SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I7P129

Volume 12 Issue 7, 378-389, July 2025

Original Article

Optimized Secure Handover in 5G Networks Using Lightweight Blockchain and Hierarchical Clustering

Kiran Mannem[1], Suresh Suggula[2], Srinivasulu Reddy Battu[3], Shilpa Bagade[4]

[1]*Department of ECE, Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad, India.*
[2]*Department of IT, Swank Tek Inc, Nutley, New Jersey, USA.*
[3]*Department of IT, ZT Systems, Secaucus, New Jersey, USA.*
[4]*Department of IT, Malla Reddy University, Hyderabad, Telangana, India.*

[1]*Corresponding Author : kiranmannem14@gmail.com*

Received: 15 May 2025 Revised: 17 June 2025 Accepted: 18 July 2025 Published: 31 July 2025

Abstract *- Efficient mobility management is essential in contemporary wireless communication systems to maintain continuous and reliable connectivity as users move across the network users. In Fifth-Generation (5G) networks, the widespread use of densely packed small cells results in a higher likelihood of handover events, increasing the chances of issues such as the ping-pong effect and radio link failures. These problems are often linked to poorly optimized handover control parameters. To mitigate these challenges, this study proposes HO-LBlock, a secure and lightweight blockchain-assisted framework designed for efficient handover and mobility management in 5G heterogeneous network environments. The proposed approach is structured around four key phases: network formation, secure authentication, hierarchical clustering, and a hybrid handover mechanism, all designed to enhance both security and efficiency in dynamic 5G environments. A grid-based network is initially constructed to enhance data transmission rates and strengthen connectivity between devices. After that, to amplify security, authentication is performed based on the Colour Code Combination (CCC) method, and the secret key is provided by a lightweight blockchain using the Elliptic Curve SIGNcryption algorithm (ECSIGN). Following this, hierarchical clustering is performed by integrating the Dunn Index and the Improved k-medoids (DUNNI) method to minimize energy consumption by selecting the Cluster Head (CH) and Substitute Cluster Head (SUB CH). Finally, a two-condition-based handover is executed by optimizing the HCPs using a data-driven optimization approach with the Combined Coral Reef Optimization and Improved Q-learning (CCROIQ) algorithm. In this work, a lightweight blockchain is employed to ensure data privacy and security during information transactions. The performance of the proposed framework is evaluated through simulations conducted in Network Simulator 3.26 (NS-3.26), and the results demonstrate its superiority over existing approaches across several critical performance indicators.*

Keywords *- Authentication, Clustering, Blockchain, Handover, Heterogeneous network, Mobility management.*

1. Introduction

With the rapid advancement of wireless communication, an increasing number of mobile devices are now able to connect within 5G networks. This next-generation technology supports a high density of heterogeneous devices, enabling significantly greater capacity [1, 2]. 5G brings a range of transformative capabilities to modern systems, including ultra-low latency, reduced energy consumption, enhanced system capacity, and large-scale device connectivity. In 5G wireless HetNets, mobility management has become extremely difficult. User equipment handovers from one service coverage area to another must be handled effectively, and in an ultra-dense 5G network, network construction management is also crucial for mobility management. [3-5]. In 5G networks, the distance between User Equipment (UE) and base stations is reduced due to the ultra-dense deployment of small cells. These smaller base stations are positioned within the coverage area of a macro base station, leading to more frequent handovers. In some previous studies, users and base stations were randomly deployed in the environment, resulting in handover delays and inefficient handovers [6, 7]. Further, the handover process should consider parameters such as RSRP and RSSI, which result in an inaccurate handover decision. Moreover, ensuring security during handover is crucial to protecting the network from various malicious attacks. To address this, several security mechanisms are incorporated [8].

In addition, the handover authentication process is necessary for verifying the identity of User Equipment (UE) within the network; however, inefficient authentication can lead to significant delays and increased handover latency. In

such cases, most existing works have not focused on enhancing security while reducing handover delay [9, 10]. In several studies, security during handover is maintained; however, insufficient consideration of handover control parameters often leads to Unnecessary Handovers (UHO), Too-Late Handovers (TLHO), Too-Early Handovers (TEHO), Ping-Pong Handovers (PPHO), and Handover Failures (HOF) [11].

Furthermore, transactions are securely stored in the blockchain; however, most existing studies have used traditional blockchain methods, resulting in time-consuming processes and high complexity [12, 13]. Additionally, mobility management has often been performed by considering only a few parameters and handover control parameters, leading to inaccurate handovers and a lack of security in several studies. This issue is a primary focus in this work [14, 15]. The proposed work addresses these existing challenges by introducing an enhanced network design along with advanced algorithms and techniques.

2. Literature Survey

This section presents a review of the literature on mobility management in 5G HetNets using blockchain technology. It also highlights and analyses the research gaps in achieving effective mobility management within 5G HetNets. In [16], the researchers proposed a lightweight authentication mechanism specifically designed for next-generation IoT systems. Their approach involved storing the sensor-generated data on a cloud server while enabling mutual authentication between the user device and the access point. A session key was subsequently created and securely transmitted to the user. The scheme also employed a smart card-based method for remote user authentication, allowing passwords to be generated and securely shared via the server. This framework was intended to enhance the overall security and efficiency of user authentication within emerging IoT environments. However, the work had a limitation: although passwords were used for authentication, they were not strong enough, making it easier for hackers to guess or compromise them. In [17], a mobility management strategy was presented that integrates blockchain with reinforcement learning. The approach addresses both wireless handover and service migration by formulating them as a multi-objective dynamic optimization problem, which is tackled using Lyapunov optimization. The authors employed a deep reinforcement learning method based on the Actor-Critic architecture to solve this. Simulation outcomes demonstrated that the proposed model effectively lowers the average computing workload and decreases handover failures. Furthermore, the study also introduced an enhanced mobile authentication protocol tailored for GLOMONET environments. However, a limitation of this work is that handover decisions were made by considering only a limited set of handover parameters, which led to inaccurate handover decisions and a High Handover Failure (HOF) ratio. This research [18] proposed a secure mobile authentication scheme that incorporates a three-factor authentication method for user login and authentication. The first factor secures a large amount of information using a smart card; the second factor involves secure password creation; and the third factor ensures the security of the session key. To validate the security of the scheme, both ProVerif and BAN logic analyses were performed. The findings indicate that the proposed approach achieves an average of 93% secure login and user authentication. However, one noted drawback is the random placement of devices without any structured grouping. This lack of organization contributes to increased communication delays, higher energy usage, and a shorter overall network lifespan.

