I. J. Computer Network and Information Security, **2024, 1, 123-132**
Published Online on February 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.01.10

Auto-metric Graph Neural Network based Blockchain Technology for Secured Dynamic Optimal Routing in MANET

Francis H. Shajin*
Department of Electronics and Communication Engineering, Anna University, Chennai, India
E-mail: shajin.mt@gmail.com
ORCID iD: https://orcid.org/0000-0002-0127-739X
*Corresponding author

Muthusamy Palaniappan
Department of Computer Science and Engineering, Jayaram Polytechnic College, Tiruchirapally, India
E-mail: mpmmuthu6@gmail.com
ORCID iD: https://orcid.org/0000-0002-8503-5258

P. Rajesh
Department of Electrical and Electronics Engineering, Anna University, Chennai, India
E-mail: rajeshkannan.mt@gmail.com
ORCID iD: https://orcid.org/0000-0001-6844-2591

Received: 26 July 2022; Revised: 19 September 2022; Accepted: 15 December 2022; Published: 08 February 2024

Abstract: Mobile ad hoc network (MANET) routing is a generous tactic used for allocating packets to the base station (BS). During the operations of routing, occurrence of malicious node embellishes the mobile ad hoc network operations. For that reason, a trusted distributed routing protocol is obliged that maintains the routing buttressing and the proficiency of mobile ad hoc network. To overcome these challenging issues, Auto-Metric Graph Neural Network based Blockchain technology is proposed in this manuscript for Secured Dynamic Optimal Routing in MANET (BC-SDOR-MANET-AGNN). The proposed approach is simulated in NS-2 tool. The proposed BC-SDOR-MANET-AGNN approach attains 76.26%, 65.57%, 42.9% minimal delay during 25% malicious routing environment, 73.06%, 63.82%, 38.84% less delay during 50% malicious routing environment when analyzed to the existing models, like enhanced hybrid secure multipath routing protocol for MANET (BC-SDOR-MANET-GAHC), an improved ad hoc on-demand distance vector routing security approach based on BC technology in MANET (BC-SDOR-MANET-AODV-MQS) and block chain-based better approach for the mobile ad-hoc networking protocol using ensemble algorithm (BC-SDOR-MANET-E-BATMAN) methods.

Index Terms: Auto-metric Graph Neural Network, Block Chain Technology, Malicious Node Attacks Mobile ad Hoc Network, Trusted Distributed Routing Protocol.

1. Introduction

Mobile ad-hoc networks contains a set of mobile nodes; wireless networks are connected in a self-configured way [1]. Hence, nodes in the mobile ad-hoc network are moved freely as regular change in the ad-hoc network topology [2, 3]. The mobile nodes within the range can communicate directly. While others need the support of intermediate nodes to route its data packets [3, 4]. The mobile ad-hoc networks are fully distributed and it operates anywhere without fixed infrastructure, such as access points/base stations [5]. This feature allows the network only at the special surroundings, like dreadful events [6, 7]. The mobile adhoc networks entails of conventional self-acclimatizing mobile node for data communication [8]. It is a hopeful expertise and it has widespread application in the field of environmental science, industry, agricultural computerization etc [8, 9]. Nevertheless, the MANET tender has hazardous difficulties with respect to secure the data by means of routing practices. But these strategies cannot avert the unsanctioned node attacks [10]. It rejects the packets when unsanctioned node acquires data packets from adjacent node [11]. Correspondingly, it

cannot communicate the data packets to its next hop neighboring node named black hole attack while routing process of MANET [12, 13]. Most of the trusted distributed routing protocol is vehemently despicable at some stage in real time manifestations, and secure to differentiate the untrusted distributed routing node [14, 15]. Similarly, there is no operative tactics from preventing spiteful node manifestations [16, 17]. Some solutions require to be put forward to overwhelm these issues, these are prompted to do this work.

This manuscript proposes a Proof-of-Work (PoW) based consensus procedure for operative token transaction in MANET depending on block chain. From this, each routing mobile node has its individual registration smart indenture. Every routing mobile node receives a secret key from the token.

The key contributions of this manuscript are given briefly,

- BC technology for SDOR in mobile adhoc network is proposed utilizing AGNN (BC-SDOR-MANET-AGNN).
- The blockchain technology is employed to distribute trusted BC token transactions based trusted distributed routing information.
- Every routing mobile node receives a secret key from the token, which provides best route for data transferring.
- The trusted distributed ideal routing information is delivered utilizing proposed BC base mobile ad-hoc networks under Auto-metric graph neural network [18].
- The security analysis is done by five viewpoints: proof of work consensus, differentiation, routing information source, dual-spending problem evading, self-modification.
- The proposed method is simulated in Network Simulator tool.
- The performance metrics, like delay performance for 25% spiteful node, delay performance for 50% spiteful node, average delay with energy consumption, blockchain token transactions throughput is examined.
- Then the performance is compared with existing BC-SDOR-MANET-GAHC [19], BC-SDOR-MANET-AODV-MQS [20] and BC-SDOR-MANET-E-BATMAN [21] methods.

The rest of this manuscript is arranged as: the literature survey is delineated in section 2, the proposed methodology is illustrated in section 3, the results and discussion are proved in section 4, section 5 concludes this manuscript.

