International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/224436 Volume 11, Issue 1, January – February (2024)

RESEARCH ARTICLE

TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol

Jayantkumar A Rathod
Department of Computer Science and Engineering, Alva's Institute of Engineering (Affiliated to Visvesvaraya Technological University, Belagavi), Moodubidire, India.
jayant1977rathod@gmail.com

Manjunath Kotari
Department of Computer Science and Engineering, Alva's Institute of Engineering (Affiliated to Visvesvaraya Technological University, Belagavi), Moodubidire, India.
mkotari@gmail.com

Received: 21 November 2023 / Revised: 01 February 2024 / Accepted: 07 February 2024 / Published: 26 February 2024

Abstract – Several practical applications are combined in a new paradigm known as 5G-based mobile ad hoc networks (MANET) with cloud. Numerous existing works perform trust assessment, intrusion detection, and route discovery to improve secure data transmission in MANET. Route maintenance was not carried out in several of the existing works, and the absence of enumerating link status and node reliability during route maintenance results in link failure and increases packet loss. By considering the existing issues, a novel Kangaroo-based intrusion detection system was proposed to eliminate malicious nodes from the network using Bidirectional- Long Short-Term Memory (Bi-LSTM). This increases data transmission security. For graphical user authentication, encryption based on ASCII values of the Reflection tree (E-ART algorithm) is employed. In this paper, a divide well merge algorithm was implemented, which is a better approach for hierarchical clustering. This method consists of two phases: a Division and Merging phase. The effective route identification and route maintenance in MANET are implemented by using an Advanced Ad-hoc On-demand Distance Vector Protocol (Advanced AODV), which discovers the route using the Fire Hawk Optimization Algorithm (FHO) to obtain optimal multipath by contemplating trust, node connectivity, throughput, node degree, bandwidth, energy and distance where this protocol offers loop-free operation and enhance its scalability to numerous numbers of terminals. In this way, route discovery and route maintenance are established to enhance secure data transmission, thereby reducing packet loss. The modified blockchain called TriChain is proposed for enhancing data transmission security. For the Proof of Work based on Reputation (PoWR) consensus algorithm is used to reduce transaction confirmation latency and block creation time thereby increasing security. In this way, route discovery and route maintenance are established to enhance secure data transmission thereby reducing packet loss. The proposed work is evaluated using detection rate, energy consumption, packet delivery rate, throughput, authentication rate and delay.

Index Terms – 5G MANET, Kangaroo Intrusion System, Bi-LSTM, Encrypts Based on ASCII Values of Reflection Tree, Advanced AODV, Fire Hawk Optimization Algorithm.

1. INTRODUCTION

The distributed wireless connection is acknowledged as a Mobile Ad Hoc Network (MANET), which is without any infrastructure and auto-configured devices (mobile phones, laptops) that are connected wirelessly. The MANET benefits with effortless communication of mobile nodes due to their communication range. A radio transmitter and the recipient are installed in each node of a MANET, enabling wireless communication between the nodes and the system [1-3] The following are the primary explanations for why MANETs may send data with comparable properties while yet using an active strategy: It is unexpected that the transmission scope of this transmission is more limited than that of the previous transmission, which prevents any number of nodes from exchanging data across the system [4-6]. The fact that portable nodes in Wi-Fi Ad-Hoc networks rely on battery packs, which are typically underpowered in most environments and take an extended period to recharge or replace, is a major problem. Route discovery and data transfer are the two phases of MANET communication, both of which are subject to different types of attacks. Adversaries can obstruct route finding during the initial phase by feigning to be destination, responding with outdated routing information, or disseminating false control traffic. Interfering with the correct route or interrupting data flow could lead to significant data loss, posing a threat to both communication phases. To ensure comprehensive security in MANETs [7-9], protective measures are essential.

Further research is necessary to enhance the efficiency of MANETs, utilizing their substantial battery life resources, which have experienced a slowdown in progress in recent years without notable breakthroughs in this domain. The proven reliance on packet delivery while a cell node's wireless port is off during times of inactivity or rest has raised concerns over energy waste. Because the technology used in cellular ad hoc systems is portable and has capacity, weight, size, and bandwidth limitations, it needs mobility [10].

The nodes can communicate with each other through forwarding packets; routing in this network is performed to transmit the data packets from source to destination, which is a very challenging process due to its high mobility, external noise, consumption of battery energy, and transmission interference. Furthermore, mobile nodes in the network are vulnerable due to their crucial features, namely open medium, dynamic topology, distributed cooperation, and resource constraints. Hence, safety and consistency should be re-enumerated, and employing secure, effective routing is necessary. Besides, the authentication was implemented initially to only permit legitimate users to access the network by registering and authorizing. Further, the nodes are clustered to enhance the communication reliability and routing throughput then the effective cluster head (CH) was selected based on high trust value. Due to the abovementioned constraints, the former works perform trust management systems and intrusion detection to enhance routing performance. The trust of all nodes is evaluated individually to identify the selfish node and auto-destructive nodes generated by erroneous nodes [11-14]. This research uses kangaroo-based intrusion detection (KIDS) to secure the data transmission by blocking malicious nodes using Bi-LSTM. Next, Detect the Efficient route using Advanced AODV based on the FHO process. Next, Perform the message hashing process using the E-ART algorithm and perform the packet transmission.

1.1. Motivation and objectives

This research aims to provide secure data transmission in MANET by executing effective route discovery and route maintenance in MANET. We are motivated by a number of the concerns brought up in the earlier research, some of which are mentioned below.

- High-Security Breaches: In the majority of current efforts, all users are regarded as valid users and allowed access to the network before the confidence of all nodes is assessed, where illegitimate users can effortlessly modify the trust value and tamper the data, increasing high-security breaches due to insecure storage of enumerated trust value. Furthermore, the data was transmitted without considering any security measures that allow the malicious nodes to access the data easily, leading to security breaches.
- Enormous Packet Loss: In several existing works, the route maintenance was not accomplished, and the lack of enumerating link status and node reliability while route maintenance leads to link failure and increased packet loss. Furthermore, some of the existing works lack clustering of the nodes and ineffective clustering without considering regional density, stability, etc.., reducing the communication reliability and affecting the routing throughput, leading to high packet loss.
- Lack of QoS: In exceeding previous works, the indirect trust is acquired randomly with a one-hop neighbor node, affecting the certainty of trust evaluation and limiting satisfying QoS. Moreover, after performing trust evaluation and intrusion detection, the cluster members don't share their energy level, position update, and further necessary details to their CH, increasing the insecure paths and reducing QoS.

The major goal of this study is to implement efficient discovery of routes and maintenance processes in MANET to ensure safe data transfer in MANET. The other objectives are defined below,

- The effective trust evaluation is performed by considering significant parameters to enhance the routing performance by identifying selfish nodes.
- To improve network security, novel intrusion detection is accomplished to detect and block malicious users.
- To perform effective route discovery, the position update and other necessary details are shared with CH by cluster members (CM).
- The enhanced routing protocol is implemented, and insecure paths are identified using necessary details of CM shared with CH that improve secure and energy-efficient route discovery.
- To reduce packet loss, route maintenance is employed by evaluating link status and node reliability that reduce link failure and packet drop rates.

1.2. Research Contributions

The main objective of this study is to increase the effectiveness of the safe transmission of data in MANET, where the advanced reactive routing protocol is implemented, by carrying out efficient route discovery and maintenance. The major contributions of this approach are mentioned below.

- To increase network security, the E-ART algorithm provides graphical user authentication, which offers a security key to only allow legitimate users access to the network.
- To improve routing performance, the trust of all nodes is evaluated to identify the selfish nodes. KIDS is executed to eliminate the malicious nodes from the network using Bi-LSTM, which increases data transmission security.
- For efficacious route discovery, an Advanced AODV routing protocol is established, and CH maintains the necessary details (position update, energy) of CM to discover the optimal route using FHO.
- For reducing packet loss, effective route maintenance is executed by determining the link status and node reliability that reduce link failure and packet dropping rate by redirecting or alternate route discovery.

1.3. Paper Organizations

The remainder of the essay is structured as follows: Current study gaps are analyzed and addressed in Section 2's survey of the published publications. The proposed work is fully explained in Section 3, along with the appropriate pseudocode and illustrations. The experimental setup is provided in Section 4, together with thorough explanations of the modelling setup, comparison study, and research summary. Section 5 provides a thorough discussion of the planned work's conclusion.

2. LITERATURE SURVEY

In addition, this section provides the research gaps of such previous works, which are summarized below; authors in [15] proposed a secure hybrid multipath routing scheme to improve secure packet transmission in MANET. Initially, the trust management system was employed to evaluate the trust of all nodes by analyzing the direct trust (DT), indirect trust (IDT), and recent trust (RT). Then, the nodes are clustered using a density peak-based FCM algorithm, and CH is selected when the node is in an important location with the greatest value. Finally, a hybrid genetic algorithm with a genetic hill climbing algorithm (GAHC) is utilized to select the effective path from multipath based on enumerating the fitness function through contemplating energy, latency, connection, and throughput. Once the routes are discovered using the GAHC hybrid algorithm, which performs optimal path selection, however, the routes were not maintained, which leads to link failure and packet dropping. Here, the node's trust was estimated by evaluating DT, IDT, and RT where trust of data bytes and data packet delivery was not considered, which results in ineffective trust evaluation. The author proposed a secure routing protocol by detecting intrusion in a MANET environment [16]. Initially, the intruders are identified by implementing the Secure-IDS framework which embraces two phases such as attack detection and prevention. The packet analyzer examines the packets by considering the number of packets per flow, packet arrival time, packet size, and count. Further, if the packet valves exceed certain threshold valves, then the attacks are classified, and the alarm is generated. Then, the secure energy routing protocol was employed, RREQ was initiated from source to destination, and RREP was sent by destination node. Furthermore, the RREQ is eliminated when the request has a lower connection cost. Finally, the shortest path was selected, and confirmation notification was sent to the destination through Path Confirm (RCON). Here, intrusion detection was performed to improve the secure data transmission in the network. However, the node's trust values were not evaluated, which increased high packet loss due to the packet dropping of the selfish node. Once the intruders were detected, the secure routing was directly performed using secure energy routing protocol where routing lack of clustering affects the communication reliability and leads to ineffective routing.

