Wireless Networks (2023) 29:3187–3205
https://doi.org/10.1007/s11276-023-03371-z

ORIGINAL PAPER

Fast user authentication in 5G heterogeneous networks using RLAC-FNN and blockchain technology for handoff delay reduction

Shivanand V. Manjaragi[1,2] · S. V. Saboji[2]

Accepted: 27 April 2023 / Published online: 19 May 2023

Abstract
In the fifth generation (5G), ultra-dense heterogeneous network (UDHN) is considered as a prominent technology to resolve network system problems. It is challenged to provide secure access since the UDHN contains access points (APs), user equipment (UE) which are characterized with the nature of dynamic, temporary as well as autonomy. The coverage of AP is less when compared to that of classical base station and the problem arises with the interaction between APs and UE during the mobility of UE. In order to attain efficient key agreement with fast and subsequent authentication, a new consensus mechanism has been proposed. By integrating the reinforcement learning method with the actor-critic learning based on fuzzy neural network (RLAC-FNN), blockchain-enabled handover authentication is enabled in 5G heterogeneous Networks. In the proposed method, the user can establish a secure and quick connection by excluding re-authentication and handover operators between heterogeneous cells with less delay. In the proposed approach, all the secondary peers have been further divided into several secondary peer groups based on credit value. The credit of all the secondary peers will be assigned based on their probability of successful participation in consensus. The secondary nodes will summarize all their results to return to the local service centre (LSC). Finally, LSC will identify the trusted and malicious peers by confirming the consensus adaptively by integrating the RLAC-FNN. The performance of the proposed method has analyzed by implementing it in Python platform and compared with existing approaches. The simulation outcomes showed that the proposed method could efficiently reduce the authentication frequency, handover delay, consensus delay, etc., than existing approaches.

Keywords Local service centre · Ultra-dense heterogeneous networks · Blockchain-enabled authentication handover · APs group · And actor-critic learning

1 Introduction

The fast development of mobile devices as well as the applications and their processing requirements tend to the advent 5G networks. Compared to 4G networks, the 5G networks are enabled with properties such as high bit rate than 10 Gb/s, improved network coverage and minimum latency. The 5G networks can extend overlay coverage and operate via heterogeneous cells [1]. The 5G users namely internet of things (IoT) devices, mobile nodes, vehicles create the handover procedure activated when moving from one cell to another. It can tend to cause delay in 5G network if the handover process is frequently happened. In the heterogeneous network, the handover management is considered as one of the primary issue. Besides, the handover fulfills ultra-reliable communications requests and very high availability as well as reliability in 5G networks [2].

The handover management compacts with each active link of an user device, which transfers the linkage between user device as well as the counterpart from a single network point to other network point. Therefore, the handover decision can define the finest acces network as well as

✉ Shivanand V. Manjaragi
shiva.vm@gmail.com

S. V. Saboji
saboji_skumar@yahoo.com

[1] Department of Computer Science and Engineering, Hirasugar Institute of Technology, Nidasoshi, Belagavi, India

[2] Department of Computer Science and Engineering, Basaveshwar Engineering College, Bagalkot, India

decide whether the process of handover has carried out. The authentication process becomes more intricated and can improve delay time, by denying the 5G intentions. Among 5G heterogeneous cells, handover process can tend to provide low performance through ineffective authentication process [3]. In 5G networks, cell resource and power restrictions among the APs need minimum complexity and high effective handover authentication events among homogeneous and heterogeneous cells [4]. The 5G network provides benefit in communication, while considering the technical aspects, privacy protection, authentication behaviour and the existence of heterogeneous cells [5].

5G requires a standard level of security in the network structure and application scenarios, particularly in authenticating the services and offering their access level for 4G. An effective approach is needed to develop 5G networks to confirm and protect privacy in faster, safer and efficient manner [6]. The security requirement is higher in 5G than other networks in which solutions are offered with intellectual control across heterogeneous cells for dependable contrivances. In current decades, the new technology of blockchain received great attention to develop the next generation of wireless networks [7]. The consensus algorithm is a core portion of the blockchain which is considered as a significant element. It has termed as fundamental to confirm the effective collaboration of blockchain network. The main problem of the blockchain is how each node is created to preserve their data consistent via interaction rules. A consensus algorithm is developed to solve this problem to accomplish correctness and consistency of ledger data on various nodes [8, 9]. It needs learning from prior approaches for accomplishing state consensus in a distributed structure. Developing the approach for choosing accounting nodes in a network, as well as how to guarantee that the ledger data creates a proper consensus in the whole network [10].

Different kinds of consensus algorithms like Proof of Elapsed Time (PoET), Casper, Proof of Stack (PoS), delegated Proof of Stale (dPoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Work (PoW) are introduced based on the development of several applications. The commonly used algorithms are Consortium blockchain as well as Public blockchain. These approaches have various benefits, drawbacks, and application in UDHN network scenarios [11, 12]. The POW approach has consumed more energy and is easily affected by the force of higher consensus cycle [13]. Howeever, for a communication system along with time delay, POW is not valuable. Enhancing the density of APs in unit zone and creating a Ultra Dense Network (UDN) is a significant means to solve the challenge of improving the traffic of network by 1000 times and enhancing the speed of user experience for 10–100 times.

