International Journal of Safety and Security Engineering
Vol. 10, No. 4, August, 2020, pp. 509-516
Journal homepage: http://iieta.org/journals/ijsse

A Trust Based Efficient Blockchain Linked Routing Method for Improving Security in Mobile Ad hoc Networks

Vejendla Lakshman Narayana*, Divya Midhunchakkaravarthy

Lincoln University College, Lembah Sireh, 15050 Kota Bharu, Kelantan, Malaysia

Corresponding Author Email: lakshmanv58@vignannirula.org

https://doi.org/10.18280/ijsse.100410

Received: 5 June 2020
Accepted: 16 July 2020

Keywords:
routing method, ad hoc network, malicious nodes, block chain, data communication, routing table, neighbor nodes, data security

ABSTRACT

Mobile Ad hoc Networks (MANETs) are non-fixed framework systems and there are such a large number of issues with them because of their dynamic topology, portable nodes, security, data transfer capacity, restricted battery strength and so forth. Trust is an association, dependability, unwavering excellence, and loyalty of the nodes in the system. A trusted routing plan is essential to guarantee the routing security and productivity of sensor systems. In perspective on these issues, this manuscript proposes a trusted routing plan utilizing block chain and building up a security model to improve the routing security and productivity for ad hoc networks. The possible routing plan is given for acquiring routing data of routing nodes on the block chain, which makes the routing data distinct and difficult to alter. The support learning model is utilized to help routing nodes progressively select increasingly trusted and productive routing connections. The proposed work introduces a Trust Based Efficient Blockchain Linked Routing Method (TbEBCLRM) for a system of trusted and untrusted nodes. The proposed method utilizes blockchain method to improve security in the ad hoc networks and to avoid malicious activities during communication is initiated. The proposed method is compared with the traditional methods and the results show that the proposed method exhibits better performance in terms of accuracy, security level, trust level and energy consumption.

1. INTRODUCTION

MANET is a kind of network used amongst other appropriate methods of group communication in a circumstance where different methods for correspondence are either unrealistic to send or expensive issue or not possible because of natural disasters [1]. MANET is remote and infrastructure less network which is formed dynamically whenever necessary. Expanding applications and remarkable attributes of MANET has made QoS provisioning its difficulties with malicious activities in the network. Multicast communication is the most reasonable sort of communication right now in various applications [2]. Multicast routing conventions are extensively arranged in tree-based topology [3]. MANETs have numerous constraints for example absence of infrastructure, portability of nodes, dynamic topology, data transfer capacity, security and so forth. MANETs can be verified by utilizing cryptographic devices, key administration, trust, and by verifying the routing [4].

Trust alludes to the performance of the node in which different nodes can depend on and utilize the information received from them. Trust is helpful in various cases like routing, identification of malicious nodes, time synchronization, security levels, dependability, ability of nodes for some observing procedure and so forth.

Trust of any node is the behavior or operations of the node to its neighboring nodes [5]. A believed node consistently works sincerely and sends right data to its neighbors to carry out the responsibilities without turning into an assailant node [6]. Trust can be measured and it is movable or modifiable relying upon the evaluation made by its neighboring nodes.

An ad hoc network can be displayed as a system with associated nodes as appeared in Figure 1 and each node has its own trust table which keeps the trust records of all its neighboring nodes' trusts [7]. The trust table may utilize parameters like, behavior of the node, closeness with the node, genuineness of the node, energy accessible to the node [8]. This trust table is differed when some new perceptions with respect to the neighboring nodes' trust are made. Trust can be characterized in different classifications based on its calculation or its methods for use in working.

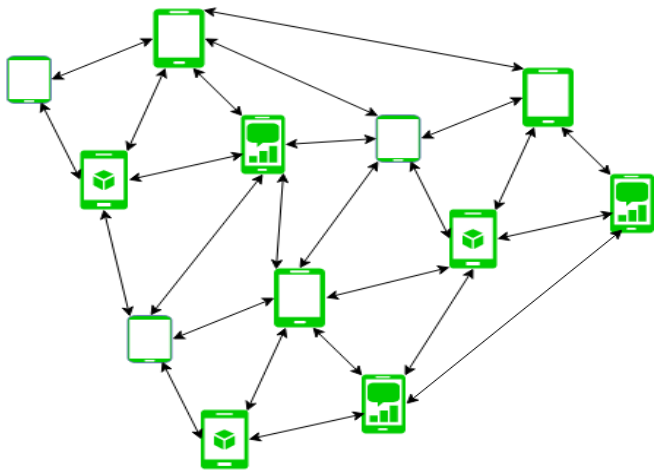

Figure 1. Ad hoc network

In Mobile Ad hoc Network a lot of versatile nodes speak with one another with no central administration, it gives a powerful system design and doesn't utilize any fundamental foundation [9]. Every versatile node contains an information receiver to send and get the information. The transmission of the node is bidirectional to empower them to send and get information through a remote medium. The node limit is constrained to a specific separation; it can speak with nodes that go under the remote scope of the other nodes [10]. The upside of the MANET is its ability to set up communication between at least two groups of nodes with no framework and permitting the gatherings to move the information while the nodes are in active state. One of the problems with MANET is the limited scope of the node. The node, which is available within the scope, can then be talked to [11]. MANET is used for irregular and rapidly structuring a huge number of nodes, an innovation with a wide range of uses, such as strategic interchanges, disaster-helping activity, human services and short-term system management in areas that are not heavily populated. A MANET consists of portable nodes with specialized remote gadgets.

