigorously tested using the NS3 simulator under various network conditions, including different network sizes, node mobility levels, and traffic loads. The analysis provides detailed insights into the protocol's performance across a range of real-world scenarios, demonstrating its adaptability and robustness.

6. **Comparative Analysis with Existing Routing Protocols**

   The research performs a thorough comparative analysis of the proposed protocol against well-established protocols such as SRABC, DSR, AODV, SETORD, HEDAR, DSDV, and OLSR. The comparison focuses on critical performance metrics, including packet delivery

ratio, latency, throughput, energy efficiency, and security, highlighting the superiority of the proposed protocol.

7. **Novel Approach to Blockchain Scalability in MANETs**

   A significant challenge addressed in this work is blockchain scalability within MANETs, particularly in environments with high node mobility. This dissertation offers an innovative solution that allows blockchain operations to remain effective despite frequent node movements, ensuring the timely creation and validation of blocks.

1.7 Dissertation Structure

The particulars of the dissertation have been organized into five chapters. Contents of all the five chapters are given as follows.

Chapter 1 gives a detailed introduction to routing methods in MANETs emphasizing particulars like Blockchain, Video transmission over MANETs, Video transmission using OLSR Routing protocol, using blockchain with MANETs.

Chapter 2 discusses the theoretical background of the study emphasizing the significant particulars like Applications of MANETs, Types of MANET routing protocols, Evaluation of Video transmission over MANET, Video Transmission schemes over MANETs, Deep Learning-based models, Optimization methods, Blockchain, Security attacks in MANETs and Simulation Tools.

Chapter 3 lists the features and operational methodology of the proposed modules. In this chapter, the PDR, throughput, packet average end delay (AED), dropped packets (DP), E2E delay, and routing overhead (ROH) have been estimated in terms of the performance analysis of the proposed blockchain-based routing protocol. The effectiveness of the proposed OLSR

protocol has been evaluated in terms of QoS metrics, including PDR, energy consumption, E2E delay, and throughput.

Chapter 4 provides more details on the simulation results and discussions. It was found that the presented OLSR protocol performed better overall than other traditional protocols, and the addition of blockchain technology improved its security. Additionally, the suggested blockchain-based routing method, which makes use of Python, was evaluated using data collected from a variety of mobile simulator models in conjunction with the NS3 simulator.

Chapter 5 concludes the research investigations with their novel concepts implemented and also induces some valuable ideas for future efforts in the analogous vicinity of research.

Chapter Two

Theoretical Background

Chapter 2: Theoretical Background

1.1 Introduction

Wireless Multimedia Sensor Networks (WMSNs) is the integration of Wireless sensor networks (WSNs) and multimedia communication technologies. The main goal of these networks' architecture is to use a network of sensor nodes to gather and send multimedia data, such as audio and video [87,88]. Wide-ranging applications such as security, surveillance, healthcare, and environmental monitoring can benefit from the use of WMSNs. For instance, WMSNs are crucial in obtaining data on variables like temperature, humidity, and air quality in environmental monitoring applications. These networks provide vital sign gathering and patient monitoring in healthcare applications; in security applications, WMSNs are used for intrusion detection and surveillance. But WMSN deployment is fraught with difficulties, chiefly because of the large amounts of data that must be transferred and analysed [35, 36].

The fundamental characteristics of wireless transmissions present the revolutionary routing techniques in Bluetooth telecommunications with significant problems. Wireless broadcasts are vulnerable to various transmission faults resulting from multi-path fading, interference from nearby devices, and interruptions by other devices while operating in a shared transmission medium [36]. Resending data is frequently necessary to address these errors, which raises latency and negatively impacts multimodal transmission performance. Additionally, each cluster functions within a specific frequency range that is impacted by variables including temperature fluctuations, impediments in the signal path, transmitter type, antenna size, and power consumption. Because of these restricted ranges, data must pass through multiple intermediary networks before arriving at its intended location [37]. Every extra hop adds latency and raises the possibility of

network interference. The problem is made worse by the network's constantly shifting topology, which is caused by node mobility. The quality of continuous video feeds is impacted when routes malfunction since the search for new ones causes delays. Furthermore, bottleneck links may result from these topology modifications, limiting bandwidth. In severe situations, network partitioning happens, which interrupts multimedia streaming and breaks connectivity between several clusters[38,39].

2.2 Mobile Ad hoc Networks (MANETs)

When the need arises, MANETs are frequently utilized in real-world situations [40]. They have a specific characteristics and protocol stack properties.

2.2.1 Definition

MANETs are sometimes referred to as on demand systems as their connections are dynamically established and do not need any permanent setup. Since the wireless network has already been installed, no additional infrastructure is required. Since the MANET terminals are self-configured, an automated network between them is generated. Additionally, since each node is mobile, the arrangement of them is not static [41,42]. Nodes within a network have limited resources as they are being utilized irrespective of applications [43]. These are also being utilized for video streaming as a result of recent technological advancements and capacity increases. In the real-world setting, applications for video streaming are growing in popularity [44]. Users began utilizing cell phones along with additional portable gadgets all around the world and in all areas of living. In this case, video streaming is another usage for the MANET units. Nevertheless, there exist several problems with MANET-based video streaming [45].

The principal problem is the limited resources of the MANET systems [46]. It is challenging to utilize video streaming due to limitations in resources. Therefore, it is now crucial to research modifying the Open systems interconnection (OSI) model's layering to include video streaming. The model used for reference has many levels, such as the data link and physical layers [47]. Video quality while streaming may be increased by making enhancements to the aforementioned layers [48]. A number of investigators made contributions in this direction.

2.2.2 Characteristics

The adoption of MANETs has summarily developed recently due to their easiness in setup, cost-effectiveness, and user-friendly features. MANETs could be deployed without any infrastructure and can be implemented instantly in different situations, including emergencies like floods, earthquakes, and battles. These networks possess self-configuration capabilities, self-organization abilities, as well as operate without any fixed infrastructure. MANETs function in a multi-hop fashion, enabling mobile nodes not only to send their personal packets but also to forward packets to other mobile nodes [50]. Likewise, the prominence of internet-based video streaming has developed recently, incorporating various applications such as High-Definition TV content (HDTC), mobile TV, video chats on mobile devices, and surveillance systems [51].

High bandwidth demands and strict delay limitations go hand in hand with video streaming since rapid delivery of packets is necessary to ensure uninterrupted multimedia transmissions. The image resolution deteriorates if packets are dropped or arrive slowly because decoding problems often spread to other parts of the stream. Owing to video's enormous bit rate demands, a multimedia stream can trigger major congestion in the network [52]. Therefore, it is critical to consider the prospective influence of every single

video user on the network's characteristics and ensure the underlying network does not consume more resources than it can handle.

However, many network architectures lack the processes necessary for the protocol layers to adjust appropriately to bottom channel situations and particular requirements of applications [53]. Although protocol layering is a useful concept for simplifying network architecture, its use in wireless systems is limited by the inability to easily separate the levels due to the features of the medium of wireless communication [54].

2.3 MANETs' Protocol Stack

The protocol stack supporting MANETs is explained in this section. This provides a comprehensive summary of MANETs and aids in their comprehension [55]. The five different tiers of the protocol stack are represented in Figure 2.1 and are the physical, datalink, network, transport, and application layers. It is comparable to the set of TCP/IP technologies. The OSI levels for session, presentation, and application have been combined under one part, the application layer, as may be observed.

The OSI model is displayed on the left side of Figure 2.2. It is a tiered structure that facilitates interaction between all kinds of hardware and software while designing networked systems.

Middleware and Application Layer
Video Transmtion /Streaming
Transport Layer
UDP TCP
Network Layer
IP Routing (AODV, DSR, OLSR, E-OLSR)
MAC Layer
IEEE 802.11/g
Physical Layer
OFDM, Bluetooth, MIMO, Zigbee, Energy Management

Figure 2.1. OSI model

The TCP/IP suite is shown in the centre of Figure 2.2. The TCP/IP suite's layers are not precisely comparable to the OSI layers due to the fact it was created prior to the OSI model. The TCP/IP suite's fifth tier, known as the application layer, is comparable to the OSI model's integrated session, presentation, and application levels. The bottom four layers of the stack are indistinguishable [56].

The MANET protocol stack, which essentially resembles the TCP/IP suite, is displayed on the right. The network layer is where both of these protocol stacks diverge most. Ad hoc routing is the method used by mobile nodes, serving as hosts as well as routers, for routing messages. Mobile nodes operate standards created for channels of wireless communication at the physical and data link layers. The European Telecommunications Standards Institute (ETSI) specification for a high-performance wireless LAN, HIPERLAN 2, the IEEE standard for wireless LANs IEEE 802.11, and lastly the commercial strategy for wireless personal area networks at a shorter range, Bluetooth, represents a few alternatives. The standard IEEE 802.11 is

employed in each of these layers of the modelling tool used for this investigation. Figure 2.2 illustrates the three models of routing protocols.

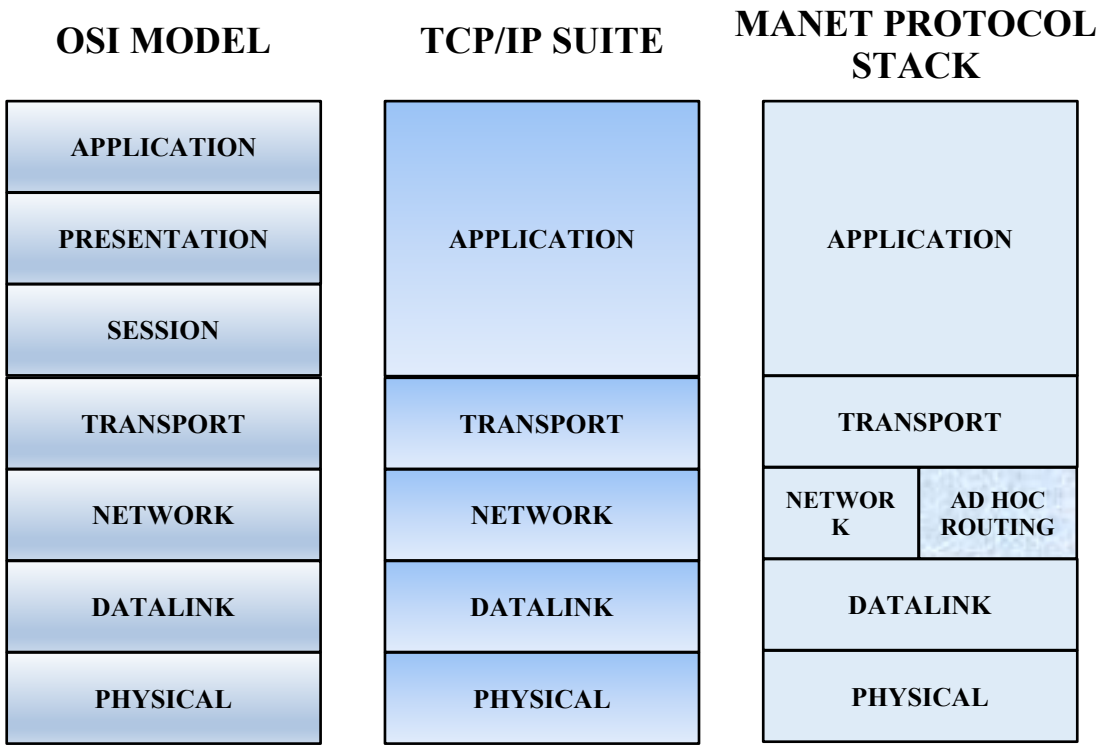


Figure 2.2. Illustration of the Three models

Network and Ad Hoc Routing are the two components that make up the network layer. Internet Protocol (IP) is the standard utilized in the network component, and Dynamic Source Routing (DSR) or Destination Sequenced Distance Vector (DSDV) constitute the methods that may be utilized in the ad hoc routing section [57].

2.4 Types of MANET routing protocols

MANETs have many routing protocols techniques can applied for video transmitted such as proactive and reactive routing protocols.

2.4.1 Routing Protocols for On-demand Video Streaming in MANETs

Before discussing multipath routing procedures for on-demand video streaming in MANETs, this section briefly presents the basics of existing

routing procedures which use only one path from source to DNs. In fact, the multipath routing procedures are the extended versions of unipath routing procedures used in the MANETs [58].

2.4.1.1 Proactive and Reactive Routing Protocols

A path is started via routing protocols from the SN to the DN. for transmitting the data between them. The routing procedures utilized in wired networks may not be optimal for MANETs because of asymmetric links and a high probability of link failures. When two nodes are in the connectivity range among them, they can communicate together [59]. Otherwise, the intermediary nodes function as routers to transfer the packets between sender and receiver. In other words, the MANETs support multi hop routing between the nodes. All the nodes in the MANET function as a router and a host depending on the context. Developing an effective routing procedure for MANETs is a challenging research problem because of their unique properties. Numerous researchers gave different classifications of routing protocols in MANETs [60]. Figure 2.3 indicates the taxonomy of MANET Routing Protocols.

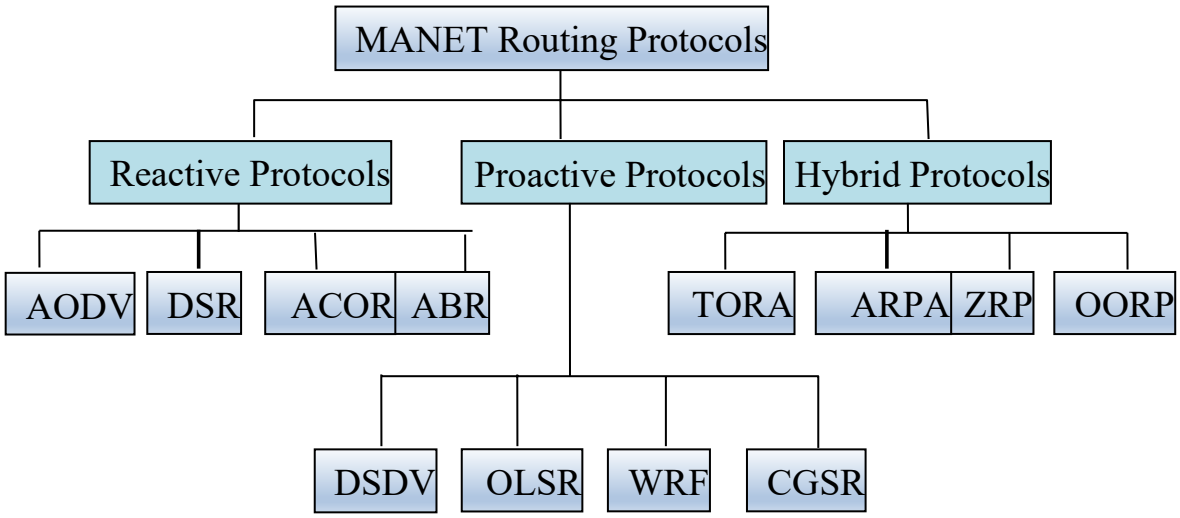


Figure 2.3. Taxonomy of MANET Routing Protocols

One important classification is based on the criteria of how routes are discovered and maintained in the MANETs. Literally, all the routing procedures of MANETs may be categorized into three foremost groups: proactive, reactive as well as hybrid routing protocols as displayed in Figure 2.3 [61-63].

In a proactive or table-driven routing process, all the nodes in MANET maintain a routing table that contains complete topology information. A route is established and maintained among every pair of nodes in MANET. Overhead is involved in maintaining the routes even though there is no data transmission between the nodes. Another drawback lies with the exchange of complete or partial routing table information periodically or when the topology change occurs in the MANET [42]. In contrast, the reactive or on-demand routing procedures establish the route among a pair of nodes only when there is data transmission between them, and the path is maintained till the end of data transfer. The route disappears, once the data transfer is finalized between the nodes [64]. The overhead of route maintenance as discussed in proactive routing is not present with reactive routing because the routes are generated and managed whenever required [65].

Finally, the hybrid routing process is a combination of both proactive and reactive routing processes. The advantages of both proactive and reactive routing procedures are merged together to form hybrid routing protocols. There are various proactive routing procedures such as DSDV, OLSR, TBRPF, etc. Examples of reactive routing procedures are AODV, DSR, etc. The best example of a hybrid routing protocol is the Zone Routing Protocol (ZRP) [66].

2.4.1.2 Reactive Routing Protocols

As the nodes in the MANETs are resource-constrained like having restricted processing power, minimum memory capability, low battery power, etc., numerous existing studies consider the on-demand routing approach for the on-demand video streaming in MANETs. The proactive routing protocols are not considered often by researchers because they consume more bandwidth for periodical updates of routing table exchanges and maintenance of unnecessary routes in the MANETs. Alternatively, reactive routing procedures establish the paths among communicating nodes only and these routes are maintained as long as there is data transmission. Also, reactive routing protocols save bandwidth and battery power of the MANET nodes.

2.4.1.2.1 Categories of Reactive Routing Protocols in MANETs

Since the reactive routing procedures discover the paths only when they are needed, the protocols use the request-reply method to find the routes between the communicating pair of nodes. The reactive routing procedures vary in the manner they find and maintain the paths. Several researchers proposed different categories of reactive routing procedures for the MANETs. All these reactive routing procedures can be grouped under two groups: source and hop-by-hop routing protocols.

In the source routing protocol, the SN initiates the path discovery procedure and it transmits a small control packet consisting of the DN's address. The control packet is transmitted by the intermediary nodes and lastly reaches the DNs. Then the reply is given back to the SN from the DN. During the path discovery process, all the nodes in the route add their own address to the control packet so that the SN knows the correct path to the DN. The SN then adds the complete path in the header of the data packet and transmits it. Each intermediary node in the route relays the packet based on

the path defined in the header. The best category of source routing procedure is the DSR protocol [67].

In DSR protocol, the SN transmits a route request (RREQ) packet and then it is routed by intermediary nodes till it touches the DN. The DN then gives a route reply (RREP) packet in the opposite path. The DSR procedure also permits the intermediate nodes to give a PREP to the SN if they know the route to the final node. The SN on receipt of the first RREP packet, starts the data transfer. All the data packets carry the correct path through which it is transmitted. During data transmission, if a link or node fails in the route, the intermediary node transmits a route error (RERR) packet to the SN thereby it may reinitiate the path discovery process to discover an alternate path to the final node.

In contrast, hop-by-hop routing procedures do not insert the complete path in the data packet's header. Instead, they store the address of the subsequent hop node on the rout to the DN. The hop-by-hop routing protocols make use of the request-reply method to determine the paths between source and DNs. The best example of a hop-by-hop routing procedure is the AODV routing method. In the case of AODV, the SN issues an RERR packet and it is forwarded by the intermediate nodes towards the DN [68].

The RREP packet is transmitted by the DN in response to RREQ. The SN on receipt of the first RREP, initiates the information transfer. During the route discovery process, each node in the path holds the addresses of the subsequent hops along the destination [69]. The SN transfers the data packet to the next hop node in the path, the node routes the packet to the subsequent hop, and so on till the packets reach the destination.

When a failure of node or link occurs during the data transfer process, the intermediary nodes report the errors with the RERR packets to the SNs. In

order to find a different way to go to the DN, the SN then restarts the path discovery process [70].

2.4.1.2.2 Hop-by-hop Reactive Routing Protocols

Different kinds of reactive routing protocols suggested in the literature of MANETs. Since DSR and AODV are the most popular protocols they are mentioned and briefly described in the prior section.

Hop-by-hop routing procedures are more flexible and adaptable compared to source routing procedures [69]. During data transmission, if a node displaces from the path, it must be informed to the SN in the case of the source routing approach because the SN sends all the data packets with the complete route [71].

The SN has to select a new alternate route to the target and new route information is added to the data packet. But in the case of the hop-by-hop routing method, the intermediary node does not inform the SN about a node displacement, instead, it transfers the packet to the subsequent fresh hop node to arrive at the DN. Note that in source routing, the route changes are updated by the SN only, but in hop-by-hop routing, the intermediary nodes are allowed to change the route dynamically as per the network changes [72].

Clearly, hop-by-hop routing protocols are more adaptable to the dynamic conditions of MANET compared to source routing protocols. Moreover, many research studies recommended preferring AODV to DSR for real-time traffic in the MANETs. AODV protocol is more stable, scalable, adaptable and flexible protocol compared to DSR protocol [34]. Many research works consider the reactive routing protocol AODV for video streaming in MANETs [72]. Table 2.1 summarizes the comparison between different MANET routing protocols.

Table 2.1: Different MANETs routing approaches Comparison

Protocol name	Route nature	Routes no.	Information stored	Period of updating	Update Information
Reactive Flat Routing Topology					
AODV	Broadcast QUERY	Multiple	Next hops to Dest.	Event driven RM	Route Error
TORA			height of neighbour's nodes	Event Driven	Nodes height
DSR			Route to Dest.	Event driven RM	Route Error
Proactive Flat routing Topology					
OLSR	Distributed	Multiple MPR flooding	MPR node, L.L., bandwidth	Periodical	(Hello&T.C.) messages
DSDV		Single	D. V.	Hybrid	D.V.
WRP			Dist. Routing cost table, MRL	Periodical	L.S. of all nodes
GSR		Single or Multiple	Topology	Periodical	L.S. of all nodes
Hybrid Flat routing					
ZRP	Proactive &Reactive (intra)	Single or Multiple	Local topology	Periodical	All state of node in the zone
ZHLS	Hierarchy Proactive/Reactive	Multiple	Local zone topology		Node/zone, Link state
Hierarchical Topology protocols					
CSGR	Hier. Cluster Proactive Distributed	Single	Table of Cluster Member, D. V.	Periodical	D.V., table of Cluster. Member.
LANMAR	Hier. Core node	Single or Multiple	nodes topology, D. V. Of L. M. nodes		Address of next hop Sender's Landmark Distance Vector
CEDAR	Proactive Core Broadcast QUERY	Single	Core/other nodes Global/Local		Dynamic/stable L. S.
Geographic Routing Protocols					
GPSR	Geo. greedy forwarding	Single	Greedy provides all nodes with their neighbour's position	Periodic update	Perimeter broadcast Mac address & IP Pos.
LAR	Geographic-reactive	Multiple	Dest. Loc., dist. to the zone		Expected zone of Dest.

2.5 Evaluation of Video transmission over MANET

The efficiency of the suggested approaches in this research has been evaluated in relation to QoS parameters, including as throughput, energy efficiency, Packet Delivery Ratio (PDR), and End-to-End (E2E) delay, Jitter, Network congestion, Routing overhead (ROH), Average end delay (AED), and Dropped packet (DP) [70-76].

2.5.1 Packet Delivery Ratio

Video packets that are dropped during transit to their destination are referred to as packet loss. To assess the performance of the network and take the required actions to guarantee successful data transfer, measuring packet loss is helpful. Packet loss is the term used to describe when a data packet leaves a certain site in a network without incident, but encounters a problem during data transit and is unable to reach its intended destination. The PDR is the ratio of packets distributed by the DN to packets broadcast by the SN.

As a result, PDR is among the most essential measures for evaluating how well video packet routing methods work. Equation 2.1 [77] shall be used to express the PDR (in percentage terms).

$$PDR = \frac{Received\ packets\ at\ destination}{Packets\ send\ by\ source} * 100\% \quad (2.1)$$

2.5.2 End-to-End (E2E) Delay or Latency

Latency, which is measured in milliseconds (ms) and indicates how long it takes for information to move from a source to a destination, is a key factor in determining how responsive and swiftly various networks and infrastructures are. E2E delay, often known as latency, is the amount of time it takes for a video packet to transit from SN to DN. The main criterion for assessing the video routing algorithm's efficacy is latency, as it directly

affects the quality of service (QoS) of WMSNs. Typically, E2E latency could be written using Equation 2.2.

$$E2E\ latency = T\frac{L}{R} \quad (ms) \tag{2.2}$$

Here, T represents processing time, L represents the length of time, and R represents the total ratio.

2.5.3 Throughput

In wireless networks, transmission speed is the rate at which data effectively travels from one place to another during a predefined period of time. Throughput provides information on the efficient procedure for transmitting and receiving packets. It is often stated in bits per second (bit/s or bps). Therefore, throughput is the duration of time required for the last packet to reach at its destination, and it can be written using Equation 2.3 [77].

$$Throughput = \frac{Data_{total}}{Time_{total}} \tag{2.3}$$

where $Data_{total}$ reflects the total number of data received or sent at the destination, and $Time_{total}$ is equivalent to the overall duration required for the transmission or reception of data.

2.5.4 Energy Efficiency

Energy efficiency is measured by the amount of data transferred per unit of energy used. It was believed that energy efficiency has a direct impact on the network's lifetime and is a crucial metric for assessing how well routing algorithms work in terms of energy consumption. This parameter can be expressed using Equation 2.4 [78] and is measured in joules (J).

$$Energy_{efficiency} = \frac{Tranfered\ data\ amount}{Consumed\ Energy} \quad (2.4)$$

2.5.5 Routing overhead (ROH)

The volume of routing control packets that are transferred across each node is known as the ROH. This measure reveals the transmission protocol's efficiency. It is predicted that proactive strategies would send more control packets compared to those that are reactive. The protocol is less successful the more control packets there are in it. ROH is expressed as a percentage (%). Equation 2.5 controls the total number of packets received from the DN, and the packets sent by each node are represented by the ROH [13].

$$ROH = \frac{total\ \ amount\ \ of\ packets\ send}{total\ amount\ of\ \ packets\ received} \quad (2.5)$$

2.5.6 Average end delay (AED)

The AED is measured in seconds (s). Equation 2.6 [13] is used to compute the total amount of time that packets take to travel between two nodes. This is how it is expressed.

$$AED = \sum_{i=0}^{n} \frac{(T_R - T_S)}{total\ amount\ of\ \ packets} \quad (2.6)$$

where T_R signifies the total time, the packet is received, T_S signifies the total time the packet is sent.

2.5.7 Dropped packet (DP)

Packet loss is computed using Equation 2.7, which compares the fraction of lost packets to transmit packets [79]. The percentage (%) represents the DP's unit.

$$DP = \frac{total\ of\ packet\ sent - total\ of\ packet\ received}{total\ of\ packet\ sent} \quad (2.7)$$

2.5.8 Jitter (J)

Jitter is a term commonly used to describe the variations in packet latency across a network over time. A network with constant latency exhibits no fluctuation (or jitter). Packet jitter is calculated as the average departure from the network's mean delay [80].

$$\boldsymbol{J = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(D_i - \bar{D})^2}} \quad (2.8)$$

Here,

N - Total number of measured packets

$\boldsymbol{D_i}$ – Delay of the i^{th} packet

$\boldsymbol{\bar{D}}$- Average delay of all the measured packets

2.6 Video Transmission schemes over MANETs

Numerous issues hinder MANETs, including inferior energy consumption, node congestion, and poor QoS. The constantly changing behavior of mobile nodes is a contributing factor to the aforementioned issues [81].

The guaranteed delivery of information from the SN to the DN within the designated transmission slot is the metric used for assessing the QoS. Pre-established assessment measures, including packet loss, transmission delay, as well as jitter, are used to analyze the results. The major objective aimed to improve efficiency, which may be attained by adhering to the specifications of pre-established assessment measures while sending information obtained from the SN to the DN. MANETs initially found use in disaster relief and the

armed forces. Due to their unique capabilities, MANETs are becoming increasingly practical to use for a variety of applications. The distributed mechanism, decentralized architecture, flexible network structure, and compact terminals are some of these characteristics. As a result, there are several problems with safety, reliability, as well as energy use that arise when developing and deploying MANETs. As a result, MANET QoS management remains an extremely difficult operation. Recently, several methods were proposed to improve QoS support as well as efficiency in MANETs [80].

A QoS aware and admission control procedures have been implemented to deliver better QoS. Hanzo & Tafazolli [82] addressed the problems of Quality-of-Service in MANET by solving the problem of degraded QoS achievement resulting from inadequate node-coordination, undependable network type, channel contention, etc. Because MANETs are flexible in nature, designing an effective design and protocol stack is a difficult undertaking. The problem of routing algorithms in MANETs, which can be utilized to offer various paths for interactions between nodes, has become the subject of numerous publications. Among the most potential algorithms for routing for MANETs are DSR, Temporally Ordered Routing Protocol (TORA), and AODV protocol.

2.6.1 Optimized Link State Routing (OLSR) Protocol

Multipoint relaying is an effective link state packet forwarding technique used by the proactive OLSR algorithm [83]. The original link state routing method is optimized by this method. Lowering the length of the control packets as well as decreasing the quantity of links that are utilized for transmitting the link state packets are the two techniques by which optimizations are carried out. By designating merely, a portion of the links in the link state changes, the overall size of the link state packets is reduced. Multi-point relays are a collection of connections or neighbors that have been

given the task of transferring packets and have been assigned for link state changes. Periodic connection state notifications are made possible by the optimization achieved through the usage of multipoint relaying. Figure 2.4 show the structure of standard OLSR protocol, if a link gets added or breaks down, the link state update mechanism fails to transmit another control packet. In extremely congested systems, the link state update optimization operates more efficiently.

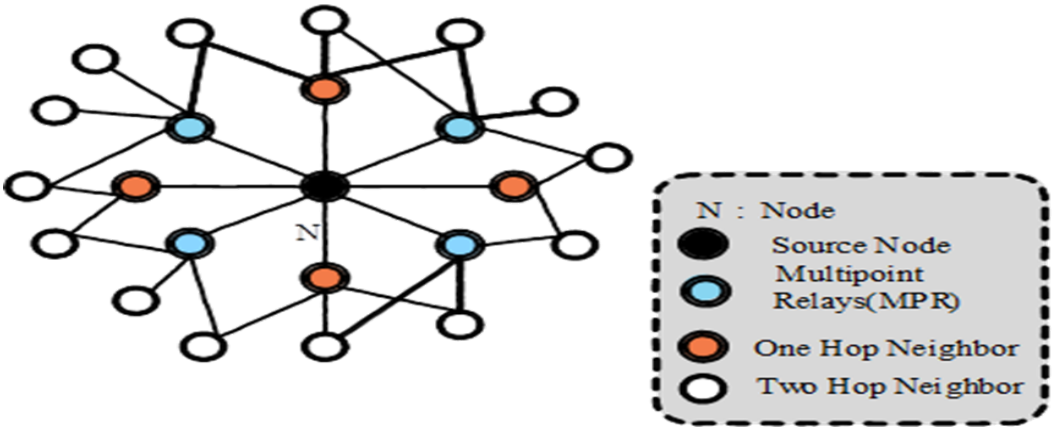


Figure 2.4. Structure of OLSR

The measure of message transfers needed when using the standard flooding-based strategy is displayed in Figure 2.4. In this instance, the volume of message transfers and the overall amount of network nodes are roughly identical. MPRset is the name given to the collection of nodes that constitute multipoint relays. Each of the nodes in the network chooses an MPRset to handle and transmit any link state packet that comes from that node. The link state packets produced by node P are processed by the neighboring nodes that are not part of the MPRset; they are not forwarded. Comparably, every node keeps track of a portion of neighbors known as MPR selectors, and these are simply the collection of neighbors that decided on the node to function as a multi-point relay. Packets that arrive from nodes within its MPR Selector set are forwarded by the node. As time goes on, both MPRset and MPR Selectors' memberships fluctuate. Any other node in a node's two-hop neighborhood

maintains a bidirectional link to the node because of the selection of the node's MPRset participants [59]. Figure 2.5 showes the example of MPRs selection in OLSR protocol.

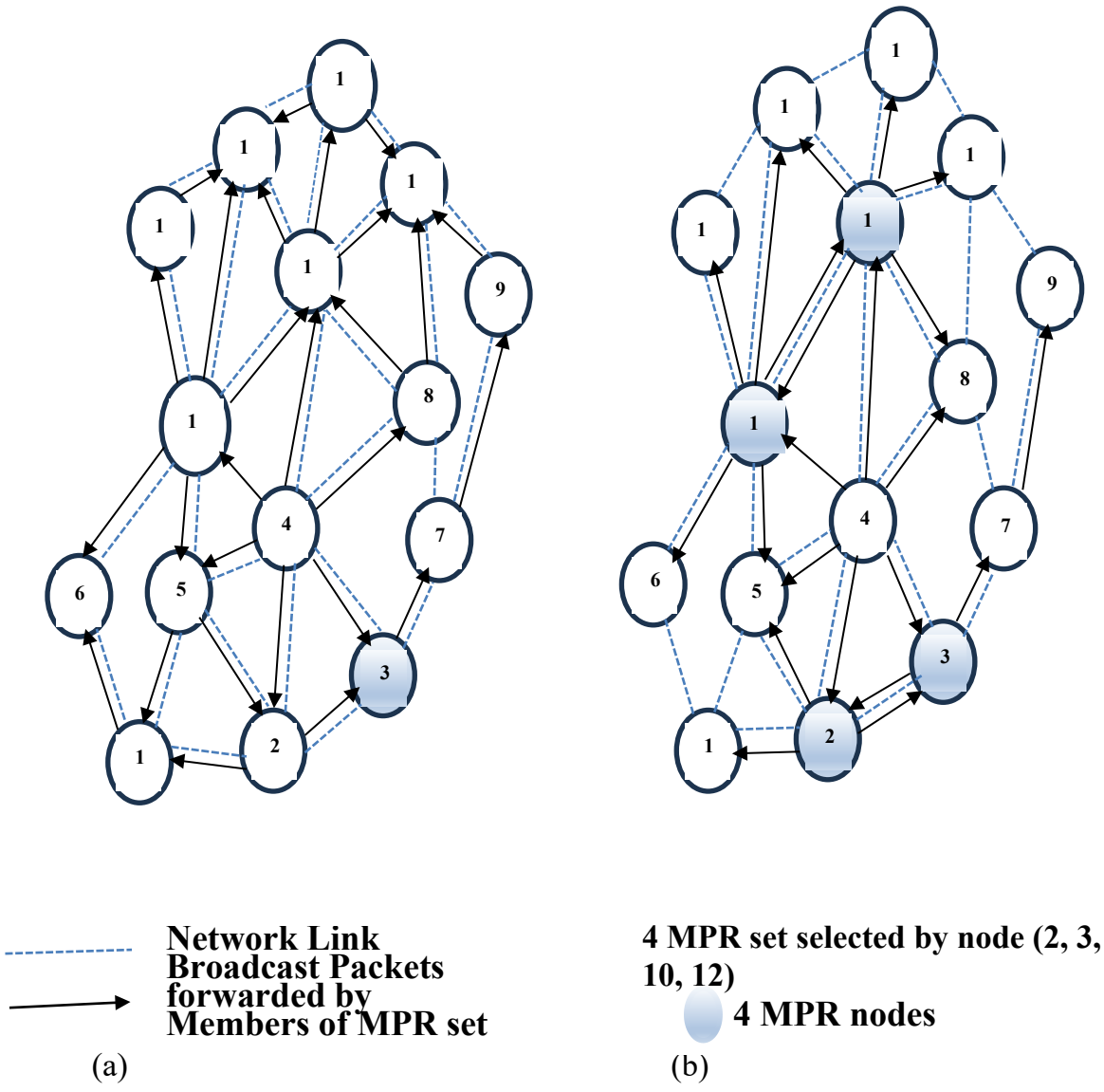


Figure 2.5. Showes the Example of MPRs selection in OLSR protocol:

(a) Flooding the network takes as many transmissions as the node counts

(b) Flooding the entire network with six transmissions using the MPR scheme

Since a node determines paths to every destination exclusively by means of the participants of its MPRset, the choice of nodes that compose its MPRset

has a considerable impact on the efficiency of OLSR. On a regular basis, each node transmits its MPRSelector set to other nodes within the near vicinity. A node frequently transmits Hello messages containing an index of neighbors with which it currently has bidirectional links as well as a record of neighbors about which it recently exchanged messages however still does not have bidirectional links for the purpose of determining the nodes that should be included in the MPRset. Upon receiving this Hello packet, the nodes make updates to their individual two-hop topology records. The Hello packet additionally shows which multipoint relays have been selected. The collection of neighbors, two-hop neighbors, and neighbor node statuses are all stored in an informational structure known as the neighboring table. Any of the three potential link status states bidirectional, multipoint relay, or unidirectional can apply to the neighboring nodes. Every entry contains a value for the timeout that, when it expires, removes the table record to attempt to eliminate outdated items from the neighbor table. In an identical way, each fresh MPRset increments the sequence number that is associated with it [84].