UDN is the most efficient network to handle the fast development of higher traffic in 5G network, particularly in the hotspot region. It has projected that the distribution density of the small APs will reach more based on the different Radio Access Technology (RAT). The huge APs can serve for high density UE, and each AP creates a Peer-to-Peer (P2P) uncentered network [14, 15]. The AP has small coverage and low power in UDN. The user can often change between APs and decrease access stability and speed for highly moving mobile users. The APs are no longer in 5G, but it consumes more business collaboration with UE. It can offer data services as well as control according to the variations of practical needs. AP is the crucial portion of the UE accessing the mobile internet. The enumerated data verifying users by AP can face a security problem that can disturb the privacy of user transaction data. Hence, providing secure access as well as effective authentication in UDN networks is termed as a new challenge for the upcoming 5G network structure and security framework.

1.1 Motivation

In 5G network, the ultra-dense small cell networks have employed to offer data rates, security as well as reliability concerns are introduced by low latency in the network. Due to the availability of various malicious attacks, security problems may occur and also the frequent handover tends to become a reliability issue. Hence, offering a secure and reliable connection is significant however, at the same time it is challenging for 5G networks. The blockchain is considered as a most encouraging technology that emcompass the prospective to transform the way in which services are provided to 5G communication network. Besides, to permit end-to-end services delivery over the whole 5G network, blockchain has the ability tocobine the authentication process with 5G network. Nowadays, the main challenge for the recent 5G platform is the necessity to assure an transparent, open as well as a fair system in the unexpected number of resources and various malicious users. With its distinctive decentralization feature, high level of security, data privacy, immutability and transparency, blockchain has turn out to be an evident choice. Hence, blockchain is needed to combine into a 5G network. However, the main problem of the blockchain is how each node is created to keep its data consistent via a rule. To solve this problem, a consensus mechanism has been presented for enabling correctness and consistency of the ledger data on various nodes.

1.2 Contribution

- The new authentication approach is developed with the utilization of blockchain-enabled consensus mechanism and RLAC-FNN to avoid re-authentication during

repeated handover of heterogeneous cells. It resolves the technical challenges related to user privacy protection, authentication and resource management in 5G UDHN.

- The proposed approach was modelled to assure low delay in which the users are replaced with least delay among heterogeneous cell. It can be accomplished with the use of private and public keys provided by block chain to ensure privacy and to enhance user authentication with minimal handoff delay in 5G networks. Quick and secure connection during handoff operations among heterogeneouscell is obtained with low delay.
- Using the block chain propagation model, the authentication outcomes of UE have transmitted in the Access Point Group (APG) through directional trust transfer. Thereby, the members of APG will share the authentication outcomes of UE, minimize the frequency of authentication while the UE moves between APs, and enhance the user experience and access efficiency.
- The APs has been organized into a secured, trusted chain as APG, so the reliability and security of APG have been enhanced. By using proposed RLAC-FNN approach, better energy consumption with less siganlling overhead than existing approaches are achieved.

The paper's organization is illustrated as follows: In Sect. 2, the related works done by various researches are discussed. In Sect. 3, the proposed methodology is discussed in detail. In Sect. 4, the experiments accomplished to determine the performance of the proposed method is illustrated. Finally, the conclusion and future work is specified in Sect. 5. The list of abbreviations is given in Table 1.

2 Related works

The work related to the proposed handover authentication is described as follows.

Sangeetha et al. [16] suggested a trust-based handover authentication scheme in Software-Defined Networking (SDN) 5G heterogeneous network to improve 5G mobile communications security. The three-way handshaking protocol was used to attain mutual authentication. Further, the security of the trust-based handover authentication scheme has been determined utilizing a trust value algorithm along with a clustering process.

Divakaran et al. [17] suggested an enhanced handover authentication model in 5G communication networks by employing fuzzy evolutionary optimization. In this authentication model, fuzzy evolutionary optimization was utilized to manage handover as well as maintain key management to enhance the effectiveness in 5G networks. Moreover, this method was modelled to reduce complexity and delay during network authentication in 5G networks.

Man Chun and Maode Ma [18] suggested a 5G authentication approach and key agreement protocol based on blockchain against Denial-of-Service (DoS) attacks. The suggested method had employed the private blockchain to offer a distributed database for storing each authentication record. Moreover, it also explored the trapdoor collision property of the Chameleon hash function, where the blockchain entries could check incoming authentication requests. The device anonymity was protected using a SUbscription Concealed Identifier (SUCI), and Elliptic-Curve Diffie-Hellman (ECDH) had utilized to establish a session key.

Xinghua Li et al. [19] suggested a Fast and Universal Inter-Slice (FUIS) handover authentication model using ring signature, chameleon hash and blockchain. For inter-slice handover, a service-oriented authentication protocol was introduced and a key agreement by generating an anonymous ticket using a property of trapdoor collision. A privacy-preserving ticket validation along with a ring signature was modelled to minimize computation overhead during the authentication process, mainly for completing the consensus phase of the blockchain.

