scientific reports

Check for updates

OPEN

# Authentication mechanism based on distributed blockchain for secure and energy efficient mobile ad-hoc networks

V.R. Sugumaran[1]✉, E. Dinesh[2], R. Ramya[3] & Elangovan Muniyandy[4,5]

**This work addresses the security issues which occurred in the Mobile Adhoc Networks (MANETs). The earlier efforts seen in MANET are more centralized and use more power. Therefore, the objective of this study is to offer high levels of security with minimal energy usage. This work creates a unique DBlock-Auth technique for MANETs to accomplish this objective. According to the Similarity Score (Sim-Score), the total networks are separated into several zones and every zone is further converted into numerous clusters. Prior to that, each node is verified through the Blockchain based PUF (BPUF) method and that authenticates each node's Physical Unclonable Functions (PUF). The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) multi-criteria method is used to choose the best CH from among the numerous clusters created by each of the acceptable node. The MuMoT technique selects the best path for data transfer inside each cluster. Finally, the Light HB technique ensures the security of data. This result of simulation is executed by using the ns2 network's simulators and that computes efficiency of Quality of Service (QoS) parameters. These simulations' results also obtained the best security levels, Packet Delivery Ratio (PDR), efficiency of energy, latency, accuracy of detections, energy usages, and throughput.**

**Keywords** MANET, DBlock-Auth, BPUF, MuMoT

**Abbreviations**

| | |
|---|---|
| MANETs | Mobile Adhoc Networks |
| DoS | Denial-of-Service |
| IDS | Intrusion Detection System |
| DLT | Distributed Ledger Technology |
| P2P | Peer-to-Peer |
| Sim-Score | Similarity Score |
| MuMoTR | Multi-Model Trust-based Routing |
| IoT | Internet of Things |
| SIEM | Security Information and Event Monitoring |
| OLSR | Optimized Link State Routing |
| PUF | Physical Unclonable Functions |
| QASO-BDT | Quantum Atom Search Optimization coupled with Blockchain aided Data Transmission |
| CG | Capillary Gateway |
| CH | Cluster Head |
| AODV | Ad Hoc On-Demand Distance Vector |
| NS-2 | Network Simulator 2 |
| VANET | Vehicular Adhoc NETwork |
| C-R | Challenge Response |

[1]Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India611002. [2]Department of Electronics and Communication Engineering, M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India639113. [3]Department Artificial Intelligence and Data Science, St Joseph's College of Engineering, Old Mahabalipuram Road, Chennai, Tamil Nadu, India600119. [4]Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India602105. [5]Applied Science Research Center, Applied Science Private University, Amman, Jordan. ✉email: sugumaran@egspec.org

| | |
|---|---|
| TOPSIS | Technique for Order Preference by Similarity to Ideal Solution |
| HB | Hummingbird |
| ANN | Artificial Neural Network |
| ECC | Elliptic Curve Cryptography |
| PDR | Packet Delivery Ratio |
| RE | Residual Energy |
| BAA | Blockchain-Assisted Authentication |
| BPUF | Blockchain based PUF |
| QoS | Quality of Service |

MANET is frequently implemented over ad-hoc link-layer networks. These are constructed from moveable nodes that are connected wirelessly in an independent, self-repairing network that does not require a fixed structure. Because the structure of the networks is always changing, MANET nodes are free to migrate whenever they choose[1]. Once it is necessary to relay messages to further designated nodes in the networks, all of the node's act as routers. MANET typically operates as follows:

- The lack of hardware and an access point.
- Independent and direct communications within the wireless devices
- The devices begin looking for and communicating with each other.
- Operate frequently, individually or collectively, within a massive network, like the Internet.
- Devices can flexibly add or delete nodes to enter or exit networks at any time.
- Once the node is spread out, any nodes in its path that leads to the desired node act as routers, transferring packets of data to the node of the destination one at a time.
- The devices have their own reserves of energy, like the batteries they use for electricity.

Nevertheless, MANET has several instantaneous applications as illustrated in Fig. 1.

Because MANET has so many uses, it is frequently employed in research. Nevertheless, the issues listed below continue to be significant for MANET.

- No centralized control: All aspects of the operation depend on how the many devices behave and cooperate.
- Regularly modifying the network's topology or the way the gadgets are set up.
- Random Device Change: Devices are randomly and quickly joining and leaving the network.
- Fewer interventions by humans
- Minimum capacity of the battery
- Low Bandwidth: These types of networks have very limited capacity and range for the transmission of data.
- Each device performs two functions: it acts as the router and the device on the other side of the network, respectively.
- They are frequently attacked.
- Theft is a risk since the devices utilized in this type of network have become so small.
- Reduced Security: This network is subject to greater security threats than traditional wired networks.

These problems have caused a significant decline in MANET performance. Cluster-based routing methods have received a lot of attention as ways to boost MANET efficiency[2]. Because of the MANET nodes' quick movement

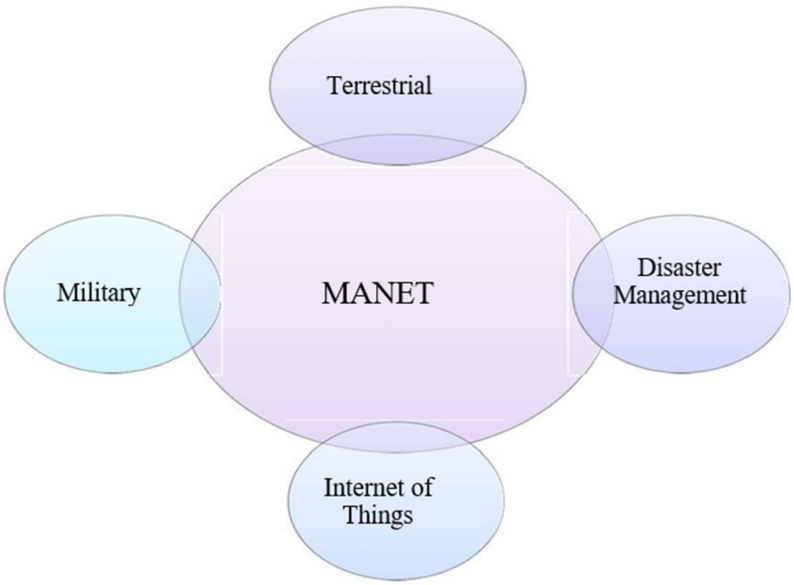


**Fig. 1**. Applications of MANET.

and dynamic cluster administration, choosing an ideal cluster head and route selection are still difficult tasks in clusters and routing.

Additionally, clustering, and optimal routing help the network run better. In contrast, MANET experiences several attackers at every level, which compromises its security. An ad hoc infrastructure may be easily assembled by nodes in a mobile environment using a common radio link[3]. However, a safe line of communication is required to allow nodes to communicate safely.

Before creating a secure connection, the node should be capable of identifying other nodes. All nodes have to reveal their identities and associated login information to the others. However, the supplied identities and login information must be protected and verified so that the recipient node cannot challenge their legitimacy or integrity. Each node needs to ensure that their identities and login information offered to receiver nodes are secured. Therefore, security design is essential for securing ad hoc networks. MANETs are vulnerable to a variety of security issues. Several separate features are used to categorize attacks in MANET. In MANET, these attacks are primarily separated into passive and active attacks. Active attacks and passive attacks are the two main classifications of attacks made against MANET.

**Passive attacks:** Passive attacks are intended to steal confidential data from networks. The data on the network is not changed when passive attacks are used; rather, the attackers attempt to take the real data by observing activity while tuning in. Since network operations are undisturbed, it is challenging to expose these types of attacks[4]. To resist these attacks, data is transmitted over the networks in an advanced, secure way.