The MPRset does not have to be ideal; in fact, it could have the same configuration as the neighbor set when the connection is first configured. In comparison to link state routing, protocol effectiveness improves with fewer nodes in the MPRset. Each node regularly generates topological control (TC) packets and is used for updating the routing table with topological information. Utilizing the multipoint relaying process, such TC packets are sent across the network and include the MPRSelector set of each node. Each node in the network obtains many of these TC packets from various nodes; the topology table is constructed utilizing the data found in the TC packets [85].

If the MPR Selector set is altered following an earlier transmission and a minimum amount of duration has passed since then, a node could send a TC

message before its usual timeframe. A DN, that is the MPR Selector, as well as a last-hop node, implying the node that sends the TC packet, are included in a record in the topology table [86]. As a result, the routing database keeps track of paths for any additional network node.

2.6.2 Coding techniques

Unipath routing in MANETs is shown in Figure 2.6 in which there are three paths: P1 (S, R1, R2, R3, D), P2 (S, R4, R5, R6, D) and P3 (S, R7, R8, R9, D), available between nodes from source S and destination D through intermediate routers R1, R2,... R9. Though multiple paths are available, the data transmission uses only one path P1 (S, R1, R2, R3, D) between source S and destination D.

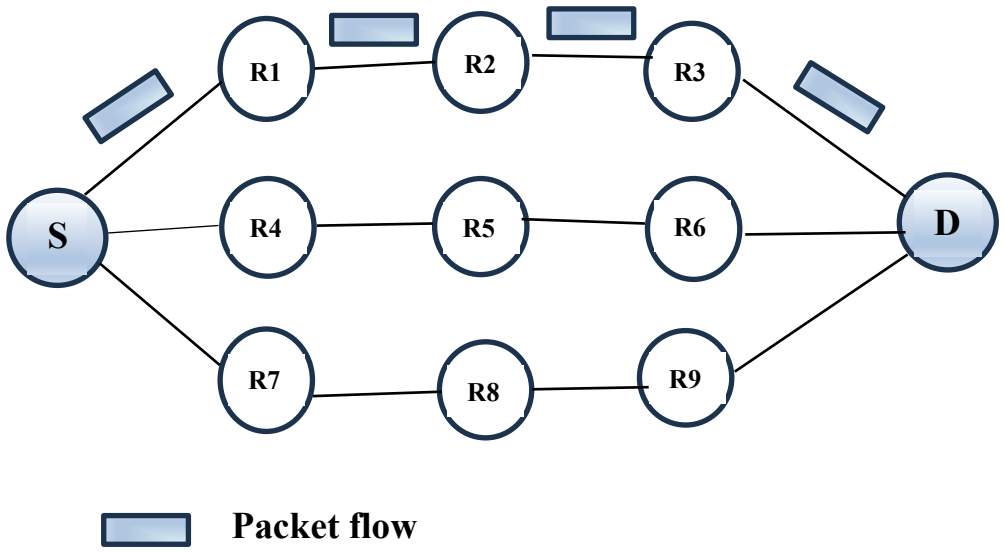


Figure 2.6. Unipath Routing in MANETs

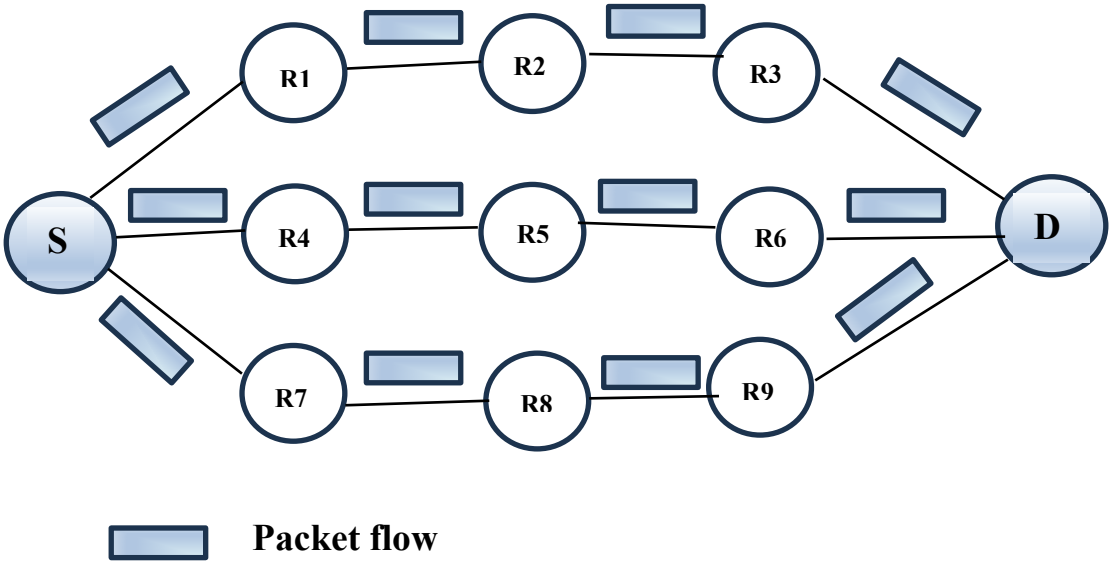


Figure 2.7. Multipath Routing in MANETs

When failure happens in the path P1 (S, R1, R2, R3, D), the data transmission cannot proceed further. In order to resume the data transmission, the route P1 (S, R1, R2, R3, D) must be repaired or an alternate path P2 (S, R4, R5, R6, D) / P3 (S, R7, R8, R9, D) must be selected. It takes time to repair the existing route or to discover an alternate route from source S to destination D. Clearly, delay-sensitive applications like on-demand video streaming cannot get the required quality of service in the MANET with unipath routing protocol. This even gets worse with the MANET because of their highly dynamic nature [86].

Alternatively, multipath routing procedures establish numerous routes from the source node to the destination node as depicted in Figure 2.7. The data transfer from the source node S to the destination node D happens simultaneously using three multiple paths P1 (S, R1, R2, R3, D), P2 (S, R4, R5, R6, D), and P3 (S, R7, R8, R9, D), Multipath routing provides reliable data transmission. If a path, say P1, fails due to node or link failure, the data transmission still proceeds through other paths P2 and P3.

Multipath routing balances the load at intermediate routers. Transmitting data through multiple paths simultaneously increases the throughput and performance of the application. On-demand video streaming applications must be serviced with minimum delay, higher throughput, and faster transmission. It can happen with multipath routing in MANETs[87].

2.7 Deep Learning-based models

Deep learning is a subfield of machine learning that uses multi-layered neural networks, or deep neural networks, to simulate the complex decision-making mechanisms seen in the human brain. In one way or another, deep learning powers the majority of artificial intelligence (AI) in modern life [81].

2.7.1 Convolutional neural network

A specific category of artificial neural network (ANN) utilized for the processing and recognition of images that are made especially to handle information from pixels is called a Convolutional Neural Network (CNN) [88]. CNNs are highly capable artificial intelligence (AI) and computational image processing devices that employ deep learning to accomplish simultaneously procedural as well as informative operations. They frequently employ machine vision, which involves the detection of images and videos, recommendation systems, and Natural Language Processing (NLP).

2.7.2 Recurrent neural network

The most common kind of ANN is termed a recurrent neural network (RNN) [89], in which the links among nodes create an ordered graph that follows a temporal pattern. It can now display temporally fluctuating behavior as a result. RNNs have the ability to deal with combinations of inputs using their inbuilt state, or memories, in contrast to neural networks with feedforward processing. They can therefore be used for applications like

speech identification or without segments, linked identification of handwriting.

2.7.3 Recursive neural network

Recursive neural networks (RvNNs) are a specific type of deep neural network that is constructed by iteratively repeating an identical collection of parameters across an organized input. This allows the network's neurons to traverse a particular structure in a logical sequence and provide linear predictions on it or a hierarchical prediction over variable-size input frameworks. In NLP, RNNs demonstrated effectiveness, for example, in learning sequence and tree structures, primarily sentence and phrase continuity descriptions that utilize word embedding. Initially, dispersed illustrations of a framework, like logical words, were imparted to RNNs [90].

2.7.4 Comparative assessment of four deep learning models-based intrusion detection system

There are several widely used CNN and RNN variations. The inception architecture CNN is suggested as a solution to the training difficulty that is effectively used in Google Net. Bi-directional long short-term memory (BLSTM), as well as Gated Recurrent Unit (GRU), are suggested employing gated methods to mitigate a number of the drawbacks of the standard RNN. The frameworks that are commonly employed for the experiments include basic CNN, the inception architecture CNN, BLSTM, and GRU [91].

2.7.5 Basic Convolutional Neural Network

Three components make up a basic CNN: the convolution layer, the pooling layer, and the fully linked layer. Putting it simply, the convolutional layer extracts specific features from the image; the pooling layer reduces the variable magnitude significantly (dimension lessening); and the fully

connected layer, which outputs the intended outcome, is comparable to the component of a conventional neural network [92].

2.7.6 Inception Architecture

In order to expedite CNN training and address the issue of an excessive number of variables, Laqtib et al. [93] used a CNN inception design, and this has been successfully implemented in Google Net, inception CNN consists of many layers, including the 1x1 Convolutional layer, 3x3, and 5x5, whose output filter banks are combined into one output vector that serves as the starting point for the subsequent stage.

2.7.7 Bi-Directional LSTM

In addition, Bi-Directional RNN is presented to address RNN's drawbacks. The entirety of the input data that has been and will be accessible for a given time period may be used to train this framework. Stated otherwise, the process involves arranging two RNNs so that the data sequence is fed into a single network in standard time order and the second network in backward time order. Every time-step, the results from the two systems are typically merged [94].

2.7.8 Gated recurrent

Another kind of RNN containing memory cells is called a Attention Based (GRU). They have a smaller cell design than LSTM, although their performance is comparable. Although it lacks a gate that outputs as well as contains fewer variables, GRU also uses a gated system to regulate data flow across cell states [95]. Table 2.2 represents the comparison of various deep learning models.

Table 2.2. Ccomparison of different deep learning models

S. No.	Deep learning method	Merits	Demerits
1	Convolutional neural network	Good accuracy, Used in many machine learning applications	Size of the network is large
2	Recurrent neural network	Provide better accuracy due to the ability of learning from past previous experience	Training the model is tough
3	Recursive neural network	Powerful learning technique in hierarchal applications	During the training, input sample tree structure must be known
4	Intrusion detection system	Detects malicious activity Used to identify the attack types and quantity	Full time monitoring is required. Expensive method compares with other techniques. Produce false positives and negatives.
5	Basic Convolutional Neural Network	Human supervision is not required Image recognition with high accuracy Large datasets can be easily handled	Challenges in interpretability Slower process compares with other techniques More time required for training
6	Inception Architecture	Performance gain is high Provide accurate result	Miss classification Required more computational resources
7	Bi-Directional LSTM	It provides additional training capability Prediction capability is more	Slower model, more time is required for training
8	Gated recurrent	Simple architecture, Computational time is less, faster training	More chances for overfitting

2.8 Optimization methods

Numerous MANET applications focus on the completion of processes in an optimist way, there are several soft computing methods used in MANET for optimization. Optimization focuses on reducing cost, and improving QoS in data and video data transmission, accordingly, the section below focuses on the different optimization techniques [96,97].

2.8.1 Osprey Optimization Algorithm (OOA)

The Osprey Optimisation Algorithm (OOA) is a novel metaheuristic algorithm that emulates the natural behaviour of ospreys. Osprey hunting tactics in the waters serve as the main source of inspiration for OOA. With this method of hunting, the osprey locates the prey, seeks it out, and then moves it to a good spot to eat. The projected OOA technique, which consists of two phases of exploration and exploitation, is statistically modelled using simulations of ospreys' natural hunting behavior [98,99].

Merging the global search phase with the concept of exploration, improves the system's ability to find the major appropriate region and steer clear of local optima. The search method from the local scale employing the chance of exploitation then boosts the approach's capability to arrive at likely superior possibilities in promising places. Here, the OOA uses equation (2.1) - (2.2) to identify the best course depending on criteria like both the node and the link stability levels.

$$C_{ij} = \lambda_1 LQ_{ij} + \lambda_2 X_{ij} + \lambda_3 S_{ij} \quad (2.1)$$

Here,$\boldsymbol{C_{ij}}$ indicates link stability from $\boldsymbol{i}$and$\boldsymbol{j}$, $\boldsymbol{X_{ij}}$ specifies safety degree, $\lambda_1, \lambda_2, \lambda_3$ denotes weighting vector, $\boldsymbol{LQ_{ij}}$denotes link quality, $\boldsymbol{S_{ij}}$ represents the factor for forecasting mobility.

$$V(Y) = \left(\sum_h \frac{Y_h^2}{n}\right) - \left(\sum_h \frac{Y_h}{n}\right)^2 \quad (2.2)$$

Where, $V(Y)$ denotes variance, h indicates the total number of nodes, Y_h denotes the message level attained from each adjacent node. The fitness value is calculated using the following equation (2.3),

$$fitnessvalue = max(\text{Node stability degree} + \text{Link stability degree}) \quad (2.3)$$

2.8.1.1 Initialization

In contrast to a replication-based method, the OOA outlines a population-based technique that makes use of the population's search capacity in the domain of problem-solving to find a workable solution. Each search agent, as an individual member of the OOA population, ascertains a variety of variables associated with their particular location across the search zone. As a result, each search agent represents a potential solution to the issue, statistically represented by a vector. Equation (2.4) gives the OOA populous, which is made up of all search agents. Equation (2.5) is utilised to initialise OOA at random searches agents' locations inside the search area.

$$p = \begin{bmatrix} p_1 \\ \vdots \\ p_2 \\ \vdots \\ p_n \end{bmatrix}_{N\times M} = \begin{bmatrix} p_{1,1} \cdots p_{1,j} \cdots p_{1,m} \\ \vdots \quad \ddots \quad \vdots \quad \iddots \quad \vdots \\ p_{i,1} \cdots p_{i,j} \cdots p_{i,m} \\ \vdots \quad \iddots \quad \vdots \quad \ddots \quad \vdots \\ p_{N,1} \cdots p_{N,j} \cdots p_{N,M} \end{bmatrix}_{N\times m} \quad (2.4)$$

$$p_{i,j} = lb_j + r_{ij}.\left(ub_j - lb_j\right),\ i = 1,2,....,N.\ \ j = 1,2,...,m. \quad (2.5)$$

Here, p denotes the position of the search agents', p_i indicates i^{th} the search agents, $p_{i,j}$ denotes j^{th} dimension, N denotes the total quantity of search agents, M represents the problem variable, r_{ij} represents the random

variable in the range between [0,1], lb_j indicates the lower bound, and ub_j represents the upper bound. The goal function can be expressed as a set of vectors using equation (2.6).

$$G = \begin{bmatrix} G_1 \\ \vdots \\ G_i \\ \vdots \\ G_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} G(P_1) \\ \vdots \\ G(P_i) \\ \vdots \\ G(P_N) \end{bmatrix}_{N\times 1} \quad (2.6)$$

Here G_i indicates the objective function of i^{th} search agents, G represents the choice of the objective function.

2.8.1.2 Exploration stage

The first stage of the OOA population update system is based on imitating the natural behavior of search agents. By examining capacity inside the search zone, the OOA makes it possible to pinpoint the optimal location without going through the local optimum. In relation to the entire search area, the positions of various search agents that yield a higher goal function score is considered suboptimal for every search agent. The set of features that each search agent collects is uniquely identified by equation (2.7).

$$GL_i = \{P_h | h \in \{1,2,..,N\} \wedge G_h < G_i\} \cup \{P_{best}\} \quad (2.7)$$

Where, GL_i indicates the feature positions of i^{th} search agents, P_{best}represents the finest search agents' locations. A simulation involving the approaching characteristic of the search agents finds the new roles of the related search representatives. Equation (2.8), which provides the numerical value of the goal function, is augmented by the new location of the search agent.

$$p_{i,j}^{L_i} = p_{i,j} + r_{i,j}.\left(SG_{i,j} - R_{i,j}.p_{i,j}\right) \quad (2.8)$$

$$p_{i,j}^{L_1} = \begin{cases} p_{i,j}^{L_1}, & lb_j \le p_{i,j}^{L_1} \le ub_j \\ lb_j, & p_{i,j}^{L_1} < ub_j \\ ub_j, p_{i,j}^{L_1} > ub_j. \end{cases} \tag{2.9}$$

$$P_i = \begin{cases} P_i^{L_1}, G_i^{L_1} < G_i; \\ P_i, else \end{cases} \tag{2.10}$$

Here $P_i^{L_1}$ represents the new position of i^{th} search agents in the preliminary point, $p_{i,j}^{L_1}$denotes j^{th}vector, $G_i^{L_1}$indicates the objective function rate, SG_irepresents an best feature of i^{th} search agents, $SG_{i,j}$denotes j^{th} vector, $R_{i,j}$ indicates the random variable in the range of [0,1].

3.6.2.3 Exploitation stage

The numerical modelling of the natural behaviors of search agents serves as the foundation for the second stage of the OOA population growth. Next, the simulation of shifting the parameter to the right spot modifies the position of the search agent. The search area improves the OOA exploitation potential of the local search area, resulting in better opportunities beyond the acknowledged methods through integration. In accordance with the OOA approach, each member of the group has a random placement for the absorbing feature chosen using equation (2.11).

$$p_{i,j}^{L_2} = p_{i,j} + \frac{lb_j + r.(ub_j - lb_j)}{t}, \; i = 1,2,...,m, \; k = 1,2,...,K \tag{2.11}$$

$$P_{i,j}^{L_2} = \begin{cases} p_{i,j}^{L_2}, lb_j \le p_{i,j}^{L_2} \le ub_j \\ ib_j, p_{i,j}^{L_2} < lb_j \\ ub_j, p_{i,j}^{L_2} < ub_j \end{cases} \tag{2.12}$$

subsequently applied to raise the score of the objective function in the current location, hence altering the associated search agent locations and enabling equation (2.13),

$$P_i = \begin{cases} P_i^{L_2}, G_i^{L_2} < G_i; \\ P_i, \ else \end{cases} \tag{2.13}$$

Here $P_i^{L_2}$ shows the second sage location of i^{th} search agents, $P_{i,j}^{L_2}$ indicates the j^{th} vector, $G_i^{L_2}$ represents the objective function value, random variable from the range between [0,1] is represented by $r_{i,j}$, Iteration area is indicated by k, and K is the number of iterations.

Algorithm 1: OOA

The problem details (objective function, constraints and variables)

Set the total amount of iterations K and the OOA size of the population N.

Create the initial distribution matrix utilizing equation (2.1) - (2.2).

Equation (2.3), assess the objective function.

$For\ k = 1 to\ K$

$For\ i = 1 to\ N$

Stage 1: Exploration

Adjust the feature locations of the i^{th} OOA individual utilizing equation (2.7).

$GL_i = \{P_h \mid h \in \{1,2,..,N\} \wedge G_h < G_i\} \cup \{P_{best}\}.$

The i^{th} search agents randomly choose the feature.

Utilizing equation (2.8), determine the new location of i^{th} OOA individual depending on the first stage of OOA.

$p_{i,j}^{L_i} = p_{i,j} + r_{i,j}.(SG_{i,j} - R_{i,j}.p_{i,j})$

Evaluate the boundary conditions of the new location of OOA Individuals utilizing equation (2.9),

$$p_{i,j}^{L_1} \leftarrow \begin{cases} p_{i,j}^{L_1}, \ lb_j \le p_{i,j}^{L_1} \le ub_j \\ lb_j, \ p_{i,j}^{L_1} < ub_j \\ ub_j, p_{i,j}^{L_1} > ub_j. \end{cases}$$

Utilizing equation (2.10), modify the i^{th} OOA individual.

$$P_i = \begin{cases} P_i^{L_1}, G_i^{L_1} < G_i; \\ P_i, \ else \end{cases}$$

Stage 2: Exploitation

Utilizing Equation (2.11) determine the new location of i^{th} OOA individual depending on the second stage of OOA.

$$p_{i,j}^{L_2} = p_{i,j} + \frac{lb_j + r.\left(ub_j - lb_j\right)}{t}$$

Evaluate the boundaries conditions of the new location of OOA individuals utilizing Equation (2.12),

$$P_{i,j}^{L_2} \leftarrow \begin{cases} p_{i,j}^{L_2}, lb_j \le p_{i,j}^{L_2} \le ub_j \\ ib_j, p_{i,j}^{L_2} < lb_j \\ ub_j, p_{i,j}^{L_2} < ub_j \end{cases}$$

Alter the i^{th} OOA individual utilizing equation (2.13),

$$P_i = \begin{cases} P_i^{L_2}, G_i^{L_2} < G_i; \\ P_i, \ else \end{cases}$$

End

Select the most suitable option

End OOA

2.9 Blockchain

Blockchain is a platform that facilitates transparent, safe, decentralized data storage and transmission. It functions as an extensive repository that maintains a record of every communication among participants from the time the blockchain was established [100]. The decentralized design of blockchain, meaning it is essentially maintained by a restricted number of individuals rather than an individual server, is one of its best features. Blockchain elements contain safety measures to safeguard the infrastructure and do not require a middleman to verify the authenticity of the chain and data [101].

Blocks are collections of network user communications. A "blockchain" is a hash chain that is ultimately formed by every single block holding the hash value of the previous block. A blockchain type-dependent set of parameters is used by a node in the network known as a "miner" to verify each of these blocks. The block joins the remainder of the blocks and gets added to the blockchain after it has been verified. The other party and the whole network can see activities [102]. Figure 2.8. explains the common structure of a blockchain.

Figure 2.8. Generic structure of a blockchain

Each participant of the system has a roughly equivalent rank and stores a replica of the blockchain. Blockchain is employed in many different application scenarios as well as is thought to be one of the most crucial approaches to speed up worldwide progress due to its exceptionally high level of safety and reliability [103]. Blockchain, the technology that is the basis of

the original cryptocurrency Bitcoin, is proposed to serve as a basis for the future expansion of the World Wide Web. Individuals within the network contest with one another to organize activities within the blockchain utilizing their computers and associated resources. The most successful participant in the competition receives currencies generated by the platform along with transaction costs [104]. This kind of recording is also known as mining. Due to the fairly spread nature of block extraction, that is carried out by peers referred to as miners an agreement process is necessary for determining whichever miner's transaction is going to be the next one to be included in the blockchain. In the Nakamoto agreement used by Bitcoin, the miner correctly packages the solution by presenting definitive evidence showing it has resolved a particular crypto-puzzle. This agreement is also known as Proof of Work (PoW) [105].

Blockchain 2.0 refers to blockchains that enable smart contracts to operate. An autonomous digital contract that operates in a secure environment without requiring outside assistance is known as a smart contract. During the past few years, the primary barrier to the implementation of smart contracts has come from the challenge of locating an encrypted, distributed environment [101]. But blockchain provides an answer to this issue. Conversely, the blockchain resolves the aforementioned issue.

Hyperledger, Ethereum, and Bitcoin are among the most popular uses of blockchain technology [103]. Of them, two serve as executable frameworks for smart contracts, while Bitcoin works as a distributed cryptocurrency in broad. Obtaining agreement from unreliable peers in an interconnected system is a challenging issue that affects the functioning of the blockchain.

When a number of mistrusting nodes come to an agreement on the final configuration of the information, this is known as consensus. To get a consensus, multiple techniques may be used. When multiple nodes are

participating in a distributed network and must come to an agreement upon just one value, it is far more challenging to reach consensus than it is if just multiple nodes participate (such as in client-server networks). The idea of reaching consensus across multiple nodes is known as distributed agreement [106].

A consensus method is a set of steps that almost all terminals perform to come to a consensus on some suggested variable or configuration. For almost thirty years, computer engineers in the corporate world and university have been researching this idea. Consensus methods have been gaining a lot of interest and acclaim, especially with the development of Bitcoin and blockchain. In the sections that follow, we provide the most popular consensus methods and look at their problems in the framework of MANETs [107].

2.9.1 Proof of Work (PoW)

Ethereum and Bitcoin, two well-known blockchain technologies, each employ the PoW consensus mechanism. PoW, the password-protected contents of a possible block's headers must be ascertained by every miner on the system and can vary under a preset range [108]. A node sends the data inside of the block to additional nodes after calculating the desired value in order to confirm that what was calculated is correct. Nodes with larger computational capacities are more likely to achieve their desired results quicker. If the most recent block that was created is capable of being validated, every single node in the network may choose to add it to its privately recorded blockchain.

PoW offers strong defense from intrusions. However, because of the fundamental causes, PoW and its various forms are not appropriate for mobile ad-hoc systems [109]. Because PoW-based consensus needs a lot of energy

to solve crypto problems, it was originally prohibitively costly for portable devices with restricted resources. Moreover, proof-of-work (PoW) involves estimating the entire network's total processing capacity, which is assessed individually by every node based on preceding blocks, to figure out the difficulties of calculating the subsequent block. However, nodes may leave a mobile ad hoc network for a variety of factors, including user mobility, power outages, and additional issues, and network outages could occur often. Conventional PoW-based consensuses in MANETs have dependability problems due to frequent alterations in the network connectivity [60].

2.9.2 Proof of Stake (PoS)

Proof of Stake (PoS) is based on the idea that individuals with larger sums of money or coins are less likely to attack the network's infrastructure [104]. Because of this, block-creators in PoS are selected depending on their balancing, which usually causes problems with the technique's fairness. Consequently, some enhancements (e.g. including randomness) were subsequently suggested. In extremely active MANETs and even in intermittently connected systems, it might be difficult to confirm the authenticity of the PoS at different nodes due to frequent divisions of networks and unreliable connectivity among nodes.

In addition, the imbalance problem can become worse in flexible MANETs. The framework's impartiality could be seriously jeopardized, for instance, if a few potential nodes control it only so that their payments are processed [110].

2.9.3 Practical Byzantine Fault Tolerance (PBFT)

Practical Byzantine Fault Tolerance (PBFT) is employed within the Linux Foundation's Hyperledger Fabric [111]. Each iteration of the latest block generation begins with the selection of a device for recording, whose

logging process is divided into 3 phases: pre-prepared, prepared, and committed. Over two-thirds of the network's nodes must agree on every one of the aforementioned stages. Moreover, a few PBFT variations were suggested. Nodes have to pledge certain amounts of Bitcoin in order to qualify as validators. The need for consent to be obtained by at least two-thirds of the nodes is a major barrier to the deployment of PBFT-based consensuses in MANETs and might cause scalability problems. Particularly, repeated partitioning of networks may result in over one-third of nodes becoming separate network elements in a mobile ad hoc network context, making PBFT useless [111-112].

2.9.4 Directed Acyclic Graph (DAG)

A newly developed category of ledger for recording actions that depend on the concept of a graph that is directed is referred to as a Directed acyclic graph (DAG). A DAG is the foundation of the blockchain Tangle. The tangle has no components. A fresh transaction adds a pair of edges to the graph once it enters the tangled network by choosing two previous requests for permission. The nodes don't need to reach a consensus on what permitted activities should be included in the ledger; in essence, all transactions may be included in the tangle. Conversely, nodes have the authority to determine which activities will remain unapproved by anybody. The Internet of Things (IoT) token IOTA, which aims to be the next version of the IoT blockchain, has Tangle as its core. It is still difficult to put in place a safe and fair payout system in DAG-based systems. In addition, the dynamic movement in and out of nodes within a MANET may affect the condition of transaction confirmation [113].

Table 2.3. Ccomparison of four consensus methods.

S. No.	Deep learning method	Merits	Demerits
1	Proof of Work	Accuracy and decentralization	Scalability is low and consumes more energy
2	Proof of Stake	Low-cost bribe attacks	Overall security reduction
3	Practical Byzantine Fault Tolerance	Energy usage is less, Environment friendly	Scalability and sybil attacks
4	Directed Acyclic Graph	Scalability, Confirmation time is faster, Transaction fees is reduced	More concurrent transactions, ledger data expansion

2.10 Interplanetary File System (IPFS)

Joan Bennett created the InterPlanetary File System (IPFS) in 2015, and Protocol Labs manages it. The IPFS is a peer-to-peer network that stores and shares data in a distributed file system. IPFS employs content-addressing, in which each file in an IPFS host's global namespace is uniquely identified. IPFS intends to build a single global network. This means that when both users broadcast a block of data with an identical hash, peers requesting content from one user will also trade data with those requesting it from the other [114].

2.11. Security attacks in MANETs

A multitude of severe problems arising from the constantly changing architecture, node movement, restricted processing power, constrained bandwidth capability, restricted battery power, and safety features of MANETs pose a danger regarding their survival and rate of acceptance. There are several issues regarding security. The largest is the absence of trust among nodes, which underlies the majority of additional safety issues, including MANET routing stability [115]. Consequently, implementing a strong trust

strategy will inevitably render the network safe. Finding the nodes that are acting improperly and do not merit the confidence of their fellow nodes is the difficult part of maintaining a stable and accessible system that performs as intended. By resolving this problem, all of the nodes that make up the network will behave properly and operate according to plan, which will improve the overall safety of the MANETs [116].

The primary issue with how packets is routed in MANETs is that uneven transmission of packets is often caused by the participant nodes' absence of reputation and confidence. Presently available mobile ad-hoc cloud trust management technologies are insufficient. This is because of increased network interactions, node confidentiality, and the difficulty in meeting a number of fundamental needs for maintaining a reliable system key handling and entity authorization, for instance with frequent partitioning of the network. Overall, well-being is thus hard to sustain [115-117].

"Trust" describes a node's capacity to offer additional nodes with data that they may utilize and rely on. Routing, identifying malicious nodes, time synchronizations, safety levels, reliability, and nodes' ability to perform a certain type of observing duty are only a few of the scenarios where trust is helpful. A node's behaviour or actions regarding its nearby nodes indicate how trustworthy it is[118]. A well-behaved component consistently performs honourably and sends the right information to its peers in order to fulfil its obligations. Trust may be quantified or modified by considering the assessments of its neighbouring nodes.

Several factors, including the operating system, energy restrictions, restricted computer capacity, and quick rapid alterations in the structure of the network, have to be brought into account in order to build confidence in MANET communications [119]. Several methods and architectures are being used to accomplish trust management in MANETs, namely trust building,

trust updating, and trustworthiness. As stated, certain researchers have set in place an authentication system to ensure that network connections are safe. Because MANETs are dynamic, a secret password holder may pose a threat regardless of the absence of malevolent intruders with illegitimate credentials. Furthermore, it is challenging to manage the authentication procedure from only one node. Trust processes are often limited to proximity [120].

Sybil attacks are a severe concern, hence MANET's safety features in the system require each node to have an individual, distinct, and durable identity. It takes place at the network layer. A Sybil intruder may both swap accounts in order to compromise the detection procedure and encourage an absence of responsibility in the network, or they can generate several identities on just one computer to launch an organized attack on the computer system. In addition, there are many types of attacks such as denial-of-service (DoS), replay, jellyfish, and neighbour attacks. When defence operations are delayed severely by a MANET using expensive anonymity routing in a combat zone, poor voice and video information transfer quality might result from resource depletion. In the context of location-based routing, there currently is no integrated method for thwarting Sybil attacks and granting authenticity. Furthermore, the majority of threat detection techniques now in use ignore QoS metrics. To achieve malice-free routing, improved safety mechanisms must be offered [121].

Jamming Attacks in MANET generally alter routing messages and drop the packet leading to a drain in the battery of individual nodes. It causes individuals to travel the incorrect packet in the wrong way and modifies packet properties like serial numbers. The existing mechanisms like authentication or cryptography prevent attackers in MANET [122]. Selfish nodes make the network resources like batteries useless. They are not

involved in network routing activities. Therefore, selfish nodes also degrade the network performance. The recommended scheme ensures an effective security mechanism and is capable of detecting the inside attacks in MANET. The most significant issue for a MANET is about providing effective security. There is no efficient security method or cooperative scheme to detect different types of attacks in a MANET because of its lack of centralized administration, open medium, and dynamic topology [123].