Xudong Jia et al. [20] suggested a blockchain-based decentralized authentication model called A^2 chain for 5G-assisted IoT. The processing of authentication requests was initially decentralized by using edge computing in the A^2 chain and avoiding the burden on the network and authentication services. Next, blockchain and sidechain technologies were utilized in the A^2 chain to execute the cross-domain identity of IoT devices and securely share the identity verification data. Further, to remove the management overhead instigated by the centralized authentication scheem, A^2 restores Public Key Infrastructure (PKI) with the Identity-Based Cryptography (IBC) algorithm.

Zaher Haddad et al. [21] suggested a blockchain-based new efficient, secured authentication and key agreement protocol in 5G network. The network's capital entity, known as the Home Network (HN), was accountable for initiating the blockchain as well as bootstrapping the network. The HN network would share the Blockchain over the entire network nodes. The authentication as well as registration process should be performed between the serving network and the UE if the new UE is switched on or comes to a new coverage area. Moreover, this protocol had secured and endured major attacks like DoS, a man in the middle, distributed DoS, compromising and Hijacking attacks.

In SDN-based 5G networks, a blockchain-based authentication handover and privacy protection were presented by Abbas Yazdinejad et al. [22]. SDN-based and Blockchain-based authentication approaches were

Table 1 List of abbreviations

Abbreviation	Explanation
AC	Actor-critic
APG	Access point group
AUC	AUthentication center
APs	Access points
B	Beyond
BAHEPP	Blockchain-enabled authentication handover with efficient privacy protection
BS	Base station
CNs	Candidate nodes
CRBFT	Credit reinforcement byzantine fault tolerance
C/S	Client-to-server
DoS	Denial-of-service
dPoS	delegated proof of stale
ECDH	Elliptic-curve diffie-hellman
FNN	Fuzzy neural network
FUIS	Fast and universal inter-slice
HN	Home network
IBC	Identity-based cryptography
ID	IDentifier
IoT	Internet of things
IT2-FS	Interval type 2 fuzzy set
LSC	Local service centre
ME	Management engine
MIMO	Multi-input multi-output
MN	Master node
NN	Neural network
PBFT	Practical byzantine fault tolerance
PDR	Packet delivery ratio
PKI	Public key infrastructure
PoET	Proof of elapsed time
PoS	Proof of stack
PoW	Proof of work
P2P	Peer-to-peer
RAT	Radio access technology
RL	Reinforcement learning
RLAC	Reinforcement learning with the actor-critic
RTT	Round trip time
SCI	Secure context information
SDH	Software-defined handover
SDN	Software-defined networking
SHA	Secure hash algorithm
SN	Sub-node
SUCI	SUbscription concealed identifier
UAV	Unmanned aerial vehicle
UDHN	Ultra-dense heterogeneous network
UDN	Ultra dense network
UE	User equipment
5G	Fifth generation
6G	Sixth generation

developed to remove re-authentication in frequent handovers amid the heterogeneous cells. The system was accomplished to guarantee the minimum delay, suitable for 5G network. Here, users could be interchanged with the minimum delay between heterogeneous cells by private and public keys offered through invented blockchain element while keeping their privacy.

Amina Gharsallah et al. [23] suggested SDN based handover management process in5G UDN. This process could utilize Software-Defined Handover (SDH) for optimizing the handover in 5G networks. Besides, a SDHManagement Engine (SDH-ME) to manage the handover control process in 5G UDN. SDH-ME was utilized to apply the SDN structure that had been accomplished through the control plane to orchestrate the data plane.

Jing Yang et al. [24] suggested a fast and unified handover authentication model in 5G SDN heterogeneous networks based on a link signature. To establish fast and unified handover authentication, a distinctive wireless channel characteristic between serving AP and user were extracted as a Secure Context Information (SCI) and forwarded to the target AP. Further, the latter could evaluate whether the user was a legitimate one, who had previously authenticated corresponding to the forwarded SCI.

A blockchain-based security authentication approach had been presented by Zhonglin Chen et al. [25] for 5G UDN. Here, an APG was employed with PBFT approach based on blockchain consensus mechanism. In APG-PBFT, the consensus mechanism would be optimized, as well as a new reverse screening approach would be adapted. Moreover, along with the APs, a trusted chain APG could be created using the APG-PBFT algorithm. By using blockchain message propagation, the results of authentication could be shared in the APG.

Muhammad Nabeel et al. [26] had presented the deployment of TurboRAN testbed for evaluating the performance of 5G& Beyond (B) cellular network. The deployment challenges were discussed and highlighted with the details of hardware components as well as the reason for selecting the hardware components were provided. Case study for the working procedure of TurboRAN was provided with the impact of mobility parameters. It is essential to highlight the TurboRAN testbed focusing on sub-6 GHz and Multi-Input Multi-Output (MIMO) capability features.

