Blockchain-based 5G handoff authentication system using joint-graph-based delegated practical byzantine fault tolerance consensus approach

Ravindra Janardan Lawande [a,1,*], Sudhir Bapurao Lande [b,2], Shailendrakumar Mahadeo Mukane [c,d,3]

[a] Department of Electronics and Telecommunication Engineering, Savitribai Phule Pune University, Maharashtra, India
[b] Department of Electronics and Telecommunication Engineering, Vidya Pratisthan's Kamalnayan Bajaj Institute of Engineering and Technology, Baramati, Maharashtra, India
[c] SVPM's College of Engineering, Malegaon (Bk), Baramati, Savitribai Phule Pune University, Pune, Maharashtra, India
[1] rjlawande25@gmail.com; [2] sudhir.lande@vpkbiet.org; [3] principal@engg.svpm.org.in
* corresponding author

ARTICLE INFO

Article history
Received October 8, 2025
Revised February 23, 2026
Accepted March 1, 2026
Available online May 31, 2026

Keywords
Blockchain
Authentication handover
Encryption
Joint graph
Frequency hopping

ABSTRACT

The 5G mobile networks offer extra benefits in terms of high data rates, lower latency, and more coverage in comparison to 4 G networks. However, the 5G network offers new levels of data transfer and processing speeds, ensuring users do not disconnect as they move from one cell to another. By considering these issues, this paper proposes a new blockchain-based, scalable, and reliable 5G handoff authentication system. The proposed approach is intended to ensure authentication using Exponential Elliptic Curve-Assisted Encryption (EEE) between the user and the base station. After the successful authentication, the user stores the details in the source base station. In a blockchain-based 5G handoff authentication system, when a user device enters the range of a new base station, it sends a handoff request using a pseudorandom frequency-hopping sequence. The serving base station sends a handover command to the mobile device, containing details about the target base station and the next frequency in the hopping sequence. This request is disseminated through an Improved gossip algorithm that minimizes communication overhead and accelerates node authentication in the blockchain for consensus and validation. Similarly, in blockchain networks, the gossip protocol ensures that every node in the network receives information about the request for handoff while ensuring that the messages sent are not redundant. Therefore, the joint graph-based Delegated Practical Byzantine Fault Tolerance (JG-DPBFT) consensus process is utilized to verify the handoff.

1. Introduction

In today's world, fifth-generation (5G) networks are available, allowing users to communicate seamlessly. Furthermore, faster communication improves the usage of resources [1]. The networks enable increased scalability, dependability, data rates, low latencies, and capacities for applications such as vehicular and device-to-device (D2D) communication [2], [3]. In addition to 5G and beyond 5G networks' efficacy, the communication platform faces other challenges. The problems are reportedly user privacy, resource management, as well as handover authentications [4]. Authentication during handover is an important difficulty in providing secure communication and data transmission [5].

Various algorithms are introduced to reduce and monitor the threads during the handover of signals to other base stations (BS) [6]. Even though a reliable approach has not yet been identified as a prominent strategy, early deep learning (DL), as well as machine learning (ML) models, have been developed to recognize the threatened network with the help of features and labels [7], [8]. The collection of features may be relevant or irrelevant in certain situations, which leads to lots of complications. In the motive of identifying the attacks, the recurrent neural network (RNN) is used as a detection model for identifying attacks with high possibility [9]. The model exhibits vanishing gradients, leading to incorrect detection in some scenarios. Hence, cryptographic algorithms are used to safeguard data during handoffs between station [10].

The algorithms minimize the risk as compared to deep learning technologies in the handoff scenario [11], [12]. Even though the threats to data remain, the attack surface in 5G networks has increased. In order to increase security, the blockchain is integrated with handoff signals [13], [14]. Blockchain is said to be a decentralized server that provides high security in storing data and request authentication [15]. Several models used fuzzy-based systems for authentication, which provide high latency in the handoff [16], [17]. To achieve competent key arrangement as well as rapid succeeding authentication, a consensus mechanism has been introduced that provides blockchain-enabled handover confirmation facilitated in 5G heterogeneous networks [18]. The approach provides latency and scalability challenges. Hence, the model that enhances both scalability and security is still in use [19], [20].

Ultra-dense heterogeneous networks (UDHN) have emerged as the main answer to numerous network issues as an result of the development of 5G technology. The UDHN's dynamic, transient, and autonomous access points (APs) and user equipment (UE) contribute to its complexity. Malicious assaults pose a threat to security in 5G networks, while frequent handovers may compromise reliability. It is especially critical for 5G networks, which must provide a dependable and safe connection while serving a broad range of applications. Blockchain technology enables end-to-end service transfer across the 5G network, including authentication. Therefore, blockchain must be integrated with 5G networks to improve security. Traditional handoff authentication mechanisms in cellular networks often rely on centralized authorities, which can introduce latency, bottlenecks, and vulnerability to single points of failure.

Blockchain technology, having a decentralized nature and robust security features, presents a promising solution for 5G handoff authentication. However, integrating blockchain into 5G networks is not without challenges, particularly due to its high computational cost and delay in consensus mechanisms. However, standard blockchain consensus algorithms, such as Proof of Work (POW), are not suitable for real-time 5G applications due to their high latency and computational inefficiency. To address this problem, this study suggests a Blockchain-based 5G Handoff Authentication System utilizing a JG-DPBFT consensus approach. The goal is to provide a lightweight, decentralized authentication mechanism that ensures secure, low-latency handoff between 5G base stations while maintaining the scalability and efficiency needed for a high-density network. This system aims to minimize delays, reduce computational overhead, and enhance the overall security and performance of 5G handoff processes.

The major contributions of this research work are:

- To design a blockchain that enables a 5G handoff-authentication framework that avoids full re-authentication during inter-cell mobility, which helps to reduce handover authentication delay.
- To introduce a JG-DPBFT mechanism. where consensus is performed by dynamically selected delegated committees rather than all blockchain nodes, which helps reduce consensus delay and expand the throughput range.
- To improve the gossip algorithm, a historical node filtering is introduced, which helps to minimize redundant message propagation during handoff authentication. This approach helps to reduce communication overhead and energy consumption.

- To support fast cryptographic authentication at the radio edge, an EEE scheme is proposed that replaces traditional scalar multiplication with exponential operations.
- To validate a comprehensive NS-3-based simulation of the individual and combined impact of the proposed components, which demonstrates that the performance gains are obtained from the combined approach of all phases.

Unlike existing studies that improve only a single layer, either cryptography or mobility prediction. The proposed approach introduced a co-designed architecture where each component contributes to a distinct performance metric. The experimental results confirm that the reduction in handoff authentication delay is primarily achieved by JG-DBPT consensus and an improved gossip mechanism.

The rest of the paper is organized as follows: Section 2 presents the related work. The proposed Blockchain-based 5G Handoff Authentication is demonstrated in Section 3. Section 4 shows the simulation results and the analysis; finally, the conclusion and future scope of the work are presented in Section 5.

2. Related works

Some of the recent research work surveyed related to Blockchain-based 5G Handoff Authentication. Table 1 compares existing models.

Table 1. Existing models with disadvantages.

Author & Reference	Year	Model	Performance	Disadvantages
Krishnan et al. [21]	2024	Secure Handover Key approach	exhibits better changeover performance	This may lead to computational overhead
Mannem et al. [22]	2024	WbPOH	Attained 5.2Mbps throughput	High complexity, which leads to delays in transmission
Baz et al. [23]	2024	Deep residual LSTM	minimize handover delay as well as optimize resource allocation	lead to increased processing requirements and latency
Mohammed et al. [24]	2024	HAFC	Less communication overhead	The model had latency and security risks
Haddad et al. [25]	2024	ZKP and Blockchain	Need low computing requirements that provide less computation	The approach provides scalability challenges
Goswami et al. [26]	2024	Blockchain based fast as well as secure handover authentication framework for 5G networks.	Less computation and communication overhead.	Obtained security issues like anonymity, traceability, and unlinkability.
Surapaneni et al. [27]	2024	Vehicle authentication handover scheme with blockchain, IPFS, and cloud computing	Maintaining better throughput and latency	This leads to scalability and high computational issues
Ma et al. [28]	2024	Blockchain technology for a group of MTCD	Efficient communication and computational costs	The model had high latency and less data transmission

Krishnan et al. [21] presented a unique method of authentication that makes use of Software Defined Networks (SDNs) called Secure Handover Key. The suggested plan incorporates resilience against leaks and perfect forward secrecy with recycled lightweight dynamic key encryption. The computing, communications, signal, and energy costs for 5G mobility applications and vehicular communication

networks (VCNs) are used to evaluate the importance of the suggested approach. Compared with traditional systems, the scheme used in this study offers better handoff performance and enhanced security. Mannem et al. [22] developed a Wolf-based Power-Optimized Handoff (WbPOH) technique to control power and signal drop. Grey wolf fitness is used for continuous monitoring and for predicting the closest-approaching Handoff signal, as well as for work-free node prediction. The single strongest signal near the range was first enabled by the intended WbPOH during the Handoff process, and subsequently the previous signal was destroyed. Furthermore, 5.2 Mbps throughput is achieved for the Worldwide Interoperability for Microwave Access (WiMAX) network and 5 Mbps for the cellular network in the suggested WbPOH. Furthermore, the WiMax network efficacy is 96%, while the claimed cellular network efficacy is 95%.

