Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776805

BLOCKCHAIN-BASED TOPOGRAPHICAL RELAY SELECTION SECURE ROUTING (B-TRSSR) TECHNIQUE FOR THE MULTI-HOP COMMUNICATION IN WIRELESS MESH NETWORKS(WMN)

M.K. Kishore
Research Scholar, Department of Electronics and Communication Engineering, GIET UNIVERSITY, Gunupur, Odisha, Pin- 756022 & Assistant professor, Department of Electronics and Communication Engineering, Usha Rama College of Engineering and Technology, Telaprolu. Ungutur Mandal, Krishna district, Andhra Pradesh -521109
Mail ID: m.koteswarakishore@giet.edu

Dr.B.Nancharaiah
Professor & HOD, Department of Electronics and Communication Engineering
Usha Rama College of Engineering and Technology, Telaprolu. Ungutur Mandal, Krishna district, Andhra Pradesh -521109, Mail ID:nanch_bn@yahoo.com

Dr. V. Gajendra Kumar
Associate Professor, Department of Electronics and Communication Engineering
GIET UNIVERSITY, Gunupur, Odisha, Pin-756022, Mail ID:rajigajendra1@gmail.com

Abstract

The most predominant technology for Internet of Things (IoT) related application is Wireless Mesh Network (WMN). Normally the issue generated in WMN is the selection of a path for secure packet transmission. A lot of methods are proposed in WMN for enabling the possibility of achieving secure packet transmission within the network or to other networks. The issues like delay, bandwidth, and security are the main constraints identified while accessing the WMN during packet transmission. In this work, a blockchain-based Topographical Relay Selection Secure Routing (B-TRSSR) technique for the multi-hop communication is proposed in consideration of the bandwidth, delay, and flow control. In this proposed method an entirely different transmission path is selected by avoiding all risky zones by ensuring the security of transmitted packets. The various security threats like tampering attacks, dropping attacks, flooding attacks, and malevolent attacks are identified and is eliminated by introducing an Adaptive Intrusion Detection System(AIDS). The issues like transmission delay, Bandwidth, and overload traffic are handled by introducing a routing metric called Bandwidth, Transmission delay, and Overload Handler (BTDOH). This was enhanced by modified Q-Learning algorithm which inturn supports the flow control strategies also. The experimentation results proves that the proposed hybrid model will supports the secure transmission of packets in Wireless Mesh Networks(WMN) in an effective manner when compared with other state of art methods.

Key Words: *Adaptive Intrusion Detection System(AIDS), Blockchain, Multihop communication, Topographical Relay Selection Secure Routing (B-TRSSR),Modified Q-Learning algorithm.*

I. Introduction

The mobility of MANET nodes allows them to roam freely throughout the network. Nodes' ability to communicate with other nodes is based on their single-hop or multihop communication area size. They are facilitating the transfer of data packets between nodes via multihop communication[1]. To ensure efficient delivery of sensed information, swarm intelligence techniques and enhanced dynamic source routing are used, with each party's path being determined by enhanced dynamic source routing. Optimizing node positions for relative transmission is accomplished through link scheduling. Transmitting nodes should have as few neighbors as possible to send data along the path with the fewest hops possible. There could be an increase in broadcasting failures due to the network's increased number of nodes[2].

Mesh WLANs self-organize and self-heal (WLANs). If damaged, it self-heals. Using WLAN mesh networks, this issue of too much high-speed Internet access may be solved. Due to their increased wireless network coverage, WLAN mesh networks are powering the global expansion of broadband internet access. Internet access the future, and wireless broadband networks power it[3]. The security technology of other WLANs cannot be used in WLAN mesh networks. There are no wires connecting the nodes in a WLAN mesh network. Passive listening and forging identities, data tampering, and other attacks are all possible in a multihop forwarding mesh network. Data tampering is possible in mesh networks. As the number of smart devices with ARM chips grows, cyberattacks become more likely. The speed and routing of wireless mesh networks improve depends on their safety[4].

In a WLAN mesh network, each node is responsible for routing its own segment. Mesh and non-mesh devices alike can connect to access points or Aps[5]. These nodes will be referred to as mesh APs from now on. Non-mesh devices can connect and share network resources with the 802.11 infrastructure mode of mesh access points[6]. WLAN mesh networks can be used by roaming users, so the assumption that the organization that owns the location will also run the network is incorrect. This enables businesses to share WiFi networks. Users, access points, mutual authentication, and encryption must all be considered when deploying mesh networks in an enterprise or campus.

In both developed and developing countries, wireless mesh networks (WMNs) allow people to connect to the Internet. Mesh networks have more channels and interfaces, and mesh routers are the backbone of these networks[7]. The latency and capacity of RMA wireless metropolitan networks (WMNs) are examined in this paper (MAC)[8]. A benefit of using Wireless Mesh Networks is that new nodes can be added to the network without requiring a complete reinstallation of the entire network (WMN). A reliable and energy-efficient routing protocol is needed to integrate smart IoT applications and Wireless Mesh Networks (WMN)[9]. Although ensuring the fastest possible WMN communication path is critical, it is problematic at the expense of low throughput and unacceptable delay.

Route-finding and data-transmission times are included in this delay. Due to link disconnection, the broadcasting mechanism generates redundant control packet transmissions[9][10]. There is a cost to reinitializing blind route discovery. Neither action takes

place outside the network in any way, shape, or form. Data transmission latency rises when networks are congested. A mesh client is any device that requires an active network connection with WMN, which is built on mesh routers. Networks with a high traffic volume may benefit from installing fixed nodes, such as mesh routers[11].

Mesh routers can transmit at higher power levels, have multiple antennas for receiving and transmitting data, and have an endless supply of energy[12]. Mesh routers communicate with mesh clients and gateways outside the client's communication range. Each hop along the mesh router backbone results in a different route for the packet. A packet can be sent to a specific node in a mesh network by a mesh router[13]. In WMNs, routers and clients communicate using different protocols. Mesh backbone traffic is unaffected by interference from mesh clients. IEEE 802.11a could be used for the backbone link in a mesh network, while IEEE 802.11b could be used for clients and routers. Both use the 802.11 standard. In areas where cable or DSL internet access isn't feasible, wireless mesh networks (WMNs) are seen as the networking technology of the future. Clients and routers are components of wireless mesh networks (WMN)[14]. There are two types of mesh routers: those that connect directly to the Internet and those that serve as gateways for other networks. Gateways serve as the backbone of the mesh network, allowing clients to connect to it. The backbone of the network is comprised of mesh routers.

In order to support wireless traffic delivery, the bandwidth between the Internet and non-gateway mesh routers needs to be distributed fairly among them. A new generation of wireless technology and spectrum access methods are being developed to meet the needs of an increasingly populous world, as the traditional static method of spectrum access is inadequate[15]. This is a result of an increase in wireless devices. Cognitive radios are desirable in a high-traffic wireless mesh network (WMN). Increased network capacity can be achieved using cognitive radios, which use spectrum more effectively[16]. They make it more challenging to allocate bandwidth. 802.11-based wireless mesh networks use the same channels for all mesh routers. WMN with cognitive radios is able to transmit at a wide range of frequencies because each node has access to multiple spectrum bands (channels). Data rates and transmission distances affect the options available to users when selecting a route and channel. Cognitive radios must not interfere with the primary users of a channel in order to use it. This is subject to change, however, as the actions of the primary user determine which channels are accessible.