Blockchain is another innovation devoted to the information sharing along with improving security to records the events occurred that cannot be changed once triggered [12]. Be that as it may, this doesn't work a similar route in the various frameworks with various working standards. The blockchain is an innovation for putting away data and transmitting in a straightforward, secure and decentralized way. It would appear that a huge database that contains the historical backdrop of the considerable number of trades made between its clients since the making of the blockchain [1]. The extraordinary element of the blockchain is its decentralized engineering as it is facilitated by a solitary server yet by certain clients [13]. The parts of the blockchain needn't bother with middle people so they can check the legitimacy of the chain and the data and are furnished with security methods that ensure the framework.

Transmissions between organized clients are gathered in blocks and every one of these blocks are approved by nodes called "minors", in light of criteria that rely upon the sort of blockchain [14]. When the block is approved, it joins different blocks and is added to the blockchain. The exchange is then noticeable to the recipient just as the whole system and the transaction is locked without allowing any kind of updates in future.

1.1 Security in Blockchain

The blockchain is as a progression of systems utilized in decentralized systems so as to keep up a steady database among all individuals [15]. It is first proposed by Satoshi Nakamoto to extract the essential strategies of the notable computerized money that is to state the Bitcoin. Not at all like the customary brought together system structure, there are no fixed focal nodes in systems dependent on block strings [16]. The architecture of Blockchain is depicted in Figure 2.

All individuals from the system have generally equivalent positions and store a similar duplicate data of blockchain [17]. Because of the high security and dependability, blockchain has been applied in numerous applications situations and is viewed as one of the key methods to advance the improvement of the world. Blockchain instruments are perfect for this necessity as they hold confirmation and approval, yet accessibility can be given by interruption discovery frameworks. Approval and confirmation might be viewed as an important piece of the trust necessity [18]. By using Blockchain method in MANET, security levels are much improved and routing process is also clear [19]. Blockchain method is involved when a route is identified, nodes involved in communication are fixed, routing table is finalized, source and destination nodes are selected, data packets are transferred to the destination, malicious nodes are identified [20]. All these operations are grouped as a Block and a transaction is finalized. Based on the block generated, the network can be analyzed for detection of malicious nodes in the network and to avoid them thus improving the security levels for data transfer [21, 22]. The process of creating Blocks is represented in Figure 3.

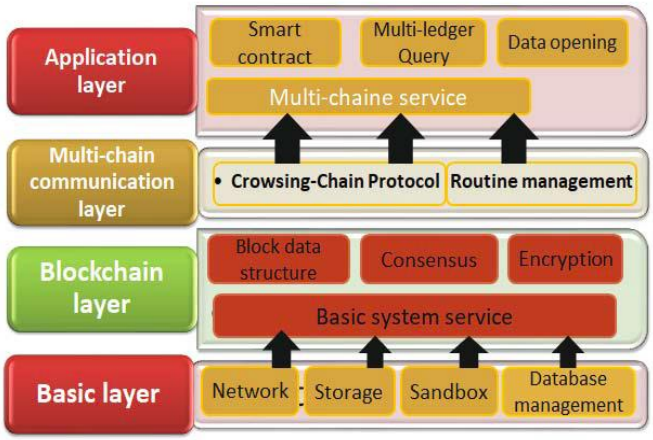

Figure 2. Blockchain architecture

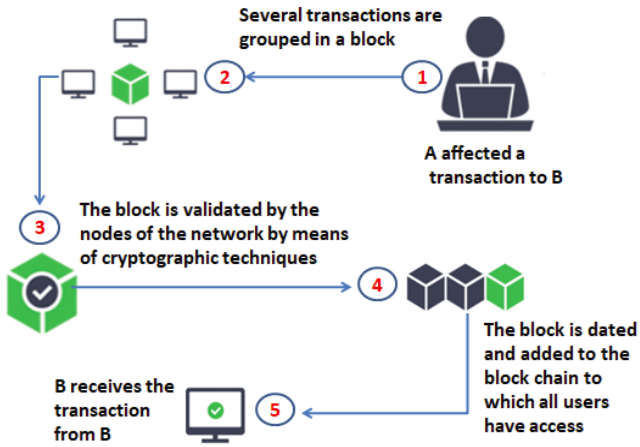

Figure 3. Operating rule of the blockchain

At the point when a few nodes have similar blocks in their fundamental chain, they are considered to have come to agreement [23]. The agreement process comprises of two stages: block approval and the broadest chain selection. These two stages are performed freely by every node [24]. The blocks are communicated on the system, and every node accepting another block retransmits it to its neighbors [25]. In any case, before this retransmission, the node plays out a block approval to guarantee that lone substantial blocks are engendered. There is a broad agenda to follow including the below observations:

- Block structure
- Verifying if the header hash meets the set up problem
- Block size inside anticipated cutoff points

- Verification everything being equal
- Checking the timestamp.

