Bi-Fitness Swarm Optimizer: Blockchain Assisted Secure Swarm Intelligence Routing Protocol for MANET

Haridas .S

Research Scholar, Hindustan Institute of Technology and Science, Chennai.India
Assistant Professor, Dept. of Computer Science,Government First Grade College, Tumkur, Karnataka.
Email: harigoleson@gmail.com

Dr.A. Rama Prasath,

Assistant Professor (Selection Grade), Department of Computer Applications,
Hindustan Institute of Technology and Science, Chennai, India.
E-mail: mraprasath@gmail.com

Abstract

Mobile Ad Hoc Networks is a communication network between devices without infrastructure and random mobility of device and hence proper management of nodes and security provisioning is a vital task and challenging that affects the quality of service (QoS). The proposed work has the following processes: (1). Zone-wise Authentication by using BLAKE-3 hashing algorithm and deployment of guard nodes throughout the network. (2). Environmental aware Clustering is performed by Rewards Optimized Deep Q Learning (RoDQL) algorithm. (3). Secure Priority based Routing is presented by Particle Swarm Optimization (PSO) method. In this step, bi-fitness optimizer is used. Finally (4) Sensitivity Aware Data Encryption algorithm is used to evaluate the sensitivity level of a packet and encrypted using blockchain based SALSA 20. The simulation is conducted by using NS3.26 network simulator that computes the performance in terms of QoS metrics.

Keywords: **BLAKE-3, SALSA-20, Secure Routing, and Bi-Fitness Optimizer**

1. Introduction

Mobile Ad Hoc Network (MANET) is a specific kind of ad hoc network that does not has any central entity to control communication. This network consists of group of mobile devices with limited resources as energy and power. Hence, it is failed when handling of computational high tasks. Further, this issue is a major that due to nodes dynamically enter / leave to the network. On account of this issue, node communication link was broken and thus packets forwarded between source to the destination will be dropped. There are various characteristics of MANET such as Dynamic Network Topology, Resource Constrained Capability, Open Medium, Distributed Co-operation and Frequent Mobility Change. On other hand, without communication infrastructure adversaries can launch different kinds of malicious behaviors throughout the network. Thus, it becomes important to address security issues in MANET.

There are numerous reasons to develop a secure MANET model for mobile users since unauthorized mobile devices participated in network for the aim of launching attacks (e.g. spoofing attacks). In routing, black hole and grey hole attackers [Rani P et.al.,2020] are possible to drop packets. In such situation, trustworthiness of node must be evaluated before data transmission. In view of security necessities, now it is clear that security is a mandatory requirement in MANET and security model avoids the attacker's involvement. Furthermore, to security, other challenges [Haridas. S & Rama Prasath. A (2020)] involving in MANET for QoS improvement are as follows. (1). High packet transmission ratio (2). Low packet loss ratio, (3). Low energy consumption and (4). Low latency

1.1 Motivation and Contributions

Routing attacks are common in MANET. To reduce any malfunctions by adversaries (packet loss, and latency) in MANET, trust management (node authentication and data confidentiality) and message authentication (Data Integrity) is invoked in network via blockchain technology.

In MANET, Quality of Service (QoS) decides the overall performance of the network. In any application, the MANET aims to achieve better QoS. In MANET the secure routing is performed using AODV, OLSR and other trust based routing protocols. This does not ensure security fully. In addition, cryptography based trusted routing is not efficient to determine misbehaving nodes in cluster based MANET. Further, trust values can be easily

modified by malicious users. Thus, blackhole and grey hole attack mitigation is not effective. Under high mobility, attackers moving are rapidly increasing so that attack detection and mitigation by historical behaviors are highly harder. Further, the route selection is based on the type of the packets was not well-known. Since all type of transmission is possible in MANET, disaster packets require short delay while the normal transmission is bearable to some amount of time delay. Furthermore, it is difficult to control the authentication process through a single entity. Due to the above issues, most important QoS metrics are affected such as Packet Delivery Ratio, Throughput, Residual Energy, End-to-End Delay and Routing Overhead. To make the communication between source node to the destination node in MANET, energy efficient, secure, decentralized and trusted scheme is required for information sharing. The primary objectives of this research are listed as follows:

- To obtain high QoS, energy-efficient clustering and secure routing mechanism is presented over distributed environment.
- To minimize energy consumption of individual nodes, clustering is constructed using Rewards Optimized Q-Learning
- To maximize the packet delivery ratio (PDR), minimum hop-count based optimum route is established from source to the destination nodes.

The Zone based [Krishnan R.S *et.al*., 2020] Blockchain consensus model is proposed in this paper for secure routing and mitigates the security attacks. To reduce the congestion among nodes in authentication, multiple Guard nodes are deployed. The main contributions of this paper are follows:

- Authentication is carried out by strong set of parameters as ID, PWD, MAC address, Biometrics (Eye Vein), which is hashed by Multicriteria Blake3 authentication algorithm. Block information is stored in terms of hash values and it's computed by Blake 3 algorithm.
- Environment aware Clustering is proposed which uses rewards optimized deep Q learning that considers energy status, number of neighbors, mobility and distance.
- For secure route selection, Bi-Fitness Swarm Optimizer is used where two swarm intelligence algorithms are used such as PSO and Artificial Swarm Intelligence. Due to the local optima issue, stable parameters are considered in PSO and others are given to the ASI method.
- Secure Priority Aware Routing is proposed which first send disaster packets to the destination node and also as per the sensitivity level of packets, it is encrypted using Salsa20 algorithm with different bits of security.

The performance of the proposed work is evaluated with respect to Attack Detection Rate, False Positive Rate, End-to-End Delay, Packet Delivery Ratio, Energy Consumption, Throughput, Routing Overhead Ratio, and Security Strength Ratio.

1.2 Paper Organization

The rest of this paper is structured as follows: In section II, related work is presented in detail with respect to each work's deficiencies and limitations. The problem definition is clearly stated in Section III, which describes the overall problems existed in previous works. Section IV presents the proposed work description with algorithm procedure and pseudocode. Section V discusses the experiment results for the proposed work and the performance is analyzed and compared to previous works for various metrics and finally it is proved that the proposed work is superior to the existing works.

2. Related work

An evolutionary self-cooperative trust (ESCT) scheme is presented [Cai Ruo et al., 2018] for trusted routing. This scheme uses direct neighbor nodes to exchange trust information and voting is given to nodes by their behaviors. And also self-detection is possible in which trust value is detected and updated in routing table. In this stage, mobile nodes compute confidence value than number of neighbor's information. Therefore, all nodes in the network are authorized since authority identity is assigned to each mobile node via dynamically exchange of hello packets between nodes. In this work, authentication is not effective because authority identity is generated by malicious nodes. The exchange of dynamic hello messages consumes more energy consumption. The trust values can be generated through malicious nodes since it is downloaded in packet header. A cooperative blackhole attack detection model was proposed [El-Semary Aly & Diab Hossam ,2019] where two nodes are participated together to affect the network. To protect blackhole attackers, secure AODV is designed in this paper, which uses Chaotic Map features. These features are added to mobile nodes pair (source and destination). Each route request consists of validation set of parameters. Weak set of parameters are not helpful to mitigate / detect blackhole attackers. In [Li, T. et al.,2019] author proposes a new model namely diagnosing anomalies with provenance and verification in routing under MANET environment. It is shortly referred as DAPV. This will detect both direct and indirect attacks occurred by adversary during routing. There are two techniques are involved in this DAPV such as (1). First collect log information of peers in the network, (2). Privacy preservation by merkle hash tree (MHT). This

