ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

Secure IoT Architecture in Mobile Ad-hoc Network Against Malicious Attacks Using Blockchain-based BATMAN

Neha Khandelwal[1*], Shashikant Gupta[1]

[1]Department of Computer Science Engineering, ITM University, Gwalior, INDIA.
**Corresponding Author (Email: neha19khandelwal8@gmail.com).*

Paper ID: 13A6R

Volume 13 Issue 6

Received 05 February 2022
Received in revised form 05 May 2022
Accepted 12 April 2022
Available online 19 May 2022

Keywords:
Internet of things; Wireless Network; Byzantine fault tolerance; Blockchain technology; Trust management; Extended-BATMAN (E-BATMAN).

Abstract

It is possible to build a decentralised wireless network using Internet of Things (IoT) sensors and other IoT-based devices. Wireless connections allow all network nodes to be moved around at will. They can connect and construct a network without current network infrastructure. Using blockchain technology in a wireless ad-hoc context, an IoT-based MANET is a fresh research topic. The key challenge for ad-hoc blockchain applications is to cope with the high computational cost of block validation while keeping blockchain features and incorporating nodes. This article presents a blockchain-based mobile network as a potential application of the ensemble approach, which has been covered in other articles. The suggested technique for MANETS routing uses the Byzantine Fault Tolerance (BFT) protocol. It is possible to integrate Blockchain into an IoT-based MANET (BATMAN) using advanced mobile ad-hoc networking (MANET) (BATMAN). Extended-BATMAN (E-BATMAN) is a method of integrating blockchain technology into the BATMAN protocol using IoT-based MANETs. Blockchain is a safe, distributed, and trustworthy platform, with each node performing its security procedures. Four characteristics are used to evaluate the proposed ensemble method: pdr, average e2e latency, network throughput, and algorithm vitality use. All of these components outperform the existing traditional techniques using the recommended ensemble approach.

Disciplinary: Information Technology.

Cite This Article:

Khandelwal, N., Gupta, S. (2022). Secure IoT Architecture in Mobile Ad-hoc Network Against Malicious Attacks Using Blockchain-based BATMAN.*International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 13*(6), 13A6R, 1-15. http://TUENGR.COM/V13/13A6R.pdf DOI: 10.14456/ITJEMAST.2022.123

1 Introduction

Blockchain technology, first announced by Satoshi Nakamoto in 2008, is still used today (Nakamoto, 2019). Network segmentation happens when two separate chains split apart. Because two chains cannot coexist, one of the links is routinely removed. Data loss may be the root of the problem. Thoughts on the long-term value of a new kind of Blockchain with high network distribution capabilities (Cordova et al., 2020). On-demand distance vector routing (AODV) (Perkins et al., 2003) and BATMAN (Clausen et al., 2003) are three innovative MANET protocols designed to overcome this issue (Sanchez-Iborra et al., 2014). Varaprasad The nodes determine the optimum forward route and push packets appropriately.

According to Laube et al. (2019), a DAG-based architecture may handle the partitioning problem in a MANET with mobile nodes. When the network topology changes, the partition problem arises. The BATMAN routing protocol, presently being developed by the German "Freifunk" community, enabled this. It will be replaced by the more efficient OLSR (Kulla et al., 2012a). The lack of trustworthiness of blockchains has only recently been realized as a mechanism to produce the demand for collaborative components in diverse frameworks, on the current situation of agreements with blockchain-enabled in-process sending motivations for multi-hop (Machado and Westphall, 2021).

Many researchers have been working on developing a secure network communication system. (Omar et al., 2012) devised an authentication technique that verifies connections are safe before any network communication can occur. Because MANETs are continually changing, a hostile actor may get the private key even if no unauthorized outsiders are present (Eschenauer et al., 2002). Yang et al. A protocol based on the system's ability to withstand Byzantine Generals faults (BFT) was designed to conduct blockchain operations (Kotla and Dahlin, 2004). A few nodes fail or behave maliciously, but the BFT system continues to operate (Aublin et al., 2013). We use DCFM (L, 2020a; S., 2015) to identify hostile intruders from trustworthy nodes. Lwin and coworkers (Lwin et al., 2020a) call it one of the most efficient systems recently suggested (2020a). The suggested system assessment mechanism, based on blockchain technology, can satisfy MANET goals.

When it comes to our work, we divide it into four separate phases that we call our framework: When the Trust value is determined, the second stage, delegated BFT, is used to pick the speaker, and the third stage uses delegated BFT based on the Extended-BATMAN protocol for transaction claims/node validation and block construction, and the fourth stage does maintenance.

2 Literature Review

This part describes several ways the suggested algorithm may be supported in various circumstances.

2.1 BATMAN: A Brief Overview

Please remember that the Batman protocol decentralizes route information, which means that routing tables are not available to the whole network through the Batman protocol (Sliwa and colleagues, 2019). It is decided which single-hop neighbours will be assigned to each node in the mesh to offer the best feasible gateway for communication with the destination node. The result is developing an efficient and very fast routing system that allows for establishing a collective intelligence network while using little CPU and, therefore, requiring less energy consumption on the side of each node (Johnson et al., 2008).

This strategy has piqued the scientific community's curiosity. As a result, a lot of effort is done to evaluate routing efficiency under various scenarios. For example, Kulla et al. (2012)b analyze their system's performance in multiple settings and node situations (Kulla et al., 2011, 2010).