Authors in [17] proposed a method for optimal route discovery and route maintenance to enhance data transmission in MANET. Initially, the work consists of four phases incorporating trust evaluation, optimal route discovery, optimal route selection, and route maintenance. The Adaptive Neuro-Fuzzy Inference System (ANFIS) was utilized for trust evaluation by examining whether the node is selfish or malicious. Then, the trust-aware routing protocol was employed for optimal route discovery into two parts: routing among regions and routing within regions. The optimal path selection was performed using an adaptive equilibrium optimiser to select an optimal path from the obtained multiple paths. Finally, route maintenance was established to identify the damaged link, and an alternative route was discovered based on an optimization technique. The ANFIS was employed for malicious node detection through trust evaluation. Still, all the users are considered legitimate users, which increases high complexity due to numerous packet transmissions by illegitimate users. Here, the ANFIS was utilized for trust evaluation, which performs effectively; however, this algorithm lacks the selection of significant membership function that affects the trust evaluation accuracy. In this work, the route discovery was generated by a trust-aware routing protocol, which enhances the route performance. Anyhow, the data was transmitted without providing any security, which increased security breaches in the network. The intrusion detection method for intensifying optimal secure routing path in MANET was done in [18]. Initially, the trust was enumerated based on six factors comprises of DT, IDT, error, data packet delivery, RT, and data bytes trust (DB). Then, the clustering is performed by fuzzy clustering trust, and the node with the highest trust value was selected as CH. Furthermore, the intruders were classified using a fuzzy naive Bayes algorithm, was determined through communication among sink nodes and CHs, and the intruder node was blocked. The routing protocol employed for generating the optimal multi-path in low-power and lossy networks was RPL. Subsequently, the optimal path selection, considering energy, throughput, and node connectivity, was accomplished using the bird swarm-whale optimization algorithm. To assess the trust values of nodes, a fuzzy clustering algorithm was utilized for node clustering. While this algorithm proves to be cluster effective, it suffers from increased latency due to the time-consuming process of determining each data point's cluster membership.

For intrusion detection, the fuzzy naive Bayes algorithm was applied to achieve optimal reduction. However, it is noteworthy that this algorithm does not give due consideration to the probability output, impacting the accuracy of intrusion detection. Despite the effective use of the routing protocol for low-power and lossy networks in generating routes, there were challenges in maintaining the route consistently during data transmission, leading to an elevated packet loss rate.

A secure routing protocol by employing novel intrusion detection in the MANET environment was proposed in [19]. Initially, intrusion detection was implemented to improve the routing performance by integrating the anomaly detection approach for energy and secure-aware routing. The intruders are identified and blocked from the network based on the dynamic threshold valves. Then, the hybrid routing method was performed using a driven zone-based routing protocol (DD-ZRP), which mainly considers the resource constraint. Finally, the optimal route was discovered, which enhances security, energy, and available resources. In this work, intrusion detection was performed based on the dynamic threshold valves where lack of trust evaluation leads to an increase in high packet dropping rate due to the presence of selfish nodes.

The author in [20] proposed a key management mechanism for secure and energy-efficient routing protocol in MANET. Initially, the trust of all nodes is estimated based on the mobility, calculation of location key, energy, and packet delivery success rate. Then, the pair of specialized nodes are selected for performing asymmetric key cryptography and named calculator key (CK) and distribution key (DK). These nodes oversee secret key production, distribution, and verification, and a pair of nodes is chosen according to energy and trust values.

The identification of malicious nodes involved initiating communication between source and destination nodes. Subsequently, the AODV routing protocol was employed for optimal routing. The trust estimation of all nodes was determined by considering factors such as mobility, calculation of location key, energy levels, and packet delivery success rate, enhancing the performance of trust evaluation. However, despite the improved trust evaluation, the detection of malicious nodes through the initial communication between source and destination nodes led to an increase in security breaches.

A novel attack detection mechanism using routing protocol in MANET was done in [21]. The route discovery was initially accomplished using an AODV routing protocol. Next, support vector machine (SVM) and artificial neural network (ANN) algorithms were incorporated with the routing protocol. The compound of ANN and SVM is utilized to identify the malicious nodes from the discovered route using AODV. For data training of ANN, the ABC performs the fitness function continued by SVM, considering energy, received data packets, coordinates, and required time. Then, the optimal route advised by ABC passes to SVM with node properties. Finally, the ANN classifies the nodes in the path are malicious or normal. The training data was optimally suggested using the ABC algorithm, which increases detection accuracy; anyhow, the ANN algorithm consumes high computational power and requires a large amount of data to train the model effectively, which leads to high complexity.

An effective routing mechanism model for resource-aware routing protocol in MANET was proposed in [22]. Initially, it combines resource-aware cooperation modelling and the Markov process (ReCoMM) for quantifying the link status for designing an effective route. The Markov process helps the ReCoMM model to examine the mobility, energy, changes in node state, and cooperation of the nodes. Based on the investigation, the Markov process adjusts the connection stability and node durability and determines the limits of cooperation value. Finally, the Markov process designs the effective resource-aware data-transmission routing protocol. Here, the Markov process examines the nodes through mobility, energy, and cooperation of nodes, which helps to improve routing performance, but the malicious nodes are not detected where the malicious users modify the data easily and lead to insecure data transmission.

A clever method of installing a system to detect and prevent intrusions (SA-IDS) in the MANET environment was presented in [23]. Initially, the One-way hash function was employed for user registration through the Trust Authority (TA). The users submit their credentials, including finger vein, biometric, and user ID, to authenticate from TA. The SA-IDS embraces four phases: packet analyzer, pre-processing, feature extraction, and classification. The Type 2 fuzzy controller was used as a packet analyzer to examine the attack pattern. Then the data are pre-processed by performing logarithmic normalization and encoding mechanism. Finally, the features are extracted, and tree construction is performed using a bootstrapped optimization algorithm with ANN for attack classification. The users are registered and authenticated using a One-way hash function through TA by providing their credentials, which are effective anyhow; this algorithm incapacitates their security level in repeated use.

The author proposed in [22] a robust trust management system for node trust evaluation in MANET. The Dirichlet trust and reputation management system is initially used to count nodes' trust and reputation without interfering with network security. The distribution of Dirichlet probability was accomplished for evaluating the reputation and trust of individual nodes based on their network performance. Furthermore, the other nodes acquired a second-hand reputation for trust enhancement. Then the candour two-dimensional trustworthiness determination approach identifies the node's behavior based on calculated reputation total and trust values. Finally, this approach encourages the nodes to contribute continuously to the network. The malicious nodes are identified based on the estimated reputation and trust values where the illegitimate users can easily compromise the trust values that affect the network security level. Blockchain-based trust management scheme for enhancing routing protocol in MANET was done in [24].

Initially, the trust management scheme performs trust estimation of the routing protocol through blockchain for enhancing tamper-proof [25]. The securely distributed and trusted blockchain framework is utilized for security improvement, where individual nodes perform the security operation repetitively. Then, the optimized link state routing protocol (OLSR) was implemented for effective routing. Here, to improve routing security, the blockchain-based optimized OSLR was accomplished for effectual routing; however, lack of clustering affects the communication reliability and reduces routing throughput, thereby limiting QoS.

In [26], an innovative algorithm was introduced by the author to bolster the security of MANETs through intrusion detection and reputation estimation. The initial step involved a pre-processing stage where a distinctive value was assigned to each node, utilizing the K-nearest neighbor (KNN) technique for efficient grouping and reduced delay. Subsequently, the trust level of each node was ascertained using both the beta distribution and Josang's mental arithmetic.The fuzzy inference system, taking into account the evaluated trust, reputation, and remaining energy, was then employed to designate the CH. Furthermore, the trusted server undertook an examination of the destination node as part of the security measures.

The study presented in [27-29] introduces a secure and energy-efficient navigation approach in MANETs, relying on the Bacteria for Ageing Optimisation method (BFOA) to identify optimal hops for routing advancement. The selection of CHs is determined by considering the current, DT, and IDT levels associated with each CH. To initiate this process, the fuzzy clustering technique is initially employed. Additionally, nodes with assigned trust values are identified based on their trust levels. Multiple sink pathways will be calculated using ECSO. The method uses distance and traffic rate as parameters to find the best pathways using ECSO. A single optimal route is selected based on node energy utilizing BO (Butterfly Optimisation), reducing network energy needs. The sink will receive encrypted data over the chosen route. This study introduces an Energy-Aware Trust algorithm (EATMR) using the AODV protocol and Multi-path Routing method to enhance WSN security. The EATMR process has two phases: node clustering using the Open-Source Development Model Algorithm (ODMA) and clustering-based routing. This research considers energy-aware trust during AODV protocol and multi-path routing. Optimal and safe routes are found using energy, trust, hop-count, and distance characteristics. Using an intrusion detection system is an efficient way to identify internal and external attack vectors. Despite several IDSs for Wireless Mesh Networks (WMNs), they only detect intrusions in certain layers. To protect against multilayer security assaults, WMNs need cross-layer IDS to identify and react to them [30].

The study [31] proposes four processing strategies to maintain security against routing protocols. In MANET, rushed attackers significantly damage packet-based data transfer, particularly node communication. This study uses an automated Bees Colony Optimisation (ADABCP) approach to identify attackers throughout the routing process, achieving the intended outcome. The HRLD routing protocol handles MANET routing and addresses communication congestion. Route Finding Manipulation (RFM) generates the Swift Implicit Response Round Trip Time (SIRT) method to improve performance.

Using machine learning techniques, the research paper [32] suggests a unique methodology for trust-based CH selection in WSNs. By making sensor node trustworthiness a crucial component in CH selection, the paper seeks to improve WSNs' efficiency, security, and dependability. Fuzzy logic and machine learning techniques are combined in the proposed ML-FBRP for WSNs. According to the study in [33], to increase the lifetime and energy consumption of the network, the suggested system makes use of a quasi-optional-based Jaya load balancing technique with CH selection protocol. The QOJ-LCH technique lengthens the lifespan of relay nodes by distributing the load evenly among them throughout the network. Additionally, it lessens the issues with load balancing in wireless sensor networks. It makes use of both single-hop and multiple-hop routing techniques. Proposed QOJ-LCH with CH selection approach improves overall power consumption and network lifetime.

A unique routing system is proposed in this paper [34] to select stable nodes and the best routes for efficient data transfer in high-speed MANETs. The Golden Eagle

Optimization (GEO) method is used in the proposed

the optimal path based on the revised goal function. Fractional calculus also makes it easier to explore the best possible routing path. When compared to other routing protocols, this one performs better on networks with different numbers of nodes and node mobility. In order to address the problem with the MANET, research study [35] introduces a robust IDS with hybrid ML techniques. The suggested method for detecting assaults makes use of the Rat Swarm Optimization Algorithm (ANFIS-RSOA) and the Adaptive Neuro Fuzzy Inference System. The author of this paper does not address a multipath routing protocol-based routing technique.