II. Related Works

WMN is an ad hoc network of mobile clients and wireless mesh routers that can be set up and dismantled anytime. In the Internet of Things, WMN is an excellent choice for devices that require constant connectivity[17]. All wireless connectivity issues will be resolved quickly with a new router from Winnebago Networks (WMN) installation. WMN is now available for use in commercial and industrial IoT applications. In Wireless Mesh Networks (WMNs), mesh-enabled nodes may benefit from the Internet of Things (IoT) solutions by gathering real-time data and providing intelligent applications[18]. IoT-enabled route planning In recent months, WMN has seen an increase in its following. Data from the Internet of Things impact the routing operations of WMN. One networking solution is to use load balancing and interference-aware

cluster-based routing. These devices are referred to as routers with gateways for the WMN wireless mesh network[19].

The wireless LAN and cellular data networks are linked together by the bridge. Sending data packets to the gateway node allows mesh network clients to access the Internet. To be effective, a WMN must be flexible and well-organized. A dependable and energy-efficient routing protocol is required when creating multihop wireless routes for mesh-based smart applications[20]. Traffic from mobile clients to gateways can overwhelm some links. This hinders smart application routing. Routing WMN traffic must be changed, no matter how expensive. Routing protocols can be table-driven or source-initiated, depending on the implementation. This distinction is based on the routing strategy used.

Routing protocols that rely on tables must recalculate previously saved routes. Routes can be seen on a route table. When the need arises, the source node in these protocols initiates route discovery. By comparing to table-driven routing protocols, on-demand routing protocols consume less bandwidth and have lower overhead. When a network discovers a new path for communication, source nodes send Route Request (RREQ) packets. WMN data packet delivery is severely hindered without low path discovery latency. Route discovery latency is reduced, network capacity is increased, and regular communication is maintained by limiting unnecessary RREQ flooding. For a secure WLAN mesh network to be deployed, it is necessary to authenticate both users and access points (APs). Strongly recommended is a secure authentication mechanism[21]. Third-party configurations are required for local authentication to work; which of these configurations are still required.

Distributing traffic loads across multiple paths in a network is possible, thereby reducing congestion. End-to-end delay is reduced thanks to multipath routing, which also improves route maintenance for secure transmissions. Maintenance costs can be reduced by using location-based routing. Reliable zone-wide communication was a major topic of discussion in the Zone Routing Protocol (ZRP)[22]. Forecast FCC was used to implement MANET routing. Using this technique, the most congested node in the routing path is eliminated. It is possible to avoid network traffic by using neighboring nodes to determine the shortest path. There may be transmission delays when a large amount of data is transmitted. In order to make optimization more manageable, LDM was introduced.

Mobile node communication must be secure in an unfriendly environment to be successful. It can be challenging to secure MANETs due to their distinct differences from wired networks. This system has peer-to-peer networking, resource limitations, and a dynamic structure[23]. Overhearing neighboring nodes' packet forwarding status is common in reputation-based schemes. A Forwarder's reputation is based on the results of monitoring. Networks are safe from routing interruption attacks thanks to ESCT's technology. This method mimics human cognition by relying on information with a high degree of trust. The trustworthiness of the information received by mobile nodes is evaluated and shared. Each node shown here is constantly improving its ability to identify and remove harmful entities from the system[24].

Community networks are equipped with an SDWMN control plane for WMN transmission redirection. Experiments have shown that a shared WMN can handle more connections while providing the same bandwidth[25]. Multiple gateways are proposed by

Hussein et al. to improve throughput and latency. Saturation throughput and packet latency have both been improved thanks to multi-hop MAC protocols. Cui et al. have updated the FPBR traffic management programme. Enhanced forward pointers are used to manage Internet and internal network traffic in wireless mesh networks[26]. Using wireless mesh networks and short-interval interference, Aboubakar et al. developed a framework to manage network resources. According to them, a Markov model can better understand the MAC layer performance of an intelligent 802.11s IEEE grid wireless mesh network[27]. Immutability and decentralization make the blockchain an ideal solution for this issue because of the new cryptography of the blockchain. Blockchain, a public ledger that records all transactions, allows for decentralized self-management through point-to-point networks and distributed time-stamping servers. As quickly as possible, identity management applications and services are being developed by a team of dedicated developers. Shapuan et al. placed a hybrid cryptographic scheme. This uses Zero-knowledge allows users to conceal transaction information by interacting with the cryptographic algorithm[28].

Blockchain transactions are verified for legality and sender identity using cryptographic signatures. A safe environment is created for all transactions. As a last line of defense, signature algorithms guard the data associated with a transaction. The names and locations of the parties involved in the transaction and the dollar amount will remain anonymous. Blockchains already have mature attack algorithms like selfish mining, eclipse, and obstinate mining[29]. A blockchain-based access control method must be quickly developed to regulate user access to WLAN mesh networks. A wide range of techniques is needed in MANET to achieve stable mesh routers. Multipath routing protocols in MANET are used to identify communication paths from source to destination. These protocols only use a single source node for data transmission. There are alternate routes between the source and gateway in the event of a failure. Backup or alternate routes are used if the primary route is blocked. If a link on the primary route fails, the source node will switch data transmission to alternate routes that lead to the gateway. There should be a re-discovery of all previously discovered routes. WMN, on the other hand, necessitates establishing a solid infrastructure. Reinforcement learning is used in energy-sensitive mesh networks. In order to find the best route, reinforcement learning updates the routing table[30]. Improved power efficiency, failure rate, and spectrum efficiency are achieved. The importance of a non-learning routing algorithm grows as network scalability increases. Several studies have shown that multipath routing improves mesh networks. Routing metrics are not worth anything if there are no multiple routes. In order to find feasible routes, some routing protocols employ an aggregated value. An aggregated value, even if it reduces the time it takes to select a route, may not be reliable. Packets are routed via a variety of paths using. Several paths to the same gateway are used by a node when this occurs. Link disconnections have been eliminated, and network throughput has increased. The number of ways to get to a particular location is determined by comparing network parameters[31]. To take advantage of the on-demand distributed routing capabilities of these protocols, WMN requires a more reliable multipath routing solution. Router for wireless mesh networks that uses local repair and multiple constraints. The authors centralized control of channels, bandwidth, and packet routing. Afterward, they presented a distributed channel allocation and routing algorithm based on local traffic loads [32].

Network topology K-connected, low-interference networks can be assigned channels using their algorithm. A quality-of-service routing algorithm can help you find the best route for connection requests requiring much bandwidth. Both algorithms are capable of locating connections with an adequate bandwidth. A centralized approximation algorithm with a constant bound was suggested by [33] as a way to jointly compute channel assignment, routing, and scheduling solutions for equitable rate allocation. The authors of [34] used a fast primal-dual algorithm to investigate a similar problem and discovered throughput upper bounds. Using this information, they devised heuristics for assigning two channels to a single signal. Cross-layer solutions were used by the researchers to address rate allocation, routing, scheduling, power control, and channel assignment. Congestion control, channel allocation, and scheduling were all addressed in a single algorithm by [35]. Network utility maximization problems for the joint channel, interface, and MAC allocation were formulated by them.