Assaults that use selective forwarding may take various shapes and exhibit characteristics of DoS, Blackhole, Gray-hole, and Neglect and Greed assaults. The attacker's node suppresses packets originating from a particular node or set of nodes intentionally in a DoS attack. Because it declines the forwarding of each packet, like a black hole attack, the attacker's node could be sending the communications down the incorrect route and taint the system's routing data [122].

One kind of danger to security is the "black hole attack," whereby network data is routed to a node that doesn't function. It's comparable to the black hole in the cosmos, where objects vanish. Because it takes the quickest connection, the node exposes itself to additional nodes and networks in a manner that allows it to misuse them. A hostile node advertises itself as being the quickest route to the DN or to the packet that it intends to interrupt using its routing protocol in a black hole assault. Without consulting its routing database, this malicious node announces that it has fresh paths available. The intruder nodes are perpetually able to respond to routing requests in this manner, allowing them to obtain and maintain information packets. A hostile and fraudulent route is generated in a format based on flooding because the asking node is going to receive the fraudulent node's response when the legitimate node does. Once this path has been established, the node must decide either to send all packets to the unidentified address or to discard them

altogether. Hence, it is very much essential to develop an effective security scheme to protect the nodes against attacks and also to focus on energy efficiency and security issues [124].

2.12. Black hole detection methods

An independent node attracts information packets in a black hole attack by pretending to be a new route that leads to the target. However, it does not send information packets to their destination rather it consumes them. Collaborative black hole attacks include malevolent nodes cooperating as a cohesive unit [125].

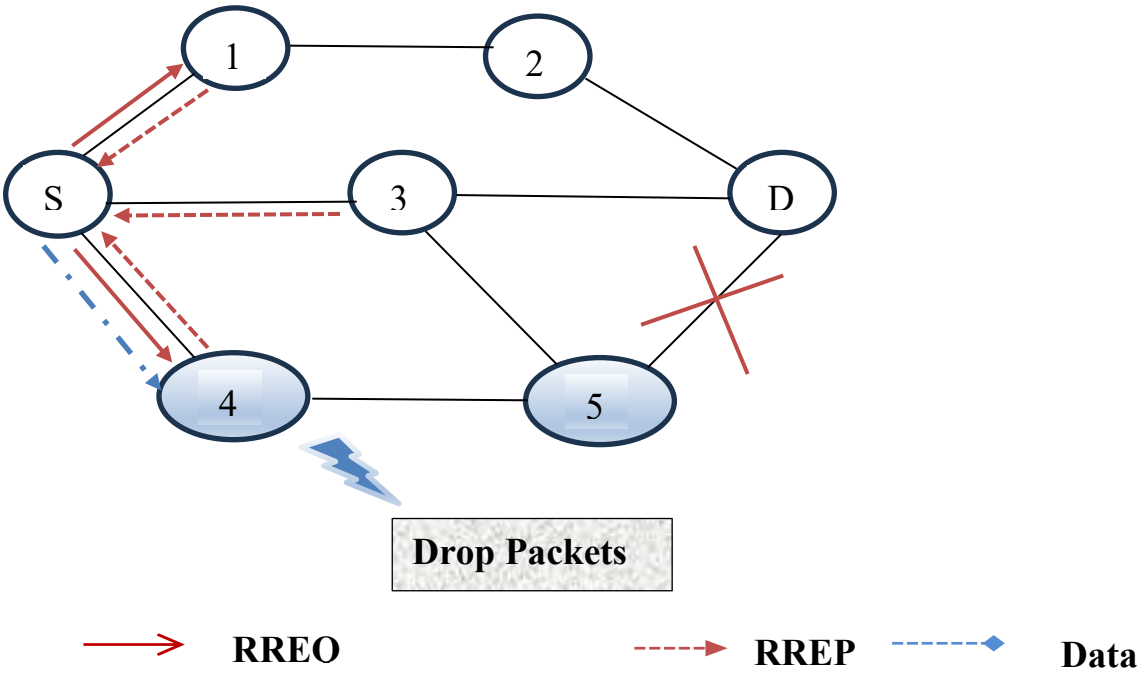


Figure 2.9. Black hole attack scenario

Figure 2.9 provides a demonstration of a black hole attack that was launched against a network. Nodes 1, 2, 3, 4, and 5 function as intermediary nodes, while Nodes 4 (B1) and 5 (B2) function as collaborating black hole nodes in the scenario wherein S is the SN and D is the DN. All adjacent nodes receive an RREQ notification from the original node whenever it wishes to

transmit an information packet to the target. In this instance, the rogue nodes join the system as well and get the RREQ notification. Following that, malevolent nodes instantly transmit the RREP communication, which travels via B1 to its target. The SN begins sending information packets to B1 continuously as soon as it gets the RREP. However, rather than sending the information packet to its destination, B1 destroys it. As a result, the information packet becomes lost and hardly arrives at its intended location.

A method for identifying a collaborative black hole attack in MANETs was presented by Sen et al. [126]. Two ideas were implemented in the method to change the AODV algorithm. Two types of tables exist: the DRI (data routing information) table and the cross-checking table. Every node keeps a DRI table updated. Details concerning whether values are true or false may be found in the DRI table. Whenever a SN broadcasts an RREQ communication to determine a quick and safe route, the intermediary nodes respond with an RREP communication containing details regarding their DRI table. This process is called cross-checking. The delivery ratio is raised from 38% to 55% through the application of this technique. This led to a 17% increase on average, but less efficiency.

Ren et al. [127] provided a method for leveraging packet transfer monitoring in disruption-tolerant systems to identify black hole attacks. This method uses a pair of tables to store the records of packet exchanges: the SRT (self-record table) and the RRT (receiving record table). By employing this approach, attacks by insiders may be effectively detected having an elevated rate of detection with a modest positive rate. RRT has the packet interchange history of the node that transmits the RREP, and SRT has the packet interchange record of the node that transmits the RREQ.

Esmaili et al. [128] devised an approach to use the OPNET simulator to analyze the AODV protocol's effectiveness in the face of a black hole assault.

Examine two secured MANET techniques in this investigation. Initially, ad-hoc routing must be secured utilizing a variety of procedures, such as Real-time transfer protocol (RTP), Destination sequence distance vector (DSDV), and Dynamic source routing (DSR). The second difference is that intrusion detection systems use a technique wherein every intermediary node returns data about the following hop along with an RREP message. This increases the PDR; however, it also significantly lowers the likelihood of black hole assaults.

Utilizing cooperative security agents, Mohite & Ragha [118] devised a technique to identify cooperative black hole attacks. Utilizing one or more of these three ideas first, SRT and RRT Tables; secondly, data routing information; and thirdly, cooperative security agents malicious nodes are able to be efficiently identified and lessen the adverse consequences of Coordinated black hole attacks in addition to black holes.

Two methods were proposed by Al-Shurman et al. [129] to identify the black hole attack. The original method relies on RREP packets arriving through several nodes. Though it takes more time, this approach is reliable. Sending RREP with an entry of the final two sequence numbers is the basis of the subsequent approach. The additional technique lowers network overhead as well as is quick and dependable. However, since hostile nodes can occasionally respond to channels and modify their tables, this strategy is not safe.

Osathanunkul & Zhang [130] developed a strategy to use S-ETX (secure-expected transmission count) to identify black hole attacks. A better variant of ETX is called S-ETX. Two changes have been added to S-TEX: initially, the initiator calculates the df and dr values; secondly, the initiator records the packets that are transmitted. Utilizing SETX improved efficiency while lowering overhead costs.

DPRAODV (Detection, Prevention and Reactive AODV) was presented by Raj & Swadas [131], as a way to identify and stop black hole attacks. Whenever AODV in DPRAODV receives RREP, it verifies the node's serial number. Sequence numbers that are larger than the specified threshold indicate the presence of a hostile node, which is added to a blocking list. An ALRAM packet is subsequently sent to neighboring nodes via the DPRAODV PDR, which raises and normalizes ROH in addition to enhancing traffic burden.

Utilizing the "Fidelity Table" approach, Tamilselvan & Sankaranarayanan [132] designed a way to differentiate between the black hole attacks. The fidelity degree for each node is recorded in the fidelity table. It indicates an intruder node if the fidelity degree is below the definite level. This approach increases packet delivery but increases overhead since a fidelity table is introduced.

The SAODV (secure AODV) method has been established by Lu et al. [125] for increasing the level of safety of AODV. The route identification procedure is the primary distinction among each. The SAODV method reduces packet loss. While packet loss in AODV is 57%, it is decreased by 49% in SAODV (8.132%).

A method for offering safety for routing in wireless MANETs was put out by Hongmei Deng et al. [133] whereby the intended node alone transmits all response messages and the intermediary node's duty is completed. Essentially, this method just detects black hole attacks; cooperative black hole attacks are not under regulation.

The objective of Kaur and Kalra's [134] "digital signature" authentication approach is to identify and stop black hole attacks. wherein the quickest path between several nodes is chosen at the final location using the

TTL mechanism. Each of the visitor node's digital signatures is stored in a table at the DN dedicated to digital signatures. Basically, this method lessens the cooperative black hole attacks.

A secured information technique was presented by Siddiqua et al. [135] to stop the black hole assault in MANETs. wherein each node keeps an eye on every one of its neighbors and compares the data from each neighboring node to its knowledge table. A knowledge table containing the node's fm and rm variables. When a node's fm value and rm value coincide, the node is declared maliciously utilizing this procedure, which first determines the reason for the packet loss prior to designating the node being a black hole node.

2.13 Blockchain to enhance MANET security

Numerous investigators investigate the utilization of blockchain-based technologies for managing trust amongst MANET nodes. The writers explain the concept of blockchain and the problems with MANET protection [110]. They additionally address the limitations of utilizing Blockchain in MANET applications. They examine the limitations associated with utilizing both PoW and PoS in a MANET environment. Since MANETs are very dynamic, PoS presents challenges while PoW can be more computationally demanding.

PBFT, is used in certain blockchain platforms, such as Hyperledger. To make technique working, two of the three nodes must concur on their agreement. Scalability with MANETs can prove problematic because of frequent link failures. Thus, PBFT could not work. The application of blockchain-based principles to trust management was additionally investigated by the researchers; this is covered in the section that follows [136].

2.13.1 Lightweight Trust Management Using Blockchain in MANETs

A randomized distributed method for establishing trust among nodes in MANETs is called Blockchain-Based Lightweight Trust Management (BLTM). Trust management plays a critical role in maintaining reliable interaction between nodes in MANETs [137]. Because they need an authoritative source to maintain trust, which would be unfeasible in a distributed network, typical central trust management approaches may not be suitable for MANETs. Consequently, managing confidence in MANETS necessitates a distributed strategy.

MANETs utilize BLTM technology to enhance both the safety and reliability of node-to-node transmission. BLTM creates an accessible and safe trust architecture between nodes by fusing the blockchain platform with the trust management approach [138].

BLTM protocol for MANETs, which is divided into four stages. They involve the stages of block maintenance, blockchain-based consensus, trust assessment, and block creation. Every node assesses the reliability of its adjacent nodes during the trust assessment stage using a variety of factors, including the packet forward rate, reply time, and packet loss rates. In accordance with the assessment, the node subsequently allocates a trust level to every one of its neighbors.

During the blockchain-based consensus stage, each node shares its neighbourhood blockchain with its neighbouring nodes in order to reach an agreement on the trust levels assigned to each node. In order to minimize the cost of computation and guarantee that agreement is obtained promptly, BLTM employs a lightweight consensus method. The method is referred to as Delegated Proof of Trust (DPoT). It is OLSR procedure compatible. To

create DPoT, they embraced the DCFM plan. To reach a consensus, DPoT makes use of the delegator and validator nodes [139].

To construct a block in the framework of a blockchain, the delegate node must decide what data should be contained within the block in order to manage it during the block creation stage. After the pool's activities are gathered into a block, the blockchain network uses the SHA-256 method to generate a hash value that is appended to the block. This hash value is derived entirely from the information contained in the transactions. To link the blocks and form a chain, the hash from the one before it is additionally included as information in the present block. Merely a specific structure, which includes a hash signature that initiates with 10 consecutive zeros, is supported by the block hash [140].

To ensure node confidence in a secure MANET, a blockchain could be used. Every blockchain block contains transaction-related data and accompanying metadata, such as a timestamp, transaction hash, delegate ID, and nonce. The hashed session contains the transaction generator ID, related transaction data, and the delegate ID. By doing this, it is made possible for block operations to be reliable and unreliable from none of the nodes that are involved. Whenever the network is initially founded, the genesis block, which is the primary block in the blockchain, is produced containing a blank list of operations [141-142].

2.14 Simulation Tools

To simulates networks systems, many of simulators can be applied, the most common is NS2 and Ns3 simulators.

2.14.1 Comparison of NS2 and NS3

Table 2.4 provides a comprehensive summary of NS2 and NS3. In comparison to NS2, NS3 appears more potent, adaptable, and versatile. However, NS3 design and configuration are unfamiliar to a lot of users [143].

Table 2.4. Assessment between NS2 and NS3

Network Simulator 2 (NS2)	Network Simulator 3 (NS3)
Not actively maintained	Actively maintained and supported
Use TCL as the scripting language	Use C++ and Python as the scripting language
Not flexible	Flexible
Recompilation is long	Recompilation is faster with a single command
Use nam animator	Use PyViz python visualizer and NetAnim animation
Simulation only	Simulation and emulation as well as the DCE environment is offered
Difficult to get power consumption	Power consumption can be achieved easily
Lack of Goodput calculation	Goodput calculation is available
MAC protocol is fixed	MAC protocol is user-defined

2.14.2 NS3 Simulation Modeling

Many classes, including core-module.h and network-module.h, must be added in order to create NS3 simulations. The NS3 API includes these types of classes as well as thorough explanations of each. In addition, NS3 uses the Python and C++ programming languages. To begin an NS3 simulation, a number of actions must be taken. In Figure 2.10, the NS3 simulation techniques are demonstrated.

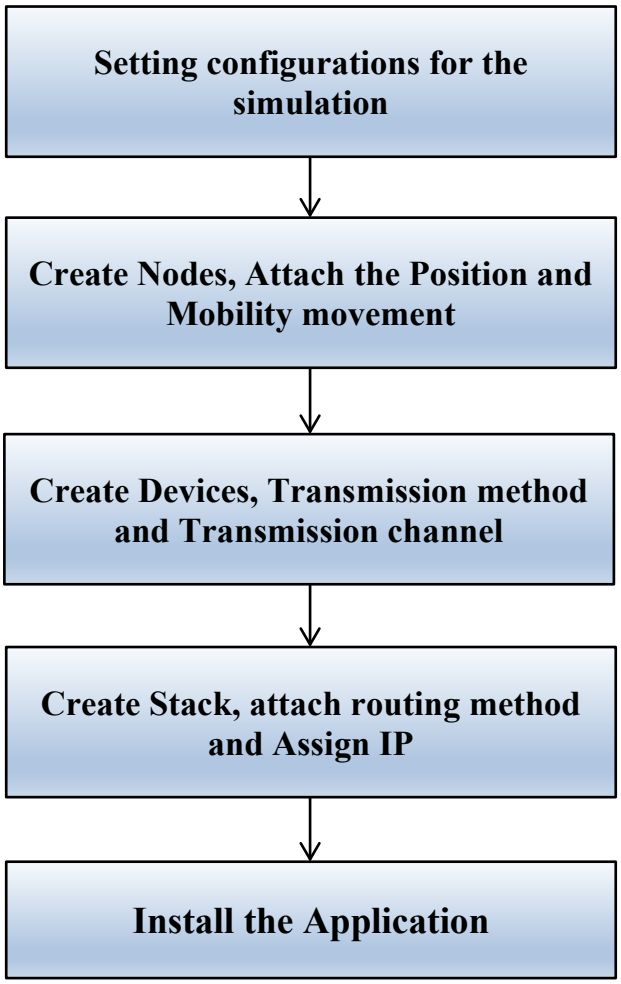


Figure 2.10. NS3 simulation procedures

Every value for parameters is shown initially. Next, employing the settings from the previous phase, simulation records are made and a structure of simulations is formed. Every function pertaining to the nodes themselves shall also be specified. The devices' Internet Layer will eventually be

developed, indicating the channel that is utilizing each device and the manner in which data is transferred among them. The devices are put in accordance with the nodes at the identical period. The routing technique, ports, and IP address are configured at the transport layer. Additionally described is the Internet stack, which houses the ports, IP address, and certain types of data. The source and sink nodes have been chosen for the data transfer in the application layer. Lastly, the simulations are prepared to operate within the time frame specified.

NS-3 is an active open-source system for simulating various network conditions, with mobile devices. It is a significant tool for academics and programmers since it provides an extensive number of models and components that accurately represent the behaviour of mobile networks. Furthermore, this study indicates that employing ns-3 mobile simulation frameworks can help to better understand mobile network performance.

Chapter Three

The Proposed System

Chapter 3: The Proposed System

3.1. Enhance OLSR for transmission video

The suggested study presents an efficient extended OLSR protocol using a deep learning model to enable optimal streaming of videos in MANETs. The proposed study includes data gathering, blackhole identification using validation, blockchain storage spaces, and trust-based optimal dependable routing. primarily, the inputs of video information's are collected from freely accessible sources. Then, to locate black hole nodes in the suggested research presents an innovative Twin-Attention based SA_DCBiGNet approach. The accessible of adjacent nodes is then examined using the trust values. The routing is then completed by the Extended Osprey-assisted OLSR Protocol (EO_OLSRP). The proposed system flowchart is shown in Figure 3.1.

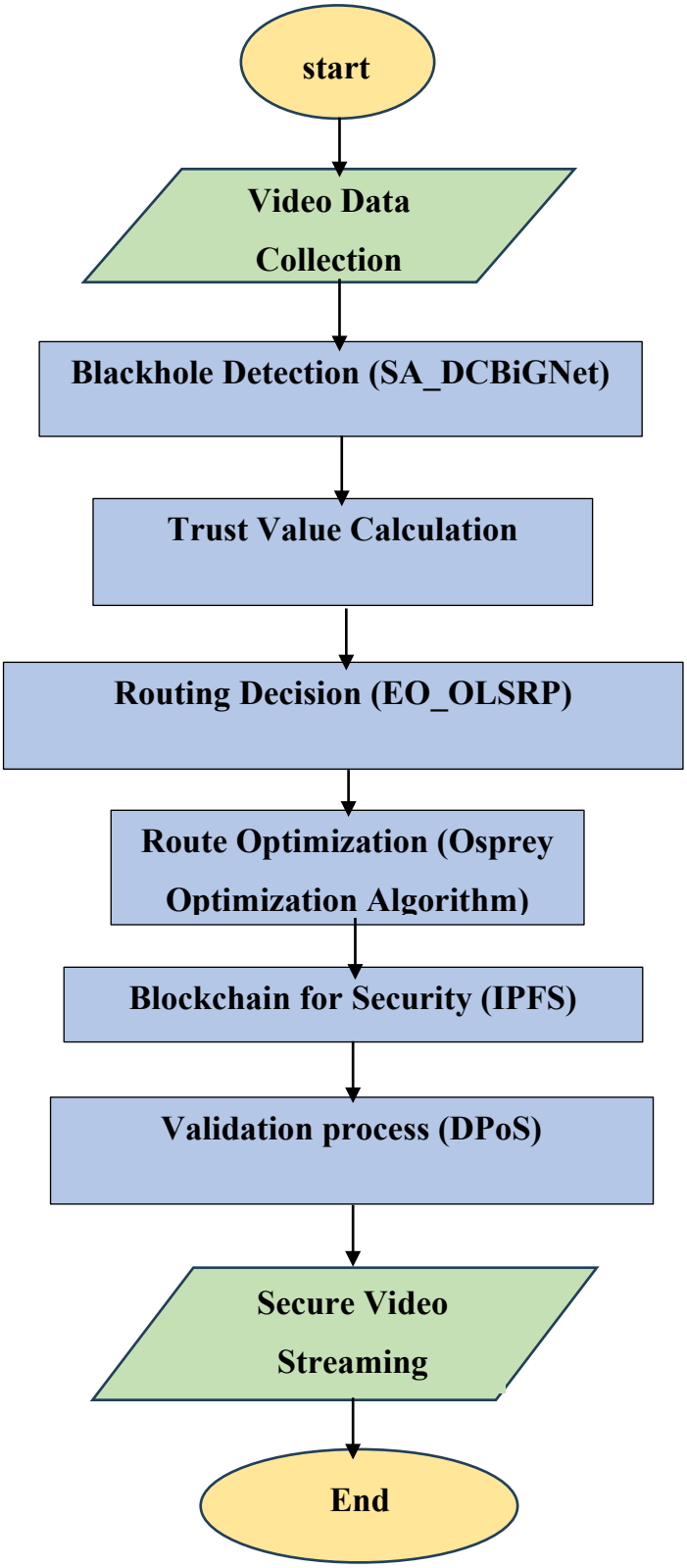


Figure 3.1. Flowchart of the proposed system

The Osprey Optimisation Algorithm (OOA) chooses the best route based on characteristics such the stability of the node and connection stability degree. Finally, Interplanetary File System (IPFS) technological enables blockchain storage to improve MANET information security. The proposed blockchain framework's validation mechanism utilises the Delegated PoS (DPoS) approach. Thus, the suggested study efficiently protects MANETs from unauthorised outsiders, thereby improving confidentiality. The higher performance obtained in the suggested study indicates that the evolved and expanded OLSR protocol is appropriate for MANET streaming video applications.

3.2 System model

The proposed technique includes various innovative characteristics that allow video transmission over the nodes. Figure 3.2 illustrates the operational principle of the suggested algorithm. In the beginning the input video is sent to the recommended module. Two modules of Linux are required to achieve proper video streaming on both ends. After that, the video stream is sent to the recommended MANET infrastructure, where at the output end, it is accepted as appropriate. After then, the data is protected and the network's simulation settings are modified to extract features from the movies for testing.

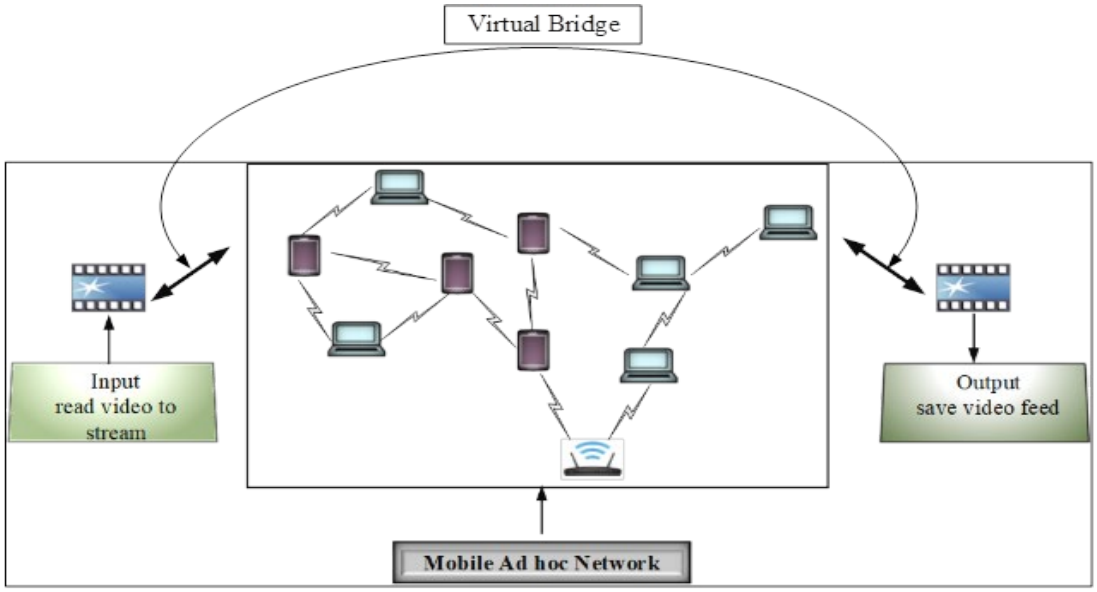


Figure 3.2: System model of MANETs

3.3 Data Collection

The process of collecting information and analysis of the collected data from different sources are called data collection. The supplied videos are subsequently gathered using the Kaggle dataset. As a result, two distinct datasets are employed to gather the videos: 1) brief videos: short videos are offered for usage in object recognition and other video analysis applications. 2) Csv: This study creates a particular set of data for Wireless Sensor Network Detection System (WSN-DS) to assistance in the finding and categorization of the following types of Denial of Service (DoS) attacks: Blackhole assaults.

3.4. Detection of black hole

The malevolent network engages in a number of undesirable activities that impair network efficiency. The malicious node then sends route response (RREP) metadata to the Source Node (SN) as soon as it obtains the route request (RREQ) from the targeted node, without taking into account the actual path taken from the point of origin. The blackhole station regularly transmits the fake route answer to the SN. The network's performance decreases when a rogue node saves data packets before wiping out the entire network.

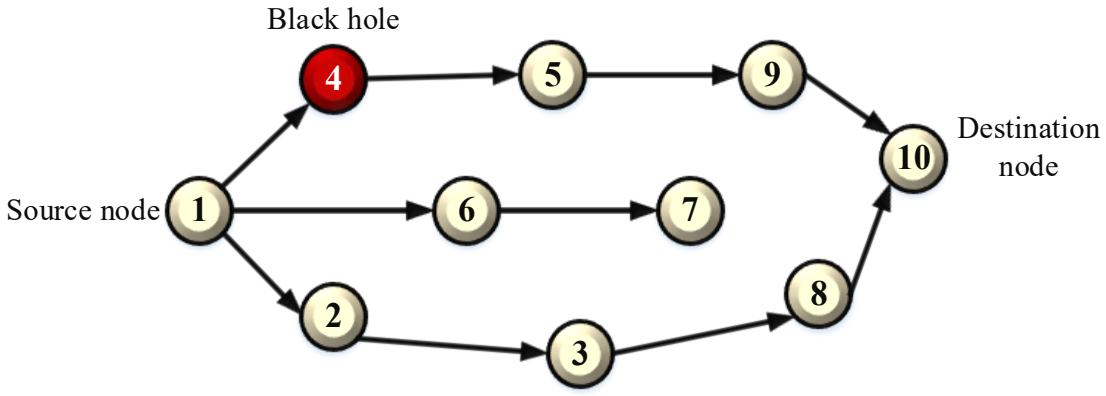


Figure 3.3: Blackhole detection

Figure 3.3 shows that the network is made up of ten nodes interconnected through a dynamic topology, each with a SN and the Destination Node (DN). When transferring data packets to the DN, the SN broadcasts a route request (RREQ) for the fastest route to the terminus. When a malevolent node or black hole, such as node 4, receives the RREQ message, it immediately responds with a bogus route to the originating node. For example, after accepting the RREP message, node 1 sends data packets using that route. The data packets are obtained by Node 4, and it subsequently eliminates them across the network, leading to the collapse in the network. Thus, the projected study introduces an innovative SA_DCBiGNet model that utilizes Twin-Attention for finding blackhole nodes. subsequently the twin attention models can focus on both local and global components of the input. The phrase "twin aspect" refers to the model's ability to handle two unique elements of the input data within a single attention layer: general structure and smaller details. As a result, by collecting the intricate connections between numerous data points, the model may be able to reveal previously unknown blackholes. Identify spatial information from the dense layers, Temperature discrepancies or brightness patterns may indicate the existence of a black hole. The term "dense" refers to the use of many convolutional layers to increase feature extraction capability. Then, bidirectional gated networks with layers identify

dependent relationships and temporal changes by analysing the data's recovered attributes both forward and backward in time. It is necessary to detect minute variations or signs that could indicate the presence of a black hole. Based on the collected properties and their temporal correlations, the network predicts the presence of a blackhole at a certain location in the data.

3.4.1. Twin Attention based Dense Convolutional Gated Network

This section discusses the anticipated SA_DCBiGNet model. The suggested SA_DCBiGNet approach consists of a dense CNN (Dense-CNN), Twin-Attention, and Bi-GRU networks. There are two types of twin attention: position attention and channel attention approach. The suggested SA_DCBiGNet model uses Twin-Attention to locate blackhole nodes. Once a blackhole node is identified, movies received from that node are ignored. Table 3.1 shows hyperparameters and values. Figure 3.4 depicts the basic structure of the SA_DCBiGNet architecture.

Table 3.1: Hyperparameters and values

Parameters	Values
Epochs	10
Batch size	32
Loss	Binary cross entropy
Learning rate	0.001
Dropout layer	4
Input dimension	(25,1)
Output dimension	(25,1)

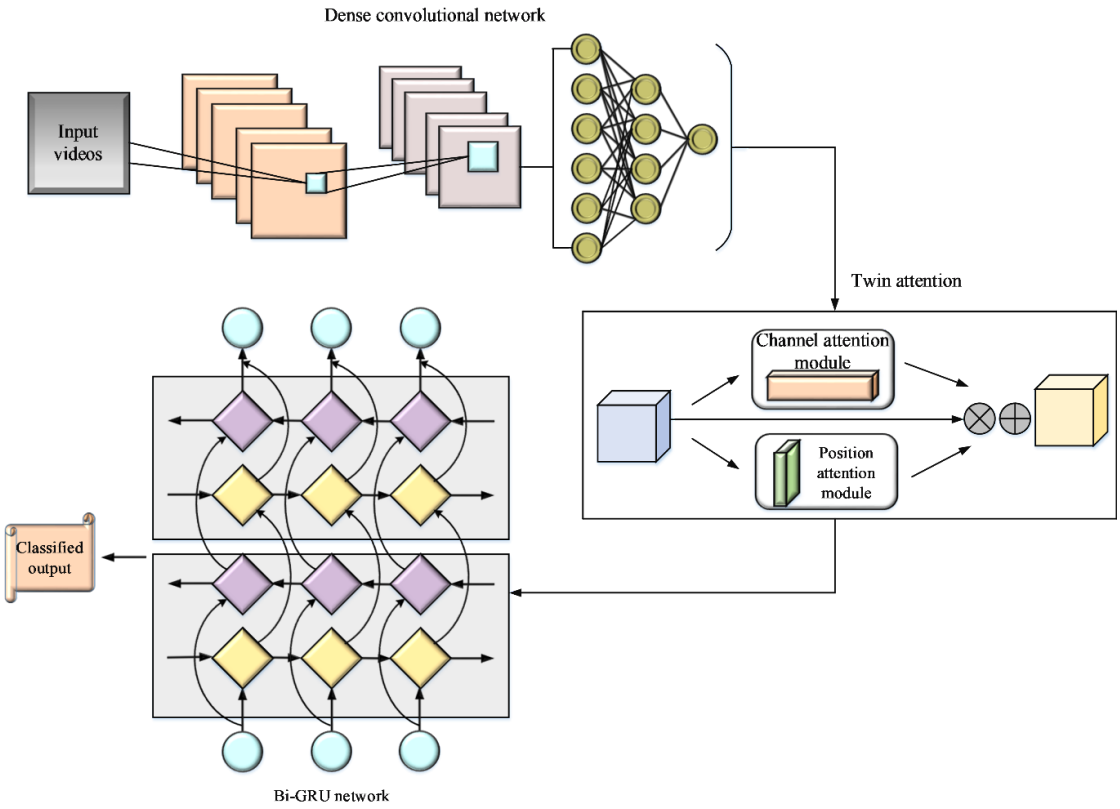


Figure 3.4: Architecture of SA_DCBiGNet

3.4.2 Dense Convolutional Neural Networks

The suggested dense network is made up of neurons that develop strategies to optimize one another. Furthermore, as the initials of Dense networks indicate, layers can be tightly interconnected, which means that each neuron passing through a specific layer receives information from every neuron passing through the preceding layer, and so forth. It also acts as a source of information for all of the neurons in the layers shown in Figure 3.5.

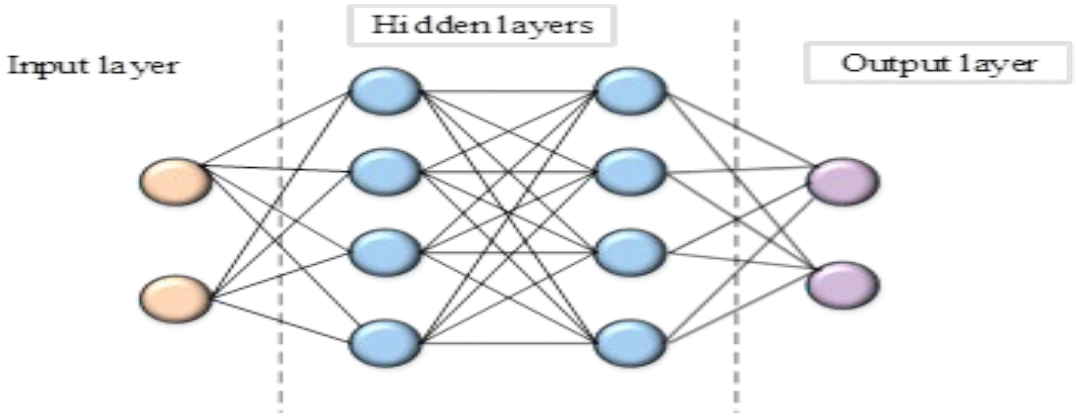


Figure 3.5: Dense neural network

A dense network is utilised for a diversity of applications, which includes linear classification and evaluation as well as unsupervised data clustering. It can analyse data with complicated patterns. The suggested CNN is a sort of neural network similar to a dense network in that it is primarily meant to analyse visual data. The technique enables the encoding of video-specific features in neural network design, making it more appropriate for tasks that need videos. Figure 3.6 represents the architecture of dense CNN.