mitigates many attacks such as IP spoofing attack, SSL attack, DOS attack, ARP spoofing attack, and Gateway monitoring attack. Frequent update of logs for peers in MANET is required to detect attacks since attack patterns change over a time. A reliable data transmission model was presented in [Elhoseny M & Shankar K ,2019] with high level of security in MANET. In this work, nodes are clustered by utilizing energy efficient routing protocol. Then, the Modified Particle Swarm Optimization is proposed for selecting optimal cluster head. A signcryption based secured routing protocol is applied for reliable and secure data transmission. With the varying number of nodes in the network, the proposed method has attained high level performance with the PDR (92.22%), network lifetime (111hours), and energy consumption (92J). Then, the accuracy of attack detection is 80 to 82% and also security level of 93%. In this work, cluster head was selected by PSO, which increases time to elect and also it, does not optimal. An energy efficient cloud assisted routing was established in [Riasudheen H et al.,2019]. Here, energy consumption rate is reduced by Fast Local Route Recovery among peer nodes and mobile nodes. When the link failure occurs, then backup nodes identified in the coverage to perform routing. Similarly, when mobile node request service from cloud via neighbors, services are scheduled and services retrieved to mobile nodes. For this situate, alternate path is selected using residual energy. Energy is the only considered parameter for routing, which does not optimal since it moves suddenly from the coverage. A cross centric based intrusion detection system was proposed by [Rajendran N et al.,2019] in secure routing for black hole attack detection. There are three processes are involved in this paper such as path origin selection, priority portion assignment (PPA) and attack reduction by IDS. For path origin selection, PIHNSPRA routing algorithm is used which chooses the path from end to end nodes with secure way and minimizes black hole attack. Node position is maintained in the priority portion assignment issue and past interaction history is managed. Trust value becomes modified by attackers since more number of attackers located in diverse regions. A simple secret key based symmetric encryption was used in [Usman M et al,2018]. This work prevents the legitimate nodes to avoid data reception from any malicious nodes. In determined path, attacker's presence is ensured between source to the destination. The simulation results proved that the proposed scheme protects nodes from malicious behaviors and shows good performance in terms of key generation, encryption, storage and communication costs. A lightweight scheme is proposed for trust interference management [Xia H et al.,2020] in mobile ad hoc environment. Trust assessment and prediction is considered in this paper that assesses the trust values based on historical behaviors. A weighted stochastic chain measure (1, 1) is presented that predicts nodes trust model for future decision making. In the conventional protocol i.e. on demand multicast routing protocol (ODMRP), four kinds of trustworthiness is added which consider the trust issue and improved with present a novel trust based routing protocol i.e. on demand trust based multicast routing protocol (ODTMRP). This work lacks from the confidentiality, integrity and authentication. Hence, trustworthiness is not effective in this work. Authors proposed a security model for MANET [Hurley-Smith D et al.,2017]. In particular, SUPERMAN model was presented which is called as pre-existing routing for MANET. The major functions of this model are Node Authentication, Access Control, and Communication Security. For secret key management, Diffie Hellman Exchange algorithm was used. Data packets encrypted by means of authenticated encryption with associated data (AEAD), which is an encryption algorithm that provides integrity, authenticity and confidentiality services. When data packets were protected then it forwards to the destination via multiple hops and it was authenticated to each hop by hashing HMAC algorithm. Hence the SUPERMAN protocol was satisfied the access control, authentication, non-repudiation and confidentiality. Access control and authentication was achieved using trusted authority, which is easily compromised when attackers involved in network. Further, routing was established by Dijisktras algorithm which provides the blind search among multiple hops.

In [Harold Robinson Y & Golden Julie E ,2019] infinitely repeated game and cooperation approach was established that finds the attackers. The objective of the proposed game theory model is to accurately predict the attackers which results high energy efficiency. The security-based route establishment improves the routing performance. The payoff is computed for every node and it identifies the malicious node at every iteration. The nodes belief value was updated for every action and it minimizes the severity caused by malicious nodes. In this work, selfish nodes rate is high that increases the packet drop rate.

A multipart trust basis public cryptography mechanism [Harold Robinson Y & Golden Julie E ,2019] was presented in MANET that minimizes the security issues. An optimal trust threshold value was proposed that dynamically change the trust values based on the public key usage. This paper does not use trusted third party for key generation and storage. Further, mutual trust relationship was predicted between the requesting node and certificate issuer node. The proposed trust-based model proves the performance in terms of security and availability.

3. Problem statement

This section summarize the main problems existed in the current works of security and QoS improvement in MANET. In [Ponguwala Maitreyi & Rao Sreenivasa ,2019], energy efficient secure routing (E2SR) was proposed that detects and mitigates routing attacks in MANET. The main problems in this work are follows: (1). This work

consumes more energy and computational power and also it requires more processing time. The reasons behind these pitfalls are follows. (1). To elect dual CH, each mobile node is involved. This increases rate of energy consumption, (2). All data packets are encrypted twice by two encryption algorithms, which increases computational complexity and induce end-to-end delay for disaster packets. (3). For secure route selection, worst case PSO is used which is suited for solving static optimization issues, but it is not efficient when functioned in dynamic networks. Since optimum value will change frequently when environment changes and node movement change in high rate. In this situate, gbest value must change in dynamically. (4). Authentication is carried by weak set of mobile node's credentials as ID and PWD, which are easily forgeable and increases vulnerability to the nodes. Hash chain based authentication requires more time and energy consumption. A secure multi-path based routing protocol was proposed in [Veeraiah N & Krishna B T ,2020]. In this work, cluster head election, intrusion detection and then secure routing was proposed. Secure nodes are selected by bird swarm optimization algorithm. Authors proposed a blockchain based trust management model in [Lwin May *et al*.,2020]. For routing, the optimized link state routing protocol -OLSR[Kanagasundaram *et.al*.,2018] is employed in which every hop is selected by trustworthiness. The problems in this paper are follows: (1). When the number of mobile nodes increases, then overhead is high at validator nodes selection due to forwarding of more control messages. (2). Frequent validator node selection is often possible since it's selected on the basis of high trust value and also its complex for high dense network. (3). Due to the use of OLSR based routing, energy consumption rate and bandwidth becomes high. (4). Block creation process also introduces high energy consumption because hash generated for block transactions is performed by double SHA algorithm. A new routing protocol was presented which is called Modified Ad Hoc on Demand Multipath Distance vector (AODMV) that defends against black hole attacks. This work does not effective in mitigation of black hole attack since full packet drops can be computed by the trustworthiness of a node, which requires historical behaviors to categorized as attacker or normal. The main drawback of this scheme from energy consumption point of view because multi paths routing adds complexity to both source and destination. Homomorphic encryption has greater computational costs due to its in-built complexity. This generated large ciphertext which pose challenges to data during transmission and also it increases the energy consumption. To summarize, in this paper we addressed the following research questions:

- *RQ1:* How to assurance for data packets while transmitting in a route?
- *RQ2:* How to ensure security and privacy for mobile nodes?
- *RQ3:* How to manage and organize data packets in blockchain environment?
- *RQ4:* How to make route prediction time to be faster and accurate when choosing the best next hop?

4. Proposed work

4.1 System Model

In the proposed work, Blockchain assisted Secure and Swarm Intelligence method-based routing protocol is presented with the following processes.

- Multi-Criteria based Authentication
- Environment Aware Clustering
- Secure Priority based Routing
- Sensitivity Aware Data Encryption

A MANET physical infrastructure is consisting of number of mobile devices, guard nodes and blockchain technology. Guard nodes are deployed in different zones and each zone consists of number of clusters.