**Active attacks:** The attacker uses active assaults to

try to obstruct interactions between network nodes[5]. This assault supports the abuse of network capabilities by the offenders and that can result in traffic jams, attacks of Denial-of-Service (DoS), controlling packet manipulation and so on.

Figure 2 shows the main assaults that have been launched against MANET. For MANET security, several research studies have proposed Intrusion Detection System (IDS), methods of authentication, and cryptographic strategies[6]. The enormous number of mobile nodes involved and the quick growth of MANET applications necessitate the use of dynamic, lightweight security techniques. Blockchain, a decentralized safe network, has recently risen to a significant position in providing security. Blockchain is a decentralized, unchangeable database that makes it easier to monitor assets and record interactions within the network of an organization. Assets might be either physical (such as a home, car, cash amount, or plot of land) or intangible. With the help of Distributed Ledger Technology (DLT), data is dispersed over a Peer-to-Peer (P2P) network as opposed to being retained in one location[7]. A consensus mechanism, such as proof of stake or proof of work, is employed to confirm the correctness of the information. Blockchain is one of the leading technologies in both current and future networks due to its outstanding characteristics such as immutability, consensus, proof of work, and clever obtaining technologies. Blockchain provides a variety of useful communication and data services through the network's platforms. When discussing a network such as MANET, a lack of communication capabilities leads to a wireless network that is incredibly undeveloped, with low-capacity sensors having serious attack issues since attackers from the outside obtain the ability to access data[8]. As a result, the MANET networks are still undeveloped and low-featured for the current state and future generations of MANET technologies, in which case

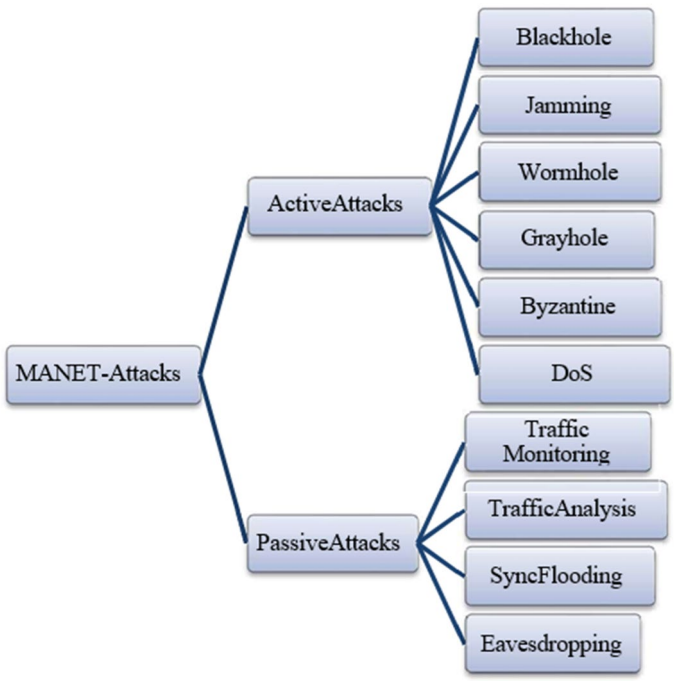


**Fig. 2**. Security threats in MANET.

blockchain is a suitable answer for underdeveloped technologies. Since blockchain ensures the confidentiality of data and the reliability of authorized involvement, this is advantageous for the implementation of MANET across a series of blocks. Blockchain additionally provides an environment of trust for the collection of data and the handling of intermediaries, such as other participants. The blockchain is a collection of methods used by a decentralized network to ensure that each user is contributing to an accurate database. Satoshi Nakamoto was the person who first proposed the concept of abstracting the underlying ideas that underlie the popular digital currency, or bitcoins[9]. Block-string-based networks do not have fixed center nodes, compared to traditional centralized networks. Every member of the network retains identical copies of the blockchain, and its positions are identical. Because of its high level of security and reliability, blockchain has been deployed in a variety of application situation and has been recognized as one of the key tactics for stimulating worldwide expansion. The consensus method's initial two phases are block validation and selecting the most extensive chains. These two steps are individually completed by each node. When a new block arrives, each node broadcasts it to its neighbors, which can receive it. The blocks are spread throughout the networks. The node performs a block check before this rebroadcast to ensure that only legitimate blocks are sent. A lengthy number of tasks have to be completed, including the following:

- Verifying the header hash meets the required complexity and block structures
- Each transaction needs to be confirmed, every block must be validated and the time stamp needs to be reviewed. Block sizes cannot be larger than expected.

Major contribution of this research works is mentioned below.

- The adoption of blockchain infrastructure has increased security in MANETs. This information serves as the foundation for the suggested study effort. The following is a list of the major contributions:
- To increase security and energy efficiency in MANET, a unique decentralized blockchain-aided authentication technique, or DBlock-Auth, is presented.
- The Similarity Score (Sim-Score)-based clustering technique is a suggested method that enables flexible clustering for network administration.
- Each node in the network is validated by the Blockchain-based PUF (BPUF) process of validation, as well as all clusters are picked with the best cluster head utilizing the TOPSIS technique to secure the process of clustering.
- The Multi-Model Trust-based Routing, or MuMoTR, method selects a secure and efficient energy path for data transfer.

## Background

Picone et al.[10] presented that the blockchain is a method that is presently getting a lot of interest and might be useful in Internet of Things (IoT) security issues. The objective of the special issue on 'blockchain privacy and security for the IoT' was to examine the innovative advancements, techniques, and difficulties linked to block chains, privacy, and security for the IoT that are revealed by both the most current studies and remaining attempts. This paper presented the recent assessment of blockchain technology and whether it might be used to control eHealth privacy. It was one of the initial attempts to provide a thorough analysis of the present techniques for evaluating blockchains and to isolate the associated difficulties and restrictions on their application. The researchers presented some essential metrics for evaluating blockchains. To point out the potential prospects of employing decentralized identity management techniques for upcoming health identification systems, the more recent content offers decentralized identity administration that uses blockchain. This work pointed out the secure fine-grained data transmitting schemes for the scenario of mobile cloud computing. The objective was to transfer a significant number of time-consuming tasks from handheld devices with limited resources to the cloud. This work presented the blockchain-based and distributed systems of data security and event management. This suggested Security Information and Event Monitoring (SIEM) depends on the technology of the blockchain to safely store and access the security events connected with the IoT sentinel, which is in control of protecting networks of connected and distributed devices. Because of their properties, this block chain ensures the traceability and non-repudiation of security event registries. This work presented a new technique of authentication to handle insiders on clouds over blockchain-based authentication techniques. This suggested strategy initializes the contributions as below; this suggested technique authenticates the two actors of outsiders and insiders, and authentications of the P2P were offered to the database users of the cloud through the technique of the blockchain. This suggested result was tested utilizing the system tool of scyther formal towards many attacks to estimate the effectiveness. This result demonstrated the system's significant effectiveness and success in preventing many threats from outsiders and insiders. The technology may also improve cloud infrastructure security by predicting potential attacks.

Lwin et al.[11], suggested blockchain-based trust management systems with the technique of lightweight consensus in the MANET. This suggested approach offers the distributed trusts parameter for the routing nodes in MANET, which is tamper-proofed through the blockchains. The blockchain approach was incorporated into MANETs through the Optimized Link State Routing (OLSR), which may be utilized as a model technology. In the OLSR, the majority of privacy issues, where each node performs the privacy action separately and repetitively, were solved by blockchain as a securely distributed and trusted framework. The routing nodes in the suggested design might additionally work together to protect themselves against network intruders through specified criteria.