The study presented in [19] assessed mobility performance using Mobility Robustness Optimization (MRO), which was developed to improve handover reliability as users move between network cells. Key parameters such as SINR, Handover Ping-Pong Probability (HPPP), and Radio Link Failure (RLF) were utilized to guide handover decisions. The findings indicate that MRO enables more precise handover management. Nonetheless, the research falls short in addressing efficient organization of users and base stations, resulting in elevated computational load, frequent handovers, and increased energy consumption. In [20], the authors proposed an adaptation of handover control parameters based on Mobility Robustness Optimization (MRO). This work adaptively sets handover control parameters using MRO to reduce PPHO, RLF, TEHO, TLHO, and UHO. MRO calculates the threshold ratio and identifies whether it results in PPHO or RLF, then adjusts the threshold between the hysteresis margin and time-to-trigger for accurate handover decisions. This reduces RLF, PPHO, TLHO, and TEHO.

However, a limitation of this work is that while handover decisions were made based on HO parameters, the handover control parameters were not optimized, leading to a higher handover failure ratio. In this paper [21], DDR-LEACH-based cluster head selection was introduced. The DDR-LEACH protocol enhances cluster head selection by assigning the role to regular nodes based on factors such as highest remaining energy, node degree, and proximity to the Base Station (BS). To handle large-scale data storage, the approach integrates an Interplanetary File System (IPFS) with a Proof of Authority (PoA) consensus mechanism. Simulation outcomes demonstrate that DDR-LEACH offers improved energy efficiency, increased throughput, and extended network lifetime due to its optimized cluster head selection strategy. However, a limitation of this work is that it uses a traditional blockchain structure, which is linear in nature and requires recoding of all blocks, resulting in time consumption, high complexity, and negatively impacting QoS in mobility management. In this paper [22], the authors

introduced an authentication process based on clustering. A cluster-based authentication mechanism was proposed for users, edge servers, and servers. Furthermore, trust evaluation was performed under two categories: data level and application level, and clusters were constructed based on numbers generated by the server. The simulation results show that the proposed approach has the potential for real-time application deployment. However, a limitation of this work is that although cluster-based authentication was performed, the authentication information was stored in a centralized manner, which is not secure and can lead to various attacks such as eavesdropping, redirection, and spoofing. In [23], a novel technique was presented to enhance Quality of Service (QoS) in 5G Heterogeneous Networks (HetNets) using a Q-learning-based approach. This method facilitates information exchange between the serving base station and neighboring stations, applying a joint reward function to support self-optimization. The proposed algorithm also incorporates Q-learning for efficient radio resource management, aiming to boost the performance of both macro and small cell user devices. Simulation results indicate that this approach delivers a 48% improvement in small-cell users' capacity compared to traditional independent learning strategies.

However, a limitation of this work is that information was exchanged with neighboring base stations without incorporating security measures, which could lead to information leakage and negatively impact QoS. In [24], the authors introduced a novel prediction-based agent to enhance mobility management in 5G networks. The proposed method leverages Admission Control (AC) policies that use predictive insights to optimize performance across both single-service and multi-service environments. The primary objective is to enable accurate mobility prediction based on available user data. However, one of the key limitations is that user information is transmitted to neighboring base stations via public channels, which may expose sensitive data to potential attacks and raise privacy concerns. The study in [25] explores mobility management in 5G networks using a network slicing approach. By integrating existing network infrastructures, the system enhances both capacity and coverage while promoting flexibility and service-centric operations. This approach makes the network more responsive to diverse user demands and application-specific requirements. Moreover, network slicing enables better customization and dynamic resource allocation, supporting the design of adaptive and highly available network environments in 5G. The current work uses fuzzy logic to address mobility and traffic management challenges by optimizing network resources. However, a limitation of this work is that while Handover (HO) is performed, secure handover is not implemented. Furthermore, the accuracy of mobility management is compromised due to the ineffective consideration of HO parameters, which also impacts QoS. The work in [26] presents data-driven machine learning approaches designed to address challenges in wireless LAN environments effectively. The proposed framework is structured into four key components: feature extraction, dataset modules, and machine learning modules. Initially, raw network data is collected and processed to derive meaningful attributes. During the feature extraction phase, relevant features are mapped to specific clients, and the count of associated clients is determined by analyzing the time intervals between the arrivals of consecutive data packets. Authentication is performed, but since a strong password is not used, hackers can easily identify the password, leading to several attacks such as spoofing, redirection, and eavesdropping.

The study presented in [27] explores mobility management in 5G networks by analyzing the impact of frequent handovers on throughput variability. The approach leverages multi-carrier radio signal quality indicators, such as Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ), and Signal-to-Interference-and-Noise Ratio (SINR), to evaluate signal strength from nearby cellular towers within a defined geographic area. This supports the essential control plane functions necessary for maintaining stable cellular connectivity. However, one limitation of this method is the random deployment of network entities without proper grouping, which leads to increased communication delays, elevated energy consumption, and a shortened overall network lifetime.

3. Problem Statement

Ensuring secure mobility management and efficient handover remains a critical challenge in Fifth-Generation (5G) Heterogeneous Networks (HetNets). Although various solutions have been proposed in recent literature, several limitations persist. The key shortcomings observed in existing approaches are summarized below:

In [28], known in this study as RL-HO, the authors introduced a mobility management framework that utilizes reinforcement learning to support handover decisions in ultra-dense 5G heterogeneous networks. The method relies on the State-Action-Reward-State-Action (SARSA) algorithm, which incorporates function approximation techniques to manage complex and expansive state-action spaces efficiently. This enables the model to make optimal handover decisions in dynamic environments. RL-HO serves as a baseline for evaluating the efficiency of our proposed mobility scheme.

- However, SARSA requires frequent visits to each state-action pair, resulting in extensive data needs and computational overhead.
- Although handovers are performed, secure handover mechanisms are absent, affecting mobility accuracy and Quality of Service (QoS).

- The framework lacks efficient user and base station management, leading to load imbalance, frequent handovers, and higher energy consumption.

In [29], commonly referenced in this study as 5GBA, the authors proposed a blockchain-based authentication mechanism tailored for 5G networks. The approach addresses single-point-of-failure vulnerabilities and enhances resistance to Distributed Denial-of-Service (DDoS) attacks by leveraging a one-time secret hash function for device authentication. To preserve user privacy, the scheme employs Subscription Concealed Identifier (SUCI), while the use of Elliptic Curve Diffie-Hellman (ECDH) ensures secure key exchange and mitigates linkability threats.

- However, ECDH-based key derivation introduces significant latency, leading to handover delays.
- Although the Database (DB) is distributed, data alteration by advanced attackers remains possible, risking data integrity and overload.