As a drifting and fascinating examination, researchers have been embracing the blockchain in the mobile ad hoc networks [26]. Attributable to its solid qualities, for example, accord, unchanging nature, conclusion, and provenance, the blockchain is used not just as a protected information storage model for basic information yet additionally as a stage that encourages the trustless transfer of information between ad hoc networks. The block structure in a blockchain is represented in Figure 4.

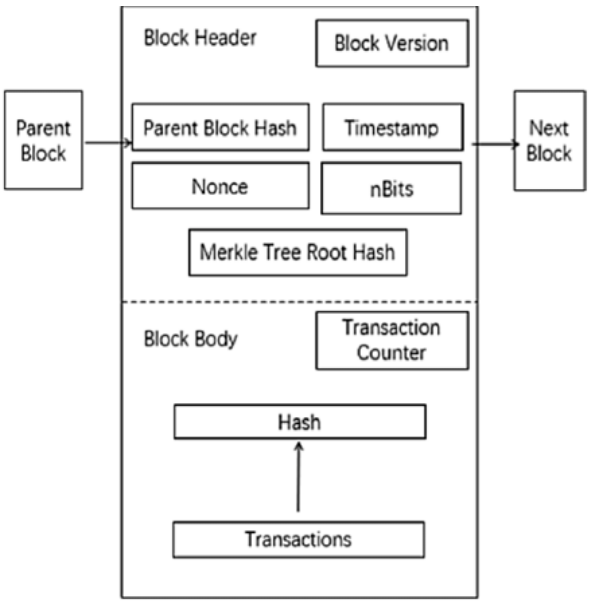

Figure 4. Block structure in Blockchain

The proposed model gives the appropriated trust structure to routing nodes in MANETs that is carefully designed by means of blockchain. Verifying data interchanges in MANETs is perhaps the greatest test for framework in providing security to the data. Blockchain as a potential answer for trust, it has been effectively looked into different fields, including remote systems. To exploit the decentralized idea of blockchain innovation, one must think about the constrained assets of MANETs when structuring a trust framework. The proposed model utilizes a model for generating blocks for every transaction occurred in MANET.

2. LITERATURE SURVEY

Ali et al. [1] proposed a decentralized lightweight verification and key perceptive convention which utilizes single direction hash capacities and bitwise restrictive OR (XOR) tasks. The proposed lightweight convention features a few highlights: it permits dynamic route unit option in the system after beginning arrangement and has obscurity and intractability among other extra highlights. The analysts received a group based system model to lessen the calculation and communication overheads. The model introduce does not verifies the users that perform multi direction model views for transaction updates.

David et al. [2] proposed a model to recompense every member node while routing information bundles. The methodology despite everything necessitates that nodes get to a focal framework, for example, a bank, to send a proof message which shows an information is conveyed. The evidence message incorporates computerized marks and node personalities, to get awards from the bank. This strategy is defenseless, as aggressors can fashion a proof message to be sent to a focal administration framework to create rewards. In this model, attacker is not avoided in sending fake messages to the members involved in communication, that effects the throughput of the system.

The Onion Router proposed by Makridakis et al. [3] utilizes a blockchain-based component for unknown routing. This routing needs an incorporated system since it necessitates that nodes to be allotted to their particular hand-off nodes, after which just these nodes will get the information. The authors introduced adapting routing conventions dependent on open record procedures, whereby data is exchanged as a benefit. The model utilized in the process exhibits a greater number of attacks since numerous nodes enter the network to involve in communication.

Reyna et al. [5] proposed a hybrid methodology for protection of data and validation model which consolidates highlights of group mark based methodologies with restriction of users. As per the analysts, the genuine personality of an intruder can be revealed during the recognition of a malevolent action. Another element of the methodology is the gathering of nodes dependent on regions that are overseen by the cluster head utilizing comparable qualifications, with the goal that can't differentiate between nodes in the gathering. In this model, while performing marking of nodes, validation model fails in detecting malicious users in the system to avoid data loss. The strong authentication model is required to validate the users to avoid malicious operations in the network.

Yeow et al. [7] used a basic blockchain idea to remove the key administration of heterogeneous systems. They joined the blockchain ideas for applications of VANET and Ethereum and empowered a simple, self-directed and decentralized framework. They used the framework for the Ethereum agreement to run a broad variety of uses on an Ethereum blockchain. This model applies an alternative blockchain to the safe spreading of message in ad hoc networks. Interestingly.

Bouaziz et al. [10] have suggested a new coach safety block chain by using an overlay scheme in the blockchain and additional nodes known as overlay block monitors. The organized overlay nodes are bundled with group leaders, who handle the blockchain and operate its principal capacity. The presentation of additional overlay nodes can cause high loads and can fail if the group head is damaged.

