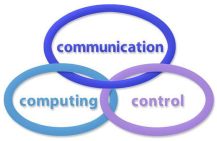
INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 18, Issue: 2, Month: August, Year: 2023
Article Number: 5144, https://doi.org/10.15837/ijccc.2023.2.5144



CCC Publications

Blockchain-assisted Secure Routing Protocol for Cluster-based Mobile-ad Hoc Networks

N. Ilakkiya, A. Rajaram

N. Ilakkiya
Department of Masters in Computer Application
E.G.S Pillay Engineering College
Nagapattinam, Tamilnadu, 611002, India
*Corresponding Author: Email: illalliyaphd@gmail.com

A. Rajaram
Department of Electronics and Communication Engineering
E.G.S Pillay Engineering College
Nagapattinam, Tamilnadu, 611002, India
drrajaram@egspec.org

Abstract

MANETs aredecentralized network that involves mobile nodes. As the overall network is mobile and has no centralization, network management, routing, and security become very challenging. Though many works have been presented, still there is a lack in organizing the network due to unauthorized access, centralized security schemes, and the dynamic nature of the nodes. This paper proposed a novel Blockchain-assisted Secure Routing (Block-Sec) protocol for MANETs. All mobile nodes are authenticated by Distributed One-Time Passcode (DOT) based authorization scheme. All authorized nodes are segregated into multiple clusters based on Weight based Dynamic Clustering (WDC) algorithm in which multiple metrics are considered in clustering and re-clustering processes. After cluster formation, each cluster is elected with optimal Cluster Head (CH) by Strawberry Optimization (SBO) algorithm with a new objective function. After cluster formation, the optimal route is selected by Fast Neural Net-assisted Fuzzy (FNNF) algorithm by combining multiple variables. Data transmission is secured by Efficient Elliptic Curve (E2C2) algorithm. With the combined algorithms, the proposed approach obtainedimproved efficiency in packet delivery ratio (PDR), throughput, time analysis, and security level.
Keywords: Blockchain, Distributed Security, Mobile Nodes, Dynamic Clustering, MANETs.

1 Introduction

With the advancements in wireless standards such as WiFi, Radio networks,etc, there are many applications have been developed. However, the overall network fully depends upon centralized base stations (BSs) or routers [1]. MANETs resolve the problem of centralization by distributing the data transmission throughout the network [2]-[4]. MANETs ensure ease of network deployment and data transmission. MANET's general architecture is given in figure.1. As shown in the figure, MANET has no central BS or routers. It is defined as the collection of wireless movable nodes that need no infrastructure for communication. The nodes presented in the network are generally mobile.

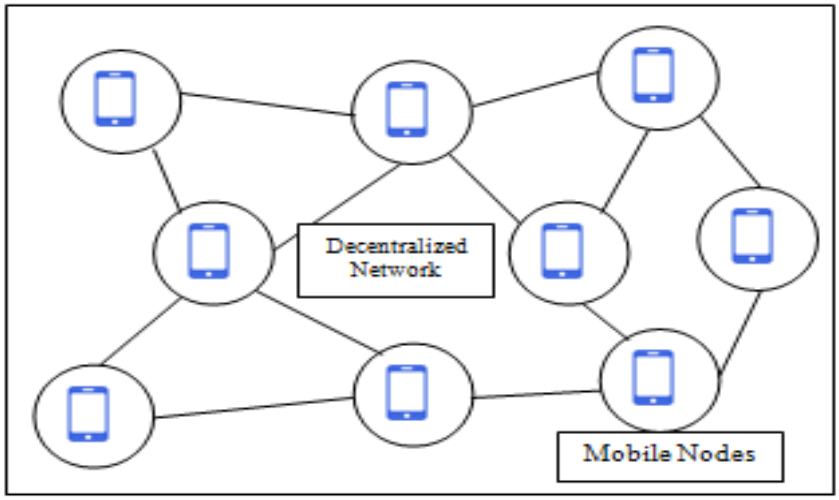


Figure 1: MANET architecture

The mobile nodes are allowed to move around the network limit [5], [6]. Each mobile node is capable to act as a transmitter, receiver as well as router. Due to its wide usage, MANET is emerging in many growing Internet of Things (IoT) applications such as environmental monitoring, pollution monitoring, etc [7]. Due to the lack of infrastructure, routing becomes challenging in MANET [8]. Mainly, routing depends upon on-demand routing and distance vector-based protocols. DSR and AODV routing protocols are the two major on-demand protocols [9]. Both protocols initiate route discovery only if needed for data transmission. However, the existing MANET protocols fail to achieve the following efficacy,

- Unable to choose the best route
- No evaluation is considered in route selection
- High possibility for link breakages
- Unable to ensure prompt data delivery
- Increases the number of retransmission
- Route breakages due to mobility

To resolve the above issues, routing is performed by considering network dynamics [10]. That is many algorithms use mobility as the major routing metric. However, it is proved that using combined metrics for route selection improves the efficiency of data transmission [11]. Generally, routing and network organization are interrelated. Routing will become simple and effective when the network is organized properly. For proper network management, MANET is clustered into multiple groups [12]. Cluster formation splits the network into multiple groups which makes data transmission easy. For cluster formation, k-nearest neighbor (KNN), and k-means algorithms have been utilized [13]. However, these conventional algorithms only consider the distance metric which is not effective. The combined cluster-based routing approaches assist in optimal data transmission [14]. On the other hand, security is the major concern in MANETs [15]. Because the network is probably deployed in the open and remote areas thus it increases the chances of tampering, data modification, and theft [16].

Network Layer	**Attacks/Issues**
Physical	• Jamming • Tampering • Denial of Service (DoS)
Link	• Eavesdropping, Overhearing, • Man-In-The-Middle
Network	• Routing Attacks such as Blackhole, • sinkhole, • wormhole
Transport	• Unauthorized access, • IP spoofing
Application	• Malicious codes, • viruses, • application thefts

In table.1, the major security issues existing in MANET are summarizedconcerning the layers [17]. As the network has no infrastructure, there is no control over the network nodes. Many research works have proposed security approaches such as authentication [18], encryption [19], and so on. However, security provisioning is

still challenging due to,
- Network mobility
- Mobile attackers
- Strength of attackers
- Central server-based authentication

On the whole, data transmission and security provisioning are two major aspects of MANET networks.

1.1 Blockchain Network

Blockchain is a technology that allows for the transparent, secure, and decentralized storage and transmission of information [20], [21]. It serves as a sizable archive that preserves a record of all user interactions ever since the blockchain was founded. The distributed design of blockchain, which is not hosted by a single server but rather by a small group of users, is a fantastic feature. Components of the blockchain contain security measures to safeguard the system and do not need an intermediary to verify the chain's authenticity or the accuracy of the data. Blockchains are shared, decentralized, and fault-tolerant databases that are available to everyone on the network and are not under the jurisdiction of any one entity. The technology is made to function against enemies in high-stakes circumstances. Blockchains are open, distributed, and fault-tolerant databases that anybody on the network may use; they are not under the jurisdiction of any one entity. The technology is built to function in dangerous scenarios against foes. In figure.2, integration of Blockchain and MANET is depicted [22], [23].

