Holochain: Secure Optimal Routing and Dynamic Task Offloading for Defense Against Multiple Attacks in MEC Assisted MANET-IoT Networks

B. HARIKRISHNAN [1,2*]
T. BALASUBARAMANIAN [1]

[1] PG & Research Department of Computer Science & Applications,
Sri Vidya Mandir Arts & Science College (Autonomous), Katteri – 636 902, Uthangarai,Tamil Nadu, India
[2] Department of Computer Science, Periyar University, Salem – 636 011, Tamil Nadu, India
[1]harugi@gmail.com; [2]balaeswar123@gmail.com

Abstract. MANET with Internet of Things (IoT) plays a vital role in processing, sensing, and acquiring of data. Many of the existing works exploits MANET-IoT, that provide better results however, they have limitations of data integrity problem, scalability issues, and energy consumption which affect the reliability of communication. In this paper, by leveraging the short comings faced by the existing works, we propose HSec-Route (Holochain based Secure Routing) approach with secure and energy efficient capability to achieve QoS constraints. Initially, nodes in the mobile network are authenticated to Holochain based centralized TA that exploits improved BLISS algorithm to ensure legitimacy of nodes by considering multiple attributes. The authenticated nodes are clustered to improve the connectivity between nodes using Enhanced Fuzzy C-Means (EFCM) algorithm by considering several metrics. Here, Cluster Head (CH) is selected to minimize energy consumption. After clustering, the routing between Cluster Members (CMs) to CH is carried out by performing two stages namely trust management stage and optimal forwarder stage. In trust management stage, both direct and indirect trusts are evaluated for every nodes to confirm forwarders legitimacy and ranking of nodes is done by Grey Absolute Decision Analysis (GADA) based on trust values. With the help of trust values and other metrics, the optimal forwarder is selected by Improved Particle Swarm Optimization (IPSO). Finally, the nodes integrity is ensured by En-route filtering and the dishonest nodes are pruned out. The simulation is carried out using NS-3.26 simulation tool and the performances are compared with existing works in terms of several validation metrics. The validation results show that our proposed work performs well than the existing works.

Keywords: MANET, IoT, Authentication, Secure optimal routing, Mobile edge nodes, Offloading, Holochain

(Received March 4th, 2022 / Accepted May 9th, 2022)

1 Introduction

A Mobile Ad Hoc Network (MANET) consists of mobile nodes. The base stations do not provide any support for these nodes. Internet of Things (IoT) is an emerging technology to transmit data over entire network efficiently. Recently, integration of MANET and IoT are emerged for designing various real-time applications, such as military units, health surveillance, etc. [1]. Traditional approaches of MANETs, viz. clustering and routing cause a significant barrier in achieving high quality of service (QoS). In this case, massive tasks are generated from nodes and forwarded to destination [2,3]. Mobile edge computing (MEC) is another networking paradigm that supports latency and resource usage reduction for number of tasks since it performs

local computing. With the use of MEC, dynamic topology of MANET, limited energy, lack of centralized infrastructure, unstable links, and frequent path selection problems are mitigated and also improved the network lifetime. In this integrated environment i.e. MANET-Edge-IoT, resource constraints and security are important problems. Specifically, this causes security problems of delay-sensitive and resource-constrained applications of MANET in IoT platforms [4]. Therefore, some of the requirements are essential to be satisfied in this integrated environment and that are follows:

- Secure data packets
- Reduce energy usage of nodes
- Predict attackers' behaviors to avoid damage
- Isolate attackers that located anywhere in the network

To mitigate higher energy consumption issues of MANET-IoT, clustering and routing processes are effectively handled with the use of a specific set of parameters, such as distance, link quality, node hop count, and remaining energy for achieving efficient QoS [5-7]. In some works, trust-based routing is performed to enhance security of MANET by mitigating malicious nodes [8]. On the other hand, path selection is implemented using link quality and energy level [9,10]. These traditional schemes do not handle large number of mobile nodes in network and also does not suit for heterogeneous environment with diverse resource and task constraints. Further, security problem addressed using conventional cryptography approaches are perform by more key size, rounds, block size, and operations. To deal with those issues, lightweight cryptography approaches are proposed, which consume fewer amount of resources due to minimum computations [11]. This is one of the great solutions for addressing security issues. Furthermore, blockchain is a decentralized approach that is used to mitigate attackers to know network and stored transactions [12]. Blockchain provides potential security solution for eliminating attackers in network and recently researchers have determined that blockchain does not support scalability and also introduces latency in storing and mining transactions [13]. To consider this seriously, blockchain structure is redefined in terms of hash graph, chain structure, consensus, smart contract, etc. However, addressing blockchain issues pose great challenge in wireless networks (resource-constrained environments). A deep learning method, Artificial Neural Network (ANN) is used to mitigate different attacks [14]. One of the great challenges in MEC is congestion/massive network traffic. For specific tasks processing, MEC gets overloaded. It is assumed to be a multi-objective optimization problem that requires to meet multiple constraints. The edge nodes must be executed with specified number of tasks requested with their region. Offloading is performed for managing overload situations however, scalability issues degrade offloading performance [15]. In this study, all the aforementioned challenges are addressed in edge assisted MANET-IoT environment.

1.1 Motivation and Objectives

In this study, energy efficient and secure scheme is designed for achieving higher QoS in MEC based MANET and IoT environment. This scheme is presented to determine multiple malicious nodes with different attack behaviours and also eliminate attackers from network for minimizing damage. There are major problems taken into account in MEC based MANET-IoT environment that are identified in this study, such as low scalability, lack of integrity and increased latency and resources. We are motivated by these problems and each one is discussed below:

- Low Scalability: For security and QoS provisioning, blockchain technology is presented. However, blockchain addresses centralized security failure issue, but low scalability and high latency problems are not resolved in blockchain based MANET environments. Hence, a conventional blockchain algorithm does not support to handle massive volume of data in a short span of time.
- Lack of Integrity: False data might be injected by attackers at any type of node (source, intermediate or destination node). On the other hand, original data can be modified by both internal and external attackers. Data transmission must be protected by integrity property
- Increased Latency & Resources: the nature of MANET and IoT based devices are resource constrained (low energy, and power) and to process data packets from those devices consume certain amount of resources and time. When the energy consumption increases, then network lifetime decreases and also number of alive nodes in network are lesser. Further, routing algorithms do not construct optimum path for travelling packets from source to destination node. Therefore, higher delay and limited resources result poor network QoS performance.

The research objective of this study is to design secure MEC based MANET-IoT network for resource constrained environment. To meet this main objective, some of the following sub-objectives are designed.

- To minimize routing overhead and end-to-end delay in packet transmission from source to destination node.
- To maximize security strength and packet delivery ratio via signature generation in en-route filtering and trust management.
- To improve rate of attack prediction and different attackers behaviours for early warning to the network.
- To minimize overall communication and computation overhead for end-to-end packet transmission from source mobile node to edge node.

1.2 Research Contributions

The secure and energy efficient frame work is proposed to mitigate problems faced by existing works in terms of security, scalability, and energy consumption. Major contributions of this research are listed below:

- The legitimacy of all mobile nodes in the networks is ensured by performing multi attribute based authentication, which exploits improved BLISS algorithm for key generation to all mobile nodes.
- The legitimate nodes are clustered to improve connectivity using Enhanced Fuzzy C-Means (EFCM) algorithm in which Cluster Head (CH) is selected based on link quality and energy availability for minimizing energy consumption.
- The secure optimal routing is performed between Cluster Members (CMs) and CHs by employing two phases, namely trust evaluation phase and optimal forwarder selection phase. The trust evaluation is done by GADA algorithm in which trust values are ranked based on trust values and optimal forwarder selection is done by Improved Particle Swarm Optimization (IPSO). All the nodes are checked for integrity using en-Route filtering before sending or receiving messages.
- The aggregated data from CH are sent to MEC nodes for data processing. The offloading between MEC nodes and cloud is done by conditional entropy only when MEC nodes are overloads. The Holochain is utilized for recording transactions and also mitigate several attacks.

1.3 Paper Organization

The remaining contents of the paper are organized as follows: Section II deals with literature survey in which existing research gaps are clearly provided. Section III provides specific problem statement in the existing works and also research solutions are given. Section IV delivers the proposed work in which all the processes are clearly explained with suitable diagrams and passcodes. Section V elaborates experimental set up in which simulation set up, comparison analysis, and research summary are given. Section VI deals with conclusion and future directions of the proposed work.