Deepa et al. [11] proposed a blockchain model for verifying the communication of smart vehicles by utilizing obvious light association and acoustic side channels. They utilized the blockchain open keys to confirm their proposed component through session cryptographic keys, using both side channels and blockchain open key organization. Furthermore, they utilized various kinds of correspondence for verifying the vehicular system.

Saad et al. [12] proposed the malicious node in the system. The watch dog node is chosen for a specific timeframe dependent on the accessible energy and the accessible storage limit of the node. The watch dog has included the obligation of observing the node for right conduct. It utilizes a cradle to check whether the data is accurately conveyed by the neighbor node. It utilizes two edges speculate limit and acknowledgment edge to pronounce the node as pernicious

and great node individually.

Huang et al. [13] proposed an Intrusion Detection System technique to beat the issues made by the malicious nodes. The irresponsible node utilizes the other node to send and get parcels yet it doesn't take part in the routing to moderate its energy and assets. The source nodes make a Portable Operator (PO) to identify the egotistical nodes in the system. The PO is sent in the route of the data delivery. PO figures the Packet Delivery Ratio (PDR) of each transitional node in the available route. In the event that a node is sending a packet of data and if PDR esteem is more prominent than the limit esteem, PO reports the trouble making of the node to the source node and take necessary action to avoid such malicious nodes in the network.

3. PROPOSED METHOD

Numerous academicians and scientists are attracted to blockchain innovations for its enormous advantages to be picked up in huge fields, including big organizations, networks, medical fields and banking. To be exact, blockchain is an innovation that is in fact involved an unlimited number of obstructions that are associated in a successive request to shape a blockchain and link different blocks. As this innovation is possibly advantageous for usage in huge fields, it has additionally picked up the interest of numerous issues in MANETs. The proposition is to produce a model whereby the reliability of node and message transmitted in MANET is ensured by setting them in an open blockchain by creating individual block for every node transaction.

A basic blockchain would not be appropriate for the avoiding MANET issues. Thus, trust based blockchain system with linked routing method is proposed. The blockchain is the medium to calculate the trust of nodes and creating a block for every transaction for the nodes in the MANET. Figure 4 shows the blocks that are secured to construct a blockchain. The new blocks are communicated after they are generated, where all the nodes in the system check and update the chain of the blockchain. The process of routing is depicted in Figure 5.

The Trust Based Efficient Blockchain Linked Routing Method is performed in following stages:

Stage 1: Establish a MANET with 'N' Nodes.

Stage 2: Select a node as MANET Trust Authenticator Node (MATN)

To select a node as a MATN, a node must satisfy the following conditions

- A Node must have more energy levels when compared to remaining nodes.
- A node must well behave throughout the transaction based on past transactions.
- A node should not behave as a malicious node throughout its transaction.
- A node must have minimum energy consumption rate.

Stage 3: The MATN node will check the Trust Factor of every node and allot a specific value.

Initially 'P' duplicate data packets are created in the MANET and then transferred in the network. A Threshold Time Limit 'T' is set and with in time the packets 'P' must be transferred to the destination. Every node transaction, energy consumption, behavior is stored and based on that, MATN will be selected.

Stage 4: The MATN node will verify the stored data and allots a Trust Identifier Value (TIV) for every node. The MATN will allot a value between '1-60' whose nodes behavior is malicious and values other than the specified range are considered as normal node.

The 'TIV' of a node and its neighbor is calculated as

$$TR(i) = \sqrt[x]{\prod_{i=1}^{N} \mathrm{P}.T_{x,y}} + \mathrm{W}^{\mathrm{i}} + \mathrm{ID(N(i))} \quad (1)$$

where, P is the total packets, T is the trust of a node, x is the instant node and y is the neighbor node.

The time instance 'TI' is also calculated for every node for creating a session for a node which has to complete its operation in time, that is calculated as

$$Tl(Ni) = \frac{RRr - RRs * Rrept - Rreqt}{H} + \mathrm{T_h}$$

Here RRr is the route request received, RRs is the route reply sent, Rrept is the route reply received time and Rreqt is the route request sent time and T_h is the constant value.

Stage 5: To perform routing, nodes whose trust values TIV > 60 only will be considered as malicious nodes are not involved in routing process.

Stage 6: A Route Availability Check (RAC) message is transmitted to all the trusted nodes by the MATN node to all the trusted nodes available specifying the sender node 'SID' and Destination node ID 'DID'.

Stage 7: The MATN node will monitor all trusted nodes and finalize the routing table by considering the nodes which send Route Available (RAV) message. The MATN will check the TIV of all the nodes involved in the routing process before updating the routing table.

