International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Improvement of Packet Delivery Ratio in Wireless Mesh Network Using Hybrid Routing Protocol in VoIP Application

A. Muniappan[1], G. Arul Dalton[2], A. Prithiviraj[3], T. Jackulin[4], A. Karthikayen[5]

Submitted: 19/11/2023 **Revised:** 31/12/2023 **Accepted:** 11/01/2024

Abstract*:* Wireless Mesh Networks (WMN) are thought to be the best solution for last-mile communication network supply because to their flexible deployment and reasonably priced implementation. One of the main components of WMNs is multi-path gearbox, which can lead to improved ruggedness, capacity, and territorial service. Multi-path WMNs are inexpensive, quick to set up, and use less wires than other network configurations. Broadband wireless technology has become more appealing as a result of the worldwide integration of Wireless Local Area Networks. VoIP has grown in popularity as a wireless LAN Internet application. Future cellular networks need to be able to process video with high quality, including VoIP. This paper proposes a blockchain-based Topographical Relay Selection Secure Routing (B-TRSSR) method for multi-hop communication that takes bandwidth, latency, and flow management into account. By avoiding all dangerous zones and assuring the security of sent packets, the suggested technique chooses an entirely different transmission path. By implementing an Adaptive Intrusion Detection System (AIDS), numerous security threats such as tampering assaults, dropping attacks, flooding attacks, and malicious attacks are discovered and eliminated. The results showed how a number of factors, such as load and mobility, may affect Wi-Fi performance. The article's performance metrics encompassed end-to-end latency, packet delay ratio, throughput, and delay jitter. An input metric for simulations is mobility.

Keywords: *Voice over Internet Protocol (VoIP), relay selection, Wireless Mesh Networks (WMN), Internet of Things (IoT)*

1. Introduction

Healthcare, smart grids, the IoT, the IoV, and intelligent modes of transportation are merely a few examples of several industries that may benefit from flexible, reliable connections offered by WMNs [1]. Multipoint to Multipoint (MTM) relationships, allowing a mesh node to connect to several mesh nodes concurrently, are employed by WMNs to take advantage of the Point-to-Point (PTP) communication used by conventional ad hoc networks to improve network scalability, confidence, and capacity. Such a feature assists in developing mesh networks that are trustworthy, low-maintenance, inexpensive, and powerful. Mesh routers and switches, gateways, and clients make up the three elementary parts of a WMN.

Consequently, a fair channel duty should make sure that all network links attain a rate of data that is suitable for all pertinent nodes. As a consequence, each link's data rate following channel assignment should match the link's intended data rate.

[1]*Professor, Saveetha School of Engineering,*
Saveetha Institute of Medical and Technical Sciences,
Thandalam, Chennai, India.
Email: inspire.munish@gmail.com
ORCID: 0000-0002-7207-8144
[2]*Associate Professor, Department of CSE,*
Saveetha Engineering College, Chennai
Email: garuldalton@gmail.com
ORCID: 0000-0002-5981-7176
[3]*Asst.Professor (Sr.Grade), Department of CSE,*
Sona College of Technology, Salem-5.
Email: prithivi@sonatech.ac.in
ORCID: 0000-0002-6936-7359
[4]*Associate Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai*
Email: karthijackulin@gmail.com
ORCID: 0000-0003-4015-7718
[5]*Professor, Department of ECE,*
Sri Sai Institute of Technology & Science, Rayachoty-516270.
Annamaya Dt. Andhrapradesh, India
Email: Akarthi_mathi@yahoo.co.in
ORCID: 0000-0003-4279-0808

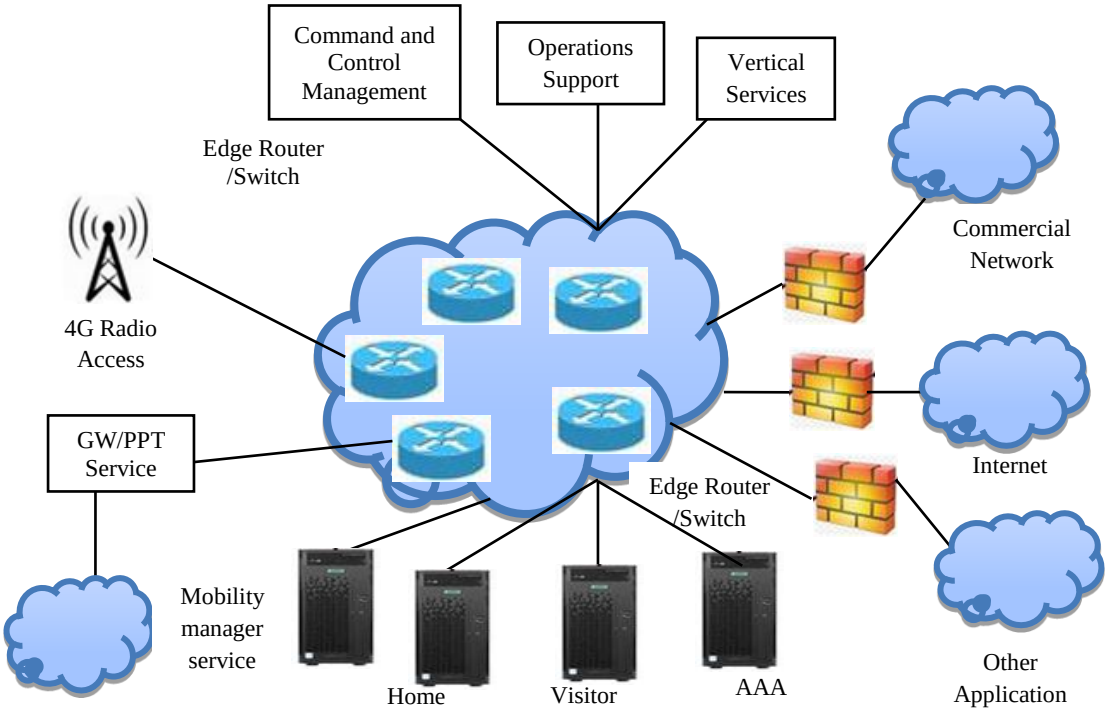

Fig. 1.1. Architecture of Wireless Mesh Networks

In above Figure 1.1 wireless mesh networks, it has been focused on how to find high-performance routing routes using several routing metrics that are meant to capture relationship quality. However, these routing evaluations were developed with the strong premise that the network has become more dependable and that all node's path packets are honest [2]. For infrastructure-based WMNs, where not all nodes always cooperate and relationship dependability is not always confident this assumption could not always stay true. In contrast to the complicated cellular network design, that involves base stations and mobile switching places, the WMN infrastructure, which includes mesh routers, could potentially be relatively easily accessed and manipulated by attackers. Attackers may be able to track packets over the network and extract information from them. By examining how it currently works, it has been shown that there is no optimum routing solution that can do all three of the following activities in WMNs: protecting privacy, providing safety against adversaries, and finding high-performance trustworthy routing pathways. Therefore, the present routing protocols must be improved further regarding privacy and security to counter various DoS attacks to provide a safe and reliable routing route with more powerful privacy protection.

To provide the highest level of privacy protection and to have the greatest possible security against adversaries, Private Preserved and Secured Reliable Routing (PSRR) for infrastructure-based mesh wireless networks are presented in this research. By selecting the safer path, the recommended protocol improves network performance as well. The use of group signature and ID-based encryption may maintain user privacy in WMNs.

The remaining part of this essay is arranged as follows. The related efforts on security, confidentiality, and reputation methods for mesh networks that are wireless are covered in Section 2. We offer the suggested protocol in Section 3. The training of security and privacy is covered in Section 4 and the Development and performance analysis are addressed. The paper is concluded with possible enhancements in Section 5.

2. Literature Review

Tian, L., et al [3] When distributing compute work by relaying, there may be malevolent relaying nodes. Therefore, during the relaying and uploading processes, Information veracity and anti-falsification are guaranteed by the trust-based blockchain technology. After receiving the relaying job, the last-hop relaying train delivers the data consensus criterion and transaction data to the blockchain system for transaction verification. The information data is confirmed by a consensus process between the inquiring train node and the other relaying train nodes in the routing path. Within the blockchain system, every train is considered a blockchain node.

Prasath, et al [4] In this method, voting is determined by a node's behavior, and direct neighbor nodes are used to share trust information. Additionally, self-detection is a possibility in which the routing table's trust value is discovered and changed. Mobile nodes compute trust value at this step rather than the number of neighbor's data. As a result, all nodes in the network are authorized because each mobile node is given an authority identity through the dynamic exchange of hello packets between nodes. Because malicious nodes generate authority identities in this work, authentication is ineffective. More energy is used when dynamic hello messages are exchanged. Since the trust values are downloaded into packet headers, malicious nodes can produce them.

Loret, et al [5] The mesh nodes in WMN often work together and interact with neighboring nodes to complete their responsibilities. It is widely acknowledged that a certain quantity of energy will be utilised to transmit the data packets out for every conversation in WMN. As a result, SOTMRP defines the trust value for inserted packets, remaining energy, data content across many

packets, and communication. To ascertain whether the information sent has arrived at its destination unharmed, the data contents are examined. The data content is examined using the packet drop ratio.

Bello, et al [6] To maximize coverage of areas of interest, reduce coverage of optional areas, and ensure connectivity for all mesh router nodes, the ideal number and locations of mesh router nodes must be found. They introduced the innovative PRACA (Placement, Routing, and Channel Assignment) scheme, which takes into account the three interconnected aspects driven by Tabu Search to reduce network-wide interference. This homework is anticipated to offer a practical modeling framework for integrating wireless network architecture and facility placement models in a three-dimensional setting.

Ilakkiya, et al [7] Additionally, choosing the optimum routes while taking energy efficiency into account is MANET's primary goal. The IEEHR paradigm for MANET is introduced in this paper to achieve this. By merging Honeycomb-based area coverage with LAR, the model decreases the transmission range while performing pathfinding. Efficiency in energy utilization, in addition to effective routing, is essential for MANET because mobile nodes have limited energy. The effectiveness with which energy is used inside a network will affect both its performance and its resilience. More energy is saved in this case when the mobile nodes are dormant and are subsequently used during the effective routing procedure.