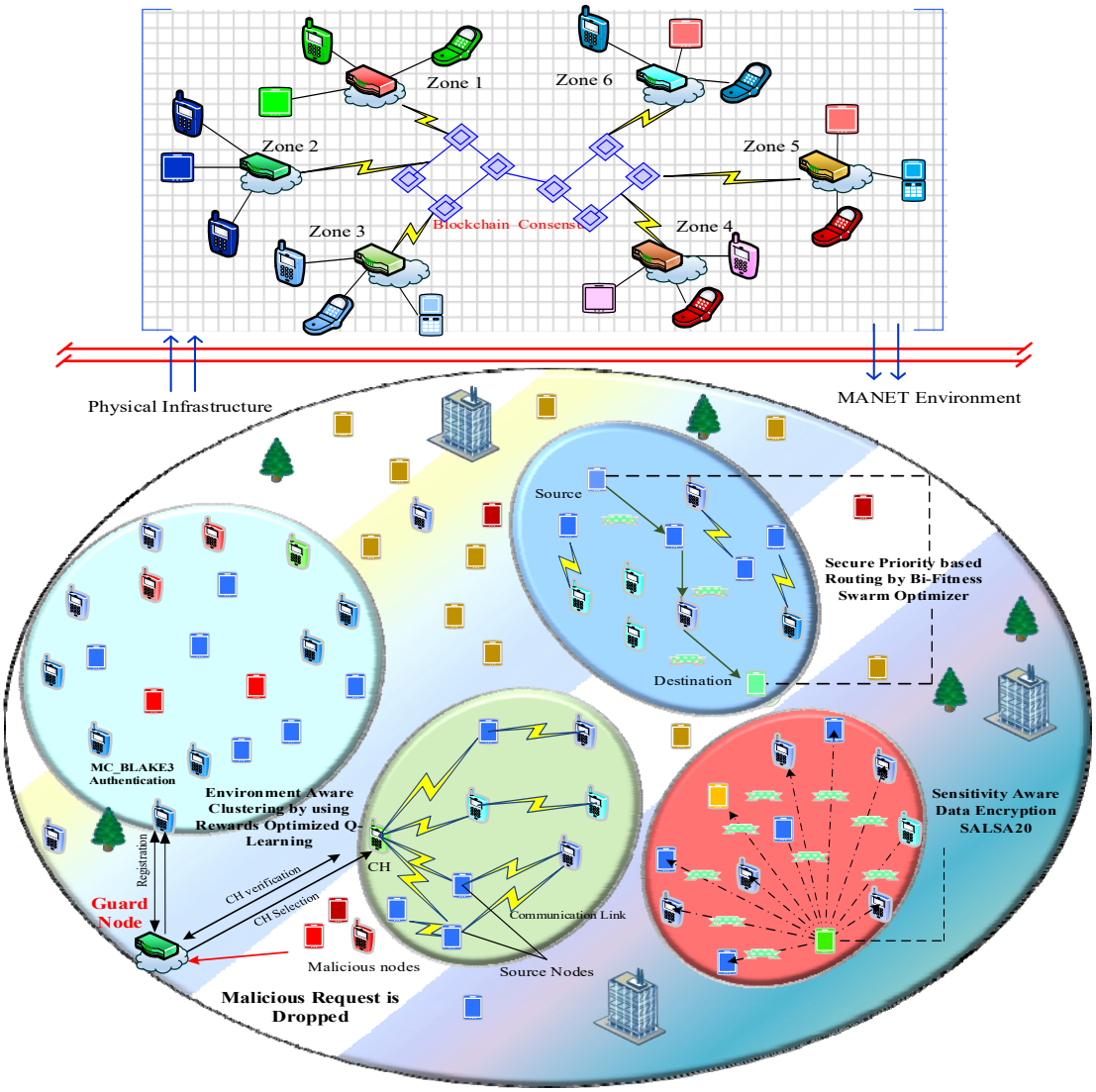

Fig.1.Proposed System Architecture

4.2 Multi Criteria based Authentication

Guard node is deployed in network for authentication and CH election, which suited for large environment. Authentication is carried out by strong set of parameters as ID, PWD, MAC address, Biometrics (Eye Vein), which is hashed by Multi-criteria Blake3 authentication algorithm. Block creation is implemented by Blake 3 algorithm that performs hashing by less number of rounds. Blake 3 is a cryptography algorithm that provides more advantages such as faster than SHA-1, 2, and 3, MD5 and Blake 2. It is secured than MD5, and SHA-1. BLAKE 3 algorithm is highly parallelizable and it is capable of huge data hashing. The proposed BLAK 3 generates the hash values for security credentials. For authentication, 256 bits are used and 4×4 matrix, which is formulated by,

$$m = \begin{pmatrix} S_0 & S_1 & S_2 & S_3 \\ S_4 & S_5 & S_6 & S_7 \\ S_8 & S_9 & S_{10} & S_{11} \\ S_{12} & S_{13} & S_{14} & S_{15} \end{pmatrix} \qquad (1)$$

Where m is a matrix for ensuring the security. It denotes the 32bits of words and totally 12 cycles are executed and 8 groups of computation are implemented for computing hashes.

The process of blake3 algorithm is explained below,

a) $A = A + B + M_{\sigma_R}(2i)$
b) $D = (D \oplus a) \gg 16$
c) $C = C + D$

d) $B = (B \oplus C) \gg 12$
e) $A = A + B + M_{\sigma_R(2i+1)}$
f) $D = (D \oplus A) \gg 8$
g) $C = C + D$
h) $B = (B \oplus C) \gg 7$

Where σ_R represents permutation, $\oplus$ represents the XOR operator, which uses for lightweight processing. From the hash values, privacy is preserved.

4.3 Environment Aware Clustering

We considered cluster-based environment which minimizes complexity and overhead in packets and control messages forwarding. Environment aware Clustering is proposed which uses rewards optimized deep-Q-learning (RoDQL) that considers energy status, number of neighbors, mobility and distance.

Clustering consists of two processes such as cluster formation and cluster management. In cluster formation, the network splits into different clusters. In each cluster, one node is elected as a CH and others are members of CH. CH are elected using several metrics. The prime motive of clustering is to efficient use of energy resources, maintain and manage routing, and location issue for solving communication and computational complexities. There are two types of cluster maintenance are given follows:

- inter cluster maintenance – For packet forwarding/routing using more CHs
- intra cluster maintenance – For packet forwarding/routing within a cluster.

CH has the complete responsibility to monitor and manage all the nodes during packet forwarding within a cluster. Clustering is a hierarchical networking scheme that employs flat topology. In this paper, cluster heads are elected by RoDQL algorithm and it is managed by guard nodes.

a) **Distance:** It is defined by the distance between two nearest nodes. Assume that d_{ij} is the distance between node i and j. It is computed based on its angular position information $angle\ (\theta_2, \theta_1)$ and radius information (r_2, r_1). It is expressed as:

$$d_{ij} = \sqrt{r_1^2 + r_2^2 - 2r_1 r_2 cos(\theta_2 - \theta_1)} \qquad (2)$$

b) **Node Mobility:** It is defined by the node speed. However node mobility is computed for dynamic network topology and it cause several issues such as link breakage, route failure and degrades network throughput due to increase of mobility. It is expressed as:

$$S_{n_i} = \frac{1}{T}\sum_{t=1}^{T}\sqrt{x(t) - x(t-1)^2 + y(t) - y(t-1)^2 + z(t) - z(t-1)^2} \quad (3)$$

Where S_{n_i} is the nearest node speed, which is calculated for each node in the network with coverage and $x(t) - x(t-1)$,$y(t) - y(t-1)$, & $z(t) - z(t-1)$ are the coordinates of the node at time t and t-1.

c) **Residual Energy Level:** It is defined by level of energy that nodes consist after certain process at a time scale t. A level of energy per bit/byte consumed for node i at time t. It is expressed as:

$$RE_{n_i} = E_P - E_T \qquad (4)$$

Where RE_{n_i} is the node residual node, E_P is the power consumption of the node in the network, and E_T is the transmission power of a node. Therefore energy consumption of a mobile node is expressed as:

$$C_E(i) = \left[T_p \times \frac{d_s}{d_r} - R_p \times \frac{d_s}{d_r}\right] + i \times L_0 \qquad (5)$$

where $C_E(i)$ is the energy consumption of node i, T_p is the power spend for transmission, d_s is the data size, d_r is the data rate, R_p is the power for receive and L_0 is loss due to overhearing.