The researchers developed an exact binary linearization algorithm and an approximate dual decomposition algorithm. Neither of the algorithms was theirs. An excellent introduction to cognitive radio networks is given by Filali et al.[36]. To come up with solutions that are both fair and efficient, numerous heuristic algorithms have been developed. An algorithm for fair spectrum allocation based on a multichannel contention graph(MCCG) was proposed by Tegou et al.[37] This was a way to measure the amount of interference. Time-spectrum blocks for cognitive radio users have been discussed using centralized and distributed protocols [38]. Local bargaining-based spectrum allocation was proposed using cognitive radios in wireless ad hoc networks. There was also the introduction of a distributed architecture for spectrum management and usage rules. According to [39], the per-node throughput for a specific WMN topology and gateway location can be determined using an approach based on collision domains.

III. Proposed Method

A. Topographical Relay Selection Secure Routing (B-TRSSR) technique

For delivering the packets in a secured manner a Topographical Relay Selection Secure Routing (B-TRSSR) technique for the multi-hop communication is proposed. Here the information sharing is from satellite or cloud to the wireless mesh networks. The available nodes from Internet of Things (IoT) are selected which is based on the availability of the channel and the connectivity of the links that is determined for moving forward to the destination nodes. The possibility of the nodes available with less channel interference and the better connectivity of the links might be responsible of the selection of the bandwidth to the effective nodes. The architecture for the proposed B-TRSSR is shown in figure 1.

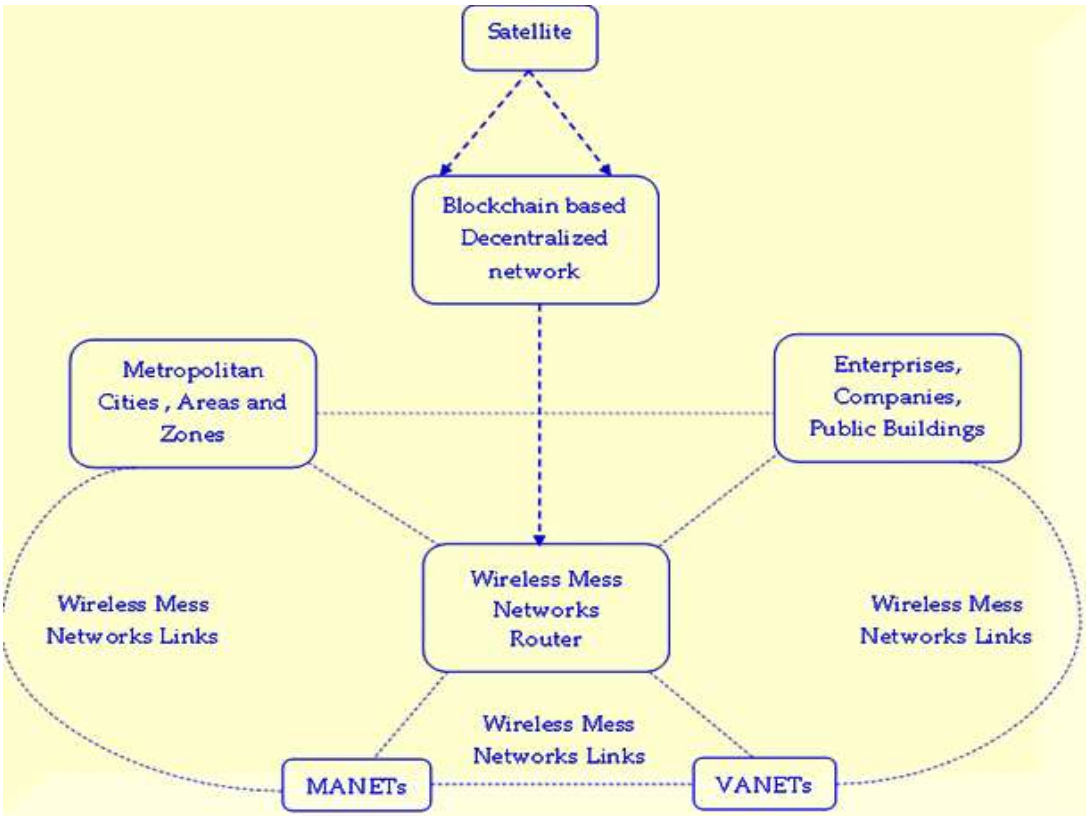

Figure 1: Architecture for the Proposed WMN Routing System

The model prescribed for the mobility is applicable to the architectures like VANET, MANET and other 5G /6G Applications. Normally this could be done by selecting the random paths which describes the movement of nodes by providing the most accurate information by finding out the mobility of the specific nodes. The example scenario behind the B-TRSSR technique is illustrated in figure 2. The un trusted nodes will be responsible for the selection of the trusted nodes and thus it will enable the connectivity over the links. The rates depicted for the channels might be determined by the selection of the trusted relay nodes. The delay nodes which are trusted might be based on the ratings provided and in consideration with the nodes which took part in the challenges provided. The available nodes which are participated in the contest might get added to the list of relay nodes. The selection of nodes for transmission might be done with the help of ratings allocated. The nodes which is not involved in the challenge contest or if it doesn't complete the contest might not get selected for the routing.

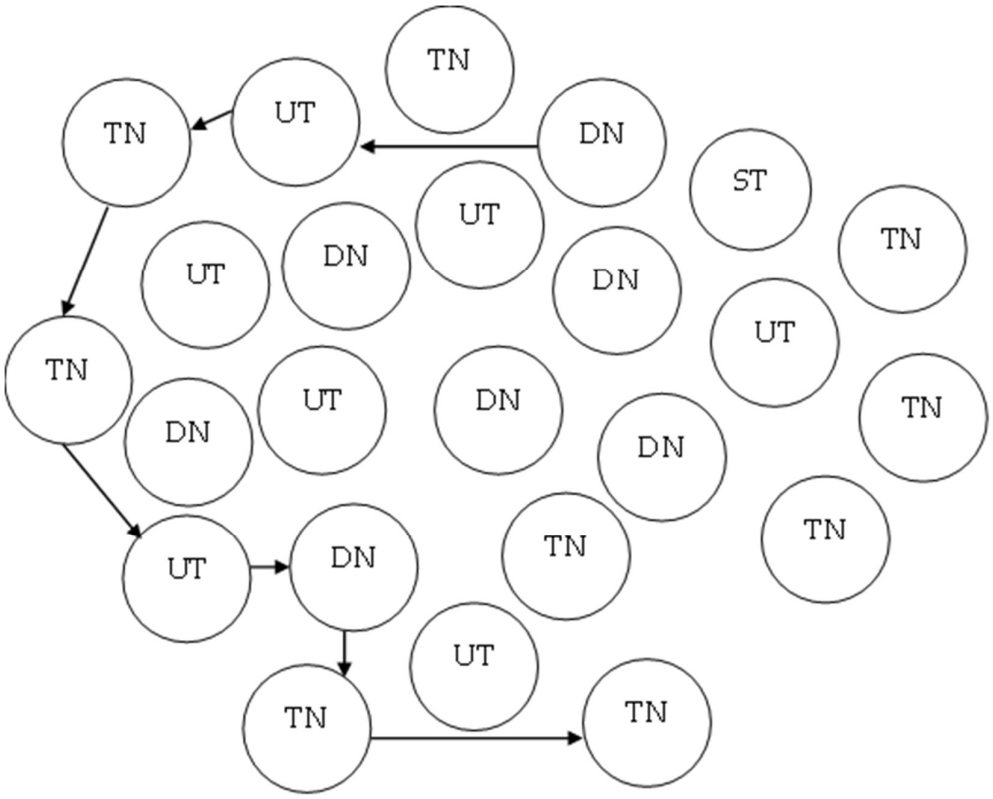

Figure 2: Example Scenario of B-TRSSR technique

The rating of the nodes is mentioned under various ratings ranging from 0 to 5. Hence the maximum possible ratings are compared with the average rating and obtained the value of 3.5 rating against the selected nodes for further processing. Hence the nodes with high rates might be taken as trustable ones and hence from here the bandwidth-related nodes are taken out for transmission of data. The ratings of the nodes will be calculated by considering the control message like the route request (R_{req}) and route reply (R_{rep}) which is send to the nodes which is present in the system dedicated for the communication. The algorithm representing the determination of the average node rating (R_N) is mentioned below in algorithm 1.