2. Literature Survey

Various works were already suggested in the literature depending on trusted routing protocol in BC based mobile ad-hoc network, a certain works are described here,

Srilakshmi et al., [19] suggested an enhanced hybrid secure multipath routing protocol for mobile ad-hoc network. Hybrid hill climbing and genetic algorithm was choosing the ideal route in multiple path. Improved fuzzy C-means was structured by density peak together with cluster heads (CHs) in a predicted manner, like direct and indirect trust. It offers minimal count of energy and lesser throughput.

Ran et al., [20] introduced a proficient ad hoc on-demand distance vector (AODV) routing security approach under BC technology in ad hoc network. The multiple path routing security algorithm based on block chain was employed to maximize the typical AODV protocol. It offers maximal secure environment, but minimal network throughput.

Singh et al., [21] suggested block chain-base BATMAN protocol utilizing mobile ad-hoc network and ensemble approach. The presented scheme provides a distributed platform to mobile ad-hoc networks routing by block chain on the basis of Byzantine Fault Tolerance protocol. It presents lesser packet delivery rate and higher performance in average end-end delay.

Wang et al., [22] introduced lightweight block chain assisted secure routing of swarm UAS networking. The lightweight block chain-based secure routing process for swarm UAS networking averts spiteful links through the attackers. The main idea behind the introduced approach was to attack the identification with safety and prevent packet drops.

Xu et al., [23] presented deep reinforcement learning assisted edge-terminal collaborative offloading algorithm of blockchain computing tasks for energy internet. Local computing, user collaboration and edge node collaboration were included. It presents lesser delay and greater average throughput transaction.

Jiao et al., [24] introduced a mobile ad-hoc cloud structure based upon BC to provide the facilities of resource distribution in MANET as secure manner. The presented structure has network, BC, and smart contract layers. The results indicate that the presented method achieves greater performance. But not identify spiteful nodes accurately.

Wang et al., [25] introduced trust routing protocol dependent upon cloud-based fuzzy Petri net with trust entropy for MANET. A reliable reasoning mode based on a fuzzy Petri net cloud model was introduced to scale the dependability of nodes. The presented model displays that the TUE-OLSR protocol was enhanced over the existing belief-based OLSR protocols.

Singh et al., [26] suggested a BC-based MANET with ensemble approach. It presents distributed environment for routing MANETS utilizing BC depending on Byzantine Fault Tolerance (BFT) protocol. Mobile Ad-hoc Networking

was utilized to combine the blockchain concept as a representational protocol in MANET. The ensemble algorithm achieved feasible presentation on average end-end delay, network throughput, energy, but the attack arrival rate was higher.

Liu [27] presented BC system for security-related data collection (B4SDC) in MANET. Using proof-of-stake (PoS) consensus mechanism by accumulating stakes through message sharing, B4SDC not only provides incentives to all participating nodes. However, the PDR rate of this sample was low.

Lwin et al., [28] presented a BC-based trust management system based on lightweight consensus algorithm in MANET. It provides a distributed trust framework for routing nodes in tamper-proof MANETs through BC. The outcomes show that the consensus approach reduced the verification time and reduced the overhead. But the block transaction latency of the model was high.

Muketkar and Kolekar [29] presented an encrypted trust-based dolphin glow optimization (E-TDGO) model for routing in MANET. This E-TDGO model includes k-path discovery, ideal path selection, and communication processes. Routing messages were encrypted by AES-128 including shared code, key for providing protection. The outcomes show that the E-TDGO can achieve the performance, delay, and detection rate, but the attack arrival rate was higher.

A M. A.B. [30] presented a self-configurable cluster process in MANET. It is used to detect transient cluster heads (CH) and replaced by other nodes. Also, the k-means algorithm was given for CH selection. It has lower power and energy loss than other protocols, but the security was less due to the high attack arrival rate.

3. Proposed Methodology

In this manuscript, BC technology for SDOR in mobile adhoc network is proposed with the help of AGNN (BC-SDOR-MANET-AGNN). Fig 1 delineates the block diagram of proposed BC-SDOR-MANET-AGNN method. The explanation regarding trusted distributed routing scheme for Mobile adhoc network is discussed with the help of Auto-metric graph neural network are given below,