Asif et al.[12] presented the physical unclonable functions and the technology aspects of blockchain. In order to address energy, latency, integration, scalability, and bandwidth needs for Internet-of- Energy infrastructure,

it specifies a developing blockchain model that combines security for hardware basics through Physical Unclonable Functions (PUFs). This hybrid strategy, referred to as PUF Chain hereafter, offers devices and information provenances that capture data origins, the creation of data history and extraction, and clone-proof identifications of devices and authentications, making it feasible to trace the origins and motivations of any potential cyber assault. Additionally, this method examines the crucial components of structure, improvement, and deployment, which may assist others in understanding how to seamlessly integrate with existing internet of things systems and improve dependability and resilience to cyberattacks.

Khalfaoui et al.[13] suggested distributed authentication for the Manets because of the lack of a centralized unit to register and authenticate nodes. Authentication of decentralized systems, depending on the fog computing technology and strategy of the blockchains, is suggested. This approach's estimation indicates that it meets a variety of security demands and effectively defends networks from attackers. This work presented the conventional methods for choosing relay nodes as vulnerable to the attacks of collusion, greater energy use, latency, and shorter network lifetimes. Mahapatra et al.[14] suggested the Quantum Atom Search Optimization coupled with Blockchain aided Data Transmission (QASO-BDT) system for the relay node selections with security-assisted transmissions of data to address these issues. The three stages of this strategy are transmission, registration, and clustering. The Capillary Gateway (CG) is used to first register all sensor nodes in the network of blockchain nodes during the node registration stage. Following the selection of a Cluster Head (CH), the nodes are clustered into multiple clusters using an improved multiple-view clustering approach. The multi-hop transmissions stage then aids in choosing the appropriate relay nodes for multi-hop transmissions utilizing QASO, and the based-on-blockchain technology transactions are completed to assure the security of the system.

Zenebech et al.[15] suggested a novel model of secure AODV known as blockchain-based authentication and verification approaches to security for the secure communications of the MANETs to identify the issues of secure routing. SHA1 and SHA5 cryptographic algorithms are employed by participants in communication based on block chain technology authentications and verifications to create a block of communications. For neighbor node incoming data to be authenticated and verified, all nodes in networks have to have access to the key's tables. The security process can remove a node from networks once communications can start since it is the attacker and add it to the denied lists. Employing the Network Simulator 2 (NS-2) with malicious node conditions, the effectiveness of the suggested technique was evaluated. That contrasted with a method of routing for symmetric key authentications. In addition to measuring the network's efficiency in terms of E2ED, packet delivery ratio, and throughput, security effectiveness was determined as regards detection rate, false positive rate, and false negative rate.

Grover et al.[16] presented that without depending on a centralized trusted authority, managing resources may be done more easily thanks to the decentralized and distributed computing infrastructure known as blockchain. Because it offers transparency, tamper resistance, and immutability, a system based on blockchain is practical in a virtual area network context. This study is intended to provide a thorough analysis of blockchain uses for virtual area network security. This work begins by introducing blockchain technology and Vehicular Adhoc NETwork (VANET) security. After that, considering technological challenges and research challenges, this work undertakes the reviews of the survey assessment on the previous result of security employing blockchains in the virtual area network. A comparative analysis of feature based methods is provided in Table 1.

## Proposed work

### Network model

The proposed networks are designed as combined networks that integrate a mobile ad-hoc network with decentralized blockchain networks. are the designations of the zones that construct mobile ad-hoc networks. Each zone Zi is subsequently divided into the total of l clusters.

The total number of nodes in the networks This node is naturally mobile and is allowed to transfer wherever it wants inside the networks. All nodes have various degrees of mobility. Before the data transmissions begin, the following presumptions are made:

| Aspect | DBlock-Auth (this paper) | Careem & Dutta (2020) | Lwin et al. (2020) |
|---|---|---|---|
| Core goal | End-to-end secure MANET: auth → clustering → trust-routed delivery with lightweight encryption | Reputation-based routing using blockchain to record node behavior and select reputed paths | Blockchain-based lightweight trust management embedded into OLSR |
| Authentication | BPUF (registration on chain + PUF C–R at auth) | No PUF; reputation transactions logged on chain | No PUF; focuses on trust computation and validation process design |
| Trust basis | MuMoTR: direct > indirect trust weighting for route selection. (Proposed Work/Trusted Route Selection.) | Reputation score per node from on-chain behavior | Distributed trust framework with lightweight consensus |
| Clustering/CH | Sim-Score (mobility, distance, node degree) + TOPSIS CH selection | Not CH-centric; route selection uses reputed nodes | Built around OLSR; not CH-centric |
| Data protection | Light HB encryption for confidentiality/integrity | Not the focus; reputation discourages misbehavior | Hardens control/data via blockchain trust; encryption not the main focus |
| Ledger/consensus | Distributed ledger (zone-organized network); consensus details abstracted in manuscript | Uses blockchain to validate routing actions & persist reputation | Proposes lightweight consensus tailored for MANET constraints |
| Testbed/metrics | NS-2; reports PDR, throughput, residual energy, security level (Table 3) | COMSNETS 2020 study; reports PDR gains vs. conventional routing (≈ + 12% noted in summaries) | Prototype/sim with OLSR integration; validation time/overhead reductions reported |

**Table 1**. Feature-level comparison of DBlock-Auth with recent blockchain-enabled MANET approaches.

- Nodes can be lightweight and moved through the networks.
- The total number of clusters in each of the fixed-number zones
- The total number of clusters in each zone ranges according to the node's movements.
- The number of malicious or attacking nodes and their quantities are present in the networks. The attacker might appear within the network or outside of it.

With the previously mentioned presumptions, the network is built, and Fig. 3 shows the design. Figure 4 depicts the flow chart.

## Block chain Based BPUF Authentication

Cluster creation with authorized nodes is the initial phase of the suggested task. This node is initially authenticated at this stage using a BPUF method. The network is protected from different attackers by the process of authentication. Nevertheless, inadequate methods of authentication fall short of the necessary degree of security. This method introduced a brand-new BPUF method in this research. The flow process is depicted in Fig. 5.

The stages that make up the BPUF function are as follows:

**Step 1: Registration**

Registration is the initial stage of the authentication procedure. The blockchain requires that all mobile nodes first register their identities. The following credentials are required for registration:

NodeID $(ID)-$ Every node has a distinct ID that has to be registered with the blockchain.

Password $(PW)-$ The password is given to each node at registration time.

PUF$-$ The distinct hardware-based functions known as a PUF are not impervious to malicious or attacking nodes.

$$N_i \rightarrow H[ID_i, PW_i, PUF_i]$$

Each of these passwords has been encoded and is kept in the blockchain.