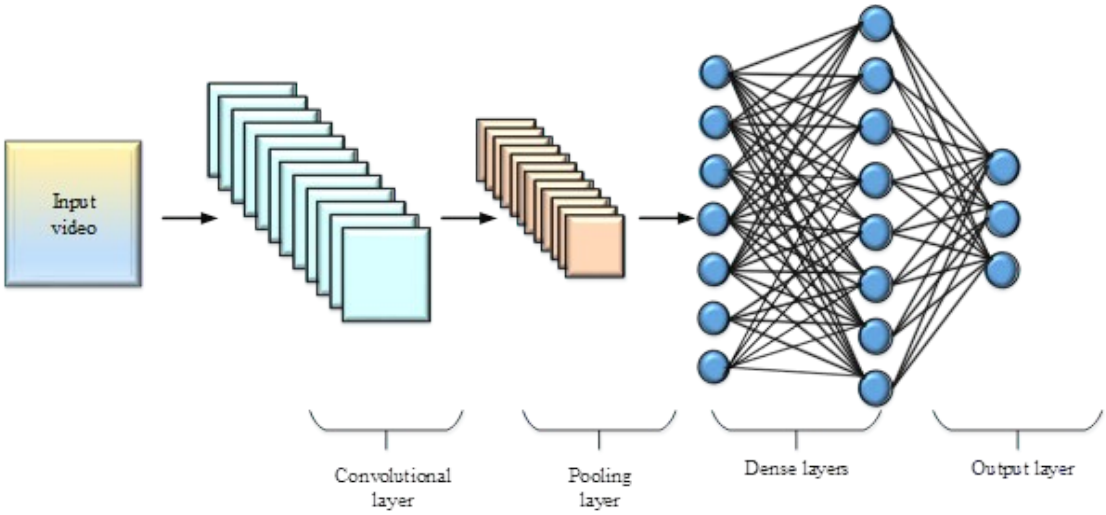


Figure 3.6: Dense convolutional neural network

As a result, the suggested CNN may drastically reduce the total amount of features while keeping a weight-sharing structure and pooling methodologies, outperforming DNNs in video evaluation. The entire connection of nodes exacerbated the issue of dimensionality. It is important to remember that CNN lacks invariance in spatial relationship, which means it is unable to record an object's location or orientation. Consequently, CNN might not be instantly effective if discussing the position of details issues. CNNs are quickly becoming popular as a result of design research findings for a number of tasks such as categorization and autonomous design.

3.4.3. Twin Attention

Twin-Attention has been suggested for integrating local and global elements in a flexible way. This sub-section discusses the twin-attention layers, which arrest systematically distant background data. Twin attenuation module is represented in Figure 3.7.

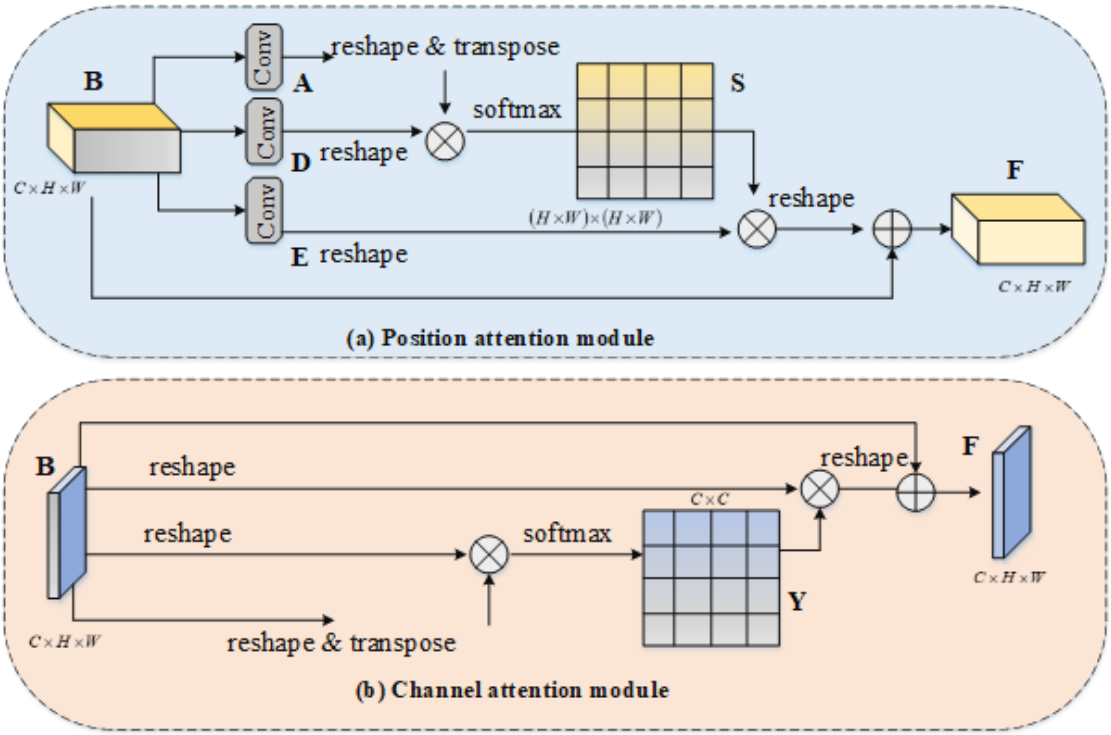


Figure 3.7. Twin-Attention module

3.4.3.1. Channel Attention

The channel attention presented a number of fascinating ideas and showed significant potential for improving deep CNN effectiveness. For more sophisticated features, a class-specific approach can be taken into consideration for each channel's layer, and several conceptual outputs are connected. The channel's attention architecture $y \in R^{C\times C}$ is immediately calculated by the primary components. Discounting the location of the attention method. Even more accurate is to reorganize $B\ to\ R^{C\times N}$ before conducting matrix multiplication along B and transposed version B. To attain the channel attention $y \in R^{C\times C}$, then finally add the SoftMax layer.

$$\boldsymbol{y_{ji}} = \frac{\boldsymbol{exp(B_i, B_j)}}{\sum_{\boldsymbol{i=1}}^{\boldsymbol{C}} \boldsymbol{exp(B_i, B_j)}} \tag{3.1}$$

Where y_{ji} denotes the outcome of i^{th} channel regarding j^{th} channel. Moreover, to transpose y and B, multiply those consequences, and then rewrite in D. The end result $F \in R^{C \times H \times W}$ can be attained by multiplying the result with a scale parameter of β after carrying out an element-wise operation with B.

$$F_j = \beta \sum_{i=1}^{C} \left(y_{ji} B_i \right) + B_j \tag{3.2}$$

As a result, β gradually obtains a weight of zero. The long-term foundational relationships between feature map elements are represented by equation (3.4), and the weighted mean of the features extracted from the remaining channels plus the initial characteristics makes up the final feature for each channel. Twin-attention enhances the capacity to distinguish between different features.

3.4.3.2 Position Attention method

A model's ability to capture local characteristics is enhanced by the suggested location attention, which encodes a greater variety of context-related data into one another. The approach for automatically collecting spatial contexts is then described. The neighbourhood feature is shown as $B \in R^{C \times H \times W}$ First, the Convolutional layer generates two features: A and D, while $\{A, D\} \in R^{C \times H \times W}$ Finally, the dimensions are altered by $R^{C \times N}$ So, the total amount of pixels is represented as $N = H \times W$ The spatial attention related with SoftMax $S \in R^{N \times N}$ is then calculated by doing matrix multiplication with the transpose vectors D and A.

$$s_{ij} = \frac{\exp\left(A_i, D_j\right)}{\sum_{i=1}^{N} \exp\left(A_i, D_j\right)} \tag{3.3}$$

Hence s_{ij} thei^{th} Position is influenced by the j^{th} position. In addition, reshaping $R^{C\times N}$and developing a new feature $E \in R^{C\times H\times W}$ By entering the feature B Over the convolution layer. The output is then moulded into $R^{C\times H\times W}$ Using matrix multiplication E and S as the transpose. To reach the outcome$F \in R^{C\times H\times W}$, then perform an element-wise method utilising features B raise the dimension factor.

$$F_j = \alpha \sum_{i=1}^{N} \left(s_{ij} E_i\right) + B_j \tag{3.4}$$

Thus, α begins with zero and gradually increases in weight. Equation (3.4) indicates that the final feature Fin each place is a weighted average of the attributes over all areas, as well as the initial parameters. The end result is a systematic integration of contexts built around spatial focus and overall intellectual awareness. Similar behaviors interact to enhance one another, enhancing semantic consistency and compactness inside the class.

3.4.4 Bi-GRU network

A Bi-GRU network is the planned GRU network that has two levels of architecture added to it. The two-layer arrangement ensures that the output layer always has full control over the context data of the input layers. The main premise of a bi-GRU network is that the input series is handled by two forward and backward networks prior each of their outputs converge in a single output layer. In a Bi-GRU network, the forward layer analyses the output from the hidden layer calculates the output from the hidden layer at each step from backward to forward, whereas the hidden layer computes its output at each step from forward to backward. Figure 3.8 shows how the

output layer merges and normalises the output values produced by the forward and backward layers at each step.

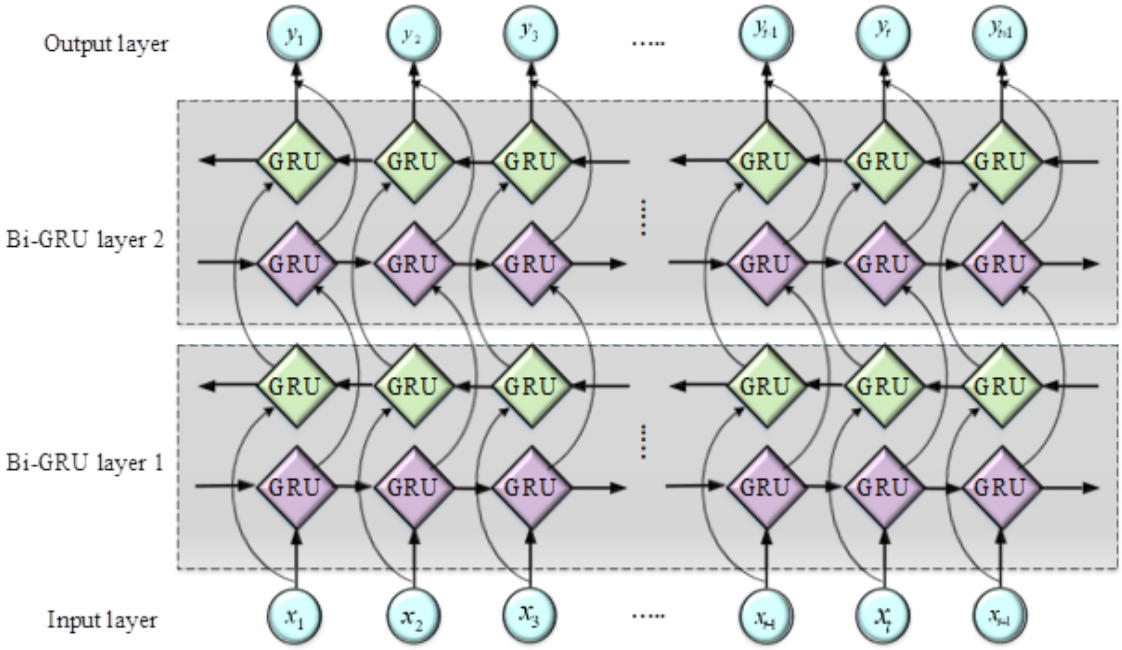


Figure 3.8: BI-GRU network

$$\vec{h}_t^1 = g\left(w_{yh^1} \rightarrow y_t + w_{h^1 h^1} \rightarrow\rightarrow \vec{h}_{t-1}^1 + a_{h^1} \rightarrow\right) \tag{3.5}$$

$$\overleftarrow{h}_t^1 = g\left(w_{yh^1} \leftarrow y_t + w_{h^1 h^1} \leftarrow\leftarrow \overleftarrow{h}_{t-1}^1 + a_{h^1} \leftarrow\right) \tag{3.6}$$

$$\vec{h}_t^2 = g\left(w_{h^1 h^2} \rightarrow\rightarrow \vec{h}_t^1 + w_{h^2 h^2} \rightarrow\rightarrow \vec{h}_{t-1}^2 + a_{h^2} \rightarrow\right) \tag{3.7}$$

$$\vec{h}_t^2 = g\left(w_{h^1 h^2} \leftarrow\leftarrow \vec{h}_t^1 + w_{h^2 h^2} \leftarrow\leftarrow \overleftarrow{h}_{t-1}^2 + a_{h^2} \leftarrow\right) \tag{3.8}$$

$$x_t = f\left(w_{h^{2x}} \rightarrow \vec{h}_t^2 + w_{h^2 x} \leftarrow \overleftarrow{h}_1^2 + a_x\right) \tag{3.9}$$

Here, $\vec{h}_t^1 \in N^H$ and $\vec{h}_t^2 \in N^H$ denotes the hidden layer output in the forward direction,H indicates the number of elements, t represents the time, $\overleftarrow{h}_t^1 \in N^H$ and $\overleftarrow{h}_t^2 \in N^H$ represents the hidden layer output in reverse direction, $x_t \in N^T$ denotes each label value for the merging term at the instant, Trepresents the number of labels, the input time represented as y_t, $f(.)$

represents the activation function, $a$and$w$ demotes the weight matrices and $g(.)$ represents the GRU processing network. Overall, Bi-GRU networks offer a realistic way for improving MANET blackhole diagnosis while also boosting network safety and dependability. The suggested (SA_DCBiGNet) model exhibits an entropy loss, which impacts the efficiency, hence the parameters require to be fine-tuned, thus loss is decreased, as indicated in equation (3.10).

$$P_{entropy-loss} = \frac{1}{N_t}\sum_{i=1}^{c} W_h^{\mathrm{mod}ules}\left[E_c^k + (1-E_c)\log\left(1-E_c^k\right)\right] \tag{3.10}$$

Here c denotes the total modules, $N_t$denotes the total samples, $E_c$represents the true vector, E_c^kshows label matrix. To lower the loss function, the variables are fine-tuned using the extended osprey optimisation method.

3.5 Trust value computation

The EO_OLSRP, which uses transmitted Topology Control (TC) and HELLO messages, determines the dependability of surrounding mobiles. if the percentage of trust is at least equivalent according to the designated trust standards, a mobile device may be selected for packet transmission. In addition to neighbour identifiers, the set of neighbours can be expanded to include the total number of messages sent by each neighbour in order to accommodate newly added modules. These variables are updated each time a TC or HELLO message is established. The trust-based optimum routing recognizes dependability in a node n controlled by an independent node y as a likelihood of performing a given predicted action, denoted as $T_y(n)$. Then, based on the knowledge gathered during a specific operation phase y, trustworthiness can be evaluated by taking a balanced mean of the confidence with each sort of activity, including information transfer, route reply, route

error, and route request. Over a period, to calculate that has acquired an in general, message transmissions through n, in which $p_c's$ are confirmed to be genuine and the total number of transmission attempts is p_a, and the total amount of communications that are accurate is p_s.

$$T_y(n) = \frac{p_c + \varepsilon p_s}{p_t + \varepsilon p_a} \tag{3.11}$$

Where $0 < \varepsilon < 1$ is the weighting factor, which represents an effective transmission ratio and indicates a high likelihood of successful transmission via the transmission link. In this situation, apply a mathematical methodology comparable to that used to quantify connection quality, it is not the same as an analysis of trust levels. In addition to evaluating trustworthiness, equation (3.11) also illustrates connection quality. To provide a more precise trustworthiness grade, additional, more sophisticated link quality measurements, such as the collision tracking and signal separation approach in addition to the link modification and power management method, may be employed. $T_x(n; j)$ denotes the dependability of node n as providing by node y over the j^{th} trustworthiness apprise cycle. When new data enters, the node updates its archive and calculates a trustworthiness score using the weighted mean or moving average model.

Assuming that the amount of $T_x(n; j)$ for the j^{th} trustworthiness updated phase is nominated as $\tilde{T}_x(n; j)$, which is calculated by measuring $n's$ existing behavior whereas y scrutinizes the precision and legitimacy of the messages that arrive from. In the $(j + 1)^{th}$ trustworthiness updated phase produce a number of the dependability, that is specified as $\hat{T}_x(n; j)$. Equation (3.12) uses the moving average technique to obtain a smooth valuation,

$$\hat{T}_y(n; j+1) = \alpha \hat{T}_y(n; j) + (1-\alpha)\tilde{T}_y(n; j), \quad for\ n \in N_1(y) \tag{3.12}$$

Here $0 < \alpha < 1$ shows a weighting factor exploited to balance the latest measurement data with the previous estimate. Assume the path $\varepsilon K_{s\to y}$, which $K_{s\to y}$ is a collection of paths that starts at a font node s and end at a end node y , for occasion $K_{s\to y} = \{allpathsfromstoy\}$. Then, $T_x(k;j)$ designates the trustworthiness of the path itemized by the node y. As a result, the path's trustworthiness is labelled as

$$T_y(p;j) = \prod_{n\in k} T_y(n;j) \tag{3.13}$$

Because of this, y can enhance its track record along a path that is determined by how reliable its nearby nodes are. A node's routing behaviour can be measured and decisions about routing can be made using the connections listed in equation (3.13).

3.5.1 Optimized Link State Routing Protocol

The OLSR standards offer no capabilities for connection testing quality. Then, as a result of the routing table's frequent modifications, bandwidth usage increases. Additionally, when it becomes more difficult to identify MPR, OLSR is finally used to complete the routing.

3.5.2 Extended Osprey Optimization Algorithm

In order to find a workable solution, this work suggests an OOA, a metaheuristic algorithm that efficiently conducts the process of searching in local and global problem-solving contexts.

The hyper parameters in the suggested model are hard to learn, which leads to a lot of training errors. In order to address these problems, the extended OOA (Ex-OOA) algorithm is used in the Opposition-based learning (OBL) technique to optimize the hyperparameters of the suggested model. The fitness function f value is used in the OBL approach to assess the relative merits of the current option. A diverse value $\bar{p}$ for the true value $p \in [v, l]$

is used in the fundamental description of OBL, and the following formula can be used to find this value:

$$\bar{p} = v + l - p \tag{3.14}$$

The following formula can be used to expand the description to n-dimensions:

$$\bar{p}_i = v_i + l_i - p_i, i = 1,2,\ldots,N \tag{3.15}$$

In the above equation $p \in R^n$ represents the real vector and $\bar{p} \in R^n$ indicates the opposite vector. Additionally, a comparison between the two replies p and$\bar{p}$ is done throughout the optimization process. It makes use of the fitness function. to evaluate the two possibilities, with the better choice being stored while the alternate is removed. Figure 3.9 display the Ex-OOA flowchart.

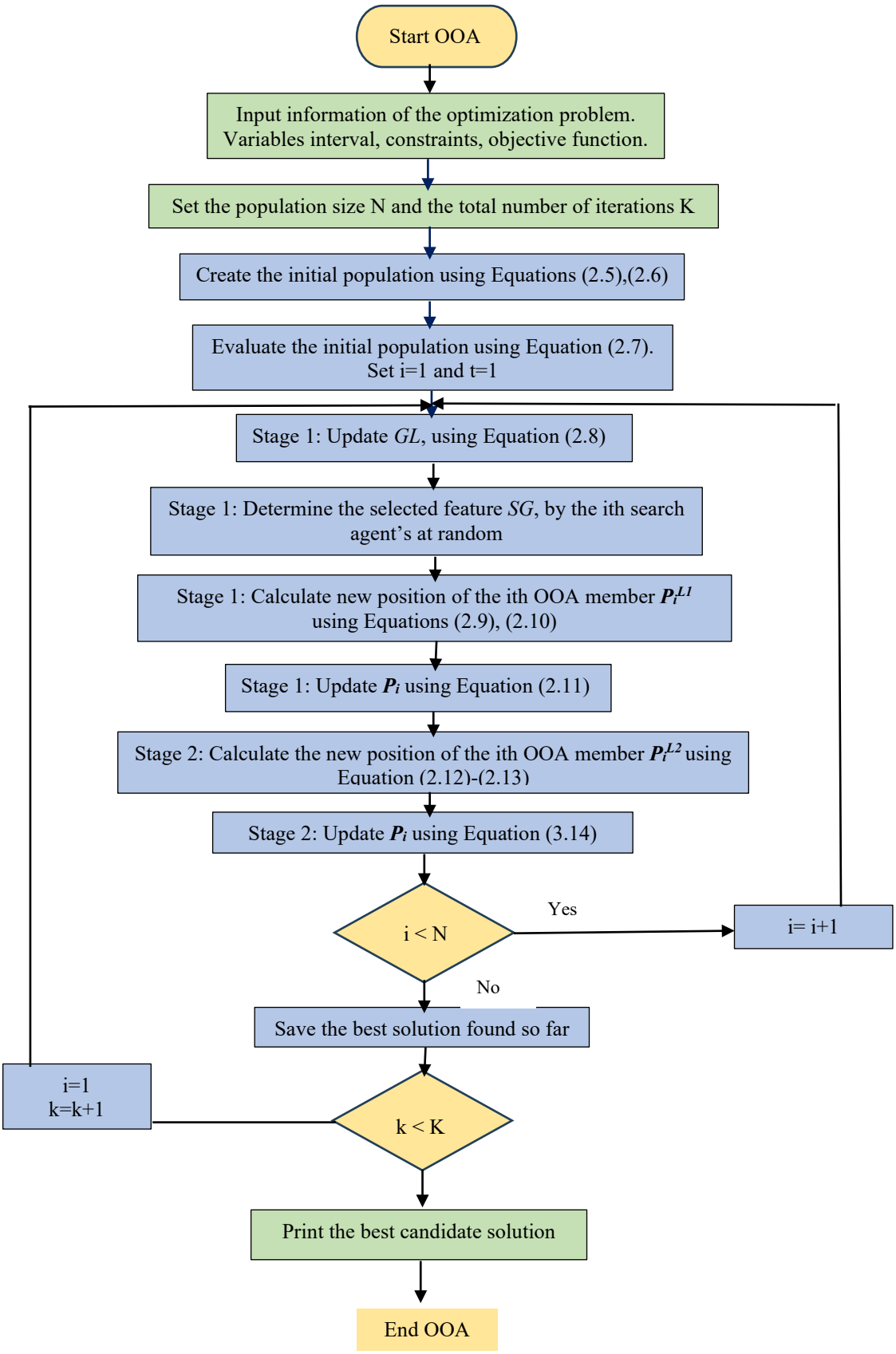


Figure 3.9 Flowchart of Ex-OOA

3.6 Interplanetary File System (IPFS)

To solve the problem of storing massive volumes of MANET data, the IPFS interface with blockchain is required. A distributed, p2p network for information storage is made possible by a novel protocol known as IPFS. Furthermore, the suggested IPFS offers the ability to store large files in a dependable and allocated manner. Figure 3.10 illustrates how many peers can transfer files via IPFS.

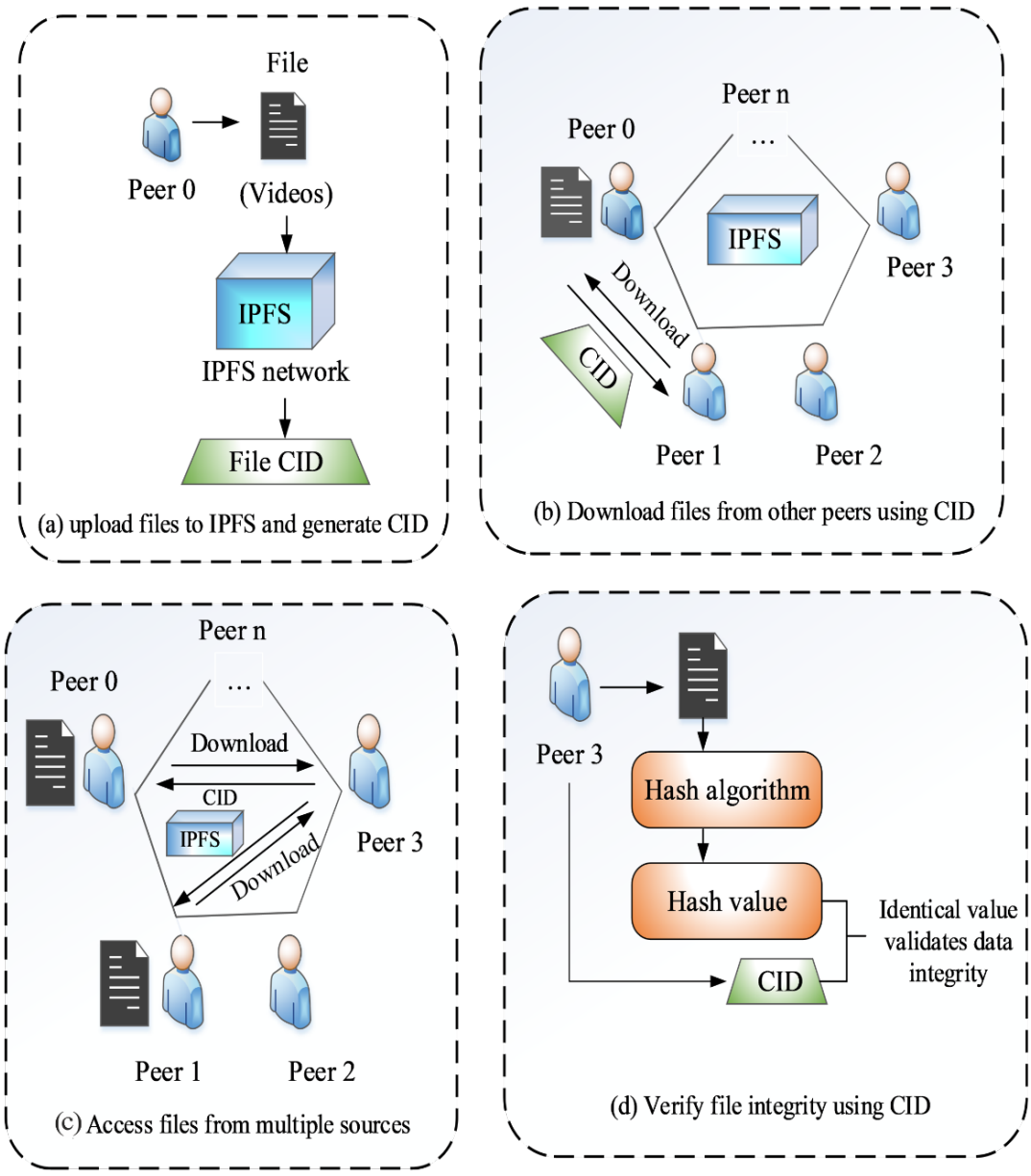


Figure 3.10 (a)-(d): Process of IPFS

For every file that is uploaded to the suggested IPFS network in Figure 3.10 (a), the algorithm for hashing and value known as the content identifier (CID), also called the file URL or address, are encrypted. Moreover, as illustrated in Figure 3.10 (b), the file may be accessed and received by other individuals having the CID. In IPPS, each peer serves as a file server, facilitating the speedy sharing and storing of enormous volumes of files. A peer may be able to get a record from many data sources, as shown in Figure 3.10 (c). Because of the distributed strategy, the principal operator cannot alter data. Because the CID would alter the content of the document shown in Figure 3.10 (d), it also acts as proof of the file's legitimacy. Since there is a great deal of potential for tackling the challenge of redundant, huge data storage in blockchain, the suggested IPFS is regarded as a responsive blockchain component. Peers can choose to add CIDs to the blockchain activities and put layout files and other information into IPFS in order to guarantee validity and dependability.

3.7 Delegated Proof of Stack (DPoS)

Network users choose passes on to vote in and help validate the previous block in the proposed Delegated Proof of Stake (DPOS) blockchain consensus method. A suggested DPoS blockchain allows its holders to cast votes to choose which nodes will sign off on transactions. A person's voting power is determined by the quantity of staked holdings. Users with greater stakes have more influence on who is appointed to the nodes. "Delegate" describes the designated nodes. Every node in the blockchain system has the ability to vote based on the assets in the suggested DPoS technique and choose the node that it deems to be the most appropriate. Compared to comparable systems, DPoS is more representative by design since it uses an independent voting procedure. Rather than doing away with the need for trust, the suggested DPoS is a method to make sure that those authorized to verify

blocks throughout the network do so truthfully and precisely. Every verified block needs to have its source validated as being the trusted node. When a sufficient number of unknown nodes complete the transaction as a result of DPoS, the process is no longer confirmed. Nevertheless, providing 3 seconds of processing-based procedures usually helps.

Each validator may offer a different incentive to those who want to cast a vote in this scenario. A portion of incentive money may be divided among the chosen users, for example, if a member is chosen to forward a block. It is well known that the process will end fast with a consensus as there aren't many validators.

Chapter Four

Results and Discussions

Chapter 4: Results and Discussions

4.1. System configurations

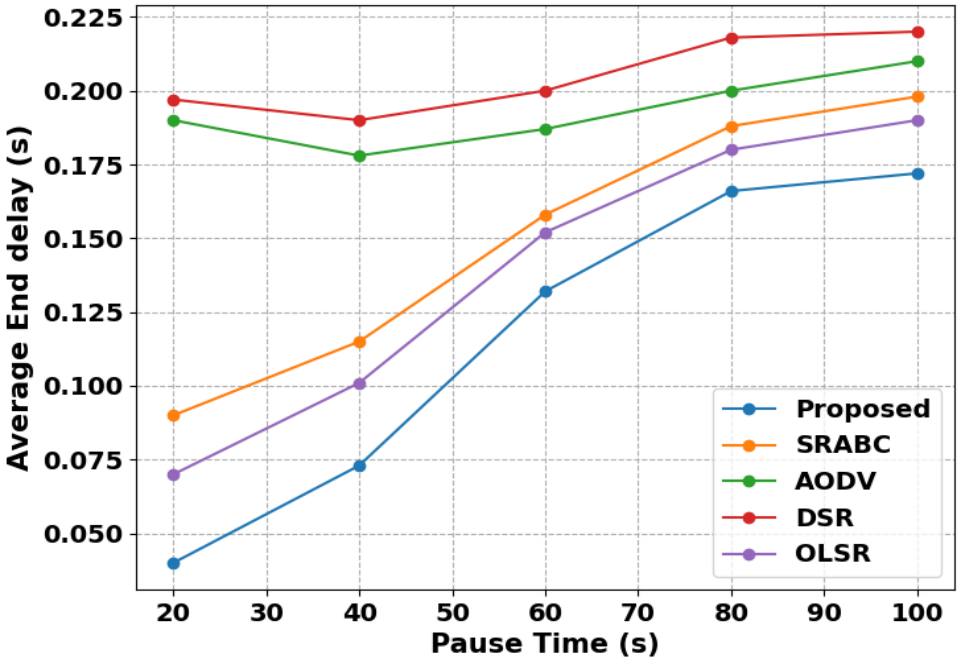
This chapter explains the performance and result comparison of the suggested approaches. The research is carried out in Python using the results of the system requirements and the simulations. For the suggested method, a total of 5 movies are gathered, whereby 20% are used for testing and the remaining 80% for instruction. The system configurations are shown in Table 4.1. Two datasets are used by the suggested method:

Table 4.1: System configurations

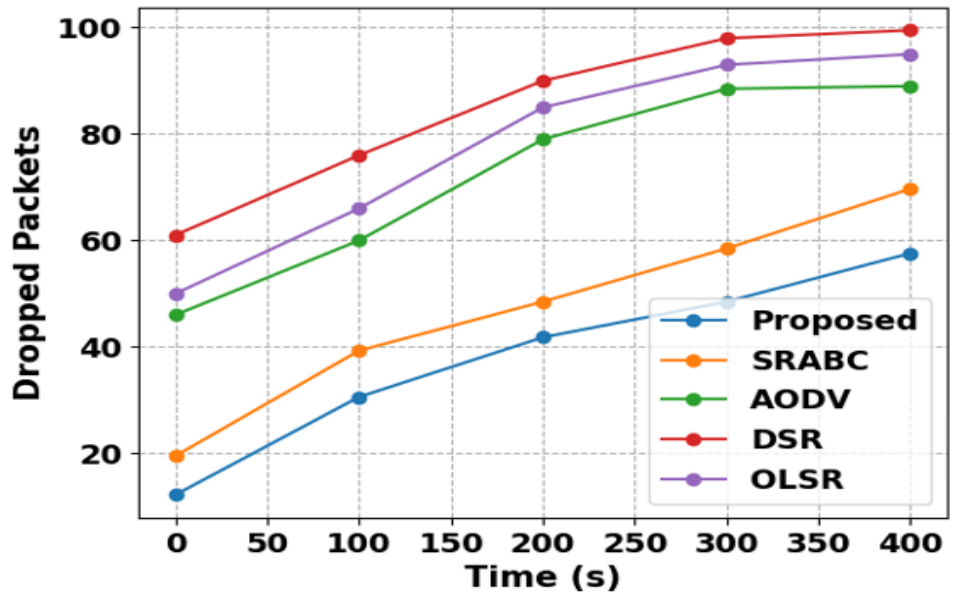
Processor	Intel® Core (TM) i3-3245 CPU@3.40Ghz 3.40 GHz
Installed memory (RAM)	4.00 GB (3.83 GB usable)
System type	64-bit Operating system
Pen and Touch	No pen or Touch Input is available for this display

4.2. Comparative Analysis with other methods

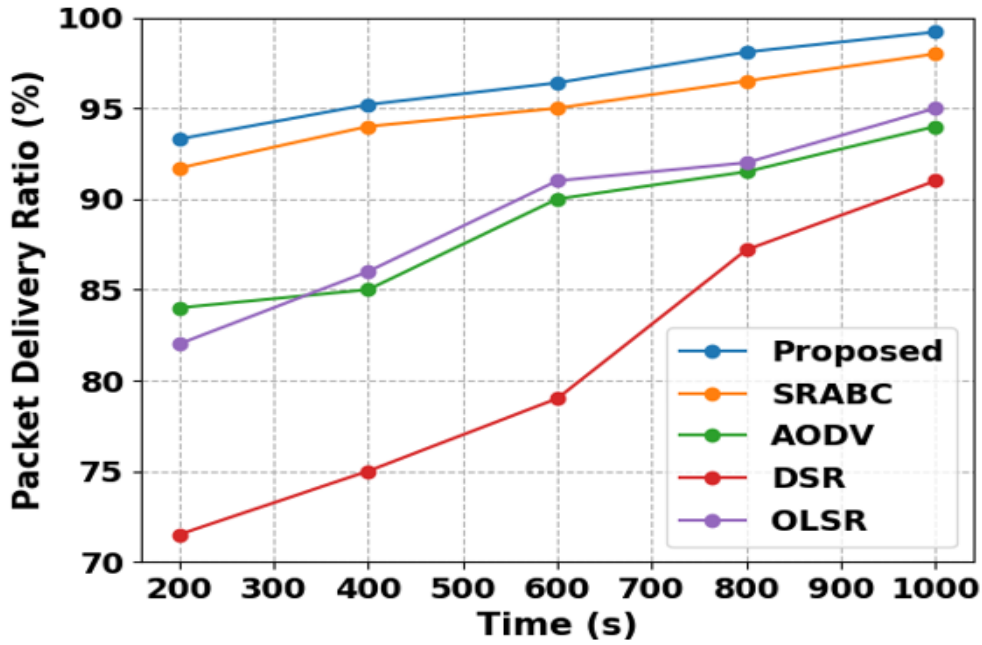
An analysis and comparison of the suggested and existing methodologies like with respect to the secure routing algorithm blockchain protect (SRABC), Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Highly Efficient Dual Authenticated Routing (HEDAR), Secured Encryption Technique with Optimum Route Discovery (SETORD), OLSR, Destination Sequenced Distance Vector (DSDV), Geographic Routing Protocol (GRP), and Hybrid Wireless Mesh Protocol (HWMP) are given in this section. A comparison of the suggested and current OLSR protocols is shown in Figures (4.1) -(4.8) To ensure the OLSR protocol's dependability, efficacy, and security in MANET implementations, validation is necessary. The OLSR protocol also strengthens security and increases performance.