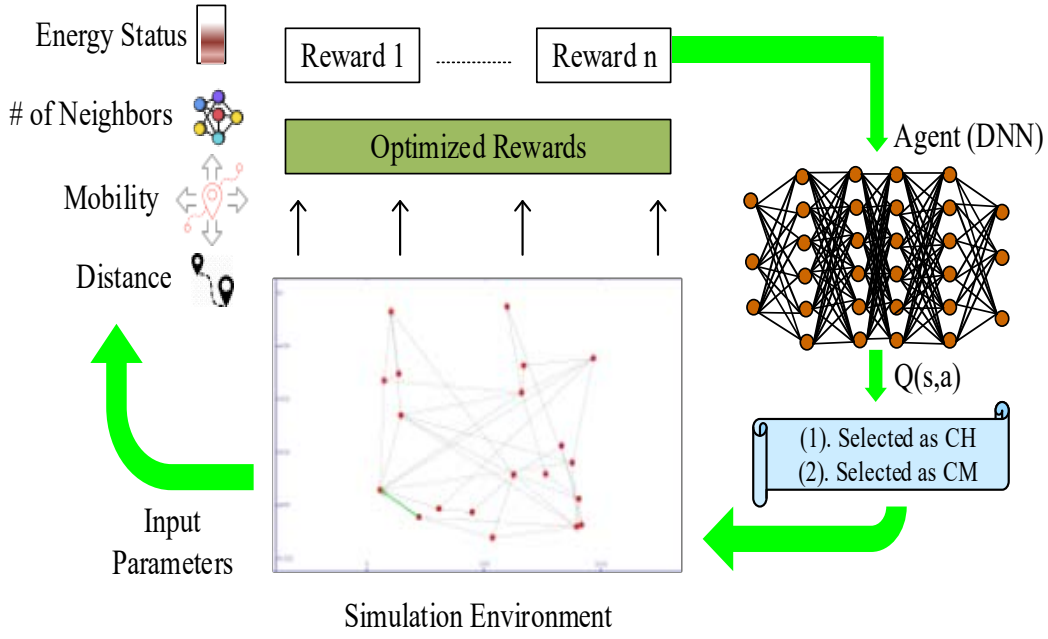

Fig.2.Flow of RoDQL algorithm

In this work, number of neighbors is known as node relative degree D_p which is computed by,

$$D_p = \left| d_p - \sqrt{N} \right| \quad (6)$$

where d_p is the node density which is computed by:

$$d_p = \begin{cases} 1 & 0 < D_{pq} < R \\ 0 & otherwise \end{cases} \quad (7)$$

RoDQL algorithm follows three principles such as (1) utilize deep neural network for representing the policy, value functions and model, (2). Optimize the policy, end-to-end model and value functions, and (3). It uses stochastic gradient descent. Fig 2 depicts the RoDQL algorithm.

For each node in the network N_i $i = \{1,2, \dots n\}$, the MDP model consists of following elements:

$$N_i = (1,2, \dots n) = \begin{Bmatrix} States\ (S_i), Actions\ (A_i), Transition\ Model\ (T_i), \\ and\ a\ set\ of\ Reward\ functions\ (R_i) \end{Bmatrix} \quad (8)$$

In a given time scale t, the state $S_{i,k} \in S_i$ of N_i is the residual energy of node RE_{n_i}, trust values Tr_{n_i}, distance d_{n_i}, transmission distance Td_{n_i}, delay D_{n_i}. The description of the reinforcement learning algorithm is follows:

a) **States S_i:** For each node N_i, states of nodes computed and change by the node RE_{n_i}, Tr_{n_i}, d_{n_i}, Td_{n_i}, and D_{n_i}. In this model S_i denotes the available set of state transitions in the environment. This element results any of the node as next hop (1st relay node R_1) for packets transmission from the source node.

b) **Actions A_i:** This denotes the set of agents action or behavior in a given time period t. It may possible to change from current state to the next state. All set of actions A_i are self-possessed by all the nodes energy value that each node can choose the next node. Thus the finite set of actions is follows:

$$A_i = \left\{ RE_{ni,k} | RE_{ni,k} \{0, \delta_k, 2\delta_k, \dots, RE_{max,k}\} \right\} \quad (9)$$

Where δ_k is the step size. For any node the possible action covers: (1) Choose one of the nodes from the set of possible nodes (2). Data packets are terminated and never route the packets.

c) Transition Model T_i: This model is depends on the action and states transition. It defines the state transition probabilities from state $S_{i,k}$ to $S_{i+1,k}$ and the state transition probability function is defined in below:

$$T_i = S_i \times A_i \times S_i \rightarrow [0,1] \quad (10)$$

From the result of the action $a_t \in A_i$. The selection probability of a particular forwarder node is a basis of neighboring node routing score.

d) **Reward functions R_i:** It is also known as reinforcement function, which purpose is to compute the immediate action a_t. It represents the state transition from one state to another state. It is computed as:

$$\rho_i = S_i \times A_i \times S_i \rightarrow R \quad (11)$$

In this stage, routing policy π_k maximize throughput of each node by reward functions. Routing policy is mapped from the given $S_{i,k}$ to $\rho_{i,k}$ that should be elected and it is written by:

$$\rho_{i,k} = \pi_k(S_{i,k}) \quad (12)$$

π_k is determined using action value function such that $Q_k^{\pi}(S_{i,k}, \rho_{i,k})$. It is an exact reward function computed starting from state $S_{i,k}$, and $\rho_{i,k}$.

The optimal policy π_k^* is the policy whose value function is greater than or equal to any other policy for all states. The final action value for the optimal policy π_k^* is also known as Q_k^* and $Q_k^*(S_{i,k}, \rho_{i,k})$ is an optimal action for the selection of large probability score at every hop that increases reward function at all the destination

If any attack patterns found by guard node, then it will immediately isolate the particular malicious node and inform this message throughout the network.

4.4 Secure Priority based Routing

Secure Priority Aware Routing is proposed which first send disaster packets to the destination node and also as per the sensitivity level of packets, it is encrypted using Salsa20 algorithm with different bits of security. For secure route selection, Bi-Fitness Swarm Optimizer is used where two swarm intelligence algorithms are used such as PSO and Artificial Swarm Intelligence [Rosenberg Louis & Willcox Gregg. (2019).]. Due to the local optima issue, stable parameters are considered in PSO and others are given to the ASI method. In first fitness swarm optimizer, node's residual energy, and delay is considered for path selection. In second fitness swarm optimizer, node's trust value, link stability, are forwarded to ASI method. In particular, node's trust value is computed by the packet forwarding & receive rate, average forwarding delay, control dropping rate, load and energy consumption rate. *Each parameter definition is follows:*

(i). DEFINITION ($packet\ forw\&\ receive\ rate\ PfR_r$): This rate is identified by proportion by the sum of packets transmitted effectively to sum of packets forwarded in a given time period. The best example for such situation is black hole attackers. These attackers received low packets forwarding and transmitting phase.

(ii). DEFINITION ($average\ forwarding\ delay - af_D$): The amount of time is required to transit packets between two nodes and the sum of total time is the average forwarding delay that is computed based on packet forwarding until the destination is received. The unit of this factor is the seconds (sec). Similar to the load factor, the normalization is also required in the average forwarding delay. For e.g. suppression attackers will cause huge delay in packets forwarding.

(iii). DEFINITION ($protocol\ deviation\ flag - pd_f$): It reflects the abnormal behavior of nodes during packets forwarding. The output of protocol deviation flag is either 0 or 1. It is a logical value, which expressed by nodes regulation. However, the protocol deviation flag is determined using any security approach since this will identified any misbehaviors of node. The logical value 1 indicates that node affected by abnormal behaviors, otherwise it is 0.

(iv). DEFINITION ($load - l$): The amount of bytes received by a node in time slot (t) at current traffic. The unit of load is the bits per second (Bits/Second). For e.g. DDoS attackers will cause by high load at various time intervals (t), (t+1), (t+2), and so on. Node tolerances related to the load is varied for several functioning of nodes experience and therefore it must be normalized before forwarding to the next hop node.