2.2 BATMAN's Attack Mitigation Scheme

As an example of a normal project, we have taken the concepts from this project and incorporated them into the recommended project. It is necessary first to discuss NIAs (Node Isolation Attacks), which are attacks that are specially addressed by denial contradictions with fake node mechanism, before moving on to the topic of denial contradictions with fake node mechanism itself. It was Kannhavong et al. who first reported about NIAs, which are a kind of denial-of-service attack on the OLSR (2006).

2.3 Trust Management in MANET via the Use of Blockchain

A blockchain is a chain of records linked together. In addition to the date, each Block contains a hash reference to the previous Block. Each successive Block binds itself to the previous Block's hash by connecting to it, and the Blockchain is established as a result of this linking. When it comes to data manipulation, blockchain architecture has shown to be quite durable.

The development of blockchain-based applications has accelerated significantly in recent years. These applications are being used in various fields, including concurrent IoTOS (IoT), economic facilities, standing schemes, and others. Mining produces a block, which requires a substantial amount of computer power and is also a probabilistic endeavour. While block mining is challenging, determining whether or not a block is valid is not tricky (Dennis and Owen, 2015). A distributed reputation model based on Blockchain technology was created by Peiris and colleagues (2020) to ensure trust, and it is now being tested. B4SDC is a blockchain-based approach for gathering security-related data in MANETs developed by several academics, including Liu et al. (2020) and other researchers.

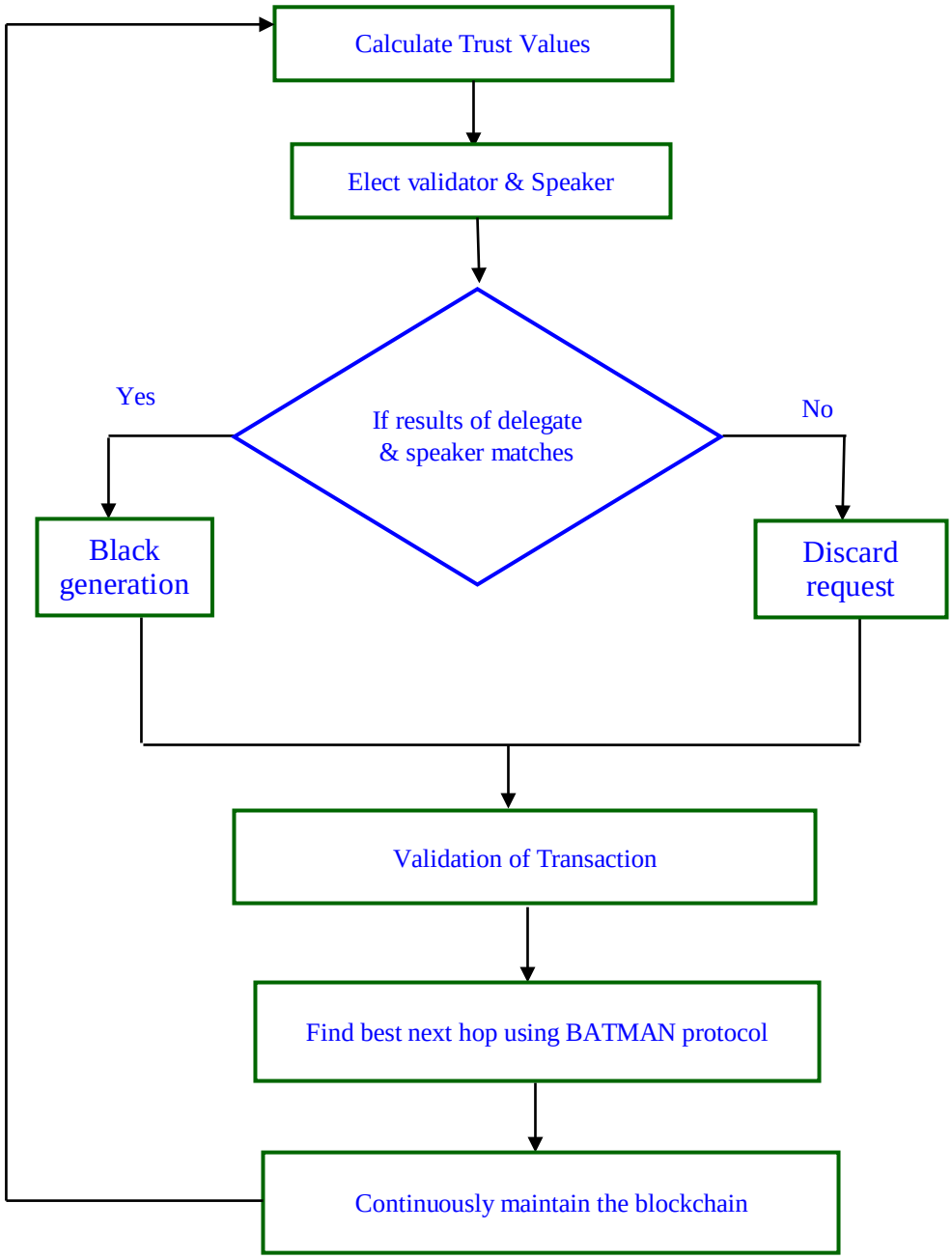

Figure 1: The suggested architecture's workflow diagram.

3 Method

We propose a distributed trust installation system based on blockchains throughout this article. We chose a blockchain-based architecture to handle trust in the IoT-based MANET ecosystem to accomplish so. Its high resource usage and extended validity time make it unsuitable for use in dynamic and latency-sensitive situations. The suggested system has multiple components, as shown in Figure 1.