2 LITERATURE SURVEY

Authors in [16] proposed an adaptive routing protocol using reinforcement learning for detecting mobility of devices at different times. The proposed protocol considers Q learning for analysing mobility of node in the network that metric is known as Q metrics. It can be able to adaptively change the network topology and it considers both static and dynamic metrics. The proposed protocol perfectly handles mobility of nodes in the network by considering ETX, hop count, link stability, and mobility degree factor. The simulation result shows that the proposed model achieves better performance in terms of link stability and packet delivery ratio in both mobile and static scenario in MANET-IoT environment. Here, AQ routing is performed for analysing mobility of node in the network; however it takes much time for routing because of collecting mobility information from individual node that increases high energy consumption and latency that degrades performance of routing. Secure routing protocol is designed in MANET with secured IoT devices using trust based method [17]. The proposed work includes five stages, such as route discovery, MSRS estimation, DS estimation, and secure route analysis. In first process, the proposed method detects multiple routes between source and destination by considering mobility condition, neighbour, energy, and transmission count, which are added in the route table. The optimal route is selected from the route table by route discovery algorithm. Then, the trustworthiness of the mobile node is evaluated for secure routing. Based on the value of data forwarding support, the optimal route is selected. The simulation result shows that the proposed model achieves better performance in terms of efficiency, throughput, and secure routing. Here, trustworthiness is evaluated based on mobility condition, neighbour, energy, and transmission count, which are not enough for calculating trustworthiness that increases retransmission rate due to poor trust.

A novel method is proposed for diagnosing anomalies in MANET using provenance and verification [18]. The proposed method detects both direct and indirect anomalies by secure routing. The proposed method includes three processes, namely provenance rules, provenance verification, and provenance reasoning. Merkle hash tree is proposed for obtaining privacy preservation. Digital signature algorithm is proposed for verification. Directed Acyclic Graph is used to construct provenance graph that can easily detect attack nodes. The simulation result shows that proposed method achieves better performance for detecting malicious and paralysed nodes. Here, Merkle hash tree is proposed for provenance verification however it takes much time for mining due to its lengthy tree construction that ultimately increases energy consumption of the nodes and as a consequence reduces efficiency of the process. Authors in [19] proposed multi path routing protocol by considering energy consumption and lifetime using mobile edge computation. The proposed multipath routing protocol has three control points, such as routing request, routing reply, and routing error. The multi path selection is based on minimum hop count, energy, and stability. For that this research used priority based path selection method for improving network lifetime and path stability. Path priority is calculated based on energy consumption, lifetime, and link priority. The route maintenance is considered based on link status of other node. The experiment result shows that the proposed method achieves better performance in terms of network lifetime, energy efficiency, and end to end delay. Here, path selection is considered only to limited parameters that are not enough to select optimal path and leads to high retransmission rate and packet loss rate, which reduce throughput and efficiency of the proposed work. The trustworthiness of the routing is not evaluated that can be easily compromised by the attackers, which leads to poor security and it reduces throughput of the proposed work.

Authors in [20] proposed sensitivity analysis of attack mitigation using trusted routing method with path discovery (TRS-PD) for MANET in industrial IoT. The proposed work includes three processes, viz. attack detection method, trust calculation method, and routing process. In first process, filed values are recorded for discovering attack patterns, namely node ID, current time, destination sequence number, and hop count. Based on these records, the proposed pattern discovery method discovered attack pattern and added into blacklist. The proposed method calculates both direct and indirect trusts based on historical values. If once node is identified as malicious then send recommendation to nearest node. The experimental results demonstrated that the proposed model achieves better performance by proposing TRS-PD method. For detecting attack patterns, the proposed work calculates trust value based on historical information, which does not provide optimal trust value that reduces security. Both the trust value and recommendations are sending through public channel which can be easily compromised by the attackers and hence reduces performance of the proposed work. Multipath secure routing algorithm is proposed using blockchain technology in ad hoc network [21]. Initially, the node chain is established in the network and all the nodes create a connection between the nodes. Secondly, the blockchain based smart contract is to meet QoS requirements. Then, the two paths are selected by blockchain using EERQ process. The routing maintenance process is used for solving failure of main paths. The simulation result shows that the proposed work achieves better performance compared to existing works. Here, the path selection is performed using blockchain however, it selects random path that may leads to packet loss and retransmission rate due to poor link quality. Moreover, the proposed blockchain technology takes much time for mining due to lengthy construction of block that increase energy consumption and latency.

The Bayesian inference based updation of distributed ledgers in the DAG based blockchain was proposed in this paper [22]. The limitations of existing blockchain algorithms, such as reduced scalability and increased transactional fees were considered and a Bayesian inference based DAG blockchain mechanism was introduced. The nodes in the network were categorized into three sections to compute likelihood distribution. The three different subsets of nodes were: all nodes in a set were included in computation of prior distribution but not during formation of sub tangle, all nodes in a set were included both in computation of prior distribution and t-th sub tangle, and all nodes in a set were only included in the sub tangle. The Bayesian inference based updation of ledgers was found to be efficient in determining connection between blocks. Authors in [23] proposed a method for detecting hybrid wormhole attack in MANET, which could be able to detect in-band and out-band wormholes using round trip time by considering hop count, packet delivery ratio, and transmission range. The proposed method reduces energy and delay by detecting wormhole attack in the network. K-means clustering algorithm is proposed for clustering the nodes. The simulation result shows that the proposed model achieves better performance in terms of throughput, end to end delay, packet delivery ratio, and

energy consumption when compared to existing algorithms. Here, wormhole attack is discovered based on performance metrics that does not detect the attack in an accurate manner due to lack of trustworthiness of the node and thus reduces performance of the attack detection. In addition, it also reduces throughput and increase packet loss rate.

Authors in [24] proposed swarm based clustering for detecting intrusions in MANET. The proposed work includes two processes, such as cluster head selection and attack detection. Here, clustering is performed by greedy swarm optimization and then cluster head is selected by considering energy consumption and mobility. Intrusion detection is performed using Gradient Deep Belief Network algorithm, which mitigates both DoS and Zero-day attacks. The simulation result shows that the proposed work achieved better performance in terms of memory consumption, attack detection rate, and computation time.

Authors in [25] proposed a novel method for secure routing in MANET. Here, CH selection is performed using fuzzy c means by considering both direct and indirect trusts. Based on the trust value, routing is performed by multipath routing protocol that used hybrid algorithm, which includes Genetic algorithm and hill climbing algorithm. Finally, the experimental result shows that the proposed work achieved better performance in terms of energy, delay, throughput, packet delivery ratio, and detection rate. Authors in [26] introduced a secure hybrid system for IoT exploited mobile ad hoc networks. Initially, the data packets are finding a forwarder based on ad-hoc on demand multi path distance vector protocol. Before transmission the data to forwarder, the packets are encrypted by false key advanced encryption algorithm in which masking of keys and original data packets are taken place by exploiting midway mask. The black hole attack initiate by the malicious nodes are mitigated using co-operative distributed routing protocol. Here, ad hoc on demand multi path distance vector protocol was used for routing discovery that creates more overheads during routing and causes packet flooding. Authors in [27] introduced trustworthy transmission of data using encryption techniques for mobile ad hoc networks. Initially, clustering of mobile nodes are done by Energy Efficient Routing Protocol and from the clustered node cluster head is selected by Modified Discrete Swarm Optimization Algorithm, which considers nodes with good communicating capability. Then, trust evaluation is done for mobile nodes towards routing in which direct and indirect trusts are assessed. Finally, data are encrypted using signcryption technique. Here, communication capability is an only metric used for selecting cluster head that is not enough for selecting optimal cluster heads, which affects reliability of communication[28].

3 PROBLEM STATEMENT

The bandwidth based routing of network packets for congestion avoidance in MANET and IoT was proposed in this paper [29]. The major problems of this research are listed as follows:

- The selection of forwarding node for transmission of packets from source to destination node was carried out by considering available bandwidth but lack of consideration of other significant factors, such as available energy of node resulted in increased packet loss.
- The estimation of bandwidth and adjustment of data rate for transmission of packets in the network was carried out based on the feedback provided by neighboring nodes but the presence of malicious nodes in the network affects integrity of the feedback and thereby affecting bandwidth estimation process.
- The bandwidth based selection of forwarding node was computed for both static and dynamic topologies but lesser link quality between nodes in dynamic situation affects effective transmission of packets.