Considering the variations identified for the various counts the route request (R_{req}) along with route reply (R_{rep}) is passed along to the separate nodes which delivers the individual nodes with value R_N could be calculated. The R_N is calculated with the mathematical expression given below

$$R_N \leftarrow \sum_{k=1}^{N}\left(\frac{\left[X_{req} - X'_{rep}\right]}{X_{req}}\right)*100 \quad (1)$$

Where, X_{req} mentions the request sent to the route and X_{rep} represents the requests which is not send for receiving the requests. Here three possible occurrences are notified across various intervals ie; Y_{req} and Z_{req}. The three various circumstances might correspond to the fine tuning of the node selection criteria.

Algorithm 1:Algorithm for Average Node Rating (R_N) determination

$Input: Ctl\_q\ to\ Nbr(N)$

$Output: Tr(N) \leftarrow R_N$

$Consideration: A \leftarrow X_k, B \leftarrow Y_k, C \leftarrow Z_k$

Begin

$X_k \leftarrow n(1,2,3,...T_l)$

$for(i = 1 to N)$

Broadcast $B_n \leftarrow R(1,2,...l)$

$$Calculate\ R_N \leftarrow \sum_{k=1}^{N}\left(\frac{\left[X_{req} - X'_{rep}\right]}{X_{req}}\right)*100$$

$Y_k \leftarrow n(1,2,3,...T_l)$

$for(i = 1 to N)$

Broadcast $B_n \leftarrow R(1,2,...l)$

$$Calculate\ R_N \leftarrow \sum_{k=1}^{N}\left(\frac{\left[Y_{req} - Y'_{rep}\right]}{Y_{rep}}\right)*100$$

$Z_k \leftarrow n(1,2,3,...T_l)$

$for(i = 1 to N)$

Broadcast $B_n \leftarrow R(1,2,...l)$

$$Calculate\ R_N \leftarrow \sum_{k=1}^{N}\left(\frac{\left[Z_{req} - Z'_{rep}\right]}{Z_{req}}\right)*100$$

if $R_N >> 3.5$

The node is added to the relay node list

if $1 > R_N > 3.5$

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

Re*turn*

The trustable nodes follow different paths by considering the ratings provided X, Y, and Z are the three possible passages dedicated to secure transmission. The three paths will be controlled by the decentralized unit framed with blockchain. The selection of nodes for trusted transmission while considering the connections across the links are evaluated to the entire region for passing across the data which is sensed along with the relay nodes. The control packets that is passed in between the nodes are passed for estimating the needed bandwidths fixed in between the selected nodes. The packets that are scheduled based on the availability of the bandwidths that makes the dedicated networks to be free of congestion and the data that are delivered without any such losses. The measurement identified for the control packets along the consideration with the connectivity and the bandwidth is represented mathematically as

$$Bandwidth, Bw(n) = \sum_{x \leftarrow R_n}\left[\frac{\sum_{ni,nj}^{data\_rate} R_n\left(w(n), \Phi\right)}{T_r(n-1)}\right] + \sum_{x=1}^{n} R_n(x) \quad (2)$$

Where, Bw(n) is the bandwidth, w(n) is the nodes data and ∅ is the channel overheads. The nodes that are moved might gets connected over the longer time period which estimates the total reference value of the connectivity provided between the links. The reference values dedicated to the link duration might be available to evaluate the probability of occurrence of the existing nodes. The probability prediction is set to the nodes with the least data rate and the nodes that are given available so far might be able to communicate to the range that is not specified within the range of communication and is mentioned in the mathematical model as

$$l_{long} = P(R_N > T_r)_x \quad (3)$$

The probability of the available links can be predicted and is obtained in order to consider the ranges of communication that exist in between the nearby nodes in the available paths. The path variation can be modelled across the paths provided. Hence the intrusion of the channel and the related congested networks that is caused because of the high data traffic which can be reduced with the availability of the free spaces in the bandwidth and high connectivity links used for the transmission purposes.

B. Blockchain-Based Authentication

The topographical information can be processed through the decentralized module which in turn keeps ride of the authenticated information through the overall access points. The nodes which get associated with the authentication can be of various types like MANETs, VANETs, 5G and 6G communications etc.