Baz et al. [23] developed an innovative technique to enhance mobility organization in 5G systems by employing a deep residual long short-term memory (LSTM) model. Proactive resource allocation and handover decisions are enabled by the model's ability to forecast future user locations and mobility patterns using past mobility data. Residual influences should be included in the LSTM model to represent intricate sequential dynamics. Prediction accuracy improves as a result. The 5G network's mobility organization design also integrated the mLSTM paradigm. While, Mohammed et al. [24] presented a Handover Authentication Scheme Based on a Fog Computing (HAFC) system for handover authentication. The suggested model facilitates safe property transfer between fog servers for 5G-assisted vehicular blockchain and quickly re-authenticates vehicle networks. The suggested HAFC system comprises both phases: the initial authentication phase and the handover and authentication step. Throughout both phases, the vehicle is authenticated to fog in the HAFC scheme server using Computational Diffie-Hellman (CDH) security.

Haddad et al. [25] introduced an anonymous method to efficiently preserve privacy in the 5G network handover protocol using Zero Knowledge Proof (ZKP) and Blockchain. The suggested approach might preserve forward/backward secrecy while being resilient to individuality capture, geographic extent tracing, and replay attacks. Furthermore, the performance assessment of the suggested strategy demonstrates that it is rapid and efficient due to its low computational requirements, small message count, and the absence of Home Network (HN) involvement in the handover protocols.

The 5G networks, with their high bandwidth, low latency, and flexibility, are becoming increasingly desirable for future IoT applications. However, small cells such as picocells, femtocells, and microcells can be deployed to provide greater bandwidth. Small cells, on the other hand, had less signaling coverage, resulting in more frequent authentication handovers. Goswami et al. [26] proposed a blockchain-based, rapid, and secure handover authentication architecture for 5G networks. The suggested framework is designed to withstand security assaults such as key compromise and phony base station attacks. Informal security demonstrates that the proposed framework is resilient to many security risks, including desynchronization, eavesdropping, and denial-of-service attacks. Furthermore, the performance analysis of the recommended framework reveals fewer processing and communication overheads.

Telecommunications improvements significantly assist the Internet of Vehicles (IoV) in various ways. Reduced latency, faster data transfer, and lower pricing are transforming the IoV ecosystem. However, while technological advancements provide benefits, they also expand cyberspace, raising security and privacy concerns. Surapaneni et al. [27] developed a vehicle authentication handover technique that uses blockchain, the InterPlanetary File System (IPFS), and a hybrid computing approach. This framework's proof-of-reputation (PoR) consensus technique improves traceability and transparency, while elliptic-curve cryptography (ECC) reduces computational latency. Furthermore, the created framework assures confidentiality, data availability, and integrity while improving throughput and latency in vehicle re-authentication.

The 5G wireless network connection enables large IoT applications, including enormous machine-type communication (MTC) systems. The group of MTC devices (MTCD) repeatedly connects to a new target base station. In contrast, frequent mutual authentication operations resulted in large signaling overheads in access, which reduced overall network performance. Ma et al. [28] proposed a competent

and safe handover verification technique based on blockchain technology for a group of MTCDs. The protocol uses blockchain to decentralize authentication away from centralized servers and distribute it across all BS. However, the suggested design can eliminate single points of failure, make DDoS attacks more difficult, and improve mutual authentication and key negotiation among group MTCDs and base stations. Furthermore, the performance assessment of the suggested protocol was effective in terms of communication locations and computing costs.

Current authentication-based handover protocols of 5G networks are mostly based on centralized or semi-decentralized networks, which create scalability bottlenecks, longer authentication latency, and susceptibility to single points of failure in higher-density deployments. Blockchain-based technologies proposed in previous research tend to implement traditional consensus models, including PoW, PoS, and PBFT, which are computationally expensive, energy-intensive, and have long consensus times, and are therefore not applicable to a real-time handover process. ML, DL based mobility and handover schemes, although effective in prediction, add complexity of processing and do not provide cryptographic security guarantees. Moreover, a number of handover models based on blockchain have the drawback of redundancy in message transmissions because of inefficient gossiping protocols, low fault tolerance in Byzantine situations, and re-authentication between cells. The combination of these constraints leads to higher handover delays, decreased throughput, and an inability to scale to large-scale 5G heterogeneous networks. Unlike the current methods, the developed IGJ-DPBFT-based handover authentication system presents an essentially different combination of enhanced gossip-based message dissemination, joint-graph-directed delegated consensus, and lightweight EEE.

In contrast to traditional PBFT and PoW-based blockchain implementations, a joint-graph structure shifts consensus responsibility to dynamically generated committees and significantly reduces communication overhead, while maintaining BFT. The enhanced gossip algorithm reduces the likelihood of unnecessary message propagation in handover requests in directly addressing the latency and scalability constraints experienced in the earlier blockchain-based algorithms. Moreover, the proposed EEE mechanism replaces computationally intensive elliptic-curve-based computations with exponential transformations, producing keys and authentication much faster without loss of security. The proposed model provides a scalable, low-latency, and energy-efficient solution to ultra-dense 5G networks, with end-to-end handover validation, and allows parallel execution of consensus, a key feature that makes the proposed model a specific solution as opposed to the traditional adaptations of conventional mechanisms.

3. Method

This paper proposes a blockchain-based, scalable, and reliable 5G handoff authentication system based on IGJ-DPBFT. However, this network is suggested to increase user authentication. The suggested approach minimizes delay in handovers between different cells by preventing re-authentication, also allowing users to establish a safe and fast connection. Delay reduction is considered one of the key goals and characteristics of 5G, which can be achieved through a compact structure. The suggested consensus mechanism improves the efficiency, stability, and scalability of consensus in distributed systems, particularly blockchain networks. In addition, the consensus process is delegated to a limited group of delegate nodes, which improves network scalability and communication costs. The joint graph structure ensures that delegates are chosen in a way that maintains balanced representation and fault tolerance throughout the network.

3.1. System model

In 5G handoff authentication, the user initially stores the data in the first base station, which is the source base station. Before storing the data, the authentication process by EEE takes place between the user and the BS. After the successful authentication, the user will store the details in the source BS. In a blockchain-based 5G handoff authentication system, when a user device moves into the range of a new BS, it sends a handoff request using a pseudorandom frequency hopping sequence. This sequence should be agreed upon in advance to avoid synchronization issues and provide Reduced Interference and Faster

Handoff. The serving base station sends a handover command to the mobile device, comprising details about the target BS and the subsequent frequency in the hopping sequence. However, the request is disseminated through a gossip process among the blockchain nodes, which serve as base stations in this context. It responds to handoff requests quickly and effectively through the improved gossip algorithm, which minimizes communication overhead and accelerates node authentication in the blockchain for consensus and validation. In blockchain networks, the gossip protocol ensures that every node in the network receives information about the handoff request and that the messages sent are not redundant. Next, the given JG-DPBFT consensus process is utilized to verify the handoff. In this case, the handoff request validation is the responsibility of a set of elected delegate nodes. To reach an agreement on the authentication choice, these delegate nodes cooperate within the blockchain. Fault tolerance enabled by JG-DPBF ensures the network remains safe even in the event that some nodes are compromised. The decision is recorded on the blockchain by the delegates once they have verified the request using blockchain data. The architectural structure of the system model is depicted in Fig. 1.

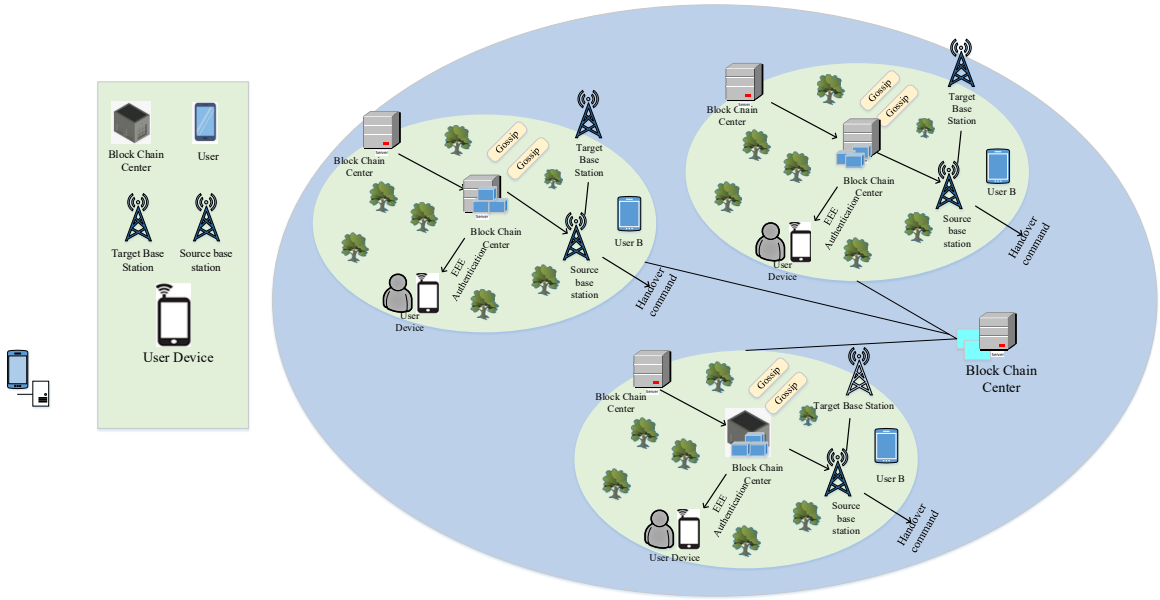


Fig. 1. System model for the overall research work in the UDHN environment.