Optimized ESDQTMR (OESDQTMR) protocol to determine

The authors of this work [36] give a thorough summary of the issue of identifying vehicles that are misbehaving on VANETs. This is a serious issue since egotistical and malevolent nodes have the potential to seriously harm the network. The categorization of attack types is taken into consideration in this section, which also explains the most popular attacks in VANETs and the several ways the authors have suggested to stop and identify them. Table 1 lists the existing work's references. However, current research has managed to address several of the most significant issues, including:

Table 1 Research Gap in Literature Survey

References	Objectives	Methods or Algorithms Used	Limitations
[15]	Secure hybrid multipath routing scheme to improve secure packet transmission in MANET	A hybrid of genetic algorithm with GAHC	Data bytes and data packet delivery were not considered, which resulted in ineffective trust evaluation
[16]	Secure routing protocol by performing intrusion detection in the MANET environment	Secure Energy Routing (SER)	High packet loss
[17]	Optimal route discovery and route maintenance to enhance data transmission in MANET	ANFIS	Increases in security breaches
[18]	Intrusion detection method for intensifying optimal secure routing path in MANET	Fuzzy naive bayes algorithm	The increased high packet loss rate
[19]	Secure routing protocol by employing novel intrusion detection in the MANET environment	DD-ZRP	Increase in high packet dropping rate due to the presence of selfish nodes
[20]	The secure and energy-efficient routing protocol in MANET	AODV routing protocol	Breaches of security
[21]	Attack detection mechanism using routing protocol in MANET	Artificial bee colony (ABC), ANN, and SVM algorithms	High computational power
[22]	Effective routing mechanism model for resource-aware routing protocol in MANET	ReCoMM	Insecure data transmission.
[23]	The SA-IDS in the MANET environment	Bootstrapped optimization algorithm and ANN	Low-security level
[24]	Robust trust management system for node trust evaluation in MANET	Candour two-dimensional trustworthiness determination approach	Affect the network security level
[25]	Blockchain-based trust management scheme for enhancing routing protocol in MANET	OLSR	Reduce the routing throughput, thereby limiting QoS

[26]	Intrusion detection and reputation estimation for enhancing security in MANET	KNN	Ineffective routing
[27]	Intrusion monitoring is essential for preventing and securing against unauthorised access	Fuzzy clustering algorithm, secure optimization routing	Computational overhead
[28]	A multipath routing and secret key technique for healthcare applications to maintain privacy	Enhanced Cuckoo Search Optimization, Butterfly Optimization	To not handle larger-scale optimization
[29]	Optimizing WSN performance by clustering-based routing	OSDM Algorithm, AODV protocol, Multi-path Routing approach (EATMR)	Can't different traffic patterns
[30]	Detecting internal and external threat vectors effectively requires an intrusion detection system.	Wireless Mesh Networks	Security of such networks requires identifying and fixing these vulnerabilities.
[31]	Node communication is significantly affected by rushing attackers in MANET.	Hybrid Random Late Detection, automation of the Bees Colony Optimization	Can't find what types of attacks.
[35]	Addressing the challenge present in the MANET	Robust IDS using hybrid ML methods	Does not focus on multipath routing.
[36]	An in-depth analysis of the issue of identifying misbehaving vehicles in VANETs and several attack types.	SVM, RFO algorithm, and Deep Belief Network (DBN). A Credit-Based Approach, DISOT (Distributed Selfish Node Detection in Internet of Things), etc.	In VANETs, no single technique can identify every rogue node. Cutting-edge innovations like neural network algorithms and blockchain,

3. PROPOSED METHOD

This research mainly concentrates on secure data transmission in the MANET environment by performing intrusion detection. In addition to that, effective route discovery and route maintenance are fabricated to enhance network security. Cloud computing reduces storage computation, and 5G technology is utilized for better communication reliability.

Figure 1 represents the architecture of the proposed cloud-assisted in 5G MANET. Furthermore, the modified blockchain is proposed for enhancing data transmission security. The modified blockchain is named TriChain, where the blockchain's structure and the block generation process are modified. Reducing confirmation of transaction latency and block formation time with the Evidence of Work determined by the Reputation (PoWR) consensus method increases security.

The PoWR algorithm drastically reduces transaction confirmation latency, enabling speedier validation and inclusion of transactions into blocks.

The PoWR consensus algorithm optimizes block creation time, guaranteeing that new blocks are generated efficiently and quickly, and boosting overall system performance. Incorporating reputation-based techniques into the Proof of Work algorithm improves network security by considering members' past conduct and trustworthiness during the consensus process.

The network balances transaction speed and security by utilizing PoWR, resulting in a more resilient and dependable system for participants. PoWR's reduced transaction confirmation latency and improved block formation time contribute to a more efficient and secure ecosystem, benefiting users and increasing network adoption. The proposed work consists of four consecutive processes such as,

- Graphical User Authentication
- Hierarchical Clustering
- Trust Enumeration and KIDS
- Effective Route Discovery and Route Maintenance

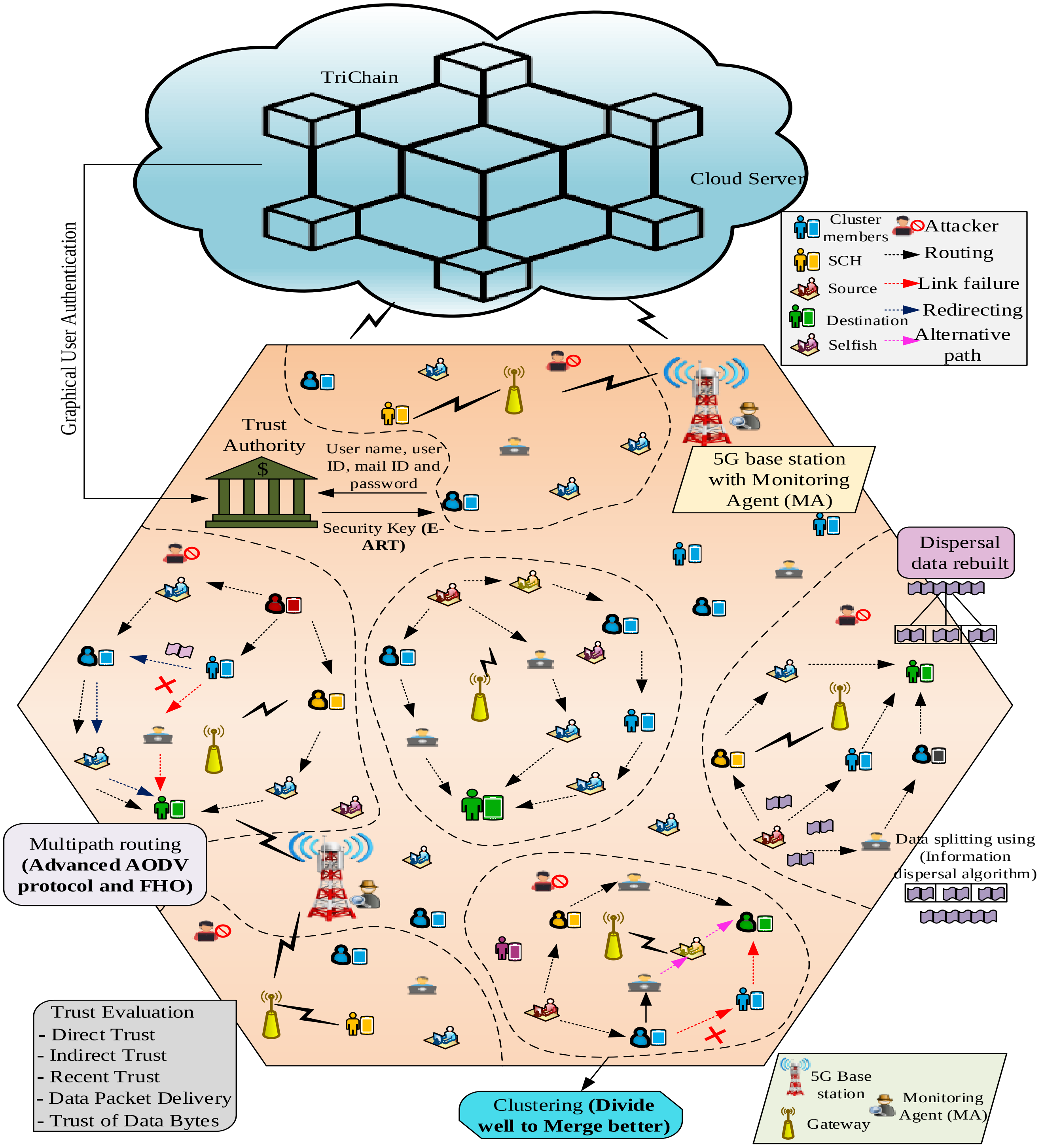

Figure 1 The Architecture of Proposed Cloud Assisted in 5G MANET

3.1. Graphical User Authentication

Initially, the users in the MANET environment are registered by providing their credentials, such as user name, user ID, and mail ID, and then entering their password. The TA generates a random secret code based on the password. It encrypts using the E-ART algorithm, which minimizes the overhead and achieves high security through dynamic offset. Figure 2 illustrates how the binary tree handles ASCII-based English language input. The ASCII character values at the tree's nodes range from 0 to 127. The 128-bit symmetric key used by the E-ART technique has both a static as well as a dynamic component. The static portion varies with each session, whereas the dynamic portion varies with each character. Using a dynamic key provides defense against traditional and contemporary cryptanalysis methods.

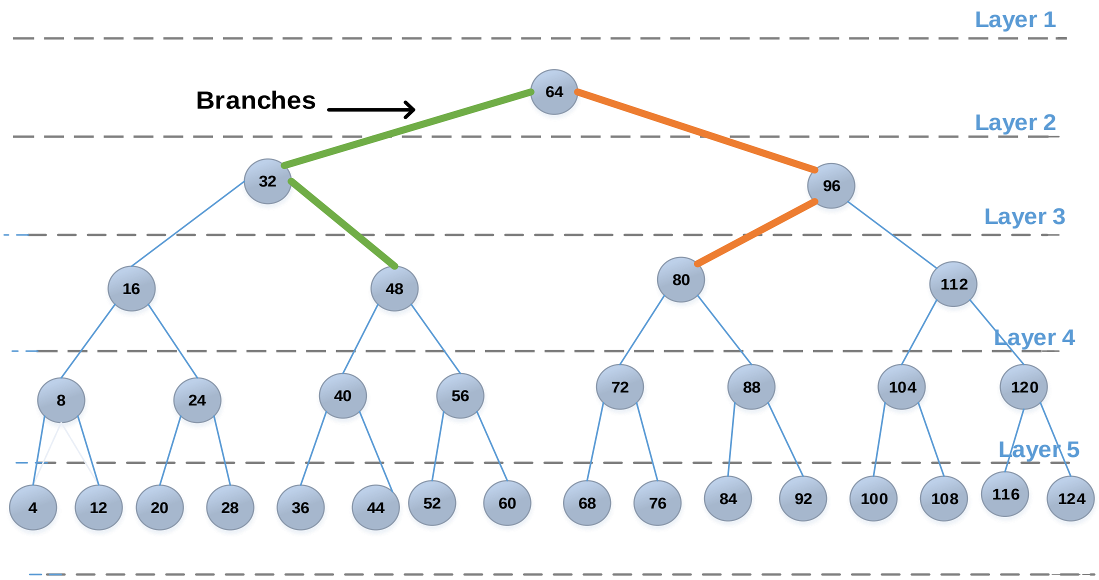

Figure 2 A Binary Tree of the E-ART (Reflection Tree Encryption Method Using ASCII Values)

3.2. A key Derivation

The initial key builds two offsets for data encryption during key derivation. While the changing offset varies each each letter value during encryption and decryption, the variable offset remains constant. The dynamic offset assures key randomization and encryption security. Main derivation: Every session or system setting allows for the renewal of this unique secret key among legal entities. This work does not focus on legal organization key management. To create offsets, an initial key uses N and Variance. 64 or 128-bit integer N. This number will calculate the variable offset. Variance calculates the pseudo-random number value in the dynamic offset. Variable offset is calculated analytically using the tree attributes presented. Figure 2 depicts the left and right nodes. It calculates N_L and its reflection node N_R using the N value derived from the initial key and generates the value of $offset_{var}$. Equations (1) and (2) state that to increase the complexity and thwart, a one-to-one mapping-based cryptanalysis is required. This number will be added to the original reflection value. The formula is as follows.:

N_L =mod Len_{max}

N_R= (Len_{max}-N_L)+1

$$offset_{variance} = \begin{cases} R \times N_L \text{mod } N_R if\ N_L < Root \\ R \times N_R \text{mod } N_L\ if\ N_L > Root \end{cases} \quad (1)$$

Dynamic offset: It is created by summing a pseudo-random integer and the second component of the original key, variance. A pseudo-random number of 64 or 128 bits is produced by the pseudo-random number generator. Utilizing each character's placement as a seed within the text. The pseudo-random number is then modified using the Variance value. To create the final encrypted characters, this offset is inserted in the last step and is changed for every character. The system is therefore incredibly strong and resistant to known powerful attacks. The following formula is used to compute the dynamic offset:

$$Dynamic\ offset = (pseudo)\ mod\ va \quad (2)$$

3.3. E-ART Architecture

The main novel aspect of the E-ART technique is how it leverages a symmetrical binary tree structure's reflecting property to improve data search efficiency. An explanation of binary trees is provided below. The root node is given the value Y. All values smaller than Y are found in the left subtree of the main tree, while all values bigger than Y are found in the right subtree. The binary tree's search complexity when seeking for a particular value is O(log(n)). An illustration of an E-ART-based binary tree is shown in Figure 2.