**Step 2: Authentication**

The next stage is authentication after registration. It is carried out twice. This node submitted to encoded $ID$ and $PW$ in authentication as below,

$$N_i \rightarrow H[ID_i] \oplus H[PW_i]$$

If node $N_i'$ sID and $PW$ were compatible, the blockchain server would then request PUF. The PUF is the credentials which is depending on Challenge Response (C-R).As a result, the nodes with the appropriate credentials are asked to participate in $(\mathrm{C}-\mathrm{R})$, which reduces needless transmission. The server starts $\mathrm{C}(\mathrm{N_i})$

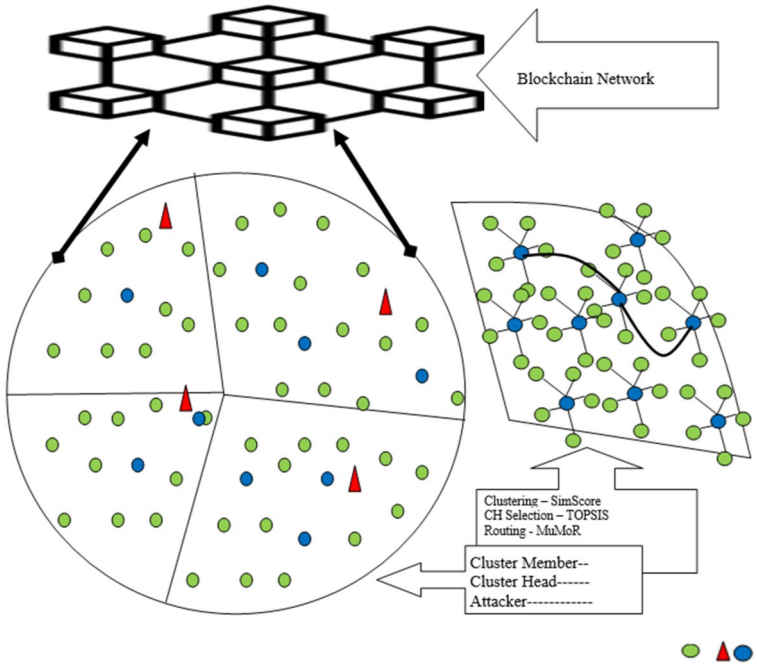


**Fig. 3**. D block-auth architecture.

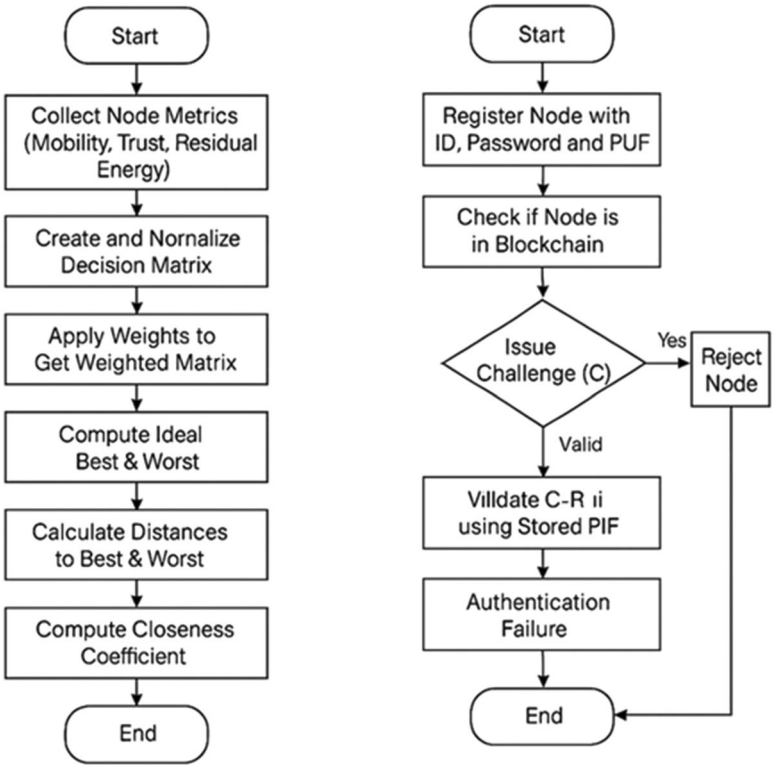


**Fig. 4**. Flowchart of TOPSIS-based cluster head (CH) selection process based on multicriteria method. b. Proposed BPUF-based node authentication process using blockchain and PUF.

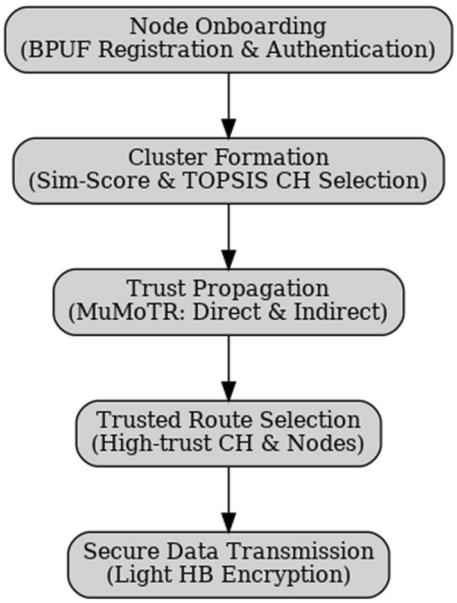


**Fig. 5**. System flow diagram of the proposed BPUF-based secure MANET framework, illustrating node onboarding, cluster formation, trust propagation, route selection, and secure data transmission.

for each and every legitimate node. The right R should be sent by the node in response to the challenges, and the blockchain will confirm it.

1. start
2. for all $N_i \in N$
3. Initiate *Registration*

Create new blocks

$$\text{Reg} \rightarrow (\text{ID}, \text{PW}, \text{PUF})$$

4. end for
5. Node $N_i \rightarrow Authentication$
6. Submit $H[ID_i] \oplus H[PW_i]$
7. If $ID_i$ && $PW$
8. == valid
9. start challenge ($C(N_i)$
10. If $R(N_i) \rightarrow C(N_i)$
11. Node is valid
12. else
13. else
14. node is malicious
15. end if
16. end process

Algorithm: BPUF-based authentication.

The preceding technique is followed throughout the authentication process. Involving the network in the authentication procedure effectively shields it from different attackers.

### CH selection and cluster formation

The next stage is to create clusters inside zones after the nodes have been verified by the BPUF approach. The Sim-score is calculated for the nodes that will form clusters in order to build clusters. The Sim-score is calculated using the following three key metrics:

1.1. Mobility (m): It refers to the movement speed of nodes inside the network. In order to calculate this factor,

$$m_F = \pm[m_i - m_j]$$

Distance (d): The distance within the 2 nodes is calculated as an expression of Euclidean distance in the manner presented below.

$$d_F = \sqrt{\sum_{i=1}^{k} (y_i - x_i)^2}$$

2. Node degree (ND): The numbers of shared nodes within the node $n_i$ and $n_j$ is known as the node degree.

The Sim-score within $N_i$ and $N_j$ is calculated as follows by integrating each of the 3 metrics:

$$\text{SimScore } (N_i, N_j) = \sum m_F, d_F, \text{ ND}$$

Both nodes form clusters whether node and Sim-score are high. Depending on the total number of nodes found in every zone, clusters are generated.

The following steps are to select the best CH for all the clusters created inside zones. The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) technique, a multiple-criteria decision- making method, is suggested for choosing the best CH. This is beneficial to choose the best course of action (choosing the best CH) after considering several factors. In this case, the accessible solutions are viewed as possibilities, and the choice of metrics is viewed as criteria. The parameters for CH selections include mobility, trust value, and residual energy level for the cluster's nodes. The step-by-step process for choosing the best CH is provided as follows:

STEP 1:

Create evaluation matrix with $u$ choices and $v$ criteria as $[\mathrm{X_{uv}}]$ .