(v). DEFINITION ($control\ dropping\ rate - cd_r$): It is expressed by the sum of dropped control packets to the sum of control packets to be forwarded in a time scale t. In other words, it is defined by the cumulative rate of control packets dropped rate to the sum of control packets forwarded from time slot 0 to t.

(vi). DEFINITION ($ditch\ rate - d_r$): This factor is not frequently used to deal with trust management problem. It is defined by the total number of times the adjacent node is determined as misbehaving or malicious node. It is computed by the total number of HELLO packets obtained by a neighbor node.

(vii).DEFINITION ($energy\ consumption\ rate - EC_R$): It is the most important factor for trust management among nodes. It is defined as the rate of energy consumption of a node from its initial state (initial energy). If a node contains very less residual energy rate, it may not possible to transit high size of packets to other node.

Energy consumption is varied at time t due to different experiences by the node such as transmission, receive and aggregation. Further, direct and indirect trust values are computed.

Trust value is calculated for the nodes in the network, which is derived by Direct and Indirect Trust metrics. It is computed by:

$$DT_{ij} = \frac{DT_{ij}}{f(t)\max(DT_{ij})} \quad (13)$$

$$IDT_{ij} = \frac{\sum RT_{ij} * D_P * RT_{in}}{\sum \delta(n) * RT_{in}} \quad (14)$$

Where D_P is the centrality degree of reporting node (n) and $f(t)\max$ is the maximum observation of DT_{ij} at time t.

Bit-fitness optimizer is a population-based algorithm that initializes the input and evaluates fitness value.With the result from two optimizers, *Path Eligibility Score* is computed. Hybrid Swarm Intelligence supports well in this work so that low energy consumption rate and bandwidth is also low.

ASI based PSO algorithm taking into account of significant sensor oriented metrics. In general PSO is a bio-inspired computational optimization and search algorithm which is enabled for the identification of an optimal solution. In PSO, the solution obtained from each generation is known as particle. This solution is stored for the purpose of obtaining best solution from the current best values. The fitness value obtained from the best solutions is stored for further comparison. Here *Pbest* is the current optimum fitness value obtained from the population. Then *Gbest* is the optimum solution obtained from the best values generated by the population. In PSO, the velocity of particles is estimated from random variables that are generated by the values of *Pbest*.

If the fitness value is identified to be better that the individual fitness values, then the corresponding value will be replaced with the individual best fitness and the updation of solution is defined as,

$$v(t+1) = v(t) + C_1 \times r() \times (x_{Pbest} - x(t)) + C_2 \times r() \times (x_{Gbest} - x(t)) \quad (15)$$

$$x(t+1) = x(t) + v(t+1) \quad (16)$$

From the above, $x(t)$ and $v(t)$ denotes the vectors of position and velocity for each particle in time t, then C_1 and C_2 defines the constant variables that is based on the self and social learning. Further the generated fitness value is better than global fitness that is represented as x_{Gbest}.

The fitness function expressed in proposed for routing is given in the following,

$$F(1) = W_1 \times N_D + W_2 \times N_{RE} \quad (17)$$

$$F(2) = W_3 \times NT_v + W_4 \times NL_{ST} \quad (18)$$

This fitness function is applied on PSO and ASI for routing the nodes based on the constraints included in the formulation. The metric that are considered are N_d as node degree, N_{RE} as remaining energy of node, D_{ij} as distance between sensor node i to j and N_{TV} as the trust value of the sensor node. Then the weighted values are represented as $W_1, W_2, W_3,$ and W_4 i.e. $W_1 + W_2 + W_3 + W_4 = 1$. Based on these metrics the route is selected for data transmission.

Algorithm 1: Bi-fitness Optimizer

1: Begin
2: Initially the sink node broadcasts hello_messsage
3: Compute fitness value of each particle $Pbest$ and $Gbest$
4: For all particles
5: Update particle position and velocity by (15) and (16).
6: Map new position with the closest x, y coordinates
7: Compute fitness of each particle
8: Update $Pbest$and $Gbest$
9: If iteration =max? then
Output the particles
Else
Increment particles
10: End if
11: End for
12: End

4.5 Sensitivity Aware Data Encryption

This stage shows that the sensitivity aware data encryption before transmission of packets from the source node. When compared to asymmetric encryption, symmetric encryption requires very less energy consumption. In particular, Salsa 20 is a symmetric algorithm that much faster than AES and generated ciphertext is not greater than original size. For sensitive data packets, SALSA 20 (256) is used whereas 128 bits level of security is applied for non-sensitive data packets.

SALSA20 is an ultra-modern stream cipher algorithm for encryption and decryption. It is contains of four functions: quarter_round, row_round, column_round and double_round. It is a high standard algorithm for encryption and decryption purpose. The benefits of SALSA20 algorithm is follows,

- It provides speed performance for encryption and decryption operations, which means that it is three to five times faster than AES
- It mitigates the most common symmetric key for differential cryptanalysis
- It does not required lookup table for each time and it thus it does not cause any complex at any time.
- In order to maximize the encryption speed, AES was expand the key size, which produces Extra Processing Overhead and also increase the key setup.

Totally, three operations are invoked in this paper as Key Stream Generation, Encryption and Decryption. The procedure for the SALSA20 is depicted in fig.3

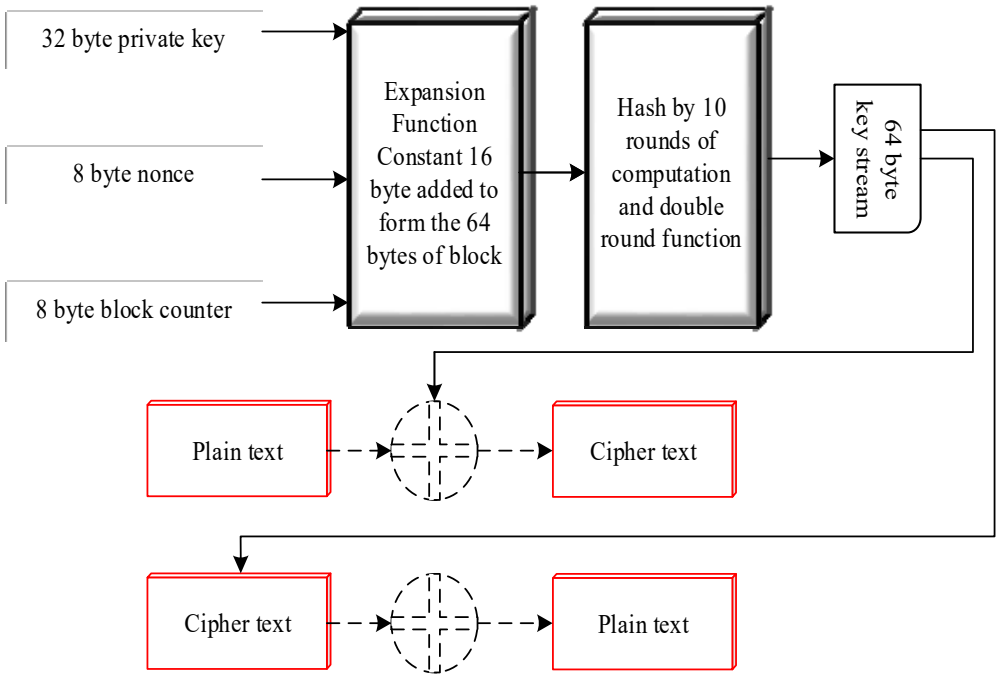

Fig.3.SALSA20 Algorithm

5. Experimental results

This section covers the simulation results with the detailed description of the three sub-sections include simulation setup, comparative study, and results & summary for the proposed model than the previous approaches.