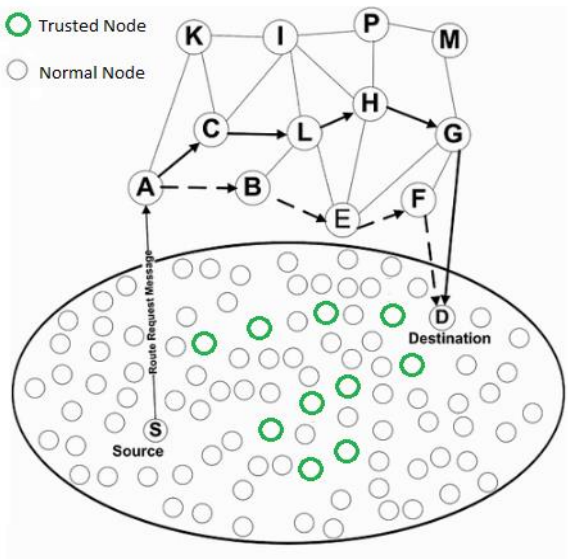

Figure 5. Routing process

Stage 8: After finalizing routing table and the communication is initiated, the MATN node will create a block and also link a block to previous blocks when sender data packets are transferred to its neighbor in Time instance Ti. The process is performed as

Foreach i in (Nodes in MANET)
Block(i) ← null;

Block(i) ← block(i).address+ Ti + physical.address;
if Hash(Block(i)) > Hash(Block(i+1))
Block(i) ←failure;
else
Block(i)+1 ← block(i+1).address+ Ti + physical.address;
Block(Ti) ← Hash(Block(i)) ←Block(i)+1 + Ti
end if
end foreach

Stage 9: When a Block is created for every transaction, each block is linked with previous block and this process is continued until the communication is completed.

The block chain generation is depicted in Figure 6, that represents the complete model in generation of blocks after every transaction. The blocks can be analyzed for identification of malicious activities in the network and also to calculate the packet delivery rate and packet loss ratio to take necessary actions to improve the performance of the network.

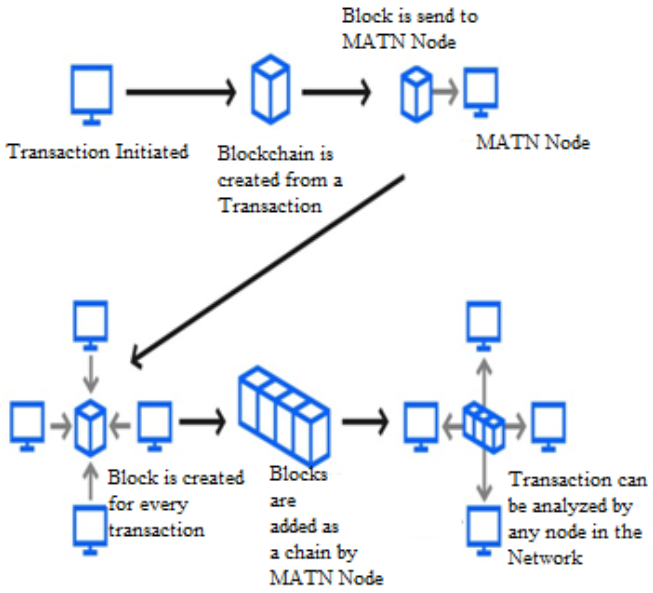

Figure 6. Blockchain generation

4. RESULTS

The proposed Trust Based Efficient Blockchain Linked Routing Method establishes a MANET utilizing NS-2.35 simulator and the parameters used for establishing a MANET is depicted in Table 1.

The parameters used for creating a Blockchain is depicted in Table 2.

The proposed method is compared with traditional methods in terms of Route Identification Time, Security levels during data transfer, Packet Delivery Rate, Packet Loss Ratio, Throughput, Time for creating a Block and Linking to other blocks, Security levels when blockchain is utilized for securing the data in the MANET. The process of crating and linking blocks is depicted in Figure 7.

The Proposed Trust Based Efficient Blockchain Linked Routing Method (TbEBCLRM) is compared with the Low Overhead Localized Flooding (LOLF) and the route identification time is less in the proposed work. The Figure 8 depicts the route identification Time that shows that the proposed method takes less time in identification of secured route.

Table 1. Parameters used

Parameter	Value
MS Version	NS 2.35
X Dimension	2500
Y Dimension	2500
Channel	Wireless Channel
Fragmented Packet Size	1024 bytes
Number of Nodes	50,100,150,200
Antenna	Omni Antenna
Transport	UDP
Propagation Model	Random Way Model
Routing Protocol	AODV

Table 2. Parameters used for creating a Blockchain

Parameter	Default
Chain-Protocol	Multichain
Chain-description	--
Root-stream-name	root
Root-stream-open	true
Chain-is-testnet	False
Target-block-time	15
Maximum-block-size	8388608(8 MB)