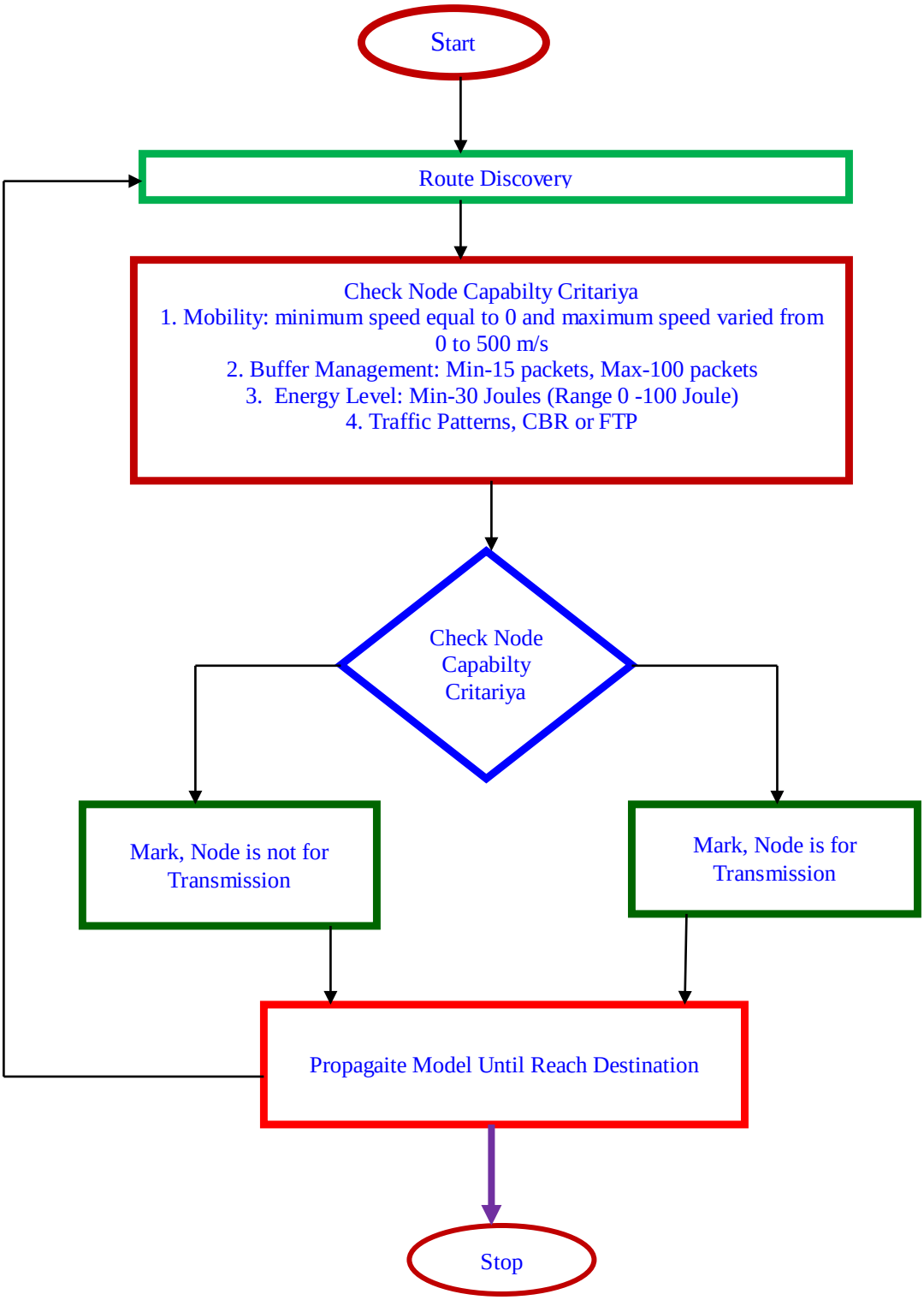

Figure 2: The Flow for computing the Trust Value.

3.1 Step 1: Calculation of the Threshold Value

This investigation was conducted to determine whether a distributed trust mechanism might be developed to improve the stability and scalability of networks. Rather than concentrating on the computation of trust value, we focus on creating the trusted network instead. The presence of an adversary near a node results in information about the attacking node being propagated across the network, reducing the possibility of that same attacker striking again. Our proposed system uses several different discovery and belief models; however, we chose denial contradictions with a fake

node mechanism (Schweitzer and colleagues, 2015) as an example of a typical scheme suited for the solution presented in this research.

An enemy node is identified in the network, and information about it is broadcast across the web for it to be removed from the network. This is made possible by the use of blockchain technology. Figure 2 illustrates the process of determining how to determine Trust Value.

As the AIMD system (Marti et al., 2000) regulates each node's Trust Value (TV), it provides clear and fair incentives and punishments for residential nodes and MANET enemies. Because of the moniker "addition and multiplication," the TVs of the node are added and multiplied together, with addition and multiplication factors () and () being used in the equations for addition and multiplication, respectively, to accomplish this. The denial contradicts the fake node mechanism detection technique using a heuristic approach to detection. To compute a network penalty, multiply the TV of the attacker node by the -1 number, which is the harshest network penalty that may be applied. As a result, negative TV node information is propagated throughout the network.

Since each resident owns the information, they may exclude particular nodes from the connection check. A trust rating of -1 signifies that the node cannot join the network. In equation 2, selfish nodes are represented by a different value. On the other hand, a functional node will contribute to the growth of the TV by increasing its value. To guarantee that the trust level decision is fair, a high TV of MPR nodes should be maintained.