The enhancement of security of nodes in MANET tied IoT environment was proposed in this paper [30]. The limitations of adopting current routing protocols in MANET environment were addressed and a game theoretic algorithm based secure routing of packets was introduced. The main problems of this research are listed as follows:

- The game theoretic mechanism based detection of malicious nodes performed modeling of activities of both legitimate and malicious nodes however, this approach provided security only against known attacks thereby affecting overall security of the network.
- The digital code mechanism was incorporated to ensure legitimacy of nodes indulging in transmission of packets but security attacks, such as wormhole attack will affect proper transmission of packets in the network even if the packets are encrypted.
- The game theoretic mechanism was utilized to detect presence of malicious nodes in the network but

integrity of messages transmitted by nodes in the network was not ensured.

The ranking based selection of critical nodes in heterogeneous environment was proposed in this paper [31]. The vulnerabilities of MANET-IoT environment were analysed and a network defense based approach was introduced. The major problems of this research are listed as follows:

- The critical nodes in the network were identified by means of computing fusion of betweenness centrality and degree centrality to perform port hopping mechanism but the security of the normal nodes was not considered that resulted in providing only partial security.
- The port hopping was carried out to secure critical nodes from malicious attacks but switching of ports are predictable due to limited number of ports in the node thereby affecting security of the critical nodes.
- The selection of critical nodes was carried out by computing centrality metrics and ranking the nodes according to it however, importance of nodes in the network was computed only based on distance between the nodes, which affects effective identification of critical node.

Authors in [32] proposed a lightweight trust management system using blockchain in MANET. The proposed blockchain based method was used for managing trust value of nodes in the network. The main problems of this paper are defined as follows:

- Here, trust values are calculated based on blockchain however, the proposed blockchain takes much time for mining in large scale environment due to linear construction of blocks thus increases high energy consumption.
- Here, node information are collected from individual that leads to high complexity at large scale environment thus increases latency and energy consumption that reduces performance of secure routing.
- The blockchain based trust management approach was found to be suitable only for limited number of nodes in the network, if scalability of nodes in the network increases the blockchain faced scalability issues.

4 HSEC-ROUTE MODEL

The proposed approach focuses on secure communication in MANET-IoT environment. The system model comprises of entities, such as mobile nodes, trusted authority (TA), edge nodes, and Holochain based cloud. The major objective of our approach is to improve security, scalability, and energy efficiency of the nodes in the network.
Fig 1 represents overall process of the proposed work. The following processes are involved in this approach:

- Multi-Attribute based Authentication
- Energy Aware Fuzzy Clustering
- Secure Optimal Routing
- Dynamic Offloading
- Attack Mitigation by Holochain

4.1 Multi-Attribute Based Authentication

The first and foremost process for securing mobile nodes in the network is authentication in which multiple unique attributes of mobile nodes are utilized to ensure legitimacy of mobile nodes. Initially, registration of mobile nodes is carried out in which mobile nodes provide their credentials, such as Physically Unclonable Function (PUF), MAC address, user finger vein, IP address, User ID, and password to centralized TA, which is managed by Holochain. The hash fingerprint of the credentials is computed by Holochain to preserve integrity of the credentials. Improved Bimodal Lattice Signature Scheme (BLISS) algorithm is incorporated for the purpose of generating public and private keys towards mobile nodes to sign their messages. Generally, the following BLISS algorithm exploits ring $R_{i\bigtriangledown}$ for operation. The procedure for BLISS signature algorithm is provided in pseudocode,

BLISS signature algorithm ()
Input: Message
$\infty, PbK = (a_1, \bigtriangledown - 1)PrK = (PrK1, PrK2)$
Output: Signature $(sig1, sig2, ch)$

1. $h_1 \leftarrow GD^l_{\blacksquare}, h_2 \leftarrow GD^l_{\blacksquare}$
2. Compute $r = \oint .a_1.h_1 + h_2 mod 2\bigtriangledown$
3. $ch = H(\mid r \mid_\alpha modP \parallel \infty)$
4. $(J_1, J_2) = GreedySC(Prk, ch)$
5. Sampling of random bit I

6. $(sig1, sig2) = (h_1, h_2) + (-1)^I(J_1, J_2)$
7. Endure with probability $\frac{1}{N_{max}}(-\frac{\|f\|^2}{2\blacksquare^2})cosh(\frac{(sig,J}{\blacksquare^2})$
8. Else restart
9. $sig2 \leftarrow (|r|_\propto - |r - sig2|_\infty)modP$
10. **Return** $(sig1, sig2, ch)$

From the above pseudocode, h_1, h_2 are sampled random polynomials with Gaussian distribution of $GD_\blacksquare.ch$ denotes challenge vector which exploits Fiat-Shamir transform to petitioning hash function, the hash function returns length α binary vector and approximate hamming weight of Hk. Greedy SC generates ch which contains secret key. Based on the sample random bit I, the result is added or subtracted by polynomials h_1, h_2.

4.2 Energy Aware Fuzzy Clustering

The connectivity between mobile nodes is improved by implementing cluster based management of environment. The mobile nodes (MN) in the network are clustered by Enhanced Fuzzy C Means Clustering (EFCM) based on the F_{tors} factors such as link quality (linQ), available energy (ene), distance (DIS), and direction (DIR) in which the cluster head (CH) possess increased energy and has linked with every other node in the cluster that can be formulated as

$$CH(MN)_{ene}^{linQ} > MNs \tag{1}$$

In EFCM, the initial step is to define centre of cluster. The cluster centre is defined based on two parameters, such as local density (μ_j) and distance $(\in_j)$, which can be formulated as

$$\mu_j = \sum_i X(D^{ij} - T^D) \tag{2}$$

where, D^{ji} is distance between sample points j and i, and T^D represents truncation distance that stratifies

$$X(x) = \begin{cases} 0, & \text{x < 0} \\ 1, & \text{x} \geq 0 \end{cases} \tag{3}$$

. The $\forall_i$ can be formulated as

$$\forall_j = min_{i;\mu i \geq \mu_j}(D^{ji}) \tag{4}$$

For a maximum density points, $\forall_j$ can be calculated as,

$$\forall_j = max_i(D^{ji}) \tag{5}$$

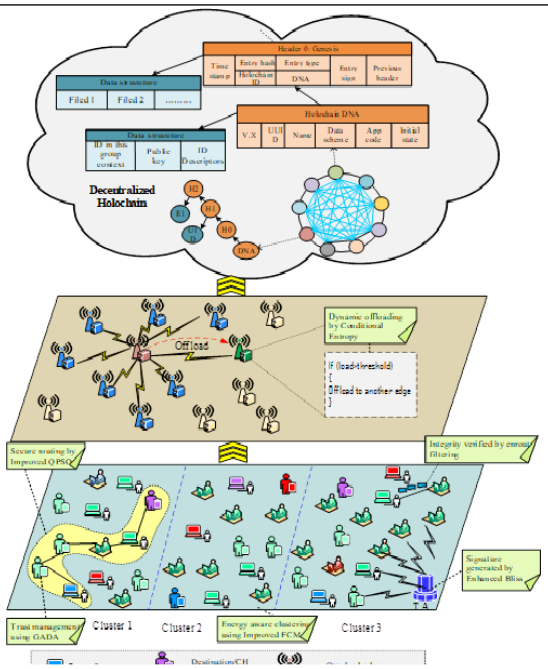

Figure 1: Architecture of Hsec-Route Model

From the above two parameters, index of density distance can be computed as

$$\exists_j = \mu_j \forall_j \tag{6}$$

The $\exists_j$ is found out by navigating all sample points (sp), then find the first H points by cataloguing all $\ni_j$ in the downhill order. The average density distance can be computed as

$$\exists_{avg} = \frac{1}{H}\sum_{j=1}^{H} \exists_j \tag{7}$$

The larger valued points are more likely to be a centre of cluster i.e. $\exists_j > \exists_{evg}$. The centre of cluster is defined by above equation (6), the selected centre of cluster is integrated to Fuzzy C-means Algorithm (FCM) to acquire clusters. FCM employs unsupervised learning approach, which is based on optimization of objective functions. FCM exploits iteration optimization that divides dataset, the results of clusters is numerical value of each point which signifies degree of membership to the centre of cluster. Let Mobile nodes $MN = \{MN_1, MN_2, ..., MN_L\}$ is the collection of L data in which for every samples MN_i has K features. The L can be divided into F fuzzy groups, which are represented as $Z = \{Z_1, Z_2, , Z_F\}$. The FCM objective function can be formulated as

$$R(B,Z) = \sum_{j=1}^{G}\sum_{i=1}^{L}(b_{ji})^{fe}(ED_{ji})^2 \quad (8)$$

From the above equation, $B = (b_{ji})$ is the affiliation matrix of dimension $L \times F, b_{ji}$ that denotes affiliation between Z_j and $MN_i, (ED_{ji})$ is Euclidean distance between sample i and cluster centre $j.fe(fe > 1)$ is the exponent of fuzzy, which can be usually fixed as 2 in the algorithm. The above objective function equation can satisfy the following conditions:

$$\begin{cases} \sum_{j=i}^{F}(b_{ij} = 1, & \text{i=1,2,....L} \\ 0 \le b_{ij} \le 1, & \text{i=1,2,....,L; j=1,2,..,F} \\ 0 < \sum_{i=1}^{L} b_{ij} < L, & \text{j= 1,2,...., F} \end{cases} \quad (9)$$