The final decision about approving or denying the handoff is communicated back to the base stations and the user device. The gossip algorithm ensures the fast propagation of this decision among blockchain nodes. This approach leverages the efficiency of gossip protocols for rapid dissemination and the security of blockchain for tamper-proof, decentralized authentication, making it ideal for reducing handoff delays in 5G networks. In combination with the suggested gossip dissemination and JG-DPBFT consensus, an end-to-end authentication pipeline can be implemented at minimal cost in terms of re-authentication while retaining cryptographic strength. It is a significant and application-specific contribution, and not simply an aggregate of existing methods. Fig. 2 depicts the workflow for the suggested model.

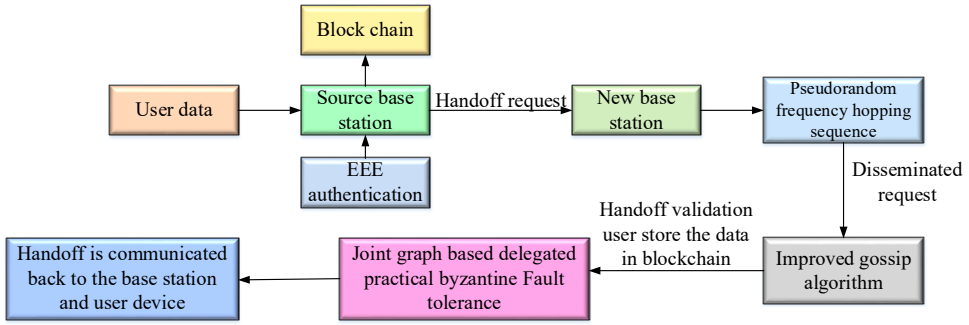


Fig. 2. Systematic flow diagram from end-to-end proposed research.

3.2. Exponential Elliptic Curve Assisted Encryption

Conventional ECC-based authentication schemes rely on scalar multiplication operations, which, while secure, introduce non-negligible computational delay during frequent handovers. The suggested EEE is not a direct successor to ECC, but an improvement that converts multiplication-based key derivation to operations in exponential form, making it more resistant to inverse key computation and less time-consuming to authenticate. In contrast to current ECC adoptions of blockchain-scripted handover protocols, EEE is specifically designed to handle rapid re-authentication and low-latency cryptographic tasks in mobility-empowered systems. EEE provides a feature. The use case diagram of authentication is shown in Fig. 3.

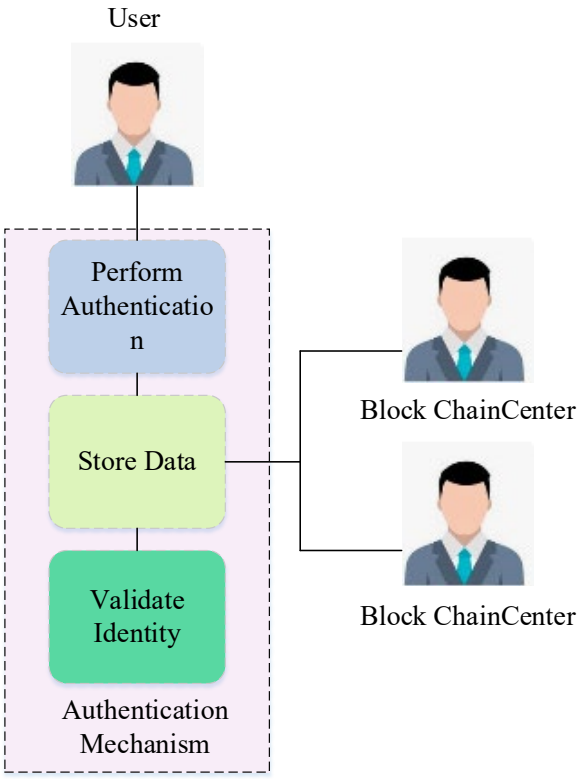


Fig. 3. Use case diagram for authentication using the EEE mechanism.

The user stored the data in the first base station, which is a source base station. Before data is stored, the EEE authentication process occurs between the user and the BS. Based on the digital theory of elliptical curves, the EEE algorithm can act as an asymmetric encryption method. To ensure reproducibility, the proposed EEE scheme is formally defined over a prime field F_p, where p is a large prime. The elliptic curve is expressed in the following equation.

$$E: y^2 = x^3 + ax + b \pmod{p} \tag{1}$$

Where $a, b \in F_p$ satisfy the non-singularity condition $4a^3 + 27b^2 \neq 0$. A base point $G \in E(F_p)$ of order n is publicly agreed upon. The private key $d \in [1, n-1]$ is selected by the base station, and the corresponding public key is computed using the exponential mapping as $T = G^d$. For message encryption, the plaintext is mapped onto a curve point $M(x, y) \in E(F_p)$. A random integer $r \in [1, n-1]$is chosen, and the ciphertext is generated as $C_1 = M + T^r$ and $C_2 = G^r$. Decryption is performed by computing $M = C_1 - (C_2)^d$. The exponential formulation replaced repeated scalar multiplications with exponentiation-based operations, reducing cryptographic computation time while maintaining equivalent security for frequency 5G handoff authentication.

3.3. Pseudorandom frequency hopping sequence

In a blockchain-based 5G handoff authentication system, when a user device enters the range of a new BS, it sends a handoff request using a pseudorandom frequency-hopping sequence [29]. The pseudorandom frequency hopping signal consists of a continuous series of random frequency pulses with equal amplitude and length. This random frequency signal remains at each frequency for seconds; the detailed process is formulated in the equation below.

$$x(t) = \sqrt{2p}\sum_{K=-\infty}^{\infty} rect\frac{t-kt}{T} cos(2\pi f_r + \varphi_k) \quad (2)$$

$$rectQ = \begin{Bmatrix} 1 & -1/2 < Q < 1/2 \\ 0 & elsewhere \end{Bmatrix} \quad (3)$$

Where represent the average power of normalized , and each frequency is determined by , the operation computed in the equation.

$$f_r = f_{ak} + \Delta f_r \quad (4)$$

Where f_{ak} is denoted as the hopped carrier frequency in the kth pulse, and Δf_r is the frequency shift due to the data of the Kth pulse. Based on equation 1, the target receiver intercepts the pseudorandom frequency-hopping signal; here, the receiver's selectivity will alter the received pulse amplitude and shape. A transfer function could be used to characterize the selectivity, and then, the receiver is linear up to the detector input. However, the receiver's transfer function is essentially constant over the spectrum of each pulse. As a result, when the pulse passes through the receiver amplifier, its shape remains unchanged.

$$x(t)=\sqrt{2P}\sum_{K=-\infty}^{\infty} B(y_K) rect\frac{t-kt}{T} \quad (5)$$

Similarly, the probability of the output pulse amplitude will reach certain threshold values, as detailed in the equation below.

$$p(\gamma > \gamma_T)=\int_{\gamma T}^{\infty} p_x(\gamma) d\gamma \quad (6)$$

If the threshold level of is equal to the value of the desired level signal at the same receiver stage, it may indicate that the hopping sequence can avoid the synchronization problem, reduce interference, and improve the faster handoff.

3.4. Improved gossip algorithm

The current gossip-based dissemination schemes in blockchain networks rely primarily on random peer selection, which is prone to message redundancy and excessive communication overhead, especially during common handover events in dense 5G networks. Conversely, the proposed improved gossip algorithm employs a list-based historical node selection algorithm that explicitly eliminates the repeated use of the same peers in message dissemination. This alteration is not a direct adaptation of the traditional gossip protocols. Rather, an adjustment to handover-focused blockchain protocols, in which fast, non-redundant transmission of authentication requests is essential. The proposed method can greatly decrease redundant transmissions and has a direct contribution to the reduction in authentication delay. In addition to that, better throughput is achieved by limiting peer selection based on node history and hierarchical layering of ledgers to peers. Thereby eliminating scalability and latency limitations found in current gossip-based models.

The serving BS sends a handover command to the mobile device that includes information about the target BS. However, this request is disseminated through a gossip process carried out among blockchain nodes. Similarly, it reaches out to the handoff request quickly and effectively through the improved gossip algorithm. In this study, the improved hierarchical network design gossip algorithm modified the messages by incorporating a list organization to store historical node data, thereby limiting the range of target nodes based on the list. However, it minimizes the likelihood of selecting duplicate nodes, allowing fewer redundant messages to be delivered during data synchronization. On the other hand, selecting new nodes can improve data synchronization, resulting in greater efficiency. In general, the gossip algorithm uses three communication modes: push, gossip, and pull gossip. Similarly, the blockchain network follows a hierarchical structure. This network combines the qualities of a centralized structure and a completely distributed unstructured network. However, it establishes a fast-forwarding layer among them and selects a high-performing node as the ledger node. Meanwhile, the ledger and peer nodes form multiple tiers inside the channel. Moreover, the nodes in the channel interconnect based on the gossip algorithm.