Shidrokh Goudarzi et al. [27] had proposed a approach based on cooperative game theory for selecting Unmanned Aerial Vehicle (UAV) during handover and optimized with the decrease of handover latency, end-to-end delay and signal overhead. In addition to that the standard modelling of software-defined network software-defined network with media-independent handover which are utilized as a forwarding switches for obtaining seamless mobility. Table 2 shows the Contribution and Limitations of existing methods.

The consensus mechanism is considered a major process in blockchain-based 5G heterogeneous networks. Recently, several consensus protocols have been proposed by different authors and applied in several decentralized platforms. Still, it is not suitable for 5G environments because of handover delay, re-authentication, etc. Therefore, a new blockchain-based handover and consensus mechanism is necessary in 5G heterogeneous networks to resolve these problems and provide fast authentication.

3 Proposed methodology

In our proposed method, a new consensus mechanism of blockchain-enabled authentication handover approach in 5G Heterogeneous Networks is proposed to enhance the user authentication. In the proposed method, users acquire a secure and quick connection through avoiding re-authentication amid handovers operators among heterogeneous cells with minimum delay. Delay reduction is considered as one of the primary intentions and features of 5G, is of great significance that can occur with solid structure. The proposed consensus mechanism will optimize the consensus node partition structure and adapt the consensus period. The LSC will use a new learning approach to detect the trusted AP in the block generation process. Our proposed algorithm improves the node separation structure to reduce the delay of the consensus algorithm. In the proposed approach, all secondary peers are further subdivided into several secondary peer groups based on credit value. All secondary peers are credited based on their likelihood of successfully participating in the consensus. Each secondary peer group contains some Candidate Nodes (CNs). Here, the CNs will return their results to secondary nodes. The secondary nodes will summarize all their results to return to LSC. Finally, LSC will identify the trusted peer and the malicious peers by adaptively confirming the consensus by integrating the RL method with the AC learning based on FNN (RLAC-FNN). In addition, the block chaining methods usually set up a certain time interval to remove the block generated during the consensus process. After this interval, the consensus result must be recomputed to form an APG trusted blockchain. This period will be adjusted automatically by sensing the number of nodes and their transactions in the proposed method.

3.1 System model

In 5G, UDHNs have been determined as a key mechanism for managing orders of magnitude rise in the volume of

Table 2 Contribution and Limitations of the existing methods

Authors	Methods	Contributions/unique characteristics	Results	Limitations
Sangeetha et al. 2022 [16]	Trust-based handover authentication scheme	To improve the security in SDN 5G heterogeneous network. Mutual authentication has been obtained with three way handshaking	Better throughput, delay, packet delivery ratio (PDR) had attained	Need to improve the handover process
Divakaran et al. [17]	Enhanced handover authentication model based on fuzzy evolutionary optimization	To reduce complexity and delay in 5G networks during the network authentication process. Hanover authentication process is enhanced with fuzzy evolutionary process	Better in handling, authentication and mitigation against different attacks	Complexity still exists
Man Chun and Maode Ma 2021 [18]	5G authentication approach and key agreement protocol based on Blockchain	To establish a secured 5G network from DoS attacks. Authentication and key agreement was provided against DoS with SUCI, and ECDH	Attained mutual authentication, accurate forward secrecy, key agreement and device anonymity	Security issues still exist
Xinghua Li et al. [19]	FUIS handover authentication model	To support inter-slice handover. Ticket validation with privacy-preservation is modelled with a ring signature for minimizing overhead	Minimized handover over	Need to minimize the time
Xudong Jia et al. 2020 [20]	A^2 chain	To establish a secure authentication information sharing process. Authentication process is decentralized with edge computing process	Minimized authentication time, storage space and communication cost	Need to improve the authentication time reduction and delay
Zaher Haddad et al. 2020 [21]	Blockchain-based new efficient, secured authentication and key agreement protocol	To provide a secure and authentication scheme for finding major attacks. Secure authentication and registration process is accomplished against DoS, a man in the middle, distributed DoS, compromising and Hijacking attacks	Secured and counter measured major attacks	Need to minimize the consensus delay
Abbas Yazdinejad et al. 2019 [22]	Blockchain-based authentication handover model	To avoid the re-authentication in frequent handover amid the heterogeneous cells in SDN-based 5G networks. Privacy protection is guaranteed with minimum delay between heterogeneous cells	Attained less signalling, less delay, and less energy consumption	Minimize signalling overhead and enhance the performance
Amina Gharsallah et al. 2019 [23]	SDN based handover management process	To improve the handover process in 5G UDNs. Handover control process is managed with SDH-ME	Minimized handover delay and handover failure ratio	Increased the risk
Jing Yang et al. [24]	Fast and unified handover authentication mechanism	To establish a fast and unique authentication process in 5G heterogeneous networksby considering the channel characteristics	Minimized overhead and latency	Susceptible to the channel condition
Zhonglin Chen et al. 2018 [25]	APG-PBFT consensus mechanism	To organize APs into a secured, trusted chain as APG for enhancing the reliability and security of APG. Consensus and message propagation is utilized for authentication	Eliminated the frequency of authentication if UE moved amid the APs as well as improved the access efficiency	Need to improve the consensus mechanism
Muhammad Nabeel et al. [26]	TurboRAN testbed deployement	Summarized relevant testbeds and deployment of turboRAN testbed. Handover procedures were investigated with capability and functionality	By tuning the parameter configurations, several handovers occured for achieving highest datarates	It is required to be incorporated for massive MIMO for enabling Sixth Generation (6G) communication
ShidrokhGoudarzi et al. [27]	cooperative game theory	An entire view of the network was provided with SDN for end-to-end policy formulation with high computational power which is not available at the UAVs	For large range of mobile nodes, higher amount of handoff strategy was obtained	Frequent handover leads to high energy consumption