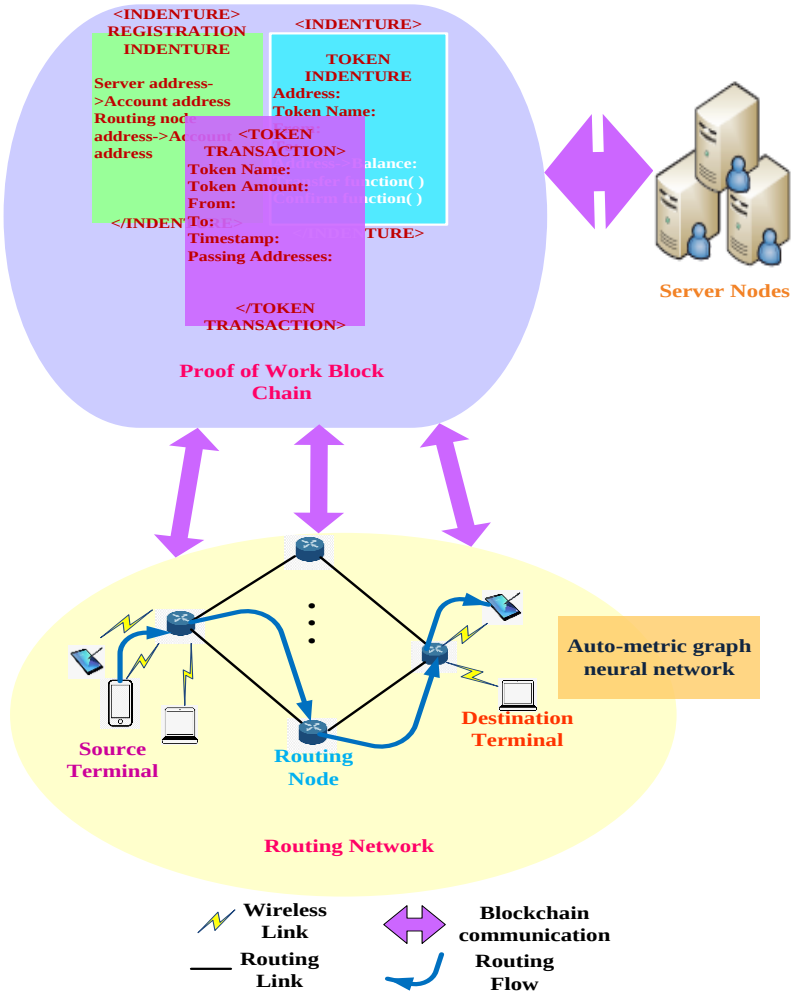

Fig.1. Entire work flow for trusted distributed routing scheme for BC base MANET

3.1. Network Model

In a mobile ad-hoc network, the area of interest is split into $k \in \{1, \ldots . K\}$ K finite grids. Consider $N = \{n_1, \ldots \ldots n_N\}$ as N wireless node collection, $M = \{m_1, \ldots \ldots m_M\}$implicates M miners' collection. Omnidirectional antennas on the nodes and the miners, which are both moving objects, provide a fixed transmission range. The distributed nodes transfer as routing node or miner. Nodes including additional processing power deem the miners' roles. The miners (MN) have various nodes that are presented in any specified grid.

3.2. BC Model

Every grid specifies the probability miner's area via every node within the grid that means the packets send through the nodes are derived by minimum one closer miner. Every miner notice at nodes' actions at the routing packets and reviews positive or negative events, which are recorded as transactions. These transactions are collected by the miner to create the blocks. Block chain presents unchallengeable record to the nodes behavior and the mining complexity is required to be proportional to the miners count on grid, also it activates as a credibility measure for verification. Mined blocks are multicast amid the miners primarily to consider the maximum reliable verified block combined with the mined block with difficult. This is termed as Most Difficult-Chain consensus. It telecasts the nodes in the grid when the miner receives an updated BC state, so that they can quickly update their local states. Future routes are computed using the information stored in the BC to determine each node's reputation.

3.3. Threat Model

Spiteful Nodes (Routing threat): By propagating fake routing data, a black hole attack is suffered by spiteful node that absorbs all incoming traffics. The chosen packets are eradicated by grey whole attack, for eg, all routing packets are transmitted however eliminated datapackets. The unlawful node forwards datapackets to improper destination or incorrect next hop node by varying the address of destination. The aforementioned threats are lessened by giving nodes reputations based on their historical forwarding behaviors.

3.4. BC based Mobile Adhoc Network

Block chain technology has certain aspects, like distributed records along hamper-resilient, transference, and information traceability. Such aspects can be useful to mobile adhoc network routing operation and its convention for block chain token transactions, which records every routing node transaction. The block chain based mobile adhoc network has server node, routing nodes, terminal nodes. The mobile ad hoc network's network mode can be specified as undirected graph, it is given in eqn (1)

$$Graph = \left[Set\ of\ \ nodes, Set\ of\ \ links\ \ for\ connecting\ \ nodes\right] \tag{1}$$

Nodes on block chain base mobile adhoc network having dissimilar mobility aspects. A few nodes exist in static or dynamic. In which, server node as static format, while routing node as dynamic format. The ingress as well as egress of nodes not influence the block chain base mobile adhoc routing networks as a consequence of its updation of dynamic status. All routing nodes are conscientious for allocating the tokens and acquiring tokens as of source to destination terminal node through routing protocols accomplished from local learning model. This method continuously queries the blockchain network for the relevant routing network status information and gathers it, making it easier to distribute tokens from the source to the destination terminal node. Every BC system adheres to a precise consensus scheme for ensuring the fairness of the transactions on BC.

Proof-of-Work (PoW) based consensus approach is considered for proficient token transaction on BC base Mobile adhoc networks. Universally, corroborator identity contains pre-authorized BC nodes. In this work, each server node activates as corroborator identity, it has complicated release in PoW fostered Block chain mobile adhoc networks. It also has peerless block chain address. The primary task of corroborator identity achieves smart indentures, authenticate block chain transactions, liberating blocks on block chain. It disconcerts that particular block if it is any malevolent corroborator identity. These particular blocks can be eliminated by votes of corroborator. This is called less-privileged nodes. It also has peerless block chain address. The main assignment of assistant identity is to instigate the token indentures, commencement of certain indenture roles, and inquiry regarding transaction information in the block chain fostered mobile adhoc networks.