Consider an equation that contains the character "P," which has the ASCII code 80. This character is located on level 3 of the binary tree, on the root node's 1R1L right and left branches. Its mirrored character is 1L1R, which is 48. Because 48 is the ASCII code for the character "0," the initial reflected value of the character "P" is 0. As a result, a reflection tree can encrypt every character in plaintext. As a result, a more efficient search technique is achieved. The initial reflected value $Value_{initial\ reflected}$ of a balanced binary tree, as shown in Figure 2 can be derived from the original value $value_{org}$ as shown in equation (3).

$$Value_{initial\ reflected} = (Len_{max} - value_{org}) + 1 \qquad (3)$$

The initial reflected value, however, still has some issues. The ASCII table's special characters, which range in size from 0 to 32 and include spaces, carriage returns, and other text formatting characters, are not discussed. Due to the one-to-one mapping of characters, it is susceptible to cryptanalysis assaults such as frequency analysis attacks.

We suggest various offsets be added to the initial reflected value to address these problems. First, a constant offset value of 32 is included in the first reflected value to avoid non-printable ASCII characters appearing. Consider the character "," for instance. Its ASCII code is 104, and Equation (1)'s first reflected value is (127 104) + 1 = 24, which denotes a non-printable character. After applying the constant offset, the newly determined reflected value is 24 + 32 = 56. Second, we suggest an additional offset called the variable $offset_{var}$ to prevent cryptanalysis attacks and increase complexity. Based on the values of the root node R, left node N$_L$, and right node N$_R$ of the E-ART tree, as stated in Equation (1), it is calculated. The reflected value's basic equation is as shown in equation (4)

$$Value_{ref} = \begin{cases} (Y\%\ Len_{max}) + offset_{con}, Y > Len_{max} \\ Y \qquad\qquad\qquad\qquad \geq Len_{max} \end{cases} \qquad (4)$$

Where Y=$Value_{initial\ reflected}$ $+ offset_{var}$ and $offset_{con}$.

The value Y is regarded as the reflected value if it is smaller than the Len_{max} character limit. To prevent the appearance of characters that are not printable, the constant offset is added to the computed value if the reflected value is bigger than $Length_{max}$. Then the encrypted secret code is split into two portions, and TA randomly selects the pair of images from its internal storage. Further, the first portion of the divided secret code is encoded in the first image; the second partition is encoded in the next image. Then, the resulting images with secret keys are provided to the user's mail by TA, and the registration is completed successfully. During the user login phase, the users are asked to upload the set of images provided by TA, and it verifies the data availability in the images and imitates data decoding. Moreover, the recovered data will be decrypted through the decryption of the OTP password, and the TA verifies the secret code from the set of images and authenticates the users. Then, the security key with the resulting images is stored in the blockchain. This authentication enhances network security by resisting illegitimate users.

3.4. Hierarchical Clustering

After successful authentication, the nodes (users) are clustered to improve routing reliability and communication scalability. In our work, we have proposed enhanced hierarchical energy-balanced clustering where this clustering technique extends the lifetime of first node death by mainly considering the relative distance, residual energy, and regional density of the nodes, then it also contemplates the dynamic threshold range of energy parameters for each round. For that purpose, we propose Dividing well to merge a better algorithm where this algorithm comprises two phases, the division phase and the merging phase, which are represented in Figure 3. The proposed algorithm benefits from determining different cluster densities, being easily tunable, and effectively detecting and neglecting the outliers.

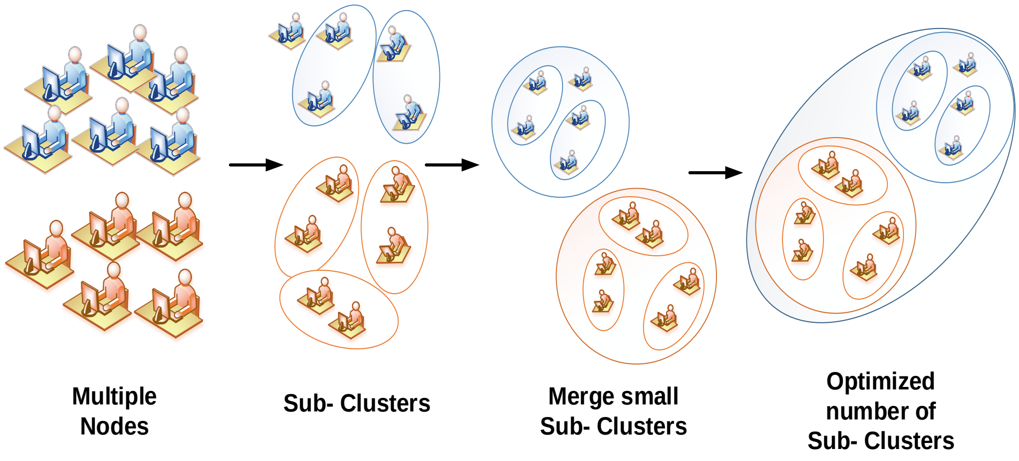

Figure 3 Hierarchical Clustering

First, the nodes are formed into an optimized number of sub-clusters. Then the small sub-clusters are merged corresponding to enhance statistical metrics and, in this way, the nodes are clustered. By performing effective clustering, the network scalability and system performance might be enhanced.

3.5. Trust Enumeration and KIDS

Once nodes are clustered efficaciously, trust evaluation and intrusion detection are performed to block the network's harmful nodes. The trust of all nodes is estimated by quantifying five factors, including DT, IDT, RT, data packet delivery, and trust of data bytes. DT is evaluated through communication and behavior. The IDT is the opinion obtained through the neighborhood of 1 hop node with high trust. The RT is determined by DT and IDT, as well as the authorization and conceding sink or destination. The trust of delivery of data packets is computed through the total data packet received ratio to packet transaction from the node, the number of packets it transmitted, and the number of packets it rejected. Furthermore, the trust of the data byte is evaluated by the communication of data in bytes among the nodes and destinations; then the enumerated trust values are stored in the blockchain to enhance security. After trust estimation, KIDS is performed to secure the data transmission by blocking malicious nodes. Each node in the MANET is outfitted with kangaroo-like traits, including the capacity to identify and respond to anomalies in the network in a KIDS. These kangaroo-like nodes are in charge of keeping an environment of secure communication by keeping track of network traffic, spotting suspicious activity, and taking the necessary countermeasures.

The system uses sophisticated routing protocols created especially for cloud-assisted 5G-MANETs and facilitates quick multipath route discovery and upkeep. The network's resilience, dependability, and load balancing are ensured by these protocols, which assist in creating various paths between the source and destination nodes. The KIDS improves the system detection performance, and IDS employs successive jumps like kangaroo, once the attack is detected for announcing. For that purpose, we have proposed Bi-LSTM, where the gateway filters the packet flow and analyses by considering the number of packets per flow, packet count, packet size, packet arrival time, and packet ID. BiLSTM stores data in both the forward and reverse directions of the neural network. The LSTM model, which extracts common temporal patterns from learning feature sequences and long-range contextual linkages from input sequences, is made up of LSTM cells.

$$i_q= \mu(X_i.[e_{q-1}, h_{q-1}, z_q]+ b_i \qquad (5)$$

$$d_q = \mu(X_d. [e_{q-1}, h_{q-1}, z_q]+ b_d \qquad (6)$$

$$e_q = d_q. e_{q-1}+ i_q. \widetilde{e}_q \qquad (7)$$

$$O_q = \mu(Y_r. [[e_q, h_{q-1}, z_q]+ b_r \qquad (8)$$

$$h_q =O_q. \text{Tanh}\ (d_q) \qquad (9)$$

The initial order, return order, and storage condition at any given moment p, as shown in equations (7), (8), and (9), are denoted by the letters subscript base, e sub q, by the letters e_q, O_q, h_q. Additionally, $i_q, and\ d_q$as shown in equations (5) and (6) stand for the input gate and output gate, respectively. The input gate, forget gate and output gate's related bias vectors are designated as b_i, b_d, and b_r, respectively. Using $\widetilde{e}$, the activations of the cells are represented. The size of these values matches that of the input vector. Sigmoid functions that are not linear are denoted by the letter l. A stacked LSTM layer that uses similar weights to another layer can interact with it. These LSTM layers can be used to produce bidirectional/unidirectional LSTM. In this case, the two layers of a BiLSTM operate in opposing temporal directions. These layers are used to discover long-term bidirectional links between time steps. Utilizing BiLSTM had the benefit of producing characteristics from both the previous and following time steps. Two bilateral LSTM layers with 256 stackable LSTM blocks each make up the BiLSTM model. After the BiLSTM layers, the softmax is used to categorize encoded sequences. Following training, the Inception model feeds the BiLSTM model with the features it has derived from the temporal sequences. The Bi-LSTM algorithm enhances intrusion detection accuracy by utilizing both forward and backward information. When the uncertainty is detected by these factors by exceeding a certain threshold range then the intruder is detected and blocked from the network. Moreover, then the superior CH is selected by considering packet delivery ratio, capacity, distance, and trust. In this way, the network security level will enhance and provide secure data transmission.

3.6. Effective Route Discovery and Route Maintenance

After trust evaluation and intrusion detection, all the nodes in the cluster share their details, including energy, position, mobility, location, number of transmissions, mobility speed, and number of neighbours to SCH, which are maintained. Also, all the nodes intermittently broadcast their current location details to update the SCH based on their packet arrival angle, current location, and transmission range. This supports improving route discovery by eliminating selfish nodes and reducing insecure paths. For that purpose, we have implemented an Advanced AODV which discovers the route using FHO.

