International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209695 Volume 8, Issue 4, July – August (2021)

RESEARCH ARTICLE

Blockchain-Enabled Consensus Routing Protocol Improving the Security Data Communication in Internet of Things Applications

Monika Parmar
Chitkara University School of Engineering and Technology, Chitkara University, Himachal Pradesh, India.
monika.parmar@chitkarauniversity.edu.in

Harsimran Jit Kaur
Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India.
harsimran.kaur@chitkara.edu.in

Received: 29 May 2021 / Revised: 01 July 2021 / Accepted: 07 July 2021 / Published: 28 August 2021

Abstract – The Internet of Things (IoT) and Blockchain distribution ledger technology as a concept is enchanting facilities and industrial developments with advanced implements in many applications. The IoT and Blockchain market is further expected to develop three times from current development by 2025. Though many IoT applications have major challenges in safest data transaction and scalability issues while increasing the number of IoT devices. Practical Byzantine Fault Tolerance (PBFT) is a widely used form of decentralized consent, however the network node's confidence in PBFT cannot be guaranteed, as well as the mechanism of reaching consensus will consume a large amount of network services. The article suggests the novel consensus process, which is referred to a Hybrid consensus blockchain algorithm and control authentication on Trust. The Internet of Things applications are integrated with a blockchain-based decentralized system that authenticates the IoT devices through distributed control authentication. This hybrid consensus blockchain method provides security for transactions and access to unauthorized devices is restricted. The PBFT algorithm using a decentralized network system using blockchain has no restriction of IoT devices. Even malicious users create the grouping into the network that has been controlled by the distributed control authentication method. Further then malicious users are rejected from the decentralized network. In this paper, we propose the Hybrid consensus blockchain and PBFT algorithm ensure the safest data transaction through blockchain technology and improves the performance of the decentralized network. Finally, we have presented a Hybrid Consensus algorithm to be utilized in the PBFT method which enables the safest data transaction.

Index Terms – Byzantine Attack, Internet of Things, Blockchain, Consensus, Decentralized Control System.

1. INTRODUCTION

IoT-based systems are made up of a variety of diverse wireless systems, like RFID systems, sensors, controllers, and so on. Computing and networking systems are smoothly integrated in these platforms [1]. In different areas, blockchain technology is gaining more and more interest from researchers. Since the functionality of various kinds of cryptographic techniques are largely dependent on the consensus mechanisms they implement, a comprehensive understanding of established consensus mechanisms is required. These implementations must be put through their paces, evaluated, and correlated. Numerous efforts to accomplish this goal have indeed been made, as specified in the relevant segments [2-4].

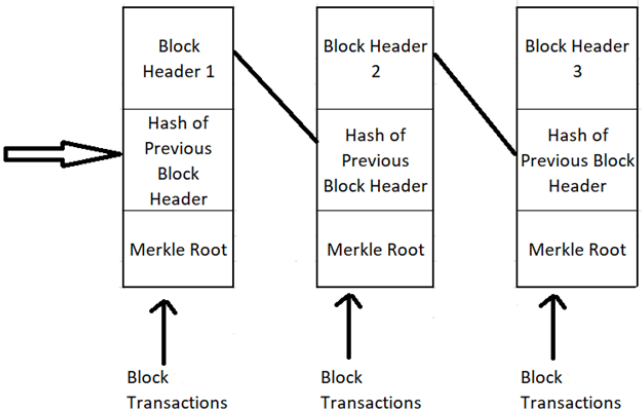


Figure 1 A Simplified Architecture of a Class of Blockchain-Based System

The accompanying main frameworks for achieving consensus are Proof-of-Work (PoW) and Proof-of-Memory (PoM) that are used in existing algorithms but for data transaction in between the nodes, routing protocol plays an important role that further have effect on system throughput, bandwidth utilization, energy consumption, overhead latency. A simplified architecture of blockchain based systems is

RESEARCH ARTICLE

presented in Figure 1. Motivation for the research is because of network optimization and security issues in IoT that are booming as a result of the significant volume of traffic that will be generated in the coming decades by IoT nodes, which are expected to number in the billions. As a result, the IoT infrastructure must be designed to minimize the impact of this massive data on other systems that use wireless and other forms of networks. Also, the lack of security would be an impediment to further IoT growth if system issues are not resolved. This goal influenced to do this research, which takes into account a range of indicators and state-of-the-art systems in order supply readers with a storage optimization and enhancing security of IoT applications. This allows researchers to look further into the problem in the near future.

The PoW approach was first used to protect towards phishing emails and DoS attacks [5]. As a result, the resource that must be spent in PoW technique is power. A community of PoW strategies tend to be a popular paradigm for defending blockchains today. The main drawback of PoW is the lots of power consumption required by each node in the system when this spending is taken into account.

It's worth noting that the PoW architecture doesn't account for a transaction between the amount of energy required and some other element [6]. As a result, developing a framework for blockchain consent that provides seems to be a critical challenge. A further standard regulation provides is PoM. It is focused on proof that certain capacity has been reserved for involvement in the consensus mechanism, i.e. "memory" is the tool that will be used. This article suggests a Prototype Consensus Blockchain architecture based on the Practical Byzantine Fault tolerant (PBFT) and distributed computing authentication to strengthen the framework.