Zeng, Z., et al [8] The foregoing security issues can be resolved thanks to the distributed peer-to-peer network that the blockchain brings, which enables untrusted people to connect with one another in a verifiable manner without the use of a trusted intermediary. A decentralized, immutable digital ledger might be referred to as a blockchain. The transaction documents, the timestamp, and the hash value of the preceding block make up the majority of each block. Because of the built-in cryptographic chaining, the hash value makes it simple to identify malicious behavior.

Ajayi, A. O., et al [9] According to the investigation, unlike OLSR, where both can negatively impact mesh scalability, BMX6 is not considerably affected as network node density and diameter rise. The Ad-hoc On-demand Distance Vector (AODV-HP) routing protocol is analysed through simulation on several radios in this article. This protocol enables discrimination between the heterogeneous nodes that comprise the hybrid wireless mesh system. Mobile mesh clients are also involved in traffic management and forwarding, with respect to metrics such as delay, packet delivery ratio, and routing costs.

Maliwatu, et al [10] A framework for the optimal multi-link routing for WMN hybrid back-haul lines, given multiple radio-equipped nodes, is presented in the dissertation. A three-tiered paradigm is suggested that distinguishes between multi-link utilisation rules and potential link configurations. The varied connection configurations can be linked with an appropriate policy to satisfy the various performance goals thanks to this decomposition. Additionally, a technique based on adaptive round-robin (ARR) is provided to increase the effectiveness of aggregate networks with non-uniform data rates.

3. Methods and Materials

3.1 WMN Overview

This section gives a detailed and helpful overview of WMN.

Classification of WMNs

PTP networks are trustworthy. However, they aren't scalable and the level of flexibility is bad. PTM networks provide a low level of flexibility and dependability but are fairly scalable [11]. Multi-point to Multi-point (MTM) systems capabilities that give great reliability, mobility, and scalability that allow a large number of users to get around these limitations. The transmission power required by each node will fall as the network's nodes grow. MTM wireless networks, however, use several hops to broaden coverage without needing to increase transmission power. Modern wireless technology such as the IEEE 802.11 group is used by MTM networks. Mesh networks are the name assigned to these networks. In this study, we focus on Wireless Mesh Networks, a particular category of MTM networks. Figure 3.1 depicts the entire taxonomy of this classification.

3.2 Advantages of WMNs

Self-Organizing and Self-Configuring: WMNs have flexible network designs and are independent of protocol deployments. The WMN's characteristics include self-healing and self-configuration. As a consequence, setup time and maintenance costs are decreased. In addition, it increases network performance. These features enable the network service suppliers to alter, grow, and alter the network as necessary to satisfy the requirements of the end clients.

Increased Reliability: There are several routes between source and destination nodes in a WMN. This offers fallback paths in the case of failure. Alternative routes may be utilized to minimize congestion in active network locations as well. Load balancing and reducing the bottleneck via other routing may significantly improve network resilience in WMNs, enabling the balancing of traffic loads within the network.

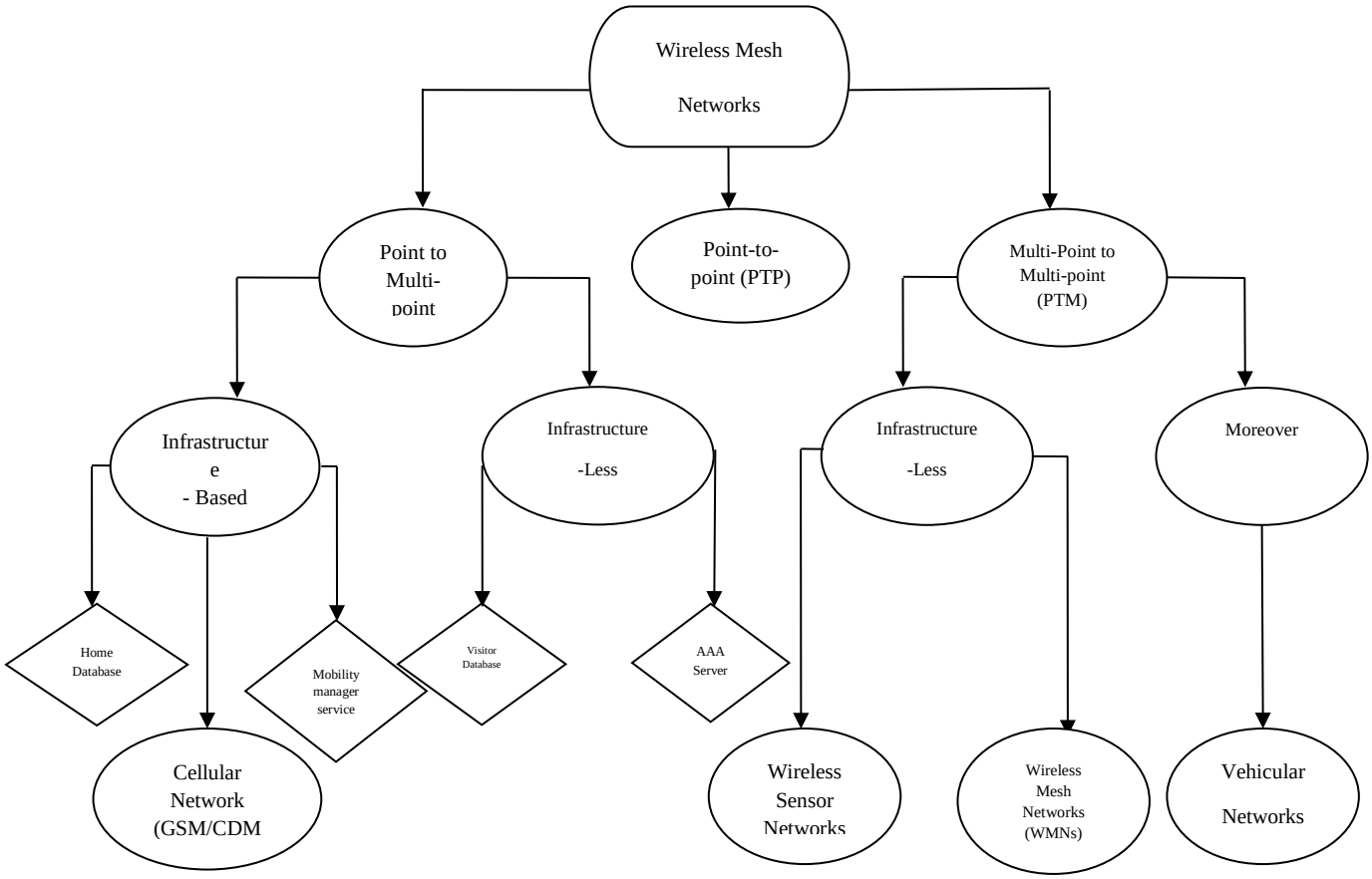

Fig. 3.1. Wireless Mesh Networks Classification

Interoperability: WiMAX, Mobile, Wi-Fi, Zigbee, wireless communication, Sensor, MANET, Vehicular, etc. are among the current standards that are compatible with WMN's combination multi-point to multi-point architecture. Therefore, progressive rollout and the reuse of current infrastructures are attractive. All of the mentioned technologies can right now or soon will be able to, create a WMN and interact with each other. Most of the modifications required for networks of any sort to be able to interact with one another may be applied to the existing standards to keep them interoperable.

Academic Supporting and Industry Standards

Many organizations are engaged in current studies on numerous WMN-related subjects, including planning for strategy, protocols, applications, and applications. Many towns, including Chaska, Minnesota [12], as well as Rio Rancho, New Mexico, already use WMNs.

Wi-Fi Mesh based on IEEE802.11: A mesh STA (station) transmits frames hop-by-hop by acting as a router. Mesh is an AP (Access Point) that Offers connection services for customers as well as relaying capabilities. Additionally, IEEE 802.11 specifies Hybrid Wifi Mesh Protocol (HWMP) as its routing protocol, which is an extendable path selection strategy.

IEEE 802.15.1 Bluetooth: Known widely as Bluetooth, this standard is focused on Wireless private area networks (PANs). In an entire mesh topology, direct connections are employed. It indicates that every wireless node is directly linked to each other. As opposed to this, in a partial mesh topology, certain wireless devices are connected to every other wireless node while others are only connected to wireless nodes that transmit data.

Zigbee, IEEE 802.15.4: Motorola was the business that initially suggested Zigbee. There are two connection configurations offered in the Wireless Personal Area Network (WPAN) standard: single-hop and multi-hop connections. By specifying a coordinator, mesh topology may be enabled through Zigbee. The coordinator is in charge of setting up the multi-hop network framework.

IEEE 802.16 WiMAX: This IEEE 802.16j wireless communication standard is designed to supply Mobile Multi-hop Relay (MMR) abilities for Metropolitan Area Networks (MANs). This will allow the implementation of some WiMAXcenter stations as relay stations for deploying multi-hop mesh structures in WiMAX. A multi-hop mesh construction can be set up to improve network coverage while eliminating the installation costs associated with fixed-line connections [13]. The IEEE 802.16j standard, which is an updated version of the IEEE 802.16-2009 standard, was approved in May 20093.

Regional hybrid routing protocol with condition awareness

The suggested RCA-HRP, in contrast to all other hybrid routing protocols for hybrid WMN, uses regional conditions to assist mesh nodes in choosing routes that are more efficient. Furthermore, RCA-HRP takes into account both client- and gateway-oriented traffic. When a mesh client requests to access a mesh router for gateway-oriented traffic, RCA-HRP takes into account the state of the entire proactive path where the access mesh router is situated. In order to more correctly assess the state of the proactive path as a whole, RCA-HRP takes into account a wide range of variables for mesh routers in the proactive path. These mesh routers take into consideration the load and speed of

their neighbouring mesh clients as well as their quantity. The energy, speed, and load of neighbours are among the regional network factors that are taken into account in client-oriented traffic. The cross-layer technique is employed in the process of gathering regional information. The Media Access Control (MAC) layer provides the queue length, which indicates the load status at each radio interface of a node. The application layer can be used to gather the energy and speed of mesh clients.