3.7. Advanced AODV

The optimal route is discovery using Advanced AODV and Fire hawk optimization algorithm by considering significant parameters that are effectively applicable to a real-time environment. The Advanced AODV is implemented for effective route maintenance through enumerating link status and reliability of nodes that reduce the high packet loss rate. For efficacious route discovery, an Advanced AODV routing protocol is established, and CH maintains the necessary details (position update, energy) of CM to discover the optimal route using FHO. When α refers to the Source Node, β represents the Destination Node, γ illustrates the Data Packet, ϖ presents the multipath, ð denotes cluster nodes. Algorithm 1 presents the Advanced – AODV.

```
Input: $\alpha$, $\beta$, $\gamma$
$\alpha$ checks the routing table for a valid route to $\beta$
If a valid route exists:
  - Send $\gamma$ through the established route
  - End procedure
 If no valid route exists:
  - $\alpha$ initiates route discovery by broadcasting RREQ in $\varpi$
  - SCH gets RREQ and transmits PREQ by equ. (17) to all ð
  - Nodes frequently update SCH for route improvement.
$\beta$ confirms data delivery with RREQ and RREP
$\alpha$ disperses the $\gamma$ using IDA into multiple shares
Transmit shares via $\varpi$ with some redundancy
Select the node in $\varpi$
Output: $\gamma$ was securely transmitted from $\alpha$ to $\beta$
```

Algorithm 1 Advanced- AODV

Only the destination host can respond to the RREQ message, according to the D field in the message. The host replicates the requesting host's destination address and sequence number into the appropriate fields of the RREP message while it is being generated. The target sequence number field receives a copy of the increased receiver sequence number if it serves as the destination host. Additionally, the host's first timeout value is set in the RREP message's lifespan parameter, and the hop count is set to zero. The address of the host from whom the receiver acquired the RREQ message is simply entered into the recipient's address field if it is an intermediary host and copies the destination sequence number from the routing database.

The host must also provide in the RREP the hop count and lifetime from the routing table. Taking the present time and the expiration time out of the routing database, the lifespan is determined. Route deletion, route expiration, and RERR messages: The host needs to delete the entry for the current path in the routing database in Figure (4) when a link breakage occurs.

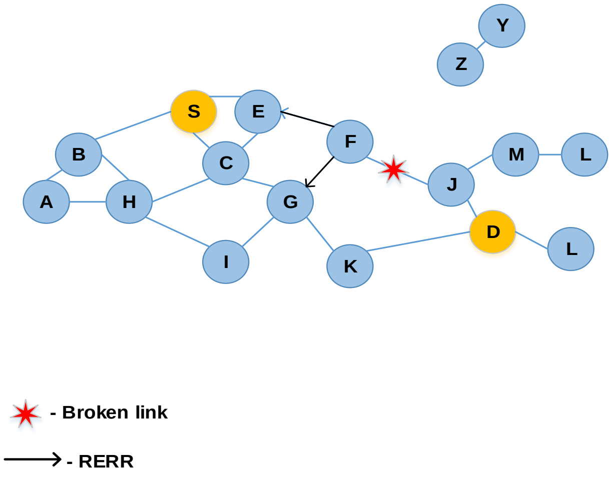

Figure 4 Linear Breakage

To obtain optimal multipath by contemplating trust, node connectivity, throughput, node degree, bandwidth, energy, and distance where this protocol offers loop-free operation and enhances its scalability to numerous numbers of terminals. Whenever the source node transmits a data packet, it ensures the routing table whether it has a well-founded route to the destination. This protocol comprises four control messages, including RREQ, RREP, RERR, and PREQ. The Information Dispersal Algorithm (IDA) is implemented where the source node disperses the messages into multiple shares and transmits through multiple paths with few redundancy data via multipath. Based on the position update, the route discovery from source to destination is initiated through RREQ in multipath to reach the destination. Furthermore, the destination node accepts the request and sends the RREP for confirming data transmission.

To enhance secure data transmission, the messages are cryptographed using the hash function E-ART algorithm to build the data integrity system which is utilized to protect data transmission from malicious users. Once the routes are discovered successfully, we perform effective route maintenance to reduce high packet loss and link failure rate. After every transmission, the SCH shares the transmission and position details with the Monitoring agent (MA) in the base station which helps to monitor the data transmission for route maintenance. The link state prediction is performed to predict the link failure to the next hop by received signal strength and through node reliability by considering response time, communication quality of each node, and energy level this helps to detect the route breakage and status of the link by the intermediate node. Once the link failure is detected, RERR is generated to SCH and the source node. Then the MA exploits two operations including redirecting or finding a new route to avoid packet loss. First, the possibility of redirection is ensured by checking other paths (i.e. the other paths in multipath). If any path completes the data transmission and the nodes remain with adequate energy and mobility, then the packets are redirected to that path. Otherwise, if the transmissions in all other paths are proceeding, then the new path is discovered using position update details by SCH. The alternative route discovery is initiated by Provincial Repair Request (PREQ), then the table ensures that it has a valid route, and then the destination node sends RREP to accomplish the data transmission. Then, the message of multiple shares via multipath is rebuilt to obtain the secure message, and the feedback is collected and stored in the blockchain to update the trust value and amplify the secure data transmission.

3.8. Fire Hawk Optimization Algorithm (FHO)

The primary goal of FHO is to effectively identify multiple paths in the ad hoc network between source and destination nodes. Multipath routing can improve network resilience and load balancing by using numerous paths concurrently, in contrast to standard routing protocols that concentrate on finding the single optimum path. The Advanced AODV employs FHO to ensure that the routing protocol does not run in loops. Routing loops can degrade network performance by producing duplicate data transmissions and consuming valuable network resources. Using FHO optimization ideas, the protocol can create loop-free pathways and avoid routing loops. In addition to considering how to acquire prey, the FHO algorithm also considers how to start and spread fires, mimicking the hunting patterns of fire hawks. Equation (10) represents a collection of potential solutions (Y) based on the location vectors of the fire hawks and their prey, which is initially established. The initial positions of these vectors in the search space are set via a random initialization technique.

$$\mathrm{Y}=\begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_j \\ \vdots \\ Y_M \end{bmatrix}=\begin{bmatrix} y_1^1 & y_1^2 & \cdots y_i^1 \cdots y_1^q \\ y_2^1 & y_2^2 & \cdots y_i^1 \cdots y_2^q \\ \vdots & \vdots & \\ y_j^1 & y_j^2 & \cdots y_j^i \cdots y_j^q \\ \vdots & \vdots & \\ y_M^1 & y_M^2 & \cdots\ y_M^i\ \cdots y_M^q \end{bmatrix}, \begin{cases} j = 1,2,\dots,M. \\ i = 1,2,\dots,q. \end{cases} \quad (10)$$

$$y_j^i(0) = y_{j,min}^i \text{ +sand. } (y_{j,max}^i\text{-}y_{j,min}^i), \begin{cases} j = 1,2,\dots,M. \\ i = 1,2,\dots,q. \end{cases} \quad (11)$$

In the above equation (11), M indicates the amount of potential solutions in the search area as a whole, y_j depicts the ith solution candidate in the search space, d is the dimension of the problem under consideration, y_j^i(0) represents the starting point of each of the solution candidates, y_j^i is the ith selection variable of the ith solutions candidate, and rand is a number that is evenly distributed in the range of (0,1), and $y_{j,max}^i$ and $y_{j,min}^i$. To identify the Fire Hawks in the search space, the issue of optimizing is taken into consideration when evaluating probable solutions using an objective function. To differentiate between predators and victims, some solution options have greater functional objective values. The selected Fire Hawks are employed to disperse fire surrounding the animals in the hunt area making hunting simpler for the hunter. Additionally, it is thought that the primary fire, which was initially utilized by the Fire Hawks to completely engulf the search area in flames, is the best choice. These characteristics are represented mathematically as shown below in equation (12) and (13).

$$\mathrm{PR}=\begin{bmatrix} PR_1 \\ PR_2 \\ \vdots \\ PR_k \\ \vdots \\ PR_a \end{bmatrix}, \text{ n= 1, 2,…, a} \quad (12)$$

$$\mathrm{FH}=\begin{bmatrix} FH_1 \\ FH_2 \\ \vdots \\ FH_k \\ \vdots \\ FH_m \end{bmatrix}, \text{ 1= 1, 2,…, m} \quad (13)$$

Where PR_k exposes the kth prey in the search space based on the total number of m preys, and FH_1 explains the lth fire hawk in a full search space of m fire hawks. The equation (14) then calculates the distance between the Fire Hawks and their prey, where Q_n^1 is represented by the following equation:

$$q_n^1= \sqrt{(y_2 - y_1)^2 + (x_2 - x_1)^2}\ , \begin{cases} 1 = 1,2,\dots,m. \\ n = 1,2,\dots,a. \end{cases} \quad (14)$$

In the equation provided, q_n^1 represents the total distance between the lth fire hawk and the kth prey. The terms (y_1-x_1) and (y_2-x_2) denote the coordinates of the entire set of prey and fire hawks in the search space, respectively. The birds' territories are defined by the proximity to the nearest adjacent prey, and the overall distance between Fire Hawks and their prey is calculated using the previously mentioned approach. Following this, Fire Hawks construct a fire at the specified location utilizing hot coals obtained from the main fire.

As certain birds may utilize flaming logs outside of Fire Hawks' territories, these actions can serve as location-updating methods within the primary search loop of the Fire Hawks Optimization (FHO) algorithm, as illustrated in equation (15) below:

$$FH_1^{new} = FH_1 + (s_1 \times GB - s_2 \times FH_{near}),\ \ 1, 1, 2, \dots n. \quad (15)$$

Where the Fire Hawks' migration towards the important fire and the territories of the other Fire Hawks is represented by the variables s_1 and s_2. A random number between 0 and 1 is used to divide the numbers evenly. In the search area believed to be the main fire, GB shows the world's best solution; 〖FH〗_1^new shows the new position vector of the lth Fire Hawk (〖FH〗_1); and 〖FH〗_near shows the

Fire Hawk that is closest to the search space. The prey's movement during each firing provides information for the next phase of the algorithm, which involves updating positions. The hawk's domain is thought to play a significant role in animal behavior. When updating a position, one may use the equation (16) below to account for these actions:

$$PR_d^{new} = PR_d + (s_1 \times FH - s_2 \times SP_1), \begin{cases} 1 = 1,2,\dots,m. \\ d = 1,2,\dots,s. \end{cases} \quad (16)$$

Where SP_1 is a safe location beneath the territory of the lth Fire Hawk; GB is the global best solution in the search space considered to be the main fire; PR_d^{new} is a fresh location position for the qth victim (PRd) that is contained by the lth Fire Hawk (FH1), and s3 and s4 are evenly spaced random numbers in a range of (0, 1). The target may also get within striking distance from other Fire Hawks.

The potential exists for the victim to come close to the Fire Hawks at the same moment, which is engulfed in nearby flames and incarcerated. Fire Hawks might even attempt to elude detection in an area outside of their more secure territory range. The equation (17) that follows may be used to include these procedures in the location change procedure.

$$PR_d^{new} = PR_d + (s_5 \times FH_{alt} - s_6 \times SP), \begin{cases} 1 = 1,2,\dots,m. \\ d = 1,2,\dots,s. \end{cases} \quad (17)$$

Where 〖FH〗_alt is a fire hawk that is present in the search area; s_5 and s_6 to evaluate the motions of preys relative to the extra Fire Hawks and the safe area beyond the territory, specify uniformly distributed random integers in the range of (0, 1).