As a consequence, it should be maintained at all times. Consequently, following equation 3, the value is altered. The MPR node's default value is 0.7. In the near term, it will be based on honest nodes that are not MPRs, and in the long run, it will be based on MPRs. Every node starts with a zero value but may gain the maximum trust value of "1" throughout the game. Each node has a TV value of zero when the network is created. In Equation 3, the numerator, i.e., $\sum_{k=1}^{n-1} m_i j^k m_i j^k + 1$ I pick j as its MPR node to relay packets for k iterations from when j connects to I to when I calculate j^s TV.

$$TV = \begin{cases} TV * \beta \ if \ nodes \ misbehabes \\ TV + \alpha, otherwise \end{cases} \quad (1)$$

$$\beta = \begin{cases} -1 \quad if \ nodes \ is \ attack \\ 0.7, \qquad otherwise \end{cases} \quad (2)$$

$$\alpha = \begin{cases} \max\left[\frac{\sum_{k=1}^{n-1} M_{ij}^k}{\sum_{k=1}^{n-1} M_{ij+1}^k}, \ 0.5\right] & if \ node \ is \ MPR \\ 0.5, & otherwise \end{cases} \quad (3)$$

$MPR \rightarrow$ multipoint relay selector set.

Algorithm 1. Trust Value Computation

1. Begin()
2. {
3. Routs discovery initialize, current position initialize
   {

4. Motion = 0 <motion< 500m/s
5. Buffer_Queuemanaging = 15 < Buffer_Queue< 100
6. Vitalitynear = 0 <vitality< 100
7. Traffic flowoutline = CBR or FTP
8. }
9. If(Node ability == yes)
10. {
11. Mark node for transmission
12. }
13. Else
14. {
15. Leave the node
16. }
17. While(current position == destination0
18. {
19. Repeat (3 to 16)
20. }

A collaborative approach to our security solutions is also being implemented to boost total system efficiency via collaboration. Even though MANETs (Hernandez Orallo et al., 2014) were previously classified as cooperative networks, early nodes undertake distinct detection processes for most security modes. This is illustrated in Figure 1 and is contrary to previous assumptions about cooperative networks. In denial of contradictions with the fake node mechanism, the search is performed after each Hello interval. However, since our strategy reduces the investigation duration in proportion to the number of neighbours around the node, the synergistic impacts of near surrounding nodes may aid in lengthening the inquiry interval in some circumstances, as shown in Figure 1. Rather than evaluating nodes individually, nodes that meet the following criteria may be examined collectively, as shown in the accompanying picture (Lwin et al., 2020a).

The first method, referred to as Algorithm 1, specifies the procedures that must be followed to calculate the trust value (TV). Line 1 has been finished with completing the route finding process and identifying the present location. On-Line 2, there is a check for node capability performed. Then, as noted in Line 5, you may either select the node for transmission or leave the node undesignated for the message. This is followed by a comparison of the current location and target position. If the current location matches the target position, the procedure is repeated from step 1 through step 5 until the target position is reached.

3.2 Step 2: Algorithm of dBFT

It is necessary to determine the trust values before proceeding with the construction of the proposed model. In the case of the nodes, this is true. The model is generated when the trust values of the nodes have been computed. The selection algorithm chooses a validator node from among the candidates. After that, the Delegated Byzantine Fault Tolerance (dBFT) system selects a speaker from among the available candidates. The node that survives acts as a delegate for the remainder of

the network's operations. Following that speaker's presentation, delegates are handed a proposal once the claims have been validated and hashes have been created. Algorithm 2 shows the dBFT steps.

Procedure 2: Delegated_Byzantive_fault_tolerance

TV- Array of belief number of hig_hours

Begin()

{

V = max(TV)

Bully election(V);

Return coordination validator

}

V→ Arrays of nodes eligible to become a validator

A popular vote selects the Validator. These are the nodes qualified to serve as validators in the network, and they are those with the highest TVs. The bully election approach (Hernandez-Orallo et al., 2014) determines which node is the block creator node among a set of similar nodes.

The permission of a nearby node is required for a trustworthy election, unlike a bully election. Neighbours with TVs over the threshold will send claim messages to each other. I j, TV-Claim, one-hop-count) prKeyi j's beliefworth and single-hop neighbour total are placed into single-hop-counter, correspondingly. The claim message is signed using I prKeyi's private and i's public keys. Also, any node with TVs over the threshold may broadcast a claim message to the whole network by piggybacking on a transmission control message (TCM). The Validator is the letter j if all of the following conditions are satisfied. This node has the highest TV and no false allegations against it. No fraudulent claims were made against nodes I and j. Unable to pick between dual or additional nodes with a similar belief value, a claim message has an extra one-hop count. In this case, the Validator is the node with the most one-hop counts. By broadcasting a claim message for node j, node I save energy. The most frequent voter should be rewarded since MANET is resource-intensive.

It's a process. A decision method is used to choose specific nodes from the list of accessible nodes to function as validation nodes. Assigning a speaker node and all other functions to representations simplifies the procedure. Inquiry representatives get hashed values for each outstanding accusation from the speaker. Next, a novel chunk of privileges or communications is supplementary if the comparison between the speaker and the representative is more than 68.9%—algorithm three delegated authority.