STEP 2:

The evaluation matrix is then normalized to create the matrix,

$$\mathrm{R} = (\mathrm{r_{uv}})\alpha\beta$$

STEP 3:

The weighted normalized decision matrix is further generated in the manner described below.

$$r_{uv} = \frac{X_{uv}}{\sum_{k=1}^{\alpha} {X_{k\alpha}}^2}$$

$$t_{uv} = r_{uv}.w_v$$

where, $w_v = \frac{w_j}{w_k}$

STEP 4:

After that, the worst $(A_w)$ and best $(\mathrm{A_b})$ alternatives:

$$A_w = \{\langle max(t_{uv}|u = 1,2,\ldots,\alpha|v \epsilon J\ -\rangle, \langle min(t_{uv}|u = 1,2,\ldots,\alpha)\rangle\}$$

STEP 5:

$$A_b = \{\langle min(t_{uv}|u = 1,2,\ldots,\alpha|v \epsilon J\ -\rangle, \langle max(t_{uv}|u = 1,2,\ldots,\alpha)\rangle\}$$

The weighted normalized decision matrix is further generated in the manner described below.

$$d_{uw} = \sqrt{\sum_{v=1}^{n}(t_{uv} - t_{wj})^2}$$

Parallel to the way distances within alternatives and best alternatives $(A_b)$ are calculated,

$$d_{ub} = \sqrt{\sum_{v=1}^{n}(t_{uv} - t_{bj})^2}$$

STEP 6:

The following equation is used to calculate the similarity to the worst conditions:

$$s_{uw} = \frac{d_{uw}}{d_{uw} + d_{ub}}$$

If $s_{uw} = 1$ if and only if the alternatives are in the best conditions

if $s_{uw} = 0$, if and only if the alternatives are in worst solutions

STEP 7:

Lastly, alternatives are ranked regarding to the $s_{uw}$ where $\mathrm{u} = 1,2,3,\ldots,\alpha$

Algorithm: CH selections by TOPSIS.

The best option that comes in first place after ranking is chosen as the best CH in all clusters.

### Trusted route selection

The best route choice for data transfer is crucial. In this work, this method introduced the MuMoR strategy, which completely hinges on trust values. The goal of MuMoR is to select the most reliable route out of those that are offered. The multi-modal trust computation procedure is taken into consideration for this purpose. In MuMoTR, the final trust score is computed as a weighted aggregation of direct and indirect trust. Direct trust, derived from firsthand interactions such as forwarding reliability, energy, and mobility, is assigned higher weight, while indirect trust from neighbor recommendations provides supplementary evidence. This balance prioritizes reliable firsthand observations while still enabling fair evaluation of nodes with limited direct history. Table 2 shows the MuMoR strategy of the proposed system.

Table 1 presents the multi-modal trust values. The cumulative trust is calculated using the numbers below:

$$\mathrm{cTV} = \frac{\sum \mathrm{DT},\ \mathrm{IT},\ \mathrm{RV}}{3}$$

In addition to trust value, the suggested MuMoR technique considers other significant characteristics. According to the MuMoR technique, each route's weight value is determined as below:

$$\mathrm{W(R_j)} = \left\{ \left( \sum_{\mathrm{i=1}}^{\mathrm{L}} \mathrm{cTV_i} \right) \left( \sum_{\mathrm{i=1}}^{\mathrm{L}} \mathrm{RE_i} \right) \right\}$$

The data transfer path with the greatest value is chosen. Improvements in security and reduced energy use are achieved by taking trust value and residual energy into account.

### Secure data transmission

The data is transferred using the best path. This method introduced the Light weight –Hummingbird (HB) procedure, initialized by the source nodes, to protect the data. The Hummingbird-2 encryption's 128-bit internal state R and 128-bit secret key SK are initialized using the 64-bit initialization vectors IV. This employs 16-bit word functions to operate. In order to safeguard the data, additional modulo procedures and exclusive OR procedures are used. The following are the steps for encrypting the data packet, or plain text.

The best route is then used for transmitting this ciphertext $CT_i$.

1. start
2. initialize available routes
3. for each $(R_i)$
4. compute each 3 metrics
5. select optimal routes $R_{Best}$
6. end for
7. Initialize SK, IV, t
8. encrypt data $CT_i$
9. Transmit $CT_i \rightarrow Destination$
10. end

Algorithm: Secure data transmission.

| TRUST | DEFINITION | COMPUTATION |
|---|---|---|
| Direct Trust (DT) | This trust value is calculated depending on the nodes' regular conduct by self<br>For example, $N_i$ calculates $N_j$ trust value depending on the communications transmitted among individuals | $DT = \begin{cases} +1, If transmission is normal \\ -1, If transmission is malicious \end{cases}$ |
| Indirect Trust (IT) | This trust value is determined by aggregating trust values from different nodes<br>For example, if $N_i$ needs to calculate IT, it will gather trust values from Lsurrounding nodes | $IT_j = \frac{\sum DT_j}{L}$ |
| Reputation Value (RV) | This is calculated as the node's harmful conduct when transferring data<br>This value concentrates on whether the given node modifies any data during transfer | $RV = \begin{cases} +1, if data is not modified \\ -1, if data is modified \end{cases}$ |

**Table 2**. Multi-Modal Trust.

| Parameter | | Value |
|---|---|---|
| Network Area | | 1000*1000 m |
| Number of Zones | | 10 |
| Number of Nodes | | 500 |
| Maximum Clusters | | 15 |
| Key Size | | 128-nbit |
| Initial Energy of Nodes | | 750 J |
| Channel Bandwidth | | 25 MHz |
| Number of Packets | | 1000 |
| Packet Size | | 32 KB |
| Number of Retransmissions | | 5 |
| Mobility Range | $\mu_L$ | 10 m/s |
| | $\mu_U$ | 40 m/s |
| Maximum Trust Value | | 100 |
| Maximum Reputation Value | | 100 |
| $\sigma$ | | 0.001 |
| Number of Attackers | | 5 |
| Simulation Time | | 100 s |

**Table 3**. Simulation Specifications.

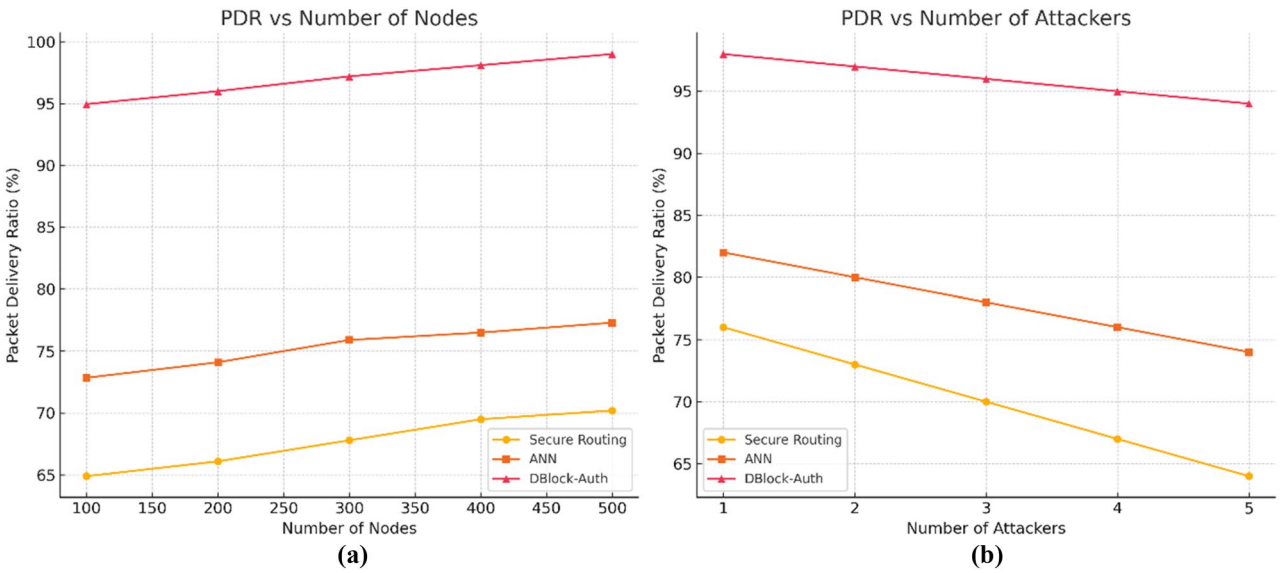


**Fig. 6**. Packet Delivery Ratio (PDR) comparison under two scenarios: (**a**) varying number of nodes and (**b**) increasing number of attacker nodes.