1.1. Problem Statement

The Traditional public blockchain is a decentralized method which needs to address unstable and complicated network. As the system becomes distributed and decentralized, and routing has become a big issue in such systems when the topology changes. The provision of privacy in these systems is seen as the primary concern. The existing consistency consensus blockchain algorithm addressed poor trust authentication schemes in between the nodes. The conventional consortium blockchain the new users authenticated by enterprises system or asset verification system. It is not enough to verify the transaction with a package of blocks [7]. Also, there can be attacks from malicious nodes in between that will affect the network's efficiency. So, to enhance the security of the decentralized network, routing protocol must be considered to have a track on the malicious activity.

The remainder of the paper is organized as in Section 2, Problem Statement is defined and System Concept is defined in Section 3. In Section 4 covers proposed methodology followed by simulation analysis and discussions in Section 5 and the comparisons of proposed algorithm with Existing Algorithms are presented in Section 6 followed by conclusion.

2. SYSTEM CONCEPT

The internet of things architecture refers to different wireless device data connectivity and is addressed with vulnerability. The concept of device connectivity with the conventional method provides the fastest data connection, data communication, and data processing, and data vulnerability. The wireless sensor devices have collaborated with IoT applications which have to perform in different conditions without data vulnerability. The term data vulnerability refers to attack interception and extending the mis-behaviors throughout the networks beyond traditional security mechanisms. The malicious interception causes the worst data vulnerability. The IoT application devices should act without any interception since it has a high potential role in the industrial and smart management system. The proposed hybrid consensus blockchain algorithm exhibits highly secure IoT applications. The properties of the Hybrid Consensus Blockchain algorithm are mentioned in [8]. The architecture diagram for Secured Cluster Routing Protocol is depicted in Figure 2.

2.1. Analysis of Algorithm

The Hybrid Fuzzy Possibility C Means Clustering (HFPCM) algorithm minimizes the usage of energy along with latency of packet transmission. The Hybrid Fuzzy Possibility C Means clustering concept provides enhanced connectivity between clustering IoT nodes. The enhanced vector machine updates the location of the mobile nodes. The IoT intermediate node improved the network lifetime and maintains the load balance. To increase the network throughput the analysis of interference and improved rate of packet reliability is a must. The secure data transmission improved the network throughput.

We considered the typical IoT network which consists of several IoT devices. The proposed IoT architecture maintains two tiers namely IoT devices and overlay networks. The IoT network devices are ready to provide the data. The IoT devices are integrated with a secure and private blockchain. The private blockchain is a decentralized setup. The decentralized blockchain is controlled through Secured Cluster Routing Protocol. The network data transactions are related to particular IoT network devices and chained with each other with the help of decentralized blockchain. The Hybrid Fuzzy Possibility C Means Clustering is responsible for the new IoT device integration and creating the ledger. The HFPCM can able to delete the existing IoT devices and delete the transaction from its ledger. The Secured Cluster Routing Protocol decentralized blockchain concept controls

RESEARCH ARTICLE

the transactions. The cluster head maintains the controlling policy and maintained the updated details about the IoT node transaction. The data transactions are grouped and linked with units of blocks [13-15]. The network data transaction details are immutable and secured by the IoT network blockchain-based architecture. Blockchain-based IoT architecture is commonly used in most IoT applications. Blockchain is consists of validation-based blocks and linked together as a distributed ledger. Any node in the IoT network can choose validation and block add-up details by resource maintaining concept. The distributed ledger will broadcast if the new transaction is accounted for in any block of the IoT network [16]. The Validation process verifying the transaction and identifies the signatures contained with every data transaction [17]. The process of validation and storing causes the system delay. But the decentralized control ensures the quickest validation and storing capability in the IoT network. The decentralized concept decreases the delay and solves the problem of centralizing server failure. The inherent anonymity ensures the identity of the users and keeps the details are private. After the identification process blockchain technology secures the IoT network over untrusted users which is a desirable IoT network.

2.2. Secured Cluster Routing Protocol with Optimized link for Clusters

The aim of this is to keep the attacker nodes off the network and develop the protocol for routing. To achieve this, Secured Cluster Routing Protocol is implemented. This illustrates how the protocol is used to define the intruder and classify them. In addition, the algorithm C Means Clustering (HFPCM) of the Hybrid Fuzzy Possibility is used to optimize the different clusters of the IoT network. It also explains the cooperative strategy focused on the Byzantine agreement to make the group more immune to attacks. The output of the HFPCM is evaluated by the simulation. The findings are compared to the other protocols that exist. The proposed methodology is shown in Figure 2.