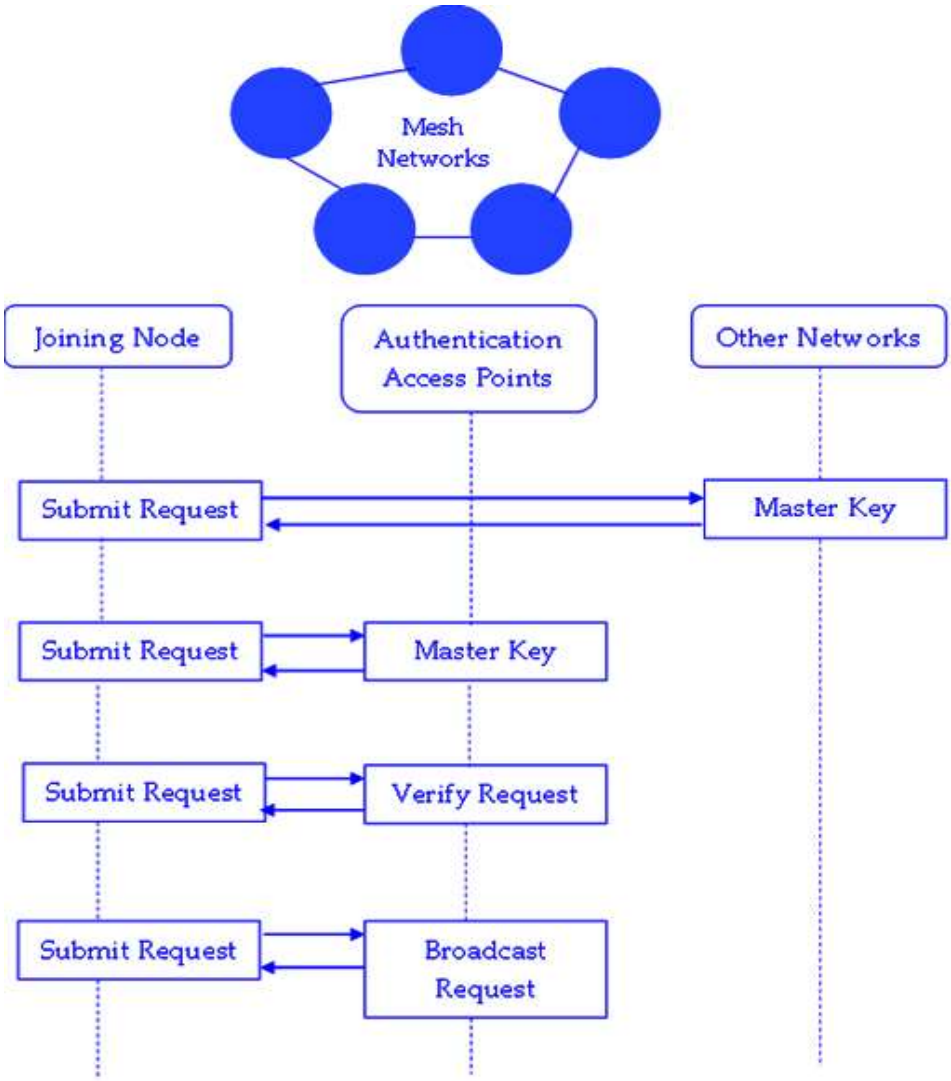

Figure 3: Authentication Procedure

The joining nodes which is associated with the access points might makes the nodes which is joined in any of the nodes will now send an authentication request to the access points.

The access point will check the total area and verifies the certificates allocated to the clients which is examined locally or globally. The client certificates allocated to the access points will verify the client-related information where the execution of the authentication is done at the End-to-End region. If the authentication is not verified yet then the request is given to the server at the joining node. After the authentication process the nodes which is joined will get the master key from the IP addresses allocated to the DHCP. Since the joining node is a mesh access point, it will try to establish the signal sections along with the authentication-based access points and it will broadcast the same request to the decentralized networks and from there it will starts to operate. The procedure for authentication process in dealing with the access point is illustrated in figure 3.

C. Cryptosystem Identification

There is no need for storing and signing the user's public key because the identity of the user in the situation can be utilised as the public key. The plan also guards against the attacker stealing the identity of the requester. Authentication on cipher-based security mechanisms do not require certificates, which simplifies configuration settings, lowers system building costs, simplifies operation and maintenance, and boosts system performance. The algorithm corresponding to the cryptosystem identification is illustrated in algorithm 2.

Algorithm 2: Cryptosystem Identification

$Input: X_k \leftarrow R, S \leftarrow (Pub_A, ID_A, Sign)$

$Output: C_I \leftarrow X_k(A_\alpha)$

Begin

$S \leftarrow A_{req}$

$N_s \leftarrow Publickey_{keyexchange}$

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

$S \leftrightarrow S > MS_{key} > A$

$MS_{key} = H_{KD}(public_{key}, N_s)$

$MS_{key} \leftarrow encrypt$

$MS_{key}\{ID_k\} \leftarrow Public_A$

$S < UM_{key} > A$

$UM_{key} = H_{key}(Public_{key}, N_s / N_A)$

$S \leftarrow M_i$

$Signs \leftarrow Signs[H_2(M_1), M_1]$

$M_1 \leftarrow \{ID_s\} MS_{key} \mid ID_A \mid N_A \mid N_S \mid Pub_A \mid Pub_S$

$S \leftarrow UserA(x_1, x_2, ...x_n)$

$N_s \leftarrow \text{Si}\, gns(H_2(pub_A \mid pub_S)$

$MA_{key} = SHA_1(MAkey, M_2 \mid sign_A \mid Sign_S)$

$Output = Hash_A(U_A)$

End

Re*turn*

The system S gets authenticated by the user A which might have some identifiable information which can support the users A for identifying the information's via third party related information which includes the methods which supports the verifications through email or phone. Then if the validation of it may end with failure and hence the public key is enabled for user A. Then another user sends the information to the Blockchain for expecting the permission to transmit the data after pertaining the authentication related information. The user A will verify the user B related information after verifying the digital signatures including the personal verification. After verification the authentication is provided to the user B to transmit its relevant data's to the user A by a method called Broadcasting.

IV. Results and Discussion

The proposed method is implemented using the mesh Access points. The wireless mesh network is developed using the different types of non-homogeneous nodes by which each node is developed by different manufacturers, and each might have the ability to work on a same network. The hardware which is used for the testing purpose might consists of surface pro3 win11(Node 1), surface pro3 win11 (Node 2), Samsung galaxy s6 tablet 128gb (node 3), Raspberry Pi 4(Node 4), Samsung S5P4418 Single Board Computer (Node 5) and laptop (intel core i3, 11 th gen, 256SSD) (Node 6). Here Nodes 1,2 and 3 are assess points connected via mesh network and is implemented on the computer. Other nodes are either mobile phones or computers. The experimentation process was carried out with six various intervals. The results obtained after experimentation might provide a greater fall back at the hops side and in between the assess points. This might send a request to the another node(either phone or laptop). The authentication might be provided after the reception of the requests from any of the nodes. The average authentication delay obtained when considering number of Hops are shown in figure 4.

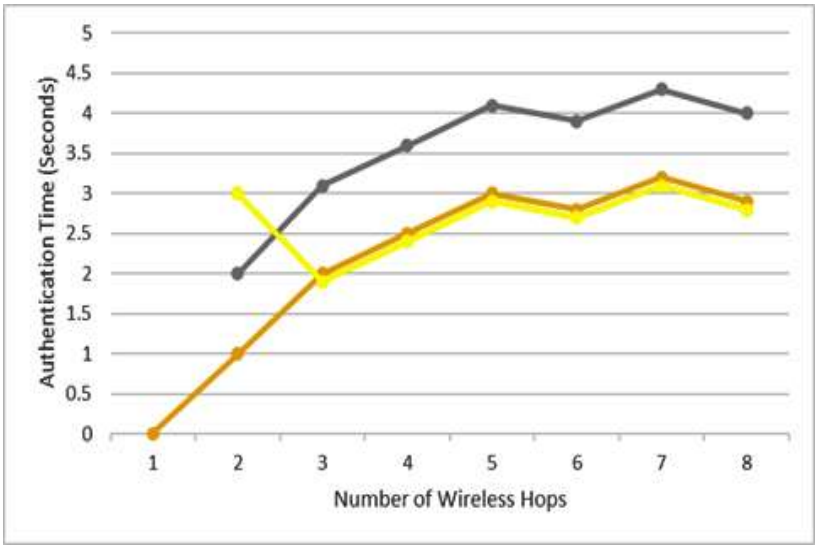

Figure 4: Average authentication delay

If the hop count is more than three then the authentication delay will transfer the packets over the TCP (Transmission Control Protocol) and other to the UDP (User Defined protocol). The TCP will transmit the datas very faster when compared to the UDP, without considering the packet loss. Since the blockchain is used there might be very less authentication delay assumed in the transmission of packets securely with decentralised node in multi hop communication. On the other hand, the simulation is performed with various other available densities of the nodes. It consists of some random nodes of the size 50/100/150/200 and are placed randomly with some areas. Considerably the velocity assumed for the mobility of the node is set to be 50 m per second. The range allocated in between the communication is 150 m. The total simulation happened here is for 30 minutes. The simulation study focuses on some of the routing parameters like the Throughput, End to End Delay, Jitter, Packet Delivery Ratio, Packet Over Head Parameters. The latency is the most important parameter which determines the delay of transmitted packets. The time taken for each packets are used for determining the

shortest path by considering the hop count from one gateway to another using the control packets and is illustrated in figure 5. Here the path length will create impact on the discovery of the routes by considering the latency. This could help in determining the route length and shortest path for secure transmission in wireless mesh networks. The discovery of the route length in association with the latency is formulated along with the density of the nodes within the network. Normally the state of art method depicts that the protocols that are existed in determining the shortest paths are obtained without any such limitations that leads to the transmission of the duplicate packets hence the latency is in the range of 5 to 11 μs.