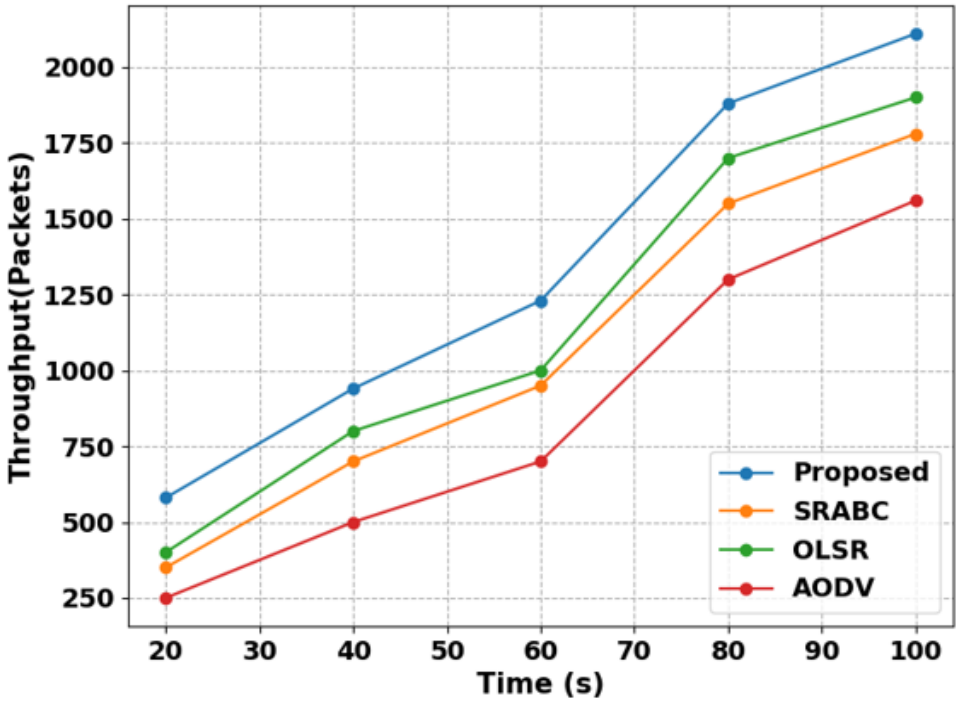
4.1 AED of proposed system and existing protocols for variant pause time



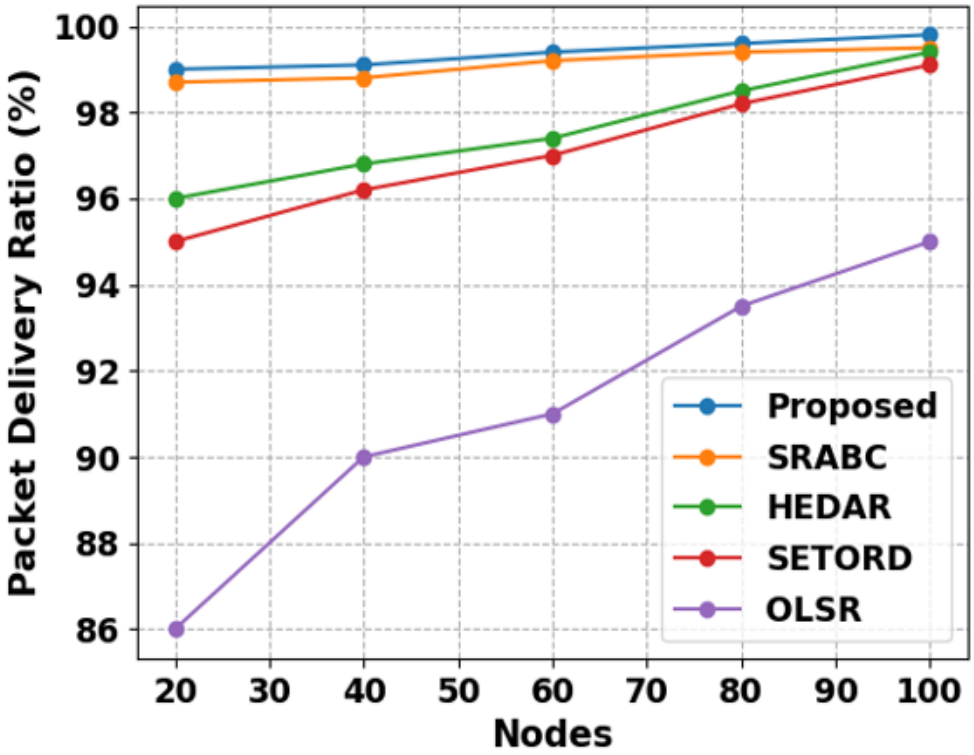
4.2 DP of proposed system and existing protocols for variant pause time



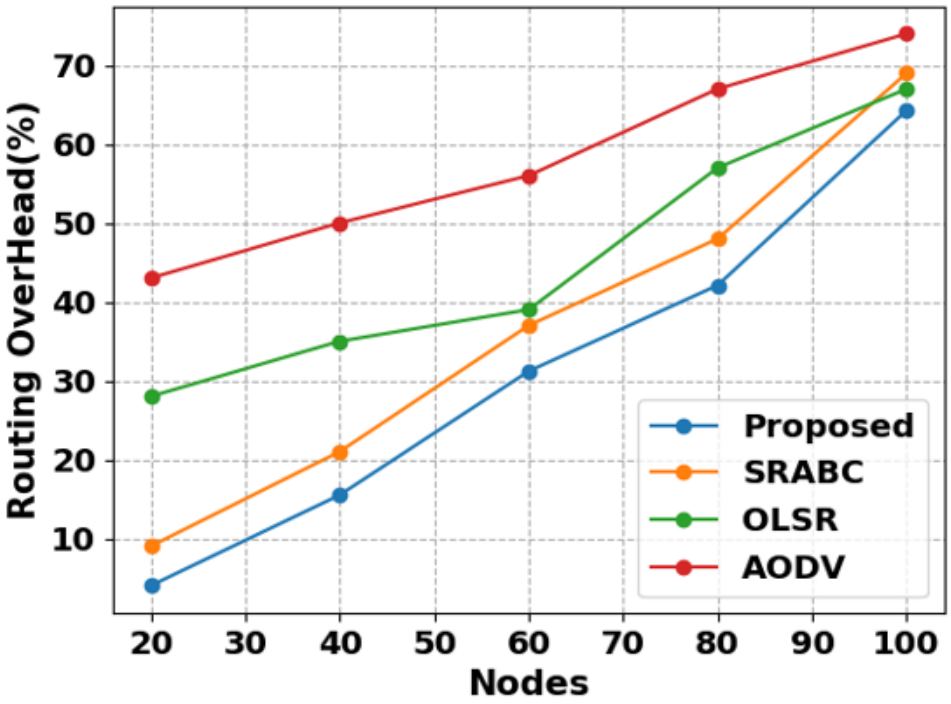
4.3 PDR of proposed system and existing protocols for variant time



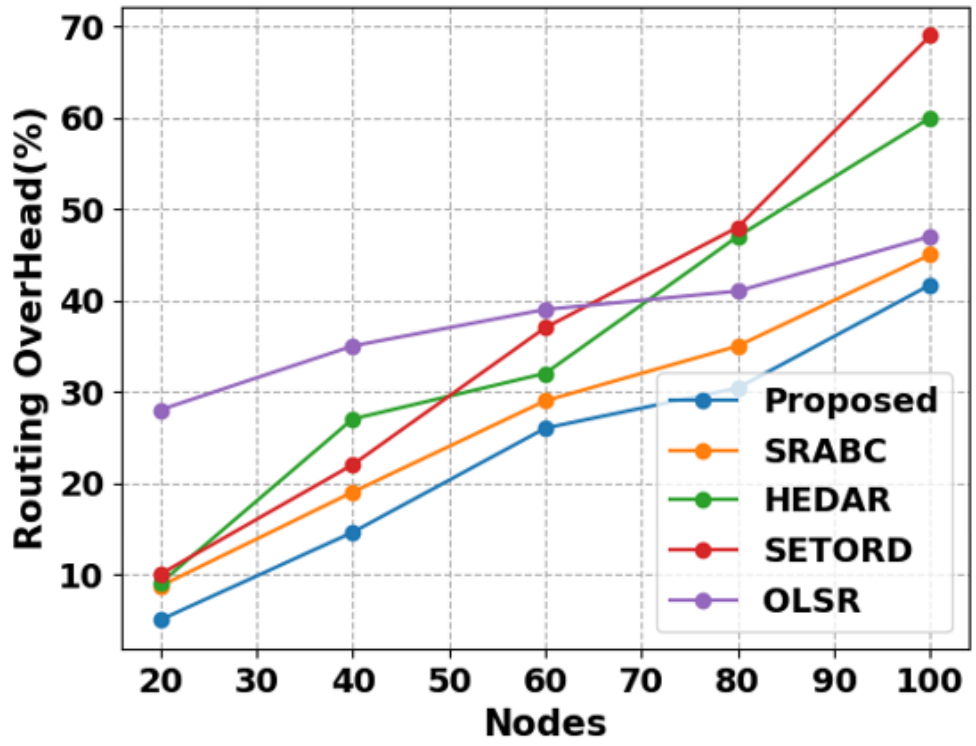
4.4 Throughput of proposed system and existing protocols for variant time



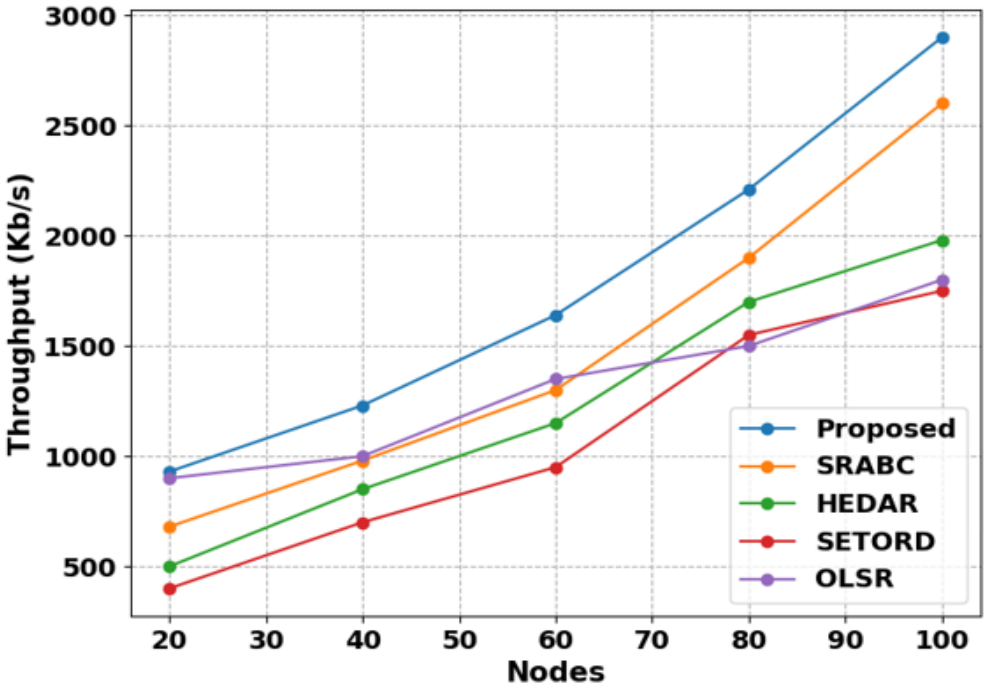
4.5 PDR of proposed system and existing protocols for variant Nodes



4.6 ROH of proposed and some existing protocols for variant Nodes



4.7 ROH of proposed and other existing protocols for variant Nodes

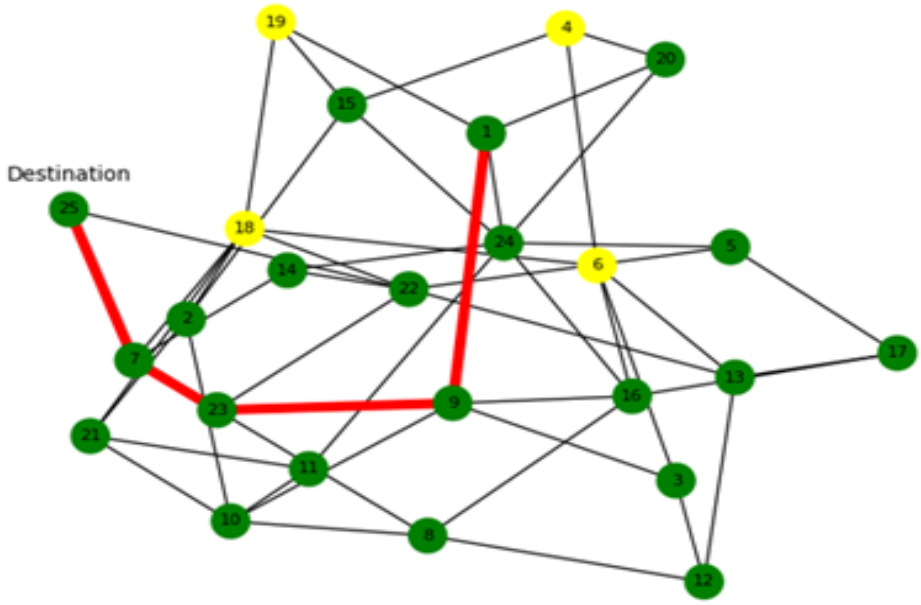


4.8 Throughput of proposed and existing protocols for variant Nodes

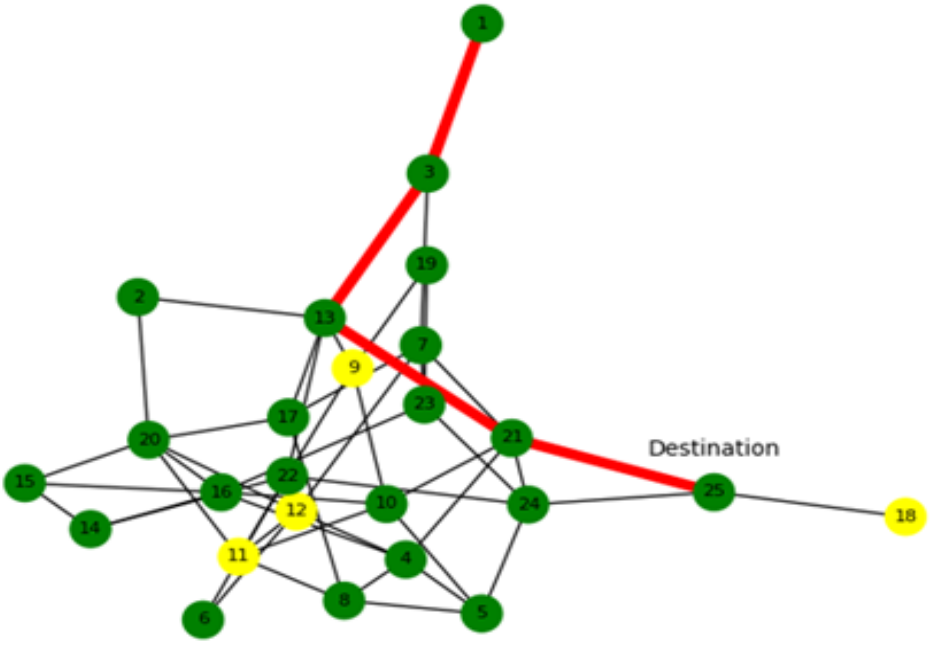
The comparison between proposed and current OLSR protocols is shown in Figures (4.1)– (4.8). Large networks with a large number of manageable nodes are present in this OLSR study. The routing solution offered by OLSR is dependable and efficient for dynamic wireless networks. Energy efficiency, scalability, low overhead, fast convergence, loop-free routing, numerous routes, and fast convergence are all features of the suggested OLSR protocol. Moreover, OLSR can be utilised in wireless networks with brief battery lives thanks to its energy-efficient design. The suggested protocol is verified by outperforming other existing protocols in every performance indicator through comparison study.

4.3. Simulation Results

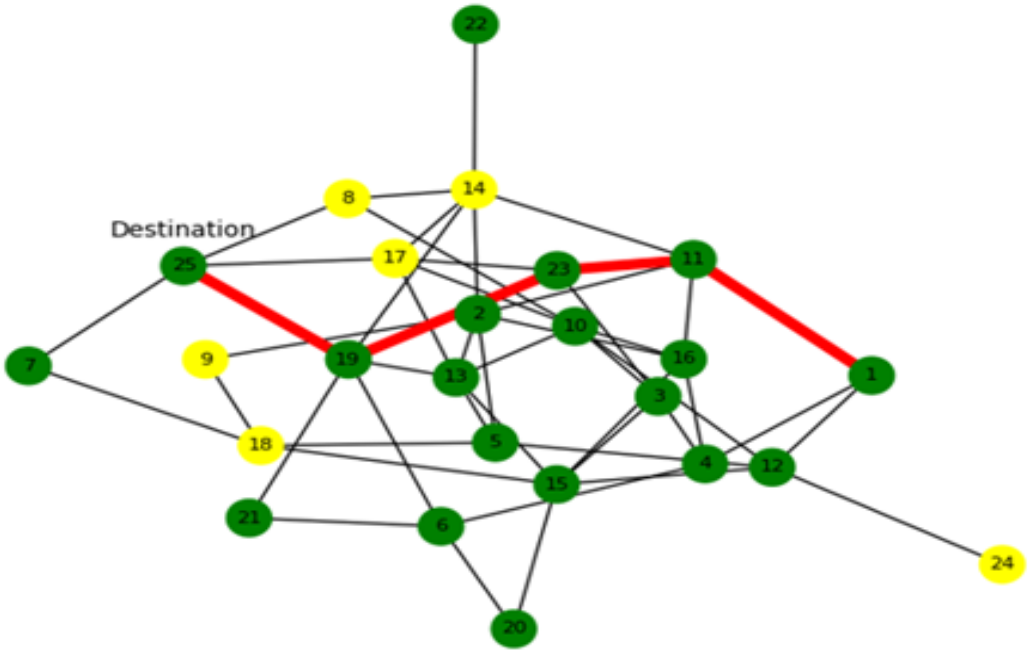
This part presents an analysis of the simulation results. Create the blockchain connection first, at random. Subsequently, nodes are identified by their respective weights, the blockchain is incorporated into the network's architecture, and communication takes place inside the MANET. A transaction across the MANET has also been completed using the most effective mode of communication. Finally, a variety of attacks have been included in the training data set, and a variety of attacks are verified in datasets through testing. Simulations are carried out to analyse the various performance metrics of the MANETs like AED, throughput of the network, DP values, ROH, PDR, and E2E delay. Analysis of the all the metrics is discussed in details in this chapter. Figure 4.9 illustrates the process of creating a MANET network node that is properly weighted.


Destination
19
4
20
15
1
25
18
24
5
14
6
22
2
17
7
13
23
9
16
21
11
3
10
8
12

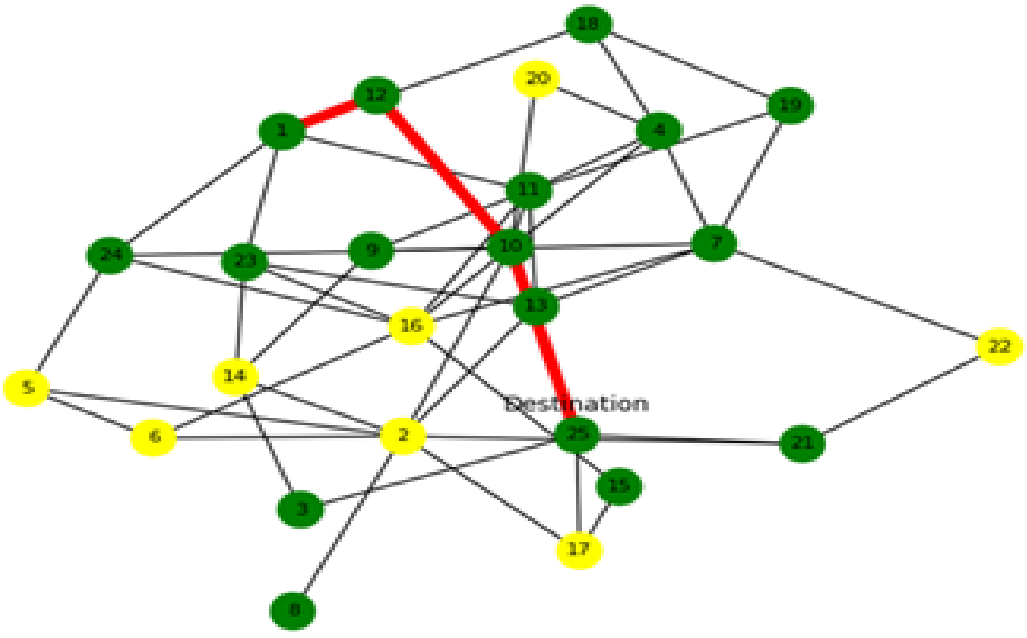
(a)


1
3
19
2
13
7
9
23
17
20
21
Destination
15
22
16
10
24
25
18
12
14
11
4
8
5
6

(b)



(c)



(d)

Figure 4.9 (a-d): Node creation in blockchain

A blockchain is used to build a node, and once the block is formed and the data hashed, each node is assigned the proper weight. Node 1 is the SN and node 25 is the DN in figure 4.9(a). The shortest pathways connect nodes 1 and 9; they also connect nodes 9 and 23; they also connect nodes 23 and 7; finally, they connect nodes 7 and 25. Transaction confirmation times and overall network performance may both benefit from this. Additionally, the shortest path computation is displayed in figures 4.9(b)–(d). Shortest path algorithms are able to swiftly recalculate routes while maintaining connectivity, allowing them to flexibly adjust to changes in network topology brought about by node mobility or link breakdowns. The shortest path algorithms are an excellent option when networks expand since they can handle larger MANETs more effective than some other routing strategies. Simulation parameters of the proposed method is are summarized in Table 4.2.

Table 4.2: Simulation parameters

Parameter	**Typical value**
Number of nodes	100
Packet Ratio	99.7
Node speed	16 ms
Maximum node speed	1-20 m/s
Data size	5MB
Pause time	100s
Size of packets	512 bytes
Topology dimensions	800m×900m
Number of malicious nodes	1-10

Network layer	Convoultional, Maxpooling, BiGru, Dropout and Dense layer.
Wireless standard and speed	MANET and 0.056sec
Mobility model	Random

By adjusting the pause time, Figure 4.10 displays the AED(s) of the suggested methods. This graph shows how, over time, the average finish delay increases with the pause time. The suggested model achieves an AED of 19.2 seconds for a pause time of 20, compared to 18.2, 14.21, and 12.34 seconds for the current SRABC, GRP, and HWMP techniques. The suggested model accomplishes in 20.5 seconds for a pause duration of 40, compared to 19.1, 15.5, and 13.4 seconds for the current approaches. The suggested model completes the task in 21.3 seconds for a pause period of 60, compared to the current techniques' 20/16.4, and 14.34 seconds. The suggested model produces in 22.6 seconds for a pause time of 80, compared to 21.2, 17.71, and 15.45 seconds for the current methods. The suggested approach achieves in 23.6 seconds for a pause period of 100, compared to the current methods' 22.18, 18.34, and 16.12 seconds. Consequently, the graph shows that the suggested method has superior E2E delay performance.

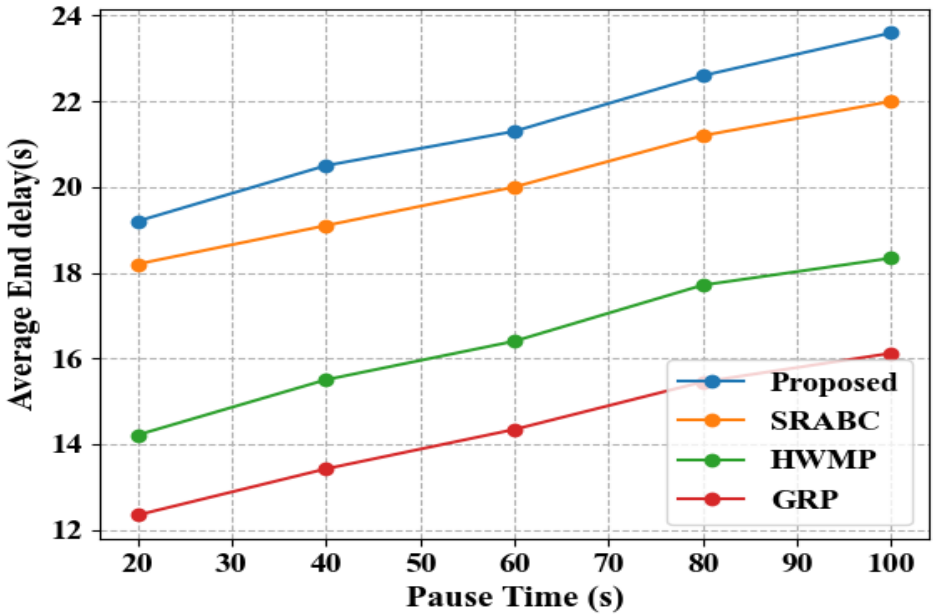


Figure 4.10: AED of proposed system by varying pause time

By altering the pause time, Figure 4.11 displays the AED(s) of the suggested and current techniques. The suggested approach achieves an AED of 0.04 seconds for a pause time of 20, compared to 0.09, 0.19, and 0.197 seconds for the current SRABC, AODV, and DSR methods. The suggested approach achieves in 0.073 seconds for a pause period of 40, compared to 0.115, 0.178, and 0.19 seconds for the current methods. The suggested approach achieves in 0.132 seconds for a pause period of 60, compared to 0.158, 0.187, and 0.2 seconds for the current methods. The suggested approach achieves in 0.132 seconds for a pause period of 60, compared to 0.158, 0.187, and 0.2 seconds for the current methods. The suggested approach achieves in 0.166 seconds for a pause time of 80, compared to 0.188, 0.2, and 0.218 seconds for the current methods. The suggested approach achieves in 0.172 seconds for a pause period of 100, compared to 0.198, 0.21, and 0.22 seconds for the current methods. Consequently, the graph shows that the suggested method has superior E2E delay performance. The suggested approach improves to 0.074 seconds for a pause period of 100,

compared to the current SRABC method's 0.198 seconds. The suggested approach improves to 0.038 seconds for a pause period of 100, compared to the current AODV method's 0.21 seconds. The proposed method enhances to 0.048 seconds for a pause period of 100, compared to 0.22 seconds for the conventional DSR method.

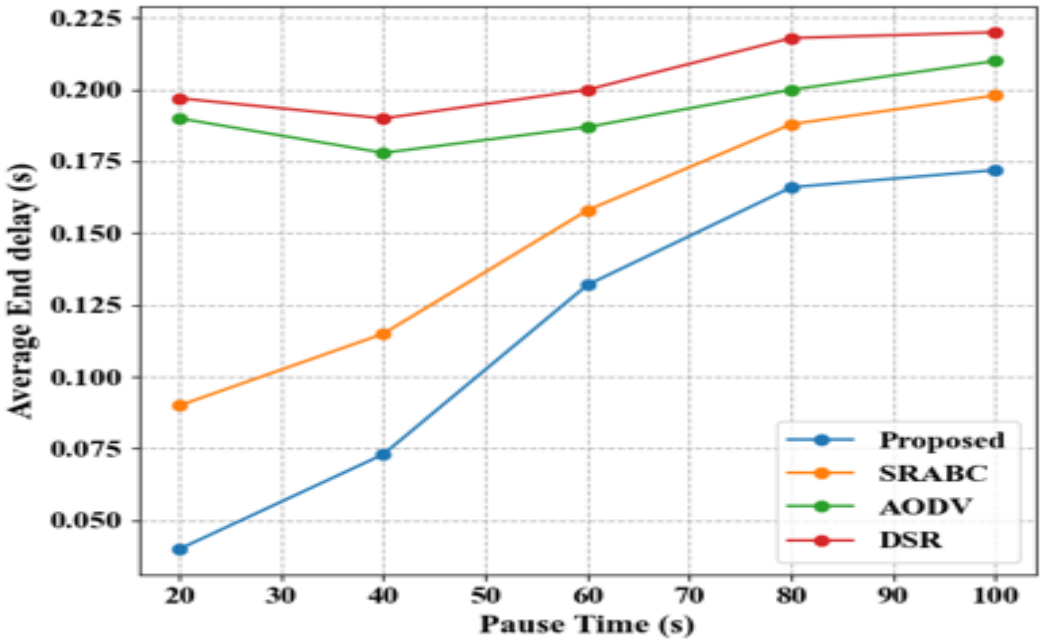


Figure 4.11: AED of proposed and other existing methods by varying pause time

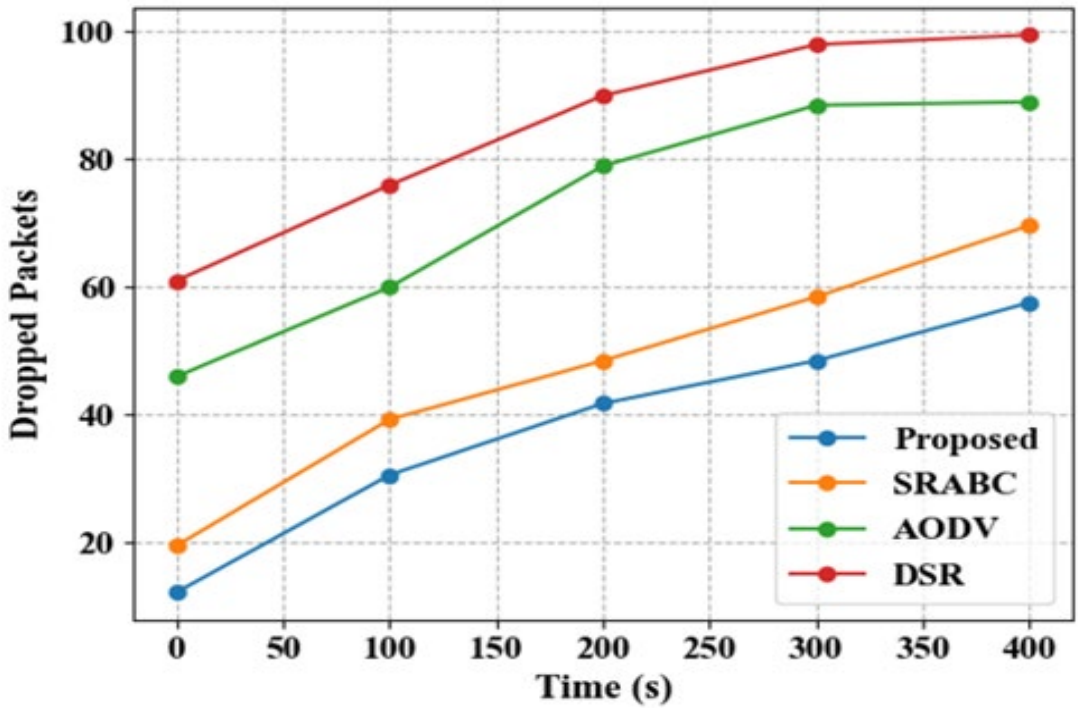


Figure 4.12: DP of proposed and existing methods by varying time

DPs from both suggested and current approaches are displayed in Figure 4.12 by changing time (s). The suggested strategy achieves 12.2 lost packets for a time of 0 sec. In contrast, the current values for AODV, DSR, and SRABC techniques are 19.5, 46, and 61. Within 100 seconds, the suggested approach accomplishes this in 30.6. In contrast, the current approaches are 39.3, 60, and 76. Within 200 seconds, the suggested approach accomplishes this in 41.8. In contrast, the current approaches yield 48.5, 79, and 90. Within 300 seconds, the suggested approach accomplishes this in 48.5. In contrast, the current approaches yield 58.5, 88.5, and 98. The suggested method achieves in 57.6 for 400 seconds. In contrast, the current approaches provide 69.7, 89, and 99.5. Thus, the produced graph demonstrates that the suggested approach attains an extremely low packet drop ratio. The suggested approach beats the current SRABC technique time of 69.7 seconds for time 400, coming in just 12.1 seconds. The suggested approach beats the current AODV technique time of 89 seconds for time 400, coming in only 31.7 seconds. The

suggested approach beats the current DSR technique time of 99.5 seconds for time 400, coming in at 41.9 seconds.