## Experimental analysis

The recommended MANET networks are built using simulation tools like Network Simulator 3 (NS-3.25). The network is set up using the programming languages C++and TCL, utilizing the network simulator NS-3.25's events-based setup. Actually, NS-3.25 supports a wide variety of wireless network protocols and allows for the addition of blockchain. Consequently, this approach is used to simulate various scenarios. Table 3 displays the crucial simulation variables.

The previously mentioned configuration results in highly desirable numbers.

## Comparative analysis

Based on the energy use, level of Security, Latency, Packet Delivery Ratio (PDR) and Throughput, this method compared the suggested and current tasks like Artificial Neural Network (ANN)- based routing, secure routing, and Elliptic Curve Cryptography (ECC) encryption approaches.

## PDR analysis

The ratio of all packets transmitted by source nodes to all packets recovered at the destination is known as the packet delivery ratio.

Figure 6 demonstrates that the suggested work's PDR is approximately 99%, which is remarkably greater than the PDR of the presently executed tasks. For instance, in 6.1, as the total number of nodes rises, the PDR continuously rises. As the total number of nodes increases, there's a greater likelihood that the optimal paths will be selected. The information is therefore sent in a reliable and efficient manner. As the total number of attackers rises, the PDR declines on the opposing side. Routing data is altered as a result of packet losses brought on by more persistent attacker activity. However, in both instances, the suggested block-sec technique generates superior PDR. The current analysis shows that cluster-based routing aids in achieving optimal routes, despite the advised security safeguards.

## Energy consumption analysis

The vital performance metric known as residual energy depicts the energy level at which each network node is currently operating. The Residual Energy (RE) is calculated as follows for $i^{th}$ node,

$$RE_i = \frac{\sum_{i=1}^{n} E_i(Ini) - E_i(Cur)}{n}$$

Thereby, $E_i(Ini)$ is primary level of energy and $E_i(Cur)$ is present level of energy of the $i^{th}$ nodes.

Figure 7 compares the projected and current works' energy consumption. As the total number of attackers on networks rises, it also increases the consumption of energy. Attackers are attempting to deplete the node's reserves of energy. When the nodes' energy level is exhausted after a certain amount of time, they will finally die. To avoid this scenario, the entire network must be protected against attacks.

## Network lifetime analysis

Figure 8 includes a time scale and a representation of the number of active nodes. Lesser nodes remain operational as time passes. With this strategy, a large number of nodes are kept active. The suggested Block-Sec technology decreases node energy usage while simultaneously defending networks from attackers by creating dynamic clusters and choosing the best routes. In terms of preserving the right levels of energy, the investigation finds that the suggested approach is appropriate for the dynamic cellular network.

## Throughput analysis

The entire amount of data that is transmitted effectively in a particular amount of time to the final destinations is known as throughput. Figure 9 compares the throughput attained by the proposed and current activities. Compared to other attributes, the throughput measurement depends on both a network's level of security and the data communication method. In this regard, both security concerns and inefficient transmission of data have an influence on throughput. From scenario 6.2, it is clear that the throughput decreases as the total number of attackers rises. This is due to the fact that data supplied within a specific time period is frequently attacked by attacker nodes, preventing the data from reaching its final location within the set time limits. Throughput levels up to 8 Mbps are attained by the suggested work, which routinely outperforms the current task by these two factors. The ideal network administration, robust security plan, and routing approach in the suggested work enable the networks to operate at their maximum throughput. This method may thus conclude that the proposed technique reduces data loss.