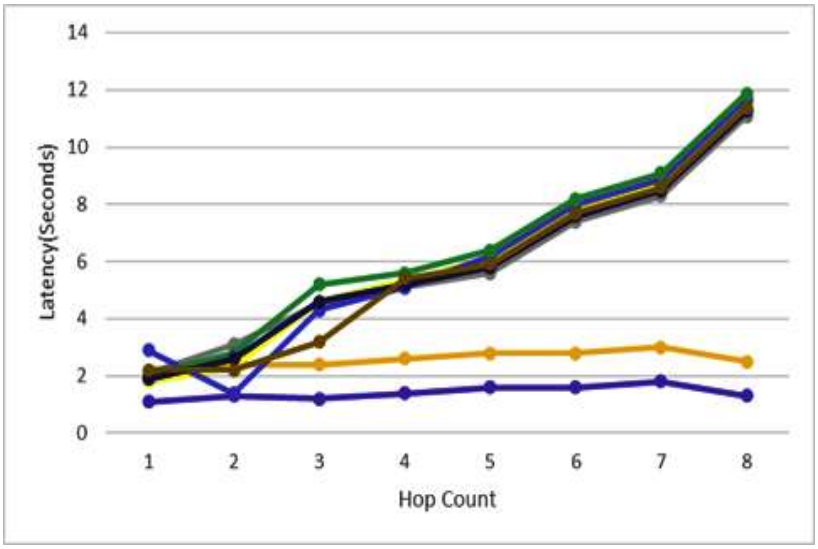

Figure 5: Latency vs Hop Count

The proposed TRSSR method initiates the gathering of the information's from the transmitted packets during the discovery process of the routes. The neighbour which is not in common mode will set a R_{req} to the client and it significantly reduces the latency range from 11 to 5μs.The determination of the values like RTT and TTL will define the maximum available time for travelling across the networks and thus creates the networks resources which inturn considers the time consumption to be very low value. And hence the maintenance of the available nodes along with the routes will reduce the route discovery by maintaining the delay due to the link interruptions. Hence the proposed work will reduce the delay time to about 15 % considering the existing methods. Then the throughput determines the total number of bits transmitted successfully to the provided gateways at a particular period of time.The obtained throughput is shown in figure 6.

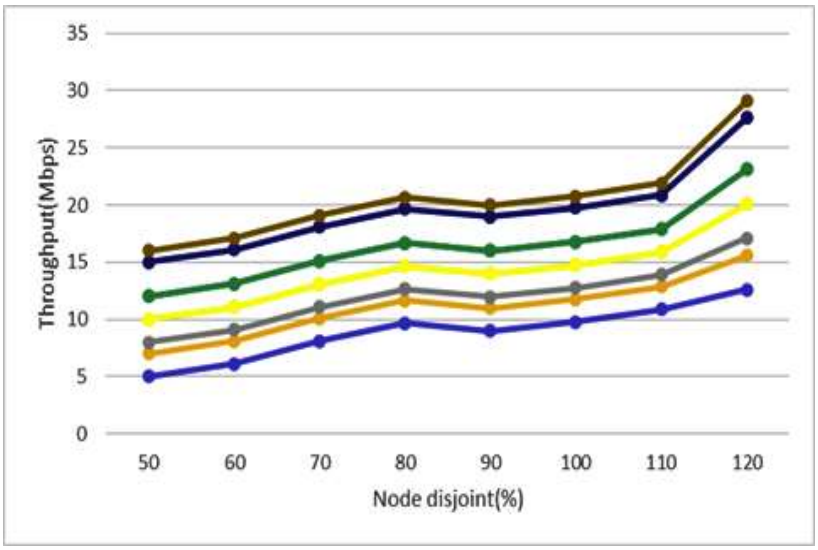

Figure 6: Throughput vs Node disjoint

Utilizing buffering characteristics for network congestion, the suggested work can estimate the spectrum resource and optimise network traffic. It offers flexibility in response to changing bandwidth constraints and effective variation approaches to the entrance. After the removal of the nodes from the neighbouring list the node disjointness is improved by the help of eliminating route packets in order to determine the reception of the duplicate packets. Hence the method proposed might improve the throughput and is allowed to degrade from 30 to 15 Mbps with the increase in the gateway pairs. Normally while supporting the heterogeneous nodes available in the network will retain the restriction of R_{req} by broadcasting the route delivery packets by increasing the throughput performance by approximately 50% more when considered to the existing methods. Then the packet received rate is calculated based on the received packets at the receiver side after the request from the sender. The packet received rate is illustrated in figure 7.

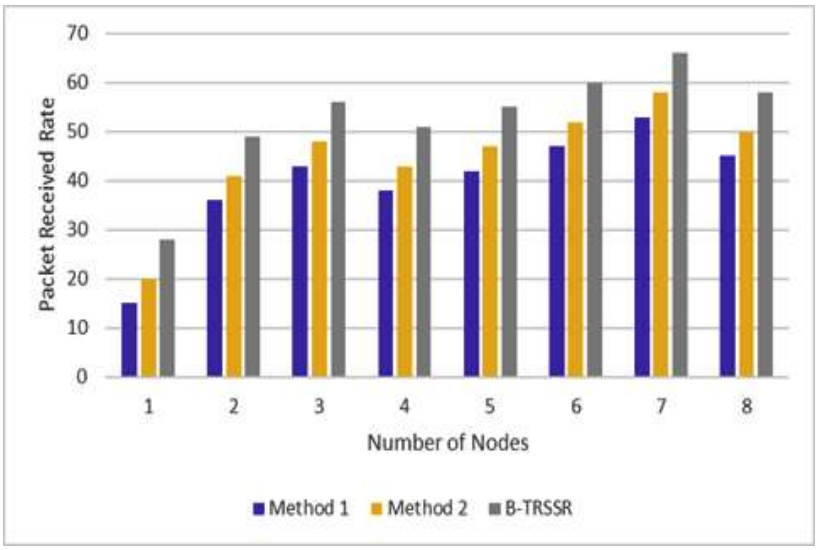

Figure 7: Packet Received Rate

The packet's received rate is determined by considering the ratio of the packets delivered rate to the packets sent rate. Considering the other methods the proposed method

provides high packets rate and thus shows the improvement in the proposed method. Then the transmission overhead is determined by comparing the proposed B-TRSSR with other state of art methods. The transmission overhead results obtained after experimentation is shown in figure 8.