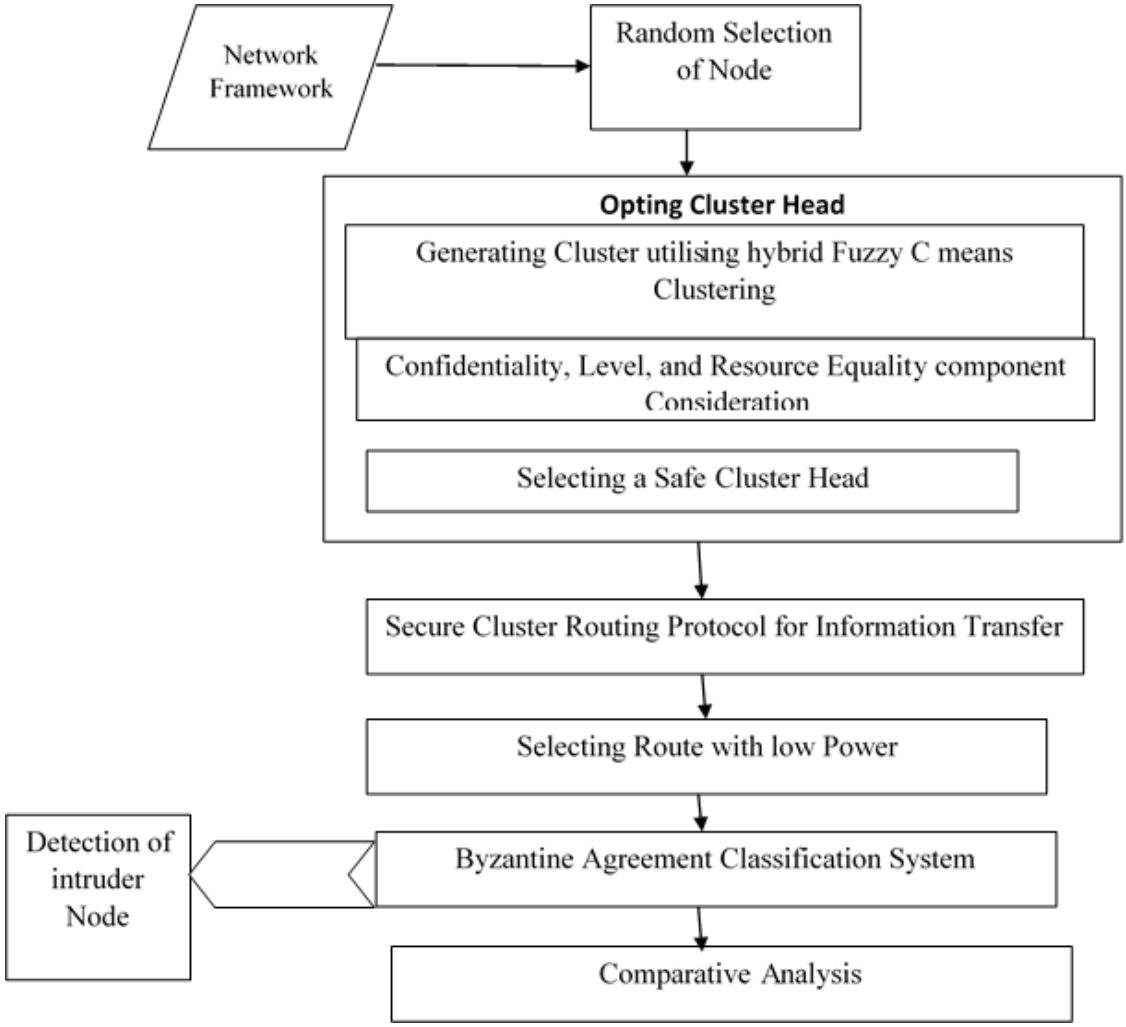


Figure 2 Architecture Diagram for Secured Cluster Routing Protocol

RESEARCH ARTICLE

3. PROPOSED METHODOLOGY

The proposed Secured Cluster Routing Protocol would use clustering to create network clusters. Secured Cluster Routing Protocol also considers the safety problems of building trustworthy cluster heads and the primary energy level for each node for better cluster head selection (CH). The Cluster Head Selection Network Model Chosen Nodes Randomly Clusters Training using Changed fuzzy possibility C Means Clusterness Degree, Energy Fairness and Protection Component Protected Clusters Head Selection Data Transmission Using the Low Energy Byzantine Detection System Malicious Node Comparison Detected Output C. The Secured Cluster Routing Protocol proposed uses the mechanism known as true CH choices for the selection of CH that distinguishes malicious nodes from genuine nodes. Each node in the network selects the closest node like the CH. It ensures that there is no defect in the election and selection process of CH.

3.1. Clustering with Hybrid FPCM

The mobile nodes are divided into separate clusters during the clustering process. The whole group is controlled with the aid of CH in each cluster. The other nodes in the group shall be referred to as cluster nodes. The cluster nodes are not transferred without delay as long as the cell nodes. CH will be responsible for the statistics collected. The CH shall then incorporate and forward data gathered from the cluster nodes through the gateway. This leads to lower power consumption and a wide range of messages sent to the portal. This reduces the conversation of a wide collection of active nodes to a minimum. Hybrid Fuzzy Possibility C Means Clustering (HFPCM) is a method of clustering based on the energy of the node to improve network life. Each CH collects the total amount of data collected from the cluster nodes and transmitted to the gateway. In the following sections, the algorithm for the method proposed is indicated.

3.2. Algorithm 1: Algorithm of Hybrid Fuzzy C Means Clustering

In any clustering process, the main component for acquiring a more efficient and better cluster is to select the properties of the respective objective. Therefore, clustering optimization depends on the chosen target characteristics. Some specifications are laid down as follows to achieve the convenient objective function as shown in Algorithm 1.