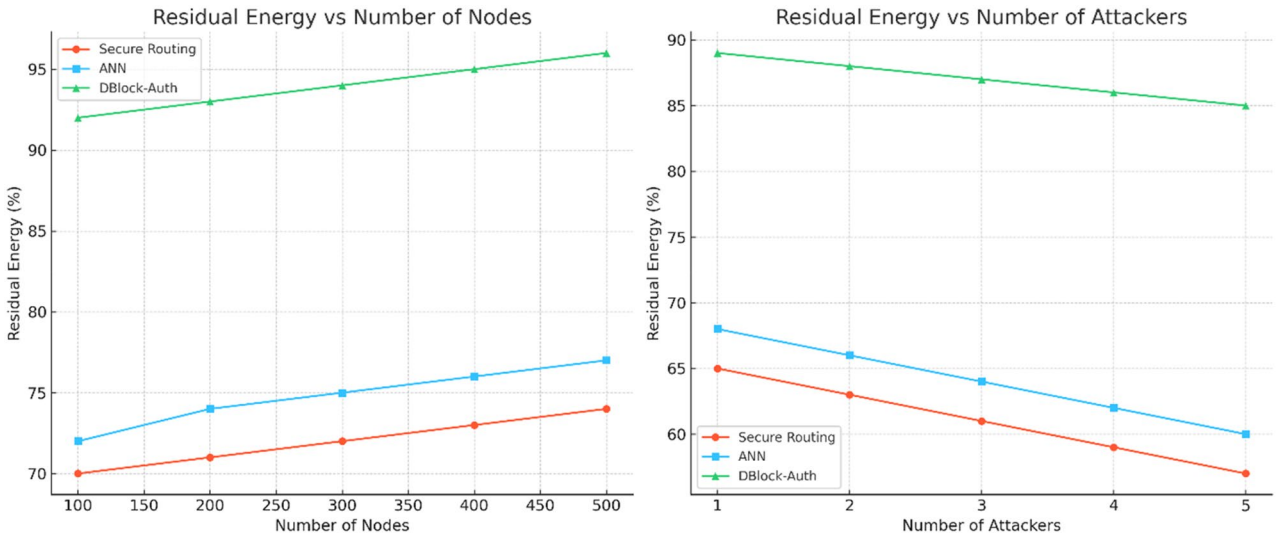


**Fig. 7**. Comparisons on energy level.

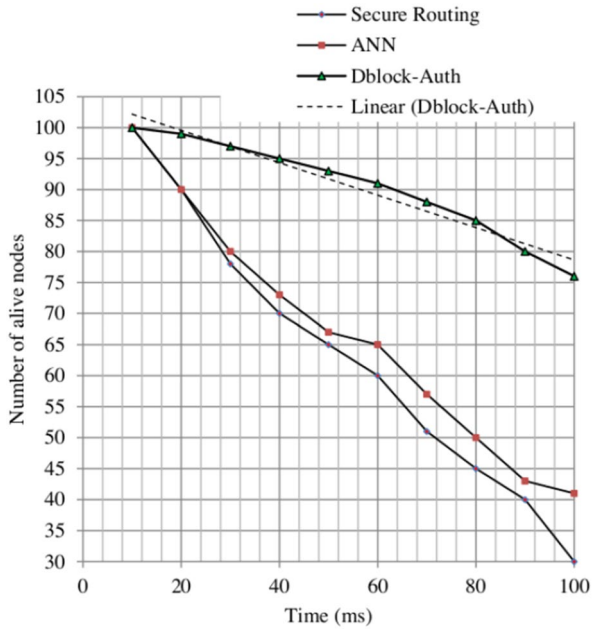


**Fig. 8**. Analysis on the number of alive nodes.

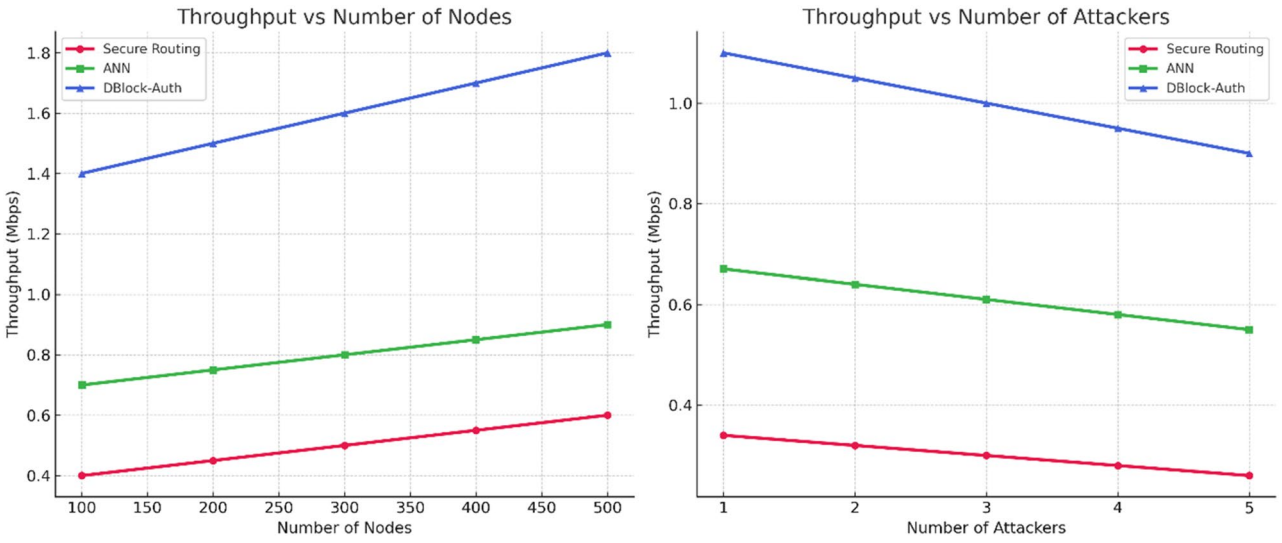


**Fig. 9**. Comparisons on Throughput.

## Encryption and decryption time analysis

This efficiency statistic examines the amount of time an encryption method takes. Thus, both the time required for encryption and decryption are used to evaluate effectiveness.

Figure 10 and Fig. 11 analyze the time requirements for encryption and decryption, respectively. These comparisons illustrate that the suggested technique of Light HB tasks is greater than the previous technique of ECC and are utilized in the technology of blockchain. Thus, transmission delays can be reduced.

## Security level analysis

The overall number of packets in the networks that were either modified or changed by attackers is counted, and this quantity is used to define the level of security as mentioned in Fig. 12. This demonstrates the presence of the attackers by demonstrating the number of information packets that have changed since several attackers remain in networks.

Depending on the study, the recommended work achieves a degree of security of 98%, which is much greater than the work already in place. The following factors raise the security level of the proposed work[1]: Significant amounts of security are provided through the utilization of the technology of blockchain and the

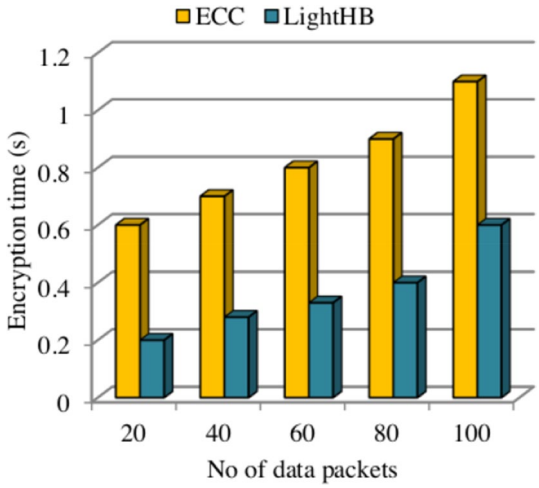


**Fig. 10**. Encryption time comparisons.

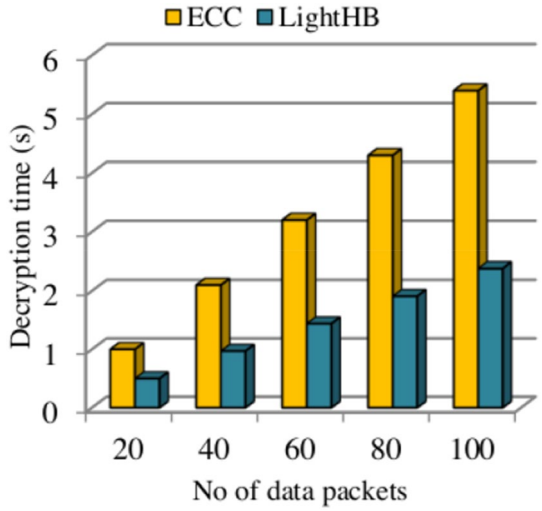


**Fig. 11**. Decryption time comparisons.

successful implementation of authentication processes by the network, preventing unauthorized nodes from entering. Therefore, malevolent, and unauthorized nodes are absent from networks[2]. To ensure there are no potentially harmful unprotected nodes, the trust value is considered while selecting the optimum path[3]. Light HB encryption shields data from eavesdropping and modification by adversary nodes.

While Light HB significantly improves confidentiality and resistance to packet tampering, it introduces a modest encryption delay due to additional key exchange and computation. This overhead is minor compared to conventional schemes and remains acceptable given the enhanced security achieved.

The proposed method, DBlock-Auth, consistently outperforms Secure Routing and ANN regarding security levels across varying numbers of nodes, achieving significantly higher security levels of 92.95% to 97.9% compared to the existing method in security level scenario 1.

The proposed method, DBlock-Auth, consistently outperforms Secure Routing and ANN in all scenarios, achieving significantly higher security levels. In Security Level Scenario 2, DBlock-Auth achieves an impressive security level of 99.3%, demonstrating its effectiveness in ensuring secure routing and authentication in networks.

The findings are presented in Table 4. Through the previously mentioned methods, the proposed work enhances the security of networks. Additionally, a recent study focused either on identifying rogue nodes or the security of data. Additionally, the network's core nodes can be compromised, bringing the security level down to 30%.