Where 〖PR〗_d^new shows the updated direction of the dth prey (〖PR〗_d) surrounded by the lth fire hawk (〖FH〗_1). Since the majority of animals gather in safe places to stay safe and secure during a hazard, equations (18) and (19) provide a mathematical description of 〖SP〗_1 and SP.

$$SP_1 = \frac{\sum_{d=1}^{s} PR_d}{s}, \begin{cases} 1 = 1,2,\dots,s. \\ d = 1,2,\dots,m. \end{cases} \quad (18)$$

$$SP = = \frac{\sum_{n=1}^{a} PR_n}{a}, \ k = 1,2,\dots,a. \quad (19)$$

Where PR_d represents the d^th prey in the search space, encircled by the lth fire hawk (FH_1), and PR_d represents the d^th prey. Algorithm 2 for Fire Hawk Optimizer (FHO).

```
Procedure Fire Hawk Optimizer (FHO)
Obtain the starting positions of the solutions candidates x in the space search with N candidates
Examine the candidates' fitness values for initial solutions
Establish the primary fire's Global Best (GB) solutions
While iterations < maximum number of iterations
    Determine the total quantity of Fire Hawks by generating an arbitrary integer n.
    Establish the presence of Fire Hawks (FH) and Preys (PR) in a search area.
    Determine the overall separation between Fire Hawks and Prey.
    Distribute the victim to establish the Fire Hawks' range
    for l=1:m
        By using Fire Hawks, calculate the altered places.
        for d= 1:s
            Determine the secure area underneath. jth Fire Hawks Territory by using equation (12) and (13)
            Determine the new positions of the prey by using the equation (14)
            Utilizing equation (16), determine the secure area beyond the j^th Fire Hawks Area.
            By using equation (17), calculate the latest locations of the victims.
        end
    end
    Examine the health of the recently evolved Fire Hawks and their prey.
    Determine the Global Best (GB) solutions as the main fire
End while
Return GB
end procedure
```

Algorithm 2 Fire Hawk Optimizer (FHO)

The experimental evaluation of the suggested solution is shown in this section. Advanced AODV method for performance evaluation. The results show that the proposed Advanced AODV achieves high efficiency.

This section consists of three components, including the modeling setup, a comparison of the results, and an overview of the findings.

4. EXPERIMENTAL RESULTS

The experimental evaluation of the suggested solution is shown in this section. Advanced AODV method for performance evaluation. The results show that the proposed Advanced AODV achieves high efficiency.

This section consists of three components, including the modelling setup, a comparison of the results, and an overview of the findings.

4.1. Simulation Setup

The simulation of the proposed Advanced AODV method as shown in Figure 5, is carried out via a network simulator version 3.26 (NS3). The specifications related to the proposed Advanced AODV method are easily affordable by this tool with the efficient structure of the network. This proposed approach is experimented with in a simulation environment of 750m × 750m. Table 2 describes the system specifications and table 3 illustrates the simulation parameters.

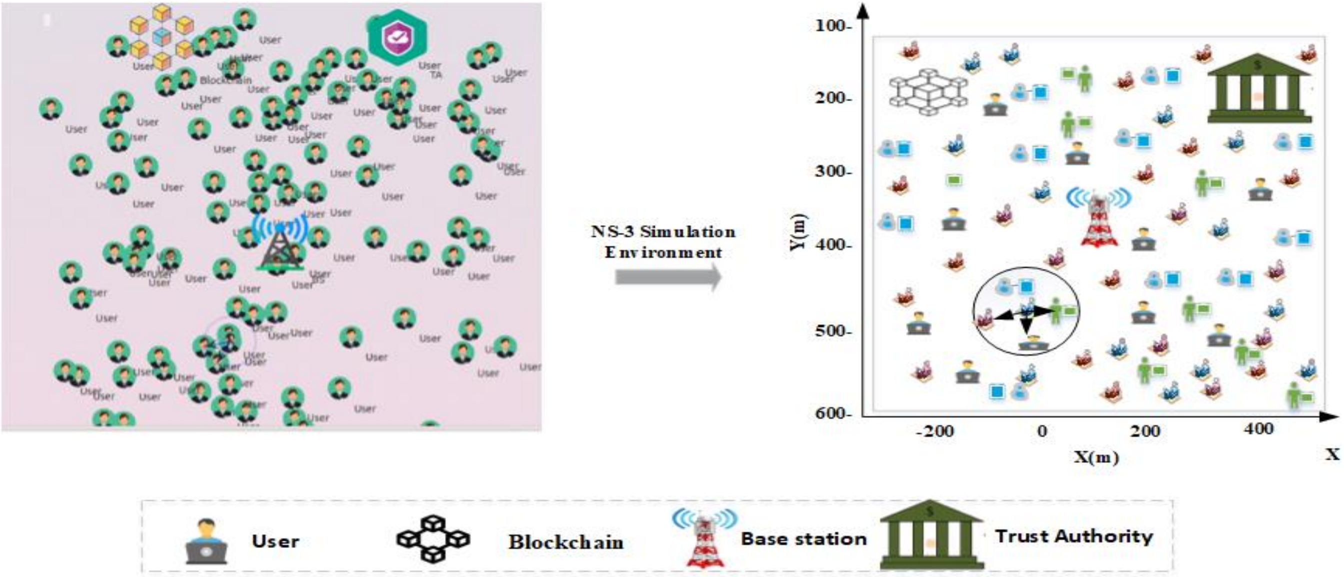

Figure 5 Simulation Environment

Table 2 System Specifications

Hardware specifications	Hard disk	500GB
	RAM	4GB
Software specifications	Network Simulator	NS- 3.26
	OS	Ubuntu 14.04 LTS

Table 3 Simulation Parameters

	Parameters	Description
Network parameters	User Nodes	100
	TA Node	1
	5G Base Station Node with monitoring agent	1
	Block Chain Node	1
Packet parameters	No. of packets	~1500
	Packet size	512 KB
	Flow timeout	2s
	Delay time	1µs
Transmission parameters	Transmission time	0.0097ms
	Data Speed	100 Mbps
	Range of Transmission	90m
	Bandwidth	6Mbps
Trichain	Block Header	90 bytes
	Size of block	72 bytes
	Counter of transaction	1-10 bytes
Proof of Work (PoW)	No. of rounds	24
	Size of word	8 bytes
	Size of key	128 bits
Simulation time	200s	

4.2. Comparative Analysis

The new strategy, such as the Group Teaching Optimization Algorithm (GTA), Genetic Algorithm with GAHC, is evaluated by comparing the proposed approach with the existing approaches. The evaluation takes into account the following factors: energy consumption, detection rate, packet delivery rate, delay, throughput, and authentication time.

4.3. Energy Consumption

The total energy consumed by the nodes for receiving, disseminating, and transferring the information is referred to as the network's energy consumption. Every node is given a starting energy value at the beginning, and every time a measurement is made in the simulation, each amount of energy is calculated by using following equation (20).

$$\text{Energy Consumption} = \beta \times \delta \qquad (20)$$

The proportionality constant " β " stands for the amount of energy consumed per node. The precise value of " β " would vary depending on the kind of nodes, how energy-efficient they are, and the workload they handle, δ defines the number of nodes.

Table 4 Numeric Results of Energy Consumption (J)

Number of users	Energy consumption (J)		
	GTA	GAHC	Proposed
20	55	50	38
40	60	55	42
60	66	59	45
80	69	65	47
100	72	68	50

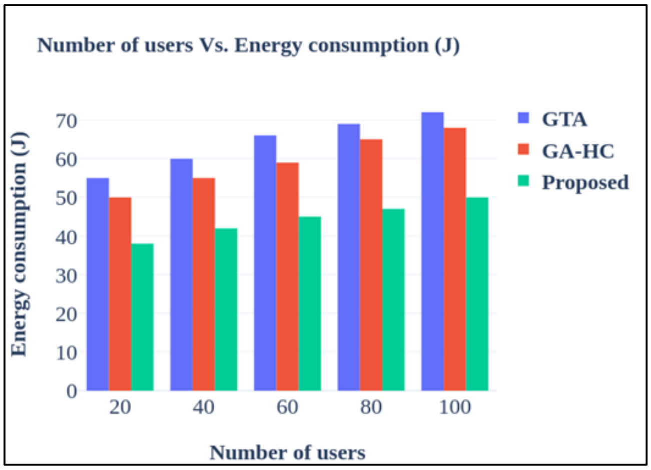

Figure 6 Number of Users Vs. Energy Consumption

Figure 6 and Table 4 compare the number of users vs. energy usage of the proposed technique with a few other existing methods. The graph that displays energy consumption (J) as a function of user count shows three scenarios: the suggested strategy, the GAHC, and the GTA. In all three cases, energy usage generally decreases as the number of users increases. Nonetheless, the suggested method demonstrates its value in attaining superior energy efficiency, continuously surpassing both GAHC and GTA for all user counts. The reduced energy consumption of the proposed technique is measured at user count 100, where it reaches 50 (J), whereas GAHC is 68 (J) and GTA is 72 (J). When everything is taken into account, the graph shows how these scenarios compare for different user numbers.

4.4. Detection Rate

It is described as the proportion of network attackers that were successfully found. We can use a formula based on the assumption since the relationship between the detection rate and node count is linear to determine the relationship between the number of nodes and the detection rate in proposed and existing approaches. It is crucial to remember, however, that the detection rate may also be affected by other factors, such as the efficacy of the intrusion detection system and network parameters. Let's call the detection rate "D" and the number of nodes "N". The relationship can be expressed as in equation (21)

$$\text{Detection rate} = \mu \times \delta \qquad (21)$$

In this equation (21), " μ " indicates the proportionality constant that encapsulates the detection rate per node. The exact value of " μ " would be determined by a lot of factors, such as the efficiency of the intrusion detection algorithms, the quality of data collected by nodes, and the level of cooperation among nodes in detecting and reporting intrusions.

Table 5 Numeric Results of Detection Rate (%)

Number of users	Detection rate (%)		
	GTA	GAHC	Proposed
10	65	77	89
20	67	79	91
30	69	82	92
40	72	83	92.5
50	75	84.2	93.2
60	79	86	94
70	81	86.9	95
80	85	88	95.8
90	87	899	97
100	89.8	91	98.7

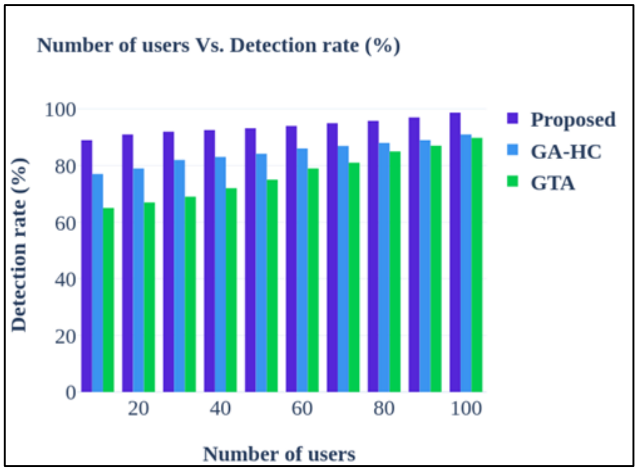

Figure 7 Number of Users Vs. Detection Rate

Figure 7 and Table 5 provide a comparison of the number of users vs. detection rate (%) for the recommended methodology and many alternative techniques. The graph shows the detection rate (%), GAHC, GTA, and the suggested strategy. As the number of users increases, the detection generally changes for all scenarios. It is noteworthy that, in comparison to GAHC and GTA, the suggested method consistently yields a higher detection rate for a variety of users. The suggested method outperforms GAHC (91%) and GTA (89.8%) with a detection rate of 98.7 (%) at 100 users. The increased detection rate of the suggested strategy is shown in the graph for different user-density situations.