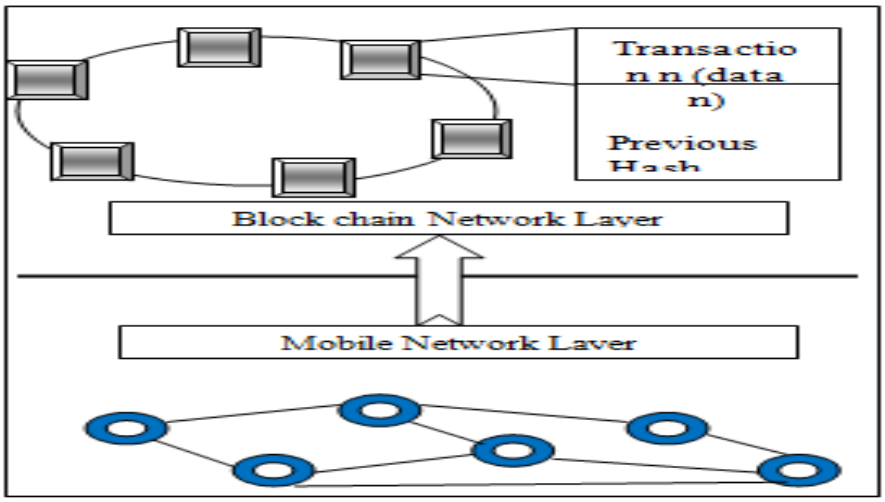


Figure 2. Blockchain and MANET integration

Each member of the network stores an identical copy of the blockchain and is in an essentially equal position. Blockchain is employed in various application scenarios and is regarded as one of the crucial strategies to speed up global growth due to its high level of security and dependability. Huge research works had been carried out for multimedia wireless networks in terms of routing, congestion avoidance, security features, packet loss and reducing delay during transmission, etc. Some of them are discussed here to relate the proficiency of our proposed work.

1.2 Research Challenges

Research Challenges existing in MANET are,

Dynamic Network Topology

Because of the dynamic network structure, nodes may migrate at any moment and in any direction. This leads to link breakages during routing

Energy Consumption

MANET involves mainly resource-constrained devices. Frequent route discovery and selection lead to high energy consumption.

Security Breaches

The involvement of the central security server increases the single node problem and is unable to provide a security level.

1.3 Research Contributions

To resolve the research problems, this paper summarizes the following research contributions,

- A novel Blockchain-assisted Secure Routing (Block-Sec) protocol is presented for MANETs
- All mobile nodes are authenticated by Distributed One-Time Passcode (DOT) based authentication scheme which uses blockchain for node validation
- The network is formatted with Weight based Dynamic Clustering (WDC) algorithm with Strawberry Optimization (SBO) algorithm-based CH selection process
- For optimal route selection, Fast Neural Net-assisted Fuzzy (FNNF) algorithm is introduced with multiple metrics
- Data transmission security is ensured by Efficient Elliptic Curve (E2C2) algorithm.

1.4 Paper Organization

The remaining paper are arranged as follows: section II provides a literature survey on existing works held on MANET secure routing. In section III, the major problem is stated which is resolved by the proposed approach. In section IV, the proposed approach is discussed. Section V evaluates the overall performance through extensive simulation observations. In section, VI the contributions are concluded with future research directions.

2 Related works

This research uses the well-known PSO (i.e., particle swarm optimization) approach to solve the problem of node mobility, and an adaptive k-nearest neighbor cluster algorithm is also developed [24]. To help with cluster formation, a multi-objective fitness function of PSO is considered. General testing in a simulated networked environment shows that the recommended method works. The complexity of MANET, where optimum energy is one of the key elements, was increased by mobile nodes migrating at random area of interest. It is far more difficult to maintain long battery life while simultaneously allowing for frequent changes in the architecture of mobile nodes.

An effective parallel computing method that manages topological structures well is the honeycomb-based paradigm [25]. Additionally, the most important objective of MANET is to choose the best routes while taking energy efficiency into account. To do this, this study introduces the IEEHR paradigm for MANET. The model reduces the broadcasting range while performing pathfinding by combining Honeycomb-based area coverage with LAR. Since mobile nodes have limited energy, efficient energy use is also necessary for MANET in addition to good routing. A network's performance and durability will both improve by how efficiently energy is spent in the network. Here, more energy is saved when the mobile nodes are asleep, which is further used up during the efficient routing process.

The trust of nodesin direct and indirect pathways are principally evaluated in this research [26], and the secure multipath is chosen while also identifying and isolating the vulnerable nodes. To protect the data packets from assaults of data transmission, the DPs are then encrypted using the SH2E method. In identifying the finest way out of the multipath chosen, the LF-SSO algorithm is then used. By determining a path trust-based path, residual energy of the node, and the path's distance, this approach increases the network lifespan. Then, using the found optimum path, the encrypted DPs are sent from the sender to taget, and lastly, relayed to the base station.[27-31]

Because of the constant node migration and the limited resources available, security management is a severe challenge [32-37]. Rekeying is only done for the so-called clusters of subnetworks to avoid having to repeatedly renew the group key for the entire wide network. This research proposes an integrated strategy of the HDGK management and FTBC to deal with this problem. The FTBC uses fuzzy logic principles to separate misbehaving nodes from genuine data transfer and classify trusted and untrusted nodes. No one methodis used for all application types, of simple clustering and improved weighted distributed clusteringare proposed to meet various demands.

Although multi-hop routing is essential in MANET, it might present difficult problems during communication including a lack of data privacy. ECC is combined with the Bee clustering strategy to offer a secure and resource-efficient data transport system [38]. Data dependability is still questionable because of attacks like data dumping attacks and black hole attacks even if it guarantees data. The neighbour routers in these situations employ the overhearing approach, and the packet forwarding statistics are calculated using the ratio of received to forwarded packets. If the network's packet forwarding ratio is low, an attack can be identified and a trustworthy another channel can be found for information transfer. The suggested work involves the SC-AODV integration, ECC, and a further overhearing mechanism into the Bee clustering strategy, which overall assures data secrecy, data dependability, and energy efficiency.

To improve PDR and network lifetime, a new routing protocol for MANETs was proposed in Hybrid Optimization-Based MPR-DC-Based MANET. This protocol uses a hybrid optimization technique that combines ACO and PSO [39]. A multipath-based routing algorithm for air pollution monitoring in MANETs was presented in [40]. This algorithm considers the nodes' available energy and the links' quality to choose the best routes and enhance network performance. [41] to control the broadcasting of many packets and guarantee the stability of all mobile nodes in a MANET, the proposed TCSSR algorithm makes use of timer count scheduling and spectator routing. To decrease packet loss and lengthen network lifespan, clustering, and stifle limitation methods are also utilized. [42] to extend the lifespan of inexpensive and compact sensor nodes in WSNs, the SICRA is presented. To save energy and balance the network load, SICRA calculates the ideal routing route by examining the transmission coverage, connection link, and other criteria.NMRouting is a neural controller based on perceptron and an MCDM controller that determines the optimum pathways for sending data packets in a neural-MCDM-based routing protocol that has been suggested for MANETs. To increase network dependability, three different queue types are also used [43]. With the use of fuzzy theory, MCDM, and an RGB model, the FSB-System is a detection system that is presented for estimating the likelihood of fire, asphyxia, and burns. Fuzzy controllers are utilized to calculate probability while temperature, smoke, and light sensors are employed to make judgments under various scenarios. Clusters of sensor nodes are set up, and data is sent from non-cluster heads to cluster heads [44].
The drawbacks of existing techniques including the complexity of MANET, where optimum energy is one of the key elements, are increased mobile node's random movement within a region of interest. It is more difficult to maintain long battery life while allowing for frequent changes in the architecture of mobile nodes. The IEEHR paradigm reduces the broadcasting range while performing pathfinding by combining Honeycomb-based area coverage with LAR, which can limit the scope of the network. While the proposed DXOR-RC6 with FE technique ensures data security and integrity in the E2-SR system, the security level of the other approaches is not explicitly mentioned. The use of multiple algorithms and techniques, such as the LF-SSO algorithm, may increase the complexity of the network and require more resources for implementation and maintenance. To overcome these drawbacks, the proposed protocol uses a DOT based authorization scheme to authenticate all mobile nodes in the network, providing a secure and reliable way of identifying legitimate nodes, The WDC algorithm is used to segregate authorized nodes into multiple clusters based on multiple metrics, which allows for better organization and management of the network. SBO algorithm is used to elect the optimal CH with a new objective function, which helps in the efficient management of the cluster and network. FNNF algorithm is used to select optimal routes by combining multiple variables, which helps in efficient routing and better performance. The proposed protocol uses the E2C2 algorithm to secure data transmission, ensuring the confidentiality and integrity of data. The combined algorithms used in the proposed protocol achieve better efficiency in PDR, throughput, time analysis, and security level, providing a more robust and reliable network