data traffic. For users, UDHN is tererned as a direct access network that uses APs to connect users to the 5G network. However, in UDHNs, users require to secure access as well as guarantee that access to the network is secured and UE has not associated to an illegal or fake AP. So, it needs the UDHN to guarantee that each AP that communicates with UE should also be secured.

Figure 1 illustrates the architecture of 5G UDHNs. In this 5G UDHNs architecture, the user-centric UDHN has been explored to constitute a assured range of APs around the UEs, and APG accomplishes user service to the UE. When the user moves, the members of the APG have been dynamically updated so that the user can experience that there contains a mobile network coverage linked with it. Thus, the demand of mobile traffic can be effectively addressed, and the user's experience can be improved. In the UDHNs architecture, the APGs are accountable for accessing the UE connection. So as long as it is ensured that APGs are secured (for instance, a rogue or fake AP does not active in APG or not included in APG), it has been guaranteed that the access of UE is secured without having to need that every APs are secured nodes that will effectually minimize the complexity of security protection. In a 5G heterogeneous network, either the members of APG or the regular access nodes in UDHN, all APs are entirely equivalent between one another, is termed as an organization that does not contain a center.

3.2 Problem formulation

The cyclic additive group is represented as G_1 and the cyclic multiplication group is represented as G_2. Both groups are having the same primary order q and p represents the generator of G_1. The bilinear mapping is formed with $G_1 \times G_1 \rightarrow G_2$ an dhteone way hash functions are denoted as H_1, H_2 and H_3 in which $H_1 : \{0,1\}^* \rightarrow G_1$, $H_3 : \{0,1\}* \rightarrow Z_q$, and $H_2 : \{0,1\}* \rightarrow Z_q$. The public key system parameters are initialized and the master key is kept as secret. When the AP is having ID to joint with the system, the AUC calculates the private key which is securely sent to the APs. It is assumed that the UE with $ID \in \{1,0\}$ sends ID to AUC to start registration process. If the ID is valid then AUC chooses collection of identities for the computation of relevant private keys.

In the initial phase, a request for APG generation has been accomplished. After providing a UE access request to the network, the APs from a particular range around the UE can accept the message and send a request. If the request message is subsequently reached at LSC, the LSC can be called to organize an APG for providing service to the UE. LSC enquires the AUthentication Center (AUC) for the APG key as well as other parameters to provide corresponding data like APG unique IDentifier (APG-ID).

Moreover, the UEs have registered in LSC to construct encryption materials depending on the possessions and further accept the encryption possessions as well as key. LSC forwards a vector consisting of UE information of the cell simultaneously. For each UE, the LSC assigns two

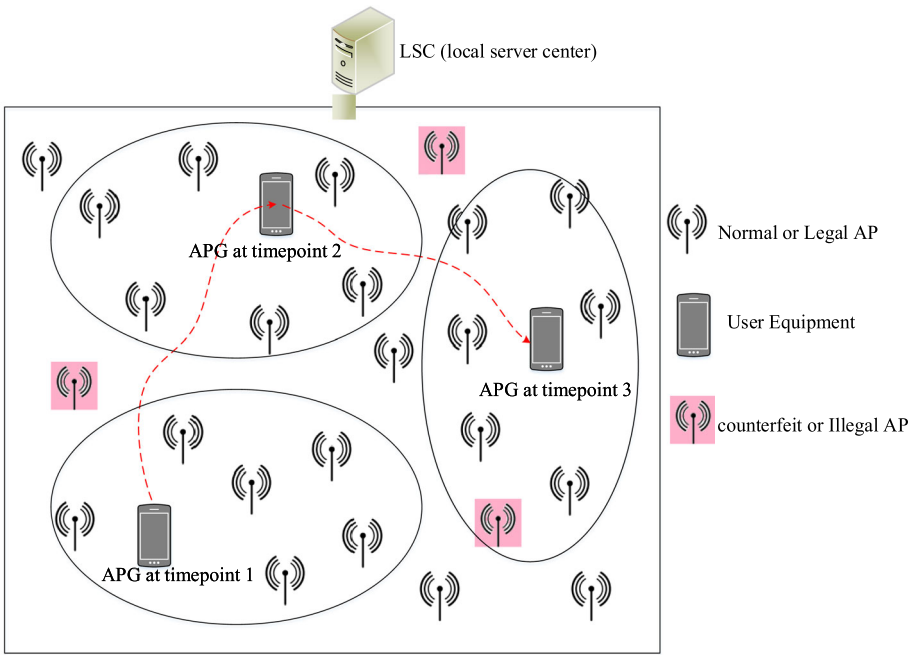


Fig. 1 Architecture of 5G UDHNs

keys, namely a private and a public key. The UE forwards the join request to the LSC to enter the specified domain or cell. This request was acknowledged through the authentication control unit and forwarded to the UE after the confirmation. The authentication control is applied to determine the unique UE information like direction, identity, Round Trip Time (RTT), location, as well as private and public key assignment.