Routing Protocol Suggestions

Mesh gateways are used to hold cluster head addresses, mesh clients, and mesh routers. The idea behind hybrid routing protocol is to cover all mesh routers by clustering the WMN's mesh routers. When there is a destination node inside the cluster, use proactive routing protocol. It should be noted in this instance that starting the route request process at the gateway is avoided. To establish communication if the destination node is not within the cluster, utilise the reactive routing protocol. In this instance, the mesh gateway (M-GW) receives this request from the CH. Next, the mesh gateway provides the target MR's location and CH address in response to the requested CH. Next, in order to find the optimal path that satisfies the QoS requirements, including bandwidth, delay, hop count, jitter, and ETX, CH initiates the route request procedure between the source MR and destination MR. Because it combines proactive and reactive protocols, the suggested routing strategy for mesh networks is known as a hybrid routing protocol.

Prior to using the suggested routing protocol, the mesh routers need to be organised into groups known as clusters. In order to do this, every mesh router broadcasts its data to its neighbours. Building the list of neighbouring mesh routers is aided by this procedure of exchanging mesh router information. This list of neighbour mesh routers facilitates the creation of clusters and the election of cluster leaders and members.

3.3 Components of WMNs

A WMN consists of three various kinds of nodes: WMN clients, WMN routers, and WMN gateways.

The WMN clients are consumer equipment, including desktops, PDAs, smartphones, etc., that can link to the network and use services like VoIP, games, location-based services, email, etc. These devices are considered portable; they have a finite amount of power, a potential for routing, and a potential for limited usage associated with the network.

In the network, **WMN routers** serve to route data traffic. No traffic may be initiated or controlled by them. While the routers have stable characteristics, their mobility is constrained. Due to its multi-hop communications technique, mesh routers have low transmission power consumption. For scalability in a multi-hop mesh environment, a mesh router additionally supports numerous channels and numerous interfaces through the Medium Access Control (MAC) protocol.

Routers called **WMN gateways** have direct connections to the Internet and wired infrastructure. Since they have multiple interfaces, WMN gateways can connect to wireless as well as wired networks, but they are costly. Therefore, the network contains just a handful of WMN gateways. In addition, where they are located greatly impacts how well the network works.

3.4 Problems and Challenges in WMNs

Despite great progress, there are a lot of problems to be addressed before the pledge of the WMN can be entirely realized [14]. A WMN has challenges at several levels, which are briefly explored below.

Physical Layer Issues

Today's leading radio models are directional antennas, single radios with a single channel, single radios in multiple channels, and multiple radios in many different channels.

Nodes are half-duplex in a single radio, single-channel environment. It suggests they are unable to send and receive signals at the same moment. A node can use many nonoverlapping channels at once under the multiple radio various channels architecture. Multiplexing is also used in directional antennas to reduce interference.

Topological and Deployment Issues

This is a basic issue, and a WMN's ability to assess network performance and provide Quality of Service for end users is important. Planning a WMN involves figuring out the number of gates to set up, where they ought to go, how to make the most of the available bandwidth, and how to keep deployment costs low.

Structured distribution and organic implementation are the two primary types of deployment. Services will be offered in a new location when using structured deployment, giving it the freedom to select the topology. By utilizing the routine nature of the deployed mesh network, this flexibility could translate into enhanced network performance. However, in a natural installation, a mesh network will be built naturally over the highest point of already existing infrastructure. Due to this, the network architect has a restricted number of topology options.

Dynamical Layer

Despite the WMN technique being conceptually "radio agnostic" (i.e., free of the physical tier), like many other networking protocols, the efficacy of the WMN is modulated by the physical layer's attributes. A WMN should have an adequate physical layer at a minimum. The adverse impacts of fading and interference are widely recognized, so multiple (typically spread spectrum) techniques have been utilized to boost the accuracy of radio waves. Sensitivity to interference is a greater concern in WMNs compared to cellular systems and 802.16 since these networks generally employ contention-based MAC methods, which are virtually collision-free.

Despite the essential need for accuracy, the skills that follow can have an enormous effect on how efficiently WMNs perform:

- **Movement:** For WMNs to facilitate user motion, the material layer needs to be able to cope with the frequency shift and swiftly diminish situations that frequently happen to mobile users.
- **Connection Adaptation:** A more resilient transmission or error-correcting code ought to be utilized to rebuild the sturdiness of a link (at an extra cost of the bandwidth) when propagation parameters are less than perfect (i.e., the majority of the time). Such a link modification is now employed by several cutting-edge technologies, notably WLANs, WMANs, and cellular systems.
- **Variable Transmission Power:** The connection adaptability technique has a further degree of flexibility if the wireless transmitter's strength can be modified. However only data from the highest levels could potentially be employed to calculate the "optimal" transmission capability.

3.5 Data Link Layer

The MAC protocol's building design at the info link tier is expected to bring up challenges for WMN. It is highly unlikely that the terminal, though representing a centralized organization, can successfully coordinate the MAC layers of terminals positioned a few hops distant.

There are several MAC protocols designed exclusively for MANETs. Multiple of those tiers likely will function more well in WMNs. The RTS/CTS option designated as MACAW, particularly defined in IEEE 802.11, is extremely useful in reducing the implications of the buried endpoint challenges.

Channel Assignment:

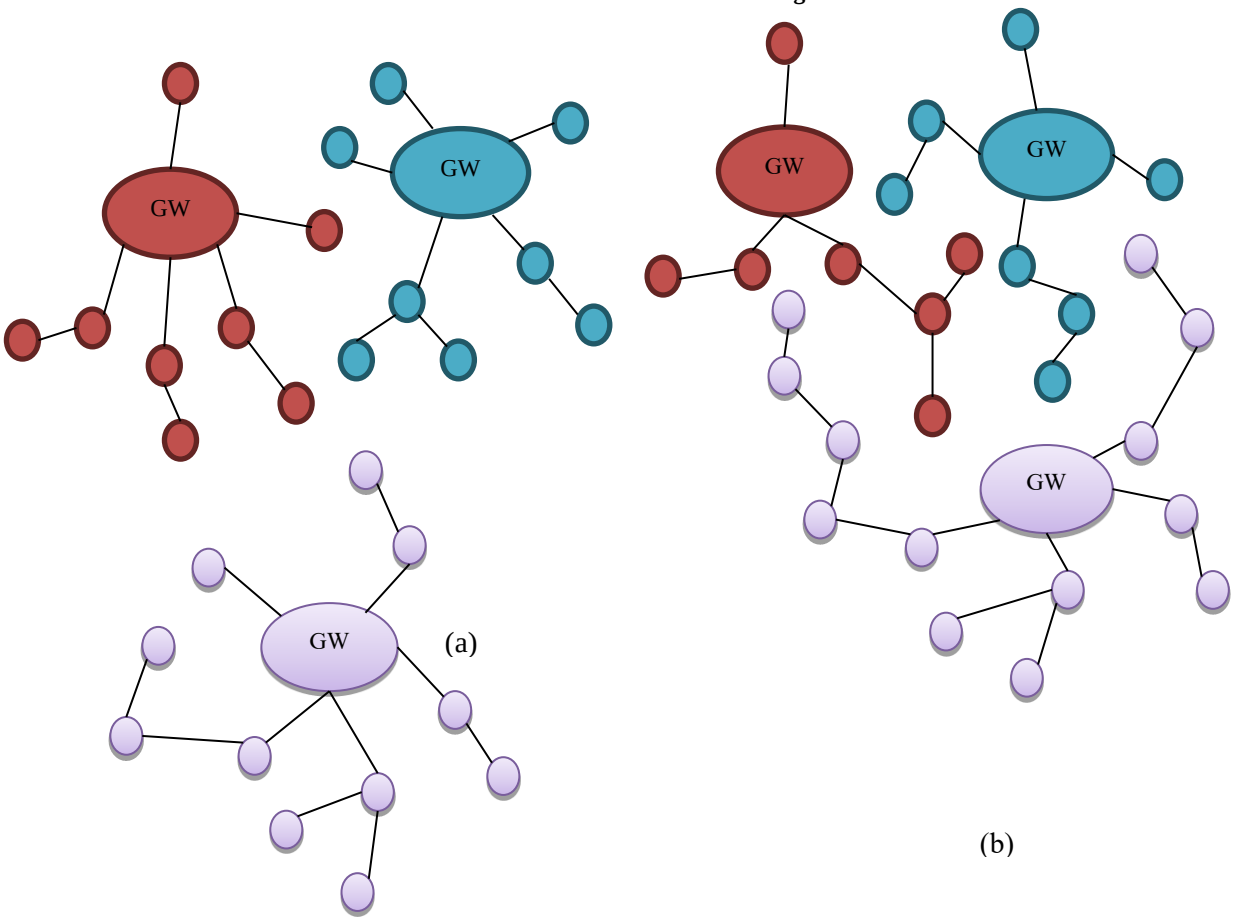

Fig. 3.2. For an Infrastructure Comprising Three Channels, Three Gateways, and 29 WMN routers, there Exist two Potential Channel Assignments.

Two hypothetical channel configurations for a WMN with C = 3 channels and M = 1 transceivers in every router are shown in Figure 3.2. Relying on the supplied load at every node in the network, one of the two allocations will either boost the network's capacity or diminish it. The two-channel funding could have an enormous disparity in network capability.

Network Layer

The networking layer's main job is to transmit information from the source to the destination via an array of hops. WMNs diverge dramatically from 3G infrastructure, WLANs, and WMANs in this aspect. These devices all utilize a single wireless link, hence a network tier is superfluous. For WMNs and MANETs, in contrast, the origin and destination may be isolated by several wireless hops, mandating the organization and transfer of the messages inside the wireless network themselves.

A. The B-TRSSR approach for topographical relay selection

A Topographical Relay Selection Secure Routing (B-TRSSR) method for multi-hop connectivity has been proposed for privately delivering packets. In the current scenario, wireless mesh networks gather data from sensors or the cloud. The Internet of Things (IoT) endpoints that are readily accessible are picked based on the channel's existence and the links' internet access, which are both taken into consideration before the transfer takes place to the destination nodes. The assignment of the bandwidth to the productive nodes may be determined by the likelihood of nodes with less channel congestion and better link connection.