Let y denotes the sending node and S_m represents the message to be disseminated. The variable LH denotes the local history list maintained by the node y, which stores the identifiers of peer nodes that have previously received a message from$y$. This list is used to avoid repeated peer selection and redundant message transmission. Let f denotes the number of peers selected for message forwarding in each gossip round and n be the total number of nodes in the network. The peer selection probability P_i for a candidate node i is defined as:

$$P_i = \frac{1}{n+1-f(i)} \tag{7}$$

Where $f(i)$ represents the frequency with which the node i has previously appeared in the local history list. This probability assignment prioritizes rarely contacted nodes, thereby increasing message coverage while reducing redundancy. At each dissemination round, the sending node$y$selects a set of f target nodes that are not present in its local history list LH. Once selected, these target nodes are appended to LH, and the message S_m is transmitted. Each receiving node repeats the same process independently, which ensures distributed propagation while minimizing duplicate transmissions. The variable Y_i denotes the number of newly reached nodes during i^{th} gossip epoch and is modeled as: $Y_i = K^i$. Where, K is the fan-out parameter representing the number of peers contacted per round. This formulation captures the exponential spread property of gossip-based dissemination while remaining bounded by the history-aware peer selection.

Algorithm 1 (Fig. 4) summarizes the improved gossip algorithm in procedural form. Step 1 initializes the message S_m and local history list LH. Steps 2-4 perform probability-based peer selection while explicitly excluding nodes already present in LH. Step 5 disseminates the message to the selected peers. This sequence ensures logical consistency among variable definition, probability computation, and message-forwarding behaviour.

Algorithm 1: Improved gossip algorithm
Sending node y
Step 1: Input, S_b, LH
Step 2: Output, S_m of the node y
Step 3: Select the node f, that does not consider to LH as the target node with probability P, and insert the selected k target nodes into LH_f

$$P = \frac{f}{n+1-f(i)}$$

Step 4: Based on step 1, update the $LH$of sending nodes y by LH_k
Step 5: Send S_m to each target node selected in step 1

Fig. 4. Improved gossip algorithm

3.5. Joint Graph-Based Delegated Practical Byzantine Fault Tolerance

Traditional PBFT and delegated PBFT systems achieve consensus among all nodes, incurring quadratic communication costs and being scalable only up to a certain node density. The proposed JG-DPBFT is fundamentally different in that it dynamically arranges blockchain nodes into subgraphs. This approach reaches consensus concurrently, followed by coordinating the results using a joint graph structure. In contrast to regular delegated consensus, JG-DPBFT allows for dynamic committee composition and block ordering in the form of graphs, alleviating node inconsistency and minimizing global synchronization costs. This structural combination with joint graphs of delegated BFT is a substantive improvement on adaptations of PBFT previously used. This enables the system to achieve low consensus latency and high fault tolerance in the face of both high mobility and frequent handovers.

The proposed JG-DPBFT has enhanced the consensus efficiency; initially, nodes delegate their consensus power to delegates. These delegates reach consensus on a group like PBFT instead of a single set of delegates communicating directly with each other via a joint graph-based structure [30]. Nodes and their connections with voting, trust, and region are represented as graphs. Nodes in graph networks store information about themselves, as well as their predecessors and successors. When consensus nodes join or leave, they change the linkages to their predecessor and successor nodes, allowing for node expansion and removal. The graph can be divided into subgraphs called committees. However, if the client makes a request, there is no need to wait for the result before generating an alternative request. Every communication is processed independently by a committee, and different committees might operate in parallel processes. Similarly, the graph structure is used to address node inconsistency in blocks. Then, delegates from each committee form a joint graph that runs the PBFT consensus protocol. However, due to network latency, various blocks may occur only on a subset of nodes, which is addressed by employing a pre-block approach to ensure the algorithm runs smoothly. The algorithm consists of three phases: transaction validation, pre-block generation, and block synchronization.

Let the blockchain network consist of n nodes, where at most f nodes may behave in a Byzantine manner, satisfying the fault tolerance condition $n \geq 3f + 1$. A committee $C \subseteq n$ of size g is dynamically selected for each consensus round based on node trust score and network connectivity. Only committee nodes participate in block proposal and validation, which reduces consensus overhead. Each node i is assigned a trust score $\tau_i \in [0,1]$, computed from its historical validation success rate, response latency, and malicious behaviour history. Nodes with $\tau_i \geq \tau_{th}$ are eligible for committee selection, where τ_{th} is a predefined threshold. The leader node is randomly elected from the committee using a hash-based selection function to prevent targeted attacks. A block is considered valid when it receives at least $2f + 1$ confirmations from committee members. The proposed JG mechanism model blocks dependencies as a directed acyclic graph, enabling deterministic block ordering and synchronization across committee and non-committee nodes.

3.5.1. Transaction validation stage

In order to determine the associated committee and random leader, the client must first send a transaction request, which is then hashed based on its content and time stamp. Pre-execution and transaction validation are conducted within the committee, and its members sign and disseminate the execution results. A committee member evaluates requests from other members by different outcomes with its computations. If the outcomes of the comparison are consistent, the message seems authentic. The random leader distributes the pre-block data and computation outcomes to all committee participants after gathering requests for the same computed results. Since members of the committee are broadcasting during this phase, the communication overhead may be computed in the following equation.

$$CTimes_1 = (2g + 1)^2 = 4g^2 + 4g + 1 \quad (8)$$

In the transaction validation stage, the leader broadcasts the transaction digest to all g committee members and collects verification responses. Each committee node exchanges validation messages with

all other committee nodes to ensure consistency. Hence, the communication cost grows quadratically with committee size, resulting in $(2g + 1)^2$message exchange in the worst case.

3.5.2. Pre-block Generation Stage

When the random leader sends a pre-block confirmation request to a committee node, it first verifies the previously collected g valid votes from another node. Once a valid vote from other nodes has been gathered, the node confirms the leader's request for pre-block confirmation. However, check if the block in demand contests the block to validate nearby with composed effective divisions. Once it has gathered feedback g The committee participants send a pre-block group request to all non-committee nodes. The non-committee nodes give the leader feedback and carry out pre-block generation operations on the block that the leader sends. When the leader node obtains a response from non-committee nodes in addition to the committee members' feedback from a total $2g + 1$, it shows block validation data to all nodes, signifying that the pre-block generation is finished. As a result, this stage includes random leader dissemination to the committee first, followed by non-committee nodes after validation, allowing it to calculate the communication overhead, as shown in the equation below.

$$CTimes_2 = (2g + g) * 2 = 6g \tag{9}$$

During pre-block generation, the leader disseminates the pre-block to committee members and receives confirmations. Additionally, committee nodes interact with selected non-committee nodes to obtain block-verification feedback. This stage involves linear communication dominated by leader-node and node-leader exchanges, resulting in $6g$ message transmissions.

3.5.3. Block synchronization stage

If the node gathers f block validation data, it executes the block synchronization process. Initially, the node hashes the gathered block authorization data and categorizes it based on the hash result. The sorted block dependence data is then broadcast by each node to all nodes. While the node obtains valid data from $2g$ nodes, it achieves local block provisions as well as block reordering information. The communication above in this phase is computed as below,

$$CTimes_3 = (2g + 1)^2 = 9g^2 + 6G + 1 \tag{10}$$

In the synchronization stage, validated blocks are propagated to ensure consistency across the committee and non-committee. Each node verifies and exchanges block dependency information using the joint-graph structure. This phase requires all-to-all communication within the committee, resulting in quadratic communication complexity. The overall communication overhead essential for the consensus algorithm is computed as follows,

$$CTimes_{total} = \sum_i^3 CTimes_i \tag{11}$$

$$CTimes_{total} = 13g^2 + 16g + 2 \rightarrow 0(n^2) \tag{12}$$

By substituting equation (10-12) into (13), the overall communication complexity is obtained. Since the committee size starts, equation g is proportional starting from the total n. The worst-case complexity remains quadratic. However, due to committee-based participation, joint-based participation, and joint-graph synchronization, the practical communication overhead is significantly lower than that of classical PBFT, which requires full network-wide all-to-all messaging. Algorithm 2 (Fig. 5) represents the algorithm of JG-DPBFT.The DPBFT algorithm employs join graph-based synchronous block processes. The transaction summary content, as well as information on the leader node, is concatenated into a string and hashed to provide a 256-bit random integer to confirm that altered nodes yield separate hashes. Similarly, the initial block has a small hash value, whereas the last block has a huge hash rate. As a result, the JG-DPBF ensures that the network remains secure even if certain nodes become corrupted.

Algorithm 2: JG-DPBFT algorithm
Step 1: **Function Broadcast message**
Step 2: If org (n) ← node then
Step 3: digestByte = [ ]$byte\ (DIgest)$
Step 4: if true ← Verify then
Step 5: else
Step 6: if true ← message pool then
Step 7: Count +++
Step 8: if count >= fault number then
Step 9: Broadcast TemCommit
// Determine the message from the leader
Step 10: digestByte = [ ]$byte\ (DIgest)$
Step 11: if true ← message pool then
Step 12: else
Step 13: if true ← Verify then
Step 14: if count >= $g + 1$ then
Step 15: Block → LocalBlock pool
Step 16: Reply (Result)
Step 17: Function broadcaster Synchronization
REQUEST
Step 18: if node =seedNode then
Step 19: if verify =True **then** // Verify block information
Step 20: Count++
Step 21: Calculate block message
Step 22: Function Handle synchronization sequence
REQUEST
Step 23: For i in block message () do
Step 24: if Verify i = True then
Step 25: First block= Min (Block dependencies)
Step 26: Last block= Min (Block dependencies)
Step 27: Result = sort (block dependencies) // Join graph structure
Step 28: Broadcast (Result)

Fig. 5. JG-DPBFT algorithm

4. Result and discussion

This section discusses the results of the suggested technique. The performance of IGJ-DPBFT can be measured using several indicators commonly used in current algorithms to assess its efficacy. Table 2 shows the simulation's network restrictions. The parameter standards are chosen based on prior studies, as is the performance of the suggested method with various restriction settings. Employing these restriction settings yields greater results in the suggested research.