Algorithm 3: Delegation Process

1. Begin()

2. {
3. CN = Validators // CN contains array of validators
4. Choicepresenter S from CN, and cogitate all remains as representatives D.
5. S is answerable for buildingnovelchunk from to comeprerogatives.
6. S confirm and analyze hash
7. D validate(outcomes of S)
8. D portion&relate (results of S)
9. IF (sk_P ≥ 68.9%)
    {

    Chunksupplementary

    }

    Else

    {

    Rejectinvitation

    }
10. }
11. End()

3.3 Step 3: Block Authentication and Block Creation

It's a process. A decision method is used to choose certain nodes from the list of accessible nodes to function as validation nodes. Assigning a speaker node and all other functions to representations simplifies the procedure. Inquiry representatives get hashed values for each outstanding accusation from the speaker. Next, a novelchunk of prerogatives or communications is additional if the comparison between the speaker and the representative is more than 68.9 percent—algorithm 3 delegated authority.

3.4 BATMAN Extended Version (EBATMAN)

It is possible to summarise the BATMAN protocol in the following way in a simplified form: The initial message, also known as the OGM, is sent to the whole network by each node to alert its neighbours that it has been discovered and is functioning properly. The IP and UDP overhead associated with the transmission is typically 52 bytes. To begin with, the OGM has the following data: the sender's address, the node that delivered the packet, the time between packets (TTL), and the sequence number.

The network selectively floods the overlay mesh network (OGM), notifying receiving nodes of other nodes' existence and letting them connect with them. The fact that an X node obtains its OGM from another node implies a Y node. It occurs when one of node Y's one-hop neighbours requests OGM from the other node. Node X receives messages quicker and more reliably with several single-hop neighbours. This improves throughput and reliability. The neighbour must transfer data via the network to connect with the distant node. Determining this neighbour as the optimal next hop for the message sender at that moment, the protocol configures its routing table

to use this neighbour. As seen in Process 4, the various stages of The Improved Method to IoT based MANET protocol are described.

Algorithm 4: The Better Approach to Mobile Ad-hoc Networking Routing Protocol Algo:

Begin()

{

1. Respectively node Brodcost O_G_Ms to her neighbours
2. Neighbours re-Broadcast O_G_M'S to prove their existence

   O_G_M's areoringator msg's of size 52 byte.

   Counting IP SUDP over_head
3. If(node_neighbour > 1)
4. {
5. Best nop node= current node;
6. }
7. Else {
8. Repeated (1,3)
9. }
10. }
11. End()

Blocks are organized in a certain way. The block structure must also contain information about how the representative node configures the Block. A block of transactions recorded in a blockchain system binds the network together. Because the hash value is produced directly from the transaction data, it must provide a hash value using the SHA-256 technique in the Block. As a consequence of this, instability is brought into the blockchain ecosystem.

3.5 Maintenance on the Block

Full and lite nodes are the two kinds of nodes in a blockchain ecosystem. Both maintain the whole Blockchain, but the latter relies significantly on the information provided by the entire node community to work successfully. This is due to the nature of MANETs. A new node is allowed admittance to the network's blockchain information.

First, a lightweight nodule is deployed to the system, able only to download data from the blocker's header. This is the first step. Although a new node enters the network as a light node, it may quickly create transactions for attacker detection/TV calculation. Until a full node becomes available, the mass node actions as a temporary complete node for the communicate chunk headers.

4 Result and Discussion

The investigational findings acquired via the suggested technique are described in this segment. Experiment 1: Results Network performance is measured by characteristics including pdr,

average e2e latency, setup throughput, and vitality use. This outcome subdivision contains 105 moveable nodes connected to the network for 105 mobile nodes.

4.1 NS2 Simulation Constraints

This evaluation of the planned method and the current algorithm is shown next. The simulation parameters are presented in Table 1.

Table 1:- Simulation Constraints

Parameters	Specification	Parameters	Specification
Network Simulator	NS-2, Version 2.35	PHY/MAC Protocol	IEEE 802.11
Network Size	1km x 1km	Propagation Model	Two-ray ground
Connection Protocol	UDP/TCP	Mobility Model	Random Way Point
Traffic type	Constant Bit Rate (CBR)/FTP	Channel Type	Wireless Channel
Source/Destination	Random	Antenna Model	Test-parabolic
Data packet size	256 bytes	Simulation time	200 Second
Data packet size	256 bytes, 512 bytes, and 1024 bytes	Language	Tcl,oTcl,C++, AWK Scripting
Simulation Protocol	BATMAN, E-BATMAN	No. of Malicious Node	5% out of the scenario
Simulation Scenario (No. of Mobile Nodes)	25,50,75,100,125	Channel Type	Wifiphy Standard

4.2 Performance Calculation

Throughput: The throughput (TP) of a network equals the total of the data sent to the based station divided by the time it takes to simulate the network.

Average end-to-end delay: The average end-to-end delay (AED) is the total time it takes for all data chunks to transit from the source nodes to the base station.

The term "end-to-end delay" refers to the time it takes a packet to transit from its point of origin to its point of destination.

Packet delivery ratio: The PDR is the fraction of informations packets transferred to packets received at a certain time (Taha et al., 2017).