By using iterative function, minimum objective function is obtained, the B and Z can be computed by

$$b_{ij} = \left\{ \frac{1}{\sum_{cc=1}^{F} \frac{ED_{ji}{}^{1/fe-2}}{Dcc_i}} \right. \quad (10)$$

$$Z_j = \left\{ \frac{\sum_{i=1}^{L}(b_{ij})^{fe} MN_i^{Forts}}{\sum_{i=1}^{L}(b_{ij})^{fe}} \right. \quad (11)$$

The proposed clustering approach minimizes the complexity and overhead in forwarding of packets and control messages in the network. The data provided by each node in the network are aggregated by CH and transmitted to the above layers for computation. The overall clustering process is shown in Figure 2.

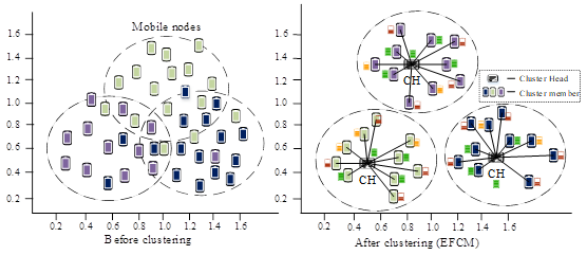

Figure 2: EFCM based Clustering.

4.3 Secure Optimal Routing

The routing of messages from cluster members (CM) to cluster head is carried out in this process. The network is considered to possess malicious attackers whose prime purpose is to disturb effective communication between nodes in the network. Keeping in mind of this context, secure routing of messages is performed that involved two phases, (i) trust management and (ii) optimal forwarder selection. The trust metric (O_T) of each node in the network is computed to select a legitimate node as a forwarder. The trust management comprises of two trust values, namely direct trust and indirect trust. The direct trust (D_T) is computed by respective node based on its history of communication (H_I) and successful transactions (S_T). The calculation of direct trust is defined as follows:

$$D_T = \sum_{i=1}^{n} H_I, S_T \quad (12)$$

The indirect trust (I_T) is computed using Holochain assisted TA by considering feedbacks of neighboring nodes (F_n) of particular node.

$$I_T = \sum_{i=1}^{n} F_T \quad (13)$$

$$O_T = \sum D_T + I_T \quad (14)$$

The Grey Absolute Decision Analysis (GADA) is adopted to rank nodes based on trust values. If N represent criteria count $(c(i); i = 1, 2, N), M$ represents the subject count $(S_i = 1, 2, , M)$ and T represents alternatives count $(a_j; j = 1, 2, T)$. The GADA algorithm includes the following process, decision matrix $[d_ij]$ decides highest criteria that is against each a_j which is defined as follows:

$$[d_{ij}] = \begin{bmatrix} e_1 \\ \vdots \\ e_M \end{bmatrix} \begin{bmatrix} d_{11} & \cdot & d_{1T} \\ \vdots & \ddots & \vdots \\ d_{M1} & \cdot & d_{MT} \end{bmatrix} \quad (15)$$

For every lower criteria, use reciprocate operator to the input data, hence the decision matrix is defined as follows:

$$[u_{ij}] = \begin{bmatrix} e_1 \\ \vdots \\ e_M \end{bmatrix} \begin{bmatrix} u_{11} & \cdot & u_{1T} \\ \vdots & \ddots & \vdots \\ u_{M1} & \cdot & u_{MT} \end{bmatrix} \quad (16)$$

Then, compute grey relational grade between e_i and other $eT; i = 1, 2, ..M$, which is known as comparison matrix $[\rho]$ of absolute grey relation pair. If ρ value is 1 then it denotes better consistency, if ρ value is 0.5 then it denotes lower consistency, hence the value of e_i is always one, which is defined as

$$\begin{bmatrix} c_1 \\ \vdots \\ c_N \end{bmatrix} \begin{bmatrix} \rho_{11} & \cdot & \rho_{1T} \\ \vdots & \ddots & \vdots \\ \rho_{M1} & \cdot & \rho_{MT} \end{bmatrix} \begin{bmatrix} \propto_1 \\ \vdots \\ \propto_M \end{bmatrix} \begin{bmatrix} \sqrt{\propto_1} \\ \vdots \\ \sqrt{\propto_M} \end{bmatrix} \quad (17)$$

where $\propto_i = 1/M(\rho_{i1} + \rho_{i2}. + \rho_{iM})$, for N criteria, $c(i); i = 1, 2, ., N$. Then, perform weight aggregation consider individual criteria weight value is defined as follows:

$$\begin{bmatrix} e_1 \\ \vdots \\ e_N \end{bmatrix} \begin{bmatrix} d'_1(1) & \cdot & d'_T(1) \\ \vdots & \ddots & \vdots \\ d'_1(N) & \cdot & d'_T(N) \end{bmatrix} \quad (18)$$

where, every criterion $c(i)$ and for $j = 1, 2, T$,

$$d'_j = \left(\prod_{j=1}^{T} d_j'^{\propto(i)} \right)^{\frac{1}{\sum_{i=1}^{M} \propto i}} \quad (19)$$

Weight aggregation performed for getting entire ranking of alternatives is calculated as follows:

$$\begin{bmatrix} d" \\ D" \\ rank \end{bmatrix} = \begin{bmatrix} d"_j & \cdot & d"_j \\ D"_j & \ddots & D"_j \\ -- & \cdot & -- \end{bmatrix} \quad (20)$$

where,

$$d"_j = \left(\prod_{j=1}^{T} d"_j^{\delta(i)} \right)^{\frac{1}{\sum_{i=1}^{M} \delta i}} \quad (21)$$

Finally, the proposed GADA provides alternative relative weights $(d'_j, d"_j$ and criteria $\delta(i)$. The trust values are ranked using GADA algorithm.

The second phase is optimal forwarder selection in which selection of next hop forwarder is executed based on parameters, such as link stability (l_s) , bandwidth (b), energy (E), Trust (O_T), queue length (l_q), and relative velocity (R_v). The selection of next forwarder is performed by implementing Improved Quantum Particle Swarm Optimization (IPSO). The ideal forwarder possesses maximal bandwidth, link stability, energy and trust, minimal relative velocity and queue length. The initial position of particles defined as follows:

$$\mathrm{U}_{id}(t+1) = U_{id}(t) + c_1 R1_{id}(t)(p_{id}(t) - Y_{id}(t) + c_2 R2_{id}(t)(G(t) - Y_{id}(t))y_{id}(t+1) \quad (22)$$

$$= Y_{id}(t) + U_{id}(t+1) \quad (23)$$

Where U_{id} and Y_{id} represent velocity and position respectively, and R1,R2 represent random numbers with uniform distribution [0,1], and c1 and c2 coefficient of acceleration. For every time, the particles moved at d dimension from one position to another position. The positions are updated periodically. The process of evolutionary includes three process, VIZ. mutation process, crossover process, and selection process. The Improved QPSO is defined as follows:

$$Q_{id}^t = \Phi Pbest_{id}^t + (-\Phi).Gbest_d^t \quad (24)$$

$$Best_d = \frac{1}{n} \sum_{i=1}^{n} Pbest_{id} \quad (25)$$

$$x_{id}^{t+1} = Q_{id}^t \pm \propto | \, Best_d - Q_{id}^t \, | \, .Ln(\frac{1}{v_{id}^t}) \quad (26)$$