5.1 Simulation Setup

To evaluate our proposed scheme we used NS3. We run the proposed scheme using hardware and software requirements that are illustrated in table.1. This ns-3 tool is equipped with better functionalities of network and supports all the specifications of MANET. Since the nodes in each network is varied and here the mobile node configurations are deployed that senses the circumstances and transmits the data. The proposed blockchain based security model is considered 1000m × 1000m simulation environment for testing different security attacks. The system configuration is depicted in Table 1. The simulation parameters considered for experiments are illustrated in Table 2. In this, we enroll code for the proposed algorithm for creating clusters, establishing routes for data transmission. Energy reduction is a major consideration in many MANET research works and our work also focuses in reducing the energy consumption.

Software Specifications	Network Simulator	NS3.26
	OS	Ubuntu 14.04 LTS
Hardware specifications	Processor	Pentium Dual Core and Above
	RAM	2GB
	Hard Disk	60GB

Table.1. System Configuration

Parameters	Description
Simulation area	1000m*1000m
Number of nodes	100 and 200 with 25% of attackers
Node mobility model	Random waypoint model
Node speed (Max)	5m/s
Forwarding capacity	2Mbps
Transmission range	250m
Number of flows	50
Packet transmission average rate (per flow)	512bytes/packet
Node buffer size	64 packet (fixed)
Nodes distribution	Random
Traffic type	TCP, UDP, and ICMP
Queue type	Priority queue
Interface type	Physical wireless
Duration for packets carrying	1s
Neighbor nodes waiting time	0.3s
Propagation delay mode	Constant speed
MAC type	Ad Hoc Wi-fi MAC

Table.2. Simulation Parameters

5.2 Comparison Study

This subsection describes evaluation of the proposed blockchain based security model in terms of several QoS metrics. The proposed model is compared with state-of-the-art works. In particular, we considered the following performance metrics as attack detection rate, false positive rate, end-to-end delay, packet delivery ratio, energy consumption, throughput, route overhead ratio, and security strength. Table 3 shows the comparison of existing approaches.

Existing work	Contributions	Drawbacks
E2SR [Ponguwala Maitreyi & Rao Sreenivasa ,2019]	(1). A hash chain dependent certificate authentication (HCCA) is proposed for authentication (2). Then clusters are formed and here dual cluster heads are elected for data transmission. (3). Secure route established between the sources to destination via worst case particle swarm optimization algorithm. (4). Data packets are encrypted before transmission to secured path by means of XOR RC6 encryption with fuzzy logic	•Low level security •High processing time (encryption and decryption) •Suitable for Small number of devices •Higher energy consumption
Multi-Path [Veeraiah N & Krishna B T, 2020]	(1). Clustered formed using Fuzzy Naïve Bayes algorithm. (2). Secure nodes are selected by hybrid optimization (BSO + WOA). (3). The selection of optimal route is based on the fitness factors as energy, trust, connectivity and throughput.	•Irrelevant optimization algorithms are combined so it is not an optimum solution. •Higher energy consumption •Higher complexity

Table.3. Drawbacks of Existing Approaches

5.2.1 Impact of Attack Detection Rate

Attack detection rate is the number of events determined as attacks in a given time. However, attacks rate is higher for both small scale and large scale networks. It is computed with the use of true positive values. It is defined as the sum of packets classified accurately as normal as total number of packets are forwarded. It is calculated as,

$$ADR = \frac{\#\ of\ detected\ attacks}{\#\ of\ attacks} \times 100\% \quad (19)$$

$$ADR = TPR = \frac{TP}{TP+FN} \quad (20)$$

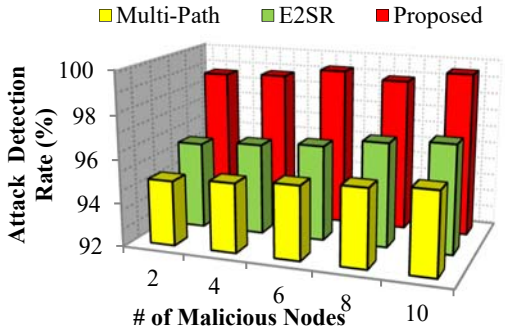

Fig.5.Attack Detection Rate vs. # of Malicious Nodes

With the integration of hybrid swarm optimization algorithms, attack detection rate is improved for our proposed work and it is computed for different number of malicious nodes aspect. This paper primarily focused on routing attacks detection and mitigation i.e. black hole attack, gray hole attacks and spoofing attacks. Firstly, packets are encrypted based on the priority level. In packet header, sensitivity level of packet is mentioned and based on that encrypted and then transmitted secure and optimum path. Fig 5 represents the attack detection rate performance. On completing the packet transmission, attacker's presence is determined before transmission in network. Existing works such as E2SR and multi-path are studied for secure routing. These works generates secret keys frequently and can be easily known by attackers.

5.2.2 Impact of False Positive Rate

False positive rate is computed by the sum of packets that are classified as anomaly in a mistake than number of packets sent. Mathematically, it is computed as follows,

$$FPR = \frac{\#\ of\ misclassified\ processes}{\#\ of\ normal\ processes} \times 100\% \quad (21)$$

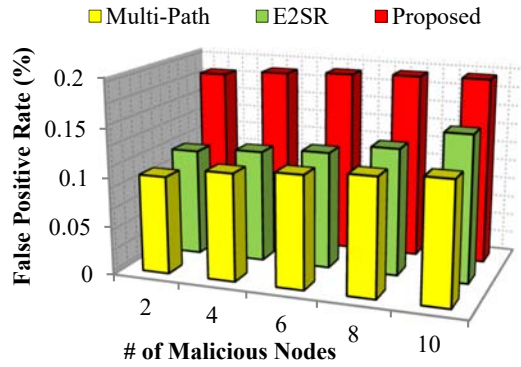

Fig.6.False Positive Rate vs. # of Malicious Nodes

In general, false positive rate is an event based metric that must be represents the accurate prediction by the proposed schemes. When malicious activities are not identified, then it is possible to think that the model gives normal packet pattern as a negative result. The aim of false positive rate is to reduce the misclassification by taking the packet header information. To increase the false positive rate, number of features taken as an input

5.2.3 Impact of End-to-End Delay

In MANET, node mobility and network topology are the key parameters that affect the performance of latency. In this paper, we compute the end-to-end delay with respect to number of malicious nodes. Fig 7 shows the end-to-end delay with respect to the number of malicious nodes. However, secure route established between source to the destination must consists of minimum hops that reduces the end-to-end delay and also packet retransmission must be minimized to avoid the end-to-end delay. In particular, end-to-end delay for disaster packet is very less which sent firstly before the normal packets deliver.

If the packets are normal, then aggregated into the single packet and then SALSA20 is applied for encryption. Finally, packets are transmitted through secure links.

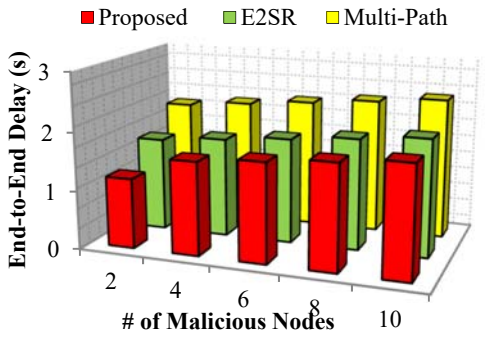

Fig.7.End-to-End Delay vs. # of Malicious Nodes

5.2.4 Impact of Packet Delivery Ratio

Packet delivery ratio is shortly referred as PDR, which is calculated between total amount of packets send by the sender and the sum of packets obtained by the receiver. Fig 8 shows the performance of PDR with respect to number of malicious nodes and node mobility. As a result malicious nodes and node mobility, existing works multi-path [Harold Robinson Y & Golden Julie E ,2019], and E2SR [Ponguwala Maitreyi & Rao Sreenivasa ,2019] does not increases PDR, result high packet losses only. Hence, existing works are failed to improving PDR when large number of adversaries is presented.