The scheme does not employ strong password mechanisms, making it vulnerable to spoofing, redirection, and eavesdropping attacks.

4. Proposed Work

To overcome the above limitations, the following solutions are proposed: A grid-based network structure is introduced to enhance scalability and reduce HetNet complexity. Authentication is strengthened using Color Code Combination (CCC) during registration, with ECSIGN-based key distribution to guard against impersonation. Hierarchical clustering of users is achieved using the DUNNI method to ensure balanced load distribution. A condition-based handover strategy is executed at the edge server, guided by optimized Handover Control Parameters (HCP). The CCROIQ algorithm, a data-driven optimization method, is employed to tune the HCP for reduced decision time and improved accuracy. Finally, a lightweight blockchain framework is integrated to assist in the selection of capable and secure nodes for reliable handovers.

4.1. System Model

In this work, grid-based network management is employed, where small base stations are connected to the edge server, reducing energy consumption and network traffic. The edge server is then linked to the macro base station, which, in turn, is connected to a lightweight blockchain (using hierarchical proof of capacity combined with asynchronous proof of work), where user registration, authentication, and handover decisions are stored. Figure 1 illustrates the architecture of the proposed HO-LBlock framework. The system's main components include IoT devices (user equipment), base stations, edge servers, and a lightweight blockchain layer that collectively support secure and efficient mobility management.

IoT devices: IoT devices refer to the users who leverage 5G communication to transfer information between devices, objects, and people. In this context, the user's location and communication are tracked to facilitate the handover process. Base Station: The base station serves as a vital intermediary between the user equipment and the server, enabling real-time communication and facilitating secure authentication. It also supports long-distance data transmission with minimal power consumption, thereby enhancing network efficiency.

4.1.1. Edge Server

It serves as the network's entry point, improving privacy protection and ensuring data security. The edge server handles clustering and secure handover, offering faster handovers while reducing energy consumption.

4.1.2. Blockchain

The blockchain, integrated with a lightweight system, uses a hierarchical network to reduce computational load and securely stores transactions.

4.2. Network Construction

This work uses a grid-based network setup, where the 5G HetNet is divided into $m \times m$ grids to improve scalability and reduce complexity. Each grid contains several IoT devices and access points, enhancing data transfer and device connectivity. Every grid cell is equally sized and identified by a unique Grid Identifier (GID), based on its transmission range. Nodes communicate only with neighboring grids in this structured layout. The grid size (H) is calculated using node positions and transmission range (U), using the formula: $\left(H = \frac{U}{\sqrt[2]{2}}\right)$.

If a node is deployed within the network, its unique Grid Identifier (GID) can be calculated using the following expression:

$$GID(q,p) = \left\{(q,p)|q = \left[\frac{A-A_0}{H}\right], G = \left[\frac{G-G_0}{H}\right]\right. \quad (1)$$

Where (A_0, G_0) represents the origin at (0,0), $A_0 \leq A$, $G_0 \leq G$ and H is the Grid size. This formulation helps define the position of a node within a specific grid. Using this, the link connectivity between a mobile node and its neighboring nodes is established. Even if a node is located at the corner of a grid, it can still communicate with its immediate neighbors.

4.3. Secure Authentication

Following network construction, the next step focuses on ensuring secure user authentication. This process consists of two main phases: registration and login. In the registration phase, a 5G network user (U) registers with a set of unique metrics, including their ID, MAC address, and Physically Unclonable Function (PUF), collectively denoted as $\oint$. Additional details such as the user's email address, password, and a security question, collectively denoted as λ, are

registered at the Base Station (B). All entity registrations are transmitted over a secure channel to prevent communication-based attacks. For password creation, a Colour-Code Combination (CCC) method is used. The user selects six different colours from the set {R, O, G, Y, B, V} and assigns a unique rating between 1 and 9 to each colour, as outlined in Table 1. These selected colours and their ratings are then securely stored in the lightweight blockchain. Figure 2 presents the detailed sequence of steps involved in the registration and login/authentication processes within the proposed framework.

- Step 1: Initially, the $\oint$ and λ are registered to the $\mathcal{B}$, which can be composed,

$$B \leftarrow Reg\{(\oint), (\lambda)\} \quad (2)$$

Where, $Reg\{(\oint), (\lambda)\}$ denotes the registration of parameters $(\oint)\ and\ (\lambda)$ respectively.

- Step 2: The password is generated using the CCC method by selecting different colours, Red (R), Orange (O), Green (G), Yellow (Y), Blue (B), and Violet (V) and assigning each a rating from 1 to 9, as shown in Table 1.
- Step 3: After that, the secret key $(\psi\xi)$ is provided using the ECSIGN approach by using $Reg\{(\oint), (\lambda)\}$

Table 1. Individual color rating

User	Colors	Rating
(U_1)	VYOBGR	865473
(U_2)	YRBOGV	985642
(U_3)	GROBVY	845637

$$B \rightarrow \text{secret key } (\psi\xi) \quad (3)$$

Once registered, the ECSIGN approach is used to generate a secret key $(\boldsymbol{\psi\xi})$, offering faster and stronger key generation compared to conventional cryptographic methods. The secret key is then securely shared with the user and stored in the lightweight blockchain. During login, the user must input their email and correctly rate the displayed colours on a 6×6 grid to authenticate. If the user forgets the password, a verification email and a security question allow limited attempts to recover access. This method offers enhanced resistance against impersonation and redirection attacks, supported by security.