Where Φ represent random value between (0,1) and Q_{id} represent the random position between $Gbest$ and $Pbest$. The final position is calculated as follows:

$$\mathrm{x}_{id}^{t+1} = \Phi.(Pbest_{id}^t - Gbest_{id}^t) + Pbest_{id}^t \pm \propto | \, Best_d - x_{id}^t \, | \, .Ln(\tfrac{1}{v_{id}^t}) \quad (27)$$

For every particle, i in the present particle swarm select two random particles, which are difference from l, j and $i \; l \; j$, the position difference between j and l is defined as follows:

$$\delta = x_l - x_k \quad (28)$$

The fitness calculation is performed to select optimal node for next forwarder which is defined as follows:

$$F = \sum w(l_s + b + E + O_T + l_q + R_v) \quad (29)$$

In this way, routing is performed successfully between CH and CM for data transmission. The integrity of messages sent by source node before forwarding to next forwarder is validated by means of En-route filtering to determine legitimacy of source node and if message is found to be from a dishonest node then it will be pruned by forwarder node. It is used to detect and drop malicious information from the path (source to destination). The major aim of enroute filtering is to improve integrity of nodes. The signature is verified by enroute filtering for detecting malicious nodes in the routing path. If verification is success then the node will forward the message to the destination. If verification is failed then the node is considered malicious and the information will be dropped from the malicious nodes. Fig. 3 represents flowchart of the secure routing, which includes process of ranking, routing, and integrity verification.

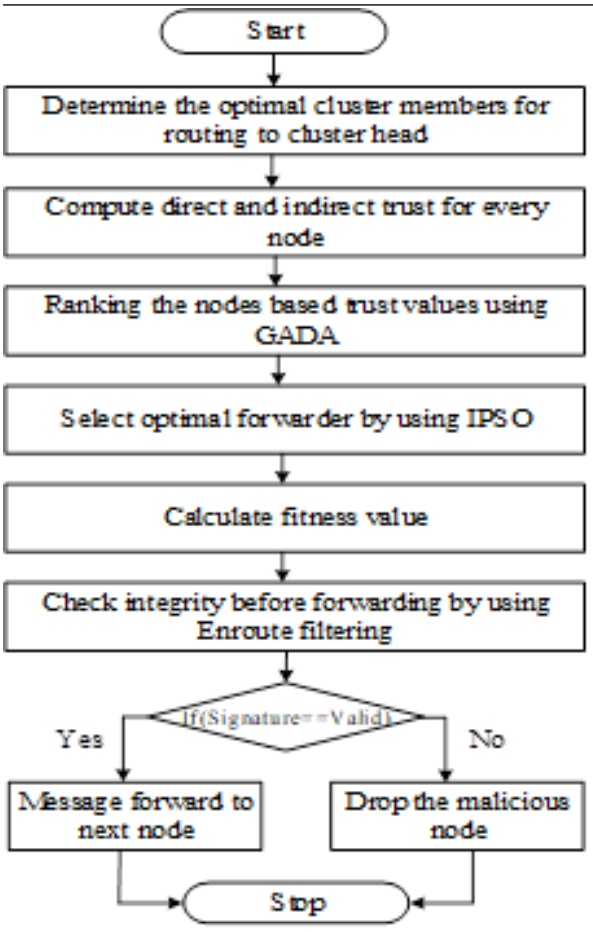

Figure 3: Flowchart of Secure Routing.

4.4 Dynamic Task Offloading

The CH transmits aggregated data collected from the CMs to the edge server for computation. The edge server considers these data as tasks and performs computation of tasks to provide increased throughput with minimal latency. In a large scale network with vast number of mobile nodes, the edge nodes get overloaded and tasks in the edge node should be offloaded to other edge node or the cloud node. This process is carried out by optimally selecting the edge node to which the tasks in the overloaded node should be offloaded. The optimal edge node is selected by considering load (L), distance (H), and energy (Æ[a]). For optimal edge node selection, threshold value is generated. If the threshold is exceed then offloading is performed. Threshold is generated by conditional entropy, which is defined as follows,

$$V = \sum L, \Im, \jmath \tag{30}$$

$$H(V) = -\sum_{i=1}^{n} P(V_i) log P(V_i) \tag{31}$$

$$= \begin{cases} \text{if H(V)} < 0.5\,, & 1 \\ \text{if H(V)} \geq 0.5, & 0 \end{cases} \tag{32}$$

where, H represents entropy that provides threshold value, and 1 represent offloading and 0 represent not offloading. This ensures increased throughput and minimal latency even in a large scale network.

Offloading ();
Begin
Initialize $E_i = E_1, E_2, .., E_n$
Initialize L, $\Im, \jmath$
For every E_i do
Compute L, $\Im$ and $\jmath$
Compute threshold value using (30)
If (Th<0.5) then
Perform offloading
Else
Not perform offloading
End if
End

4.5 Attack Mitigation by Holochain

In MANET environment, routing is performed efficiently to maximize privacy of nodes and minimize transmission delay. However, several nodes (i.e. malicious nodes) try to obtain sensitive information from data packet. In this work, Holochain is implemented to increase security by mitigating numerous types of attacks present during routing and it is used for performing authentication processes. Holochain is mainly used to overcome major drawbacks of blockchain, such as high computation complexity and storage by its resource constrained nature. The Holochain is a completely distributed network that preserves data and information of the nodes in an effective manner. Holochain is found to be more scalable and less complex thereby enabling it suitable for resource constraint environment. In Holochain, communications between the mobile nodes are stored as transactions and the integrity of transactions is validated by the respective agents without being verified by all the nodes in the network. This property of Holochain resists against several consensus based attacks. It reduces security risks with peer to peer network and distributed ledger technology for improving energy efficiency. The major advantage of holochain network is to ensure individuality by an individual ledger even it performs communication with

other respective peers to perform computing in fully distributed manner. Holochain stores communication information by each agent in the form of transactions with the help of source code and validation rules in a local manner. The holochain structure is otherwise called as source chain which consists of multiple agents and each agent consists of three major components, such as DNA, genesis, and holochain blocks (i.e. transactions). The explanation of these components are described as follows:

DNA: It consists of unique validation rules set for each holochain applications and it is applied to every nodes present in the network to verify network integrity without the need of global consensus.

Genesis: Creating hash to assure that the holochain applications follows the predefined validation rules and such hash is called as genesis, which is stored after DNA in the source chain. It has two specific entries in which the first entry is the DNA hash and the second entry is the ID of agents that consists of public key of nodes.

Holochain Blocks: Each transaction are generated as blocks and stored in local chain based on entry. Every entry consists of various components in their header, such as entry type, hash data, timestamp, hash value of existing header, and digital signature. In general, the block consists of header, node ID and node private data. Holochain increases security with less complexity and storage, which overcome the drawbacks of blockchain in terms of following metrics,

- High Scalability
- Better Consensus Mechanism
- Low Complexity
- Efficient Communication Resource
- Low Network Traffic

Table 1 describes the comparison between the blockchain and holochain technologies.

Table 1: Holochain vs Blockchain

Characteristics	Blockchain	Holochain
Consensus	POS, POW, PBFT, DPOS	No consensus is needed
Chain approach	Global information stored in blocks	Information stored in separate agents
Chain consists	Consists whole ledger data	Consists a part of whole ledger data
Handling of error	Rejecting data	Rejecting data and blacklisting node
Scalability	Minimum	Maximum
Integrity of data	Validate by Miners	Validate by past cryptographic record
Mining approach	Essential	Non-Essential
Utilization of energy	High	Low
Redundancy of data	Extreme	Optimal
Transition degree	Maximum 1000/s	Maximum 56000 bps/Hz
Transition shared with	All nodes	Some nodes
Cryptocurrency	Bitcoin	Holo fuel
Processing cost	Maximum	Minimum

5 EXPERIMENTAL RESULTS

This section deals with experimentation of proposed Holochain based Secure optimal Routing (HSec-Route) for providing security to MECs and achieve QoS. This section is further divided in to sub-section as follows,

5.1 Simulation Setup

The performance of the proposed HSec-Route is evaluated in NS-3 simulation tool of version 3.26 that has system configuration of software specifications and hard ware specifications. In software specifications, the network simulator used is NS-3.26 and operating system used for experimentation is Ubuntu- 14.04 LTS (32 bit — primary single OS only).