3.5. Auto-metric Graph Neural Network based BC Technology for SDOR

The SDOR information is distributed using proposed BC based mobile adhoc network under Auto-metric graph neural network. Usually, the number of tokens assigned to each destination routing node and the routing addresses of all authorized destination nodes. AGNN is a meta-learning procedure, aimed for SDOR in mobile ad-hoc networks. The routing node classification of small graph creation is employed to train the AGNN. The AGNN is directly used for Secured Dynamic Optimal Routing that comprised graph structure initialization, layer structure, loss function, malicious node attacks detection with the help of meta-learning training procedure. Initially, the graph structure input data represents (R) including (k) known and (M) unknown routing nodes that is exhibited in eqn (2),

$$R = \{[(p_1, l_1), \ldots\ldots, (p_{n-1}, l_{n-1})], [\tilde{p}]; l_n \in (1, C)\} \quad (2)$$

The entire networks devices represent (p) including label(l), count of classes denotes (C) as $(n = Ck + 1)$. The routing nodes select randomly along node label. Initialize $g = (N, E, W)$ graph structure, (N) implies node set, (E) signifies edge probability matrix, weights imply (W). The features of secure routing node p_i is scaled by eqn (3),

$$p_i = [l_i, \eta_i, r_i, m_i] \quad (3)$$

Consider η_i denotes risk factor, l_i implicates label encoding, r_i specifies cognitive score, m_i as features and l_i as zero vectors for routing node along unknown labels. The weights of safe routing nodes are identical to 1 value, meaning that the edge probability matrix is 1 and the graph initialization is fully connected. After the graph structure is initialized, this is given as input to GNN layer using the constraint of probability. The information is transferred among the nodes to update the routing node features, which obtains unknown routing node label (malicious node attacks). The risk factor base edge matrix probability is scaled, then weight matrix identified automatically via features. The probability matrix determination including risk factors $(\eta_1, \eta_2, \eta_3 \ldots\ldots \eta_N)$ is mentioned as equation (4),

$$e_{i,j}^k = \begin{cases} 1 & if \quad \left|\eta_i^k - \eta_j^k\right| \le \phi \\ 0 & otherwise \end{cases} \quad (4)$$

Let edge weight amongst routing nodes p_i and p_j owns to [0,1], the $(e_{i,j})$ element is $e_{i,j} = \frac{1}{\left(K+1-\sum_{k=1}^{K} e_{i,j}^k\right)}$, (K) implicates count of risk factors, (k) implies risk factor feature, (φ) specifies threshold value that is applied to measure the similarity of risk factor aspects amongst 2 nodes that is represented $(f_1, f_2, f_3 \ldots\ldots\ldots\ldots f_N), f \in S^d$ here S^d implies feature dimension. Weights matrix betwixt routing nodes and features are scaled utilizing eqn (5),

$$W_{i,j}^{(x)} = e_{i,j}\left(ab(f_i - f_j\right) \quad (5)$$

Here $W_{i,j}^{(x)}$ weights amid the nodes along (x) number of layers with respect to absolute difference ab ; f_i, f_j denotes feature set amongst the nodes. The routing nodes have been updating to achieve proper result using eqn (6),

$$gn(P^x) = L - Re\,L\,U(\textstyle\sum_{B^x} BP^x \beta_B^x) \quad (6)$$

Consider gn implicates node updating factor, P^x implicates overall number of nodes in (x) number of network layers, $L - Re\,L\,U$ specifies non-linear activation function, β_B^x implies training parameters employed for modifying features dimension of every node. The result concatenates through P^x to maintain features of input routing node, the obtained outcome of AGNN layer is exhibited in eqn (7),

$$P^{(x+1)} = [P^x, gn(P^x)] \quad (7)$$

In lieu of coupled with input nodes for final layer after modifying feature dimension, the output of attacker nodes injects directly to the soft max layer to normalize the output. To update the parameters, the AGNN model's loss function is calculated is exhibited in eqn (8),

$$lf(\widehat{M}, M) = -\textstyle\sum_l m_l \, log\, P\left(\widehat{M} = m_c | R\right) \quad (8)$$

Consider M specifies prediction outcome of attack node, $\widehat{M}$ specifies label of attack node, (R) denotes the input data, (C) signifies number of classes. AGNN is created by graph structure, loss function and GNN layer. Then extract sample data that is given to layer to develop graph structure, here the data transmits within the network nodes are updated through AGNN. At last, the attack node or unknown routing node is detected. By using loss function, the network parameters are updated in eqn (9),

$$\beta_{B_{(t+1)}} = S(lf_t, \beta_{B(t)}) \quad (9)$$

Here S implies factor to update parameters β_B depending upon $lf_{(t)}$ loss function along (t) training epoch. The parameters updated later training epoch performance, then get final result for categorizing unknown label nodes (malicious attack nodes) in the new graph.