All cryptographic operations and simulations were performed on a machine with an Intel Core i7 processor (3.2 GHz), 16 GB of RAM, and Ubuntu 20.04. The suggested EEE authentication and JG-DPBFT consensus mechanisms were implemented in software without hardware acceleration. All compared consensus protocols were evaluated under identical network conditions and without aggressive parameter tuning, ensuring that performance differences reflect architectural characteristics rather than configuration bias.

The experiments have been conducted using the ns-3 simulator. The user traffic is modeled using a constant bit rate (CBR) model; the packet size is 512 bytes, and the packet interval is 20 ms. The Random Waypoint model is used to simulate UE mobility at a speed of 210 m/s over a simulation time of 300 s. Network load is varied by varying the number of active UEs from 10 to 50, and constant traffic patterns are held constant across all compared schemes. Underlying wireless connections are configured as a standard 5G-like setup, and all base stations are linked together with a wired backhaul. Simulation does not inject any explicit active attack traffic; rather, Byzantine behavior is simulated at the protocol

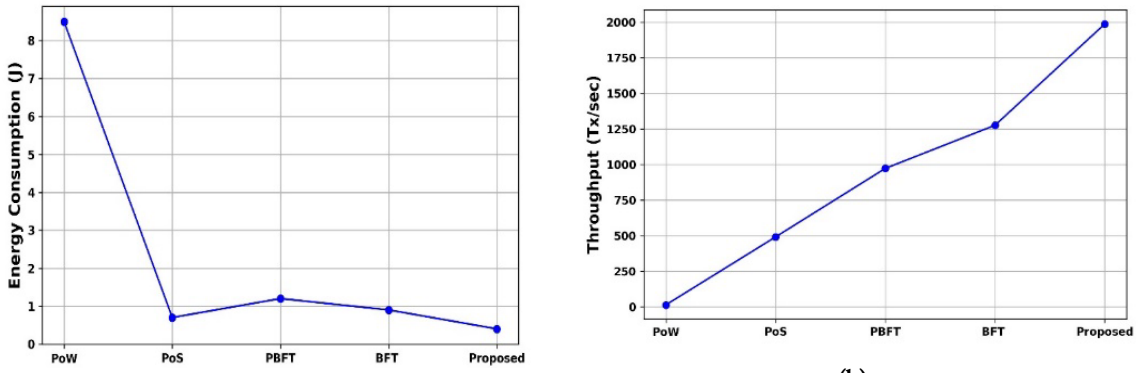
level by permitting the compromised nodes to arbitrarily violate the consensus protocol within the modeled fault tolerance. Such environments remain fixed to maintain valid and comparable comparisons.

Table 2. Simulation parameters used for evaluation.

Parameter	Value
Simulation Time	200 seconds
Number of UEs	20 mobile nodes
Number of gNodeBs	4 (deployed in grid pattern)
Mobility Model	RandomWaypointMobilityModel
Area Size	1000 m x 1000 m
gNodeB Placement	Grid (2x2 layout)
Backhaul Type	PointToPoint (5 Mbps, 2 ms)
Core Network Model	ns-3 LTE Evolved Packet Core (EPC)
Frequency	3.5 GHz
Bandwidth	100 MHz
Tx Power	23 dBm (UE), 30 dBm (gNodeB)
Noise Figure	5 dB
Channel Model	ThreeGppUrbanMacroPropagationLossModel + RayleighFading
Antenna Model	IsotropicAntennaModel
Propagation Delay	ConstantSpeedPropagationDelayModel
Number of Blockchain Nodes	5 (1 per edge server)
Consensus Protocol	JGB-DPBFT (Joint-Graph Based DPBFT)
Block Creation Interval	0.5 seconds
Smart Contract Execution Time	25 ms
Block Size	1 KB
Blockchain Communication Delay	10 s

4.1. Performance evaluation

The outcomes of IGJ-DPBFT are shown and related to other algorithms such as POW, proof of stack (POS), Practical BFT (PBFT), and BFT. Fig. 6(a) depicts the energy consumption for both the current and the suggested methods. The energy usage was calculated using the received and transmission rates. The suggested method offers lower energy consumption than current methods at 0.4 J. In contrast, the conventional network-based technique consumes more energy due to frequent re-authentication. Fig. 6(b) depicts the throughput analysis; the proposed approach achieves high network performance at a rate of 1987 Tx/sec. In the traditional technique, a greater network size and low throughput in communication between delegates might slow down each round.



(a) (b)

Fig. 6. Energy consumption and throughput performance in a 5G ultra-dense network with 4 gNodeBs (grid layout) and 20 mobile UEs.

The comparison between energy use and throughput is shown in Table 3. The proposed consensus method achieved the best overall performance, requiring only 0.4 J of energy while delivering the highest throughput of 1,987 transactions/s. Compared with conventional methods, it reduced energy consumption by 95.3% relative to PoW, 42.9% relative to PoS, 66.7% relative to PBFT, and 55.6% relative to BFT, while significantly improving transaction processing capacity. These results demonstrate

that the proposed approach provides a more energy-efficient and scalable solution for blockchain consensus.

Table 3. Analysis of Energy Consumption and Throughput.

Methods	Energy Consumption (J)	Throughput (Tx/sec)
PoW	8.5	15
PoS	0.7	492
PBFT	1.2	973
BFT	0.9	1276
Proposed	**0.4**	**1987**

The performance of consensus delay is associated with existing approaches such as POW, POS, PBFT, and BPFT, as illustrated in Fig. 7(a). Compared with the standard methodology, the suggested method has a shorter delay. However, with the suggested model, the delay is in the order of 90 ms due to the rapid consensus process. Similarly, consensus computing with a short minimum time length can efficiently learn the parameters employed in the process. Fig. 7(b) shows a performance assessment of the consensus period. The examination clearly shows that the suggested technique takes the least time, at 199 ms, while the old model takes significantly longer at 25864 ms, 2864 ms, 876 ms, and 576 ms.

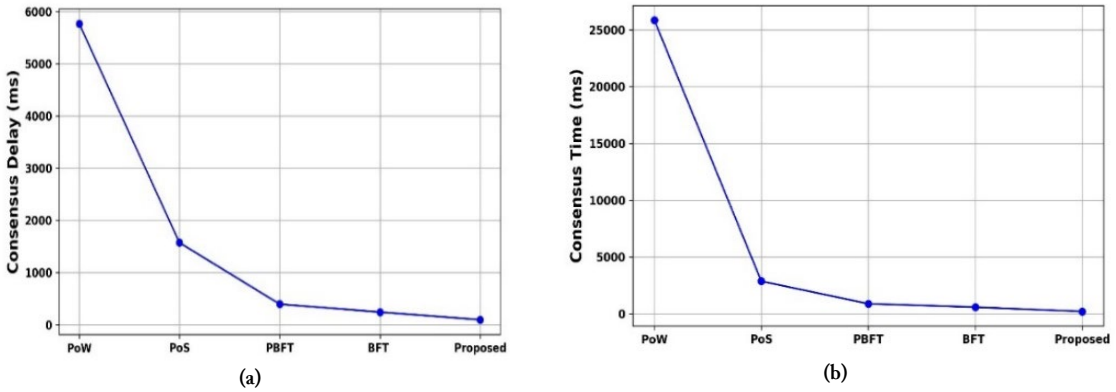


Fig. 7. Consensus delay and consensus time measured during handovers in a grid-based 5G topology with 20 mobile UEs.

Frequent UE mobility and blockchain-based authentication over wired backhaul influence performance. Fig. 8(a) depicts the usage of bandwidth in the path employing several existing and suggested models. The suggested method is more competent than the current network-based methodology. The suggested method increases the number of packets sent between the source and destination in the cell at a rate of 146 Mbps.

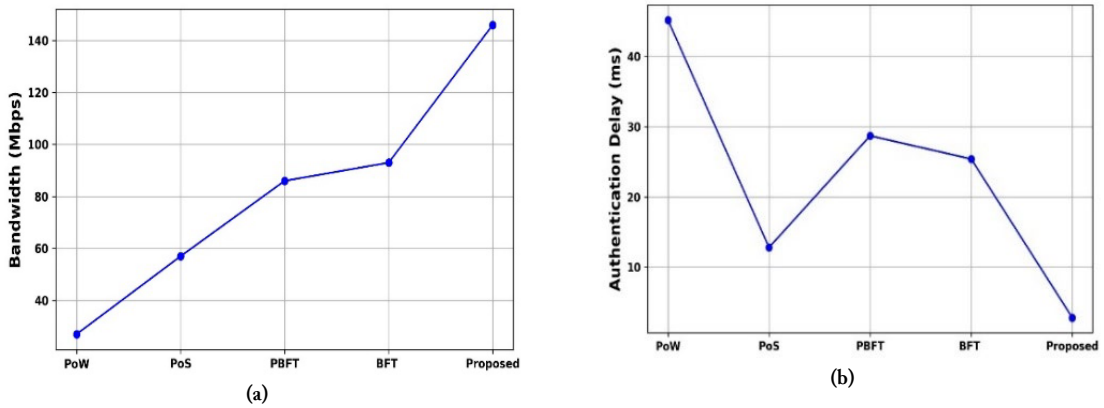


Fig. 8. Bandwidth utilization and handover authentication delay in a multi-cell 5G network with mobile users.