Table 2: Simulation Setup

Parameter	Value
# of mobile nodes	100
Time taken for simulation	800 s
Model for mobility	Random way point
# of edge nodes	4
# of Holochain	1
# of trusted authority	1
Area of simulation	1000m x 1000m
Node connection range	100m
Bandwidth of the channel	3Mbps
Varying packet size	64 512 bytes
Varying mobility nodes(%)	10% 60 %
Data rate	512-2048 bits/secs
Range of transmission	200
Initial energy (J)	200 J

In hardware specifications, the processor used is Intel(R) Core(TM) i5-4590S CPU 3.00 GHz 3.00 GHz, Random Access Memory storage capacity is 8 GB, and hard disk capacity is 60GB. Table 2 shows configurations used for the simulation in proposed HSec-Route approach.

5.2 Comparative analysis

In this sub-section, evaluation of the proposed HSec-Route method based on Holochain security model with various metrics regarding QoS is described. The proposed HSec-Route method is compared with several existing methods, such as Block-Trust and EDM-IoT

by considering several performance metrics, namely packet delivery ratio, security strength, end to end delay, routing overhead, throughput, attack prediction rate, route acquisition delay, and energy consumption respectively.

5.2.1 Impact of Packet Delivery Ratio

Packet delivery ratio (PDR) is defined as ratio of total number of packets transmitted by the source node ψ to number of packets delivered at the destination node λ. The formulation of packet delivery ratio is expressed as follows:

$$P = \frac{\psi}{\lambda} \tag{33}$$

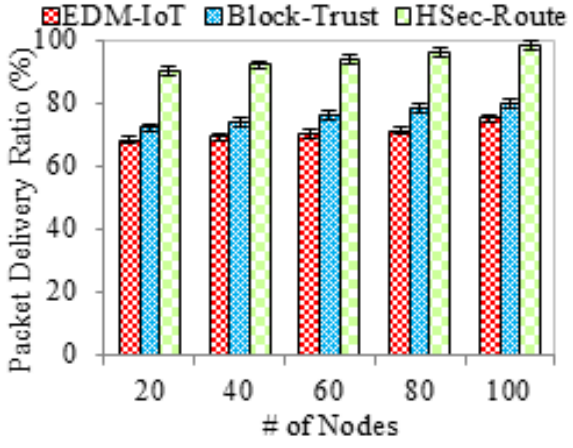

Figure 4: Comparison of Packet Delivery Ratio

Fig. 4 illustrates comparison of packet delivery ratio of number of nodes between proposed HSec-Route method and several existing methods. Increasing number of nodes increases packet delivery ratio. In EDM-IoT method, transmission of data was performed by port hopping mechanism however, limited number of ports in network increases transmission overhead that increases the data loss, which decreases packet delivery ratio. To overcome transmission overhead, optimal forwarder node is selected using IPSO algorithm in the proposed HSec-Route method to improve packet delivery ratio. The result shows that packet delivery ratio of the proposed HSec-Route method is 23%, which is greater than the existing methods.

5.2.2 Impact of Security Strength

This metric is used to analyze security level in transmission of data packets. High security strength indicates effective security during data transmission.

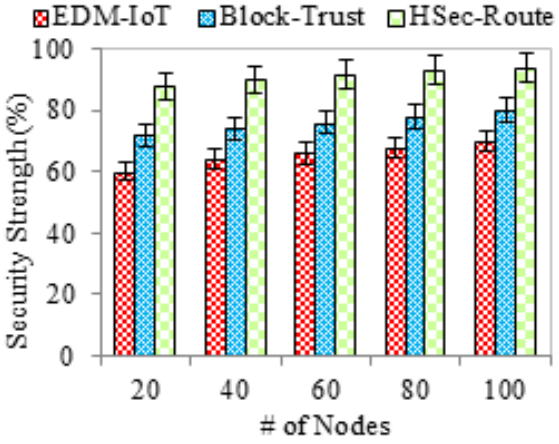

Figure 5: Comparison of Security Strength.

Fig. 5 illustrates comparison of security strength to number of nodes between the proposed HSec-Route method and existing methods. Increasing the number of nodes increases the security strength. EDM-IoT method focused on providing security of critical nodes however, security of general nodes was not considered that reduces security strength. In the proposed HSec-Route method, safe transmission of data is performed by encrypting data packets using bliss algorithm and holochain is used to improve the security which increases the security strength when compared with the existing works. The result shows that the proposed HSec-Route method achieves 94% of security strength, which is 24% greater than existing approaches.

5.2.3 Impact of End to End Delay

End to end delay is defined as amount of time taken by the data packet to transmit from source node to the destination node. The formulation of end to end delay is represented as follows:

$$D_{-} = \eta^{-} - u' \tag{34}$$

where, denotes the data packet delivery time and Æ° represents fixed transmission time. Fig. 6 represents the comparison of end to end delay of number of nodes between proposed HSec-Route and state-of-the-art works. End to end delay increases with increasing the number of nodes. In Block-Trust method, information of nodes is gathered from a single node that increases complexity which increases the end to end delay. In proposed HSec-Route method, optimal selection of forwarder nodes for routing and management of network by holochain based on distributed ledger decreases end to end delay when compared to existing

works. The comparative results illustrates that the proposed HSec-Route method achieves low end to end delay, which is 10 ms lower than existing methods.

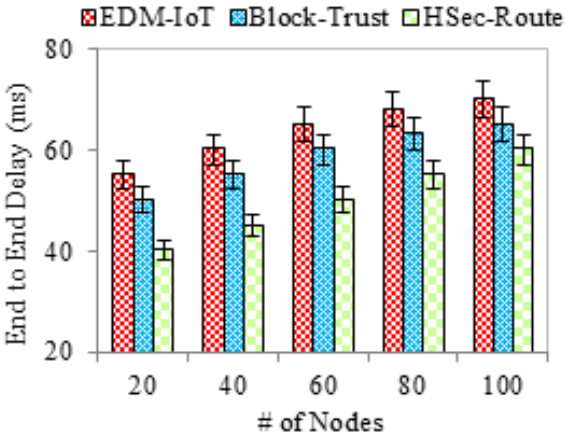

Figure 6: Comparison of End to End Delay.

5.2.4 Impact of Routing Overhead

Routing Overhead is defined as ratio of number of data packets produced for selecting routes (d') to number of data packets transmitted (t). It also referred as number of routing packets used to discover and maintaining routes. The formulation of routing overhead is represented as follows:

$$o = \frac{d'}{t} \tag{35}$$

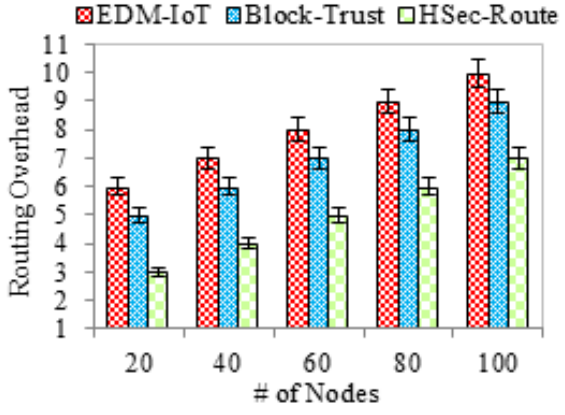

Figure 7: Comparison of Routing Overhead

Fig. 7 shows comparison of routing overhead of number of nodes between proposed HSec-Route method and previous methods. Routing overhead increases with increasing number of nodes. Selecting random hops increases the probability of retransmission which increases routing overhead. In addition, the existing methods transmit the data to the cloud server this increases the routing overhead. In the proposed HSec-Route method, the CH aggregates the data from the CMs and transmits the aggregated data to the edge server for computation. The result illustrates that the proposed HSec-Route method achieves low routing overhead when compared to previous works.

5.2.5 Impact of Throughput

Throughput is defined as ratio of the amount of data transmitted from the sender node to receiver node at a specific time interval. The computation of throughput is expressed as follows,

$$\jmath = \frac{\delta}{\theta} \tag{36}$$

where, δ represents time for data delivery and θ denotes amount of data, which are send from transmitter to receiver.