3.6. Analysis of Security in BC based Mobile adhoc Network

The server node with the routing node executes the management of trusted distributed ideal routing information depending on Proof of work block chain. Security analysis in Block chain based mobile adhoc network is depicted by five viewpoints: proof of Work consensus, BC token transaction, RIS, evading double spending problem, self-modification, which is deliberated below,

A. Proof of Work Consensus

It is employed in BC mobile adhoc network that aids the server node to upload the transaction (packet transmission) through the updation of outing information. Thus, the hackers are not able to interfere with routing informative.

B. Block Chain Token Transaction Distinguishability

BC token transaction is separated by server node. The proposed BC mobile adhoc network based, this server node stores information regarding the transactions of allocating token indentures, routing node transactions of working procedures in the indentures. Here, all the transaction information records on the blocks of proposed BC mobile adhoc network that not separate transversely throughout the block chain network.

C. Routing Information Source (RIS)

Every routing mobile node in the proposed BC mobile ad hoc network receives the appropriate RIS. This source is dependable, also it cannot be determined by the hackers.

D. Avoidance of Double-spending Issue

According to the token indenture, the address of each routing mobile node is only recorded for every time slot. As a result, the routing node is unable to recruit token transactions for other routing node that was occupying the same time slot. Thus, double spending problem is avoided.

E. Self-amendment

In spiteful mobile node, it not creates any routing link transaction, because the proposed BC routing algorithm's regularized constraint value for routing link is too lower.

4. Result with Discussion

The efficiency of BC-SDOR-MANET-AGNN (proposed) method is discussed in this section. The proposed approach is simulated in Network Simulator tool. The performance metrics is evaluated to verify the robustness of proposed method. Then, the simulation performance for proposed BC-SDOR-MANET-AGNN attains average packet delay performance with 25% malicious node and 50% malicious nodes compared with existing BC-SDOR-MANET-GAHC [19], BC-SDOR-MANET-AODV-MQS [20] and BC-SDOR-MANET-E-BATMAN [21] methods. The simulation parameter of proposed system is portrayed in Table 1.

Table 1. Simulation parameter

Parameters	Values
Number of network node	0-100
Area size	$1000m \times 1000m$
Bandwidth	10 Mps
Maximum node speed	50 (m/s)
Minimum node speed	5 (m/s)
Time interval for sending packets	40/0
Simulation time	900 s

An experimental setup of the proposed BC-SDOR-MANET-AGNN method for securing routing information is analyzed. Here, 30 virtual servers are used to test the update of BC transactions on the chain. Each data stored by BC-SDOR-MANET-AGNN is derived from public BC transactions. With respect to Geth 1.8.19a, collaborative BC is built, which provides stable Ethereum transaction facilities. The BC-SDOR-MANET-AGNN model is used to mimic real data sending and receiving between the routing nodes and a slot. Information including average latency along with energy consume, then the BC token transactions throughput is finally documented.

4.1. Performance Metrics

Some of the performance metrics are average delay, average transaction latency, average energy consumption, block chain token transaction throughput is considered here.

A. Delay

It is computed with malicious nodes (25% and 50%) at the area of simulation. The delay can be calculated with the help of equation (10),

$$Delay = Time\ taken\ \ for\ sending\ tokens\ \ from\ source \text{ node to } destination\ node \tag{10}$$

B. Average Token Transaction Delay

It is taken via packaging period of transaction. This captured the time that passed when miners added the token transaction to the block chain with a higher arrival rate.

C. Average Token Transaction Energy Consume

In Ethereum networks, the different unit is applied to calculate how many works the attacker has generated. To pay the BC miner, it converts as related ether currency.

4.2. Simulation Results

Fig. 2(a) and 2(b) signifies the simulation outcome of average packet delay with 25%, 50% spiteful nodes. Fig.3(a) to 4(b) shows the simulation result of evaluation metrics of the block chain token transactions.

Fig.2(a) represents average packet delay with 25% spiteful nodes. The proposed BC-SDOR-MANET-AGNN reaches 26.44%, 15.03% and 20% lower average packets delay at 0.5 arrival rate estimated with existing models. The proposed method reaches 32.59%, 26.03% and 10.784% lower average packets delay at arrival rate 1.5 analyzed to the existing methods. Fig 2(b) displays average packet delay with 50% spiteful nodes. The proposed BC-SDOR-MANET-AGNN provides 17.64%, 29.33% and 16.167% lower average packets delay at 0.5 arrival rate compared to the existing methods. The proposed BC-SDOR-MANET-AGNN achieves 12.67%, 15.69% and 7.36% lower average packets delay at arrival rate 1.5, compared with previous BC-SDOR-MANET-GAHC, BC-SDOR-MANET-AODV-MQS and BC-SDOR-MANET-E-BATMAN methods.