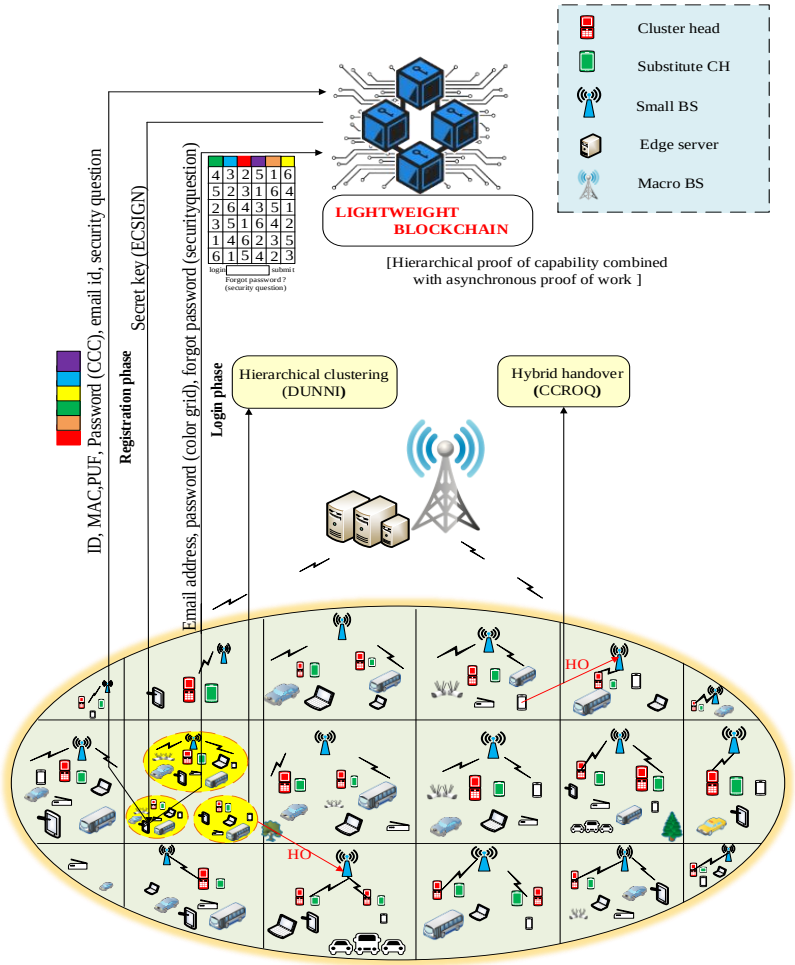

Fig. 1 Architecture of 5G mobility management

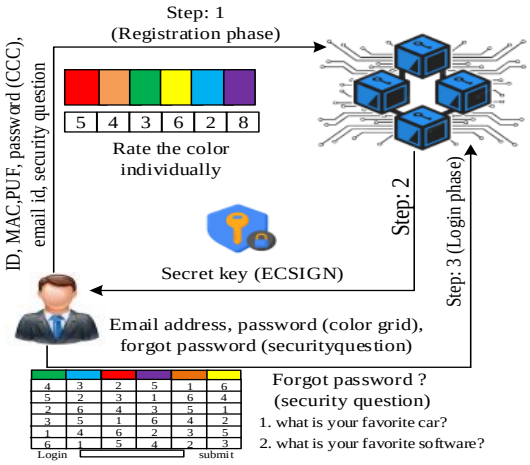

Fig. 2 Secure authentication using CCC

Properties of the lightweight blockchain. ECSIGN ensures quick and strong key generation for each session.

4.4. Hierarchical Clustering

Clustering To enhance load balancing and handover performance, users are grouped using a hierarchical clustering method called DUNNI, which combines the Dunn Index with an improved k-medoids algorithm.

Clustering is based on user location and distance, and the optimal Cluster Head (CH) is selected based on proximity to the cluster centroid, available energy, Number of users, and inter-user distance. To prevent overload on CHs, Sub-Cluster Heads (Sub-CHs) are introduced when needed, reducing handover failures and ensuring balanced network performance.

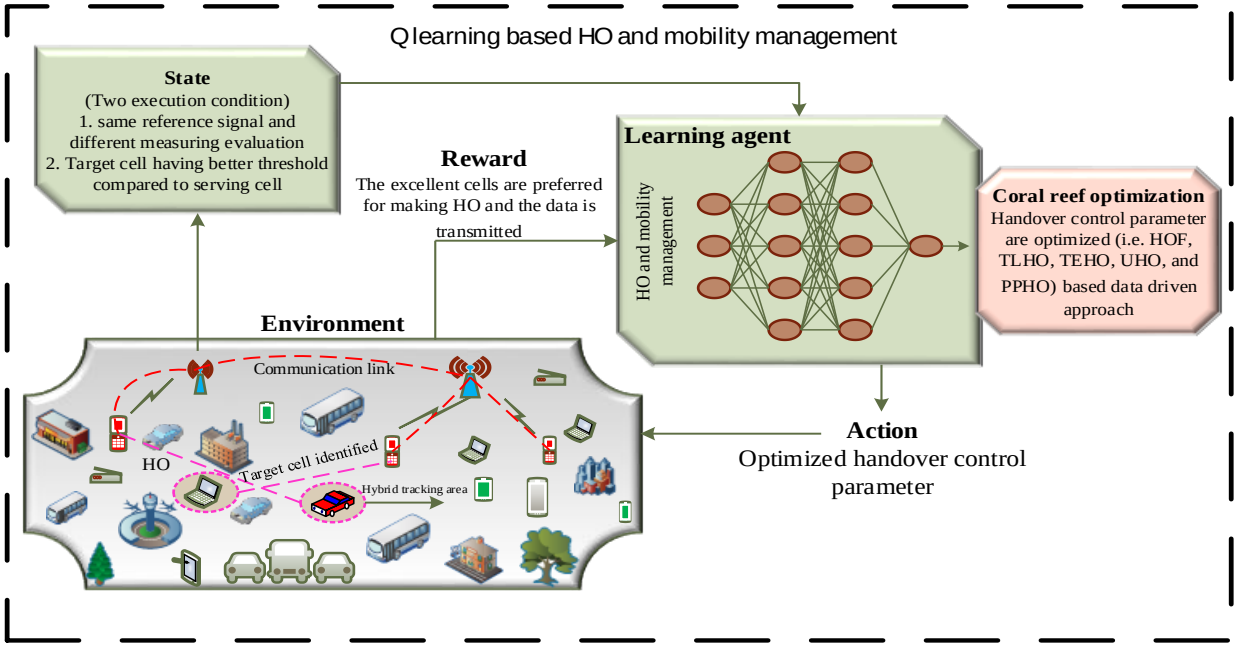

Fig. 3 Handover and mobility management

The dissimilarity between users is computed as:

$$f_{ij} = \frac{w+t}{x+w+t+z} \tag{4}$$

This forms a dissimilarity matrix F:

$$F = \begin{pmatrix} f_{11} & \cdots & f_{1N} \\ \vdots & \ddots & \vdots \\ f_{NN} & \cdots & f_{NN} \end{pmatrix} \tag{5}$$

This matrix is used as the distance metric for hierarchical k-medoids clustering. The Dunn Index is calculated to assess clustering quality:

$$EK = min\left\{\frac{\min dist(y_i,y_j)}{\max dist(L_g)},\ y_i \in E_i, y_j \in E_j, E_l \in E\right\} \tag{6}$$

Where y_i and y_j Are decision elements in clusters E_i and E_j Respectively. The Dunn index based on dissimilarity matrix F:

$$FK\left(Tree_i, Tree_j\right) = min\left\{\frac{\min f_{ij}}{\max f_{max}}\right\} \tag{7}$$

The algorithm continues refining clusters until a stopping criterion is met (e.g., a fixed number of clusters or stability in cluster centres). The best decision tree in each cluster is used to compute the integrated Dunn Index. The k-medoids algorithm minimizes the objective function:

$$O_n = \sum_{i=1}^{A} \sum_{y \epsilon v_i} f\left(y, t(i)\right)^2 \tag{8}$$

Where $f\left(y, t(i)\right)$ represents the distance from point y to

its cluster center $t(i)$ And A is the Number of clusters. The distance function is:

$$f_l(X,W) = \sum_{i=1}^{M} |X_i - W_i| \quad (9)$$

Where X is a user data point, W is the cluster center, and M is the Number of numerical attributes.