3 Problem statement

The issues related in secure routing for mobile networks is a critical issue because of the dynamic and decentralized network. One of the main challenges is to ensure that data is transmitted securely between nodes while minimizing energy consumption and maximizing the delivery rate. However, attackers can exploit vulnerabilities in the network to intercept or manipulate data, compromising the security and reliability of the network. To address this problem, a Min-Max function is formulatedfor balancingbetween energy consumption, delivery rate, and security level trade-off. The objective is to minimize energy consumption and the number of retransmissions while maximizing the delivery rate and security level. This objective is achieved by formulating the problem as a Min-Max function, where the energy consumption is minimized and the no. of retransmissions is to be optimized while the maximum delivery rate and the security level are to be maintained. The presence of attackers further complicates the problem, as they can exploit vulnerabilities in the network to compromise the security and reliability of the network. Therefore, the problem is formulated to minimize and maximize the consecutive functions in the presence of attackers. This formulation ensures that the network is secure, reliable, and efficient, even in the presence of attackers. The problem of secure routing in the mobile network is formulated as the problem of the Min-Max function as follows,
Where E_C, R_T represent energy consumption and the number of retransmissions and D_R,S_L represent delivery rate and security level respectively. The problem is formulated as minimizing and maximizing the consecutive functions in the presence of attackers.

4 Proposed Work

The proposed Block-Sec work aims at achieving high-level security with a reasonable data transmission rate. The overall work is explained in detail.

4.1 Network Model

The proposed mobile network has n number of mobile nodes M_1,M_2,..M_n with the mobility range of denote the lower and upper bound of the mobility range respectively. All mobile nodes are allowed to move around the network with varying mobility speedswithin the range. The overall network is divided into multiple clusters for ease of management. All mobile nodes within the network are authorized before cluster formation. The proposed Block-Sec architecture is illustrated in figure.3. With the help of the Blockchain network, the nodes are validated in a distributed manner. For data, transmission is carried through the optimal route selected in the network. Overall data transmission is secured by using lightweight cryptography techniques.

4.2 Mobile Node Authentication

Authentication is the process of validating the authorization of the nodes presented in the network. For authentication, the DOT protocol is proposed which uses the distributed Blockchain network. In general, authentication credentials are stored in a single server which lacks with single node failure problem. To avoid this major issue, we presented a Blockchain network for authentication.

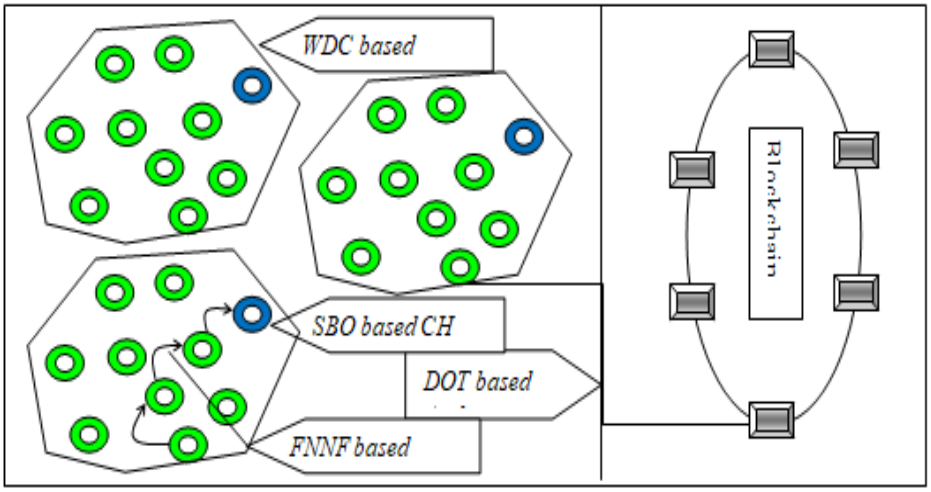


Figure.3 Proposed Block-Sec Architecture

WDC is an algorithm used for the formation of clusters in MANETs. The algorithm considers multiple metrics such as node mobility, distance, and energy levels to create and update clusters dynamically. WDC-based cluster formation helps to improve performance of the overall network by reducing the overhead and improving the routing efficiency.

A blockchain is a decentralized, distributed ledger that is used to record transactions securely and transparently. In the context of mobile networks, a blockchain network can be used to secure data transactions and ensure data integrity. The use of blockchain in mobile networks helps to reduce the risks of unauthorized access and enhances the security of the overall network.

The Cluster Head (CH) is an important node in the cluster-based routing protocol for MANETs. The optimal selection of CH is critical for the performance of the network. Strawberry Optimization (SBO) is an optimization algorithm that can be used for selecting the optimal CH in MANETs. SBO-based CH selection helps to improve the network performance by reducing energy consumption and increasing the reliability of the network.

DOT-based Authentication: Distributed One-Time Passcode (DOT) is a scheme used for node authentication in MANETs. In this scheme, each node is assigned a unique passcode, which is used for authentication. DOT-based authentication helps to improve the security of the network by preventing unauthorized access and ensuring that only authorized nodes can participate in the network.

FNNF-based Optimal Routing: Fast Neural Net-assisted Fuzzy (FNNF) is a routing algorithm used in MANETs. The algorithm uses multiple variables such as distance, mobility, energy levels, and security levels to select the optimal route for data transmission. FNNF-based optimal routing helps to improve network performance by reducing the number of retransmissions, improving the delivery rate, and increasing the security of the network.

The proposed DOT involves two main phases such as,

1. Registration in DOT – This process is initiated when a node is joining into the network. The proposed DOT protocol receives three main authentication credentials such as mobile node ID (M_ID), password (M_PW) and certificate (M_C). The certificate is generated by the main server in the network. The server is connected with the Blockchain network (i.e.) single node failure can be avoided. If i^ththe mobile node needs to register,

then it initiates the RegIni message with $M_ID(i)$,$M_PW(i)$ and $M_C(i)$ as follows,

$$M_i \rightarrow \text{Reglni} M_ID\ (\text{i}) \times M_PW\ (\text{i})\ .M_C\ (\text{i})$$

After successful registration, the server replies RegSuc messages to M_i with required private and public key pairs (K_pu (i),K_pr (i)) with time stamp (T_S) as follows,

$$\text{Block} \rightarrow \text{RegSuc} K_p\text{u}\ (\text{i}),K_pr\ (\text{i}),T_S$$

Also, the server generates unique passcode (U_ID (i)) by using the XOR function as follows,

$$U_ID\ (\text{i}) = \text{H}(M_ID) \oplus \text{H}(M_PW) | K_pu$$

H()represent the corresponding hash value. With the unique ID creation, the registration phase is completed. All these credentials are stored in the Blockchain network in a distributed manner. Authentication Phase – Once the node is registered, then it will have three major credentials with public and private key pairs. Whenever the node needs to participate in the network the node needs to be authenticated with the Blockchain. For authentication, the node needs to initiate AuthIni message to the Blockchain network. The AuthIni message is composed of,

$$\text{AuthIni} \rightarrow \text{Sign} M_ID\ (\text{i}),M_PW\ (\text{i}) + U_ID\ (\text{i})$$

The credentials need to be signed digitally by the mobile nodes. On receiving AuthIni message, the server validates the credentials with the Blockchain. If the credentials are correct, then it returns one-time passcode with the time stamp as follows,

$$OTP_t \rightarrow \text{R} \oplus M_ID\ (\text{i})\ \_\text{t}$$

The OTP_t is a session passcode that is valid only for the period t. That is, the node M_i can submit the passcode to the CH to join the network. It can be seen that, after the session is completed the OTP will become invalid which ensures no adversary can reuse the code after sometime. In this manner, the nodes are authenticated in the network.