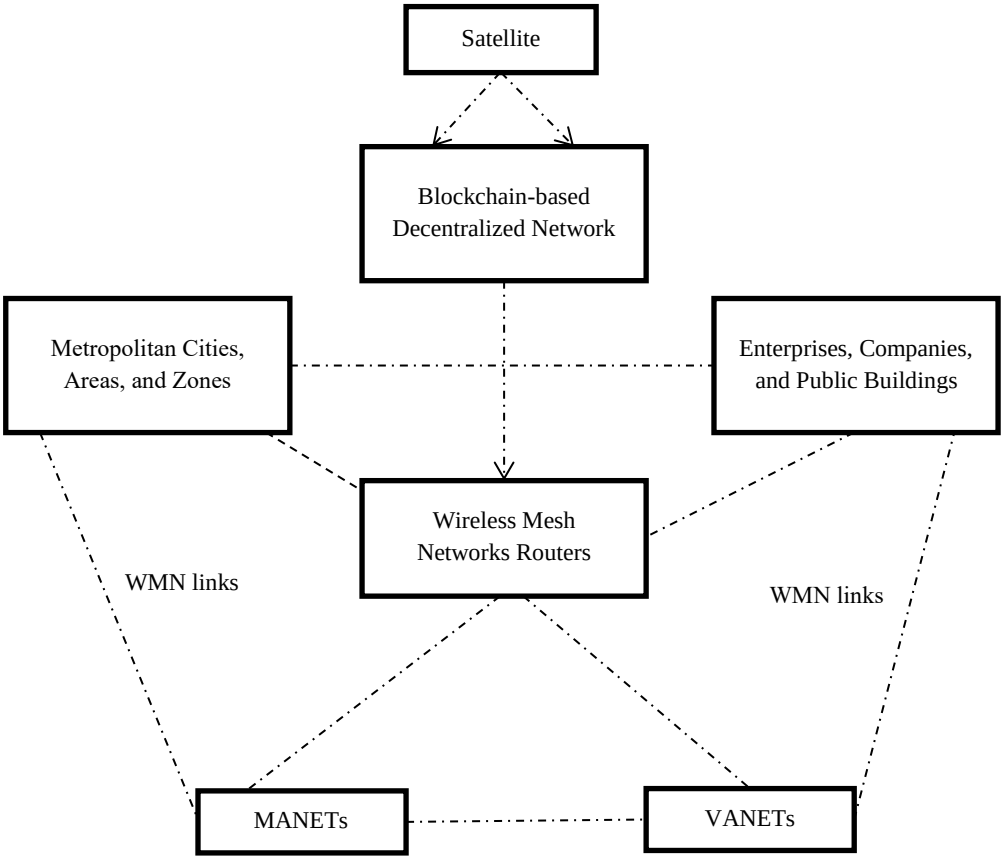

Fig. 3.3. Demonstrates the Suggested WMN Routing System's Layout.

The portable model advocated is scalable with 5G and 6G technologies in addition to infrastructures like VANET and MANET. This usually happens by selecting random channels that, by identifying the mobility-specific nodes, produce the most accurate overview of the movement of nodes. Figure 3.3 portrays the scenario employed to demonstrate the B-TRSSR technique [16]. The untrusted nodes will be in control of picking the reputable nodes, encouraging transmission over the links. The selection of reputable relay nodes could impact the rates exhibited for the channels. The recognized delay nodes might be identified based on the evaluations presented and taking into mind the nodes that performed the tasks issued. The list of relay nodes might be broadened to encompass the accessible routers that are taking part in the tournament. The scores assigned may be used to assist in selecting the nodes for transfer. Nodes that don't engage in the task event or do not finish the task may not be eligible for the routing.

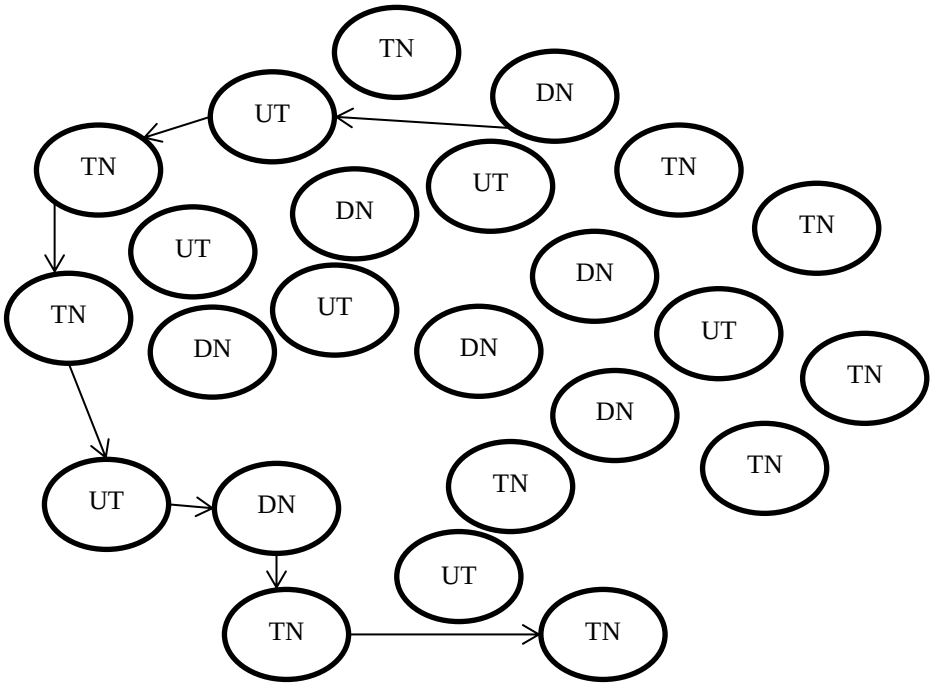

Fig. 3.4. B-TRSSR Procedure Example Circumstance

The nodes' ratings are presented under multiple ratings, varying from 0 to 5. As a consequence, the finest possible grades will be compared to the typical assessment and a value of 3.5 has been achieved for the designated nodes in Figure 3.4. Those nodes with significant speeds can consequently be deemed as being trustworthy ones, and it is from these nodes that the bandwidth-related clusters are gathered for sending information. The assessment of the nodes will be derived upon taking into careful consideration the management inquiries, such as the route request $(S_{req})$and route reply(S_{rep}), that are transferred to the terminals that already exist in the communication system. The methodology representing the estimation of the average node rating (S_N) is described below in Algorithm 1. Understanding the modifications observed for the distinguished tracks the route request (S_{req}) together with route reply (S_{rep}) is delivered along to the various nodes which supply the individual nodes with value S_O may be discovered. The subsequent formula for mathematics is utilized to estimate the S_O:

$$S_O \leftarrow \sum_{l=1}^{O}\left[\frac{[Y_{req}-Y'_{rep}]}{Y_{req}}\right] * 100 \quad (1)$$

Here Y_{rep} signifies queries that haven't been submitted to receive requests and Y_{req} implies requests that were made to the route. Here, Z_{req} and A_{req}, two possible scenarios, are notified at different times. The fine-tuning of the cluster selection standards may relate to the three distinct circumstances.

Algorithm 1: Algorithm to find Average Node Rating (S_O)

Input: Ctl_r to Nbr (O)
Output: $Us(O) \leftarrow S_O$
Consideration: $B \leftarrow Y_l, C \leftarrow Z_l,\ D \leftarrow A_l$
Begin
$Y_l \leftarrow o(1,2,3,\dots U_m)$
for(j=1toM)
Broadcast $C_o \leftarrow S(1,2,\dots m)$
Calculate $S_O \leftarrow \sum_{l=1}^{O}\left[\frac{[Y_{req}-Y'_{rep}]}{Y_{req}}\right] * 100$
$Z_l \leftarrow o(1,2,3,\dots U_m)$
for(j=1toM)
Broadcast $C_o \leftarrow S(1,2,\dots m)$
Calculate $S_O \leftarrow \sum_{l=1}^{O}\left[\frac{[Z_{req}-Z'_{rep}]}{Z_{req}}\right] * 100$
$A_l \leftarrow o(1,2,3,\dots U_m)$
for(j=1toM)
Broadcast $C_o \leftarrow S(1,2,\dots m)$
Calculate $S_O \leftarrow \sum_{l=1}^{O}\left[\frac{[A_{req}-A'_{rep}]}{A_{req}}\right] * 100$
If $S_0 \gg 3.5$
The node is added to the relay node list
If $1 > S_0 > 3.5$
The node is added to the trusted node list
else
The node is added to the untrustable node list
End for
End for
End for
End if
Return

Considering that Y, Z, and A are the three potential paths assigned for secure transmission, the trustworthy nodes take independent routes when considering the ratings. The decentralized organization established with blockchain is going to be in charge of the three routes. To pass data that is detected alongside the relay nodes, the pick of nodes for trustworthy communication is evaluated to the full region whilst taking linkages across links into account. Control transmissions are sent amongst nodes to figure out the minimum bandwidths that remain constant between the chosen nodes. The specialized networks are unhindered by overcrowding and send data rather than any such losses under the transmissions that have been allocated focused on the bandwidths' accessibility. The mathematical depiction of the control packages evaluation in conjunction with accessibility and bandwidth concerns is

$$Bandwidth, Cx(o) = \sum_{y \leftarrow S_o}\left[\frac{\sum_{oj,ok}^{data\_rate} S_0(x(o),\vartheta)}{U_s(o-1)}\right] + \sum_{y=1}^{o} S_o(y) \quad (2)$$

The bandwidth is Cx(o), the nodes' data is x(o), and the channel expenditures are ϑ. To analyze the complete baseline value of the communication supplied by the links, the moved hubs can stay connected over an extended time interval. To figure out the possibility that actual nodes are going to appear, the reference values for link longevity may be supplied. The mathematical model specifies that the odds of forecasts are set to the terminals with the smallest information rate and the hubs that are currently available might be allowed to talk to a distance that is not stated within the limits of conversation.

$$m_{long} = Q(S_O > U_s)_y \quad (3)$$

The interaction stretches between adjacent nodes in the reachable paths could potentially be taken into thought to estimate and determine the probability of the existing links. Analysis of the path fluctuation can be accomplished by employing particular paths. As an outcome, there is network interference and network disruption tied to the excessive data traffic, both of which are capable of being reduced via the presence of open bandwidth as well as the extensive interaction connects employed for transmission.