4.5. Throughput (%)

Throughput is the quantity of data that can be sent over a network or system in a specific length of time. Changes in topology, noise on communication lines, the strength of the source node's transmission, and the presence of malicious nodes are all factors that can impact it. In general, as the number of connections rises, the overall efficiency of a network can vary. The relationship between the number of nodes (N) and the throughput (T) can be described by the following equation (22):

$$\text{Throughput} = \partial \times \delta \qquad (22)$$

In this case, " ∂ " indicates the proportionality constant that describes the throughput per node. The actual value of " ∂ " would be determined by factors such as network capacity, node transmission rate, and the effectiveness of network protocols and algorithms.

Figure 8 and Table 6 provide a comparison of the number of users vs. Throughput (%) for the proposed technique and a few other existing approaches. The graph that displays Throughput (%) as a function of user count displays three scenarios: the suggested method, GAHC, and GTA. Throughput generally rises with the number of users in all three scenarios. However, the suggested method consistently outperforms both GAHC and GTA for all user counts, demonstrating its value in obtaining higher throughput. When there are 100 users, the proposed method's peak throughput is 93%, whereas GAHC is 85% and GTA is 71%. All things considered, the graph shows how different scenarios differ in terms of the number of users.

Table 6 Numeric Results of Throughput (%)

Number of users	Throughput (%)		
	GTA	GAHC	Proposed
20	65	79	87
40	67	80	88.2
60	68	82.2	89.1
80	69.2	83.5	91.2
100	71	85	93

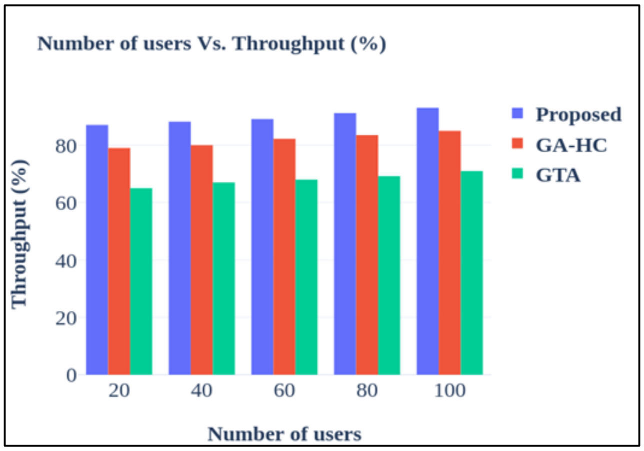

Figure 8 Number of Users Vs. Throughput

4.6. Packet Delivery Rate (%)

The fraction of packets that are successfully delivered to all packets sent is referred to as the packet delivery rate in a network. It measures the efficiency of packet transmission and indicates the reliability of the network in delivering data without loss or errors. The following equation (23) can illustrate the correlation between node density and (N) and the packet delivery rate (PDR):

$$\text{PDR}= \vartheta/(N)\times 100 \qquad (23)$$

Where ϑ refers to the number of successful delivery packets and N indicates the total amount of packets transmitted. The packet delivery rate is reported as a percentage (%) in this case. The numerator reflects the percentage of packets that reached their destinations successfully, while the denominator represents the total quantity of packets sent.

Table 7 Numeric Results of Packet Delivery Rate (%)

Number of users	Packet delivery rate (%)		
	GTA	GAHC	Proposed
20	65	71	80
40	67	82	83
60	70	85.5	86.5
80	75.5	86.5	88
100	80.6	89	90

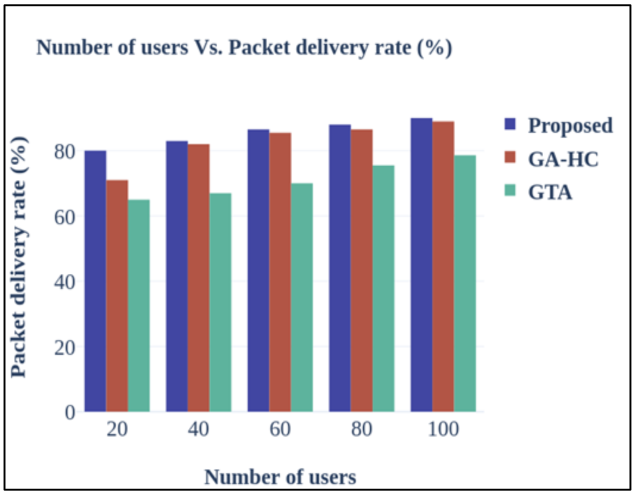

Figure 9 Number of Users Vs. Packet Delivery Rate

Figure 9 and Table 7 illustrate the comparison of the number of users vs. packet delivery rate between the proposed method and several existing methods. The packet delivery rate of improvement is depicted in the graph for three distinct scenarios: the proposed technique, GAHC, and GTA. Different scenarios have different levels of packet delivery rate as the number of users rises. The suggested approach often outperforms GAHC and GTA, obtaining a flawless packet delivery rate of 80% across all users. Notably, the proposed approach outperforms both GAHC (89%) and GTA (8.6%) with a packet delivery rate of 90% at a number of users 100. The graph highlights the packet delivery rate that the proposed technique provides in different user conditions.

4.7. Authentication Time

The time it takes for a system or process to verify and validate the identity of a person or entity is referred to as authentication time. It typically measures the time required to validate credentials, perform cryptographic operations, and complete additional authentication procedures. The authentication time in the proposed technique would be determined by the specific authentication procedures and algorithms used and the processing capability of the nodes involved. The number of nodes and the authentication time might vary based on factors such as the authentication procedure's complexity, the algorithms' efficiency, and the nodes' processing power.

$$Authentication\ Time\ = \varphi \times \qquad (24)$$

In this case, φ indicates the proportionality constant that encapsulates the authentication time per node, and then δ refers to the number of nodes. The actual value of "φ" would be determined by a variety of factors, including the computational complexity of the authentication methods, processor speed, the efficiency of cryptographic operations, and any additional stages or overhead involved in the authentication process.

Table 8 Numeric Results of Authentication Time (s)

Number of users	Authentication time (s)	
	GTA	Proposed
20	46	40
40	50	45
60	59	49
80	65	52
100	79	58

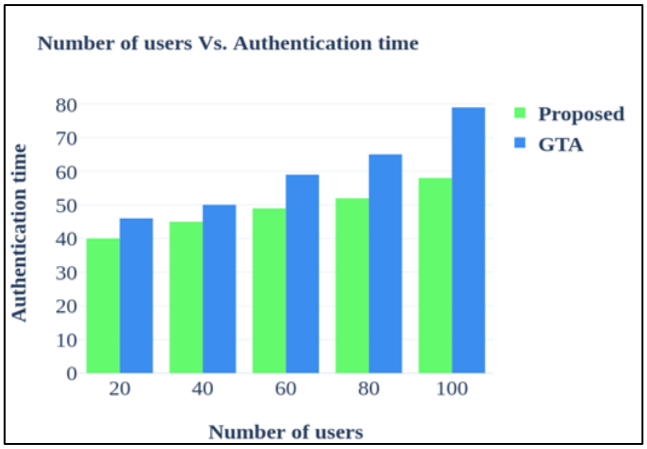

Figure 10 Number of Users Vs. Authentication Time

Figure 10 and Table 8 provide a comparison between the number of users vs authentication time for the proposed methodology and many existing approaches that are presently in use. The suggested approach and the GTA scenario's authentication times are shown against the number of users in a graph. Every scenario sees a steady decrease in authentication time as user volume increases. With a value of 58 (s) for users 100, the suggested method notably beats GTA and has the lowest authentication time across all user levels. The graph shows how, for a variety of user counts, the suggested solution performs better than the other two situations in terms of authentication performance and authentication time reduction.

4.8. Delay

In the context of evaluating the proposed work, "delay" often refers to the amount of time needed for the packets of data in a network to move from the starting node to the point of destination. It shows the time delay or latency that packets encounter during transmission. The delay can be estimated mathematically using the following equation (25):

$$Delay = \eta + \xi + \psi \qquad (25)$$

When η refers to Transmission Time, ξ refers to Propagation Time, ψ refers to Queueing Time.

Table 9 Numeric Results of Delay (s)

Number of users	Delay (s)	
	GTA	Proposed
20	52	49
40	55.5	53.2
60	62	56
80	67	57
100	70	60

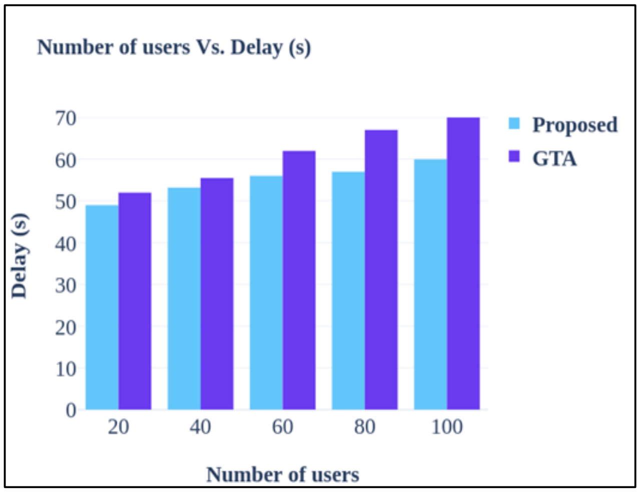

Figure 11 Number of Users Vs. Delay (s)

A comparison of the number of users vs. delay for the suggested technique and several other ways that are currently in use can be seen in Figure 11 and Table 9. A graph displays the latency of the GTA scenario and the recommended method vs the total number of users. As user traffic rises in all scenarios, latency steadily decreases. The recommended approach significantly outperforms GTA and has the lowest delay across all user levels, with a value of 60 (s) for users 100. The graph illustrates how the recommended approach outperforms the other two scenarios in terms of delay performance and delay reduction over a range of user numbers.

4.9. Research Summary

We establish a network with 100 User Nodes, 1 TA Node, 1 5G Base Station Node with a monitoring agent, and 1 Block Chain Node. Register using user name, ID, mail ID, and password. The TA generates a random secret code and encrypts using the E-ART technique. Graphical User Authentication follows. Next, we use Divide well to merge better algorithm to perform Hierarchical Clustering based on node relative distance, residual energy, and regional density. Using Bi-LSTM, KIDS blocks hostile nodes to safeguard data transfer. Figures (6) – (11) and Tables (4-9) show the graphical and numeric results depiction of comparative results, and Table 10 provides the overall numerical results of the comparative analysis.