• There should be a compact space between the clusters with their data points.

• There should be a more succinct gap between the clusters

• Objective function determines the quality between data and clusters that is optimal. In addition, the Wen-Liang Hung provides an approach based in particular on the FCM's prototyped learning of the α parameter, namely Hybrid suppresses Fuzzy C-means. The α parameter relies on the strength of an exhibition distinction within the clusters and is revised in each iteration.

The α is given as shown in Equation 1:

$$\alpha = \exp\left(-\min_{i\neq k}\frac{\|v_i - v_k\|^2}{\beta}\right) \quad (1)$$

In which β is represented as a normalized term with the goal of that β is taken

As a sample variance.

Specifically, β is indicated as shown in Equation 2:

$$\beta = \frac{\sum_{j=1}^{n}\|x_j - \bar{x}\|^2}{n} \quad (2)$$

Where, $$\bar{x} = \frac{\sum_{j=n}^{n} x_j}{n}$$

In addition, another significant aspect to be revealed is the usual costs of this parameter and any iteration statistics that may lead to error. This will cause the parameter of weight for the identification of normal value to be considered. In cooperation with every cluster, each element of the data set includes one weight. The use of weight, therefore, allows for preferable classification. This determines the weight and is shown in Equation 3,

$$w_{ij} = \exp\left(-\frac{\|x_j - v_i\|^2}{\left(\sum_{j=1}^{n}\|x_j - \bar{v}\|\right)\frac{c}{n}}\right) \quad (3)$$

To adjust the fluid and ordinary disconnection, the achieved weight is used. Each scheme that is previously described is usually repeatable because no change in the characteristics of the goal is calculated as long. CH should be placed adjacent to the facts to arrange the information point. There are two assertions in the objective function.

i. Use of the fuse weighting model, Fuzzy function,

ii. Priority selection of the route

The two coefficients are used to display typicality and membership without the objective function. As an exhibitor of space in two objective functions, this association offers weighting exposits.

Step1: Initiate node state

Step2: Cluster formation using HFPCM

Step3: Procedure call Secure CH selection ()

RESEARCH ARTICLE

Step4: = {$n1$, $n2$. . .,nn} // node's Neighbour Lists Vi = {$V1$, $V2$. . . , Vn }

Step5: If (Size of Neighbor List > Peak Cluster Volume)

Step6: Prune Neighbor List to Peak Cluster Volume

Step7: Then arrange Neighbor List based on Vi;

Step8: For every node "i" in Neighbor List:

Step 9: If (Neighbor / Di < = 2/3)

Step10: then

Neighbor node is node of mistrust

Compute Vi with ct < 0 by using

$$\text{Vi} = aX\frac{Di}{Dmax} + \frac{bX\text{Fi}}{\text{Fmax}} + ct\ X\ Neighbor + Di - \frac{2}{3} + d\ XE \ldots$$

Step11: Categorize each node as either normal or malicious node by using probability model

Step12: Else if

$Nneighbor\ Di$ > 2

Step13: then Node is a normal node

Step14: Do step 10 once more

Step15: Else if

Di > Platform Size

Step16: Then Entity is an intruder node

Step17: excluding the component from the decision-making process

Step18: Cluster Head = neighbor node with peak value V

Algorithm 2 Protected Group Header Choosing Algorithm

In our proposed system all cluster head keeps the transaction in the blockchain as shown in Algorithm 2. Every transaction involved two blocks and the sender and receiver accepts the transaction. Even other IoT devices have involved the transaction and those are controlled by the cluster head for every transaction.

The proposed Hybrid Fuzzy Clustering method is utilized for fault tolerance and controls unauthorized users when the authentication process completes the selection process. The expressions shown in Equation 4 are applied.

$$H_{FC}(\%) = \frac{\text{Degree of target positions (PRT x PCP x P KN)/ Nodes}}{\sum i=1 =(\text{PRT x PCP x P KN)/ Nodes}} X\ 100 \qquad (4)$$

P_{RT} is related to a requested transaction with an external department and indicates various levels. P_{CP} denotes comparing job positions with known neighbours. The target positions were noted from multiple nodes and divided from the overall P_{RT}, $P_{CP,}$ and P_{KN} values from the destination value. The above equation clearly shows that the network probability of collusion is too high while the number of IoT devices is small. The random selection process is applied to this equation the probability of collusion got decreased.

The proposed Blockchain-based HCHF method is providing the security features using an authentication process. The authentication controller maintains the user registration across the network and keeps the system without malicious activities. The external user registration is involved by the authenticator. The distributed control authentication process controls the open network user registration through an authentication system. The blockchain-based decentralized system accepts the IoT devices which have completed the authentication process. The successful completion of the authentication process connects the IoT devices with the blockchain-based decentralized system through this IoT devices are communicated. It is impossible to get transaction access from a malicious user. The cost-effective Secured Cluster Routing Protocol controls the threat activities and improves the secure data transaction [9] [10]. Already existing techniques utilizes the Proof-of-Work algorithm. The miner is the block creator and broadcasts their blocks to the network. In PoW algorithm is expensive block creation and involved in data transaction costing for every operation which makes it costlier in PoW implementation and provides security against traditional network attacks. It is not an easy distribution system to implement throughout the network and spread out the data transactions. Though the node sustainability is not required too high. Since the lifetime of the node is not needed to do the extensive data transaction.