B. Blockchain-based authorization

The handling of topographic information can be achieved via an autonomous component which in turn preserves authority over the permitted information via all entry points. The terminals that are linked to the authentication system may consist of numerous types, notably MANETs, VANETs, 5G, and 6G interactions, among others.

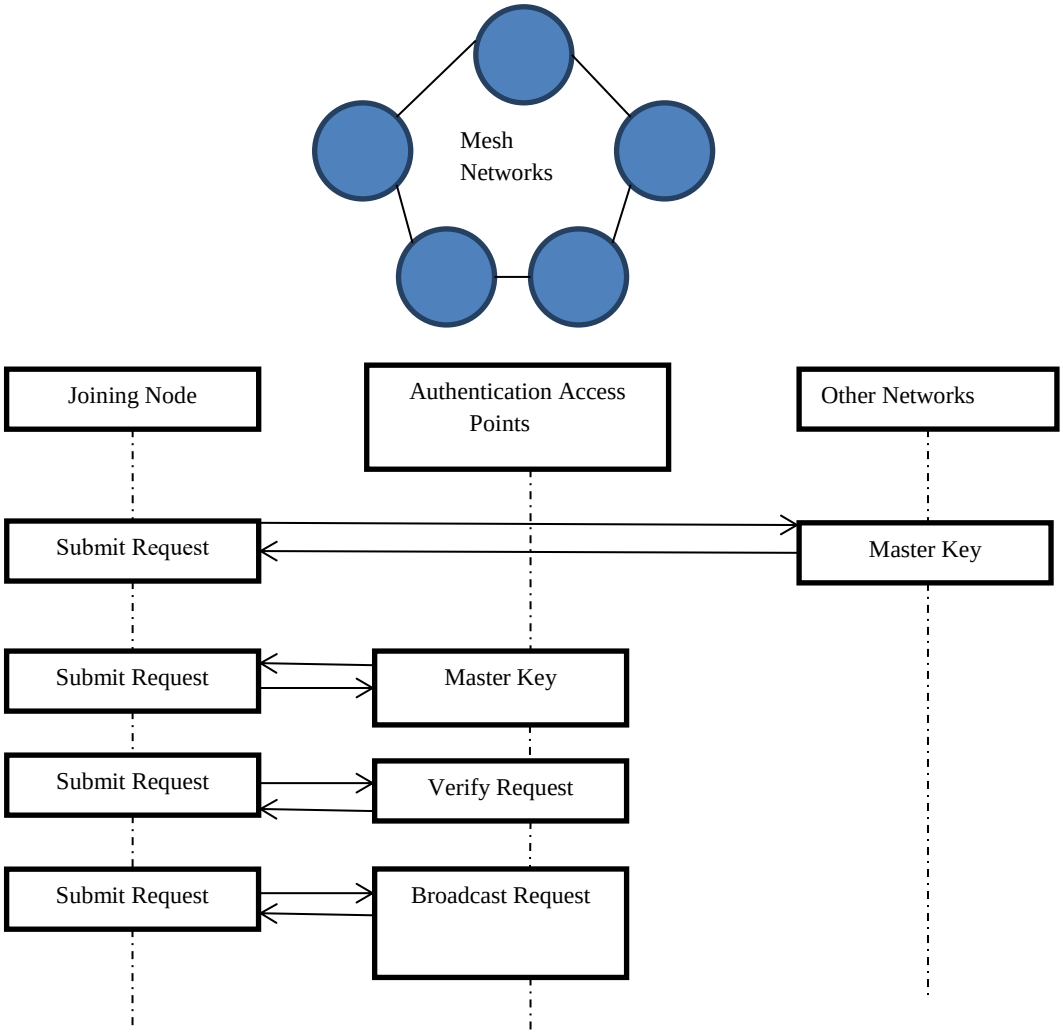

Fig. 3.5. Technique for Authentication

Every node that has been successfully joined to one of the connection points can now forward a query for authentication to the access points as a consequence of connecting with the nodes that are associated with access points. The point of entry will evaluate the entire region and authenticate the credentials distributed to the clients that undergo examination locally or internationally. When verification is undertaken in the End-to-End jurisdiction, customer licenses assigned to the access points will check out consumer-related data. If the authentication has not been verified yet, the newly connected node's server accepts the inquiry. Following the authentication technique, the two connected nodes will receive the master key from the DHCP-assigned IP addresses. On account of the integration node's designation as a mesh gateway, it will try to establish up-signal portions and authentication-based connection points, publish the same request to decentralized networks, and then initiate the operation. Figure 3.5 conveys the protocol for coping with the access point whilst on the verification procedure.

C. Cryptosystem Detection

Due to the user's login details being employed with the public key in the circumstance, there is no necessity to preserve and confirm the user's public key. This approach also prevents the attacker from assuming the requester's identity. Since certificates are not needed for authentication on cipher-based security mechanisms, configuration settings are made simpler, system construction costs are decreased, system operation and maintenance are made simpler, and system performance is increased. Algorithm 2 supplies a visual representation of the algorithm connected to the cryptosystem identification.

Algorithm 2: Detecting Cryptosystem

Input: $Y_l \leftarrow S,\ T \leftarrow (Pub_B,\ JE_B,\ Sign)$

Output: $D_J \leftarrow Y_l(B_\beta)$

Begin

$T \leftarrow B_{req}$

$O_T \leftarrow Publickey_{keyexchange}$

$Publickey_{keyexchange} \leftarrow EI_{key}$

$T \leftrightarrow T > NT_{key} > B$

$NT_{key} = I_{LE}(public_{key},\ O_t)$

$NT_{key} \leftarrow encrypt$

$NT_{key}\{JE_l\} \leftarrow Public_B$

$T < VN_{key} > B$

$VN_{key} = I_{key}(Public_{key}, O_T/O_B)$

$T \leftarrow N_j$

$Signs \leftarrow Signs[I_2(N_1), N_1]$

$N_1 \leftarrow \{JE_t\}NT_{key}|JE_B|O_B|O_T|Pub_B|Pub_T$

$T \leftarrow UserB(y_1, y_2, \ldots y_0)$

$O_T \leftarrow Signs\ (I_2(pub_B|pub_T))$

$NB_{key} = TIB_1(NBkey, N_2|sign_B|Sign_T)$

$Ouput = Hash_B(T_B)$

End

Return

User B validates the system T, which might contain certain personally identifiable information that can help user B identify the information via third-party associated data, including the techniques that facilitate phone or email confirmations. This is why the public key has been turned on for user B despite the fact verification of it can collapse. After providing the authentication-related information, another user transmits information to the Blockchain to request approval to send the data. Upon affirming electronic signatures, incorporating the personal assurance, user B will make sure the user C-related data. User C is permitted testing so that they can communicate their specific information to user B.

3.6 Single Relay Model and ISHDAF Mutual Information Evaluation

The mutual information in this instance is defined as

$$\mathrm{I_{DT}} = \frac{1}{2} \cdot \log_2 \left(1 + \frac{|\mathrm{g_{rd}}|^2 \mathrm{P_{R1}}}{\mathrm{M_o}}\right), \quad (4)$$

This, according to information theory, must be bigger than S. Making simpler (1), and the predicate $\mathrm{I_{DT}} >$ S results in the relationship $|g_{rd}|^2\ 2 > (2^{2S} - 1)\mathrm{M_O}/P_{R1}$. Given that the relay node S is still inactive and that the threshold is T1 = $(2^{2S} - 1)M_o/P_{R1}$ and $|g_{rd}|^2 >$ T1, the source node R continues to transmit directly to the target node D in the second slot.

$$\mathrm{I_{DT}} = \frac{1}{2} \cdot \log_2 \left(1 + \frac{|\mathrm{g_{rd}}|^2 \mathrm{P_{R1}}}{\mathrm{M_o}}\right), \quad (5)$$

To achieve $|\mathrm{g_{rd}}|^2 > \mathrm{T_1}/2$, (2) must also be larger than S. The source sends the message when $\mathrm{T_1}/2 < |g_{rd}|^2 \leq T_1$ and the relay is left idle in the next slot.

$$I_{DE} = \frac{1}{2} \cdot \log_2 \left(1 + \frac{|g_{rd}|^2 P_{R1}}{M_o} + \frac{|g_{rd}|^2 P_{S1}}{M_o}\right). \quad (6)$$

The mutual information is stated as follows if the relay network sends using the AE protocol:

$$I_{AE} = \frac{1}{2} \cdot \log_2 \left[1 + \frac{|g_{rd}|^2 P_{S1}}{M_o} + \left(\frac{|g_{rs}|^2 P_{R1}}{M_o}, \frac{|g_{sd}|^2 P_{S1}}{Mo}\right)\right], \quad (7)$$

Where e $(x, y) = xy/ (1 + x + y)$.

The IRGDAE cooperative network's mutual information can be summed up as follows. When $|\mathrm{g_{rd}}|^2 > \mathrm{T_1}$. The link R-D's direct transmission failed when $T_1/2 < |g_{rd}|^2 \leq \mathrm{T_1}$. However, the retransmission in the second slot of time is successful, and the shared data is $\mathrm{I_{DST}}$.