Based on the dissimilarity matrix (5), the algorithm hierarchically clusters users using the Dunn index-based evaluation. It iteratively assigns users to clusters by minimizing the objective function (8) and updates cluster centers using the k-medoids method (9) until convergence or a maximum number of iterations is reached. The final cluster centers are selected based on the best Dunn index score, ensuring optimal separation and compactness.

4.5. Hybrid Handover

After clustering is completed, the handover decision is managed by the edge server using a Conditional-Based Handover (CHO) approach. This method includes two execution conditions: (1) the same Reference Signal (RS) with different measurement evaluations, such as RSRP, RSRQ, SINR, and SNR, and (2) the target cell is selected only if its signal quality exceeds a defined threshold relative to the serving cell. Based on these conditions, key Handover Control Parameters (HCPs), such as Handover Margin (HOM) and Time-To-Trigger (TTT), are utilized to guide the decision-making process. The HCPs are then optimized using a data-driven approach via the CCROIQ algorithm. This optimization enables faster and more efficient handover decisions, while minimizing Key Performance Indicators (KPIs) such as Handover Failure (HOF), Too Late Handover (TLHO), Too Early Handover (TEHO), Unnecessary Handover (UHO), and Ping-Pong Handover (PPHO), thereby improving load balancing. The target cell is identified using a hybrid tracking area method, which includes location updates and paging. Additional metrics such as user direction, speed, location, and cell load are also considered to ensure accurate and efficient handover. To secure data during the handover process, the ECSIGN encryption method is used. This ensures that communication remains protected against attacks such as spoofing, eavesdropping, Man-In-The-Middle (MITM), and data poisoning. The working principle of Q-learning in handover and mobility management is illustrated in Figure 3.

The proper selection of Handover Margin (HOM) and Time-To-Trigger (TTT) values is crucial for seamless connectivity. Large HOM and TTT values result in stable behaviour but can delay Handover (HO) decisions, leading to poor responsiveness. Conversely, small values may reduce delay but can cause ping-pong and unnecessary HOs.

The HO optimization problem is formulated as:

$$U_{T,opt} = arg_{U_T} minW \quad (10)$$

Where W represents the Key Performance Indicator (KPI) dependent on the feature vector U= $[U_T, U_N]$. These KPIs reflect typical mobility-related handover problems that must be minimized for optimal performance. The Handover Control Parameters (HCPs) are optimized using the CCROIQ algorithm to improve decision-making efficiency and minimize latency. This optimization considers the long-term benefits of using Q-learning, a Reinforcement Learning (RL) model that ensures stable and high-utility HO decisions. If W=$\{l_1, l_{2,\ldots,} l_n\}$ is the set tasks and F=$\{f_{j,z} | 1 \le j \le N, 1 \le z \le M\}$ is the decision matrix in a 2D space, the utilization of the resource $f_{j,z}$ The task assignment is calculated as:

$$Y_{j,z} = \sum_{task\ l_i \epsilon f_{j,z}} Y_{j,z}^{i} = \frac{\sum_{mn \epsilon f_{j,z}} mn.mips}{f.mips_{j,z}} \quad (11)$$

In Equation (11), $mn.mips$ is the allocated $mips$ to any task and $f.mips_{j,z}$ Is the total $mips$ of each decision-making for HO? The total utilization is defined as:

$$WY = \sum_{f_{j,z}} Y_{j,z} \quad (12)$$

$$\bar{Y} = \frac{WY}{n} \quad (13)$$

Let $\overline{DBR} = 1 - DR$ represent the decision balancing rate. The final fitness function used for decision selection is:

$$DR = \alpha \times \bar{Y} + \zeta \times \overline{DBR}\ ,\ (\alpha + \zeta = 1) \quad (14)$$

Where α and ζ determine the importance of each objective in the HO optimization process.

Q-learning setup:

- State: Condition-based HO performance.
- Action: Probability of selecting the next HO decision in step N.
- Reward: Hybrid handover decision

The Q-learning model prevents local optimization traps and uses a long-term strategy to maximize average HO performance while reducing unnecessary Hos. The following is the pseudocode for the HO decision.

. Pseudocode for HO decision
Input Clustered user Output Next HO hop decision Begin Initialize solution vectors using Equation (22) Evaluate fitness using Equation (25) For each iteration: Select the best decision vectors R_z Update decision $Y_{j,z}^{i} \rightarrow Y_{j,z}^{i+1}$ End Return optimal decision End

Secure Storage with Lightweight Blockchain: All HO decisions and data transactions are recorded using a

lightweight blockchain. The blockchain implements a Hierarchical Proof-of-Capability (PoC) consensus mechanism integrated with asynchronous Proof-of-Work (PoW). This setup ensures:

- Low-latency and energy-efficient block generation
- Improved node selection and reduced storage overhead
- Enhanced tamper-resistance and security

Blockchain security operations are described as follows:

$$F = RswHash\ (FH, n) \tag{15}$$

$$proof\ =\ Rswproof(FH, n) \tag{16}$$

$$T/F = Rswver(UH, n, proof, f) \tag{17}$$

Here, *Rsw* is used for hash creation and verification, leveraging the node's private key and current timestamp. In the dual-leader PoC model, election hash values are generated, and nodes with higher capability are selected to form secure blocks. This setup ensures protected, authenticated handover decisions across heterogeneous networks.

5. Results

This section provides a detailed performance evaluation of the proposed HO-LBlock framework for efficient mobility management in 5G HetNets. The experimental study is structured into two subsections: simulation setup and comparative analysis. The results clearly indicate that the proposed approach delivers substantial improvements over existing methods across key performance metrics.