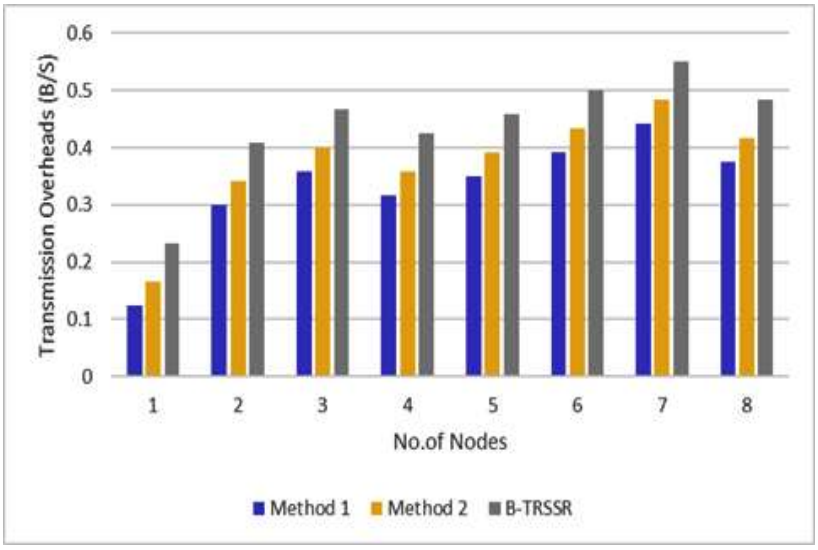

Figure 8: Transmission Overhead

The proposed method processes very less overheads when compared to the existing methods hence the minimum count allows the routing with selected hop counts in the region of selected paths that gets included in the network area. The another parameter called end to end delay is calculated at various determination points by setting up the difference in the packet sent duration and the packets received time . The experimentation results obtained after determination of end to end delay for the available node density is illustrated in figure 9.

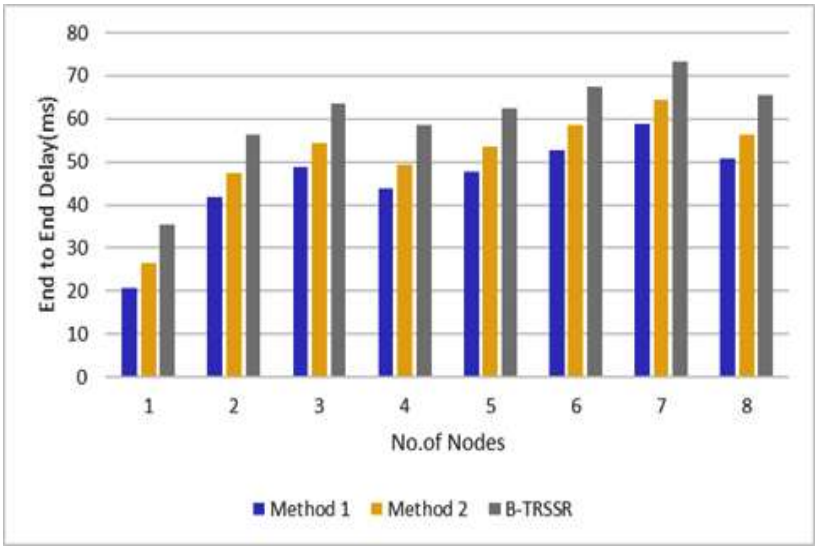

Figure 9: End to End Delay

From the above figure it is very clear that the end to end delay values of the TRSSR is better when compared to the existing methods where the number of nodes considered here is in the range of 100/200/300 respectively.

V. Conclusion

In this work, a blockchain-based Topographical Relay Selection Secure Routing (B-TRSSR) technique for the multi-hop communication is proposed in consideration of the bandwidth, delay, and flow control. Here, an entirely different transmission path is selected by avoiding all risky zones by ensuring the security of transmitted packets. The various security threats like tampering attacks, dropping attacks, flooding attacks, and malevolent attacks are identified and is eliminated by introducing an Adaptive Intrusion Detection System(AIDS). The issues like transmission delay, Bandwidth, and overload traffic are handled by introducing a routing metric called Bandwidth, Transmission delay, and Overload Handler (BTDOH). This was enhanced by modified Q-Learning algorithm which inturn supports the flow control strategies also. The experimentation results proves that the proposed hybrid model will supports the secure transmission of packets in Wireless Mesh Networks(WMN) in an effective manner when compared with other state of art methods.

References

1. Pei, Zhonghui, Xiaojun Wang, Zhen Lei, Hongjiang Zheng, Luyao Du, and Wei Chen. "Joint optimization of multi-hop broadcast protocol and MAC protocol in vehicular Ad Hoc Networks." *Sensors* 21, no. 18 (2021): 6092.
2. Baniata, Hamza, Ahmad Anaqreh, and Attila Kertesz. "DONS: Dynamic Optimized Neighbor Selection for smart blockchain networks." *Future Generation Computer Systems* 130 (2022): 75-90.
3. Kumar, T. Ananth, R. Rajmohan, M. Adithya, and R. Sunder. "A novel security scheme using deep learning based low overhead localised flooding algorithm for wireless sensor networks." *International Journal of Data Science* 6, no. 1 (2021): 19-32.
4. Guo, Hongzhi, Jingyi Li, Jiajia Liu, Na Tian, and Nei Kato. "A survey on space-air-ground-sea integrated network security in 6G." *IEEE Communications Surveys & Tutorials* 24, no. 1 (2021): 53-87.
5. Farej, Ziyad Khalaf, and Azhar W. Talab. "Extended Range Evaluation of a BLE Mesh Network for Control Application." In *2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, pp. 31-35. IEEE, 2021.
6. Jiang, Xin, Mingzhe Liu, Chen Yang, Yanhua Liu, and Ruili Wang. "A blockchain-based authentication protocol for WLAN mesh security access." *Comput. Mater. Continua* 58, no. 1 (2019): 45-59.
7. Zhao, Shasha, and Gan Yu. "Channel allocation optimization algorithm for hybrid wireless mesh networks for information physical fusion system." *Computer Communications* 178 (2021): 212-220.
8. Minh, Quy Nguyen, Ban Nguyen Tien, and Quy Vu Khanh. "An Improved Multi-Channel Multi-Interface Routing Protocol for Wireless Mesh Networks." *International Journal of Interactive Mobile Technologies* 16, no. 11 (2022).
9. Anita, C. S., and R. Sasikumar. "Neighbor Coverage and Bandwidth Aware Multiple Disjoint Path Discovery in Wireless Mesh Networks." *Wireless Personal Communications* (2022): 1-20.