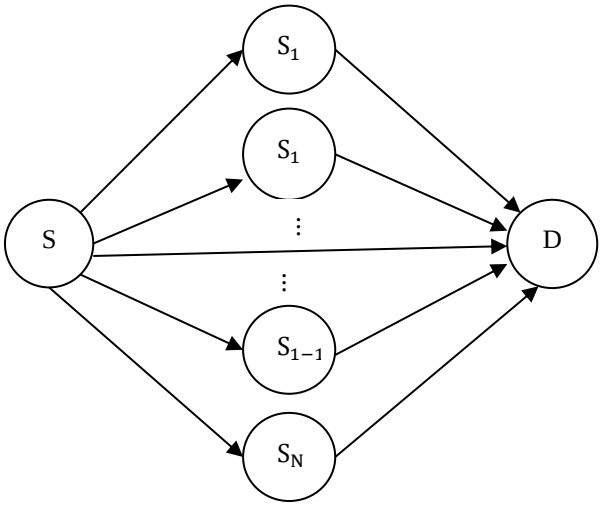

Fig. 3.6. System Model of The Multiple Relay Communication**.**

Multiple Relay System Model and Relay Selection Strategy

Transmission between the source node R & relay node $\mathrm{S_i}$ won't be interrupted if the relays properly decipher the signals that come from the source in Figure 3.6. The mutual data involved in the transmission in this instance is determined to be

$$I_{rsi} = \frac{1}{2} \cdot log_2 \left(1 + \frac{P_{R2}|g_{rsi}|^2}{M_o}\right). \quad (8)$$

$$\Omega_{\mathrm{DE}} = \{\mathrm{S_i}: |\mathrm{g_{rsi}}|^2 > \mathrm{T_1}\}, \quad (9)$$

$\Omega_{\mathrm{AE}} = \{\mathrm{S_i}: |\mathrm{g_{rsi}}|^2 > \mathrm{T_1}\}$.

Optimal Relay Selection

There are two actions to do to accomplish the highest RMS at the destination. First, from the sets Ω_{DE} and Ω_{AE}, respectively, the most effective relays of $\mathrm{S_b^{DE}}$ and $\mathrm{S_b^{AE}}$ are chosen. Between relay $\mathrm{S_b^{DE}}$ and relay $\mathrm{S_b^{AE}}$, the best relay Rb may then be selected.

$$\gamma^{\mathrm{AE}} = \gamma_1{}^{\mathrm{AE}} + \gamma_2{}^{\mathrm{AE}}, \quad (10)$$

Where the instantaneous RMS is written as $\gamma_1^{\mathrm{SE}} = \mathrm{P_{R2}}|\mathrm{g_{rd}}|^2/\mathrm{M_O}$ in the first slot and $\gamma_2^{AE} = \mathrm{P_{R2}P_{S2}}|\mathrm{g_{rsi}}|^2|\mathrm{g_{rsd}}^2|/\mathrm{M_O}(\mathrm{P_{R2}}|\mathrm{g_{rsi}}|^2 + \mathrm{P_{S2}}|\mathrm{g_{rsd}}|^2 + \mathrm{M_O})$ in the second slot. To select the optimal relay for the set Ω_{AE}, the instantaneous SNR γ^{AE} is maximized, and as a consequence, the candidate relay S_b^{AE} with the greatest RMS γ_2^{SE} is identified and stated as

$$\mathrm{S_b^{AE}} = argmax_{S_i \epsilon \Omega_{AE}} \left\{\frac{P_{R2}P_{S2}|g_{rsi}|^2|g_{rsd}|^2}{M_O(P_{R2}|g_{rsi}|^2 + P_{S2}|g_{rsd}|^2 + M_O)}\right\}. \quad (11)$$

The signals that come from the source and relay are merged by the NSC scheme for the cooperative system using the DE protocol, and the immediate RMS at the point of destination is obtained as

$$\gamma^{DE} = in(\gamma^{DE}m, \gamma^{DE}), \quad (12)$$

Where the RMS from the initial slot is $\gamma_1^{\mathrm{DE}} = \mathrm{P_{R2}}|\mathrm{g_{rsi}}|^2/\mathrm{N_O}$ and that from the next slot is $\gamma_1^{\mathrm{DE}} = \mathrm{P_{R2}}|\mathrm{g_{rd}}|^2/\mathrm{M_O} + \mathrm{P_{S2}}|\mathrm{g_{sid}}|^2/\mathrm{M_O}$. If each relay in set Ω_{DE} can effectively decode the signals, the destination's instantaneous SNR is γ_2^{DE}. The ideal relay R_b^{DE} is thus composed as

$$\mathrm{S_b^{AE}} = \arg\max_{\mathrm{S_i} \epsilon \Omega_{\mathrm{AE}}} \left\{\frac{\mathrm{P_{R2}}|\mathrm{g_{rd}}|^2}{\mathrm{M_O}} + \frac{\mathrm{P_{R2}}|\mathrm{g_{rid}}|^2}{\mathrm{M_O}}\right\}. \quad (13)$$

Finally, the greater instantaneous RMS between $\mathrm{S_b^{DE}}$ and $\mathrm{S_b^{AE}}$ may be used to choose the best relay $\mathrm{R_b}$. The signal that originates from the point of origin is then sent appropriately in the appropriate manner. It is written as

$$\mathrm{R_b} = \max\{\ \mathrm{S_b^{AE}},\ \mathrm{S_b^{DE}}\}. \quad (14)$$

Meanwhile, the suggested relay selection strategy's cooperative transfer of the GDAE scheme's mutual information is

$$I_{\mathrm{GDAE}} = \{I_{DE'}, |g_{rsb}|^2 \geq T_2\} \quad (15)$$

$I_{\mathrm{GDAE}} = \{I_{AE'}, |g_{rsb}|^2 \geq T_2\}$,

Where $|g_{rsb}|^2$ is the channel gain of link R-$\mathrm{S_b}$ ·

4. Implementation and Experimental Parts

Analysis and simulation results:

The voice samples used in our projected experiment were the same as those included in the experimental conclusion. We monitor that the talk-spurt durations of our verbal channels—eight vocal streams for five discussions—cannot be effectively classified as exponential limits. Utilizing the Johnson exponentially investigation, the exponentially for 55% of spoken signals is ignored at the 75% esteem grade.

This research utilized standard MAC parameter values, which are displayed in Table 1, and the Packet Delivery Ratio (PDR), Jitter

Distribution Statistics (JDS), Average End to End Delay (AEED), Packet Collision Ratio (PCR), and Delay Time (DT) were computed by contrasting those figures with the outcomes found.

Table 1. Parameters for stimulation

Parameter	Wi-Fi	Wi-Fi-Max	Bluetooth	Description
Traffic method	Continuous	Continuous	Continuous	Uses CBR
Total nodes	change	Change	change	No. of network members
Node positioned	Invariable	Invariable	Invariable	Guidelines for node arrangement
Mobility	5-91(m/s)	5-91(m/s)	5-91(m/s)	Node travelling with its speed
Simulation time	9s	9s	9s	Top execution time
Power	81	21	31	These are the wavelengths that are used
Terrain dimension	1900, 1900	1900, 190, 0	1900, 190, 0	Phy.area the nodes are placed
Radio frequency	39 eq	39 eq	39 eq	These are the utilized frequencies
Routing etiquette	aodv	aodv	aodv	These standards are implemented in routing.
Mac protocol	1600 ns	NA	NA	Lag in broadcasting
Bandwidth	4000000	1600000	1200000	These are the employed bandwidths.
MAC propagation	802.3	804.1	804.12	These are the approved behaviors.

Scenario 1 - Packet delivery ratio:

PDR is an extremely significant aspect to be taken into contemplation when sending packets. PDR is the percentage computed by partitioning the entire quantity of packages transferred by the aggregate volume of packets collected. Figure 4.1 demonstrates this info, which solely accounts for traffic flowing along the reverse route. Table 2 highlights the different parameters that may influence the parameter values. These parameters encompass incoming packets, team balance, action range, and the movement of nodes. Several kinds of variables might have taken part, especially action range, node mobility, group size, and packet dimensions.

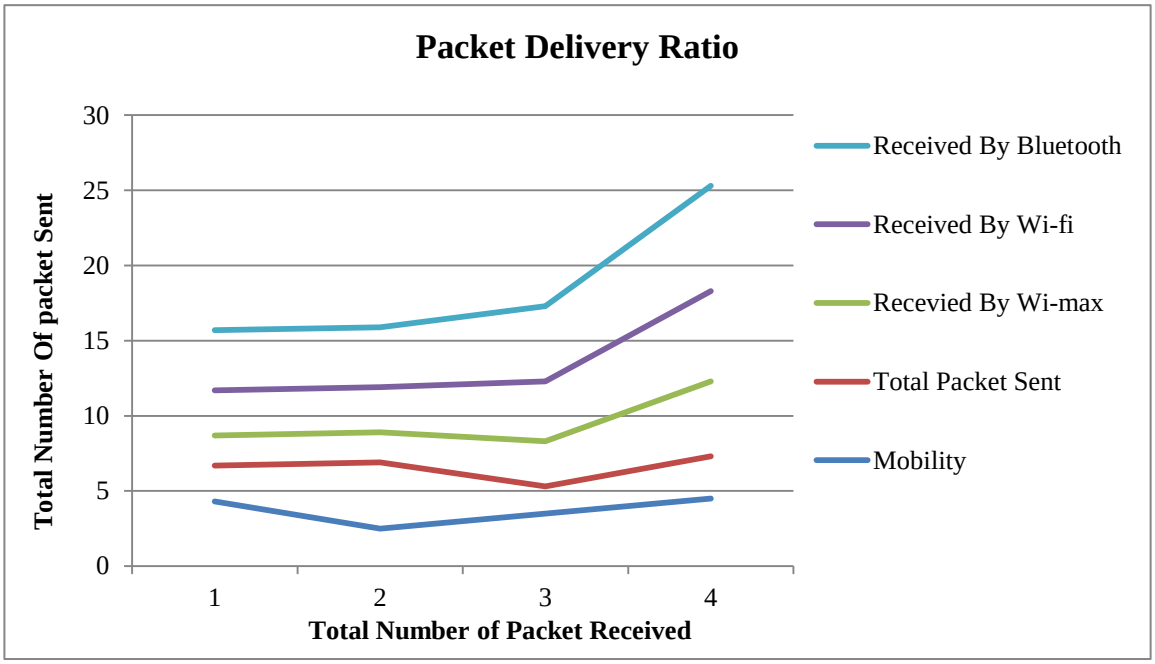

Fig. 4.1. Packet Delivery Ratios

Table 2. Packet Delivery Ratio

Movement	Aggregate packet transmitted	Collected by Wi-Max	Collected by Wifi	Collected by Bluetooth
6	4987	4987	1124	511
11	4987	4987	1357	801
16	4987	4987	1426	955
21	4987	4987	1771	1291
26	4987	4987	1959	1602
31	4987	4987	2377	1901
36	4987	4987	2501	2001
46	4987	4987	3188	3004

Scenario 2 - Jitter Distribution Statistics

For an assortment of accurately defined dynamical experiments over a network infrastructure with a learning style, the dispersed filtering constraints can be conquered. This class is vulnerable to confrontational underhandedness assaults which might end up in unexpected victories or defeats with a predefined frequency. The parameter values for sensing equipment are not uniform across each of the devices, as depicted in Table 2. The systemic technique encompasses quite a few unforeseen failings and quirks that are beneficial in real-life situations associated with networked machines. Figure 4.2 suggests the setup of a dispersed filtering mechanism throughout a problematic scenario with decreasing evaluations exposed to misleading threats.