We have implemented the Blockchain-based decentralized Hybrid Cryptographic Hash Function (HCHF) method in the Internet of Things. The malicious activity involves the transmission routing details and captures the packet transmission. This process slowly increases the packet loss rate. The improved system identifies suspicious behaviour and controls malicious traffic. The blocking malicious module controls the packet loss rate. As shown in Table 1, the simulation parameters are below.

Simulation Parameter	Value
Network Simulator	Ns3.27
Number of Nodes	10 - 100
Node Range	150 m

RESEARCH ARTICLE

Propagation Delay Mode	120 Km / h to 140 Km / h
Transmission Range	1100 m – 1300 m
Packet Carry Duration	0.5 Second
Packet Size	512 Bytes

Table 1 Simulation Parameters

The acceptance of a new device participation structure is a major advantage for the IoT applications portfolio. Since the utilization of the application, the range has been increased due to no limit on the user registration also the performance of the system is maintained through blockchain-based IoT architecture and it is determined the data transaction flow which helps to maintain the throughput of the entire network.

The available transaction details and the verified block contents are allowed for the further transaction process. The transaction history maintained the hash function, the previous details can be verified and the current blocks are available to add up the details to the blocks. The HCHF follows the set of rules to satisfy the security aspects and data transactions. The unlimited user registration creates high throughput performance.

4. SIMULATION ANALYSIS AND DISCUSSIONS

For analysis, Throughput, Bandwidth, Overhead Latency, and Scalability of the proposed system are taken into consideration. Simulating Parameters Involved and the Dependent Parameters is shown in Table 2.

Parameters Involved	**Dependency on another Parameter**
Throughput	Data Packet Loss
Bandwidth	Data Packet Delivery Ratio
Overhead Latency	Mean Time Delay Propagation Delay
Scalability	Network Lifetime Bandwidth Throughput

Table 2 Simulating Parameters Involved and the Dependent Parameters

Throughput of the proposed system is calculated in percentage and is defined as the ratio of data packets received at the receiver node to the data packets transmitted from transmitter node. Throughput is measured in bps(bits/sec) and can be calculated as shown in Equation 5.

$$\text{Throughput (\%)} = \frac{DPR}{DPT} * 100\ \% \quad (5)$$

Where, DPR is data packet received and DPT is data packet transmitted [18]. The throughput of the proposed system while considering nodes set from 10 to 100 is taken into account. In addition, bandwidth level ensures high data security and high data privacy. The comparison analysis of traditional results with the proposed IoT setup showcases poor data security. Throughput is further dependent on Data Packet Loss that is ratio of number of data packets not received to the total number of packets sent from the transmitter node [19]. Bandwidth is the maximum data packets that can be sent through the network in a particular period of time. It must be high for a network to be efficient. As Bandwidth in turn depends on multiple factors including throughput, data packet delivery ratio. Data packet delivery ratio is the ratio of number of data packets received to the number of data packets sent.

In Overhead Latency, the amount of time a node spends transmitting or receiving a data is referred to as overhead and Latency is the time it takes for a data with a minimal number of packets to travel from its source node to its destination node. Network Latency can be calculated as the addition of propagation delay in the network and serialization delay [20-22].

Network Latency = Propagation delay + Serialization delay

$$\text{Where, propagation delay} = \frac{\text{distance in between the nodes}}{\text{Speed of the network}}$$

$$\text{And, serialization delay} = \frac{\text{Size of data packet}}{Transmission\ Rate\ (bps)}$$

Overhead Latency is dependent on the mean time delay and is calculated as the subtraction of start time from end time. The potential of a network to manage rapid variations in load caused by unexpected rises or reductions in the volume of information it handles is referred to as network scalability. Scalability metric include throughput, bandwidth, and memory. Also, scalability is dependent on network lifetime that represents the ratio of length of energy usage to the overall energy.

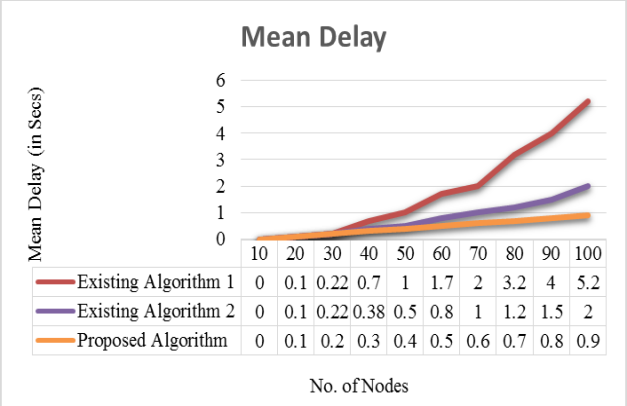
5. COMPARISON OF PROPOSED SYSTEM WITH EXISTING ALGORITHMS

The comparison of the proposed system with existing algorithms is shown in Figure 3-7 for five different parameters. The proposed algorithm is compared with existing algorithm 1[11] and existing algorithm 2 [12].