The set of information from users registered in LSC, namely the public key, has been forwarded to other cells, then UE joints the cell. If the UE needs to hand over the current AP to another AP in the identical cell, the UE forwards the associate request to the target AP and disconnects with the current AP. Normally, the distinctive behavior of UE has been shared amid neighboring and adjacent cells, so there is no necessity for a re-authentication process while sending over the heterogeneous cells. The LSC checks the AUC to guarantee that the UE is a trusted cell. The UEs are registered in the accessible cell and aims to move to the adjacent heterogeneous cell, which forwards the request to AP of the identical cell. The private key Q has been known between the AP and UE, and it can switch between the AP of a cell. Then, the public key R has used in signing transactions as well as decoding the information for privacy protection. The UE forwards the message to other neighboring public key cells to avoid the necessity for a frequent re-authentication process in the heterogeneous cells. This process stimulates authentication while transiting through APs and some heterogeneous networks.

3.3 Blockchain-based handover and fast security authentication

In order to provide a handover and fast authentication process, a blockchain-enabled authentication handover approach based on RLAC-FNN has been proposed. Block chain approach is needed to combine the concept of hashing algorithm, public key encryption, peer to peer protocols, and consensus algorithm. It is basedon decentralized network in which the main task is the protection of stored list of records against tampering. Block chain manages the database by enhancing the speed of operations, and information security level by reducing the required time and individual error. The concept of block chain mechanism does not require centralized data storage or central supervisor. There is no additional requirement of organizational authority instead of consensus algorithm for managing the decentralized network.

Then, for authentication, the LSC sends an instruction for consensus computing to all AP providing service to UE. The new consensus computing process is based on RLAC-FNN. Based on the consensus outcomes, the trusted APs are selected since there contain one or more fake or untrusted AP.

3.4 New consensus computing process based on RL with the ACbased on FNN

In the blockchain-based 5G networks, the main objective is to attain a consensus on the blockchain transaction information in complete network. A new consensus computing algorithm using RLAC-FNN has been proposed the process of consensus computation. Relating to the blockchain decentralized scheme, the Client-to-Server (C/S) paradigm has shifted to the P2P paradigm. Thereby, the system contains no client. The consensus node is divided into three categories: Master Node (MN), CN and Sub-Node (SN). For each consensus node, the credit attribute has been set so that the system will dynamically split the consensus node, and the nodes will leave and join the system dynamically. Then some of the elementary parameters applied in the system can be provided as:

- Set an attribute credit E as an index to determine the reliability of consensus node's, which means the probability of participating in consensus successfully. It is considered as a significant basis for dividing the consensus nodes.
- The node with the highest credit value is assigned as the MN. P signifies the number of consensus nodes, where $P \geq 3G + 1$ and G resembles the maximum number of malicious nodes a system will bear. Normally, P uses $3G + 1$.
- The value of admission credit E_{BAS} has been preset. $P - 1$ CNs with credit $E \geq E_{BAS}$ are chosen as SNs. The nodes with credit value less than E_{BAS} or recently included nodes are chosen as CN.

During system initialization, the credit value of each consensus node is set to E_{BAS} and P consensus nodes have chosen randomly as SN. Then, the MN has elected from the SN, and the number q is allocated. Because the blockchain consensus system is decentralized and P2P-based, every consensus node must initiate in an identical state. This resembles that the information deposited in each consensus node requires consistency. To guarantee consistency needs verification and data backup. After completing the backup as well as verification process, the model initiates the consensus process. In the proposed consensus process, message delivery applies digital signature schemes as well as Secure Hash Algorithm-256 (SHA-256) to guarantee the authenticity and message integrity. The consensus process is initiated by the MN and set as the interval for MN consensus as U. Then the particulars of the proposed algorithm are provided below as follows.