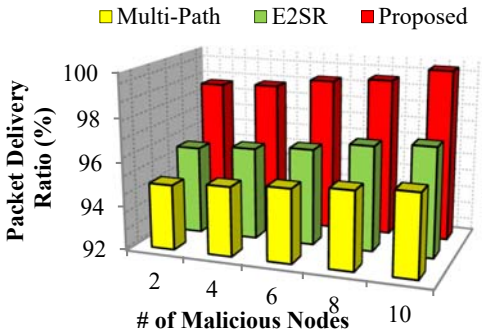

Fig 8 Packet Delivery Ratio (%) vs. # of Malicious Nodes

Our proposed work is support for secure route selection by bi-fitness optimizer that improves fitness via individual parameter tuning. When malicious nodes percentage increases then PDR rate is gradually increases. Since malicious nodes percentage improvement does not affects our proposed work.

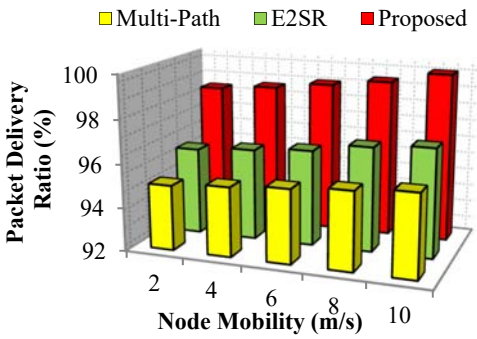

Fig 9 Packet Delivery Ratio (%) vs. Node Mobility

The blockchain environment achieves higher security strength and therefore from blockchain performance, PDR analysis is concluded. With the increase in number of zones for mobile communication, then the PDR is increases gradually. For instance, 2% of malicious nodes produce 95% of PDR for multi-path model, 96% for E2SR and 98% for proposed work, respectively.

For insecure environment, legitimate mobile node's mobility monitoring is an important one. Investigation of node mobility increases the path and link stability. This often gives the indirect output i.e. high packet delivery ratio. Fig 9 depicts the performance of PDR with respect to node mobility.

5.2.5 Impact of Energy Consumption

Energy consumption is a QoS based metric that determines the difference between the initial energy of node and then residual energy after the energy consumption for packet transmission or any other operations implementation in the network. However, energy consumed for several processes as packet transmission, route request, reply message reception, waiting to sleep after packet acknowledgement. Fig shows the energy consumption for the number of malicious nodes. From the graphical analysis, it is observed that the proposed blockchain model consumes lesser energy compared to E2SR and multi-path model. In particular, the proposed work has obtained 5J for 2 malicious nodes.

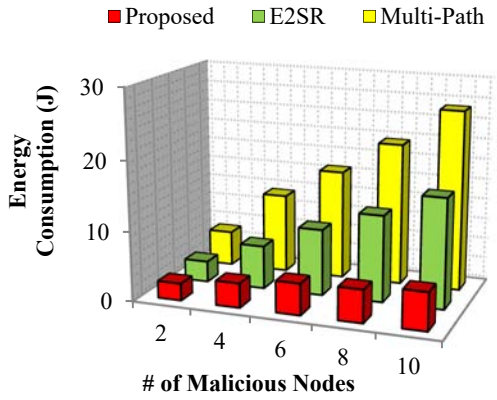

Fig.10.Energy Consumption vs. # of Malicious Nodes

Fig 10 shows the performance of energy consumption in terms of simulation time. In our proposed work, timer is used to listen the node's current state namely, sleep, listen or active. According to the network density, mobility of node, energy consumption is affected over a time. The proposed work learns environment and adaptively changes the rewards for deep reinforcement learning (DRL) algorithm.

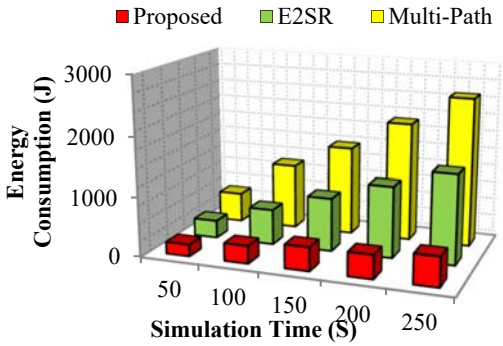

Fig.11.Energy Consumption vs. Simulation Time

5.2.6 Impact of Throughput

In MANET, throughput is defined as sum of data forwarded from the sender to the receiver node. On the other hand, it is defined as the complete data transmission through communication link to the receiver node. We compute the throughput with respect to the malicious nodes count, which is depicted in fig.12.

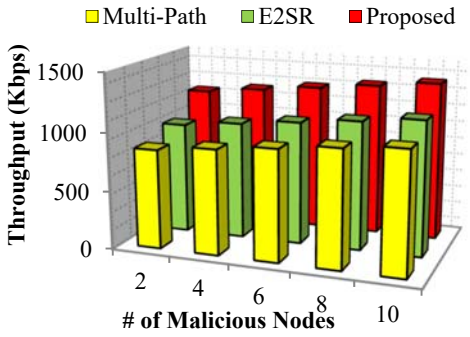

Fig.12.Throughput (Kbps) vs. # of Malicious Nodes

The exact throughput is computed for the proposed and existing works. However, throughput is affected by number of nodes, network communication links, and buffer size. For instance, if link is stressed then throughput is lesser. Packet transmission via optimum route refers to the high volume of throughput that flow packets without any fault. After the simulation analysis of throughput with respect to number of malicious nodes, it is proved that the proposed blockchain model is obtained higher throughput than the earlier works as multi-path and E2SR. In previous works, increase in node mobility and density and saturated links affect the throughput. These measures are not handled with the solution. When monitoring throughput, it will provide the complete network performance. We optimize throughput values that deliver the higher network performance to users.

5.2.7 Impact of Routing Overhead Ratio

This metric is defined as the ratio between sums of packets generated for route selection to the sum of packets transmitted. However, routing overhead refers to the amount of routing packets forward in route discovery and maintenance.

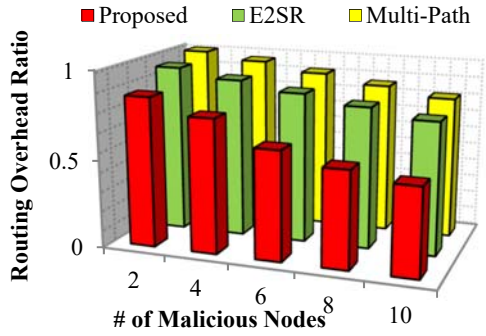

Fig.13.Routing Overhead Ratio vs. # of Malicious Nodes

These control messages forwarding introduce the routing overhead. Active route is determined by control messages to the neighbor nodes. Under low mobility environment, routing overhead is less, but highly dynamic networks produce frequent control messages forwarding. Another reason behind a high routing overhead is size of packet header transmitted through a link. Fig shows the performance of routing overhead ratio for number of malicious nodes. From the result, it is observed that the proposed model has obtained small routing overhead due to monitoring of link stability. Further, the selected route transfers packets in a reliable way. Network topology is controlled by CH, which reduces the sum of routing packets transmitted. For instance, when number of malicious node is 2, then the routing overhead by proposed model is 0.85, and the previous works are 0.95 and 0.99 for E2SR and multi-path, respectively.

5.2.8 Impact of Security Strength Ratio

Security strength is a positive metric that measures the security level during data packets transmission. The effectiveness of the security mechanisms are support for improving security strength. In this paper, SALSA20 algorithm is used for data packets encryption. Further, blockchain model is presented for improving the security strength. Blockchain is a best recommendation security key and packets management. Fig 14 represents the security strength with respect to the number of malicious nodes. To ensure the strong security strength for sensitive packets, we used higher bits for encryption. Hence, when number of malicious nodes is increase, then security strength ratio will be improved.