Figure 3 depicts the mean delay. The Proposed algorithm experimental output showed less delay as compared to the existing algorithms.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209695 Volume 8, Issue 4, July – August (2021)

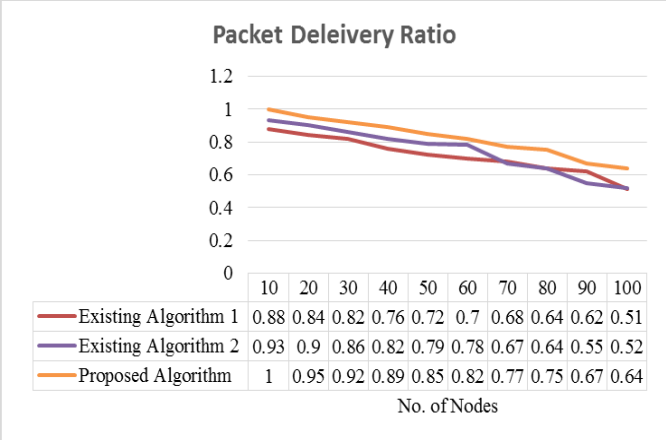
RESEARCH ARTICLE



	10	20	30	40	50	60	70	80	90	100
Existing Algorithm 1	0	0.1	0.22	0.7	1	1.7	2	3.2	4	5.2
Existing Algorithm 2	0	0.1	0.22	0.38	0.5	0.8	1	1.2	1.5	2
Proposed Algorithm	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9

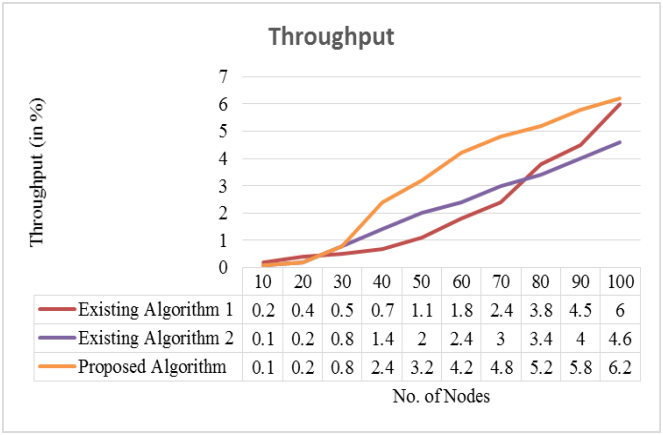
Figure 3 Comparison of Existing Algorithm with Proposed Algorithm for Mean Time Delay

Figure 4 showed the packet delivery ratio. Proposed algorithm improved the transmission rate dramatically as it prioritizes package rebroadcasting and lowers packet delay for each interaction; finally, the data transmission rate is raised.



	10	20	30	40	50	60	70	80	90	100
Existing Algorithm 1	0.88	0.84	0.82	0.76	0.72	0.7	0.68	0.64	0.62	0.51
Existing Algorithm 2	0.93	0.9	0.86	0.82	0.79	0.78	0.67	0.64	0.55	0.52
Proposed Algorithm	1	0.95	0.92	0.89	0.85	0.82	0.77	0.75	0.67	0.64

Figure 4 Comparison of Existing Algorithm with Proposed Algorithm for Data Packet Delivery Ratio

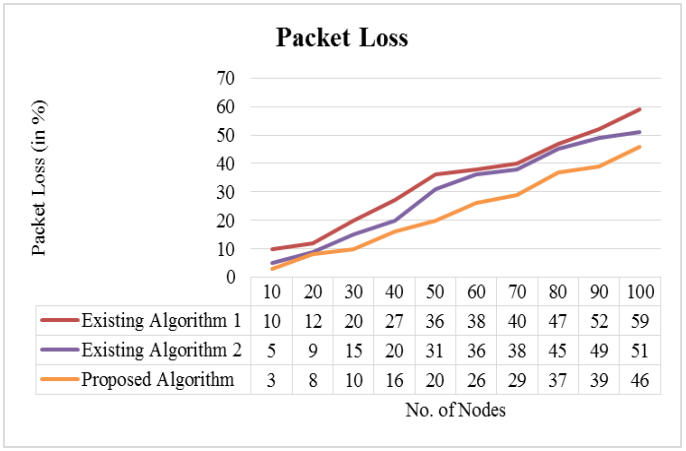


	10	20	30	40	50	60	70	80	90	100
Existing Algorithm 1	0.2	0.4	0.5	0.7	1.1	1.8	2.4	3.8	4.5	6
Existing Algorithm 2	0.1	0.2	0.8	1.4	2	2.4	3	3.4	4	4.6
Proposed Algorithm	0.1	0.2	0.8	2.4	3.2	4.2	4.8	5.2	5.8	6.2

Figure 5 Comparison of Existing Algorithm with Proposed Algorithm for Throughput

Proposed Algorithm rejects if some packet obstruction occurred for each transaction because throughput enhances the total efficiency of data transmission. Figure 5 showed improved throughput for proposed algorithm as compared to existing algorithms.