Fig. 8(b) compares the authentication handover delays of the proposed method to those of several current algorithms. The old POW-based technique requires the user to register on the blockchain and

re-authenticate in the cell after moving between cells numerous times. These approaches necessitate re-approval and verification protocols that differ across cells. As proposed, the user is not required to re-authenticate when switching between cells, since they are valid end-to-end, and during handover, eliminating the authentication wait. However, associated with current approaches, the proposed consensus mechanism lowered the handover authentication delay to 2.8 milliseconds. Similarly, increasing network utilization dramatically increases the handover authentication delay. Table 4 compares prevailing and proposed bandwidth and authentication methods.

Table 4. Analysis of bandwidth and authentication delay.

Methods	Bandwidth (Mbps)	Authentication Delay (ms)
PoW	27	45.2
PoS	57	12.8
PBFT	86	28.7
BFT	93	25.4
Proposed	146	2.8

Fig. 9(a-c) presents a comprehensive assessment of authentication techniques, focusing on encryption, decryption, and key generation timeframes, providing crucial information on how well existing and planned algorithms support secure data and processing. However, the proposed method performs exceptionally well, with encryption, key creation, and decryption taking only 0.0654, 0.124, and 0.135 milliseconds, respectively. Existing AES key creation has a high computational cost, and this technique results in slow encryption and a long decryption times. However, during decryption, the older DES technique exhibits delegate overload and longer processing lags. Furthermore, traditional AES had a high frequency of handoffs, which could increase the overall cost of encryption. Table 5 compares the current and proposed authentication methods.

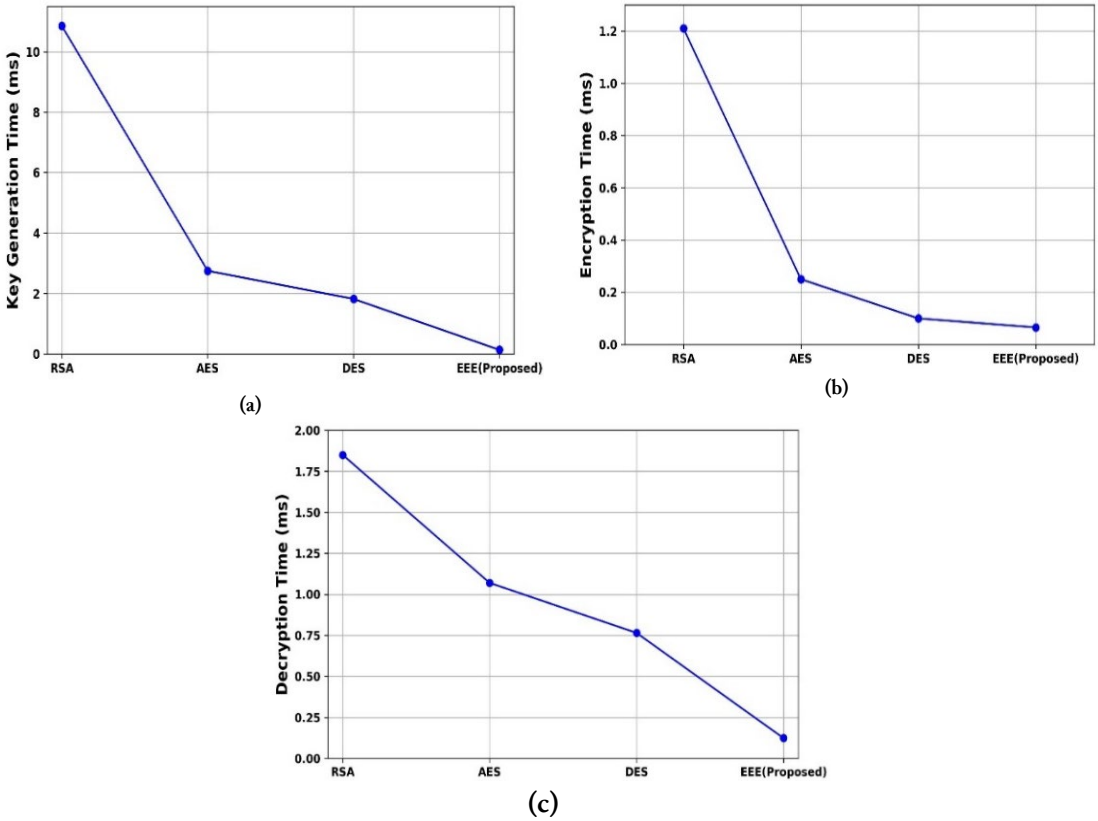


Fig. 9. Comparison of cryptographic key generation, encryption, and decryption time during handover authentication. Results reflect processing overhead at edge blockchain nodes triggered by UE mobility events.

Table 5. Comparison of the relative analysis of authentication.

Models	Encryption Time (ms)	Decryption Time (ms)	Key Generation Time (ms)
RSA	1.21	1.85	10.85
AES	0.25	1.07	2.75
DES	0.1	0.765	1.82
EEE(Proposed)	0.0654	0.124	0.135

Fig. 10(a-c) represents the performance evaluation of consensus time, energy consumption and throughput analysis based on the number of nodes.

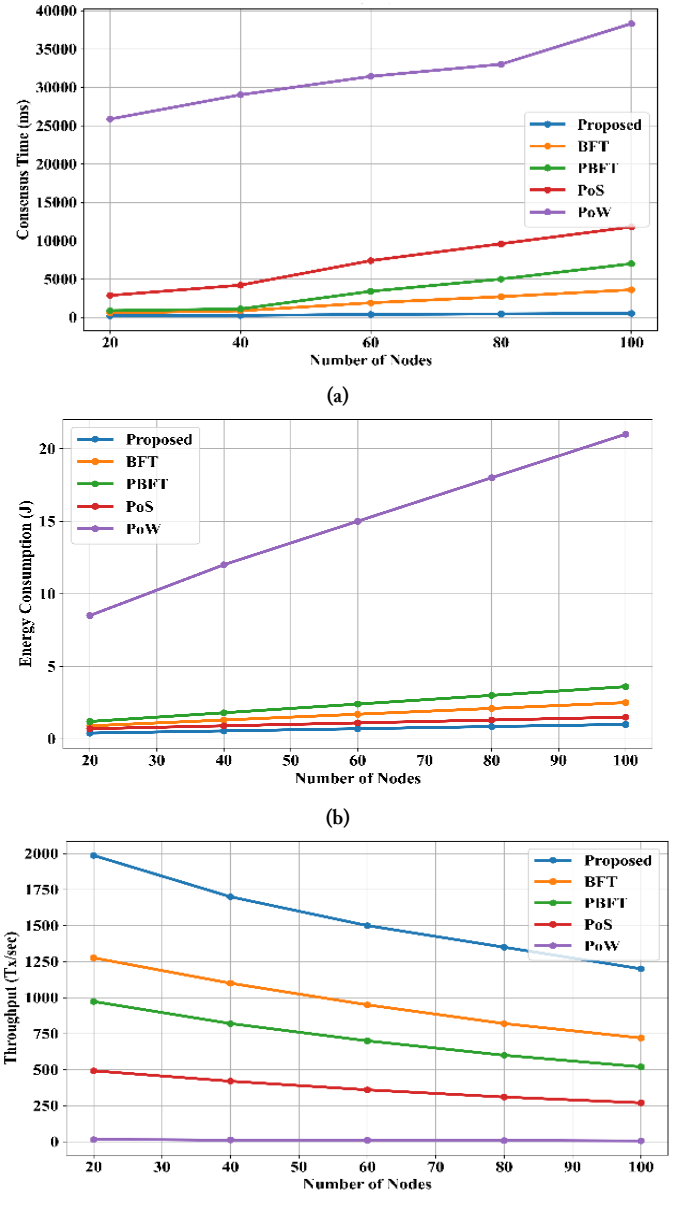


Fig. 10. (a-c): Impact of increasing blockchain node count on consensus delay, energy consumption, and throughput. Simulations use the same mobile UE scenario and wired backhaul-supported 5G grid topology.