- The initiator starts the transaction through signing the transaction as well as broadcasting it to the consensus node.
- The legality of the received transaction is verified by the consensus node. When the received transaction is illegal, the transaction is discarded directly. Otherwise, it is considered legal, so the transaction information has been cached, as well as the MN constructs a block.
- After U, a proposal message is created by the MN q for the constructed block and provide a unique number p to the proposal. The unique number can maximize with each newly constructed proposal. Moreover, to request the SN for participation, the MN q broadcasts the proposal message to the SN. During the consensus process based on credit value, the messaging format is assigned as $<<\Pr oposal\, message, q, p, Mes.Sig, e, >, Block>$, where, e resembles the message digest determined using the SHA-256 algorithm and $Mes.Sig$ indicates the message signature.
- First, the SNs verify the MN number, proposal number, and proposal's message signature. The SNs will forward a verification message to MN if the verification has passed. Then the format for sending the verification message is given as $<consensus.com, q, p, Mes.Sig, e, s_t, l, D>$, where, consensuscom represents the consensus confirmation l indicates the SN number. s_t resembles the verification type of SN l to the proposal message digest. D denotes the reputation of the SN l. s_t can be either -1 or 1, relating to *false* or *true*, considerably, where *true* represents the proposal message digest e is consistent with cached data through the SNs. Else, *false* indicates the inconsistency, and the SN mistrusts the MN. On the other hand, if the verification flops, the SN has discarded the proposal message.
- Then, the MN utilizes RL to carry out consensus confirmation for the received verification message. When the MN has received $2G$ confirmation messages, it is regarded that the consensus is attained as well as published a block. However, if the MN has received $2G$ suspicious messages, the consensus node broadcasts a message to change and reselect the MN. During the consensus timeout, if sufficient messages are not received, every node discards the generated block at the consensus computation process, reselect the MN, and minimize the credit of the discarded MN. Further, again re-elect the MN but no longer choose the original MN. Eventually, it generates a new round of consensus. When the MN successfully publishes the block, and after publishing the newly generated block, such node forwards a credit adjustment message to each SN.
- If the consensus node has received the published block, this consensus process has finished. Further, such a node can update the credit corresponding to the adjusted data, clear the cache, update the consensus node, as well as establish a fresh round.

The proposed algorithm of RLAC-FNN is given in algorithm 1 and the SHA-256 based block chain based approach is given in algorithm 2.

Algorithm 1: RLAC-FNN for consensus confirmation

Input: data $Y(u)$

Step 1: The parameters, learning rate and weight vectors are initialised

Step 2: Then the amount of fuzzy rules n_j^1 and error are computed

Step 3: Follow step 4 to step 6 when the number of iterations u is not reached

Step 4: Produce the vectors of Bernoulli variables for updating truth value

Step 5: Ordinal index of fuzzy rules and output is calculated for estimating error

Step 6: The process is terminated if the calculated error is less than the error tolerance or the maximum number of iterations are reached. Otherwise, the gradient decent of vector is calculated and the parameters are updated with RLAC

Step 6.1: Collect the parameters $s_t(l)$, $D(l)$ and as $v(l)$ from FNN as state for RLAC for a specific time

Step 6.2: for each fuzzy rule k normalized firing strength P_w^k is computed

Step 6.3: The critic value function and action output is calculated

Step 6.4: After calculating and invoking the actual action the reward is received and the state is transmitted

Step 6.5: then the prediction error function $f_d(l)$ and critical value function $F_d(l)$ is calculated

Step 6.6: Condition for rule unit is checked and if, the conditions are satisfied then the parameters are updated else continue to the next step

Step 6.7: Weight, centre and depth are adjusted

Step 6.8: It is checked that whether the units are required to be merged or not. If the condition is satisfied then similar units are merged otherwise next step is proceeded

Step 6.9: The number of iterations for RLAC is checked. If the number of iterations are not completed then it is continued from 8.2

Step 6.10: After updating the parameters, it is repeated from step 4 to step 8 until the number of iterations are attained

Step 8.11: $K(l)$ is returned to step 8

Output:consencus confirmed or not

Algorithm 2: SHA-256 based block chain approach

Input: message

Step 1: Som additional bits are added to the input message in which the message length is 64 bit shorter than the multiple of 512. While adding the bits, the first bit is one and the remaining bits are filled with zero

Step 2: The charecters for this 64 bits are computed by applying modulo operation to the original text without padding

Step 3: The default values are initialized for eight buffers

Step 4: Then the entire message is divided into several blocks and each block contains 512 bits

Step 5: Each block passes through 64 rounds operations and the output of each block is fed to the input of next block

Step 6: The entire process is completed until the last 512-bit block is processed., Then the output is considered as final hash digest

Output: 256 bit hash digest

3.4.1 Consensus confirmation

The consensus confirmation process integrates the AC model and FNN. It primarily consists of an action network that generates AC network, which has been employed to compute the actions. The primary objective of AC is to decide whether the SNs are in agreement and establish a source for credit adjustment. Initially, the structural learning of AC-FNN has applied to determine the number of AC-FNN rules and assign the initial values for the parameters of the AC network. Online structural learning is a process that provides if–then rules depending on the input data. It has been performed using fuzzy clustering that determines the fuzzy rule based on the rule firing strength. The first input data $Y(u)$ is utilized to determine the first fuzzy rule. The first epileptic Interval Type 2 Fuzzy Set (IT2-FS) parameters for the first if–then rule are set in Eq. (1).

$$n_j^1 = y_j(u), \quad \varsigma_j^1 = \varsigma_{jFixed}^1, \quad j = 1, 2, 3, ...z \tag{1}$$

where, n_j^1 indicates the mean of the membership function, ς_{jFixed}^1 resembles the pre-defined value that must be greater than 0, which denotes the interval range of initial IT2-FS. The firing strength is computed at each iteration u. Further, the average value of firing strength P_w^k is computed for each rule k. After this, for subsequent input data $Y(u)$, the determination of the number of rules has computed depending on $J = \underset{1 \le k \le N_h(u)}{Arg\,Max}\ P_w^k$, where, J represents the number of hidden rules,$N_h(u)$ denotes the number of immediate rules at iteration u. Moreover, a new if–then rule has determined at $N_h(u+1) = N_h(u) + 1$ if $P_w^j \le P_{th}$, where P_{th} resembles the pre-determined threshold. The consensus confirmation process based on AC-FNN is given in Fig. 2.