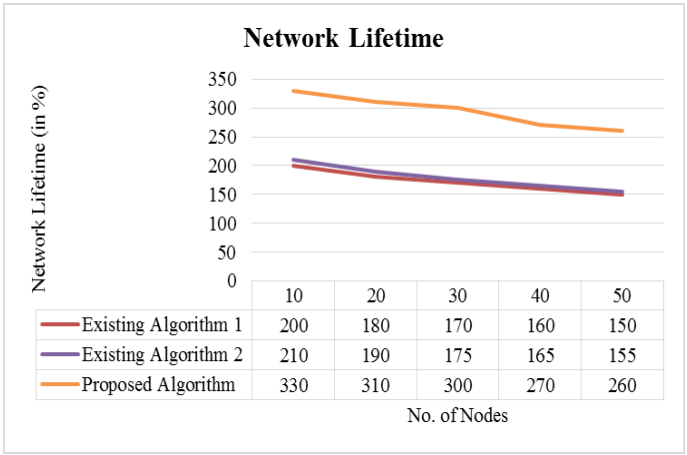
Packet loss is depicted in figure 6. As the speed of the network increases, the number of packets lost increases as well. The proposed algorithm includes a technique of protection. When compared to prior approaches, the quality of packets discarded is lower.



	10	20	30	40	50	60	70	80	90	100
Existing Algorithm 1	10	12	20	27	36	38	40	47	52	59
Existing Algorithm 2	5	9	15	20	31	36	38	45	49	51
Proposed Algorithm	3	8	10	16	20	26	29	37	39	46

Figure 6 Comparison of Existing Algorithm with Proposed Algorithm for Data Packet Loss

Network Lifetime is depicted in Figure 6. This approach makes it straightforward to identify intrusion before packet exchange begins. In comparison to earlier strategies, the proposed strategy reduces the lifetime of the network.



	10	20	30	40	50
Existing Algorithm 1	200	180	170	160	150
Existing Algorithm 2	210	190	175	165	155
Proposed Algorithm	330	310	300	270	260

Figure 7: Comparison of Existing Algorithm with Proposed Algorithm for Network Lifetime

The comparisons of proposed algorithm with existing algorithms are presented in Table 3.

RESEARCH ARTICLE

Parameters	Existing Algorithm 1	Existing Algorithm 2	Proposed Algorithm
Technique Applied	Proof of Work Algorithm	Proof of Work Algorithm	HFPCM-Hybrid Fuzzy Possibility
Throughput	Low	Average	High
Fault Tolerance	PBFT	Traditional Network	Hybrid Cryptographic Hash Algorithm
Security Improvement	Low Security	Normal Security	High Security
Overhead Latency	Low Priority & High Latency	Average Priority & Medium Latency	High Priority & Low Latency
Scalability	Low Adaptability	Medium Adaptability	High Adaptability
Packet Delivery Ratio	Low	Medium	High
Packet Loss	High	Medium	Low
Mean Time Delay	High	Medium	Low

Table 3 Comparison with Existing Algorithms

The comparison analysis of overhead latency and scalability with concurrent clients indicated improved performance. The traditional management setup doesn't control the latency and scalability. Overall performance shows improved throughput and confirms IoT environment secure data transmission without a response delay. The distributed selection without reducing the performance that the proposed method achieves the high throughput.

6. CONCLUSION

Internet of Things data security and privacy are high impact factors for reaching the high expectations of the current technology to transform many reasons of our industrial developments and economy. To achieve cluster-based routing, establish multipath selection, inhibit, identify, mitigate, and prevent the system from compromised users, and also provide a stable route for successful collaboration, the Efficient Secured Cluster Routing Protocol and Hybrid Fuzzy possibility C-means Clustering (HFPCM) method are used. The proposed method helped to diagnose fraudulent nodes and invalidate their certificates in a short amount of time and with little resources. If there are any hacked nodes in the system the protocol aids in their quick revocation. Clusters are constructed to speed up the revocation procedure. This reduces network traffic while also improving performance in terms of accuracy. In this, the Cluster Routing Protocol helped to eliminate the influence of compromised nodes by appointing an unreachable and energy-saving node to operate as cluster head. It actively categorizes the attacker nodes and prevents them from reporting an erroneous cluster head choice. Cluster routing system employs the Byzantine agreement technique to alleviate the selfishness that rendered the system immune to attacks. It has numerous advantages, such as lower energy consumption and shorter transmission times. It boosts the network's lifetime and promotes route stability. To resolve the problem of data transmission, Fuzzy logic is implemented to improve efficient data transmission. The experimental output indicates the better packet delivery ratio, network life, output, and packet loss reduction, meantime delay. Blockchain consequences are used to rectify the delay in packet transmission also clustering is used here to improve the packet loss and transmission time. The algorithm shows improved throughput efficiency and minimal loss of data packets during transmission.

REFERENCES

[1] M. Abu-elkheir, M. Hayajneh, and N. A. Ali, "Data Management for the Internet of Things: Design Primitives and Solution," pp. 15582–15612, 2013, doi: 10.3390/s131115582.

[2] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: a survey," *arXiv*, no. January, 2020.

[3] M. J. Mihaljević, "A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off," *IEEE Access*, vol. 8, pp. 141258–141268, 2020, doi: 10.1109/ACCESS.2020.3013199.

[4] J. Skrzypczak, F. Schintke, and T. Schutt, "RMWPaxos: Fault-Tolerant In-Place Consensus Sequences," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 10, pp. 2392–2405, 2020, doi: 10.1109/TPDS.2020.2981891.