From this analysis, the proposed model has obtained better results. According to the performance analysis in terms of energy consumption, throughput, and consensus delay, the suggested IGJ-DPBFT model is much better than the conventional schemes like PoW, PoS, PBFT, and BFT. PoW shows the

highest energy consumption, exceeding 21 J, with 20 to 100 nodes; the proposed model shows minimal energy consumption of less than 1 J with 100 nodes, indicating low computational power during authentication. PoW and PBFT also exhibit sharp degradation during node density, decreasing to less than 10 Tx/s and 310 Tx/s, respectively, whereas the proposed model exhibits a higher throughput over 1200 Tx/s and higher node densities, which keeps the data transmission efficient during mobility. On the same note, the consensus time of existing models grows exponentially, and PoW and PBFT are 38321 ms and 11800 ms, respectively, at 100 nodes, compared to the proposed model at less than 520 ms, offering faster block validation and lower authentication time. In general, the current techniques are characterized by high latency, energy consumption, and lack of scalability because of the multiple re-authentication and intensive consensus protocols, whereas the suggested IGJ-DPBFT model delivers quick, energy-efficient, and scalable handoff authentication applicable to ultra-dense 5G networks. Table 6 represents the valuation of training time and inference time for the cryptographic mechanism in the proposed framework. Table 7 represents the total handover latency evaluation for the existing and proposed models.

Table 6. Cryptography mechanism-based average time evaluation.

Operation	Description	Average Time (ms)
EEE Key Generation	Elliptic curve private–public key pair generation	1.35
EEE Signature Generation	Authentication request signing	0.86
EEE Signature Verification	Authentication verification at BS	1.91

Table 7. Latency breakdown of the proposed model by handover.

Latency Component	Description	Average Delay (ms)
Propagation Delay	UE–BS and BS–blockchain node communication	32.4
Cryptographic Processing	EEE authentication and signature verification	6.8
Consensus Execution	JG-DPBFT block validation and commit	48.1
Total Handover Latency	End-to-end authentication and consensus	87.3

The reported low-latency performance is substantiated through a detailed time-budget analysis that decomposes the total handover delay into propagation, cryptographic verification, and consensus execution components. These results confirm that the observed sub-100ms consensus latency arises from architectural efficiency rather than favourable simulation settings.

4.2. Ablation study analysis and confidence interval test

Tables 8 and 9 present the results of the ablation study and the confidence interval test to demonstrate model robustness. An ablation study represents the performance evaluation of various phase configurations. The improved gossip reduces redundant messaging and lowers consensus delay. EEE mechanism integration reduced authentication time and energy compared to standard ECC replacement.

Table 8. Ablation study.

Model variant	Authentication Delay (ms)	Handoff Success Rate (%)
Proposed	2.82 ± 0.09	99.6 ± 0.8
Without Improved Gossip	5.60 ± 0.21	92.1 ± 1.6
Without Joint-Graph Delegation	7.30 ± 0.28	88.3 ± 2.1
Without EEE (replace with standard ECC)	6.80 ± 0.24	90.7 ± 1.9
Without Gossip & Without JG (both removed)	9.42 ± 0.35	82.7 ± 2.7
Baseline PBFT (for reference)	28.7 ± 0.9	86.9 ± 2.3

Table 9. Confidence interval test for the existing and proposed models.

Scheme	Authentication Delay (ms)	Consensus Delay (ms)	End-to-End Handover Latency (ms)
PoW	182.4 ± 9.6	420.7 ± 18.3	603.1 ± 21.4
PoS	141.8 ± 7.2	312.5 ± 14.9	454.3 ± 16.8
PBFT	118.6 ± 6.1	164.3 ± 9.7	282.9 ± 12.4
BFT	109.2 ± 5.8	151.6 ± 8.9	260.8 ± 11.6
JG-DPBFT (Proposed)	**42.7 ± 2.3**	**68.9 ± 4.1**	**111.6 ± 6.2**

As the experimental analysis shows, the proposed JG-DPBFT-based handover framework outperforms PoW, PoS, PBFT, and BFT in terms of authentication time, consensus latency, and end-to-end handover time. The outcomes are presented as the mean values with 95 % confidence intervals across a series of independent simulations, which results in the confirmation that the performance gains are statistically consistent, and not because of the variability in a single run. This is mainly because of committee-based consensus, fewer complexities of messages, and lightweight cryptographic operations, all with consistent performance in the considered network conditions. All values represent the mean and 95% confidence interval computed over 10 independent ns-3 simulation runs with different random seeds.

4.3. Computational complexity analysis

The computational complexity of the proposed IGJ-DPBFT scheme is significantly reduced by delegating consensus to selected committee nodes rather than performing full-network validation, as in PoW and PBFT. The improved gossip algorithm optimizes message dissemination by minimizing redundant transmission, reducing computational complexity from $O(n^2)$ to approximately $O(k\ log\ n)$, where k represents selected target nodes. The JG-DPBFT divides nodes into sub-graphs, enabling parallel validation, lowering consensus complexity from $O(n^3)$ in traditional PBFT, to $O(n^2)$. Additionally, the EEE encryption mechanism replaces heavy multiplication-based elliptic operations with exponential operations, thereby reducing the time complexity of key generation and encryption. Overall, the combined mechanism reduces total computational cost while enhancing scalability and latency of large-scale 5G deployments. Table 10 represents the state-of-the-art model comparison with the proposed approach.

Table 10. State-of-the-art models comparison.

References	Year	Performance metrics
[21]	2024	Authentication delay- 2.90ms
[22]	2024	Handoff failure-0.06%
[23]	2024	Handoff success rate-89.5%
[26]	2024	Communication cost-1088 bits
[31]	2025	Handoff success rate-90.5%
[32]	2025	Authentication delay-890 ms
Proposed	-	**Authentication delay- 2.82ms, Handoff failure rate-0.04% Handoff success rate-99.6% Communication cost-1021 bits Throughput-96.12 Mbps**

From this analysis, it is evident that the proposed model achieved higher values than the existing approaches. The presence of novel layers and modules in the hand-off management systems in the proposed model helped to achieve better results.

4.4. Security model and formal analysis

4.4.1. Threat model

A partially synchronous 5G network is considered, with blockchain-based stations and edge nodes implemented. The adversary is a probabilistic, poly time (PPT) attacker that can do the following: The

proposed architecture is analysed under a partially synchronous network model in which an adversary may compromise up to f Byzantine nodes, with $f < \frac{n}{3}$, capable of arbitrary behaviour such as message manipulation, replay, and omission. Compromised nodes can act in an arbitrary manner, such as by sending malicious messages or trying to break consensus. The opponent may intercept, replay, delay, or alter messages on wireless and backhaul connections, but cannot compromise common cryptographic primitives. Permissioned blockchain membership and identity binding address Sybil attacks. The denial-of-service attacks are believed to be finite and cannot permanently block honest node communication.

4.4.2. Security goals

The JG-DPBFT consensus mechanism is safe as long as the proportion of the participating nodes is less than one-third. At least 2f+1 block members must provide confirmation, ensuring that at least one honest node is involved in any committed decision. Since honest nodes will never accept conflicting blocks, it is impossible to commit two distinct blocks at the same sequence number, thereby avoiding an inconsistent authentication record.

4.4.3. Safety of JG-DPBFT

In partial synchrony, when the network delay is bounded, consensus progress is assured once the network delay has reached a global stabilization time. The leaders in the committee are not chosen permanently, which impedes abuse by the rogue nodes. Since a minority of the nodes are malicious, an honest leader will ultimately facilitate the successful execution of a consensus round, so that valid handover authentication requests will ultimately be committed.

4.4.4. EEE authentication security (RoR model)

The Real-or-Random (RoR) model of authenticated key exchange is used to analyze the EEE-based authentication scheme. Under this model, the attacker is able to view protocol executions, inject messages, and disclose some session keys, but needs to make a difference between a real session key and a random value in a test run. EEE security is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) hardness. The ECDLP can be solved by any adversary that is capable of solving it with non-negligible advantage using the real session key, and is computationally infeasible. Thus, the generated session keys are computationally indistinguishable from random and guarantee session secrecy and authentication.

4.4.5. Replay resistance

New nonces and session-specific parameters are added in every authentication exchange, so that previously sent messages cannot be reused to facilitate illicit entry. This causes honest nodes to reject replayed handover authentication messages.

5. Conclusion

This study proposed a new consensus procedure for handoff verification based on the IGJ-DPBFT handover model, which enhances 5G network user authentication and handover latency. However, in this paper, the use of blockchain technology and a new EEE authentication approach was proposed to protect user privacy in a safer, faster, and more effective manner to advance the 5G network, as well as to provide intelligent access control across different cells. The reduction in delay, consensus network security, and energy saving are some of the characteristics and objectives of 5G networks. Finally, in contrast with traditional PoW, PoS, PBFT, and BFT, the suggested consensus mechanism based on IGJ-DPBFT has attained less energy consumption, less consensus time, high throughput, and minimum handover authentication delay, respectively.

The research is only tested in terms of simulation using ns-3 under controlled network conditions. There are no actual deployment or hardware in the loop experiments. Explicit malicious-node attack scenarios are not tested, even though the consensus design presumes Byzantine behavior. Moreover, the security of the suggested EEE scheme and JG-DPBFT protocol is analytically characterized and lacks formal cryptographic or consensus proofs. These will be considered in subsequent extensions of this

work. In the future, a new solution will be developed to improve the consensus approach, along with security enhancements applicable to various types of blockchain. However, future work in this research mainly focuses on extending support to 6G networks, which are expected to involve terahertz communication and ultra-dense node deployment.

Declarations

Author contribution. Ravindra Janardan Lawande: Writing- Original Draft Preparation, Specifically Writing the Initial Draft.Sudhir Bapurao Lande: Review & Editing Preparation, Project administration, Formal analysis, Investigation. Shailendrakumar Mahadeo Mukane: Resources, Specifically Critical Review, Conceptualization.