Procedure 1: DOT protocol for authentication

1 – Initialize DOT
2 – For all $M_i \in M$
3 – Generate *RegIni*
4 – Register $M_{ID}(i),M_{PW}(i),M_C(i)$
5 – Submit $RegIni \rightarrow Blockchain$
6 - Generate $U_{ID}(i)$
7 – End For
8 – Initiate *AuthIni*
9 – Validate$Sign(AuthIni)$
10 – If $Sign(AuthIni) == Valid$
11 – Generate OTP_t
12 – Else
13 – Terminate
14 – End If
15 – End Process

The above procedure explains the steps involved in the proposed DOT protocol. The proposed authentication protocol allows cluster formation with only valid nodes which improves the security level.

4.3 Secure Cluster Formation

Once the nodes are authenticated, the next step is to form various clusters to make the data transmission simple and effective. We proposed a WDC method that uses weight value similarity for cluster formation. The major issue in cluster-based MANET is the stability of the clusters is always questionable since the nodes move away adequately which leads to collapse in the network. Thus, we presented the WDC method to improve cluster stability. First, each node M_i computes weight value based on the following three metrics, Mobility – It is represented asμ in terms of the moving node velocities in the network. Connectivity – It is represented as C_i which denotes the current node connectivity(i.e.) the no. of nodes connected with the particular node. Centroid Distance – It is represented as CD_i. It is computed as the distance between the network's central point and the current position of the node as Euclidean distance. Altogether, the weight value for the node M_i (W_i) is computed as follows,

$$W_i{=}\Sigma\ \mu{,}C_i{,}CD_i$$

Each node computes the W_i, then initiates the cluster formation process. The WDC-based cluster formation involves the following steps, Handshake Session – First, each node transmits the CluFor message as follows,

$$\text{CluFor}{\rightarrow}M_ID\ \text{(i)}{,}W_i{,}OTP_t$$

Decision-Making Session – On receiving CluFor message, each node makesa decisionbased on two conditions as follows, Condition 1:Validate OTP_t
Condition 2:Compute weight difference WD
$WD_(i,j)$=Difference[W_i,W_j]
The decision is True only if both conditions are satisfied. Cluster formation – If M_i receives CluFor from node M_j, it first checks condition 1. If the condition is satisfied (i.e.) M_j is valid, then it moves to the next condition 2. If the $WD_(i,j)$ is low, then the node accepts the formation message. Similarly, node M_j validates the M_i. After decision-making, each node transmits CluCon message to the optimum nodes to form clusters. This mutual session authentication improves the security level in the network. Also, consideration of $WD_(i,j)$ ensures that all nodes in the cluster have the same level of mobility and distance. So that, the clusters formed by the WDC method will be stable. Optimal CH selection At the end of the WDC method, the overall network is segregated into v number of clusters denoted as G_1,G_2,..,G_v. The next step is to select the optimal CH in each cluster. In each cluster, CH is responsible to manage the nodes within the group. Thus, the CH must be optimal and capable of handling the cluster management process. For optimal CH selection, we proposed an SBO algorithm with multiple objectives. The SBO algorithm is inspiredby the growth procedure of strawberry plants. The strawberry plant's growth depends upon runners and roots. Here, the runner represents the global search while a local search is represented by roots. The overall algorithm deals with the following factors,
The problem domain is spread out with the runners
The mother strawberry plant is developed and improved through the roots and hair. This growth is random in the problem domain.
The daughter plants which are developed from the mother plants improve the growth through roots and runners.
The daughter plants exist only if the growth is healthy otherwise it dies
The above facts are considered in the algorithm.
Initialization: Initialize the number of solutions as the strawberry plants. Here, the solutions are the nodes presented in each group G_j.
Problem Formulation: The objective function f(x) is the combination of functions that needs to be considered in the CH selection process. In the proposed SBO, the objective is to select optimal CH and the problem ofoptimization is formulated as follows,

$$\text{Min f(S)}{\rightarrow}\ K^OF\ \text{if}\ S_l\ {<}\text{s}{<}\ S_u$$

Here, S is the solution vector and l,u represent the lower and upper bound respectively and OF denotes the objective function.
OFFormulation: The OF of the proposed work is to select optimal and effective CH for each group. For that, we presented a multi-objective formulation in which multiple metrics are considered in OF formulation. The proposed OFis given as follows,

$$OF_i{=}\text{Max}\ (E_i{,}ST_i\ )\&\text{Min}\ (AD_i)$$

The objective function for M_i (OF_i) is computed in terms of energy level (E_i), successful transmissions (ST_i) and average cluster distance (AD_i). By combining all three parameters, the objective is formulated to select optimal CH in the formed clusters. Duplication: In the SBO algorithm, the position of the solutions is computed and updated as follows,

$$V_prob\ (\mathrm{i})=[V_root\ (\mathrm{i})\ V_runner\ (\mathrm{i})\ ]$$
$$=\mathrm{V(i(V(i)\ )+[}d_root\ \mathrm{r1}.d_runner\ \mathrm{r2]}$$

Where V_prob is the location of the i^th solution and r1,r2 are the constant values.The V_root,v_runner are computed as follows,

$$V_root\ (\mathrm{i})=V_(1.root)\ (\mathrm{i}).V_(2.root)\ (\mathrm{i}).\ldots.V_(v.root)\ (\mathrm{i})\ V_runne\ (\mathrm{i})=V_(1.runner)\ (\mathrm{i}).V_(2.runner)\ (\mathrm{i}).\ldots.V_(v.runner)\ (\mathrm{i})$$

Elimination: For each node presented in the cluster, update the position based on OF_i and the unsuitable solutions are eliminated by the following expression,

$$\mathrm{f}(V_(j.prob)\ (\mathrm{i})\ )=OF_Max,OF_Min$$

The probability is computed as follows,

$$P_j=\mathrm{f}(V_i)/(\Sigma\ f(V_(j.prob)\ (\mathrm{i})\ )\ )$$

The solution which has a lower probability is eliminated and the solution space is updated. Similarly, the node which has a higher probability is selected as the mother plant and other plants update their position based on it. In this way, the optimal node which satisfies the maximum and minimum functions is selected as CH.

Procedure 1: DOT protocol for authentication

1 – Initialize DOT
2 – For all $M_i \in M$
3 – Generate $RegIni$
4 – Register $M_{ID}(i), M_{PW}(i), M_C(i)$
5 – Submit $RegIni \rightarrow Blockchain$
6 - Generate $U_{ID}(i)$
7 – End For
8 – Initiate $AuthIni$
9 – Validate$Sign(AuthIni)$
10 – If $Sign(AuthIni) == Valid$
11 – Generate OTP_t
12 – Else
13 – Terminate
14 – End If
15 – End Process

The above procedure explains the steps involved in cluster formation and CH selection in a combined manner. At the end of the SBO algorithm, each cluster will have optimal CH which has a higher energy level and lower cluster distance.