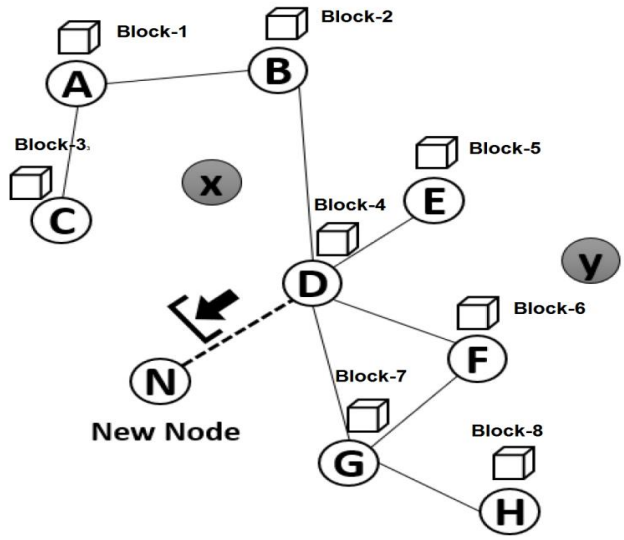

Figure 7. Nodes creating blocks during data transfer

The Proposed Trust Based Efficient Blockchain Linked Routing Method (TbEBCLRM) is compared with the Low Overhead Localized Flooding (LOLF) and the security levels of the proposed method are very high when compared to the traditional method. The Figure 9 illustrates the security levels.

The Packet Delivery Rate comparison levels are clearly illustrated in the Figure 10 and the results depicts that the proposed method is exhibiting better performance.

The Proposed Trust Based Efficient Blockchain Linked Routing Method (TbEBCLRM) is compared with the Low Overhead Localized Flooding (LOLF) and the throughput of the proposed method is high improving the system performance that is depicted in Figure 12.

The Packet Loss Ratio levels are clearly illustrated in the Figure 11 and the results depicts that the proposed method is exhibiting better performance in delivering the data packets to the destination.