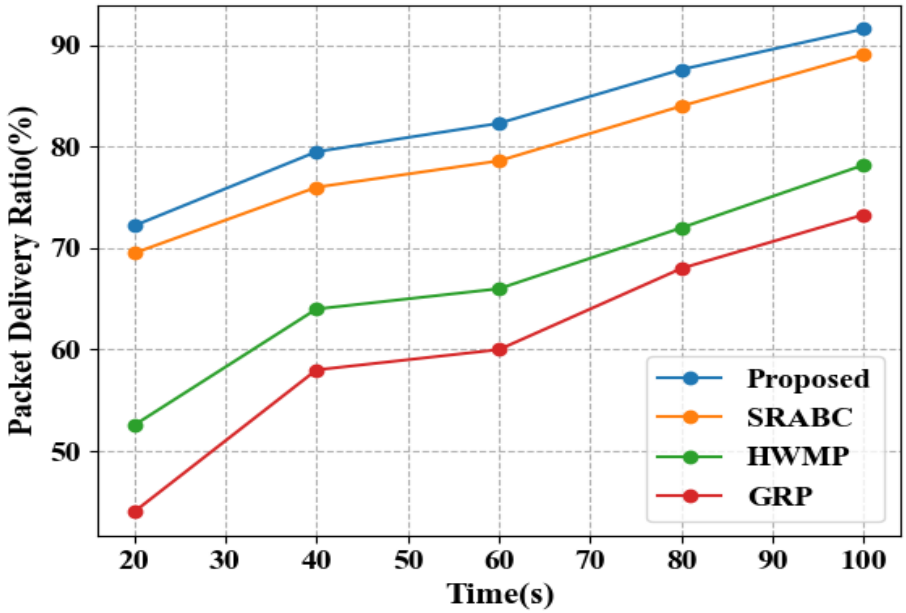


Figure 4.13: Packet delivery ratio (%) of proposed methods by varying time

The PDR (%) of the suggested approaches is displayed by changing time in Figure 4.13. The suggested method's PDR for the time of 20 is 72.2%. Whereas the current HWMP and SRABC approaches yield 52.54% and 69.5%, respectively. The suggested approach is 79.5% for the time of 40, whereas the current methods are 76%, 64%, and 58%. The suggested way is 82.3% for a time of 60, while the current approaches are 78.6%, 66%, and 60%. The suggested way is 87.6% for a time of 80, while the current approaches are 84%, 72%, and 68%. The suggested way is 91.6% for a time of 100, while the current approaches are 89.1%, 78.2%, and 73.3%. The graph unequivocally shows that, in comparison to the earlier method, the PDR achieves the maximum value.

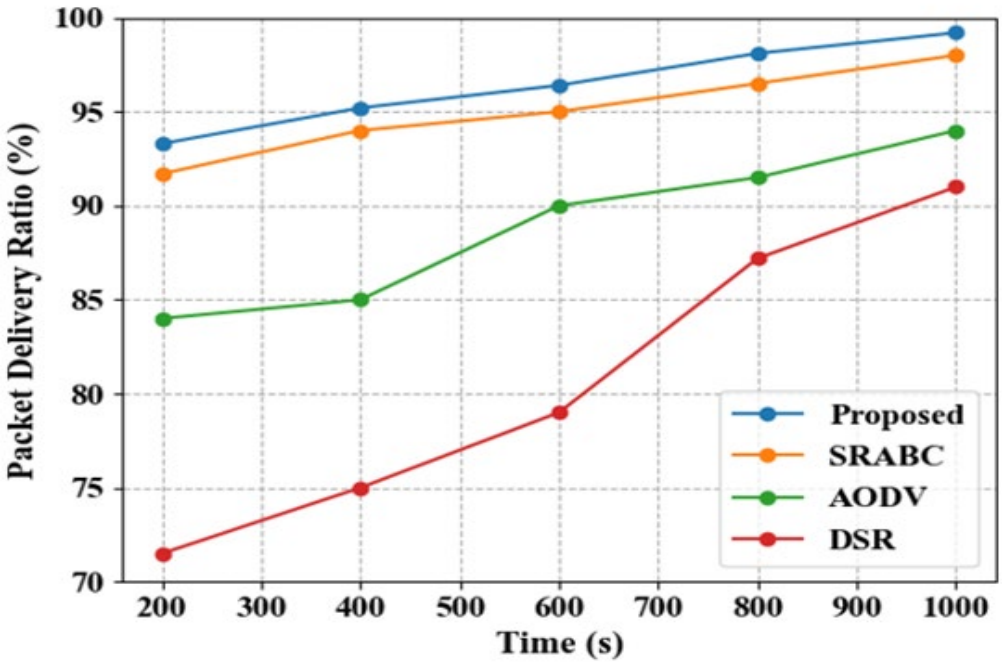


Figure 4.14: PDR (%) of proposed and existing methods by varying time

The PDR (%) of the suggested and current techniques is displayed by changing time in Figure 4.14. The suggested method's PDR is 93.3% for the time of 200. However, the current accuracy of the DSR, AODV, and SRABC techniques is 71.5%, 91.7, and 84. It is 95.2% for a time of 400 using the suggested strategy. In contrast, the current approaches are 75%, 85%, and 94%. The suggested approach is 96.4% for a time of 600. In contrast, the current approaches are 79%, 90%, and 95%. The suggested strategy is 98.1% for a time of 800. In contrast, the current approaches are 91.5%, 87.2%, and 96.5%. It is 99.1% for a time of 1000 using the suggested way. In contrast, the current approaches are 98%, 94%, and 91%. Therefore, as compared to alternative strategies, the suggested strategy yields a greater packet ratio. The suggested approach beats the current SRABC technique time of 98 seconds for time 1000, coming in only 1.2 seconds. The suggested approach reduces the time of the current AODV method, which is 94 seconds, to 5.2 seconds for time 1000. The suggested approach reduces the time of the current DSR method, which is 91 seconds, to 8.2 seconds for time 1000.

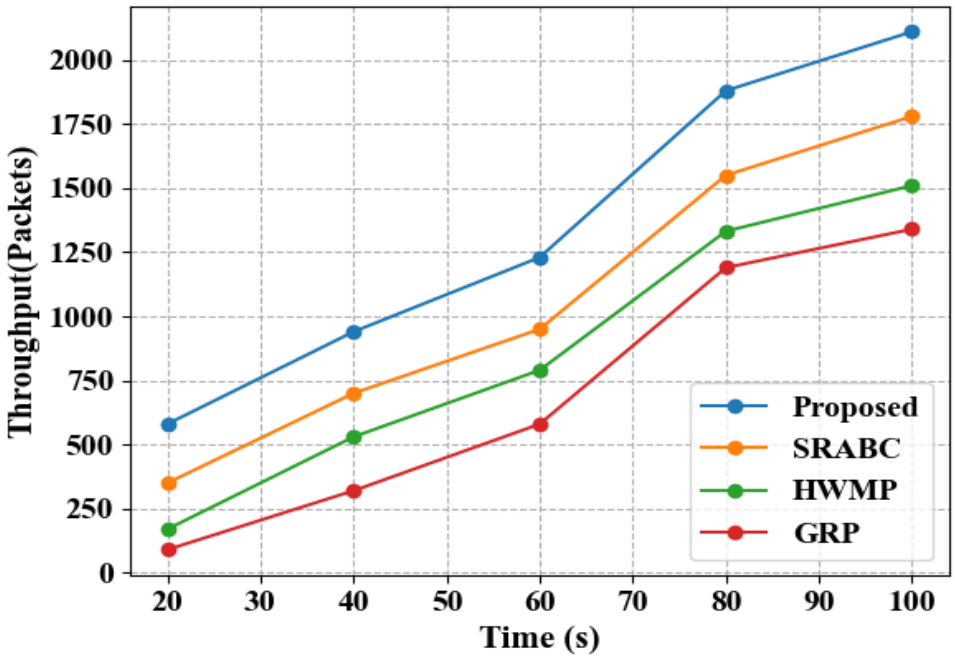


Figure 4.15: Throughput (packets) of proposed methods by varying time

The throughput (packets) of the suggested techniques is displayed by changing time in Figure 4.15. Compared to the current SRABC, HWMP, and GRP techniques, which produce throughputs of 350, 170, and 90 for a time of 20, the suggested model achieves a throughput of 580. The suggested model performs 940 times faster for a time of 40 than the current approaches, which are 700, 530, and 320. The suggested model reaches 1230 for the time of 60, compared to the 950, 790, and 580 achieved by the current approaches. In terms of time, the suggested model performs better in 1880 than the current approaches of 1550, 1332, and 1190. The suggested model performs 2110 times faster for a time of 100 than the current approaches, which are 1780, 1510, and 1340. Therefore, the suggested approach aims to lower overall overhead costs while enabling increased actual throughput. Table 4.3 shows the comparison of proposed system with already existing methods with respect to time.

Table 4.3: Comparison of proposed and existing methods for time

Packet delivery ratio (%)	**Time(s)**	**20**	**40**	**60**	**80**	**100**
	Proposed	72.2	79.5	82.3	87.6	91.6
	SRABC	69.5	76	78.6	84	89.1
	HWMP	52.54	64	66	72	78.2
	GRP	44	58	60	68	73.3
Average End Delay(s)	Pause Time	20	40	60	80	100
	Proposed	19.2	20.5	21.3	22.6	23.6
	SRABC	18.2	19.1	20	21.2	22
	HWMP	14.21	15.5	16.4	17.71	18.34
	GRP	12.34	13.42	14.34	15.45	16.12
Throughput (Packets)	Time(s)	20	40	60	80	100
	Proposed	580	940	1230	1880	2110
	SRABC	350	700	950	1550	1780
	HWMP	170	530	790	1332	1510
	GRP	90	320	580	1190	1340
Packet Delivery Ratio (%)	**Time(s)**	**200**	**400**	**600**	**800**	**1000**
	Proposed	93.3	95.2	96.4	98.1	99.2
	SRABC	91.7	94	95	96.5	98
	AODV	84	85	90	91.5	94
	DSR	71.5	75	79	87.2	91
Dropped Packets	**Time(s)**	**0**	**100**	**200**	**300**	**400**
	Proposed	12.2	30.6	41.8	48.5	57.6
	SRABC	19.5	39.3	48.5	58.5	69.7
	AODV	46	60	79	88.5	89
	DSR	61	76	90	98	99.5
Average End Delay (s)	**Pause Time**	**20**	**40**	**60**	**80**	**100**
	Proposed	0.04	0.073	0.132	0.166	0.172
	SRABC	0.09	0.115	0.158	0.188	0.198
	AODV	0.19	0.178	0.187	0.2	0.21
	DSR	0.197	0.19	0.2	0.218	0.22

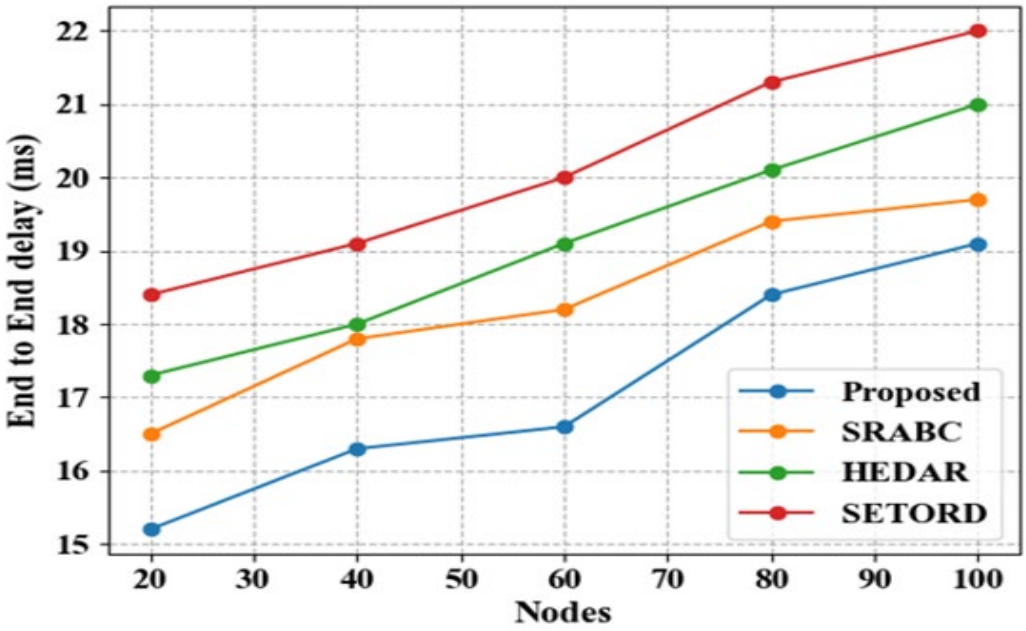


Figure 4.16: E2E of proposed and existing methods by varying Nodes

The proposed and current methods' E2E delays by different nodes are displayed in Figure 4.16. Compared to the current SRABC, HEDAR, and SETORD approaches, which achieve E2E delays of 16.5, 17.3, and 18.4 for node 20, the suggested method obtains an E2E delay of 15.2. The suggested approach achieves 16.3 for node 40, compared to the 17.8, 18, and 19.1 achieved by the current approaches. The suggested method achieves 16.6 for node 60, compared to 18.2, 19.1, and 20 for the existing methods. The suggested approach outperforms the current ones, which are 19.4, 20.1, and 21.3, for node 80, by 18.4. The suggested method obtains 19.1 for node 100, compared to 19.7, 21, and 22 for the existing methods. The figure shows that the E2E delay is negligible as compared to the previous method. The suggested approach improves to 0.6 for node 100 from the current SRABC method node of 19.7. The suggested approach increases to 1.9 for node 100, while the current HEDAR method node is 21. The suggested technique increases to 2.9 for node 100, where the current SETORD method node is 22.

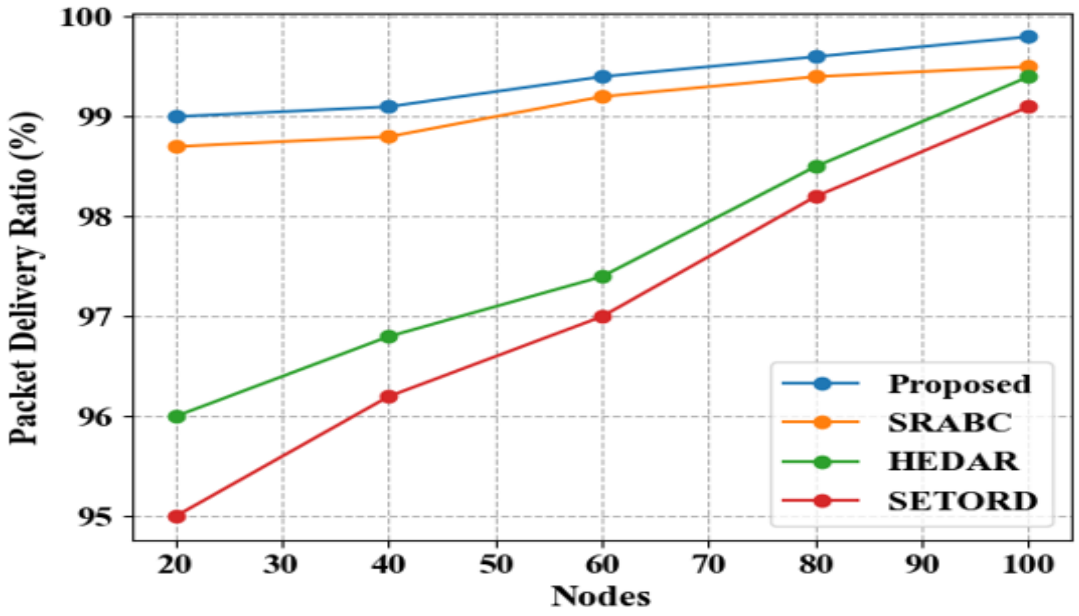


Figure 4.17: PDR (%) of proposed and existing methods by varying Nodes

The PDRs of the suggested and current approaches by different nodes are displayed in Figure 4.17. The suggested approach delivers a PDR of 99 for node 20, compared to 98.7, 96, and 95 for the current SRABC, HEDAR, and SETORD approaches. The suggested method obtains 99.1 for node 40, compared to the 98.8, 96.8, and 96.2 achieved by the existing methods. The suggested approach outperforms the current approaches, which are 99.2, 97.4, and 97, for node 60, achieving 99.4. The suggested method obtains 99.6 for node 80, compared to the 99.4, 98.5, and 98.2 achieved by the existing methods. The suggested method obtains 99.8 for node 100, compared to the 99.5, 99.4, and 99.1 achieved by the current methods. Therefore, compared to other ways, the suggested method yields better outcomes. The proposed method improves on the current SRABC method node of 99.5 to 0.3 for node 100. The proposed method improves on the current HEDAR method node of 99.4 to 0.4 for node 100. For node 100, where the present SETORD method node is 99.1, the proposed technique improves to 0.7.

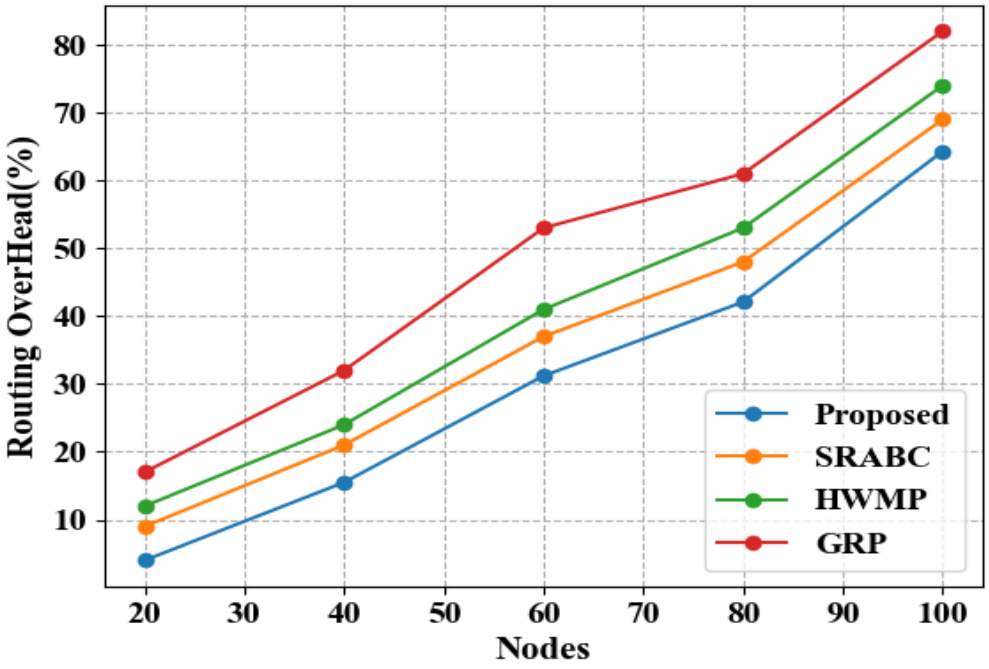


Figure 4.18: Routing overhead (%) of proposed methods by varying Nodes

The ROH (%) of the suggested techniques via different nodes is displayed in Figure 4.18. In comparison to the current SRABC, HWMP, and GRP techniques, which yield ROHs of 9, 12, and 17, the suggested model achieves a ROH of 4. The suggested model performs 15.5 times faster for time 40 than the current approach, which is 21, 24, 32. The suggested model obtains 31.2 for time 60, compared to the current method's 37, 41, and 53. The suggested model achieves 42.1 for time 80, compared to 48, 53, and 61 for the current strategy. The suggested model performs 64.3 times faster for time 100 than the current approach, which is 69, 74, and 82. The graph shows that the suggested method lowers routing expenses.

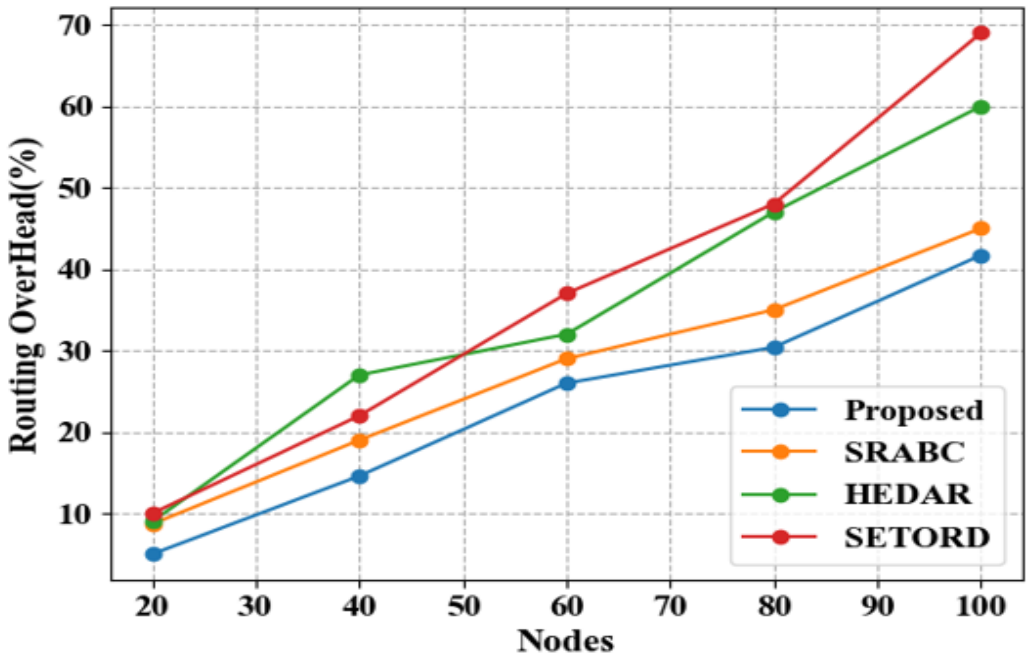


Figure 4.19: ROH of proposed and other existing methods by varying Nodes

The ROH (%) of the suggested and current approaches by different nodes is displayed in Figure 4.19. The ROH of the proposed solution is 5% for 20 nodes, compared to 8.7%, 10%, and 9% for the current SRABC, HEDAR, and SETORD systems. The suggested solution outperforms the current 19, 27, and 22 algorithms by 14.6% for 40 nodes. The suggested approach outperforms current techniques, which are 29, 32, and 37%, for 60 nodes, by 26%. The suggested solution outperforms existing methods, which are 35, 47, and 48%, for 80 nodes, by 30.4%. The suggested approach delivers 41.7% for 100 nodes compared to 45, 60, and 69% for existing approaches. Thus, the suggested technique boosts security and might allow routing to certain networks. For node 100, the recommended method rises to 3.3, although the SRABC method node at that point is 45. The proposed method outperforms the existing HEDAR method node of 60, improving to 18.3 for node 100. The proposed method improves the present SETORD method node of 69 to 27.3 for node 100.

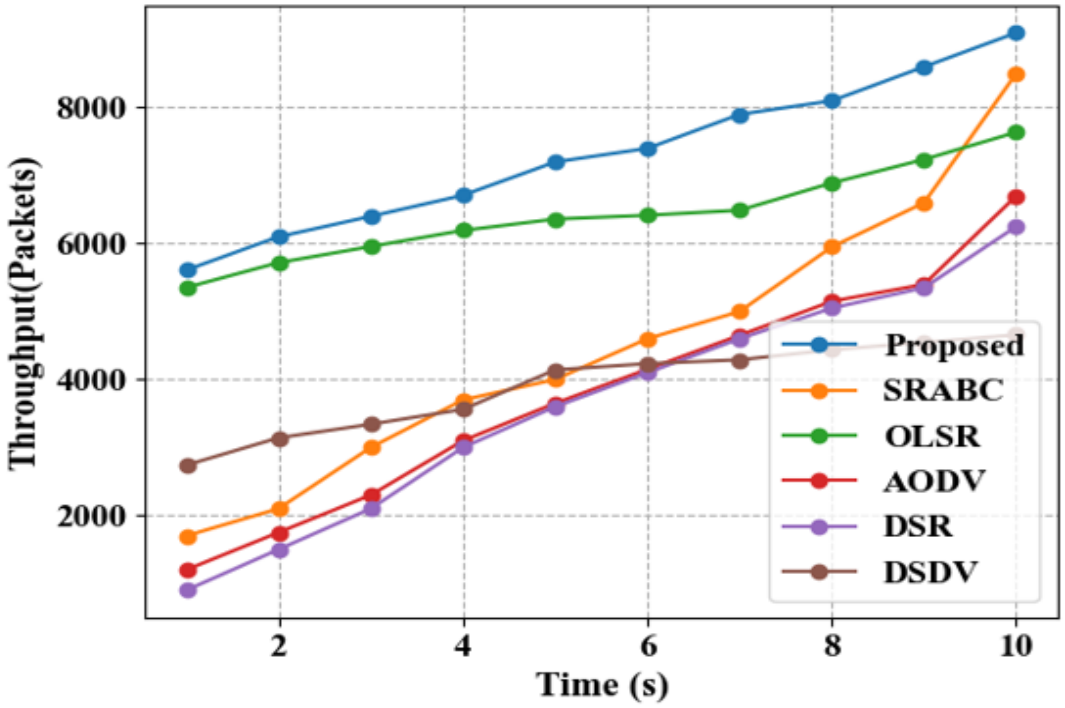


Figure 4.20: Throughput of proposed and existing methods by varying time

The throughput (packets) of the suggested and current approaches are displayed by changing time in Figure 4.20. The suggested method's throughput is 6100 for a duration of 2 seconds. On the other hand, 2100, 5719, 1750, 1500, and 3141 are the current approaches for SRABC, OLSR, AODV, DSR, and DSDV. The suggested approach for a duration of 4 seconds is 6710. On the other hand, the current approaches are 3560, 3700, 6193, 3100, and 3000. The suggested approach is 7400 for a duration of 6 seconds. In contrast, the 4600, 6415, 4150, 4100, and 4233 approaches are currently in use. The suggested approach is 8100 for a duration of 8 seconds. In contrast, the current approaches are 4436, 5950, 6891, 5150, and 5050. Proposed technique 9100 is for a period of 10 seconds. In contrast, the techniques now in use include 8500, 7637, 6700, 6250, and 4656. As a result, the suggested technique provides an efficient transmission rate along with increased throughput. A summary of throughput (packets) time is presented in Table 4.4.

Table 4.4: Analysis of Throughput (packets) time.

Throughput (Packets)	Time (s)	2	3	4	5	6	7	8	9	10
	Proposed	6100	6400	6710	7200	7400	7900	8100	8600	9100
	SRABC	2100	3000	3700	4000	4600	5000	5950	6600	8500
	OLSR	5719.18	5956.02	6193.41	6359.54	6415.3	6489.48	6891.27	7237.06	7637.46
	AODV	1750	2300	3100	3650	4150	4650	5150	5400	6700
	DSR	1500	2100	3000	3600	4100	4600	5050	5350	6250
	DSDV	3141.67	3341.94	3560.35	4141.62	4233.52	4289.28	4436.71	4546.72	4656.69

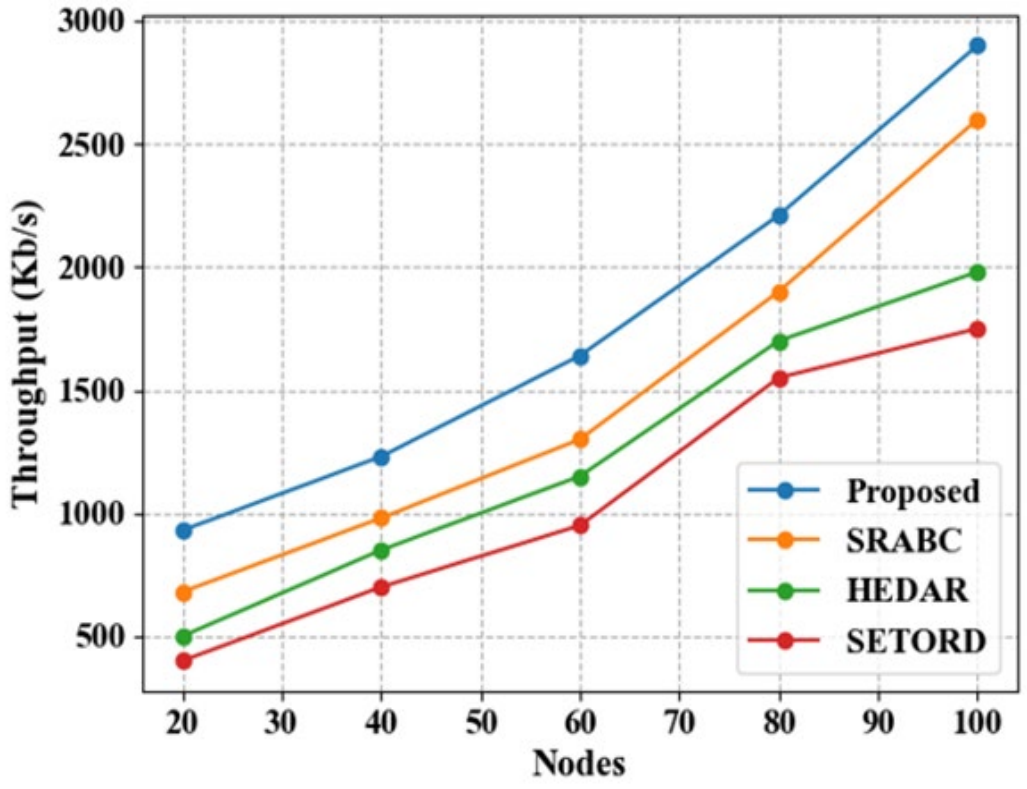
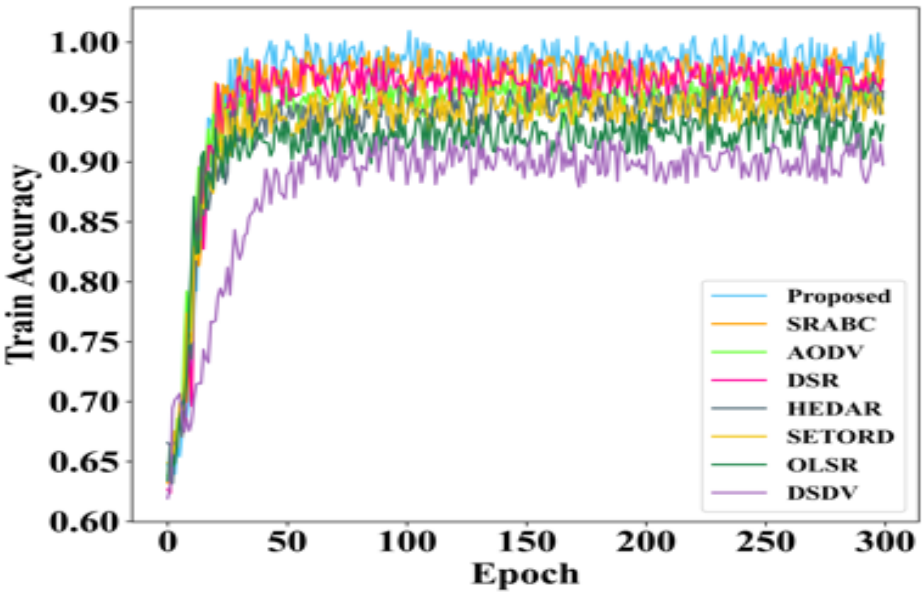


Figure 4.21: Throughput of proposed and existing methods by varying Nodes

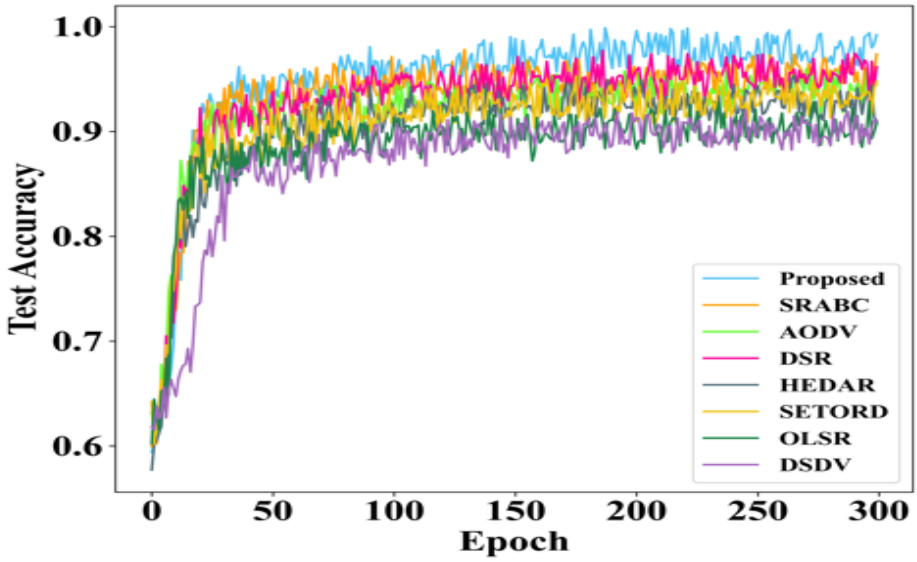
The throughput (Kb/s) of the suggested and current approaches via different nodes is displayed in Figure 4.21. The suggested method's throughput is 930 for 20 nodes. As opposed to the current 680, 500, and 400 SRABC, HEDAR, and SETORD techniques. The suggested procedure for 40 nodes is 1230. In contrast, the current approaches are 980, 850, and 700. The proposed approach is 1640 for 60 nodes. In contrast, the current approaches are 950, 1150, and 1300. 2210 is the suggested technique for 80 nodes. In contrast, the approaches used now are 1900, 1700, and 1550. The recommended approach is 2900 for 100 nodes. On the other hand, the current approaches are 1750, 1980, and 2600. As a result, the suggested approach increases throughput over the earlier ones. The analysis nodes of the suggested and current approaches are displayed in Table 4.5. The suggested approach improves to 300 for node 100 from the current SRABC method node of 2600. The suggested approach increases to 920 for node 100 from the 1980 HEDAR technique node that is currently in use. The suggested technique improves to 0.7 for node 100, where the current SETORD technique node is 99.1.