Cluster Management: In dynamic MANETs, cluster management is one of the main issues. In the proposed approach, cluster management is performed by CH. The proposed clustering approach itself uses mobility similarity in weight value computation. Thus, the nodes with similar mobility are formulated into the same cluster which means a frequent re-clustering process is not necessary.

Further, the cluster management is performed by CH as follows,

1. If any node increases its mobility and needs to move from the cluster, then it needs to send CluTer message to the corresponding CH.
2. CH analyzes the distance and mobility to avoid unnecessary termination. If the mobility and distance differ

from the initial state, then CH sends a success message to that node.
3. After successful termination the particular node moves to the next cluster and initiates the same procedure for cluster join. Each time the node is needed to be authenticated by the Blockchain network.

Procedure 2: Cluster formation and CH selection

1 – Initialize all M_i
2 – For each M_i
3 – Compute W_i
4 – Initiate $CluIni$ message
5 – Compute $WD_{i,j}$
6 – Make a Decision
7 – if$1 > \frac{WD_{i,j}}{WD_{j,i}} > 0.5$
8 – Make M_i, M_j is cluster G_u
9 – Else
10 – Go to the next node
11 – End If
12 – End for
13 – For each G_u
14 – Initialize plants
15 – Compute OF_i
16 – Update V_{Prob}
17 – Find F_i
18 – Return CH
19 – End for
20 – End

4.4 Optimal Routing

Once the clusters are formed, the transmission of the data between the sender and receiver. For optimal route selection, we presented the FNNF approach which integrates a neural network with a fuzzy approach for fast route selection. the integration of neural networks and fuzzy elements is depicted in table.2.

Table 2. Integration of fuzzy and FNN

ANN Element	**Equivalent Fuzzy Element**
Input Layers	Fuzzification of inputs to [0,1]
Hidden layers	Application of rules from the inference engine
Output layer	Defuzzification of output get from the system

The FNNF system has three major layers as follows, Input Layer: The input layer of the FNNF algorithm receives inputs. In the proposed work, the available routes are the input for the FNNF approach. It can be given as (R_1,R_2,..,R_A) where R_A is the available routes between the source and target. For each $R_j \epsilon$R, the necessary metrics are learned in this layer. This layer is responsible for the Fuzzification process. All input values are deduced to [0,1] interval. Hidden Layer: In this layer, fuzzy rules are appliedto the input parameters. Here, we considered three major parameters such as trust value ($T_(j)$)), energy level ($E_(R(j))$) and hop count (HC_j). Each parameter is explained as follows, $T_j \rightarrow$it is defined as each node'strust value presented in the particular route R_j. It is given as,

$$T_j=(\sum_{i=1}^{x} T_i j)/\mathrm{x}$$

Where x is the no. of nodes present in the route R_j. $E_R(j)$ →it is defined as the total energy level of the given route as follows,

$$E_R=(\sum_{i=1}^{x} E_R ij)/\mathrm{x}$$

HC_j→it gives the total number of nodes presented in the route Based on the parameters, the fuzzy rules are appliedto hidden layers. The fuzzy rules are illustrated in table.3.

Table.3 Fuzzy rules for FNNF

$T_(ij)$	$E_(R(j))$	HC_j	Output
Low	Low	Low	Low
Low	Low	High	Low
Low	High	Low	Medium
Low	High	High	Low
High	Low	Low	Medium
High	Low	High	Low
High	High	Low	High
High	High	High	

As given in the table, the rules are appliedto the hidden layers. Based on the output value, each route is given with weight value as follows,

$$w_R= \sigma.\mathrm{fn}(OP_R)$$

Here, σ denotes the sigmoid function and OP_R is the output by the fuzzy rules as [High-Medium-Low]? For optimal route selection, If-Then rules are implemented in the hidden layers as follows,

If $T_i j$=High & $E_(R(j))$=High &HC_j=Low
Then OP_R=High=1

Output Layer: this layer is responsible for the Defuzzification process. In this layer, the values that lie in the [0,1] range are defuzzified to normal values. The route which has a high weight value is further selected as the optimal route R_opt for data transmission. As the route is trusted and the energy level is more than enough, data transmission is efficient and the number of retransmission is minimized. In addition, trusted route selection with authorized nodes mitigates the problem of routing attacks such as wormholes, blackholes, and sinkholes. Though the data is transmitted through a trusted route, it is necessary to secure data to mitigate man-in-the-middle and eavesdropping attacks. As we discussed earlier, each node is given with K_pu and K_pr generated at the initial phase. In Blockchain ECC algorithm is generally used. Here, we improved ECC to E2C2 algorithm by improving the key generation approach. For key generation, we have proposed FourQ-curve which are defined as follows,

$$-x^2+y^2=1+dx^2\ y^2$$

From the points x,y the keys are generated which satisfy the above equation. Thus the proposed work ensures a high level of security in data transmission through trusted route selection as well as crypto technique. The proposed method is used to improve cluster stability and optimal CH selection in cluster-based MANET. To form secure clusters, the Weighted Difference-based Clustering (WDC) method is used, which utilizes weight value similarity for cluster formation. The weight value of each node is calculated based on three metrics: Centroid Distance, Connectivity, and Mobility. These three metrics are combined to calculate the weight value for each node. The cluster formation process involves three sessions: Handshake Session, Decision-Making Session, and Cluster Formation Session. The Handshake Session initiates with the transmission of the CluFor message, which contains the M_ID (i), W_i, and OTP_t. In the Decision-Making Session, each node validates the $OTP_t$and computes the weight difference between two nodes, $WD_(i,j)$. If both conditions are met, the cluster formation process begins. Cluster Formation involvestransmission each node CluCon message to the optimum nodes to form clusters. Mutual session authentication improves the security level in the network. After the WDC method, the overall network is segregated into v number of clusters denoted as G_1,G_2,..,G_v. The next step is to select the optimal CH in each cluster. For this purpose, the Strawberry-Based Optimization (SBO) algorithm is proposed. The SBO algorithm is inspired by the growth procedure of strawberry plants, which involves runners and roots. The SBO algorithm is initialized with the number of solutions as the strawberry plants. The optimization problem is formulated to select the optimal CH in each cluster. The objective function of the proposed work is to select optimal and effective CH for each group by combining energy level, successful transmissions, and average cluster distance. The solutions' position is computed and updated by using the V_prob (i) expression, which consists of V_root (i)and $V_runner(i)$. Finally, unsuitable solutions are eliminated by using the OF_Max, OF_Min expression.

5 Experimental Analysis

The evaluation of proposed work is discussed in this section in terms of simulation observations.

5.1 Simulation Setup

The proposed MANET network is implemented in the network simulator – 3 (NS-3.25) simulation tool. The ns-3.25 is one of the event-based simulators that use C++ and TCL languages for network configuration. Ns-3.25 supports major wireless network standards and allows the integration of Blockchain. Thus, we used ns-3 for simulations.

Table 4. Simulation Parameters

Parameter	**Value**
No. of nodes	150
Maximum clusters	15
Network area	300*300m
The initial energy of nodes	750J
Bandwidth	25 MHz
No. of packets	1000
Packet size	32 KB
Number of retransmissions	5
Mobility Range	μ_L 10 m/s
μ_U	40 m/s
r1	0.01
r2	0.1
σ	0.001
Number of adversaries	5
Simulation time	100s

In table.4 summarizes the major simulation parameters used in the proposed work. With the above setting, important performance metrics are observed.