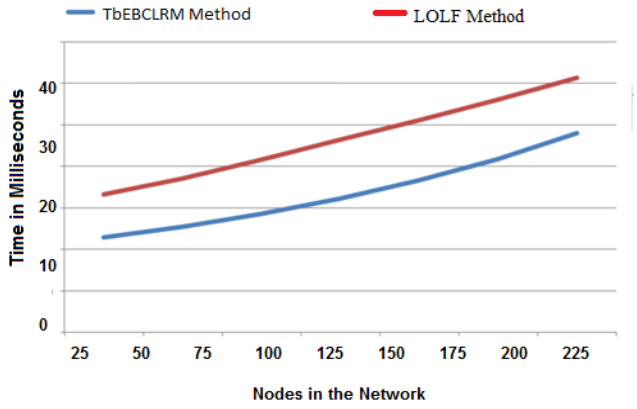

Figure 8. Route identification time

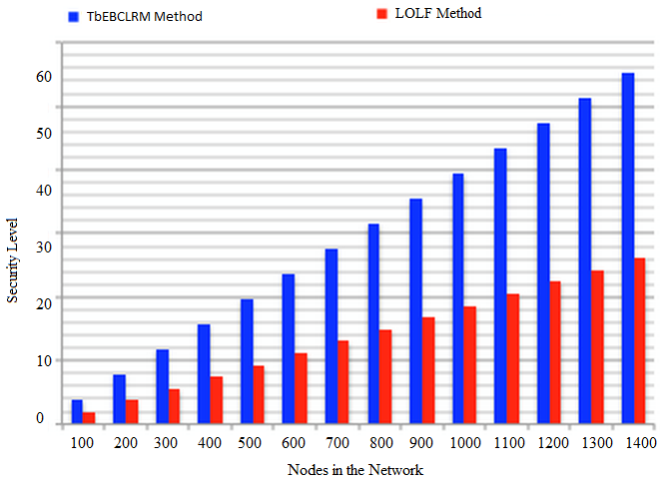

Figure 9. Security levels

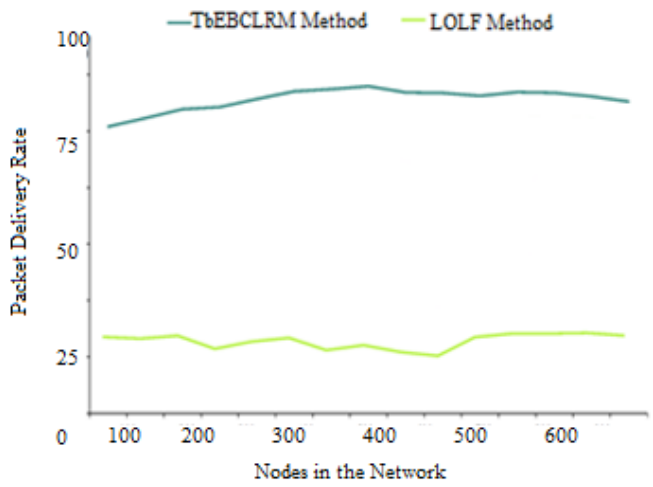

Figure 10. Packet delivery rate

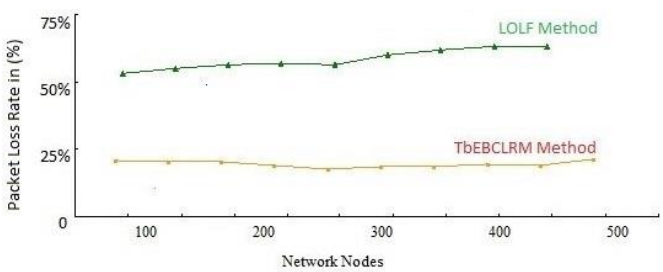

Figure 11. Packet loss ratio

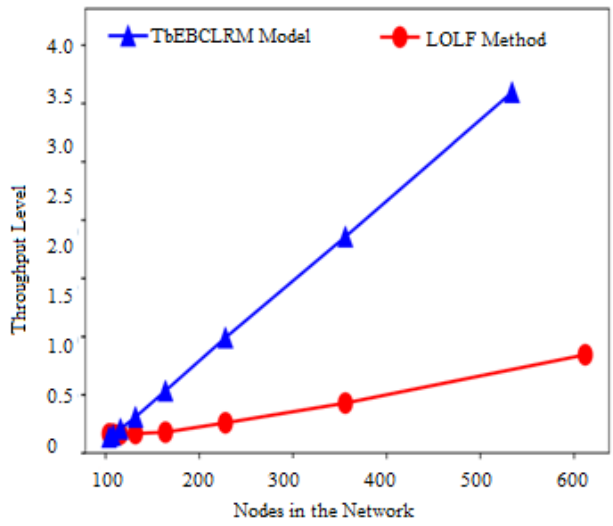

Figure 12. Throughput

The Blockchain transaction blocks are linked to other blocks forming a chain and the transactions cannot be modified or altered that provides the security to users data. The Time levels are clearly depicted in Figure 13.

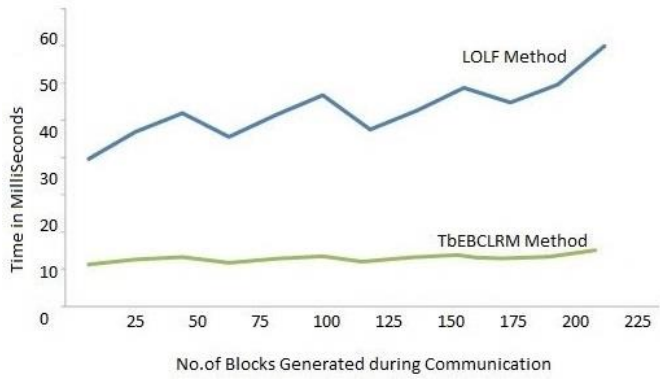

Figure 13. Blockchain linking time levels

The security levels in the MANET when Blockchain methodology is utilized is illustrated in the Figure 14. The proposed method is providing high security when compared to watch dog method.

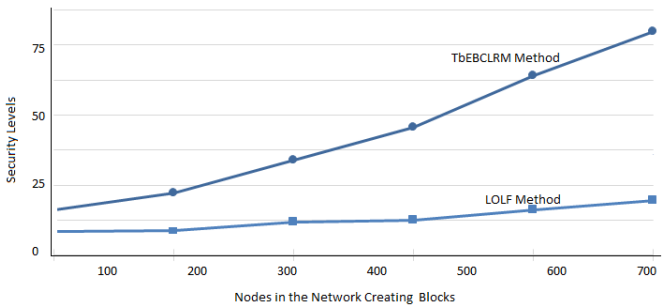

Figure 14. Security when blockchain is utilized

5. CONCLUSION

MANET is an infrastructure less model that is dynamically structured when communications cannot be established via a fixed infrastructure-based network. In order to establish and

use MANET for communication, numerous data transfer nodes must be involved. Data security must be provided for the purpose of preventing malicious network activities. Routing is a way of selecting nodes that have no malicious behavior that needs to be selected with utmost care. In order to provide a reliable routing status and to enhance the display of the routing system, a reliable routing plan will be introduced. The blockchain model provides a plausible plan to route data as a decentralized framework. A blockchain token is used to talk to the routing data packets, and the validator nodes confirming each routing exchange to the blockchain model. Routing nodes can gain dynamic and trusted routing data on the blockchain system by making each routing exchange as a recorder evident and carefully designed. The proposed work is carried out to establish a safe and strong route for the communication of data and to avoid malicious activities in the network. A Trust-based, efficient Blockchain linked routing method is proposed furthermore, MANETs can fulfill the framework objectives, such as reliability, adaptability and accessibility, by using the distributed, carefully designed access to the confidence level of nodes of the system. In future work, in various MANET routing conventions, the feasibility of the proposed plan in selecting routing can be enhanced that can deal with the question of reliability of messages.

REFERENCES

[1] Ali, M., Nelson, J., Blankstein, A., Shea, R., Freedman, M.J. (2019). The blockstack decentralized computing network. Blockstack Technical Whitepaper.