[5] M. Du, Q. Chen, and X. Ma, "MBFT: A New Consensus Algorithm for Consortium Blockchain," *IEEE Access*, vol. 8, pp. 87665–87675, 2020, doi: 10.1109/ACCESS.2020.2993759.

[6] G. Yu, B. Wu, and X. Niu, "Improved Blockchain Consensus Mechanism Based on PBFT Algorithm," *Proc. - 2020 2nd Int. Conf. Adv. Comput. Technol. Inf. Sci. Commun. CTISC 2020*, pp. 14–21, 2020, doi: 10.1109/CTISC49998.2020.00009.

[7] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The Energy Consumption of Blockchain Technology: Beyond Myth," *Bus. Inf. Syst. Eng.*, vol. 62, no. 6, pp. 599–608, 2020, doi: 10.1007/s12599-020-00656-x.

[8] T. M. Silva Filho, B. A. Pimentel, R. M. C. R. Souza, and A. L. I. Oliveira, "Hybrid methods for fuzzy clustering based on fuzzy c-means and improved particle swarm optimization," *Expert Syst. Appl.*, vol. 42, no. 17–18, pp. 6315–6328, 2015, doi: 10.1016/j.eswa.2015.04.032.

[9] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," *arXiv*, 2019, doi: 10.6028/NIST.IR.8202.

[10] H. M. Xin and K. Yang, "Routing protocols analysis for internet of things," *Proc. - 2015 2nd Int. Conf. Inf. Sci. Control Eng. ICISCE 2015*, no. i, pp. 447–450, 2015, doi: 10.1109/ICISCE.2015.104.

[11] R. Yasaweerasinghelage, M. Staples, and I. Weber, "Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation," *Proc. - 2017 IEEE Int. Conf. Softw. Archit. ICSA 2017*, no.

RESEARCH ARTICLE

October, pp. 253–256, 2017, doi: 10.1109/ICSA.2017.22.
[12] He, Li, and Zhixin Hou. "An improvement of consensus fault tolerant algorithm applied to alliance chain." 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC). IEEE, 2019.
[13] F. Dang *et al*., "Understanding fileless attacks on linux-based IoT devices with HoneyCloud," *MobiSys 2019 - Proc. 17th Annu. Int. Conf. Mob. Syst. Appl. Serv.*, pp. 482–493, 2019, doi: 10.1145/3307334.3326083.
[14] Y. Ren *et al*., "Data query mechanism based on hash computing power of blockchain in internet of things," *Sensors (Switzerland)*, vol. 20, no. 1, 2020, doi: 10.3390/s20010207.
[15] P. Gotovtsev, "How IoT can integrate biotechnological approaches for city applications-review of recent advancements, issues, and perspectives," *Appl. Sci.*, vol. 10, no. 11, pp. 1–20, 2020, doi: 10.3390/app10113990.
[16] D. V. Jose and A. Vijyalakshmi, "An overview of security in internet of things," *Procedia Comput. Sci.*, vol. 143, pp. 744–748, 2018, doi: 10.1016/j.procs.2018.10.439.
[17] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving internet of things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, pp. 1–14, 2020, doi: 10.3390/computers9010008.
[18] J. Choi, Y. In, C. Park, S. Seok, H. Seo, and H. Kim, "Secure IoT framework and 2D architecture for End-To-End security," *J. Supercomput.*, vol. 74, no. 8, pp. 3521–3535, 2018, doi: 10.1007/s11227-016-1684-0.
[19] O. Flauzac, C. Gonzalez, and F. Nolot, "New security architecture for IoT network," *Procedia Comput. Sci.*, vol. 52, no. 1, pp. 1028–1033, 2015, doi: 10.1016/j.procs.2015.05.099.
[20] B. Ndibanje, H. J. Lee, and S. G. Lee, "Security analysis and improvements of authentication and access control in the internet of things," *Sensors (Switzerland)*, vol. 14, no. 8, pp. 14786–14805, 2014, doi: 10.3390/s140814786.
[21] A. Kaushik and D. Thomas, "Blockchain – Literature Survey," pp. 2145–2148, 2017.
[22] J. Sun, J. Yan, and K. Z. K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financ. Innov.*, vol. 2, no. 1, 2016, doi: 10.1186/s40854-016-0040-y.

Authors

Monika Parmar is a Ph.D. candidate in the Department of Electronics and Communication Engineering at Chitkara University, Punjab. She has been a researcher in IoT and Blockchain since 2017. She is Currently working as an Assistant Professor in Chitkara University, Himachal Pradesh.

Dr. HarsimranJit Kaur is an associate professor at the department of Electronics and Communication Engineering at the Chitkara University, Punjab. She received her Ph.D. from Chitkara University in the year 2016. Her research interest is in Nano-phononics and Integrated Optics, Wireless Communications.

How to cite this article:

Monika Parmar, Harsimran Jit Kaur "Blockchain-Enabled Consensus Routing Protocol Improving the Security Data Communication in Internet of Things Applications", International Journal of Computer Networks and Applications (IJCNA), 8(4), PP: 268-276, 2021, DOI: 10.22247/ijcna/2021/209695.