Table 4.5: Comparison of Proposed and existing methods for Nodes

Routing Overhead	Nodes	20	40	60	80	100
	Proposed	4	15.5	31.2	42.1	64.3
	SRABC	9	21	37	48	69
	HWMP	12	24	41	53	74
	GRP	17	32	53	61	82]
Throughput (Kb/s)	Nodes	20	40	60	80	100
	Proposed	930	1230	1640	2210	2900
	SRABC	680	980	1300	1900	2600
	HEDAR	500	850	1150	1700	1980
	SETORD	400	700	950	1550	1750
Packet Delivery Ratio (%)	Nodes	20	40	60	80	100
	Proposed	99	99.1	99.4	99.6	99.8
	SRABC	98.7	98.8	99.2	99.4	99.5
	HEDAR	96	96.8	97.4	98.5	99.4
	SETORD	95	96.2	97	98.2	99.1
End To End Delay (ms)	Nodes	20	40	60	80	100
	Proposed	15.2	16.3	16.6	18.4	19.1
	SRABC	16.5	17.8	18.2	19.4	19.7
	HEDAR	17.3	18	19.1	20.1	21
	SETORD	18.4	19.1	20	21.3	22
Routing Overhead (%)	Nodes	20	40	60	80	100
	Proposed	5	14.6	26	30.4	41.7
	SRABC	8.7	19	29	35	45
	HEDAR	9	27	32	47	60
	SETORD	10	22	37	48	69



(a)

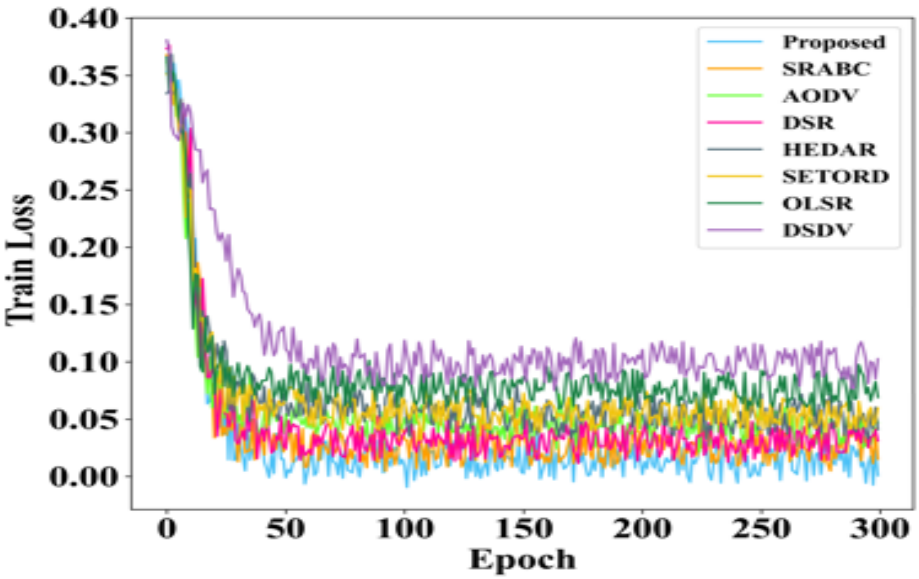


(b)

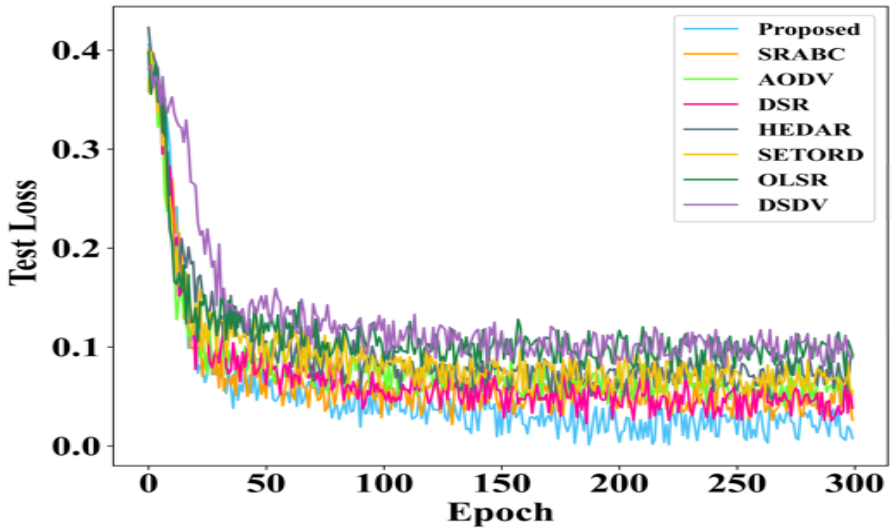
Figure 4.22: (a) training accuracy (b) testing accuracy

The accuracy of training and testing current and suggested approaches for various epoch values is displayed in Figure 4.22. The accuracy of the suggested method grows up to 50 epochs during the training stage. Then, there is a dramatic increase precisely up to the hundredth iteration, and then climb to the 150th epoch. For the suggested strategies, the training accuracy

stays consistent between 250 and 300 epochs after 200. Additionally, there is a progressive increase in accuracy up to the 100th epoch during the assessment of the accuracy level, followed by a dramatic surge up to the 200th epoch. For the suggested methodologies, the testing accuracy is constant between 250 and 300 epochs after 200. As a result, the suggested method works since more repetitions lead to higher accuracy and better results.



(a)



(b)

Figure 4.23: (a) Training loss (b) testing loss

The training and testing losses of the suggested approaches for various epoch values are displayed in Figure 4.23. The loss of the suggested approach falls up to 50 epochs during the training phase. After epoch values 100, there is a dramatic dip in the loss value, followed by epoch values 150 to 200, and then epoch values 250 to 300, when the loss value stays constant. Thus, the suggested approach shows superior results when compared to the training and testing loss values.

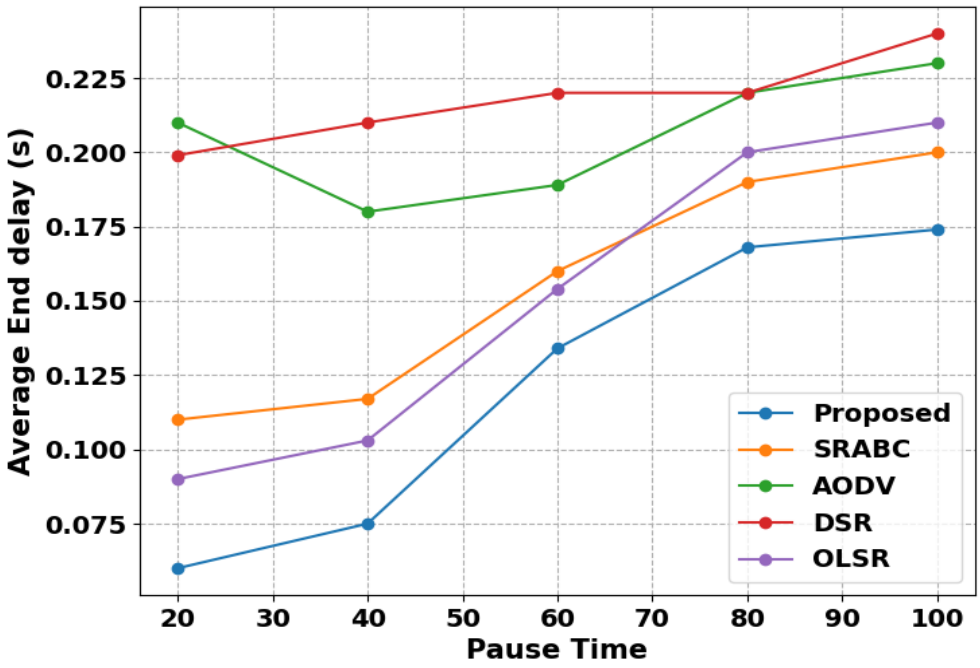


Figure 4.24: AED with 4 videos for training and 1 for testing by varying time

With four training films and one testing video, Figure 4.24 compares the suggested and existing method. The proposed method achieves 0.06 seconds for pause time 20, compared to 0.11, 0.21, 0.199, and 0.09 seconds for the current SRABC, AODV, DSR, and OLSR approaches. The suggested approach is 0.134 seconds for pause time 60, compared to the current methods of 0.16, 0.189, 0.22, and 0.154 seconds. The suggested approach is 0.174

seconds for pause time 100, compared to the current methods of 0.2, 0.23, 0.24, and 0.21 seconds. As a result, the suggested method requires less processing time than the current ones.

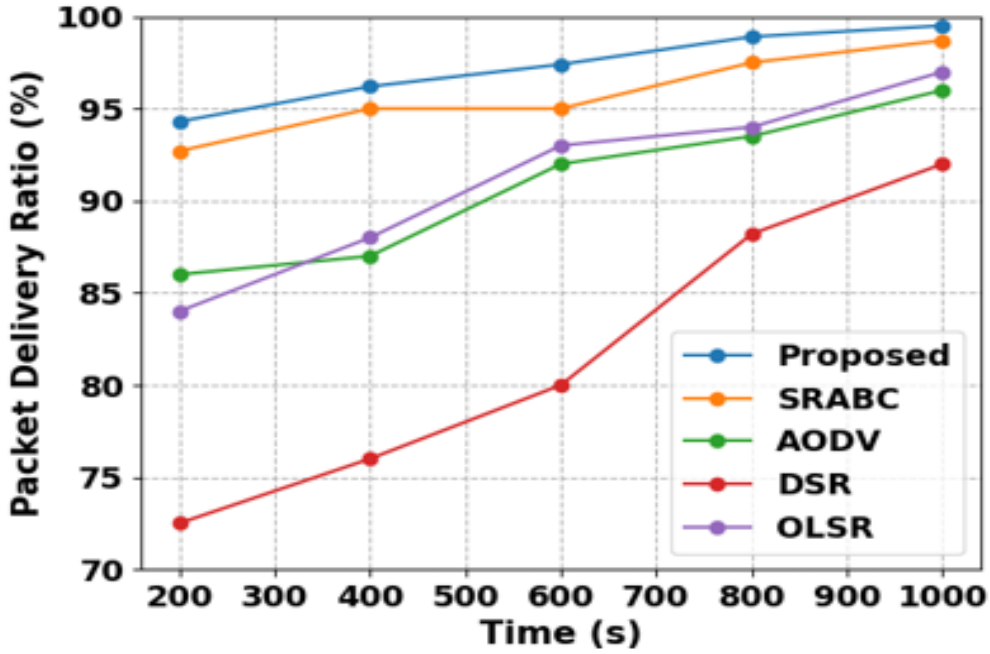


Figure 4.25: PDR with 5 videos for training and 2 for testing by varying time

With five training films and two testing movies, Figure 4.25 compares the suggested and existing methods. Compared to the existing SRABC, AODV, DSR, and OLSR approaches, which obtain 92.7, 86, 72.5, and 84 seconds for time 200, the suggested method achieves 94.3 seconds. The suggested approach is 96.2 seconds for pause time 400, compared to the existing ways of 95, 87, 76, and 88 seconds. The suggested approach is 98.9 seconds for pause time 800, which is less than the existing ways of 97.5, 93.5, 88.2, and 94 seconds. The suggested way for pause time 1000 is 99.5 seconds, while the current approaches are 98.7, 96, 92, and 97 seconds. The current approaches entail growing the network, which results in congestion and decreased network efficiency. Furthermore, the suggested approach yields a superior outcome.

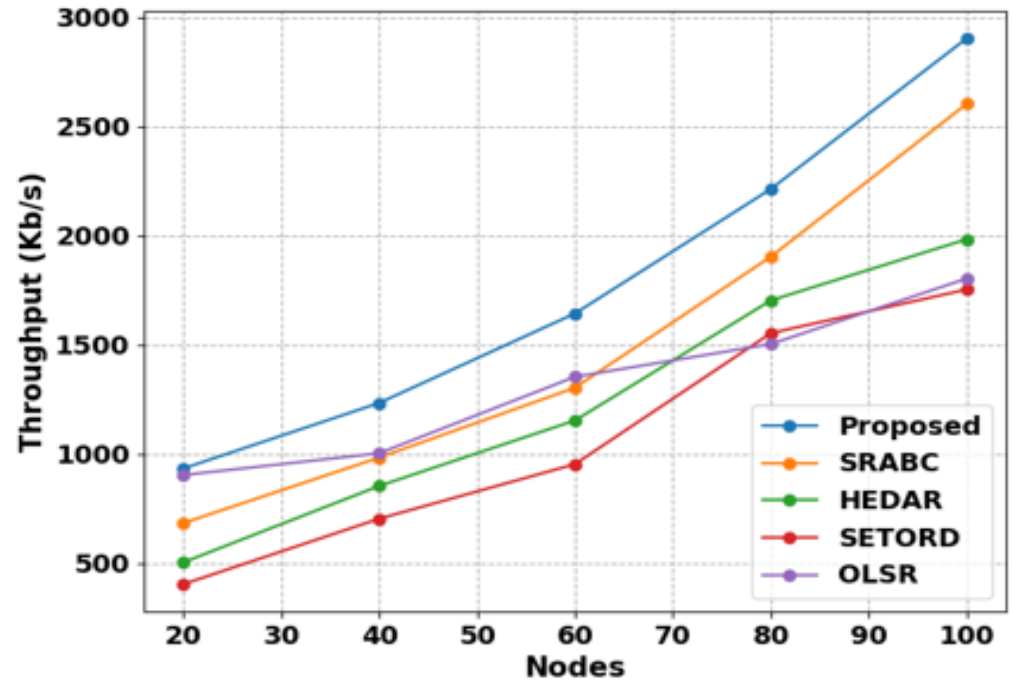


Figure 4.26: Throughput with 6 videos for training and 3 for testing by varying Nodes.

Figure 4.26 compares the suggested and current methods using three testing and six training movies. The suggested approach for node 20 achieves 932 seconds, compared to 682, 502, 402, and 902 for the current SRABC, HEDAR, SETORD, and OLSR techniques. The suggested approach, 1232, is superior to the current ones, 982, 852, 702, and 1002, for 40 nodes. The suggested approach, 2212, is superior to the current ones, 1902, 1702, 1552, and 1502 for 80 nodes. The suggested approach, 2902, is superior to the current methods, 2602, 1982, 1752, and 1802 for pause time 100. More data is required for the current models to be trained than for the suggested approach. The results of further video training and testing by changing time and nodes are displayed in Table 4.6.

Table 4.6: Values of additional videos are training and testing by varying time and Nodes

	Nodes	**20**	**40**	**60**	**80**	**100**
Average End Delay	**Proposed**	0.06	0.075	0.134	0.168	0.174
	SRABC	0.11	0.117	0.16	0.19	0.2
	AODV	0.21	0.18	0.189	0.22	0.23
	DSR	0.199	0.21	0.22	0.22	0.24
	OLSR	0.09	0.103	0.154	0.2	0.21
packet delivery ratio	**Proposed**	**94.3**	**96.2**	**97.4**	**98.9**	**99.5**
	SRABC	92.7	95	95	97.5	98.7
	AODV	86	87	92	93.5	96
	DSR	72.5	76	80	88.2	92
	OLSR	84	88	93	94	97
Throughput	**Proposed**	**932**	**1232**	**1642**	**2212**	**2902**
	SRABC	682	982	1302	1902	2602
	HEDAR	502	852	1152	1702	1982
	SETORD	402	702	952	1552	1752
	OLSR	902	1002	1352	1502	1802

4.4. Summary

In this chapter, a detailed results and discussion of the proposed system is presented. The characteristics of deep learning-based security detection techniques are examined in this chapter, which could help MANETs create situation-appropriate solutions. After gathering the input videos, the suggested study found blackhole nodes that, under some circumstances, behave differently from other nodes. Such traits can be efficiently recognised by this straightforward detection approach. Next, data and network trust levels are evaluated using trust value in order to detect attacks and provide security fixes. Then, to reduce network-related traffic data, the OLSR protocol offers a useful routing method that is used in MANETs. Subsequently, the OSPREY optimisation technique adjusted the parameters, such as the degree of node and link stability. Blockchain storage is thus made possible via IPFS technology, enhancing the security of MANET data for file and application exchange. Finally, the system's greater consensus, which produces an improved delegation limit, makes the validation process using the DPoS approach practicable. In terms of 0.172 (AED), 57.6 (DP), 99.8

(PDR), 19.1 E2E delay, 41.7 (ROH), and 9100 throughputs, the suggested model performs better.

Chapter Five

Conclusions and Future Works

Chapter 5: Conclusions and Future Works

5.1. Introduction

This chapter presents the conclusions drawn from the dissertation. It also covers interesting aspects that can be explored in the future and suggests some of the best directions to continue work on this problem.

5.2. Conclusions

This dissertation makes a substantial contribution to addressing the complex challenges associated with secure and efficient video transmission over Mobile Ad Hoc Networks (MANETs). By integrating advanced deep learning techniques and blockchain technology, the proposed system offers a novel and effective approach to overcoming the inherent issues of security vulnerabilities, performance limitations, and node mobility that characterize MANET environments. These challenges are particularly pronounced in scenarios where large-scale multimedia data, such as video streams, are transmitted over dynamically changing networks.

A core contribution of this work is the development and deployment of a deep learning-based mechanism for identifying and mitigating blackhole attacks, which are a significant security threat to MANETs. Blackhole nodes, which maliciously drop packets and disrupt network performance, are detected using a novel deep learning model Twin-Attention based Dense Convolutional Bidirectional Gated Network (SA_DCBiGNet). This model enhances the ability to accurately identify these malicious nodes, thus improving the overall security and stability of the network. The accuracy and efficiency of this deep learning model provide a key advantage in maintaining network reliability and continuity, especially in high-demand applications like video streaming.

In addition to security improvements, this research also introduces the Extended Osprey-aided Optimized Link State Routing Protocol (EO_OLSRP), which incorporates trust-based mechanisms to evaluate and select optimal routing paths. The protocol enhances the Packet Delivery Ratio (PDR) by ensuring that only trustworthy nodes participate in data transmission. The use of trust values adds an extra layer of security to routing decisions, thereby minimizing transmission errors and improving overall network reliability. Moreover, the routing protocol is optimized through the Osprey Optimization Algorithm (OOA), which evaluates node and link stability to select the most efficient routes. This dual approach of trust-based routing and optimization ensures better network performance in terms of reduced packet loss, enhanced throughput, and lower delays.

A major advancement in this dissertation is the integration of blockchain technology to secure data transmission within MANETs. Blockchain, particularly through the use of the Interplanetary File System (IPFS) for decentralized data storage and the Delegated Proof of Stake (DPoS) consensus mechanism, provides a robust solution to the challenges of data integrity and security. The combination of IPFS and DPoS ensures that data remains tamper-resistant and secure, even in the face of frequent node mobility. This decentralized approach to data storage significantly reduces the risk of unauthorized access or manipulation, a common concern in traditional MANET environments.

The performance of the proposed system was rigorously tested and evaluated under various network conditions. Using the NS3 simulator, the system was assessed based on critical performance metrics such as PDR, throughput, end-to-end delay (E2E), and routing overhead (ROH). The results demonstrated that the proposed system outperformed existing routing protocols across all key performance indicators. For instance, with 100 nodes,

the proposed system achieved a PDR of 99.8%, a throughput of 2900 Kb/s, and an end-to-end delay of 19.1 milliseconds. These metrics are significantly higher compared to traditional routing protocols such as SRABC, HEDAR, and SETORD, which struggle to maintain performance under similar network conditions.

Specifically, the proposed system achieved superior performance in several areas:

- **Packet Delivery Ratio (PDR)**: The system maintained a PDR of 99.8%, demonstrating its efficiency in ensuring that video packets reach their destination with minimal loss. This is a critical metric for maintaining video quality and ensuring continuous streaming, especially in environments with high node mobility.
- **Throughput**: The system delivered a throughput of 2900 Kb/s, outperforming alternative methods like SRABC, which achieved lower throughput under the same conditions. High throughput is essential for ensuring smooth video playback, and the proposed system excels in this regard by effectively managing bandwidth and network resources.
- **End-to-End Delay**: The proposed system reduced E2E delay to 19.1 milliseconds, a crucial improvement that ensures minimal lag during video streaming. This reduction in delay significantly enhances the user experience, particularly in real-time applications where low latency is essential.
- **Routing Overhead (ROH)**: With a routing overhead of 64.3%, the proposed system demonstrates an optimized balance between performance and resource utilization. This metric highlights the efficiency of the system in maintaining high network performance without overwhelming the network with excessive routing information.

Beyond these performance metrics, the proposed system also offers enhanced security and data integrity through its integration of blockchain technology. The use of the IPFS for decentralized storage ensures that data is securely stored and transmitted without the risk of being tampered with. The DPoS consensus mechanism further adds to the system's reliability by ensuring that only authorized nodes are allowed to validate and store data. This combination of decentralized storage and secure consensus provides a highly robust and secure data transmission environment, which is critical in applications where the confidentiality and integrity of video data are paramount.

The comprehensive evaluation of the proposed system, including comparative analysis with established protocols such as SRABC, HEDAR, and SETORD, clearly demonstrates the superiority of the system. The proposed deep learning and blockchain-enabled routing protocol not only outperforms traditional methods in terms of PDR, throughput, and delay but also significantly enhances the security and stability of MANETs. This is particularly important in scenarios where high-quality video streaming is required, such as in military operations, emergency response systems, and real-time surveillance applications.

In conclusion, this research provides a holistic solution to the challenges of video transmission over MANETs. By combining deep learning techniques for security with blockchain technology for data integrity, the proposed system ensures secure, efficient, and reliable video streaming in highly dynamic environments. The research not only advances the state-of-the-art in MANET routing protocols but also sets the stage for further innovations in secure video transmission over decentralized networks. This work demonstrates that the integration of deep learning and blockchain can lead to

significant improvements in both performance and security, addressing long-standing challenges in the field of MANETs.

5.3. Future Works

As part of the ongoing development and future enhancements of the proposed system, several key areas will be explored to further expand its capabilities and address a broader range of challenges within Mobile Ad Hoc Networks (MANETs) and beyond.

- **Expansion of Attack Detection**

  The current system's attack detection mechanism, focused primarily on identifying blackhole attacks, will be extended to detect a wider array of network-based threats. By incorporating additional criteria and enhancing the deep learning model, the system will be capable of identifying a more diverse set of security threats, including denial-of-service (DoS) attacks, sybil attacks, and wormhole attacks, thereby providing a more robust security framework for MANET environments.

- **Optimization of Data Packet Transfer in Large-Scale Networks**

  To ensure optimal performance in large-scale MANET deployments, the proposed method will be refined to further improve the quality of links between mobile nodes. This enhancement will focus on ensuring that data packet transfers remain efficient even in networks with high node densities and complex topologies. The system will be equipped to handle the increased data traffic without sacrificing performance, providing seamless communication in more extensive network setups.

- **Enhancing Node Connectivity for Greater Network Longevity**

  Improved node connectivity is crucial for maintaining network stability and extending the lifespan of the network. Future iterations of the system will focus on optimizing node relationships to achieve better connectivity, which will, in turn, increase the network's capacity and durability. This will involve fine-tuning the trust-based routing mechanisms to ensure more resilient and stable connections, particularly in highly dynamic environments with frequent node mobility.

- **Utilization of Advanced Optimization Techniques**

  To further enhance the performance of the proposed system, advanced optimization techniques such as genetic algorithms and particle swarm optimization will be explored to optimize the hyperparameters of the deep learning models used for routing and security. These optimization techniques will enable the system to dynamically adjust its parameters for varying network conditions, improving its adaptability and performance in real-time scenarios.

- **Evaluation in Other Wireless Network Types**

  The versatility of the proposed system will be tested by adapting and evaluating its performance in other types of wireless networks, such as Vehicle Ad Hoc Networks (VANETs). Given the similarities between MANETs and VANETs, particularly in terms of node mobility and network dynamics, the system’s attack detection, routing optimization, and blockchain security mechanisms will be tested in vehicular environments to ensure applicability across different wireless network paradigms.

References

[1] I. H. Sarker, M. M. Hoque, Md. K. Uddin, and T. Alsanoosy, “Mobile Data Science and Intelligent Apps: Concepts, AI-Based Modeling and Research Directions,” Mobile Networks and Applications, vol. 26, no. 1. Springer Science and Business Media LLC, pp. 285–303, Sep. 14, 2020. doi: 10.1007/s11036-020-01650-z.

[2] T. Lynn, P. Rosati, E. Conway, D. Curran, G. Fox, and C. O’Gorman, “Infrastructure for Digital Connectivity,” Digital Towns. Springer International Publishing, pp. 109–132, 2022. doi: 10.1007/978-3-030-91247-5_6.

[3] Q. Liu, K. G. Mkongwa, and C. Zhang, “Performance issues in wireless body area networks for the healthcare application: a survey and future prospects,” SN Applied Sciences, vol. 3, no. 2. Springer Science and Business Media LLC, Jan. 19, 2021. doi: 10.1007/s42452-020-04058-2.

[4] S. Al Ajrawi and B. Tran, “Mobile wireless ad-hoc network routing protocols comparison for real-time military application,” Spatial Information Research, vol. 32, no. 1. Springer Science and Business Media LLC, pp. 119–129, Sep. 14, 2023. doi: 10.1007/s41324-023-00535-z.

[5] S. Kumar and S. Mehfuz, “Intelligent probabilistic broadcasting in mobile ad hoc network: a PSO approach,” Journal of Reliable Intelligent Environments, vol. 2, no. 2. Springer Science and Business Media LLC, pp. 107–115, Jul. 2016. doi: 10.1007/s40860-016-0023-9.

[6] M. Fleury, D. Kanellopoulos, and N. N. Qadri, “Video streaming over MANETs: An overview of techniques,” Multimedia Tools and Applications, vol. 78, no. 16. Springer Science and Business Media LLC, pp. 23749–23782, May 09, 2019. doi: 10.1007/s11042-019-7679-0.

[7] N. Kuntze, C. Rudolph, and J. Paatero, “Establishing Trust between Nodes in Mobile Ad-Hoc Networks,” Trusted Systems. Springer Berlin Heidelberg, pp. 48–62, 2012. doi: 10.1007/978-3-642-35371-0_4.

[8] H. Luo and M.-L. Shyu, “Quality of service provision in mobile multimedia - a survey,” Human-centric Computing and Information

Sciences, vol. 1, no. 1. Springer Science and Business Media LLC, Nov. 22, 2011. doi: 10.1186/2192-1962-1-5.

[9] K. U. R. Khan, R. U. Zaman, A. V. Reddy, and M. A. Ahmed, "Effective Layer-3 Protocols for Integrating Mobile Ad Hoc Network and the Internet," Distributed Computing and Networking. Springer Berlin Heidelberg, pp. 377–388, 2008. doi: 10.1007/978-3-540-92295-7_45.

[10] R. Huysegems et al., "HTTP/2-Based Methods to Improve the Live Experience of Adaptive Streaming," Proceedings of the 23rd ACM International Conference on Multimedia. ACM, Oct. 13, 2015. doi: 10.1145/2733373.2806264.

[11] J. Dunkel and R. Hermoso, "Towards MANET-based Recommender Systems for Open Facilities," Applied Intelligence, vol. 52, no. 8. Springer Science and Business Media LLC, pp. 9045–9066, Dec. 28, 2021. doi: 10.1007/s10489-021-03117-4.

[12] A. Boushaba, A. Benabbou, R. Benabbou, A. Zahi, and M. Oumsis, "An intelligent multipath optimized link state routing protocol for QoS and QoE enhancement of video transmission in MANETs," Computing, vol. 98, no. 8. Springer Science and Business Media LLC, pp. 803–825, Mar. 22, 2015. doi: 10.1007/s00607-015-0450-0.

[13] H. A. Ahmed, and H. A.A. AL-Asadi,"An Optimized Link State Routing Protocol with a Blockchain Framework for Efficient Video-Packet Transmission and Security over Mobile Ad-Hoc Networks". *J. Sens. Actuator Netw.* 2024, *13*, 22. https://doi.org/10.3390/jsan13020022.

[14] D. Q. Nguyen, P. Minet. "Analysis of Multipoint Relays Selection in the OLSR Routing Protocol with and without QoS Support". [Research Report] RR-6067, INRIA. 2006, pp.15. ffinria00120811v2f

[15] J. Singh, G. Singh, D. Gupta, G. Muhammad, A. Nauman, "OCI-OLSR: An Optimized Control Interval-Optimized Link State Routing-Based Efficient Routing Mechanism for Ad-Hoc Networks". *Processes* 2023, *11*, 1419. https://doi.org/10.3390/pr11051419

[16] J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, "The transparency challenge of blockchain in organizations," Electronic

Markets, vol. 32, no. 3. Springer Science and Business Media LLC, pp. 1779–1794, Mar. 17, 2022. doi: 10.1007/s12525-022-00536-0.

[17] M.A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J.A. Brown, "Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks", Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers* 2020, *9*, 44. https://doi.org/10.3390/computers9020044

[18] R. Agrawal, N. Faujdar, C. Andres T. Romero, O. Sharma, G. M. Abdulsahib, O. I. Khalaf, R. F. Mansoor, and O. A. Ghoneim, "Classification and comparison of ad hoc networks: A review", Egyptian Informatics Journal, Volume 24, Issue 1, March 2023, Pages 1-25

[19] N. Ghodichor, R. Thaneeghavl., D. Sahu, G. Borkar, and A. Sawarkar, "Secure Routing Protocol To Mitigate Attacks By Using Blockchain Technology In Manet." arXiv, 2023. doi: 10.48550/ARXIV.2304.04254.

[20] M. T. Lwin, J. Yim, and Y.-B. Ko, "Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks," Sensors, vol. 20, no. 3. MDPI AG, p. 698, Jan. 27, 2020. doi: 10.3390/s20030698.

[21] A. R. Prasath, "Bi-Fitness Swarm Optimizer: Blockchain Assisted Secure Swarm Intelligence Routing Protocol for MANET," Indian Journal of Computer Science and Engineering, vol. 12, no. 5. ENGG Journals Publications, pp. 1442–1458, Oct. 20, 2021. doi: 10.21817/indjcse/2021/v12i5/211205158.

[22] Lwin MT, Yim J, Ko YB. Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. Sensors (Basel). 2020 Jan 27;20(3):698. doi: 10.3390/s20030698. PMID: 32012774; PMCID: PMC7038462.

[23] Kim, S.; Kim, D. Data-Tracking in Blockchain Utilizing Hash Chain: A Study of Structured and Adaptive Process. *Symmetry* 2024, *16*, 62. https://doi.org/10.3390/sym16010062

[24] J. P. Queralta, F. Keramat, S. Salimi, L. Fu, X. Yu, and T. Westerlund, "Blockchain and Emerging Distributed Ledger Technologies for Decentralized Multi-robot Systems," Current

Robotics Reports, vol. 4, no. 3. Springer Science and Business Media LLC, pp. 43–54, Sep. 29, 2023. doi: 10.1007/s43154-023-00101-3.

[25] Z. Hussein, M. A. Salama, and S. A. El-Rahman, “Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms,” Cybersecurity, vol. 6, no. 1. Springer Science and Business Media LLC, Nov. 03, 2023. doi: 10.1186/s42400-023-00163-y.

[26] A. Malik, B. Bhushan, S. Bhatia Khan, R. Kashyap, R. Chaganti, and N. Rakesh, “Security Attacks and Vulnerability Analysis in Mobile Wireless Networking,” 5G and Beyond. Springer Nature Singapore, pp. 81–110, 2023. doi: 10.1007/978-981-99-3668-7_5.

[27] G. Ben Brahim, N. Mohammad, W. El-Hajj, G. Parr, and B. Scotney, “Performance evaluation and comparison study of adaptive MANET service location and discovery protocols for highly dynamic environments,” EURASIP Journal on Wireless Communications and Networking, vol. 2022, no. 1. Springer Science and Business Media LLC, Jan. 10, 2022. doi: 10.1186/s13638-021-02081-4.

[28] K. Chandravanshi, G. Soni, and D. K. Mishra, “Design and Analysis of an Energy-Efficient Load Balancing and Bandwidth Aware Adaptive Multipath N-Channel Routing Approach in MANET,” IEEE Access, vol. 10. Institute of Electrical and Electronics Engineers (IEEE), pp. 110003–110025, 2022. doi: 10.1109/access.2022.3213051.

[29] S. Venkatasubramanian, A. Suhasini, and S. Hariprasath, “Detection of Black and Grey Hole Attacks Using Hybrid Cat with PSO-Based Deep Learning Algorithm in MANET,” International Journal of Computer Networks and Applications, vol. 9, no. 6. EverScience Publications, p. 724, Dec. 30, 2022. doi: 10.22247/ijcna/2022/217705.

[30] G. M. Borkar, and A.R. Mahajan, “Security aware dual authentication-based routing scheme using fuzzy logic with secure data dissemination for mobile ad-hoc networks”, Journal of Applied Security Research, Volume 13, 2018 - Issue 2. https://doi.org/10.1080/19361610.2017.1387737

[31] S. M. S. Bari, F. Anwar and M. H. Masud, "Performance study of hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN mesh networks," *2012 International Conference on Computer and*

Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, 2012, pp. 712-716, doi: 10.1109/ICCCE.2012.6271309.

[32] R. S. Sharma, K. Bright, & G. Dinesh, "Hybrid model for Protocol Independent Secure Video Transmission using improvised OSLR with optimized MPR and DYDOG," Journal of Algebraic Statistics, vol. 13, no. 2, pp. 1669–1679, 2022.

[33] P. Maharjan et al., "An enhanced algorithm for improving real-time video transmission for tele-training education," Multimedia Tools and Applications, vol. 81, no. 6. Springer Science and Business Media LLC, pp. 8409–8428, Feb. 02, 2022. doi: 10.1007/s11042-022-12045-5.

[34] Vidhya Ramesh, Dr.P.Subbaiah, N. Koteswar Rao, Raju M.Janardhana, "Performance Comparison and Analysis of DSDV and AODV for MANET", *International Journal on Computer Science and Engineering*, volume 2, no. 2, 2010.

[35] R. Goyat, G. Kumar, R. Saha, and M. Conti, "Pribadi: A decentralized privacy-preserving authentication in wireless multimedia sensor networks for smart cities," Cluster Computing. Springer Science and Business Media LLC, Dec. 27, 2023. doi: 10.1007/s10586-023-04211-7.