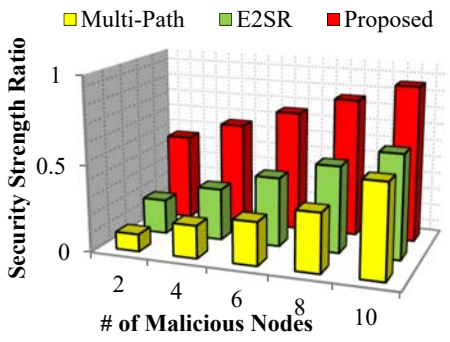

Fig.14.Security Strength Ratio vs. # of Malicious Nodes

5.3 Results Summary

In this subsection, we summarize how the proposed work has improved the better performance compared to previous works. Fig 5 – 14 explains about the superior performance of the proposed model in terms of QoS, security and energy consumption, namely attack detection rate, false positive rate, end-to-end delay, packet delivery ratio, throughput, energy consumption, routing overhead ratio, and security strength ratio. With the use of decentralized blockchain environment, security risks are mitigated in this paper. Further, the major motives for results improvement are follows:

- We considered cluster based environment which minimizes complexity and overhead in packets and control messages forwarding. Guard node is deployed in network for authentication and CH election, which suited for large environment. Block creation is implemented by Blake 3 algorithm that performs hashing by less number of number of rounds
- Optimum path is selected between the source and destination node and does not introduce the complexity. Hybrid Swarm Intelligence supports well in this work so that low energy consumption rate and bandwidth is also low. Trust computations and management is an attractive and vital role in prediction of routing attacks (black hole, grey hole and flooding) because malicious nodes detected primarily by trust computations. Hence, decentralized trusted environment is designed in this paper that establishes trust values in a reputed manner. This work finds well routing attacks such as black hole, and grey hole by use of blockchain technology, which classifies trustworthiness by different credentials as Packet Forwarding Rate, Average Forwarding Delay, Load, Control Dropping Rate and Energy consumption Rate.
- We proposed a lightweight blockchain technology that uses modified hashing for block transactions. This uses Blake 3 algorithm instead of double SHA-256 algorithm. Salsa 20 is much faster than AES and generated ciphertext is not greater than original size.

Table 4 summarizes the quantitative analysis of the proposed model that compared to the previous works such as E2SR and Multi-Path for all the performance metrics under security threats.

Performance Metrics	Proposed vs. Previous Approaches		
	Multi-path	E2SR	Proposed
Attack Detection Rate (%)	95.4	96.48	99.1
False Positive Rate (%)	0.114	0.13	0.187
End-to-End Delay (s)	1.64	1.8	2.2
Packet Delivery Ratio (%)	95.4	96.48	99.02
Energy Consumption (J)	4.11	9.36	15.66
Throughput (Kbps)	948	1050	1250
Routing Overhead Ratio	0.656	0.85	0.898
Security Strength	0.284	0.4	0.7

Table.4 Comparison of the Proposed vs. Earlier Approaches

6. Conclusion and future work

In this paper, bi-fitness optimizer is proposed for secure cluster-based routing in MANET. To ensure the secure communication among mobile nodes, in this paper we presented a blockchain technology. All communications are forwarded to the blocks and hash values for each transaction is generated. Firstly, mobile nodes are authenticated using multiple factors as ID, pwd, PUF, and eye-vein. To mitigate man-in-the-middle attack, hashed patterns are generated by using BLAKE 3 algorithm. Then clusters are formed by using the rewards optimized deep Q learning (RoDQL) algorithm. In this step, frequent cluster formation is avoided by learning of environments. Secure route is established by means of hybrid swarm intelligence algorithms i.e. particle swarm

optimization and artificial swarm intelligence. These two algorithms determine two fitness functions to meet the several objectives such as low energy consumption, low packet retransmission rate, high throughput and stability. Further, blockchain based zone-wise trust values are computed and stored in a block that purpose is to provide the data integrity. To hide the data packets, we proposed a fast and lightweight symmetric algorithm called as SALSA20 that encrypt both sensitive and non-sensitive packets before transmission. Finally, the simulation is executed to enhance the QoS of MANET in terms of attack detection rate, false positive rate, end-to-end delay, packet delivery ratio, throughput, routing overhead, and security strength.

In future, we have planned to integrate MANET to the other environments such as cellular networks, or Internet of Things or Cloud environment. Further, multimedia packets transmission is implemented to improve the QoS for real-time packets.

REFERENCES

[1] Balaji, S., Julie, E. G., Robinson, Y. H., Kumar, R., Thong, P. H., & Son, L. H. (2019). Design of a security-aware routing scheme in Mobile Ad-hoc Network using repeated game model. Computer Standards & Interfaces, 66, 103358
[2] Elhoseny, M., & Shankar, K. (2019). Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique. IEEE Transactions on Reliability, 1–10.
[3] El-Semary, Aly & Diab, Hossam. (2019). BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs based on Chaotic Map. IEEE Access. PP. 1-1.
[4] Haridas,S & Rama Prasath,A (2020). Enhancement of Network Lifetime in MANET: Improved Particle Swarm Optimization for Delay-less and Secured Geographic Routing. Jour of Adv Research in Dynamical & Control Systems, Vol. 12, 07-Special Issue, 2020
[5] Harold Robinson, Y., & Golden Julie, E. (2019). MTPKM: Multipart Trust Based Public Key Management Technique to Reduce Security Vulnerability in Mobile Ad-Hoc Networks. Wireless Personal Communications
[6] Hurley-Smith, D., Wetherall, J., & Adekunle, A. (2017). SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks. IEEE Transactions on Mobile Computing, 16(10), 2927–2940.
[7] Kanagasundaram, H., & A, K. (2018). EIMO-ESOLSR: Energy Efficient and Security-Based Model for OLSR Routing Protocol in Mobile Ad-Hoc Network. IET Communications.
[8] Krishnan R.S., Julie E.G., Robinson Y.H., Kumar, R., Son, L., Tuan, T.A., & Long, H.V. (2020). Modified zone based intrusion detection system for security enhancement in mobile ad hoc networks. Wireless Networks, 26, 1275-1289.
[9] 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, 1–1.
[10] Lwin, May & Yim, Jinhyuk & Ko, Young-Bae. (2020). Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. Sensors. 20. 698.
[11] Ponguwala, Maitreyi & Rao, Sreenivasa. (2019). E2-SR: A Novel Energy Efficient Secure Routing Scheme to Protect MANET from Adversaries in Internet of Things. IET Communications. 13.
[12] Rajendran, N., Jawahar, P. K., & Priyadarshini, R. (2019). Cross centric intrusion detection system for secure routing over black hole attacks in MANETs. Computer Communications
[13] Rani, P., Kavita, Verma, S., & Nguyen, N. G. (2020). Mitigation of Black hole and Gray hole Attack using Swarm Inspired Algorithm with Artificial Neural Network. IEEE Access, 1–1
[14] Riasudheen, H., Selvamani, K., Mukherjee, S., & Divyasree, I. R. (2019). An Efficient Energy-Aware Routing Scheme for Cloud-Assisted MANETs in 5G. Ad Hoc Networks, 102021.
[15] Rosenberg, Louis & Willcox, Gregg. (2019). Artificial Swarm Intelligence. Proceedings of SAI Intelligent Systems Conference IntelliSys 2019: Intelligent Systems and Applications pp 1054-1070
[16] Usman, M., Jan, M. A., He, X., & Nanda, P. (2018). QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Generation Computer Systems.
[17] Veeraiah, N., & Krishna, B. T. (2020). An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence.
[18] Xia, H., Cheng, X., Zheng, Y., & Liu, A. (2020). A Novel Light-weight Subjective Trust Inference Framework in MANETs. IEEE Transactions on Sustainable Computing, 1–1.

AUTHORS PROFILE

Haridas S, Assistant Professor, Dept. of Computer Science, Government First Grade College, Tumkur, Karnataka, India. Research Scholar, Hindustan Institute of Technology and Science, Chennai. His research interests are in the area wireless network.

Dr. A. Rama Prasath Assistant Professor (Selection Grade), Department of Computer Applications, Hindustan Institute of Technology and Science, Chennai, India. His research interests are in the area of evolutionary algorithms, image processing and wireless networks.