4.3 Outcomes

The Extended-BATMAN algorithm is compared to the present BATMAN protocol. This study's average throughput and E-BATMAN approach are shown in Figure 3. Figure 3 explain throughput, units of throughput are kbps. We have to compare three scenarios on different numbers of nodes. Scenarios like BATMAN _MANET Normal Scenario, BATMAN_MANET Under Attackers, BATMAN_MANET [Lwin MT [2020b]] with Attackers, Proposed _BBATMAN_MANET with Attackers. Nodes like 25, 50,75,100,125 are compared to all these scenarios. In normal scenarios maximum of 1024 kbps and a minimum of 942 kbps of throughput. In Under Attackers scenarios maximum of 226 kbps and a minimum of 215 kbps of throughput. In [Lwin MT [2020b]] with Attackers scenarios maximum of 1032 kbps and a minimum of 978 kbps of throughput. In Proposed

_BBATMAN_MANET with Attackers scenarios maximum of 1245 kbps and a minimum of 1235 kbps of throughput.

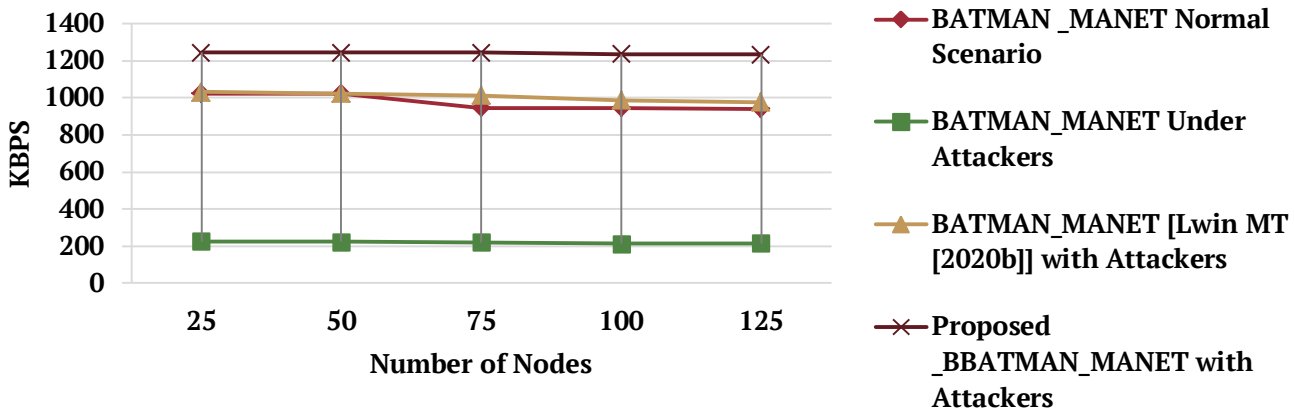

Figure 3: Average throughput (kbps) under attack

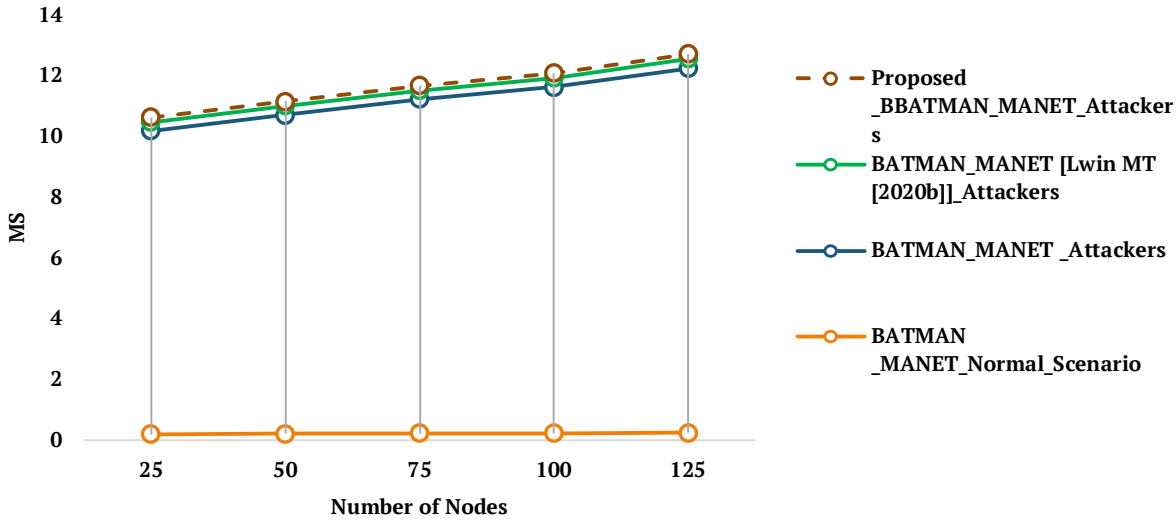

Figure 4: Average e2e-delay test results.

Figure 4 explains e2e-delay, units of end-to-end delay are milliseconds. We have to compare three scenarios on different numbers of nodes. Scenarios like BATMAN _MANET Normal Scenario, BATMAN_MANET Under Attackers, BATMAN_MANET [Lwin MT [2020b]] with Attackers, Proposed _BBATMAN_MANET with Attackers. Nodes like 25, 50, and 75,100,125 are compared to all these scenarios. In normal scenarios maximum of 0.26 ms and a minimum of 0.21ms of e2e delay. In Under Attackers scenarios maximum of 12ms and a minimum of 10ms of e2e delay. In [Lwin MT [2020b]] with Attackers scenarios maximum 0.31ms and minimum 0.28ms of e2e delay. In Proposed _BBATMAN_MANET with Attackers scenarios maximum of 0.17 ms and a minimum of 0.15 ms of e2e delay.