Table 2. Simulation setup

Network parameters	Value
Number of users	200
Number of small base stations	10
Number of macro base stations	1
Number of Edge servers	1
Blockchain	1
Simulation area	$\mathbf{1200}\boldsymbol{m} \times \mathbf{1800}\boldsymbol{m}$
Simulation duration	320s
Initial energy	130J
Node mobility	9 m/s
Simulation modules	Wi-Fi, Ipv4, Internet
Transmission range	160m
Number of packets	~1400
Mobility model	Random waypoint
Channel bandwidth	130 MHz
Packet data rate	130 Mbps
Traffic types	TCP/IP, UDP
Number of retransmissions	8
Packet sizes	64,128, 256,512, 1024 bytes

5.1. Simulation Setup

The proposed work was implemented using the NS-3.26 network simulator to evaluate the performance of the HO-L Block framework. Several network parameters were configured, and performance metrics were measured.
Table 2 summarizes the simulation setup used for experimentation.

5.2. Comparative Analysis

This subsection presents a comparative analysis between the proposed HO-L Block framework and two existing approaches: RL-HO and 5GBA. The comparison is based on critical performance metrics including handover execution time, handover delay, failure rate, time-to-trigger (TTT), and average transaction performance. The main objective of this study is to achieve precise and efficient handover decision-making while ensuring security using a lightweight blockchain mechanism. The results indicate that HO-L Block consistently achieves better performance than RL-HO and 5GBA across all evaluated parameters.

5.2.1. Time Analysis

This metric evaluates the time the proposed HO-LBlock framework takes to complete a Handover (HO) decision, particularly under attack conditions. A lower execution time indicates a more efficient system. Figure 4 compares execution time versus accuracy for HO-Lblock, RL-HO, and 5GBA. The proposed method shows significantly reduced decision time, only 3 seconds under second-attack conditions, compared to 5 seconds for RL-HO and 9 seconds for 5GBA. For 10 simulated attacks, HO- Lblock averaged 10 seconds, while.

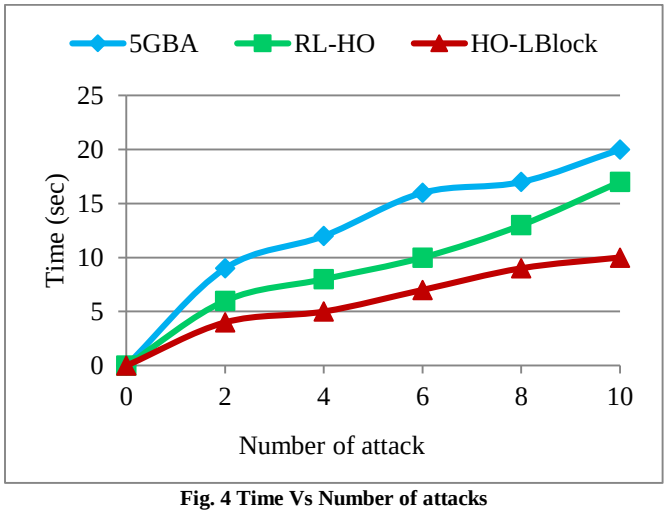

Fig. 4 Time Vs Number of attacks

RL-HO and 5GBA required 18 and 20 seconds, respectively. This improvement is due to our secure authentication via the CCC method and efficient key generation using ECSIGN, which ensures secure and fast data handling. These results demonstrate the superior performance of HO-Lblock in time-critical scenarios.

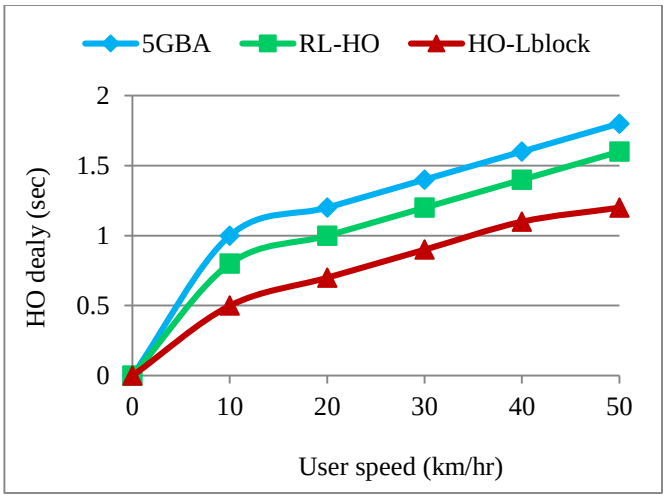

Fig. 5 HO delay Vs user speed

5.2.2. Handover Delay Analysis

This metric measures the total delay experienced by a mobile node during the handover process, including session re-establishment from the source to the destination node. HO delay typically correlates with user speed. Figure 5 shows that the proposed HO-Lblock framework achieves significantly lower HO delay compared to RL-HO and 5GBA. While existing methods rely mainly on data-driven optimization based on user location, our approach combines conditional and data-driven strategies using CCROIQ for optimizing handover control parameters. As a result, HO-Lblock reduces delay to 0.3 seconds at specific user speeds, compared to 0.6 and 0.8 seconds for RL-HO and 5 GBA, respectively. On average, for a user speed of 50, H O-Lblock maintains a delay of 1.

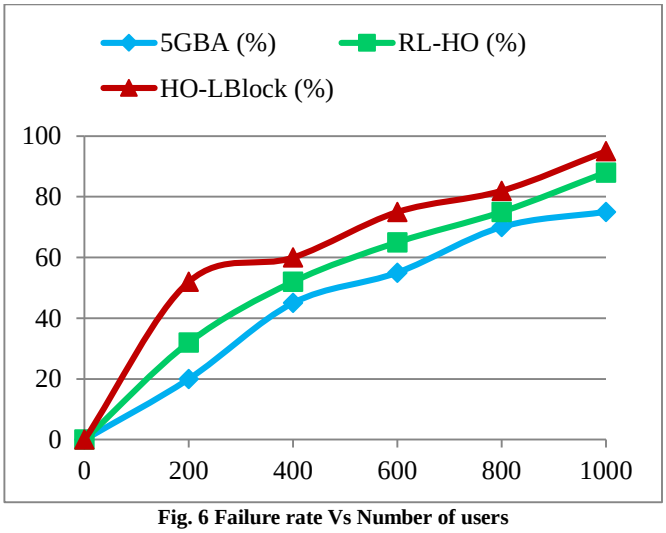

Fig. 6 Failure rate Vs Number of users

Second, outperforming RL-HO (1.5 sec) and 5GBA (1.8 sec). These results clearly show the effectiveness of our approach.