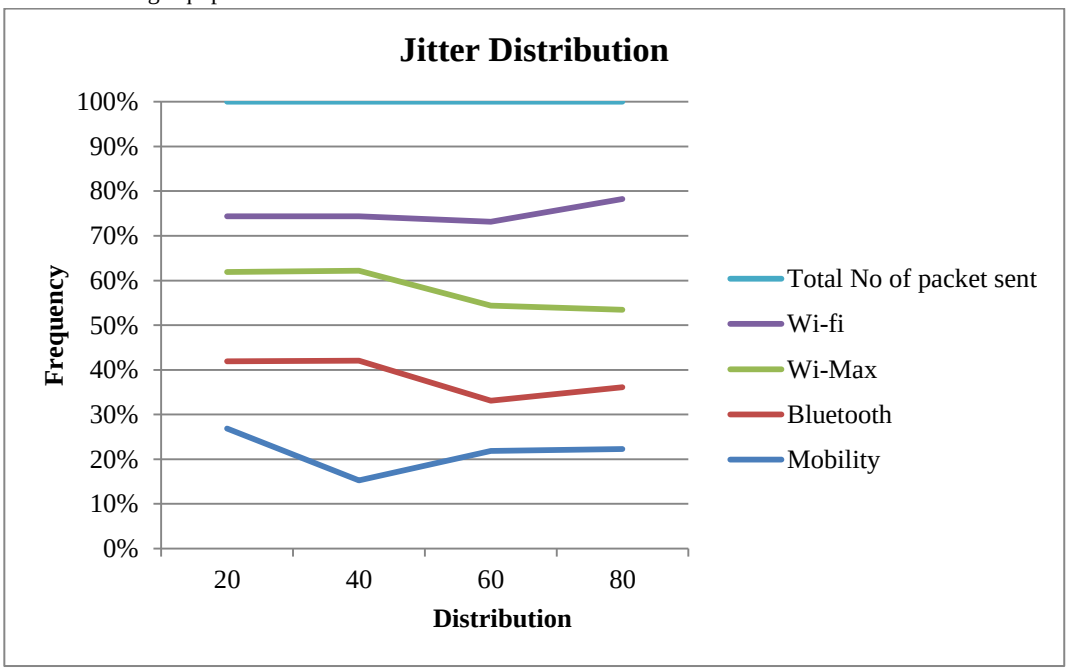

Fig. 4.2. Jitter Distribution Statistics

Table 3. Jitter Distribution Statistics

Mobility	Packets transferred in aggregate	Wi-max	Wi-Fi	Bluetooth
6	11	8	3	10
11	21	13	4	12
16	31	20	4	20
21	41	22	4	22
25	51	33	5	27
31	61	50	5	32
36	71	55	6	40
41	81	79	9	42

Scenario 3 - Average End to End Delay

The total amount of the last packet latency is prompted by the network infrastructure. Figure 4.3 showcases the progression, distribution, and lags in communication. Slowdowns all across the whole method from initiation to completion, encompassing buffering and propagation, are termed as "final process." The cumulative lag of the journey is the aggregate of the delays at every node. Table 3 exhibits the node-to-node lag and parameter readings for each link.

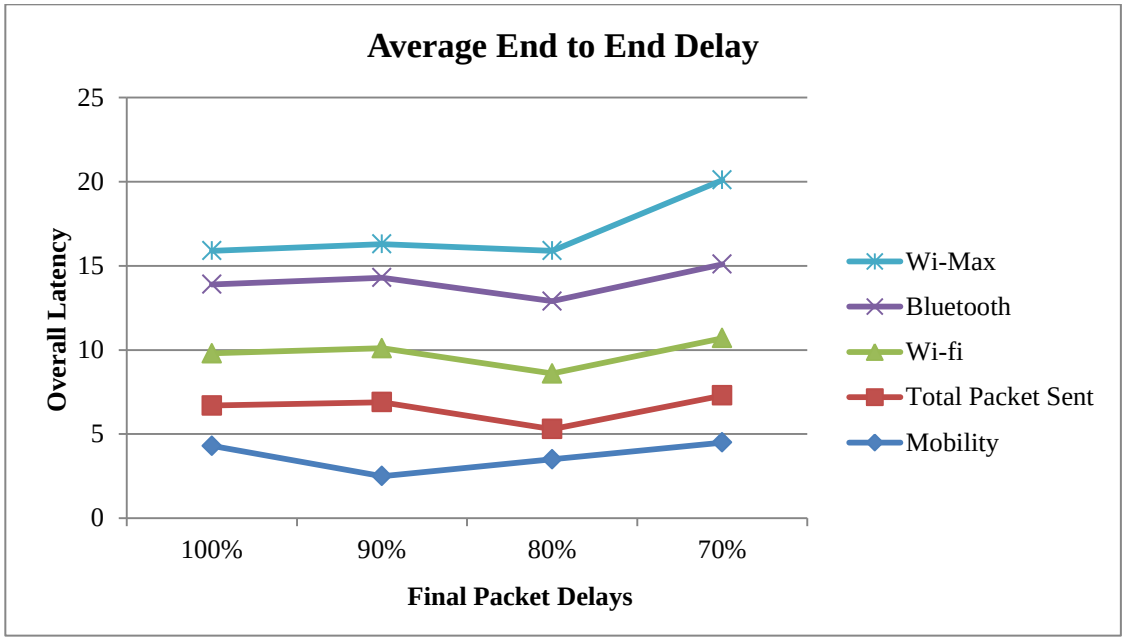

Fig. 4.3. Average End to End delay

Table 4. Average End to End Delay

Mobility	Packets transferred in aggregate	Wi-max	Wi-Fi	Bluetooth
6	0.01	0.005237	0.021	0.03
11	0.02	0.005346	0.02088	0.0204
16	0.05	0.005268	0.001984	0.001975
21	0.07	0.005326	0.0019246	0.00192
26	0.09	0.005329	0.001835	0.001822
31	0.11	0.005433	0.00182	0.001803
36	0.16	0.005329	0.001733	0.001722
41	0.17	0.005330	0.001730	0.001703
46	0.18	0.005329	0.001644	0.001624

Scenario 4 - Packet collision ratio

The occurrence characterized as a "packet collision" in an online system is the synchronous delivery of two or more packages at an identical destination node from distinct source nodes. There is a significant risk of collision when several packets transit from a certain source node to the same destination node. The total number of particles that arrive at a specific place is proportional to the total number of individual packets [18]. This shows the total number of packets that a specific node has witnessed; they are shown in Table 5 along with the parameter values. The packet collision ratio is defined as the proportion of all packets lost as a result of packet collisions involving additional packets. This is the ratio as a function of the total number of packets. The packet loss rate is the percent of data packets that fade away at a certain time-end node owing to errors like a collision or contamination. It affects in a specific way assuming the total number of packets (including malformed and colliding packets). Figure 4.4 displays how the graph demonstrates that a certain amount of collisions has an excellent effect on Wi-Fi operation.

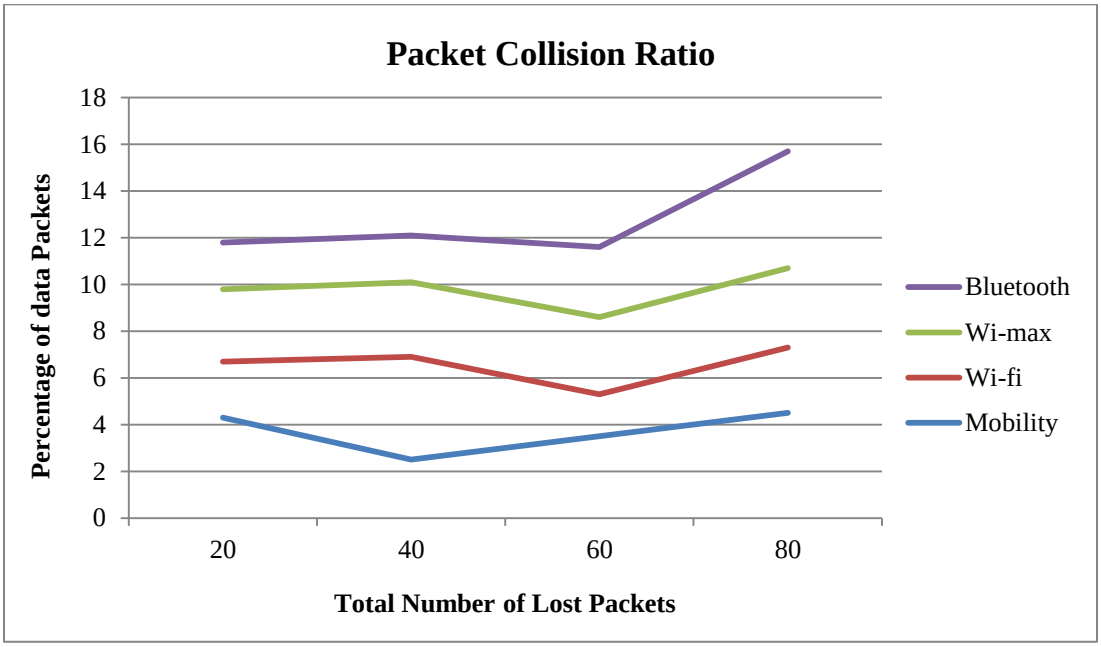

Fig. 4.4. Packet Collision Ratio

Table 5. Packet collision Ratio

Movement	Wifi	Wi-Max	Bluetooth
16	46	7	58
21	38	5	47
26	30	4	40
36	22	4	25
56	20	3	19
61	14	3	12

Scenario 5 - Packet throughput

Argued alternatively, it supports the bit-per-second velocity for movement. The matrix demonstrates the state of modern technology. It is either the best or it isn't the best because of the matrices, which allow the system to provide the maximum throughput and speed. Even though outflow bandwidth can be dictated by intake or exit efficacy, it frequently needs to be derived by evaluating the efficacy parameter values [19], which are presented in Table 6. Wi-MAX is a wireless connection with rapid speed. As Figure 4.5 points out, the harmful effect of Wi-Fi technology is very rare [20, 21].