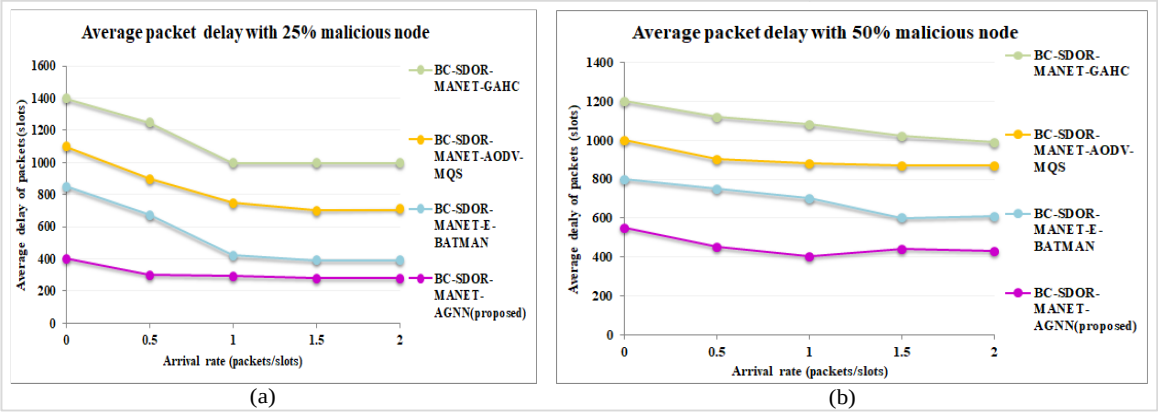

Fig.2. (a). Performance of average packet delay with 25% malicious node, 2(b): Performance of average packet delay with 50% malicious node

Fig.3(a) depicts average transaction delay of block chain scheme. In 0.5 arrival rate, the proposed BC-SDOR-MANET-AGNN provides 62.711%, 58.49% and 52.173% minimal average transaction delay. The proposed BC-SDOR-MANET-AGNN attains 61.53%, 50.15% and 54.545% minimal average transaction latency at 1.5 arrival rate. Fig.3(b) displays average transaction energy consume of block chain scheme. At 0.5 arrival rate, the BC-SDOR-MANET-AGNN attains 62.5%, 59.09%, 55% minimal average transaction energy consume evaluated with existing methods. The proposed BC-SDOR-MANET-AGNN reaches 52.631%, 52.631%, 43.75% minimal average transaction energy consume at 1.5 arrival rate evaluated with existing BC-SDOR-MANET-GAHC, BC-SDOR-MANET-AODV-MQS and BC-SDOR-MANET-E-BATMAN methods respectively.

Fig 4(a) displays average token transaction throughput of block chain scheme. The proposed BC-SDOR-MANET-AGNN achieves 42.011%, 41.732%, 41.453% better average transaction throughput at 2000 concurrent request rate analyzed with existing methods. The proposed BC-SDOR-MANET-AGNN attains 25.833%, 20.8%, 0.667% higher average transaction throughput at 4000 concurrent request rates assessed with existing models. Fig.4(b) shows the performance of average overheads. At 50 time interval, the proposed BC-SDOR-MANET-AGNN provides 63.398%, 51.515% and 42.857% lesser overhead assessed to the existing models. At time interval 100, the proposed BC-SDOR-MANET-AGNN provides 48.571%, 30.46%, and 18.97% lesser overhead assessed to the existing models. At time interval 150, the proposed BC-SDOR-MANET-AGNN method provides 41.51%, 50.178% and 31.788% minimal overhead examined with previous BC-SDOR-MANET-GAHC, BC-SDOR-MANET-AODV-MQS and BC-SDOR-MANET-E-BATMAN methods respectively.

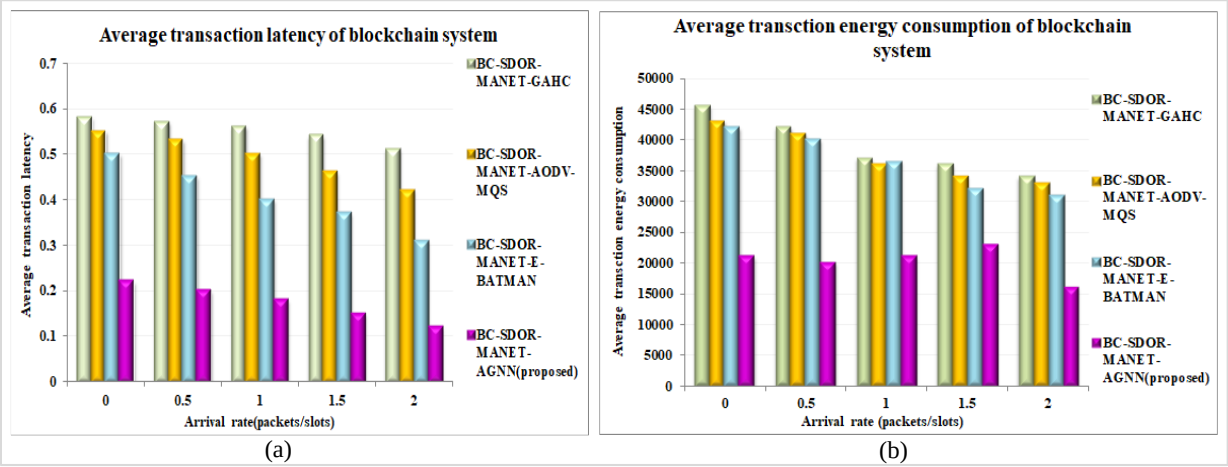

Fig.3. (a): Average transaction delay of block chain 3(b): Average transaction energy consumption of block chain