5.2 Comparative Analysis

For comparison, we used PDR, RE) time analysis (encryption and decryption), throughput, and security level. For better analysis, two scenarios are created for analysis as follows,
Scenario 1: In this scenario, we vary the no. of nodes while the no. of attackers is static (i.e.) 5. In this scenario, we can observe the ability of the proposed work in varying network scales.
Scenario 2: we set the number of nodes as static (i.e.) 100 and change the number of attackers from 1 to 5. From this scenario, we can observe the efficacy of the proposed work in the presence of attackers.
For comparison, two existing works such as PSO-Secure routing [30], and Fuzzy clustering [31] are considered. Both works have developed in the MANET environment.
a) PDR Analysis
The ratio between the total no. of packets received by the destination and the total no. of packets transmitted by the source nodeis known as PDR.

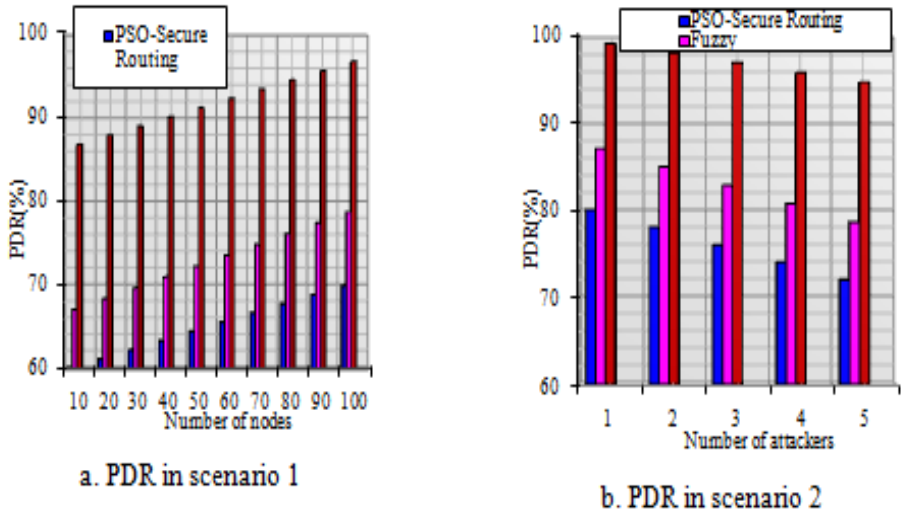


Figure 5. Comparison on PDR

In figure.5, the PDR is analyzed in both scenarios. Here, it can be seen the PDR achieved by the proposed work is nearly 97% which is far better than the existing works. In scenario 1, the PDR is increased gradually with an increase in several nodes. On increase in node quantity, the opportunity for selecting the optimal route will be increased. Thus, the data is transmitted through an effectual and trusted route. On the other hand, when the number of attackers is increased the PDR is decreased. This is because the involvement of increased attackers modifies the route information and leads to packet loss. However, in both scenarios, the proposed Block-Sec method achieves better PDR. This analysis shows that the proposed security mechanism tackles the attackers and cluster-based routing assist in achieving optimal routing.

b) Energy Level analysis

Residual energy is the important performance measure that defines the current energy level of the nodes presented in the network. For i^th node, the residual energy (RE) is computed as follows,

$$RE_i=(\sum\_i = 1^n \ E_i(\text{Ini})\text{-}E_i(\text{Cur}))/\text{n}$$

Here E_i (Ini) is the initial energy level and E_i (Cur) is the current energy level of the i^th node.

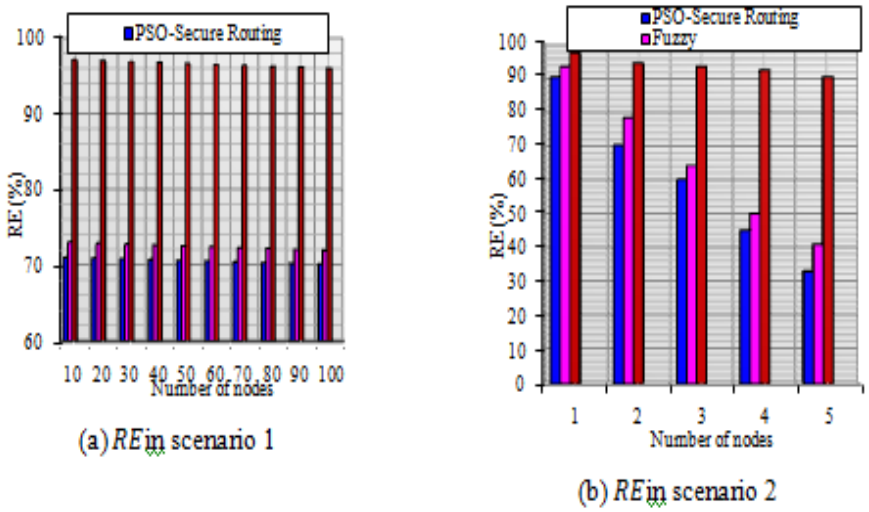


Figure 6. Comparison ofenergy level

Figure.6 compares the energy level among proposed and existing works. In general, the increased energy consumption when the increase in no. of attackers in the network. The involvement of attackers attempts to drain the node's energy level. After a particular period, the node's energy level will be drained completely and the nodes become dead. To avoid this situation, it is necessary to protect the overall network from attackers.

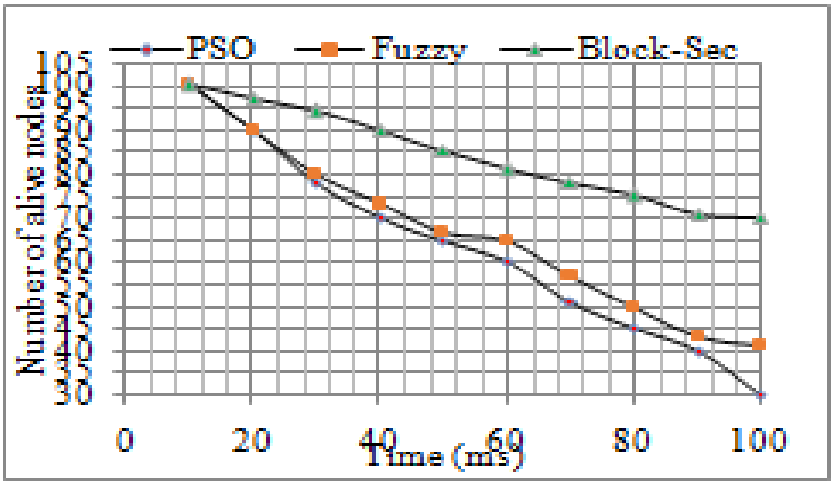


Figure 7. Number of nodes alive concerningthe time

Figure 7 shows the no. of alive nodes oversome time. It can be seen that the number of alive nodes decreases with the increase in the period. With that, the proposed work maintains a large no. of nodes as alive. This shows that the proposed Block-Sec approach protects the network from attackers as well as saves the energy level of nodes through dynamic cluster formation and optimal route selection. From the analysis, it is clear that the proposed approach is suitable for the dynamic mobile network in maintaining the proper energy levels. **c) Time Analysis**

We analyze the time consumed in providing security by various methodologies. The time analysis is performed in two ways: i) by encryption time and ii) by decryption time.

i) Encryption time: the time taken by the cryptography technique to convert plaintext into ciphertext. Itis computed at the source node.

ii) Decryption time: the time taken by t

he cryptography technique to convert ciphertext into plaintext. It is computed at the destination.