[36] G. K. Srikanth and P. P. Jadhav, "Design and Analysis of Multipath Routing Protocols in Mobile Ad Hoc Networks," Proceedings of Fifth International Conference on Computer and Communication Technologies. Springer Nature Singapore, pp. 297–306, 2024. doi: 10.1007/978-981-99-9707-7_28.

[37] Shreya Mane, "Conceptual Aspects on Mobile Ad-Hoc Network System," International Journal of Engineering Technology and Management Sciences, vol. 6, no. 6. International Journal of Engineering Technology and Management Sciences, pp. 555–564, Nov. 28, 2022. doi: 10.46647/ijetms.2022.v06i06.095.

[38] K. G. Mkongwa, C. Zhang, and Q. Liu, "A Reliable Data Transmission Mechanism in Coexisting IEEE 802.15.4-Beacon Enabled Wireless Body Area Networks," Wireless Personal Communications, vol. 128, no. 2. Springer Science and Business Media LLC, pp. 1019–1040, Sep. 12, 2022. doi: 10.1007/s11277-022-09987-2.

[39] B. Raj, I. Ahmedy, M. Y. I. Idris, and R. Md. Noor, “A Survey on Cluster Head Selection and Cluster Formation Methods in Wireless Sensor Networks,” Wireless Communications and Mobile Computing, vol. 2022. Hindawi Limited, pp. 1–53, Mar. 28, 2022. doi: 10.1155/2022/5322649.

[40] H. R. Sadjadpour, R. Ulman, A. Swami, and A. Ephremides, “Wireless Mobile Ad Hoc Networks,” EURASIP Journal on Wireless Communications and Networking, vol. 2007, no. 1. Springer Science and Business Media LLC, Aug. 02, 2007. doi: 10.1155/2007/63708.

[41] B. Tavli and W. Heinzelman, Eds., Mobile Ad Hoc Networks. Springer Netherlands, 2006. doi: 10.1007/1-4020-4633-2.

[42] A. M. Soomro et al., “Comparative Review of Routing Protocols in MANET for Future Research in Disaster Management,” Journal of Communications. Engineering and Technology Publishing, pp. 734–744, 2022. doi: 10.12720/jcm.17.9.734-744.

[43] A. Khalid, R. A. Rehman, and M. Burhan, “CBILEM: A novel energy aware mobility handling protocol for SDN based NDN-MANETs,” Ad Hoc Networks, vol. 140. Elsevier BV, p. 103049, Mar. 2023. doi: 10.1016/j.adhoc.2022.103049.

[44] P. Goyal, V. Rishiwal, and A. Negi, “A comprehensive survey on <scp>QoS</scp> for video transmission in heterogeneous mobile ad hoc network,” Transactions on Emerging Telecommunications Technologies, vol. 34, no. 7. Wiley, Apr. 13, 2023. doi: 10.1002/ett.4775.

[45] B. Alaya and L. Sellami, “Multilayer Video Encoding for QoS Managing of Video Streaming in VANET Environment,” ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 18, no. 3. Association for Computing Machinery (ACM), pp. 1–19, Mar. 04, 2022. doi: 10.1145/3491433.

[46] I. Ullah, T. Hussain, A. Khan, I. Ali, F. Ali, and C. Choi, “Analyzing the impacts of node density and speed on routing protocol performance in firefighting applications,” Fire Ecology, vol. 19, no. 1. Springer Science and Business Media LLC, Oct. 19, 2023. doi: 10.1186/s42408-023-00220-4.

[47] M. N. Sudha, V. Balamurugan, W.-C. Lai, and P. B. Divakarachari, “Sustainable Multipath Routing for Improving Cross-

Layer Performance in MANET Using an Energy Centric Tunicate Swarm Algorithm," Sustainability, vol. 14, no. 21. MDPI AG, p. 13925, Oct. 26, 2022. doi: 10.3390/su142113925.

[48] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," Multimedia Systems, vol. 15, no. 5. Springer Science and Business Media LLC, pp. 273–282, Sep. 12, 2009. doi: 10.1007/s00530-009-0166-0.

[49] A. Sakhri, A. Ahmed, M. Maimour, M. Kherbache, E. Rondeau, and N. Doghmane, "A digital twin-based energy-efficient wireless multimedia sensor network for waterbirds monitoring," Future Generation Computer Systems, vol. 155. Elsevier BV, pp. 146–163, Jun. 2024. doi: 10.1016/j.future.2024.02.011.

[50] A. M. Eltahlawy, H. K. Aslan, E. G. Abdallah, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "A Survey on Parameters Affecting MANET Performance," Electronics, vol. 12, no. 9. MDPI AG, p. 1956, Apr. 22, 2023. doi: 10.3390/electronics12091956.

[51] A. Kumar, R. K. Shukla, and R. S. Shukla, "Survey of Comparative Analysis of Different Routing Protocols in MANETs: QoS," Cyber Technologies and Emerging Sciences. Springer Nature Singapore, pp. 419–424, Aug. 30, 2022. doi: 10.1007/978-981-19-2538-2_43.

[52] N. Tizon and B. Pesquet-Popescu, "Scalable and Media Aware Adaptive Video Streaming over Wireless Networks," EURASIP Journal on Advances in Signal Processing, vol. 2008, no. 1. Springer Science and Business Media LLC, May 19, 2008. doi: 10.1155/2008/218046.

[53] I. Nosheen, S. A. Khan, and F. Khalique, "A Mathematical Model for Cross Layer Protocol Optimizing Performance of Software-Defined Radios in Tactical Networks," IEEE Access, vol. 7. Institute of Electrical and Electronics Engineers (IEEE), pp. 20520–20530, 2019. doi: 10.1109/access.2019.2896363.

[54] N. Hasan, A. Mishra, and A. K. Ray, "Cross-Layer Optimization Aspects of MANETs for QoS-Sensitive IoT Applications," Advances in Communication, Devices and Networking. Springer Singapore, pp. 433–444, Aug. 31, 2021. doi: 10.1007/978-981-16-2911-2_45.

[55] J. Pal Singh and A. Kr. Gupta, “Protocol Stack based Security Vulnerabilities in MANETs,” International Journal of Computer Applications, vol. 69, no. 21. Foundation of Computer Science, pp. 1–7, May 31, 2013. doi: 10.5120/12092-8192.

[56] M. A. Abid and A. Belghith, “Leveraging Seminal Protocol Stacks to Support MANETs,” Procedia Computer Science, vol. 10. Elsevier BV, pp. 414–421, 2012. doi: 10.1016/j.procs.2012.06.054.

[57] I. Alameri, J. Komarkova, T. Al-Hadhrami, and A. Lotfi, “Systematic review on modification to the ad-hoc on-demand distance vector routing discovery mechanics,” PeerJ Computer Science, vol. 8. PeerJ, p. e1079, Sep. 05, 2022. doi: 10.7717/peerj-cs.1079.

[58] J. Tao, G. Bai, H. Shen, and L. Cao, “ECBRP: An Efficient Cluster-Based Routing Protocol for Real-Time Multimedia Streaming in MANETs,” Wireless Personal Communications, vol. 61, no. 2. Springer Science and Business Media LLC, pp. 283–302, May 14, 2010. doi: 10.1007/s11277-010-0023-7.

[59] Hai, T., Zhou, J., Lu, Y. *et al.* Enhanced security using multiple paths routine scheme in cloud-MANETs. *J Cloud Comp* 12, 68 (2023). https://doi.org/10.1186/s13677-023-00443-5.

[60] Neelam Malyadri, M. Ramakrishna, A Novel and Optimized Collaborative Diversity-Driven Routing Mechanism in MANETs, SN Computer Science, vol.5, no. 1, 2023. DOI: 10.1007/s42979-023-02317-8

[61] O. Sbayti, K. Housni, M. H. Hanin, and A. El Makrani, “Comparative study of proactive and reactive routing protocols in vehicular ad-hoc network,” International Journal of Electrical and Computer Engineering (IJECE), vol. 13, no. 5. Institute of Advanced Engineering and Science, p. 5374, Oct. 01, 2023. doi: 10.11591/ijece.v13i5.pp5374-5387.

[62] P. Sarao and M. Sharma, “Reactive and Proactive Route Evaluation in MANET,” Journal of Communications. Engineering and Technology Publishing, pp. 143–149, 2022. doi: 10.12720/jcm.17.2.143-149.

[63] M. N. Abdulleh, S. Yussof, and H. S. Jassim, “Comparative Study of Proactive, Reactive and Geographical MANET Routing Protocols,” Communications and Network, vol. 07, no. 02. Scientific

Research Publishing, Inc., pp. 125–137, 2015. doi: 10.4236/cn.2015.72012.

[64] A. Singh, M. Kumar, R. Rishi, and D. K. Madan, “A Relative Study of MANET and VANET: Its Applications, Broadcasting Approaches and Challenging Issues,” Communications in Computer and Information Science. Springer Berlin Heidelberg, pp. 627–632, 2011. doi: 10.1007/978-3-642-17878-8_63.

[65] B. Sharma and D. Saxena, “Design and Analysis of Energy Efficient Service Discovery Routing Protocol in MANETs,” SN Computer Science, vol. 4, no. 5. Springer Science and Business Media LLC, Jun. 28, 2023. doi: 10.1007/s42979-023-01899-7.

[66] Alok Singh Chauhan and H Mary Henrietta, “Design an Improved Trust-based Quality of Service AwareRouting in Cognitive Mobile Ad-Hoc Network,” Wasit Journal of Computer and Mathematics Science, vol. 2, no. 4. Wasit University, pp. 38–46, Dec. 30, 2023. doi: 10.31185/wjcms.218.

[67] D. Kukreja, S. K. Dhurandher, and B. V. R. Reddy, “Enhancing the Security of Dynamic Source Routing Protocol Using Energy Aware and Distributed Trust Mechanism in MANETs,” Intelligent Distributed Computing. Springer International Publishing, pp. 83–94, 2015. doi: 10.1007/978-3-319-11227-5_8.

[68] L. H. Binh and T.-V. T. Duong, “An improved method of AODV routing protocol using reinforcement learning for ensuring QoS in 5G-based mobile ad-hoc networks,” ICT Express, vol. 10, no. 1. Elsevier BV, pp. 97–103, Feb. 2024. doi: 10.1016/j.icte.2023.07.002.

[69] W. Kenny and S. Weber, “Below Cross-Layer: An Alternative Approach to Service Discovery for MANETs,” Ad Hoc Networks. Springer Berlin Heidelberg, pp. 212–225, 2013. doi: 10.1007/978-3-642-36958-2_15.

[70] S. H. H. Nazhad, M. Shojafar, S. Shamshirband, and M. Conti, “An efficient routing protocol for the QoS support of large-scale MANETs,” International Journal of Communication Systems, vol. 31, no. 1. Wiley, Aug. 02, 2017. doi: 10.1002/dac.3384.

[71] K. Nisar et al., “QoS Analysis of the MANET routing protocols with Respect to Delay, Throughput, & Network load: Challenges and Open Issues,” 2020 IEEE 14th International Conference on

Application of Information and Communication Technologies (AICT). IEEE, Oct. 07, 2020. doi: 10.1109/aict50176.2020.9368835.

[72] S. M. S. Bari, F. Anwar, M. H. Masud," Performance Study of Hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN Mesh Networks", *International Conference on Computer and Communication Engineering (ICCCE 2012)*, 3-5 July 2012, Kuala Lumpur, Malaysia, (2012).

[73] T. K. Priyambodo, D. Wijayanto, and M. S. Gitakarma, "Performance Optimization of MANET Networks through Routing Protocol Analysis," Computers, vol. 10, no. 1. MDPI AG, p. 2, Dec. 22, 2020. doi: 10.3390/computers10010002.

[74] R. Suresh Kumar, P. Manimegalai, P. T. Vasanth Raj, R. Dhanagopal, and A. Johnson Santhosh, "Cluster Head Selection and Energy Efficient Multicast Routing Protocol-Based Optimal Route Selection for Mobile Ad Hoc Networks," Wireless Communications and Mobile Computing, vol. 2022. Hindawi Limited, pp. 1–12, Jun. 09, 2022. doi: 10.1155/2022/5318136.

[75] S. Goswami, S. Joardar, C. B. Das, S. Kar, and D. K. Pal, "Performance Analysis of Three Routing Protocols in MANET Using the NS-2 and ANOVA Test with Varying Speed of Nodes," Ad Hoc Networks. InTech, May 11, 2017. doi: 10.5772/66521.

[76] S. Afzal, V. Testoni, C. E. Rothenberg, P. Kolan, and I. Bouazizi, "A holistic survey of multipath wireless video streaming," Journal of Network and Computer Applications, vol. 212. Elsevier BV, p. 103581, Mar. 2023. doi: 10.1016/j.jnca.2022.103581.

[77] Zhipeng Cao et al 2020 J. Research on the e2e Latency Calculation Considering the Gate Mechanism in TimeSensitive Networking, Phys.: Conf. Ser. 1584 012029

[78] Liping Tao, Yang Lu, Xu Ding, Yuqi Fan, Jung Yoon Kim, "Throughput-oriented associated transaction assignment in sharding blockchains for IoT social data storage", Digital Communications and Networks, Volume 8, Issue 6, 2022, Pages 885-899, https://doi.org/10.1016/j.dcan.2022.05.024.

[79] Varun Kohli, Sombuddha Chakravarty, Vinay Chamola, Kuldip Singh Sangwan, Sherali Zeadally, "An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions",

Digital Communications and Networks, Volume 9, Issue 1, 2023, Pages 79-89, https://doi.org/10.1016/j.dcan.2022.06.017.

[80] Yiru Jiang, Dezhi Han, , Mingming Cui, Yuan Fan, and Yachao Zhou, A Video Target Tracking and Correction Model with Blockchain and Robust Feature Location, Sensors (Basel). 2023 Mar; 23(5): 2408. doi: 10.3390/s23052408.

[81] Sarker, I.H. Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. *SN COMPUT. SCI.* 2, 420 (2021). https://doi.org/10.1007/s42979-021-00815-1

[82] L. Hanzo II. and R. Tafazolli, "QoS-Aware Routing and Admission Control in Shadow-Fading Environments for Multirate MANETs," IEEE Transactions on Mobile Computing, vol. 10, no. 5. Institute of Electrical and Electronics Engineers (IEEE), pp. 622–637, May 2011. doi: 10.1109/tmc.2010.208.

[83] T. Clausen and P. Jacquet, Eds., "Optimized Link State Routing Protocol (OLSR)," RFC Editor, Oct. 2003. doi: 10.17487/rfc3626.

[84] Abdelmajid HAJAMI, Kamal OUDIDI and Mohammed ELKOUTBI, A Distributed Key Management Scheme based on Multi hop Clustering Algorithm for MANETs, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, February 2010.

[85] Ankit Kumar Jaiswal, Siddharth Tiwari, Modified OLSR (MOLSR) Protocol for improving optimal route selection with Dynamic MPR selection in Mobile Adhoc Network, IJSRSET, Volume 1, Issue 6, 2015.

[86] Diaa Eldein Mustafa Ahmed, Othman Omran Khalifa, Performance Evaluation of Enhanced MANETs Routing Protocols Under Video Traffics, for Different Mobility And Scalability Models Using OPNET, American Journal of Engineering Research, Volume-6, Issue-7, pp-329-346. 2017.

[87] Frias, V.; Delgado, G.; Igartua, M. (2006). [IEEE 2006 14th IEEE International Conference on Networks - Singapore (2006.09.13-2006.09.15)] 2006 14th IEEE International Conference on Networks - Multipath Routing with Layered Coded Video to Provide QoS for

Video-Streaming Over Manets, pp. 1–6. doi:10.1109/ICON.2006.302583.

[88] Y. Xu, H.-K. Lam, and G. Jia, “MANet: A two-stage deep learning method for classification of COVID-19 from Chest X-ray images,” Neurocomputing, vol. 443. Elsevier BV, pp. 96–105, Jul. 2021. doi: 10.1016/j.neucom.2021.03.034.

[89] S. M. A. Al Mamun and M. Beyaz, “LSTM Recurrent Neural Network (RNN) for Anomaly Detection in Cellular Mobile Networks,” Machine Learning for Networking. Springer International Publishing, pp. 222–237, 2019. doi: 10.1007/978-3-030-19945-6_15.

[90] A. Jain, J. Singh, S. Kumar, Țurcanu Florin-Emilian, M. Traian Candin, and P. Chithaluru, “Improved Recurrent Neural Network Schema for Validating Digital Signatures in VANET,” Mathematics, vol. 10, no. 20. MDPI AG, p. 3895, Oct. 20, 2022. doi: 10.3390/math10203895.

[91] Kollias, Dimitrios; Zafeiriou, Stefanos P. (2020). *Exploiting multi-CNN features in CNN-RNN based Dimensional Emotion Recognition on the OMG in-the-wild Dataset. IEEE Transactions on Affective Computing, (), 1–1.* doi:10.1109/TAFFC.2020.3014171

[92] V. Hnamte and J. Hussain, “Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach,” Telematics and Informatics Reports, vol. 11. Elsevier BV, p. 100077, Sep. 2023. doi: 10.1016/j.teler.2023.100077.

[93] S. Laqtib, K. E. Yassini, and M. L. Hasnaoui, “A deep learning methods for intrusion detection systems based machine learning in MANET,” Proceedings of the 4th International Conference on Smart City Applications. ACM, Oct. 02, 2019. doi: 10.1145/3368756.3369021.

[94] L. H. Son, A. Kumar, S. R. Sangwan, A. Arora, A. Nayyar, and M. Abdel-Basset, “Sarcasm Detection Using Soft Attention-Based Bidirectional Long Short-Term Memory Model With Convolution Network,” IEEE Access, vol. 7. Institute of Electrical and Electronics Engineers (IEEE), pp. 23319–23328, 2019. doi: 10.1109/access.2019.2899260.

[95] Balkisu Musa Hari and A. A. Aminu, “Attention Based Gated Recurrent Neural Network for Wormhole Attack Detection in MANETs,” Zenodo, Oct. 2023, doi: 10.5281/ZENODO.8424623.

[96] Gajendra Ahirwar, Ratish Agarwal, Anjana Pandey, An Extensive Review on QoS Enhancement in MANET Using Meta-Heuristic Algorithms, Wireless Personal Communications, vol. 131, no. 2, PP. 1-26, 2023. 10.1007/s11277-023-10470-9

[97] J. Wang, E. Osagie, P. Thulasiraman, and R. K. Thulasiram, “HOPNET: A hybrid ant colony optimization routing algorithm for mobile ad hoc network,” Ad Hoc Networks, vol. 7, no. 4. Elsevier BV, pp. 690–705, Jun. 2009. doi: 10.1016/j.adhoc.2008.06.001.

[98] Dehghani M and Trojovský P (2023) Osprey optimization algorithm: A new bio-inspired metaheuristic algorithm for solving engineering optimization problems. Front. Mech. Eng 8:1126450. doi: 10.3389/fmech.2022.1126450

[99] B Chigra, Y., Ghadi, A., Bouhorma, M. (2021). A Survey of Optimization Techniques for Routing Protocols in Mobile Ad Hoc Networks. In: Ben Ahmed, M., Mellouli, S., Braganca, L., Anouar Abdelhakim, B., Bernadetta, K.A. (eds) Emerging Trends in ICT for Sustainable Development. Advances in Science, Technology & Innovation. Springer, Cham. https://doi.org/10.1007/978-3-030-53440-0_1

[100] N. Mouchfiq, C. Benjbara, and A. Habbani, “Security in MANETs: The Blockchain Issue,” Communications in Computer and Information Science. Springer International Publishing, pp. 219–232, 2020. doi: 10.1007/978-3-030-61143-9_18.

[101] T. Rathod et al., “Blockchain for Future Wireless Networks: A Decade Survey,” Sensors, vol. 22, no. 11. MDPI AG, p. 4182, May 31, 2022. doi: 10.3390/s22114182.

[102] Shrestha, Rakesh; Bajracharya, Rojeena; Shrestha, Anish P.; Nam, Seung Yeob (2019). *A new-type of blockchain for secure message exchange in VANET. Digital Communications and Networks, (), S2352864818303092–.* doi:10.1016/j.dcan.2019.04.003.

[103] A. H. Mohammed, A. A. Abdulateef, and I. A. Abdulateef, “Hyperledger, Ethereum and Blockchain Technology: A Short Overview,” 2021 3rd International Congress on Human-Computer

Interaction, Optimization and Robotic Applications (HORA). IEEE, Jun. 11, 2021. doi: 10.1109/hora52670.2021.9461294.

[104] M. S. Tamboli, R. R. Vallabhuni, A. Shinde, K. Kataraki, and R. B. Makineedi, "Block chain based integrated data aggregation and segmentation framework by reputation metrics for mobile adhoc networks," Measurement: Sensors, vol. 27. Elsevier BV, p. 100803, Jun. 2023. doi: 10.1016/j.measen.2023.100803.

[105] Ahmad Abdullah Aljabr, Avinash Sharma, Kailash Kumar, Mining Process in Cryptocurrency Using Blockchain Technology: Bitcoin as a Case Study, Journal of Computational and Theoretical Nanoscience, vol. 16, no. 10, pp. 4293-4298, DOI: 10.1166/jctn.2019.8515

[106] Wani, S.; Imthiyas, M.; Almohamedh, H.; Alhamed, K.M.; Almotairi, S.; Gulzar, Y. Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight. *Symmetry* 2021, *13*, 227. https://doi.org/10.3390/sym13020227.

[107] Sudhani Verma, Divakar Yadav, Girish Chandra, Introduction of Formal Methods in Blockchain Consensus Mechanism and Its Associated Protocols, IEEE Access 10(37):66611-66624, 2022. DOI: 10.1109/ACCESS.2022.3184799

[108] A. Kumar, D. Kumar Sharma, A. Nayyar, S. Singh, and B. Yoon, "Lightweight Proof of Game (LPoG): A Proof of Work (PoW)'s Extended Lightweight Consensus Algorithm for Wearable Kidneys," Sensors, vol. 20, no. 10. MDPI AG, p. 2868, May 19, 2020. doi: 10.3390/s20102868.

[109] Lai, R.; Zhao, G.; He, Y.; Hou, Z. A Robust Sharding-Enabled Blockchain with Efficient Hashgraph Mechanism for MANETs. *Appl. Sci.* 2023, *13*, 8726. https://doi.org/10.3390/app13158726

[110] N. Ghodichor, R. T. V, D. Sahu, G. Borkar, and A. Sawarkar, "Secure Routing Protocol to Mitigate Attacks by using Blockchain Technology in MANET," International Journal of Computer Networks & Communications, vol. 15, no. 2. Academy and Industry Research Collaboration Center (AIRCC), pp. 127–146, Mar. 30, 2023. doi: 10.5121/ijcnc.2023.15207.

[111] O. Onireti, L. Zhang, and M. A. Imran, “On the Viable Area of Wireless Practical Byzantine Fault Tolerance (PBFT) Blockchain Networks,” 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, Dec. 2019. doi: 10.1109/globecom38437.2019.9013778.

[112] M. A. A. Careem and A. Dutta, “Reputation based Routing in MANET using Blockchain,” 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, Jan. 2020. doi: 10.1109/comsnets48256.2020.9027450.

[113] R. Eluri, Boyapati Vara Prasad, and Matta Asha Aruna Sheela, “Multipath Routing With Directed Acyclic Graphs in MANETS,” figshare, 2020, doi: 10.6084/M9.FIGSHARE.12236600.

[114] N. Sangeeta, Nam SY. Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability. Electronics. 2023; 12(7):1545. https://doi.org/10.3390/electronics12071545

[115] G. S. Mamatha, “A New Security Solution Architecture (SSA) for MANETS against Network Layer Attacks,” Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg, pp. 263–271, 2012. doi: 10.1007/978-3-642-27299-8_28.

[116] P. Parwekar and S. Arora, “Security Issues and Its Counter Measures in Mobile Ad Hoc Networks,” ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol I. Springer International Publishing, pp. 301–309, 2014. doi: 10.1007/978-3-319-03107-1_33.

[117] V. Mankotia, R. K. Sunkaria, and S. Gurung, “AFA: Anti-Flooding Attack Scheme Against Flooding Attack in MANET,” Wireless Personal Communications, vol. 130, no. 2. Springer Science and Business Media LLC, pp. 1161–1190, Mar. 09, 2023. doi: 10.1007/s11277-023-10325-3.

[118] V. Mohite and L. Ragha, “Cooperative Security Agents for MANET,” 2012 World Congress on Information and Communication Technologies. IEEE, Oct. 2012. doi: 10.1109/wict.2012.6409138.

[119] M. Javaid, A. Haleem, R. P. Singh, R. Suman, S. Khan, “A review of Blockchain Technology applications for financial services”,

BenchCouncil Transactions on Benchmarks, Standards and Evaluations, Volume 2, Issue 3, July 2022, 100073. https://doi.org/10.1016/j.tbench.2022.100073.

[120] Shamshekhar S. Patil, Arun Biradar, Novel authentication framework for securing communication in internet-of-things, International Journal of Electrical and Computer Engineering, 10(1):1092, 2020. DOI: 10.11591/ijece.v10i1.pp1092-1100

[121] Chia-Cheng Hu (2011). *Delay-sensitive routing in multi-rate MANETs. , 71(1), 53–61.* doi:10.1016/j.jpdc.2010.08.018.

[122] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad, The Selective Forwarding Attack in Sensor Networks: Detections and Countermeasures, I.J. Wireless and Microwave Technologies, 2012, 2, 33-44, 2012. DOI: 10.5815/ijwmt.2012.02.06.

[123] Y. Ding, D. Luo, H. Xiang, W. Liu, and Y. Wang, "Design and implementation of blockchain-based digital advertising media promotion system," Peer-to-Peer Networking and Applications, vol. 14, no. 2. Springer Science and Business Media LLC, pp. 482–496, Sep. 10, 2020. doi: 10.1007/s12083-020-00984-5.

[124] Oluwatobi Ayodeji Akanbi, Black Hole Attack, Computer Communications, 2014.

[125] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," 2009 International Conference on Computational Intelligence and Security. IEEE, 2009. doi: 10.1109/cis.2009.244.

[126] J. Sen, S. Koilakonda, and A. Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks," 2011 Second International Conference on Intelligent Systems, Modelling and Simulation. IEEE, Jan. 2011. doi: 10.1109/isms.2011.58.

[127] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting blackhole attacks in Disruption-Tolerant Networks through packet exchange recording," 2010 IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM). IEEE, Jun. 2010. doi: 10.1109/wowmom.2010.5534944.

[128] H. A. Esmaili, M. R. K. Shoja, and H. Gharaee, “Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator,” arXiv, 2011, doi: 10.48550/ARXIV.1104.4544.

[129] M. Al-Shurman, S.-M. Yoo, and S. Park, “Black hole attack in mobile Ad Hoc networks,” Proceedings of the 42nd annual Southeast regional conference. ACM, Apr. 02, 2004. doi: 10.1145/986537.986560.

[130] K. Osathanunkul and N. Zhang, “A countermeasure to black hole attacks in mobile ad hoc networks,” 2011 International Conference on Networking, Sensing and Control. IEEE, Apr. 2011. doi: 10.1109/icnsc.2011.5874910.

[131] P. N. Raj and P. B. Swadas, “Dpraodv: A Dynamic Learning System Against Blackhole Attack in Aodv Based Manet,” arXiv, 2009, doi: 10.48550/ARXIV.0909.2371.

[132] L. Tamilselvan and V. Sankaranarayanan, “Prevention of Co-operative Black Hole Attack in MANET,” Journal of Networks, vol. 3, no. 5. Academy Publisher, May 01, 2008. doi: 10.4304/jnw.3.5.13-20.

[133] H. Deng, W. Li, and D. P. Agrawal, “Routing security in wireless ad hoc networks,” IEEE Communications Magazine, vol. 40, no. 10. Institute of Electrical and Electronics Engineers (IEEE), pp. 70–75, Oct. 2002. doi: 10.1109/mcom.2002.1039859.

[134] R. Kaur and J. Kalra, “Detection and Prevention of Black Hole Attack with Digital Signature,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 8, 2014.

[135] A. Siddiqua, K. Sridevi, and A. A. K. Mohammed, “Preventing black hole attacks in MANETs using secure knowledge algorithm,” 2015 International Conference on Signal Processing and Communication Engineering Systems. IEEE, Jan. 2015. doi: 10.1109/spaces.2015.7058298.

[136] Lahbib, Asma; Toumi, Khalifa; Laouiti, Anis; Laube, Alexandre; Martin, Steven (2019). *[IEEE 2019 IEEE Wireless Communications and Networking Conference (WCNC) - Marrakesh, Morocco (2019.4.15-2019.4.18)] 2019 IEEE Wireless Communications and Networking Conference (WCNC) - Blockchain based trust management mechanism for IoT. , (), 1–8.* doi:10.1109/WCNC.2019.8885994.

[137] M. T. Lwin, J. Yim, and Y.-B. Ko, “Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks,” Sensors, vol. 20, no. 3. MDPI AG, p. 698, Jan. 27, 2020. doi: 10.3390/s20030698.

[138] Lwin, M.T.; Yim, J.; Ko, Y.-B. Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. *Sensors* 2020, *20*, 698. https://doi.org/10.3390/s20030698.

[139] Wenhong Wei, Huijia Wu, Ying He, Qingxia Li, A multi-objective optimized OLSR routing protocol, 2024 Apr 26;19(4):e0301842. Doi: 10.1371/journal.pone.0301842.

[140] Zheng, Zibin; Xie, Shaoan; Dai, Hongning; Chen, Xiangping; Wang, Huaimin (2017). *[IEEE 2017 IEEE International Congress on Big Data (BigData Congress) - Honolulu, HI, USA (2017.6.25-2017.6.30)] 2017 IEEE International Congress on Big Data (BigData Congress) - An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. , (), 557–564.* doi:10.1109/BigDataCongress.2017.85.

[141] Vjatseslav Balahontsev, Alexander Tsikhilov, Alex Norta, Chibuzor Udokwu, A Blockchain System for the Attestation and Authorization of Digital Assets, 2019. DOI: 10.13140/RG.2.2.25027.96807/1.

[142] Yang Liu, Song Peng, Miaomiao Zhang, Shidong Shi, Jianhao Fu, Towards secure and efficient integration of blockchain and 6G networks, 2024; 19(4): e0302052, 2024. doi: 10.1371/journal.pone.0302052

[143] P. Rajankumar, P. Nimisha, and P. Kamboj, “A comparative study and simulation of AODV MANET routing protocol in NS2; NS3,” 2014 International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, Mar. 2014. doi: 10.1109/indiacom.2014.6828091.

المستخلص

الشبكات المتنقلة المخصصة (MANETs) تواجه تحديات كبيرة، تشمل التوجيه غير المثالي، الثغرات الأمنية أثناء نقل البيانات، وتدهور الأداء بسبب متطلبات البث الأحادي(Unicasting) ، والبث المتعدد(Multicasting) ، والبث الجغرافي .(Geocasting) تتفاقم هذه التحديات بسبب الطبيعة الديناميكية لشبكاتMANETs ، والتي تتميز بالتغير المتكرر في الطوبولوجيا وسرعات التنقل المتفاوتة للعقد. يتطلب التعامل مع هذه التحديات استراتيجية توجيه فعالة تضمن كلًا من الأمان والنقل الأمثل للبيانات عبر الشبكة.

لمعالجة هذه المشاكل، تقدم هذه الدراسة بروتوكول التوجيه المحسن بالحالة المترابطة (OLSR)مدعومًا بنموذج تعلم عميق وتقنية البلوكشين لغرض نقل الفيديو. تم تطوير شبكة جديدة قائمة على الانتباه المزدوج والتشابك الكثيف ثنائي الاتجاه (SA_DCBiGNet) لاكتشاف العقد السوداء(Black Hole Nodes) ، في حين تم استخدام بروتوكول التوجيه المحسن المدعوم بـ Osprey (EO_OLSRP)وخوارزمية التحسين الموسعة لـ Osprey (EOOA) لاختيار المسارات المثلى بناءً على استقرار العقد والروابط. كما يتضمن النموذج تخزين البيانات باستخدام نظام الملفات الموزع (IPFS) لتعزيز أمان البيانات، ويتم التحقق من النظام من خلال آلية الإجماع القائمة على إثبات الحصة المفوض .(DPoS) يضمن هذا النهج تحقيق أمان عالٍ وكفاءة في التوجيه ونقل البيانات (الفيديو).

تم تقييم النموذج المقترح باستخدام عدة نماذج محاكاة للشبكات المتنقلة بالتعاون مع المحاكي NS3، وقد حقق نتائج متفوقة مقارنة بالطرق الحالية. يحقق النموذج نسبة تسليم حزم (PDR) تبلغ 99.8%، مع وصول الإنتاجية إلى 2900 كيلوبايت في الثانية، ويقلل من الحمل الزائد للتوجيه إلى 41.7% وزمن التأخير من طرف إلى طرف إلى 19.1 ميلي ثانية. مقارنةً بالطرق التقليدية مثل SRABCو HEDARوSETORD، يحقق النموذج المقترح تحسينات كبيرة لنقل الفيديو في مؤشرات الأداء الرئيسية، مما يثبت فعاليته في تعزيز أمان وأداء شبكاتMANETs .

جمهوريـــــــــــة العـــــــــراق
وزارة التعليم العالي والبحث العلمي
جامـــــــــعة الكوفـــــــــــــة
كليه علوم الحاسوب والرياضيات
قسم علـــــوم الحاســـــــــوب

تحسين الأمان والأداء في الشبكات المتنقلة المخصصة (MANETs)باستخدام تقنية البلوكشين والتعلم العميق

أطروحة مقدمة الى

مجلس كلية علوم الحاسوب والرياضيات / جامعة الكوفة كجزء من متطلبات نيل درجة الدكتوراه في علوم الحاسوب

من قبل:

هدى عبد الرحيم أحمد

بإشراف

أ.د. حامد علي عبد الأسدي

1446هـ **2024 م**