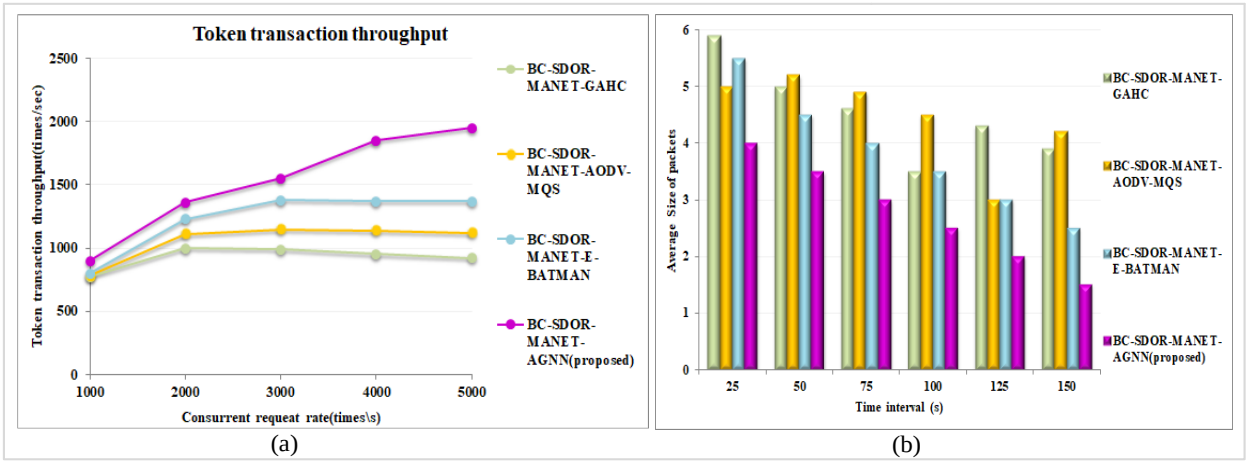

Fig.4. (a): Average token transaction throughput of block chain system, 4(b): Performance comparison of averageoverheads

5. Conclusions

In this manuscript, BC technology for SDOR in mobile ad-hoc network was implemented effectually based upon Auto-metric graph neural network (BC-SDOR-MANET-AGNN). Here, security analysis is carried out using five perspectives, including the proof-of-work consensus method, the distinguishability of BC token transactions, the source of the routing information, the prevention of dual spending, and self-modification. The proposed technique is activated in Network Simulator tool. The efficiency of proposed BC-SDOR-MANET-AGNN achieves 66.64%, 63.06%, 53.98% lesser average transaction delay of BC, 64.52%, 62.02%, 50.72% lesser average transaction energy consume of BC scheme assessed to the existing methods. Globally, mobile networks becoming more and more popular that is expanding the market for mobile services. If Wireless networks were created by taking into account the entirety of the design, including the interactions with other layers, the proposed BC-SDOR-MANET-AGNN technique has a bright future. Thus, the proposed security architecture is applicable for the mobile-Governance (m-Governance) scenarios. The m-Governance environment needs less cost infrastructure which also offer high quality transmission and constant connectivity.

References

[1] C. Machado, and C.M. Westphall, "Blockchain incentivized data forwarding in MANETs: Strategies and challenges. *"Ad Hoc Networks*, vol. 110, pp.102321, 2021.

[2] M.T.Lwin, J. Yim, and Y.B.Ko, "Blockchain-based lightweight trust management in mobile ad-hoc networks."*Sensors*,vol. 20, no.3, pp.698, 2020.

[3] G.Liu, H.Dong, Z.Yan, X. Zhou, and S.Shimizu, "B4SDC: A blockchain system for security data collection in MANETs."*IEEE Transactions on Big Data*, 2020.

[4] M.Banerjee, J.Lee, and K.K.R.Choo, "A blockchain future for internet of things security: a position paper."*Digital Communications and Networks*, vol. 4, no. 3, pp.149-160, 2018.

[5] S.Sharma, and S.Saxena,"Blockchain and UAV: Security, Challenges and Research Issues."*In International Conference on Unmanned Aerial System in Geomatics*, (pp. 99-107). 2019 Springer, Cham.