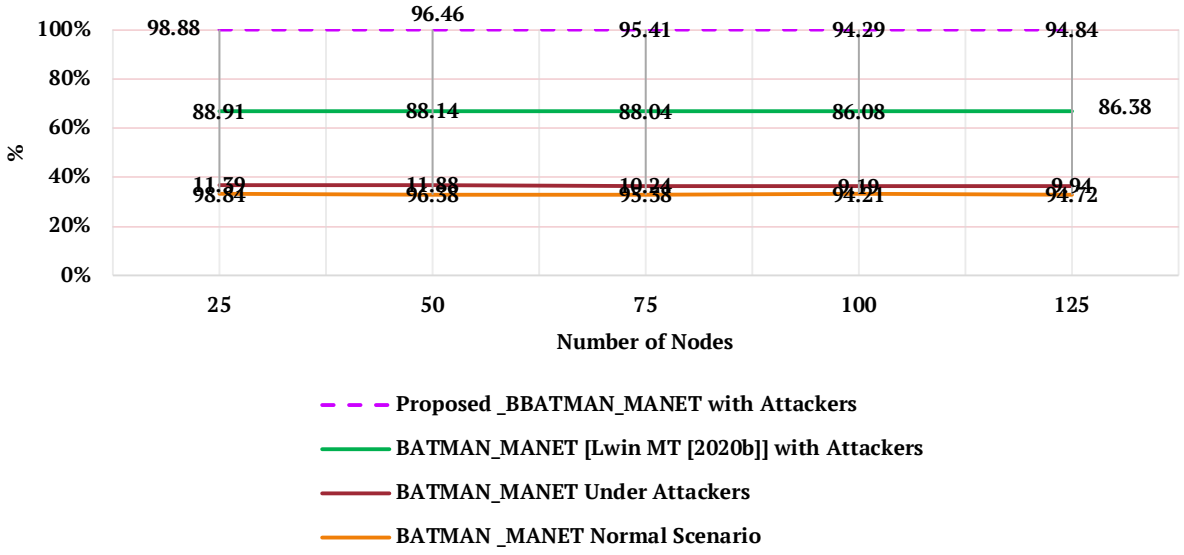

Figure 5: Average Packet Delivery Ratio under Attack.

Figure 5 explain about Packet Delivery Ratio (PDR), units of PDR are percent (%). We have to compare three scenarios on different numbers of nodes. Scenarios like BATMAN _MANET Normal Scenario, BATMAN_MANET under Attackers, BATMAN_MANET [Lwin MT [2020b]] with Attackers, Proposed _BBATMAN_MANET with Attackers. Nodes like 25, 50, 75, 100, and 125 are compared to all these scenarios. In normal scenarios maximum of 98.84 % and a minimum of 94.72 % of the Packet Delivery Ratio. In Under Attackers scenarios maximum of 11.39 % and a minimum of 9.94 % of Packet Delivery Ratio. In [Lwin MT [2020b]] with Attackers scenarios maximum of 88.91 % and a minimum of 86.38 % of Packet Delivery Ratio. In Proposed _BBATMAN_MANET with Attackers scenarios maximum of 98.88 % and a minimum of 94.84 % of Packet Delivery Ratio.

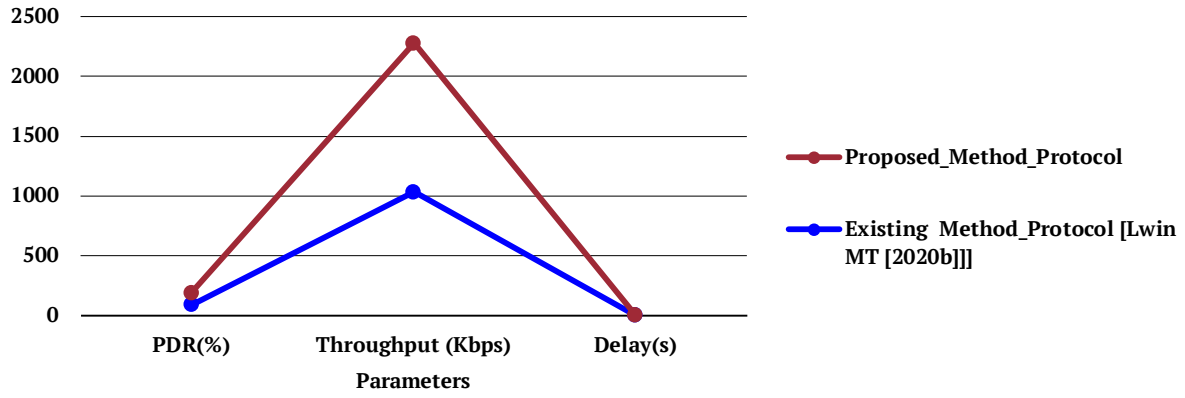

Figure 6: An evaluation of the proposed E-BATMAN protocol compared to the current BATMAN protocol using evaluation parameters (Lwin et al., 2020b).

Figure 6 shows the results of comparing parameters such pdr (%), latency (s) and throughput (kbps). The suggested method outperforms earlier work (Lwin et al., 2020b) on all criteria.

5 Conclusion

This research suggested a unique technique for generating distributed trust value in MANETs, which is described in detail below. The blockchain idea was applied in the Better Approach to Mobile Ad-hoc Networking protocol, dubbed Extended the Improved Method to

Mobile Ad-hoc Networking (Enhance-BATMAN). The model outcomes indicated that a distributed trust value gives high network safety. Using the proposed E-BATMAN protocol ensures no data is lost even if the attacker moves and attacks other network nodes, lowering overall complexity. The network is safe. Aside from that, respectively node's role is summary. Our MANET-based blockchain-based proposed system is also consistent and accessible. We want to examine our suggested solution in MANETs with various routing protocols in the future.