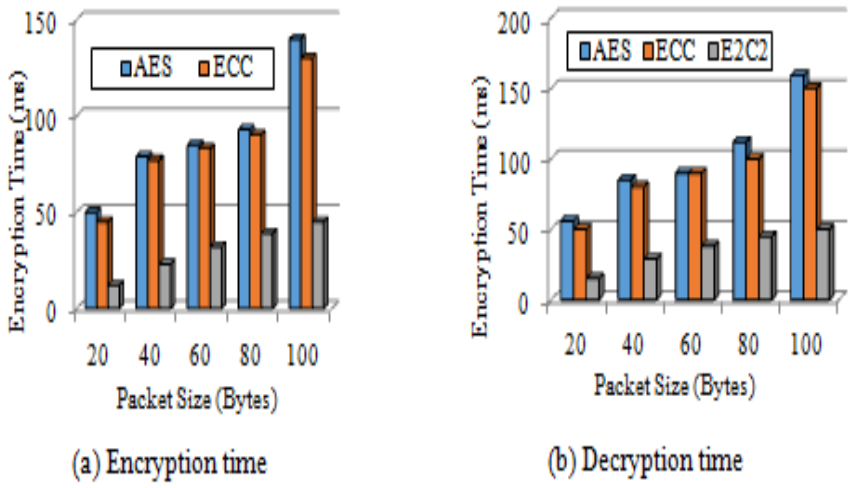
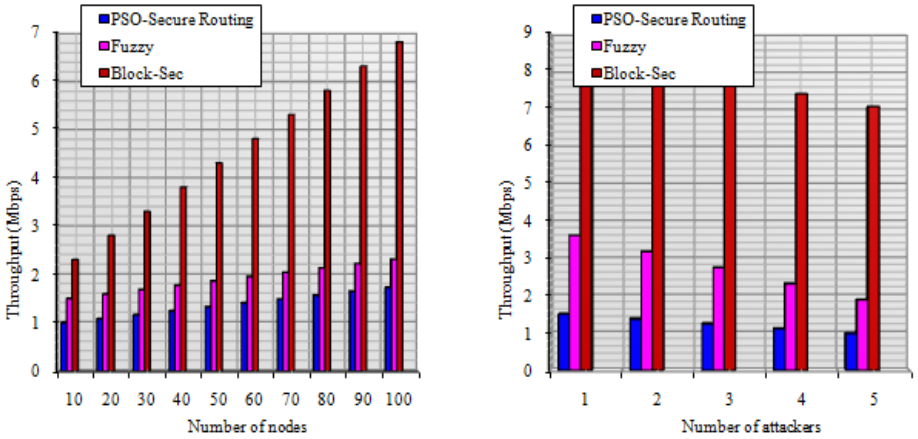


Figure 8. Comparison of time analysis

In figure.8, encryption and decryption time analysis are presented. When it comes to encryption and decryption the time consumption fully depends upon the packet size. When increase in the packet size then the time consumption is also increased. Here, we compared the time consumed by Advanced Encryption Standard (AES), Elliptic Curve Encryption (ECC), and proposed E2C2 crypto techniques. In general ECC algorithm consumes lower time than the AES algorithm in both encryption and encryption. When it comes to the E2C2 algorithm it further minimizes the time consumption by generating a lightweight key by Four-Q curve. From the analysis, it is clear that the proposed encryption algorithm is efficient in data security.

d) Throughput Analysis



(a) Throughput in scenario 1 (b) Throughput in scenario 2

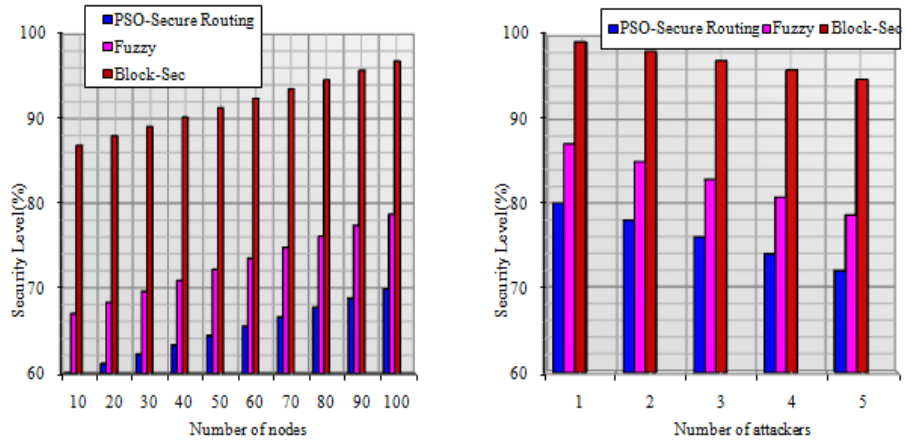
Figure 9. Comparison on throughput

The total amount of successful data transmission to the destination at a given time is known as Throughput. In figure.9, the comparison of obtained throughput with proposed and existing works.In contrast to other parameters, the throughput metric depends upon both the security level of the network andthe data transmission methodology. That is to say, throughput is affected by both security threats and non-optimal data transmission. It can be seen from scenario.2 that when the number of attackers is increased then the throughput is decreased. This is because the data transmitted at a given period is majorly attacked by the attacker nodes so that the data is not received at the destination within a given period.

In both scenarios, the proposed work achieves better throughput of up to 8 Mbps which is 2 times better than the existing works. The presence of an effectual security scheme and optimal network management with the routing approach in the proposed work helps in achieving the highest throughput value in the network. Thus, we can summarize that the data loss is minimized drastically in the proposed work.

e) Security Level Analysis

The security level is measured in terms of the total amount of packets altered or modified in the network by attackers. It shows the involvement of the attackers (i.e.) when the number of attackers presented in the network is large, then it modifiesa large number of data packets.



(a) Security level in scenario 1 (b) Security level scenario 2

Figure 10. Comparison of security level

In figure.10, the security level attained by the proposed and existing security approaches has been compared. The analysis shows that the proposed work attains 98% of the security level which is far better than the existing works. The proposed work ensures security level through the following aspects,

1. Integration of Blockchain ensures high-level security and the involvement of effectual authentication through the Blockchain network prevents unauthorized nodes in the network limit. Thus the network is free from malicious and unauthorized nodes.
2. The optimal route is selected by considering the trust value which ensures that the data will not be modified as there are no untrusted malicious nodes

3. Data is secured by using an E2C encryption approach which will not be shared or altered by any malicious nodes

With the above aspects the proposed work achieves a better security level in the network. At the same time, existing work either focus on malicious node detection or data security. Further, the centralized nodes in the network may become compromised which limits the security level to 30%.

6 Conclusion

A new Block-Sec-based MANET architecture is proposed to ensure high-level security in a mobile environment. The major issue of secure routing and data transmission is realized by integrating distributed Blockchain network with the MANET environment. First, the mobile nodes are authorized by the DOT approach. This approach authorizes the nodes based on dynamic one-time passwords and digital signatures validated in the Blockchain. All authorized nodes are considered the WDC approach which uses weight value-based similarity for cluster formation. In each cluster, the optimal cluster head node is selected by the SBO algorithm by considering multiple metrics. Further, data transmission is performed through the optimal route selected by the FNNF algorithm based on significant trust-based parameters. Data security is ensured by the E2C2 algorithm which is an effectual cryptography technique. With all security approaches, the proposed work shows betterment in PDR, energy efficiency, throughput, time analysis, and security level.

In the future, we intend to integrate Intrusion Detection System (IDS) for the MANET environment to detect the attacks accurately.

Acknowledgement

There is no acknowledgement involved in this work

References

[1] Pérez, Ramses Fuentes, et al. Prototype of MANET Network with Ring Topology for Mobile Devices (2021)

[2] Rajathi L.V. and RubaSoundar K. -. A Survey on Various MANET Protocols. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences (2022)

[3] Malik, Kamal, and AnshuBhasin. A survey of mitigation techniques of packet drop attacks in MANET SSRN Electronic Journal (2022)

[4] Korir, FridahChepkemoi, and Wilson Cheruiyot. A survey on security challenges in the current MANET routing protocols. Global Journal of Engineering and Technology Advances (2022)

[5] Mohamed, Hossam El-Din, et al. Using MANET in IoT Healthcare Applications: A Survey (2021)

[6] Al-Shakarchi, Sanaa J. H. and RaaidAlubady. A Survey of Selfish Nodes Detection in MANET: Solutions and Opportunities of Research. 2021 1st Babylon International Conference on Information Techn7logy and Science (BICITS) (2021): 178-184.