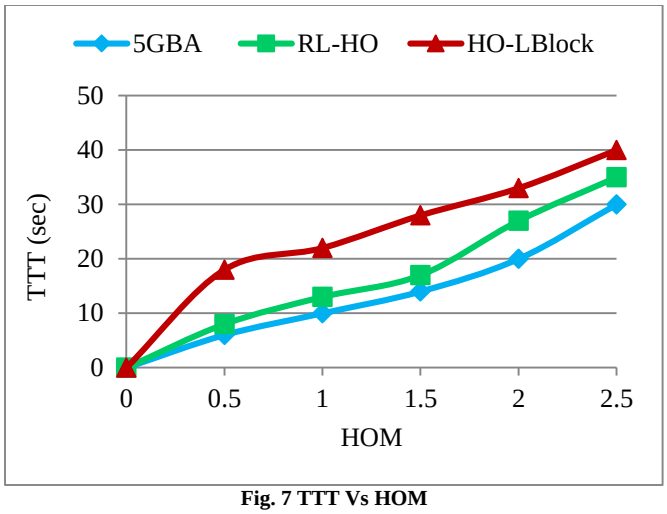

Fig. 7 TTT Vs HOM

5.2.3. Failure Rate Analysis

Failure rate in 5G HetNets refers to the probability that a Handover (HO) fails at a specific time, given that the connection has remained stable until then. It is calculated as:

$$E(t) = \frac{U(t)}{F(t)} = \frac{U(t)}{1-F(t)} \quad (18)$$

Where $U(t)$ represents unsuccessful Hos, and $F(t)$ Represents unsuccessful Hos. Figure 6 compares the failure rate across different user counts. The proposed HO-Lblock framework consistently shows a lower failure rate than RL-HO and 5GBA. While RL-HO relies on semi-gradient SARSA with key HO parameters, our method uses the CCROIQ algorithm to optimize handover control, reduce decision time, and improve load balancing. For 200 users, HO-Lblock reduces the failure rate to 45%, compared to 33% in RL-HO and 20% in 5GBA. Under 100 attacks Scenario, the average failure rate in HO-Lblock is 95%, outperforming RL-HO (85%) and 5GBA (80%). These results confirm the robustness of our proposed approach.

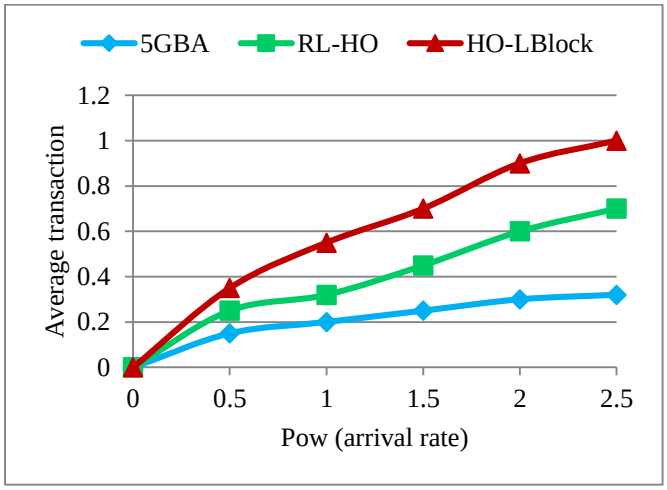

Fig. 8 Average transaction Vs PoW

5.2.4. Time To Trigger Analysis

Time To Trigger refers to the duration during which specific conditions must be satisfied to initiate a handover. It is defined by:

$$\mathrm{RSS_T} - \text{hysteresis} > \text{threshold} \tag{19}$$

When the serving cell's RSS is strong enough, TTT helps reduce radio link failures and the ping-pong effect, ensuring stable connectivity. Figure 7 shows the TTT performance with varying Handover Margin (HOM).

The proposed HO-LBlock method dynamically adjusts TTT based on threshold values tied to KPI metrics, enabling more effective HO decisions. In contrast, RL-HO and 5GBA use static TTT values without such optimization. For a HOM value of 2.5, HO-Lblock achieves a TTT of 40 seconds, outperforming RL-HO (35 sec) and 5GBA (32 sec).

With increasing HOM, our method achieves a TTT of up to 18 seconds, while RL-HO and 5GBA reach only 8 and 5 seconds, respectively. These results highlight the adaptability and efficiency of our approach.

5.2.5. Average Transaction Analysis

This metric evaluates the average value of Handover (HO) transactions in 5G HetNets. It is calculated as:

$$\Delta = \frac{\vartheta}{\zeta} \tag{20}$$

Where ϑ is the total value of all transactions and ζ is the Number of HO transactions. A higher average transaction value reflects better service quality during the handover process.

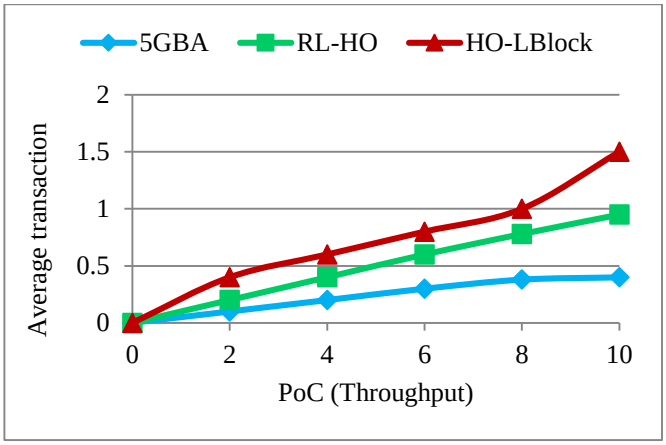

Fig. 9 Average transaction Vs PoC

Figure 8 shows the average transaction performance with respect to PoW (arrival rate). The proposed HO-L Block achieves a higher average transaction (0.26) than RL-HO (0.18) and 5GBA (0.1). At an arrival rate of 2.5, HO-L Block reaches a value of 1, outperforming RL-HO (0.7) and 5GBA (0.3).

This improvement is attributed to the use of CCC-based secure authentication and ECSIGN for secure key generation. Figure 9 compares average transaction values concerning PoC (throughput). HO-LBlock outperforms RL-HO and 5GBA due to its hierarchical clustering approach, which effectively balances traffic and mitigates load at congested cluster heads.

At 10 units of throughput, the proposed method achieves a transaction value of 1.5, while RL-HO and 5GBA reach only 1 and 0.5, respectively. These results confirm that HO-LBlock delivers improved transaction efficiency under both arrival rate and throughput conditions.

6. Conclusion

This paper addresses key challenges in 5G mobility management, particularly inaccurate Handover (HO) decisions and a lack of security. To address these issues, a secure and hybrid Handover (HO) framework is introduced. The method starts with grid-based network construction to effectively manage high traffic loads. Secure user authentication is achieved using a CCC-based password mechanism, with secret keys generated via the ECSIGN algorithm.