Funding statement. No funding is provided for the preparation of the manuscript.

Conflict of interest. The authors declare no conflict of interest.

Additional information. No additional information is available for this paper.

References

[1] B. Patel, V. K. Yarlagadda, N. Dhameliya, K. Mullangi, and S. C. R. Vennapusa, "Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering," *Eng. Int.*, vol. 10, no. 2, pp. 117–130, Oct. 2022, doi: 10.18034/ei.v10i2.715.

[2] V. O. Nyangaresi and A. J. Rodrigues, "Efficient handover protocol for 5G and beyond networks," *Comput. Secur.*, vol. 113, no. February, p. 102546, Feb. 2022, doi: 10.1016/j.cose.2021.102546.

[3] M. S. M. Gismalla *et al.*, "Survey on Device to Device (D2D) Communication for 5GB/6G Networks: Concept, Applications, Challenges, and Future Directions," *IEEE Access*, vol. 10, pp. 30792–30821, 2022, doi: 10.1109/ACCESS.2022.3160215.

[4] J. Huang and Y. Qian, "A Secure and Efficient Handover Authentication and Key Management Protocol for 5G Networks," *J. Commun. Inf. Networks*, vol. 5, no. 1, pp. 40–49, Mar. 2020, doi: 10.23919/JCIN.2020.9055109.

[5] D. Mishra and E. Natalizio, "A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements," *Comput. Networks*, vol. 182, no. December, p. 107451, Dec. 2020, doi: 10.1016/j.comnet.2020.107451.

[6] E. Skondras, I. Kosmopoulos, E. Michailidis, A. Michalas, and D. Vergados, "A Group Handover Scheme for Supporting Drone Services in IoT-Based 5G Network Architectures," *Drones*, vol. 6, no. 12, p. 425, Dec. 2022, doi: 10.3390/drones6120425.

[7] H. Hemavathi, S. R. Akhila, Y. Alotaibi, O. I. Khalaf, and S. Alghamdi, "Authentication and Resource Allocation Strategies during Handoff for 5G IoVs Using Deep Learning," *Energies*, vol. 15, no. 6, p. 2006, Mar. 2022, doi: 10.3390/en15062006.

[8] R. A. Paropkari, A. Thantharate, and C. Beard, "Deep-Mobility: A Deep Learning Approach for an Efficient and Reliable 5G Handover," in *2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, IEEE, Mar. 2022, pp. 244–250. doi: 10.1109/WiSPNET54241.2022.9767158.

[9] X. Yan and M. Ma, "A privacy-preserving handover authentication protocol for a group of MTC devices in 5G networks," *Comput. Secur.*, vol. 116, no. May, p. 102601, May 2022, doi: 10.1016/j.cose.2021.102601.

[10] "A lightweight and secure handover authentication scheme for 5G network using neighbour base stations," *J. Netw. Comput. Appl.*, vol. 193, p. 103204, Nov. 2021, doi: 10.1016/J.JNCA.2021.103204.

[11] S. Gupta, B. L. Parne, N. S. Chaudhari, and S. Saxena, "SEAI: Secrecy and Efficiency Aware Inter-gNB Handover Authentication and Key Agreement Protocol in 5G Communication Network," *Wirel. Pers. Commun.*, vol. 122, no. 4, pp. 2925–2962, Feb. 2022, doi: 10.1007/s11277-021-09036-4.

[12] M. Y. Wang, M. H. Chen, and M. H. Jiang, "Blockchain-based predictive framework for security authentication in 5G ultra-dense networks," *https://doi.org/10.1117/12.3061894*, vol. 13562, p. 1128, Apr. 2025, doi: 10.1117/12.3061894.

[13] M. Hojjati, A. Shafieinejad, and H. Yanikomeroglu, "A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks," *IEEE Access*, vol. 8, pp. 216461–216476, 2020, doi: 10.1109/ACCESS.2020.3041710.

[14] J. Divakaran, A. Chakrapani, and K. Srihari, "Fuzzy Logic Based Handover Authentication in 5g Telecommunication Heterogeneous Networks," *Comput. Syst. Sci. Eng.*, vol. 46, no. 1, pp. 1141–1152, Jan. 2023, doi: 10.32604/csse.2023.028050.

[15] S. V. Manjaragi and S. V. Saboji, "Fast user authentication in 5G heterogeneous networks using RLAC-FNN and blockchain technology for handoff delay reduction," *Wirel. Networks*, vol. 29, no. 7, pp. 3187–3205, Oct. 2023, doi: 10.1007/s11276-023-03371-z.

[16] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May 2022, doi: 10.1109/TNSE.2022.3142287.

[17] F. Yu, M. Ma, and X. Li, "A Blockchain-Assisted Seamless Handover Authentication for V2I Communication in 5G Wireless Networks," in *ICC 2021 - IEEE International Conference on Communications*, IEEE, Jun. 2021, pp. 1–6. doi: 10.1109/ICC42927.2021.9500334.

[18] M. M. Salim, V. Shanmuganathan, V. Loia, and J. H. Park, "Deep Learning Enabled Secure IoT Handover Authentication for Blockchain Networks," *Human-centric Comput. Inf. Sci.*, vol. 11, p. 21, 2021, doi: 10.22967/HCIS.2021.11.021.

[19] B. Goswami and H. Choudhury, "A Blockchain-Based Authentication Scheme for 5G-Enabled IoT," *J. Netw. Syst. Manag.*, vol. 30, no. 4, p. 61, Oct. 2022, doi: 10.1007/s10922-022-09680-6.

[20] Z. Haddad, M. Baza, M. M. E. A. Mahmoud, W. Alasmary, and F. Alsolami, "Secure and Efficient AKA Scheme and Uniform Handover Protocol for 5G Network Using Blockchain," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2616–2627, 2021, doi: 10.1109/OJCOMS.2021.3131552.

[21] P. Krishnan, K. Jain, A.-S. D. Alluhaidan, and P. Prabu, "Highly secured authentication and fast handover scheme for mobility management in 5G vehicular networks," *Comput. Electr. Eng.*, vol. 116, no. May, p. 109152, May 2024, doi: 10.1016/j.compeleceng.2024.109152.

[22] K. Mannem, P. N. Rao, and S. C. M. Reddy, "Power optimized intelligent Handoff mechanism for 5G-Heterogeneous network," *Multimed. Tools Appl.*, vol. 83, no. 19, pp. 56697–56718, Dec. 2023, doi: 10.1007/s11042-023-17709-4.

[23] A. Baz, J. Logeshwaran, Y. Natarajan, and S. K. Patel, "Enhancing mobility management in 5G networks using deep residual LSTM model," *Appl. Soft Comput.*, vol. 165, no. November, p. 112103, Nov. 2024, doi: 10.1016/j.asoc.2024.112103.

[24] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. Al-Dhlan, "HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks," *IEEE Access*, vol. 12, pp. 6251–6261, 2024, doi: 10.1109/ACCESS.2024.3351278.

[25] Z. Haddad, "Enhancing privacy and security in 5G networks with an anonymous handover protocol based on Blockchain and Zero Knowledge Proof," *Comput. Networks*, vol. 250, no. August, p. 110544, Aug. 2024, doi: 10.1016/j.comnet.2024.110544.

[26] B. Goswami and H. Choudhury, "A Secure and Fast Handover Authentication Scheme for 5G-Enabled IoT Using Blockchain Technology," *Wirel. Pers. Commun.*, vol. 138, no. 4, pp. 2155–2181, Oct. 2024, doi: 10.1007/s11277-024-11559-5.

[27] P. Surapaneni, S. Bojjagani, and A. K. Maurya, "Handover-Authentication Scheme for Internet of Vehicles (IoV) Using Blockchain and Hybrid Computing," *IEEE Access*, vol. 12, pp. 140483–140501, 2024, doi: 10.1109/ACCESS.2024.3468473.

[28] R. Ma, J. Zhou, and M. Ma, "A Blockchain-assisted Group Handover Authentication Protocol for 5G Wireless Networks," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, May 2024, pp. 78–83. doi: 10.1109/IWCMC61514.2024.10592452.

[29] M. Marcozzi and L. Mostarda, "Analytical model for performability evaluation of Practical Byzantine Fault-Tolerant systems," *Expert Syst. Appl.*, vol. 238, no. March, p. 121838, Mar. 2024, doi: 10.1016/j.eswa.2023.121838.

[30] Z. Zeng, C. Jiang, Y. Zhou, and T. Zhou, "A Time–Frequency Domain Analysis Method for Variable Frequency Hopping Signal," *Sensors*, vol. 24, no. 19, p. 6449, Oct. 2024, doi: 10.3390/s24196449.

[31] S. M. Topazal *et al.*, "Intelligent device to device handover management techniques for 5G/6G and beyond," *J. Supercomput.*, vol. 81, no. 5, p. 737, Apr. 2025, doi: 10.1007/s11227-025-07182-1.

[32] S. Yao, X. Zhang, and J. Xu, "A Blockchain-based Lightweight Privacy-Preserving Authentication Protocol for Access and Handover in Space-Ground Integrated Networks," in *Proceedings of the 2025 5th International Conference on Computer Network Security and Software Engineering*, New York, NY, USA: ACM, Feb. 2025, pp. 50–58. doi: 10.1145/3732365.3732373.