10. Singal, Gaurav, Vijay Laxmi, Manoj Singh Gaur, D. Vijay Rao, Riti Kushwaha, Deepak Garg, and Neeraj Kumar. "QoS–aware Mesh-based Multicast Routing Protocols in Edge Ad Hoc Networks: Concepts and Challenges." *ACM Transactions on Internet Technology (TOIT)* 22, no. 1 (2021): 1-27.
11. Panicker, Jithu G., Mohamed Azman, and Rajiv Kashyap. "A LoRa wireless mesh network for wide-area animal tracking." In *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1-5. IEEE, 2019.
12. Sharma, Teena, Abdellah Chehri, and Paul Fortier. "Review of optical and wireless backhaul networks and emerging trends of next generation 5G and 6G technologies." *Transactions on Emerging Telecommunications Technologies* 32, no. 3 (2021): e4155.
13. Nouri, Nabil Abdelkader, Zibouda Aliouat, Abdenacer Naouri, and Soufiene Ali Hassak. "Accelerated PSO algorithm applied to clients coverage and routers connectivity in wireless mesh networks." *Journal of Ambient Intelligence and Humanized Computing* (2021): 1-15.
14. Zhou, Kunxiao, Huaqiang Yuan, Zusheng Zhang, Xin Ao, and Hui Zhao. "Joint topology control and channel assignment employing partially overlapping channels in multirate wireless mesh backbone." *International Journal of Wireless Information Networks* 25, no. 2 (2018): 209-220.
15. Sun, Yaohua, Mugen Peng, Yangcheng Zhou, Yuzhe Huang, and Shiwen Mao. "Application of machine learning in wireless networks: Key techniques and open issues." *IEEE Communications Surveys & Tutorials* 21, no. 4 (2019): 3072-3108.
16. Joseph, Abin John, Nidhin Sani, K. Suresh Kumar, T. Ananth Kumar, and R. Nishanth. "Towards a Novel and Efficient Public Key Management for Peer-Peer Security in Wireless Ad-Hoc/sensor Networks." In *2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, pp. 1-4. IEEE, 2022.
17. Khan, Ajmal, Adnan Munir, Zeeshan Kaleem, Farman Ullah, Muhammad Bilal, Lewis Nkenyereye, Shahen Shah, Long D. Nguyen, SM Riazul Islam, and Kyung-Sup Kwak. "RDSP: Rapidly deployable wireless ad hoc system for post-disaster management." *Sensors* 20, no. 2 (2020): 548.
18. Ahmed, Farooq, Asif Hussain Khan, Jabar Mehmood, Nadeem Sarwar, Atizaz Ali, Muzamil Mehboob, and Ahmed Waqas. "Wireless Mesh Network." *International Journal of Computer Science and Information Security (IJCSIS)* 14, no. 12 (2016).
19. Kumar, Rohit, U. Venkanna, and Vivek Tiwari. "Opt-ACM: An optimized load balancing based admission control mechanism for software defined hybrid wireless based IoT (SDHW-IoT) network." *Computer Networks* 188 (2021): 107888.
20. Yadav, Ajay Kumar, Santosh Kumar Das, and Sachin Tripathi. "EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network." *Computer Networks* 118 (2017): 15-23.

21. Jiang, Xin, Mingzhe Liu, Chen Yang, Yanhua Liu, and Ruili Wang. "A blockchain-based authentication protocol for WLAN mesh security access." *Comput. Mater. Continua* 58, no. 1 (2019): 45-59.
22. Gupta, Vishal, Hemant Sethi, and Surinder Pal Singh. "A Secure Hybrid and Robust Zone Based Routing Protocol for Mobile Ad Hoc Networks." In *Mobile Radio Communications and 5G Networks*, pp. 405-414. Springer, Singapore, 2022.
23. Yahya, Yahya Ahmed, Sara Raed, Ahmed MH Darghaoth, and Sayf A. Majeed. "Secure Routing Protocol for Wireless Sensor Networks: Survey." In *2022 8th International Engineering Conference on Sustainable Technology and Development (IEC)*, pp. 155-160. IEEE, 2022.
24. Mahapatra, Surya Narayan, Binod Kumar Singh, and Vinay Kumar. "Secure energy aware routing protocol for trust management using enhanced Dempster Shafer evidence model in multi-hop UWAN." *Wireless Networks* (2022): 1-18.
25. Fogli, Mattia, Carlo Giannelli, and Cesare Stefanelli. "Software-Defined Networking in wireless ad hoc scenarios: Objectives and control architectures." *Journal of Network and Computer Applications* (2022): 103387.
26. Cui, Heqi, Peng Sun, and Azzedine Boukerche. "A novel cloud-based traffic aware data routing protocol for smart connected vehicles." *Computing* (2022): 1-20.
27. Aboubakar, Moussa, Mounir Kellil, and Pierre Roux. "A review of IoT network management: Current status and perspectives." *Journal of King Saud University-Computer and Information Sciences* (2021).
28. Shapuan, Nadiah, and Eddie Shahril Ismail. "A Strong Designated Verifier Signature Scheme with Hybrid Cryptographic Hard Problems." *Journal of Applied Security Research* (2021): 1-13.
29. Kumar, K. Suresh, AS Radha Mani, S. Sundaresan, T. Ananth Kumar, and Y. Harold Robinson. "Blockchain-based energy-efficient smart green city in IoT environments." In *Blockchain for Smart Cities*, pp. 81-103. Elsevier, 2021.
30. Liu, Y., K-F. Tong, and K-K. Wong. "Reinforcement learning based routing for energy sensitive wireless mesh IoT networks." *Electronics Letters* 55, no. 17 (2019): 966-968.
31. Ru, Xinxin, Xiaoguang Gao, Yangyang Wang, and Xiaohan Liu. "Learning Bayesian network parameters with soft-hard constraints." *Neural Computing and Applications* (2022): 1-15.
32. Zlobinsky, Natasha, David Johnson, Amit Kumar Mishra, and Albert A. Lysko. "Metaheuristic optimisation for radio interface-constrained channel assignment in a hybrid Wi-Fi–Dynamic Spectrum Access wireless mesh network." In *International Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference*, pp. 56-76. Springer, Cham, 2022.
33. Amer, Amira A., Ihab E. Talkhan, Reem Ahmed, and Tawfik Ismail. "An Optimized Collaborative Scheduling Algorithm for Prioritized Tasks with Shared Resources in Mobile-Edge and Cloud Computing Systems." *Mobile Networks and Applications* (2022): 1-17.

34. Zhang, Guoqiang, Kenta Niwa, and W. Bastiaan Kleijn. "Revisiting the Primal-Dual Method of Multipliers for Optimisation Over Centralised Networks." *IEEE Transactions on Signal and Information Processing over Networks* 8 (2022): 228-243.
35. Dalal, Surjeet, Bijeta Seth, Vivek Jaglan, Meenakshi Malik, Neeraj Dahiya, Uma Rani, Dac-Nhuong Le, and Yu-Chen Hu. "An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks." *Soft Computing* 26, no. 11 (2022): 5377-5388.
36. Filali, Abderrahime, Zoubeir Mlika, Soumaya Cherkaoui, and Abdellatif Kobbane. "Dynamic SDN-based radio access network slicing with deep reinforcement learning for URLLC and eMBB services." *IEEE Transactions on Network Science and Engineering* (2022).
37. Tegou, Thomas I., Antonios Tsiflikiotis, Dimitrios D. Vergados, Katherine Siakavara, Spiros Nikolaidis, Sotirios K. Goudos, Panagiotis Sarigiannidis, and Mohammad Obaidat. "Spectrum allocation in cognitive radio networks using chaotic biogeography-based optimisation." *IET Networks* 7, no. 5 (2018): 328-335.
38. Aloqaily, Moayad, Haythem Bany Salameh, Ismaeel Al Ridhawi, Khalaf Batieha, and Jalel Ben Othman. "A multi-stage resource-constrained spectrum access mechanism for cognitive radio IoT networks: Time-spectrum block utilization." *Future Generation Computer Systems* 110 (2020): 254-266.
39. Liu, Wei, Chang Xu, Zhao Tian, Dong-Kun Li, Guan-Zhong Lu, and Wei She. "Research on gateway deployment for throughput optimization in wireless mesh networks." In *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1-5. IEEE, 2019.