Table 10 Numerical Outcomes

Performance metrics	GTA	GA-HC	Proposed
Energy consumption (J)	72	68	50
Detection rate (%)	89.8	91	98.7
Throughput (%)	71	85	93
Packet delivery rate (%)	78.6	89	90
Authentication time (s)	79	-	58
Delay (s)	70s	-	60s

5. CONCLUSION AND FUTURE WORK

This study primarily focuses on secure data transfer in a MANET environment using intrusion detection. Furthermore, effective route discovery and route maintenance are designed to improve network security. Cloud computing is used to minimize storage computation, while 5G technology is used to improve connection reliability. The new strategy is evaluated by contrasting the suggested approach with the current approach. Here we propose a divide well merge algorithm to perform hierarchical clustering. Next, we use the FHO-based Advanced AODV to find the best route. Using the suggested KIDS, attack detection and security are accomplished along with optimum routing which minimizes MANET's energy usage. The proposed methods in terms of Energy consumption with 50 J, Detection rate at 98.7%, Throughput at 93 %, Packet delivery rate at 90%, Authentication time at 58s, and Delay at 60s. The performance of our approach is discussed with numerical analysis from which it can be proved that our technique performs better than the current approaches across the board. In future, an advanced and improved clustering technique for intrusion detection along with a hybrid cryptography technique can be used to effectively transmit data and improve the overall system performance.

REFERENCES

[1] Uppalapati S, 2020. Energy-Efficient Heterogeneous Optimization Routing Protocol for Wireless Sensor Network. Instrumentation Mesures Métrologies 19(5). Vol. 19, No. 5, October, 2020, pp. 391-397

[2] Lakshmi, G. V., & Vaishnavi, P. (2023). A trusted security approach to detect and isolate routing attacks in mobile ad hoc networks. Journal of Engineering Research. https://doi.org/10.1016/j.jer.2023.100149

[3] Allimuthu, U., & Mahalakshmi, K. (2023). Efficient Mobile Ad Hoc Route Maintenance Against Social Distances Using Attacker Detection Automation. “Mobile Networks and Applications” Volume 28 Issue 1 Feb 2023 pp 128–159 https://doi.org/10.1007/s11036-022-02040-3

[4] Srilakshmi U, Veeraiah N, Alotaibi Y, Alghamdi S A, Khalaf O I, & Subbayamma B V, 2021. An improved hybrid secure multipath routing protocol for MANET. EEE Access. https://doi.org/10.1109/ACCESS.2021.3133882.

[5] Bharany S, Sharma S, Badotra S, Khalaf O I, Alotaibi Y. Alghamdi S, & Alassery F, Energy-efficient clustering scheme for flying ad-hoc networks using an optimized LEACH protocol. Energies 2021, 14, 6016. https://doi.org/10.3390/en14196016 https://www.mdpi.com/journal/energies

[6] Rajkumar B, & Narsimha G, 2016. Secure multipath routing and data transmission in MANET. International Journal of Networking and Virtual Organisations, 16(3), 236-252.

[7] Elmahdi E, Yoo S M, & Sharshembiev K, 2020. Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. Journal of Information Security and Applications, 51:102425, DOI:10.1016/j.jisa.2019.102425.

[8] Singh P, Khari M & Vimal S, 2021. EESSMT: An energy efficient hybrid scheme for securing mobile ad hoc networks using IoT. Wireless Personal Communications, 1-25. 10.1007/s11277-021-08764

[9] Mukhedkar M M & Kolekar U, 2020. E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network. International Journal of Communication Systems, 33(9):e4252, DOI:10.1002/dac.4252.

[10] Rajendra Prasad P S, 2020. Efficient performance analysis of energy aware on demand routing protocol in mobile ad-hoc network. WILEY. Engineering Reports 2(3) , DOI:10.1002/eng2.12116

[11] Ahmad I , Rahman T, Zeb A , Khan I , Othman M T B & Hamam H , 2022. Cooperative energy-efficient routing protocol for underwater wireless sensor networks. Sensors, 22(18), 6945.

[12] Bhardwaj A, & El-Ocla H, 2020. Multipath routing protocol using genetic algorithm in mobile ad hoc networks. IEEE Access, 8, 177534-177548.

[13] Gorgich S, & Tabatabaei S, 2021. Proposing an energy-aware routing protocol by using fish swarm optimization algorithm in WSN (wireless sensor networks). Wireless Personal Communications, 119(3), 1935-1955.

[14] Rajan D P, Premalatha J, Velliangiri S & Karthikeyan P, 2022. Blockchain enabled joint trust (MF-WWO-WO) algorithm for clustered-based energy efficient routing protocol in wireless sensor network. Transactions on Emerging Telecommunications Technologies, 33(7), e4502.

[15] Srilakshmi U, Veeraiah N, Alotaibi Y, Alghamdi S.A, Khalaf O I & Subbayamma B V, 2021. An Improved Hybrid Secure Multipath Routing Protocol for MANET. IEEE Access, PP, 1-1.

[16] Prasad R & Shankar S, 2022. Secure Intrusion Detection System Routing Protocol For Mobile Ad-Hoc Network. Global Transitions Proceedings. Volume 3, Issue 2, https://doi.org/10.1016/j.gltp.2021.10.003

[17] Hemalatha R, Umamaheswari R & Soundaram J, 2021. Optimal route maintenance based on adaptive equilibrium optimization and GTA based route discovery model in MANET. Peer-to-Peer Netw. Appl., 14, 3416-3430.

[18] Veeraiah N & Krishna B T, 2020. An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence, 15, 1313-1327.

[19] Chugh N, Tomar G S, Bhadoria R S, & Saxena N, 2021. A Novel Anomaly Behavior Detection Scheme for Mobile Ad Hoc Networks. Electronics. Electronics 2021, 10(14), 1635; https://doi.org/10.3390/electronics10141635

[20] Bondada P, Samanta D, Kaur M. & Lee H, 2022. Data Security-Based Routing in MANETs Using Key Management Mechanism. Applied Sciences. Volume 12 Issue 3 10.3390/app12031041

[21] Rani P L, Kavita Verma S, Kaur N, Woźniak M, Shafi J & Ijaz. M.F, 2021. Robust and Secure Data Transmission Using Artificial Intelligence Techniques in Ad-Hoc Networks. Sensors (Basel, Switzerland), Sensors, 2021, № 1, p. 251 https://doi.org/10.3390/s22010251 .

[22] Theerthagiri P, 2021. ReCoMM: Resource-aware cooperation modelling using Markov process for effective routing in mobile ad hoc networks. Sadhana 46(4):209. DOI:10.1007/s12046-021-01743-9

[23] Islabudeen M & Devi M K, 2020. A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks Against Security Attacks. Wireless Personal Communications, 112 (1) 193–224. https://doi.org/10.1007/s11277-019-07022-5

[24] Chiejina E, Xiao H., Christianson B, Mylonas A & Chiejina C, 2022. A Robust Dirichlet Reputation and Trust Evaluation of Nodes in Mobile Ad Hoc Networks. Sensors (Basel, Switzerland), 22(2), 571, https://doi.org/10.3390/s22020571

[25] Lwin M T, Yim J & Ko Y, 2020. Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. Sensors (Basel, Switzerland). 20(3), 698; https://doi.org/10.3390/s20030698

[26] Farahani G, 2021. Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks. Security and Communication Networks, Volume 2021 https://doi.org/10.1155/2021/8814141

[27] Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access, 10. pp. 14260-14269. ISSN 2169-3536.

[28] Masood, J. A. I. S., Jeyaselvi, M., Senthamarai, N., Koteswari, S., Sathya, M., & Chakravarthy, N. K. (2023). Privacy preservation in wireless sensor network using energy efficient multipath routing for healthcare data. Measurement: Sensors, 29, 100867.

[29] Yin, H., Yang, H., & Shahmoradi, S. (2022). EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks. Telecommunication Systems, 81(1), 1-19.

[30] Al-Anzi, F. S. (2022). Design and analysis of intrusion detection systems for wireless mesh networks. Digital Communications and Networks, 8(6), 1068-1076.

[31] Allimuthu, U., & Mahalakshmi, K. (2022). Intelligent route discovery towards rushing attacks in ad hoc wireless networks. Journal of Ambient Intelligence and Humanized Computing, 13(2), 921-960.

RESEARCH ARTICLE

[32] Tyagi, L. K. ., & Kumar, A..(2023). A Hybrid Trust Based WSN protocol to Enhance Network Performance using Fuzzy Enabled Machine Learning Technique. International Journal of Intelligent Systems and Applications in Engineering, 11(9s), 131–144.

[33] M. S. Muthukkumar, S. Diwakaran, "Efficient Load Balancing in WSN Using Quasi –oppositional Based Jaya Optimization with Cluster Head Selection", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.2, pp.85-96, 2023. DOI:10.5815/ijcnis.2023.02.07.

[34] Binuja Philomina Marydasan, Ranjith Nadarajan(2023). An Energy-Conserved Stability and Density-Aware QoS-Enabled Topological Change Adaptable Multipath Routing in MANET. International Journal of Computer Networks and Applications (IJCNA) DOI: 10.22247/ijcna/2023/223692 Volume 10, Issue 6, November – December (2023).

[35] Sivanesan N, Rajesh A, K. S. Archana. ANFIS-RSOA Approach for Detecting and Preventing Network Layer Attacks in MANET. International Journal of Computer Networks and Applications (IJCNA) DOI: 10.22247/ijcna/2023/223693 Volume 10, Issue 6, November – December (2023).

[36] Ainaz Nobahari,Danial Bakhshayeshi Avval, Abbas Akhbari, and Solmaz Nobahary Investigation of Different Mechanisms to Detect Misbehaving Nodes in Vehicle Ad-Hoc Networks (VANETs). Hindawi Security and Communication Networks Volume 2023, Article ID 4020275, 40 pages https://doi.org/10.1155/2023/4020275.

Authors

Mr. Jayantkumar A Rathod, completed his Bachelor of Engineering in Computer Science and Engineering from S.D.M.College of Engineering and Technology, under Karnataka University Dharwad, India. He obtained his M.Tech in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi, India. He is presently working as Associate Professor and pursuing his Ph.D at Alva’s Institute of Engineering and Technology, Moodubidire , India. He has around 18 years of teaching experience and 3 years of research work. He has published around 15 papers in various reputed journals. His area of interest include Ad-Hoc Networks, Cryptography and Network Security, Wireless Sensor Networks, Data Mining, Deep Learning.

Dr. Manjunath Kotari did his **Bachelor of Engineering** in Computer Science & Engineering from **R.V.College of Engineering, Bangalore**. He obtained his **M.Tech** in Computer Science and Engineering from **NMAM Institute of Technology, Nitte** and completed his **Ph.D** from Visvesvaraya Technological University, Belagavi, Karnataka, India. His research work focuses on Distributed Systems & Network Security. He has around 22 years of teaching experience. Presently he is working as **Professor & Head** in the Department of Computer Science and Engineering at Alva's Institute of Engineering & Technology, Moodubidire. India. He has published two patents and waiting for grants. He has many papers published in reputed journals. His areas of interest are Network Security, Computer Architecture and VLSI CAD. He has served as a Member of BoS and BoE for VTU and other various Universities. He is a Member of VTU-LIC (Local Inquiry Committee). Member of Professional Bodies such as IEEE, CSI, ISTE, IAENG and ISTD.

How to cite this article:

Jayantkumar A Rathod, Manjunath Kotari, “TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol”, International Journal of Computer Networks and Applications (IJCNA), 11(1), PP: 61-81, 2024, DOI: 10.22247/ijcna/2024/224436.