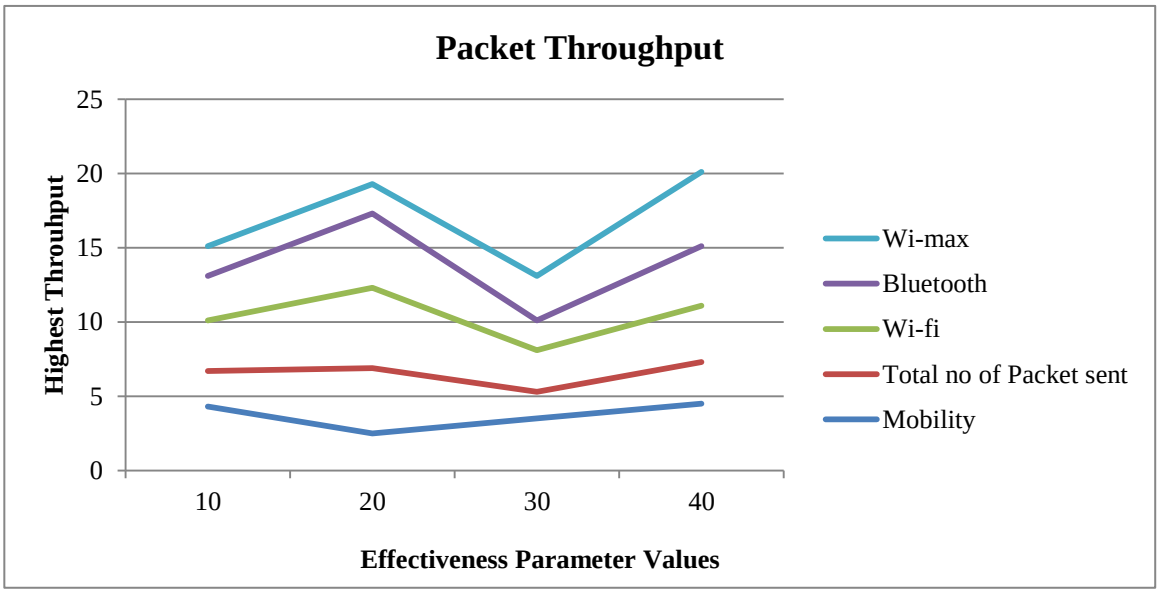

Fig. 4.5. Packet Throughput

Table 6. Packet throughput

Mobility	Packets transferred in aggregate	Wi-max	Wifi	Bluetooth
6	11	26	3	12
11	21	30	4	19
16	31	33	4	22
21	41	50	6	30
26	51	52	6	39
31	61	60	7	42
36	71	61	8	53

5. Conclusion

The proposed blockchain-based Topographical Relay Selection Secure Routing (BTRSSR) method takes into account bandwidth, latency, and flow management for multi-hop communication. In this case, a completely different transmission channel is chosen by avoiding all dangerous areas and assuring the security of sent packets. By implementing an Adaptive Intrusion Detection System (AIDS), numerous security threats such as tampering assaults, dropping attacks, flooding attacks, and malicious attacks are discovered and are eliminated.

This paper has offered a thorough examination of the most important wireless access networks that are now under development, along with an explanation of how these advancements may be combined to offer last-mile technology. While it has been shown to be the best, the WI-MAX specification is not anticipated to take the place of Bluetooth or Wi-Fi. The behaviour of certain WSN network typologies that are applicable to real-world industrial applications has been shown and examined. Our primary contribution is the technologies we offer and analyse, which are essential for VoIP and video on demand implementation. We do this by investigating a wide range of design possibilities and testing the suggested optimisation methods. The results of the VoIP capacity tests are positive for VoIP deployment in wide area networks. Furthermore, the VoIP capability outcomes and VoD bandwidth tests show that the localization of trip patterns plays a critical impact. According to our research, the voice and video capacity drops when the number climbs from 3 to 5 hops by a significant margin of more than 65%. Implementing VoIP and VoD in WMNs may be successful, according to the VoIP capacity testing. Traffic pattern specialisation has a major impact on VoIP's high level, according to VoIP study as well. The capacity for VoD in an integrated scenario will be higher if the traffic patterns are more specialised than in a stand-alone situation.

More investigation could determine the ideal parameters for the suggested algorithm and examine its efficacy in other procedures and scenarios. Further study could look into other methods for optimising VoIP over WMN performance, such as error correction and QoS mechanisms. The viability and usefulness of putting the suggested algorithm into practise in actual networks should potentially be investigated in more detail.

References

[1] Ghaleb, F. A., Al-Rimy, B. A. S., Boulila, W., Saeed, F., Kamat, M., Rohani, F., &Razak, S. A. (2021). Fairness-oriented semichaotic genetic algorithm-based channel assignment technique for node starvation problem in wireless mesh networks. *Computational Intelligence and Neuroscience*, *2021*.

[2] ThandavaMeganathan, N., &Palanichamy, Y. (2015). Privacy preserved and secured reliable routing protocol for wireless mesh networks. *The Scientific World Journal*, *2015*.

[3] Tian, L., Li, M., Si, P., Yang, R., Sun, Y., & Wang, Z. (2023). Design and Optimization in MEC-Based Intelligent Rail System by Integration of Distributed Multi-Hop Communication and Blockchain. *Mathematical Problems in Engineering*, *2023*.

[4] Prasath, A. R. (2021). Bi-Fitness Swarm Optimizer: Blockchain-Assisted Secure Swarm Intelligence Routing Protocol for MANET. *Indian Journal of Computer Science and Engineering*, *12*(5), 1442-1458.

[5] Loret, J. S., & Kumar, T. G. (2021). An Authenticated Trust Based Security Mechanism for Video Transmission in Wireless Mesh Networks. *Journal of Internet Technology*, *22*(4), 757-764.

[6] Bello, O. M., &Taiwe, K. D. (2016, March). Mesh node placement in wireless mesh network based on multiobjective evolutionary metaheuristic. In *Proceedings of the International Conference on Internet of Things and Cloud Computing* (pp. 1-6).

[7] Ilakkiya, N., &Rajaram, A. (2023). Blockchain-assisted Secure Routing Protocol for Cluster-based Mobile-ad Hoc Networks. *INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL*, *18*(2).

[8] Zeng, Z., Zhang, X., & Xia, Z. (2022). Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks. *Wireless Communications and Mobile Computing*, *2022*, 1-10.

[9] Ajayi, A. O., Adigun, A. A., & Ismaila, W. O. (2015). A review of routing protocols for practical rural wireless mesh networks (WMNs). *International Journal of Computer Applications*, *114*(16).

[10] Maliwatu, R. (2021). A new connectivity strategy for wireless mesh networks using dynamic spectrum access.

[11] Kishore, M. K., Nancharaiah, B., & Kumar, V. G. (2023). BLOCKCHAIN-BASED TOPOGRAPHICAL RELAY SELECTION SECURE ROUTING (B-TRSSR) TECHNIQUE FOR THE MULTI-HOP COMMUNICATION IN WIRELESS MESH NETWORKS (WMN). *Journal of Data Acquisition and Processing*, *38*(2), 1763.

[12] Kishore, M. K., Nancharaiah, B., & Kumar, V. G. (2023). NOVEL OPTIMIZATION ALGORITHM TO ENHANCING THE PERFORMANCE FOR VOIP AND MDVC VIDEO TRANSMISSION IN WIRELESS MESH NETWORK. *Journal of Data Acquisition and Processing*, *38*(2), 1749.

[13] Shillington, L., & Tong, D. (2011). Maximizing wireless mesh network coverage. *International Regional Science Review*, *34*(4), 419-437.

[14] Bao, J., Wu, J., Liu, C., Jiang, B., & Tang, X. (2017). Optimized power allocation and relay location selection in cooperative relay networks. *Wireless Communications and Mobile Computing*, *2017*.

[15] Ghaleb, F. A., Al-Rimy, B. A. S., Boulila, W., Saeed, F., Kamat, M., Rohani, F., & Razak, S. A. (2021). Fairness-oriented semichaotic genetic algorithm-based channel assignment technique for node starvation problem in wireless mesh networks. *Computational Intelligence and Neuroscience*, *2021*.

[16] Thandava Meganathan, N., & Palanichamy, Y. (2015). Privacy preserved and secured reliable routing protocol for wireless mesh networks. *The Scientific World Journal*, *2015*.

[17] Seyedzadegan, M., Othman, M., Ali, B. M., & Subramaniam, S. (2011, November). Wireless mesh networks: WMN overview, WMN architecture. In *International conference on communication engineering and networks IPCSIT* (Vol. 19, p. 2).

[18] Bayer, N., Xu, B., Rakocevic, V., & Habermann, J. (2010). Application-aware scheduling for VoIP in wireless mesh networks. *Computer Networks*, *54*(2), 257-277.

[19] Kishore, M. K., Nancharaiah, B., & Kumar, V. G. (2023). NOVEL OPTIMIZATION ALGORITHM TO ENHANCING THE PERFORMANCE FOR VOIP AND MDVC VIDEO TRANSMISSION IN WIRELESS MESH NETWORK. *Journal of Data Acquisition and Processing*, *38*(2), 1749.

[20] Chai, Y., & Zeng, X. J. (2019). Regional condition-aware hybrid routing protocol for hybrid wireless mesh network. *Computer Networks*, *148*, 120-128.

[21] Rao, Y. M., Subramanyam, M. V., & Prasad, K. S. (2018). Cluster based hybrid routing protocol for wireless mesh networks. *Wireless Personal Communications*, *103*, 3009-3023.