## Summary

The objective of this research is to provide advanced security in mobile ad hoc network architectures with minimal power consumption. In order to do this, the study content develops a special distributed Blockchain-Assisted Authentication (BAA) method for MANET. This study develops an improved distributed BAA method

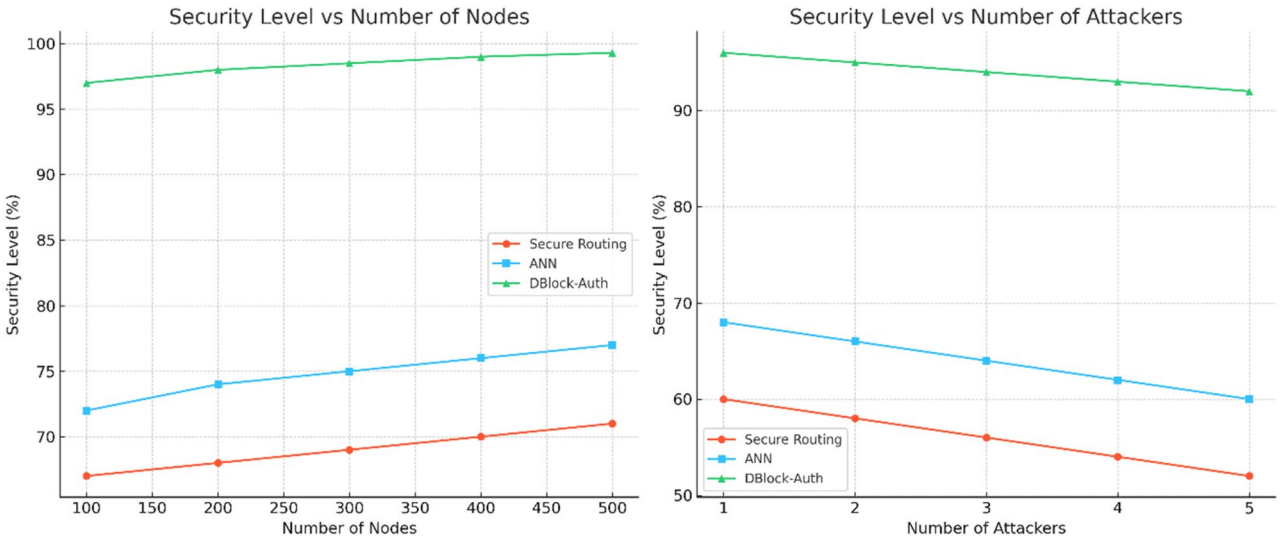


**Fig. 12**. Comparisons on Security Level.

| Performance Metric | | Secure Routing | ANN | Dblock-Auth |
|---|---|---|---|---|
| **PDR (%)** | Based on number of nodes | 64.9 | 72.85 | 94.95 |
| | Based on number of attackers | 76 | 82 | 98 |
| **Residual Energy (%)** | Based on number of nodes | 70 | 72 | 92 |
| | Based on number of attackers | 65 | 68 | 89 |
| **Throughput (Mbps)** | Based on number of nodes | 0.4 | 0.7 | 1.4 |
| | Based on number of attackers | 0.34 | 0.67 | 1.1 |
| **Security Level (%)** | Based on number of nodes | 67 | 72 | 97 |
| | Based on number of attackers | 60 | 68 | 96 |

**Table 4**. Summarization of achieved results.

for MANET to achieve this. The whole network's zones are then divided into several clusters depending on comparable ratings. The BPUF mechanism, which demonstrates every node's PUF, is used to verify all of the nodes preceding it. The optimal CH is selected from within the various clusters produced by each of the acceptable nodes using the TOPSIS multiple-criteria technique. The optimum route for the transmission of data within all clusters is chosen through the MuMoT methodology. In the end, the security of data is ensured by the Light-HB method. The suggested work delivers advanced security with little energy usage, according to this investigation. This study makes a valuable contribution to MANET security by combining blockchain, PUF-based authentication, trust-driven routing, and lightweight encryption with rigorous analysis and promising results. Future extensions may address scalability under large-scale deployments, stability under extreme mobility, and resilience against advanced adversarial scenarios to further strengthen the framework.

## Data availability

Data's supporting this study is included within this published article.

Received: 11 April 2025; Accepted: 7 October 2025
Published online: 12 November 2025

## References

1. D. Arya, P. Mehra, P. Jain and A. Bhatia. "A Study on MANET: Along with recent trends, applications, types, protocols, goals, challenges." *2023 1st International Conference on Intelligent Computing and Research Trends (ICRT)*, Roorkee, India. 1–5, https://doi.org/10.1109/ICRT57042.2023.10146716 (2023).

2. J. Swain, B. K. Pattanayak and B. Pati. "Study and analysis of routing issues in MANET." *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, India. 506–509, https://doi.org/10.1109/ICICCT.2017.7975251 (2017).
3. R. Sheikh, Mahakal Singh Chande and D. K. Mishra. "Security issues in MANET: A review." *2010 Seventh International Conference on Wireless and Optical Communications Networks - (WOCN)*, Colombo, Sri Lanka. 1–4, https://doi.org/10.1109/WOCN.2010.5587317 (2010).
4. N. Kshatriya, K. Mallawat and A. S. Biswas. "Security in MANET using detection engine." *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, Pune, India. 128–132, https://doi.org/10.1109/CAST.2016.7914953 (2016).
5. Tu, J., Tian, D. & Wang, Y. An active-routing authentication scheme in MANET. *IEEE Access* **9**, 34276–34286. https://doi.org/10.1109/ACCESS.2021.3054891 (2021).
6. S. S. Zalte and V. R. Ghorpade. "Intrusion Detection System for MANET." *2018 3rd International Conference for Convergence in Technology (I2CT)*, Pune, India. 1–4, https://doi.org/10.1109/I2CT.2018.8529441 (2018).
7. M. A. A. Careem and A. Dutta. "Reputation based Routing in MANET using Blockchain." *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Bengaluru, India. 1–6, https://doi.org/10.1109/COMSNETS48256.2020.9027450 (2020).
8. Z. Li, X. Yin, P. Yao and J. Huang. "Implementation of P2P computing in design of MANET routing protocol." *First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06)*, Hangzhou, China. 594–602, https://doi.org/10.1109/IMSCCS.2006.233 (2006).
9. G. Kaur and P. Thakur. "Routing protocols in MANET: An overview." *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Kannur, India. 935–941, https://doi.org/10.1109/ICICICT46008.2019.8993294 (2019).
10. Picone, M., Cirani, S. & Veltri, L. Blockchain security and privacy for the Internet of Things'. *Sensors* **21**(3), 892 (2021).
11. Lwin, M. T. & YimKo, J. Y. B. Blockchain-based lightweight trust management in mobile ad-hoc networks. *Sensors* **20**(3), 698 (2020).
12. Asif, R., Ghanem, K. & Irvine, J. Proof-of-puf enabled blockchain: Concurrent data and device security for internet-of-energy'. *Sensors* **21**(1), 28 (2020).
13. Khalfaoui, H., Farchane, A. & Saf, S. Decentralized authentication mechanism for mobile Ad hoc Networks'. *Infocommun. J.* **14**(3), 28–34 (2022).
14. Mahapatra, S. N., Singh, B. K. & Kumar, V. A secure multi-hop relay node selection scheme-based data transmission in wireless ad-hoc network via block chain'. *Multimed. Tools Appl.* **81**(13), 18343–18373 (2022).
15. Zenebech, B. Blockchain Cryptographic-based Authentication and Verification for Secure Communication in Mobile Ad-hoc Network (MANET) (Doctoral dissertation). (2021).
16. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review'. *Vehicular Commun.* **34**, 100458 (2022).


## Author contributions

All authors (V R. Sugumaran, E. Dinesh, R. Ramya, Elangovan Muniyandy) contributed to the study, conception, and design. All authors commented on the manuscript. All authors read and approved of the final manuscript.

## Declaration

## Competing interests

The authors declare no competing interests.

## Additional information

**Correspondence** and requests for materials should be addressed to V.S.

**Reprints and permissions information** is available at www.nature.com/reprints.

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.