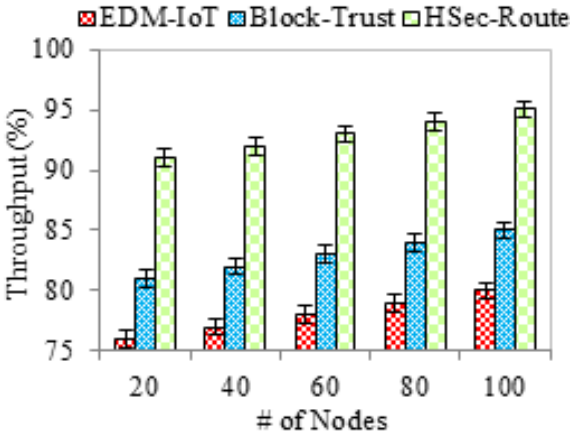

Figure 8: Comparison of Throughput.

Fig. 8 shows comparison of throughput of number of nodes between the proposed HSec-Route method and several previous methods. Increasing the number of nodes increases the throughput. In the existing works, route selection is performed by finding the shortest distance to transmit data without considering any security to the nodes that increases the packet loss which decreases the throughput. In the proposed HSec-Route method, edge server is used to reduce the complexity and dynamic task offloading is performed to avoid overhead of edge server which increases the throughput efficiently when compared with the existing works.

The comparison result shows that the proposed HSec-Route method achieves 95% of throughput which is 15% greater than the previous approaches.

5.2.6 Impact of Attack Prediction Rate

Prediction of attacks is performed based on values (i.e. true positive). Attack prediction rate is defined as the ratio of the number of attacks predicted to the total number of attacks. The formulation of attack prediction rate is expressed as follows,

$$\wp = \frac{r}{n} \tag{37}$$

Where, r denotes the number of attacks predicted and n

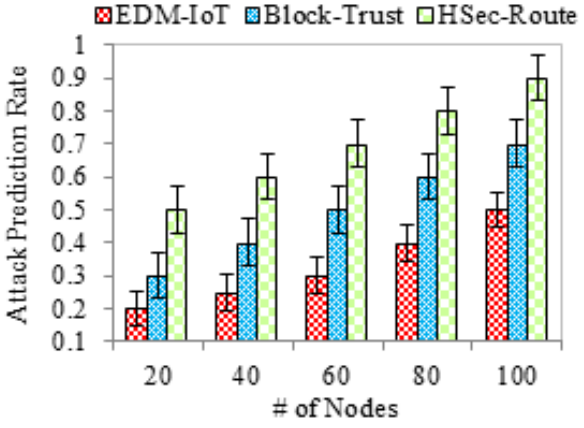

Figure 9: Comparison of Attack Prediction Rate

represents the total number of attacks. Fig 9 illustrates the comparison of attack prediction rate to the number of nodes between the proposed HSec-Route and the previous state-of-the-arts. Increasing the number of nodes increases the attack prediction rate. EDM-IoT method attains partial security due to providing securing only for critical nodes that decreases the attack prediction rate. In the proposed HSec-Route method, authentication and encryption of data is performed to improve the security. Holochain is used to mitigate various attacks such as grey hole attack, black hole attack etc., which increases the attack prediction rate. The comparative result shows that the proposed work achieves high attack prediction rate when compared with previous methods.

5.2.7 Impact of Route Acquisition Delay

Route acquisition delay is defined as amount of time taken between sending the route request (RREQ) to the destination node by the source node and getting the route reply (RREP) from the destination node. Lower the time interval increases QoS of network. Fig. 10 represents comparison of route acquisition delay to the number of nodes between proposed HSec-Route method and several previous works. Increasing the number of nodes increases route acquisition delay. Existing method perform routing based on optimal selection of shortest routing paths that increases complexity when large scale scenario. To improve the routing performance, efficient clustering of nodes is performed by EFCM clustering algorithm with optimal CH selection and optimal forwarder selection is performed in proposed HSec-Route method to reduce the latency, number of retransmissions and increase packet delivery ratio which decreases route acquisition delay when compared to existing works. The comparison result shows that the route acquisition delay of proposed work is reduced, which is 20 ms lower than existing works.

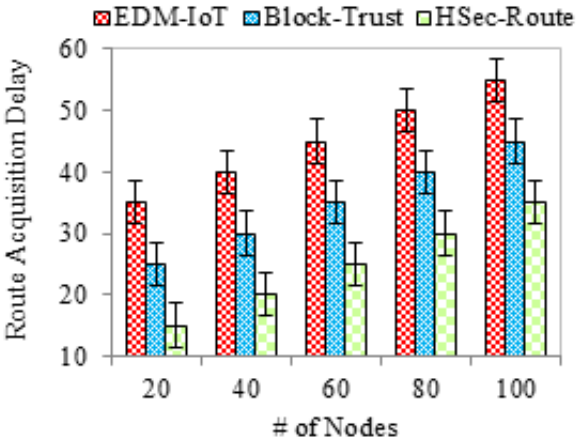

Figure 10: Comparison of Route Acquisition Delay.

5.2.8 Impact of Energy Consumption

Energy consumption is defined as difference of nodeâs initial energy to the residual energy of node after performing data packet transmission. This metric can be measured as follows:

$$E^{\cdot\cdot} = \mho - \eth \tag{38}$$

where, $\mho$ denotes initial energy and $\eth$ denotes residual energy. Fig. 11 shows comparison of energy consumption to number of nodes between proposed HSec-Route method and previous methods. The consumption of energy increases when increasing number of nodes. In Block-Trust method, blockchain was used to calculate trust value of nodes however, mining time increases in large scale environment that increases the energy

consumption. In the proposed HSec-Route method, holochain based distributed ledger is used to increase security that reduces complexity. In addition, optimal forwarder selection is performed using IPSO algorithm that reduces latency and packet delivery ratio which minimize the energy consumption. The result illustrates that proposed HSec-Route method consumes low energy which is 20 kW lower than existing works.

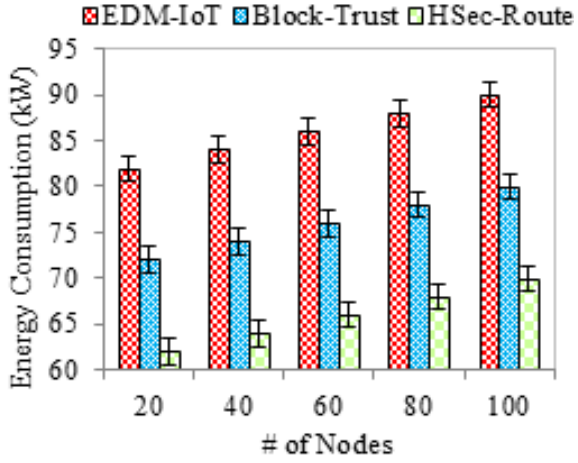

Figure 11: Comparison of Energy Consumption.

5.3 Security Analysis

The security of transmitted messages are considered in this work because, data transmitted in MANET network are sensitive in nature. Routing and privacy problems are raised due to the various attacks and these attacks are caused by malicious nodes. Numerous attacks are mitigated in MANET network by performing several processes in the proposed HSec-Route method and such attacks are described as follows:

Black Hole Attack: The nature of this attack is to attract sender node to transmit data packets through this malicious node by minimum number of hop routes. Once source node transmits data packets to malicious node, it drops packet on the way without transmitting it to next forwarder node. This increases transmission delay between nodes. To overcome this attack, direct and indirect trusts are performed in the proposed HSec-Route method to identify trust value of nodes thereby mitigating the malicious nodes with false trust value.

Grey Hole attack: The malicious nodes perform this type of attack by acting like a general node (i.e. legitimate). If the source node sends data through this node, it drops sensitive data packets only thereby it is difficult to recognize this attack. In this proposed work, this attack is identified with the help of indirect trust by symmetrical pattern and this attack will be mitigated by eliminating such malicious nodes when forwarding data packets.

Intruder Attack: In this attack, attackers are present outside the network. They enter into MANET network by manipulating legitimate node present in the respective network. Then they attract source nodes to drop packets, which increases security threat for sensitive data. The proposed HSec-Route method performs authentication by considering multiple attributes, such as PUF, MAC address, etc., to secure network from this attack.