[7] Alam, Tanweer and Mohamed Benaida. The Role of Cloud-MANET Framework in the Internet of Things (IoT). Computational Materials Science eJournal (2018)

[8] Lakshmi, G. Vidhya and P. Vaishnavi. An Efficient Security Framework for Trusted and Secure Routing in MANET: A Comprehensive Solution. Wireless Personal Communications 124 (2022): 333 - 348.

[9] Jabbar, Waheb A. et al. MEQSA-OLSRv2: A Multicriteria-Based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT. IEEE Access 6 (2018): 76546-76572.

[10] Serhani, Abdellatif, et al. AQ-Routing: mobility-, a stability-aware adaptive routing protocol for data routing in MANET–IoT systems. Cluster Computing 23 (2019): 13-27.

[11] Gomathi, K. and B. Parvathavarthini. A Secure Clustering in MANET through Direct Trust Evaluation Technique. 2015 International Conference on Cloud Computing (ICCC) (2015): 1-6.

[12] Piyalikar et al. Forecast Weighted Clustering in MANET. Procedia Computer Science 89 (2016): 253-260.

[13] Suma, R., and Suma. Integration of particle swarm optimization with an adaptive K-Nearest Neighbor for energy-efficient clustering in MANET. (2020)

[14] A Hybrid Approach For Node Co-Operation Based Clustering In Manet. (2018)

[15] Krishnan, Rahul. A Survey on Game Theory Approaches for Improving Security in MANET. (2018)

[16] Gupta, Alok and Nikhil Ranjan. A Survey of Attacker Identification and Security Schemes in MANET. (2020)

[17] Muruganandam, S. et al. A Survey: Comparative study of security methods and trust manage solutions in MANET. 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) 1 (2019): 125-131.

[18] Usha, G. et al. Survey of Single and Cross Layer Security in MANET. Indian journal of science and technology 9 (2016)

[19] Sumra, Dr.Irshad Ahmed, et al. Security issues and Challenges in MANET-VANET-FANET: A Survey. EAI Endorsed Transactions on Energy Web 5 (2018): 155884

[20] Rao, A. Arjuna et al. Survey of Routing Protocols and Routing Attacks in MANET with Different Security Technique in Cryptography for Network Security. (2018)

[21] Poongodi, M. et al. 5G based Blockchain network for authentic and ethical keyword search engine. IET Commun. 16 (2021): 442-448

[22] Zhang, Lei et al. How Much Communication Resource is Needed to Run a Wireless Blockchain Network? IEEE Network 36 (2021): 128-135

[23] Nikhade, Jitendra R. and Vilas M. Thakare. BlockChain Based Security Enhancement in MANET with the Improvisation of QoS Elicited from Network Integrity and Reliance Management. Ad Hoc Sens. Wirel. Networks 52 (2022): 123-171.

[24] Suma, R. and Suma.. Integration of particle swarm optimization with an adaptive K-Nearest Neighbor for energy-efficient clustering in MANET. (2020)

[25] J, Martin Sahayaraj et al. IEEHR: Improved Energy Efficient Honeycomb based Routing in MANET for Improving Network Performance and Longevity. International Journal on Recent and Innovation Trends in Computing and Communication (2022)

[26] Alappatt, Valanto and Joe Prathap P. M.. Trust-Based Energy Efficient Secure Multipath Routing in MANET Using LF-SSO and SH2E. International Journal of Computer Networks and Applications (2021)

[27] DrishyaS., R. et al. A Stable Clustering Scheme with Node Prediction in MANET. Int. J. Commun. Networks Inf. Secur. 13 (2021)

[28] Ponguwala, Maitreyi and Sreenivasa Rao. E2-SR: a novel energy-efficient secure routing scheme to protect MANET-IoT. IET Commun. 13 (2019): 3207-3216

[29] Kondaiah, Ramireddy and BachalaSathyanarayana. Trust Factor and Fuzzy Firefly Integrated Particle Swarm Optimization Based Intrusion Detection and Prevention System for Secure Routing of MANET. International Journal of Computer Networks & Communications 10 (2018): 13-33.

[30] Khan, Md. Sameeruddin and Md. Yusuf Mulge. Efficient and Secure Data Transmission in MANETs against Malicious AttackUsing AODV Routing and PSO Clustering with AES Cryptography. (2017).

[31] Nagendranth, M. V. S. S. et al. Type II fuzzy-based clustering with improved ant colony optimization-based routing (t2fcatr) protocol for secured data transmission in manet. The Journal of Supercomputing 78 (2022): 9102 - 9120.

[32] Gomathi, K. et al. An Efficient Secure Group Communication in MANET Using Fuzzy Trust Based Clustering and Hierarchical Distributed Group Key Management. Wireless Personal Communications 94 (2017): 2149-2162.

[33] Sakkarapani, Krishnaveni and C. Chandra Prabha. Secure Multi-Path Routing Using Splitting and Merging Based Clustering for Reducing Power Usage in MANET. (2021)

[34] Mohindra, AnubhutiRoda and Charu Gandhi. A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in MANET. (2021)

[35] Veeraiah, N. and B. Tirumala Krishna. An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence 15 (2020): 1313-1327.

[36] Rani, Simpel. A Hybrid and Secure Clustering Technique for Isolation of Black hole Attack in MANET. (2018)

[37] B, Revathi and Arulanandam K. Design And Development of Robust And Secure Cluster Routing Algorithm For Manet Based IOT. International Journal of Computer Trends and Technology (2021)

[38] Sajyth, RB and G. Sujatha. Design of Data Confidential and Reliable Bee Clustering Routing Protocol in MANET. 2018 International Conference on Computer Communication and Informatics (ICCCI) (2018): 1-7.

[39] Rajaram, A., & Baskar, A. (2023). Hybrid Optimization-Based Multi-Path Routing for Dynamic Cluster-Based MANET. Cybernetics and Systems.

[40] Baskar, A., & Rajaram, A. (2022). Environment monitoring for air pollution control using multipath-based optimum routing in mobile ad hoc networks. journal of environmental protection and ecology, 23(5), 2140-2149.

[41] Anand, R. P., & Rajaram, A. (2020, December). Effective timer count scheduling with spectator routing using stifle restriction algorithm in manet. In IOP Conference series: materials science and engineering (Vol. 994, No. 1, p. 012031).IOP Publishing.

[42] Rathish, C. R., & Rajaram, A. (2018). Sweeping inclusive connectivity based routing in wireless sensor networks. ARPN Journal of Engineering and Applied Sciences, 3(5), 1752-1760.

[43] M. S. Gharajeh, FSB-System: A Detection System for Fire, Suffocation, and Burn Based on Fuzzy Decision Making, MCDM, and RGB Model in Wireless Sensor Networks, Wireless Personal Communications, vol. 105, no. 4, pp. 1171–1213, Mar. 2019.

[44] M. S. Gharajeh, A Neural-MCDM-Based Routing Protocol for Packet Transmission in Mobile Ad Hoc Networks, International Journal of Communication Networks and Distributed Systems, vol. 21, no. 4, pp. 496–527, Sept. 2018.

Cite this paper as:

Ilakkiya N.; Rajaram, A. (2023). Blockchain-assisted Secure Routing Protocol for Cluster-based Mobile-ad Hoc Networks, *International Journal of Computers Communications & Control*, 18(2), 5144, 2023.
https://doi.org/10.15837/ijccc.2023.2.5144