[2] David, B., Dowsley, R., Larangeira, M. (2018). MARS: Monetized ad-hoc routing system (a position paper). 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, pp. 82-86. https://doi.org/10.1145/3211933.3211948

[3] Makridakis, S., Polemitis, A., Giaglis, G., Louca, S. (2018). Blockchain: The next breakthrough in the rapid progress of AI. Artificial Intelligence Emerging Trends and Applications. https://doi.org/10.5772/intechopen.75668

[4] Wong, E.L., Shmatikov, V. (2011). Get off my prefix! the need for dynamic gerontocratic policies in inter-domain routing. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Hong Kong, pp. 233-244. https://doi.org/10.1109/DSN.2011.5958222

[5] Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88: 173-190. https://doi.org/10.1016/j.future.2018.05.046

[6] Cha, S.C., Chen, J.F., Su, C., Yeh, K.H. (2018). A blockchain connected gateway for BLE-based devices in the Internet of Things. IEEE Access, 6: 24639-24649. https://doi.org/10.1109/access.2018.2799942

[7] Yeow, K., Gani, A., Ahmad, R.W., Rodrigues, J.J.P.C., Ko, K. (2018). Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues. IEEE Access, 6: 1513-1524. https://doi.org/10.1109/access.2017.2779263

[8] Qu, C., Tao, M., Yuan, R. (2018). A hypergraph-based blockchain model and application in Internet of Things-enabled smart homes. Sensors, 18(9): 2784. https://doi.org/10.3390/s18092784

[9] Glissa, G., Rachedi, A., Meddeb, A. (2016). A secure routing protocol based on RPL for internet of things. 59th IEEE Global Communications Conference, Washington DC, USA, pp. 1-7. https://doi.org/10.1109/glocom.2016.7841543

[10] Bouaziz, M., Rachedi, A. (2016). A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology. Computer Communications, 74: 3-15. https://doi.org/10.1016/j.comcom.2014.10.004

[11] Deepa, C., Latha, B. (2017). HHSRP: A cluster based hybrid hierarchical secure routing protocol for wireless sensor networks. Cluster Computing, 1-17. https://doi.org/10.1007/s10586-017-1065-3

[12] Saad, M., Mohaisen, A. (2018). Towards characterizing blockchain-based cryptocurrencies for highly-accurate predictions. IEEE Conference on Computer Communications Workshops INFOCOM Workshops (INFOCOM WKSHPS), Honolulu, HI, pp. 704-709. https://doi.org/10.1109/INFCOMW.2018.8406859

[13] Huang, H.Y., Bashir, M. (2016). The onion router: Understanding a privacy enhancing technology community. Proceedings of the Association for Information Science and Technology, 53(1): 1-10. https://doi.org/10.1002/pra2.2016.14505301034

[14] Kiayias, A., Russell, A., David, B., Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. Lecture Notes in Computer Science, 10401: 357-388. https://doi.org/10.1007/978-3-319-63688-7_12

[15] Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. 2016 IEEE Symposium on Security and Privacy, San Jose, USA, pp. 839-858. https://doi.org/10.1109/sp.2016.55

[16] Airehrour, D., Gutierrez, J., Ray, S.K. (2016). Secure routing for internet of things: A survey. Journal of Network and Computer Applications, 66: 198-213. https://doi.org/10.1016/j.jnca.2016.03.006

[17] Anveshini, D. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4): 391-397. https://doi.org/10.1504/ijwmc.2020.108539

[18] Gopi, A.P. (2019). Avoiding interoperability and delay in healthcare monitoring system using block chain technology. Revue d'Intelligence Artificielle, 33(1): 45-48. https://doi.org/10.18280/ria.330108

[19] Mounika, B., Anusha, P. (2020). Use of blockchain technology in providing security during data sharing. Journal of Critical Reviews, 7(6): 338-343. https://doi.org/10.31838/jcr.07.06.59

[20] Pasala, S, Pavani, V., Lakshmi, G. (2020). Identification of attackers using blockchain transactions using cryptography methods. Journal of Critical Reviews, 7(6): 368-375. https://doi.org/10.31838/jcr.07.06.65

[21] Biryukov, A., Pustogarov, I. (2015). Proof-of-work as anonymous micropayment: Rewarding a Tor relay. The International Conference on Financial Cryptography and Data Security, 8975: 445-455. https://doi.org/10.1007/978-3-662-47854-7_27

[22] Goka, S., Shigeno, H. (2018). Distributed management system for trust and reward in mobile ad hoc networks. 2018 15th IEEE Annual Consumer Communications &

Networking Conference (CCNC), Las Vegas, NV, pp. 1-6. https://doi.org/10.1109/ccnc.2018.8319278

[23] Hernndez-Orallo, E., Olmos, M.D.S., Cano, J., Calafate, C.T., Manzoni, P. (2015). CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes. IEEE Transactions on Mobile Computing, 14(6): 1162-1175. https://doi.org/10.1109/tmc.2014.2343627

[24] Raja, L., Baboo, S.S. (2014). An overview of MANET: Applications, attacks and challenges. International Journal of Computer Science and Mobile Computing, 3(1): 408-417.

[25] Schweitzer, N., Stulman, A., Shabtai, A., Margalit, R.D. (2015). Mitigating denial of service attacks in OLSR protocol using fictitious nodes. IEEE Transactions on Mobile Computing, 15(1): 163-172. https://doi.org/10.1109/TMC.2015.2409877

[26] Wu, B., Chen, J., Wu, J., Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. Wireless Network Security. Signals and Communication Technology, pp. 103-135. https://doi.org/10.1007/978-0-387-33112-6_5