All registration and login processes are handled through a lightweight blockchain. Hierarchical clustering is carried out using the DUNNI algorithm to elect efficient CH and SUB-CH nodes, reducing processing overhead. For accurate and timely HO decisions, a hybrid method combining condition-based and data-driven strategies is employed.

The Handover Control Parameters (HCPs) are optimized using the CCROIQ algorithm, and all communications are securely recorded on the blockchain. The framework is evaluated using NS-3.26, and its performance is compared against existing approaches (RL-HO and 5GBA) across key metrics, including execution time, HO delay, failure rate, TTT, and average transaction.

The results confirm that our HO-LBlock framework significantly outperforms previous methods, offering a secure, efficient, and scalable solution for mobility management in 5G heterogeneous networks.

Acknowledgement

The authors acknowledge the use of OpenAI's ChatGPT to assist with language refinement and provide suggestions during the manuscript preparation process. All final decisions and responsibility for the content of this article rest solely with the authors.

References

[1] Jawad Tanveer et al., "An Overview of Reinforcement Learning Algorithms for Handover Management in 5G Ultra-Dense Small Cell Networks," *Applied Sciences*, vol. 12, no. 1, pp. 1-25, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Maraj Uddin Ahmed Siddiqui et al., "Mobility Management Issues and Solutions in 5G-and-Beyond Networks: A Comprehensive Review," *Electronics*, vol. 11, no. 9, pp. 1-27, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Kotaru Kiran, and D. Rajeswara Rao, "Analytical Review and Study on Various Vertical Handover Management Technologies in 5G Heterogeneous Network," *Infocommunications Journal*, vol. 14, no. 2, pp. 28-38. 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sajjad Ahmad Khan et al., "Handover Management over Dual Connectivity in 5G Technology with Future Ultra-Dense Mobile Heterogeneous Networks: A Review," *Engineering Science and Technology, an International Journal*, vol. 35, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Abdelfatteh Haidine et al., *Artificial Intelligence and Machine Learning in 5G and beyond: A Survey and Perspectives*, Moving Broadband Mobile Communications Forward - Intelligent Technologies for 5G and Beyond, IntechOpen, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Muhammad Mohtasim Sajjad et al., "Inter-Slice Mobility Management in 5G: Motivations, Standard Principles, Challenges, and Research Directions," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 93-100, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Vuyo S. Pana, Oluwaseyi P. Babalola, and Vipin Balyan "5G Radio Access Networks: A Survey," *Array*, vol. 14, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Kang Tan et al., "Machine Learning in Vehicular Networking: An Overview," *Digital Communications and Networks*, vol. 8, no. 1, pp. 18-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Gaofeng Hong et al., "Decentralized Vehicular Mobility Management Study for 5G Identifier/Locator Split Networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Nirmin Monir et al., "Seamless Handover Scheme for MEC/SDN-Based Vehicular Networks," *Journal of Sensor and Actuator Networks*, vol. 11, no. 1, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Emre Gures et al., "Machine Learning-Based Load Balancing Algorithms in Future Heterogeneous Networks: A Survey," *IEEE Access*, vol. 10, pp. 37689-37717, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Syed Hussain Ali Kazmi et al., "Routing-Based Interference Mitigation in SDN Enabled Beyond 5G Communication Networks: A Comprehensive Survey," *IEEE Access*, vol. 11, pp. 4023-4041, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] W.T. Alshaibani et al., "Mobility Management of Unmanned Aerial Vehicles in Ultra–Dense Heterogeneous Networks," *Sensors*, vol. 22, no. 16, pp. 1-32, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ibraheem Shayea et al., "Handover Management for Drones in Future Mobile Networks—A Survey," *Sensors*, vol. 22, no. 17, pp. 1-36, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Tidiane Sylla et al., "Multi-Connectivity for 5G Networks and Beyond: A Survey," *Sensors*, vol. 22, no. 19, pp. 1-32, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ashok Kumar Das et al., "On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure," *IEEE Access*, vol. 9, pp. 71856-71867, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Haibin Zhang et al., "Mobility Management for Blockchain-Based Ultra-Dense Edge Computing: A Deep Reinforcement Learning Approach," *IEEE Transactions on Wireless Communications*, vol. 20, no. 11, pp. 7346-7359, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jihyeon Ryu et al., "SMASG: Secure Mobile Authentication Scheme for Global Mobility Network," *IEEE Access*, vol. 10, pp. 26907-26919, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Wasan Kadhim Saad et al., "Performance Evaluation of Mobility Robustness Optimization (MRO) in 5G Network With Various Mobility Speed Scenarios," *IEEE Access*, vol. 10, pp. 60955-60971, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Tarek Al Achhab, Fariz Abboud, and Abdulkarim Assalem, "A Robust Self-Optimization Algorithm Based on Idiosyncratic Adaptation of Handover Parameters for Mobility Management in LTE-A Heterogeneous Networks," *IEEE Access*, vol. 9, pp. 154237-154264, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Sana Amjad et al., "Blockchain Based Authentication and Cluster Head Selection Using DDR-LEACH in Internet of Sensor Things," *Sensors*, vol. 22, no. 5, pp. 1-20 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Md. Rafiqul Islam et al., "Cluster-Based Authentication Process in a Smart City," *Security and Communication Networks*, vol. 2022, no. 1, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Muhammad Usman Iqbal et al., "Improving the QoS in 5G HetNets Through Cooperative Q-Learning," *IEEE Access*, vol. 10, pp. 19654-19676, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Vicent Pla et al., *Optimal Admission Control Using Handover Prediction in Mobile Cellular Networks*, 1st ed., Mobility Management and Quality-Of-Service for Heterogeneous Networks, River Publishers, pp. 1-22, 2009. [Google Scholar] [Publisher Link]

[25] Randeep Singh et al., "Analysis of Network Slicing for Management of 5G Networks Using Machine Learning Techniques," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Muhammad Asif Khan et al., "ML-Based Handover Prediction and AP Selection in Cognitive Wi-Fi Networks," *Journal of Network and Systems Management*, vol. 30, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Ahmad Hassan et al., "Vivisecting Mobility Management in 5G Cellular Networks," *Proceedings of the ACM SIGCOMM 2022 Conference*, Amsterdam Netherlands, pp. 86-100, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] Qianyu Liu et al., "Autonomous Mobility Management for 5G Ultra-Dense HetNets via Reinforcement Learning With Tile Coding Function Approximation," *IEEE Access*, vol. 9, pp. 97942-97952, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] Man Chun Chow, and Maode Ma, "A Secure Blockchain-Based Authentication and Key Agreement Scheme for 3GPP 5G Networks," *Sensors*, vol. 22, no. 12, pp. 1-26, 2022. [CrossRef] [Google Scholar] [Publisher Link]