6 Availability of Data and Material

All information is included in this study.

7 References

Aublin PL, Mokhtar SB, Que'ma V.Rbft: Redundant byzantine fault tolerance. In 2013 IEEE 33rd International Conference on Distributed Computing Systems. 2013: 297-306.

Clausen T, Jacquet P, Adjih C, Laouiti A, Minet P, Muhlethaler P, Qayyum A, Viennot L. Optimized link state routing protocol (OLSR). 2003. http://hal.inria.fr/inria-00471712

Cordova D, Laube A, Pujolle G, et al. Blockgraph: A blockchain for mobile ad hoc networks. In 2020 4th Cyber Security in Networking Conference (CSNet), IEEE. 2020:1-8.

Dennis R, Owen G. Rep on the Block: A next generation reputation system based on the Blockchain. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE.2015:131-8.

Eschenauer L, Gligor VD, Baras J (2002) On trust establish- ment in mobile ad-hoc networks. In: International workshop on security protocols, Springer.2002:47-66.

Hernandez-Orallo E, Olmos MDS, Cano JC, Calafate CT, Manzoni P.Cocowa: A collaborative contact-based watchdog for detecting selfish nodes. IEEE transactions on mobile computing. 2014;14(6):1162-75.

Johnson D, Ntlatlapa NS, Aichele C (2008) Simple prag- matic approach to mesh routing using batman.2nd IFIP International Symposium on Wireless Communications and Information Technology in Developing Countries, CSIR, Pretoria, South Africa.

Kannhavong B, Nakayama H, Kato N, Nemoto Y, Ja- malipour A.Analysis of the node isolation attack against olsr-based mobile ad hoc networks.In 2006 International Symposium on Computer Networks, IEEE, 2006:30-5.

Kotla R, Dahlin M. High throughput byzantine fault tolerance. In 2004International Conference on Dependable Systems and Networks, IEEE. 2004:575-84.

Kulla E, Ikeda M, Barolli L, Miho R. Impact of source and destination movement on manet performance considering batman and aodv protocols. In 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, IEEE. 2010:94-101.

Kulla E, Ikeda M, Hiyama M, Barolli L, Miho R. Performance evaluation of olsr and batman protocols for vertical topology using indoor stairs testbed. In2011 International Conference on Broadband and Wireless Computing, Communication and Applications, IEEE. 2011:159-66.

Kulla E, Hiyama M, Ikeda M, Barolli L. Performance comparison of OLSR and BATMAN routing protocols by a MANET testbed in stairs environment. Computers & Mathematics with Applications. 2012a;63(2):339-49.

Kulla E, Ikeda M, Oda T, Barolli L, Xhafa F, Takizawa M. Multimedia transmissions over a manet testbed: problems and issues. In the6th International Conference on Complex, Intelligent, and Software Intensive Systems, IEEE.2012b:141-147.

Laube A, Martin S, Al Agha K. A solution to the split & merge problem for blockchain-based applications in ad hoc networks. In the 8th International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), IEEE. 2019:1-6.

Liu G, Dong H, Yan Z, Zhou X, Shimizu S. B4SDC: A blockchain system for security data collection in MANETs. IEEE Transactions on Big Data. 2020.DOI: 10.1109/TBDATA.2020.2981438

Lwin MT, Yim J, Ko YB.Blockchain-based lightweight trust management in mobile ad-hoc networks.Sensors. 2020;20(3):698.

Machado C, Westphall CM. Blockchain incentivized data forwarding in manets: Strategies and challenges. Ad Hoc Networks. 2021;110:102321.

Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehaviour in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on Mobile computing and networking, 2000;255-265.

NaOmar M, Challal Y, Bouabdallah A. Certification- based trust models in mobile ad hoc networks: A survey and taxonomy. Journal of Network and Computer Applications. 2012;35(1):268-286

Peiris P, Rajapakse C, Jayawardena B. Blockchain-based distributed reputation model for ensuring trust in mobile adhoc networks. In 2020 International Research Conference on Smart Computing and Systems Engineering (SCSE), IEEE.2020:51-56.

Perkins C, Royer EM, Das S. Ad-hoc on demand distance Vector routing (AODV). 2003. http://media.gradebuddy.com/documents/3107203/4e440567-1f3b-4e47-8585-8d2c24b05758.pdf

Sanchez-Iborra R, Cano MD, Garcia-Haro J. Performance evaluation of batman routing protocol for voip services: a qoe perspective. IEEE Transactions on Wireless Communications. 2014;13(9):4947-4958.

Neha Khandelwal is a Research Scholar at the Department of Computer Science Engineering, ITM University, Gwalior, India. She got a Masters's degree in Artificial Intelligence from VaishnavCollege of Engineering, Indore, India. Her research is related to Computer Applications and Modern Computer Technology.

Dr.Shashikant Gupta is an Associate Professor at the Department of Computer Science Engineering, ITM University, Gwalior, India He got his Master's and Ph.D. degrees in Information Technology in Engineering. His research encompasses Computer Applications and Modern Computer Technology.

Note: This article is an extended work of the previous article entitled "Blockchain-based BATMAN protocol using Mobile ad-hoc Network (MANET) with an Ensemble Algorithm" https://doi.org/10.21203/rs.3.rs-673489/v1