Worm Hole Attack: This attack creates a structure by multiple nodes in the shape of tunnel to reduce the hop count of the routing path. If the source node transmits the packet through this structure, that node is attacked by this attacker that results in replay attacks and denial of service (DoS). This attack is mitigated in the proposed work by the selection of CH considering high energy and link stability. The CH has all the CMs link information and identifies the malicious node easily by this information

6 CONCLUSION AND FUTURE WORK

The secure, and energy efficient MEC based MANET-IoT framework by achieving QoS constraints for addressing problems in the existing works are performed in the present work. All mobile nodes in the network are authenticated to Holochain assisted centralized TA ensure their legitimacy by considering multiple attributes in which TA exploits improved BLISS algorithm for key generation to mobile nodes. The legitimate nodes are clustered by EFCM algorithm to enhance connectivity between nodes by considering factors, such as link quality, energy availability, distance, and direction. Once clusters are formed, CH selection is to minimize energy consumption in which CH is selected based on energy availability and link quality. After forming clusters and selecting CHs, secure optimal routing is taken place between Cluster Members (CMs) and CHs in which two phases are performed namely trust evaluation phase and optimal forwarder selection phase. Both direct trust and indirect trust is computed for every mobile node is carried out in trust evaluation phase, and based on trust values ranking of mobile is done by using GADA algorithm. By exploiting ranking trust values and other metrics, such as bandwidth, link stability, queue length, and relative velocity optimal forwarder is selected using IPSO algorithm. All mobile nodes in MANET-IoT environment are checked for integrity by En-route filtering before transmitting or receiving mes-

sages from other mobile nodes. After secure optimal routing, aggregated data from CH are provided to MEC for processing. If MEC node is found to be overload then offloading to another MEC node or cloud is performed using conditional entropy. Finally, Holochain saves the every transaction of the mobile nodes and mitigate several attacks. The proposed work achieves better performance than the existing works in terms of validation metrics. Future directions will be to improve the scalability by constructing an efficient network topology.

7 Bibliography

1. Gowrishankar, J & Kumar, P Narmadha, T & Natarajan, Yuvaraj. (2020). A Trust Based Protocol For Manets In Iot Environment. 29. 2770-2775.

2. Song, Y., Luo, H., Pi, S., Gui, C., & Sun, B. (2020). Graph Kernel Based Clustering Algorithm in MANETs. IEEE Access, 8, 107650-107660.

3. Bhardwaj, A., & El-Ocla, H. (2020). Multipath Routing Protocol Using Genetic Algorithm in Mobile Ad Hoc Networks. IEEE Access, 8, 177534-177548.

4. Simpson, S.V., & Nagarajan, G. (2021). A fuzzy based Co-Operative Blackmailing Attack detection scheme for Edge Computing nodes in MANET-IOT environment. Future Gener. Comput. Syst., 125, 544-563.

5. Veeraiah, N., Ibrahim Khalaf, O., Rajendra prasad, C., Alotaibi, Y., Alsufyani, A., Alghamdi, S.A., & Alsufyani, N. (2021). Trust Aware Secure Energy Efficient Hybrid Protocol for MANET. IEEE Access, 9, 120996-121005.

6. Krishnan, C.G., Gomathi, S.S., AnushaBaminiA., M. (2021). High energy efficient lifetime management system and trust management framework for manet using self-configurable cluster mechanism. Peer-to-Peer Netw. Appl., 14, 1229-1241.

7. Muruganandam, S., J, A. (2021). Real-time reliable clustering and secure transmission scheme for QoS development in MANET. Peer-to-Peer Netw. Appl., 14, 3502-3517.

8. Wang, X., Zhang, P.F., Du, Y., Qi, M. (2020). Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network. IEEE Access, 8, 47675-47693.

9. Chen, Z., Zhou, W., Wu, S., Cheng, L. (2020). An Adaptive on-Demand Multipath Routing Protocol With QoS Support for High-Speed MANET. IEEE Access, 8, 44760-44773.

10. Pattnaik, P.K., Panda, B.K., Sain, M. (2021). Design of Novel Mobility and Obstacle-Aware Algorithm for Optimal MANET Routing. IEEE Access, 9, 110648-110657.

11. Tu, J., Tian, D., Wang, Y. (2021). An Active-Routing Authentication Scheme in MANET. IEEE Access, 9, 34276-34286.

12. Singh, U., Sharma, S.K., Shukla, M., & Jha, P. (2021). Blockchain-based BATMAN protocol using Mobile ad-hoc Network (MANET) with an Ensemble Algorithm.

13. Careem, M.A., Dutta, A. (2020). Reputation based Routing in MANET using Blockchain. 2020 International Conference on COMmunication Systems NETworkS (COMSNETS), 1-6.

14. Rani, P.L., Kavita, .., Verma, S., & Nguyen, G.N. (2020). Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network. IEEE Access, 8, 121755-121764.

15. Alghamdi, S.A. (2020). Three-Tier Architecture Supporting QoS Multimedia Routing in Cloud-Assisted MANET with 5G Communication (TCM5G). Mob. Networks Appl., 25, 2206-2225.

16. Serhani, A., Naja, N., Jamali, A. (2019). AQ-Routing: mobility-, stability-aware adaptive routing protocol for data routing in MANETâIoT systems. Cluster Computing, 23, 13-27.

17. Sathyaraj, P., & Devi, D. (2021). Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method. J. Ambient Intell. Humaniz. Comput., 12, 6987-6995.

18. Li, T., Ma, J., Pei, Q., Song, H., Shen, Y., & Sun, C. (2019). DAPV: Diagnosing Anomalies in MANETs Routing With Provenance and Verification. IEEE Access, 7, 35302-35316.

19. Zhang, D., Chen, L., Zhang, J., Chen, J., Zhang, T., Tang, Y., & Qiu, J. (2020). A Multi-Path Routing Protocol Based on Link Lifetime and Energy Consumption Prediction for Mobile Edge Computing. IEEE Access, 8, 69058-69071.

20. Jhaveri, R., Patel, N.M., Zhong, Y., & Sangaiah, A.K. (2018). Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT. IEEE Access, 6, 20085-20103.

21. Ran, C., Yan, S., Huang, L., & Zhang, L. (2021). An improved AODV routing security algorithm based on blockchain technology in ad hoc network. EURASIP Journal on Wireless Communications and Networking, 2021, 1-16.

22. Son, B., Lee, J., & Jang, H. (2020). A Scalable IoT Protocol via an Efficient DAG-Based Distributed Ledger Consensus. Sustainability, 12, 1-11.

23. Tahboush, M., & Agoyi, M. (2021). A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET). IEEE Access, 9, 11872-11883.

24. Dilipkumar, S., & Durairaj, M. (2021). Epilson Swarm Optimized Cluster Gradient and deep belief classifier for multi-attack intrusion detection in MANET. Journal of Ambient Intelligence and Humanized Computing, 1-16.

25. Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S.A., Khalaf, O.I., & Subbayamma, B.V. (2021). An Improved Hybrid Secure Multipath Routing Protocol for MANET. IEEE Access.

26. Singh, P., Khari, M., Vimal, S. (2021). EESSMT: An Energy Efficient Hybrid Scheme for Securing Mobile Ad hoc Networks Using IoT. Wireless Personal Communications.

27. Elhoseny, M., & Shankar, K. (2020). Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique. IEEE Transactions on Reliability, 69, 1077-1086.

28. Mendonça, R. V., Teodoro, A. A., Rosa, R. L., Saadi, M., Melgarejo, D. C., Nardelli, P. H., & Rodríguez, D. Z. (2021). Intrusion detection system based on fast hierarchical deep convolutional neural network. IEEE Access, 9, 61024-61034.

29. Akhtar, N., Khan, M., Ullah, A., & Javed, M.Y. (2019). Congestion Avoidance for Smart Devices by Caching Information in MANETS and IoT. IEEE Access, 7, 71459-71471.

30. Khan, B.U., Anwar, F., Olanrewaju, R.F., Kiah, M.L., & Mir, R.N. (2021). Game Theory Analysis and Modeling of Sophisticated Multi-Collusion Attack in MANETs. IEEE Access, 9, 61778-61792.

31. Niu, Z., Li, Q., Ma, C., Li, H., Shan, H., & Yang, F. (2020). Identification of Critical Nodes for Enhanced Network Defense in MANET-IoT Networks. IEEE Access, 8, 183571-183582.

32. Lwin, M.T., Yim, J., & Ko, Y. (2020). Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. Sensors (Basel, Switzerland), 20.