[6] G.P.Joshi, E.Perumal, K.Shankar, U.Tariq, T.Ahmad, and A.Ibrahim, "Towardblockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks."*Electronics*,vol.9, no.9,pp.1358, 2020.
[7] N. Hu, Z.Tian, Y.Sun, L.Yin, B. Zhao, X. Du, and N. Guizani, "Building agile and resilient uav networks based on sdn and blockchain."*IEEE Network*, vol. 35, no.1, pp.57-63, 2021.
[8] V.L.Narayana, A.P.Gopi, and K.Chaitanya, "Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology."*Rev. d'IntelligenceArtif*, vol.33, no. 1, pp.45-48, 2019.
[9] V.Verma, and V.K. Jha, "Detection and Prevention of Vampire Attack for MANET."*In Nanoelectronics, Circuits and Communication Systems*, (pp. 81-90), 2021. Springer, Singapore.
[10] M. Usman, M. Jan, X. He, P. Nanda, "QASEC: A secured data communication scheme for mobile Ad-hoc networks."*Future Generation Computer Systems*, vol.109 pp.604-610, 2020.
[11] H. Kanagasundaram, A. Kathirvel, "EIMO-ESOLSR: energy efficient and security-based model for OLSR routing protocol in mobile ad-hoc network."*IET Communications*, Vol.13, no. 5, pp.553-559, 2019.
[12] P. Singh, M. Khari, and S. Vimal, "EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT." *Wireless Personal Communications*, pp.1-25, 2021.
[13] H. Xu, H. Si, H. Zhang, L. Zhang, Y. Leng, J. Wang, and D. Li, "Trust-based probabilistic broadcast scheme for mobile ad hoc networks." *IEEE Access*, vol. 8, pp.21380-21392, 2020.
[14] E. Elmahdi, S.M. Yoo, and K. Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks." *Journal of Information Security and Applications*, vol. 51, p.102425, 2020.
[15] B.K. Tripathy, S.K. Jena, P. Bera, and S. Das, "An adaptive secure and efficient routing protocol for mobile ad hoc networks." *Wireless Personal Communications*, vol. 114, no. 2, pp.1339-1370, 2020.
[16] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: a trust-based secure multipath routing protocol for enhancing the qos of the mobile ad hoc network." *Security and Communication Networks*, *2021*, 2021.
[17] R. Prasad, "Enhanced Energy Efficient Secure Routing Protocol For Mobile Ad-Hoc Network." *Global Transitions Proceedings*, 2021.
[18] X.Song, M.Mao, and X.Qian, "Auto-Metric Graph Neural Network Based on a Meta-Learning Strategy for the Diagnosis of Alzheimer's Disease."*IEEE Journal of Biomedical and Health Informatics*, vol.25, no.8, pp.3141-3152, 2021.
[19] U.Srilakshmi, N.Veeraiah, Y.Alotaibi, S.A.Alghamdi, O.I. Khalaf, and B.V.Subbayamma, "An Improved Hybrid Secure Multipath Routing Protocol for MANET."*IEEE Access*, vol. 9, pp.163043-163053, 2021.
[20] C.Ran, S.Yan, L.Huang, and L.Zhang,"An improved AODV routing security algorithm based on blockchain technology in ad hoc network." *EURASIP Journal on Wireless Communications and Networking*, vol.1, pp.1-16, 2021.
[21] U.Singh, S.K.Sharma, M.Shukla, and P.Jha, "Blockchain-based BATMAN protocol using Mobile ad-hoc Network (MANET) with an Ensemble Algorithm." 2021.
[22] J.Wang, Y.Liu, S.Niu, and H.Song, "Lightweight blockchain assisted secure routing of swarm UAS networking."*Computer Communications*, vol. 165, pp.131-140, 2021.
[23] S.Xu, B.Liao, C.Yang, S.Guo, B.Hu, J.Zhao, and L.Jin, "Deep reinforcement learning assisted edge-terminal collaborative offloading algorithm of blockchain computing tasks for energy Internet." *International Journal of Electrical Power & Energy Systems*, vol.131, pp.107022, 2021.
[24] Z. Jiao, B. Zhang, L. Zhang, M. Liu, W. Gong, C. Li, "A Blockchain-Based Computing Architecture for Mobile Ad Hoc Cloud."*IEEE Netw*. Vol. 34, no. 4, pp.140-149, 2020.
[25] X. Wang, P. Zhang, Y. Du, M. Qi,"Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network."*IEEE Access*, Vol. 8, pp.47675-47693, 2020.
[26] U. Singh, S.K. Sharma, M. Shukla, and P. Jha, "Blockchain-based BATMAN protocol using Mobile ad-hoc Network (MANET) with an Ensemble Algorithm," 2021.
[27] G. Liu, H. Dong, Z. Yan, X. Zhou, and S. Shimizu, "B4SDC: A blockchain system for security data collection in MANETs." *IEEE Transactions on Big Data*, 2020
[28] M.T. Lwin, J. Yimand Y.B. Ko, "Blockchain-based lightweight trust management in mobile ad-hoc networks." *Sensors*, vol. 20, no. 3, p.698, 2020.
[29] M.M. Mukhedkar, and U. Kolekar, "E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network." *International Journal of Communication Systems*, vol. 33, no. 7, pp.e4252, 2020.
[30] A.B. AM, "High energy efficient lifetime management system and trust management framework for manet using self-configurable cluster mechanism." *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp.1229-1241, 2021.

Authors' Profiles

Francis H Shajin graduated from Anna University, India. He has more than 10 years of experience in research and development field. He has published more than 35 papers in international journals. His current research interests include very-large-scale integration, soft computing, image processing, machine learning and networking.

Muthusamy Palaniappan Received M.E., (Computer Science and Engineering) degree from Anna University, Chennai, Tamilnadu during the year 2010. He got the PhD, Degree from VELs University, Chennai. Currently working in Jayaram Polytechnic College, Tiruchirapally-621014. His research interests Computer Networks and Securities.

P. Rajesh graduated from Anna University, India. He has more than 10 years of experience in research and development field. He has published more than 35 papers in international journals. His current research interests include artificial intelligence, power system, smart grid technologies and soft computing.

How to cite this paper: Francis H. Shajin, Muthusamy Palaniappan, P. Rajesh, "Auto-metric Graph Neural Network based Blockchain Technology for Secured Dynamic Optimal Routing in MANET", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.1, pp.123-132, 2024. DOI:10.5815/ijcnis.2024.01.10