The architecture of both the actor-network and the critic network is typically the same. Both adapt a backpropagation Neural Network (NN) with the hidden layer. Consider, $s_t(l)$ and $D(l)$ in the l^{th} verification message as input for the action network, obtain an output $v(l)$. The critic network uses $s_t(l)$, $D(l)$ as well as $v(l)$ as input and provides the output $K(l)$ as the approximate value of return $H(l)$, which has been applied to evaluate the critic network's outcomes considerably. So, the approximation value has been utilized to simulate the outcome of $v(l)$ better. Further, the action output $v(l)$ and $s_t(l)$ are compared to choose the reinforcement signal $S(l)$. When $v(l)$ and $s_t(l)$ contain identical signs, the output is considered as successful and $S(l)$ is provided as "0" whereas, if it contains different signs, the output is considered as unsuccessful and $S(l)$ is regarded as "1". The schematic diagram of the critic network is depicted in Fig. 3.

Initially, the weight of the critic network and actor-network are assigned randomly at the consensus process. During the NNs learning process, the critic network employs $S(l)$ for updating the weight and estimating the optimum $K(l)$. Then the actor-network utilizes the optimum $K(l)$ to update weight and attain the optimal outcomes.

3.4.2 Critic network

The learning objective of the critic network is to reduce the error between the actual value and approximation value of the value function while optimizing for highest return. Then the prediction error function $f_d(l)$ of the critic network is expressed in Eq. (2).

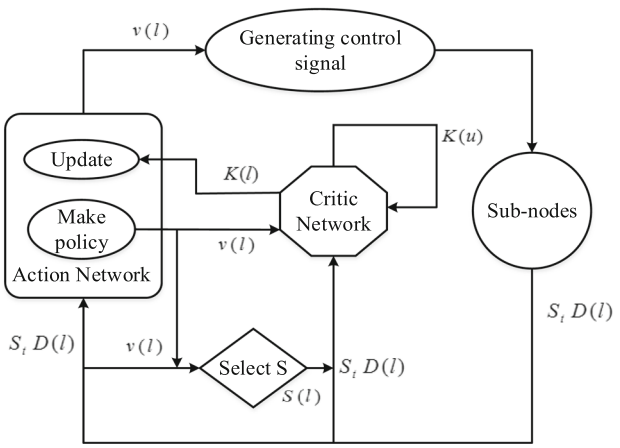


Fig. 2 Consensus confirmation based on AC-FNN

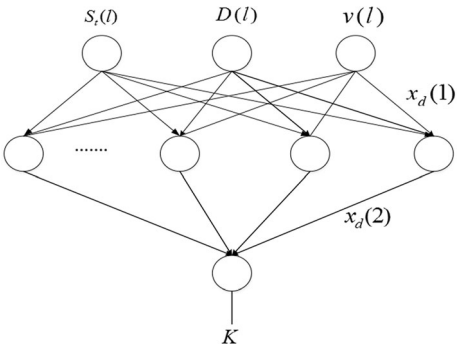


Fig. 3 Schematic diagram of critic network

$$f_d(l) = \beta K(l) - [K(l-1) - S(l)] \tag{2}$$

where, β represents the constant parameter. The prediction error has the property of approaching zero over time while converging actor critic learning. If the distribution error and average error is zero then the average prediction error is large. The prediction error in the critical network is computed by learning the reinforcement signal. The minimized objective function $F_d(l)$ of the critic network is given in Eq. (3).

$$F_d(l) = \frac{1}{2} f_c^2(l) \tag{3}$$

Besides, the output $K(l)$ in the critic network can be expressed in Eqs. (4), (5), and (6).

$$\gamma_j(l) = \sum_{k=1}^{p_{in}+1} x_{d_{jk}}^{(1)}(l) y_k(l), \qquad j = 1, 2, 3....., P_i \tag{4}$$

$$\varepsilon_j(l) = \frac{1 - \exp^{-\gamma_j(l)}}{1 + \exp^{-\gamma_j(k)}}, \qquad j = 1, 2, 3, ..., P_i \tag{5}$$

$$K(l) = \sum_{j=1}^{P_i} x_{d_j}^{(2)}(l) \varepsilon_j(l), \tag{6}$$

where, γ_j indicates the j^{th} hidden node input for the critic network, P_i resembles the total number of hidden nodes present in critic network, ε_j represents the corresponding output. x_d signifies the weight vector in the critic network, $y_k(l)$ represents the input vector, $P_{in} + 1$ defines the total number of inputs provided to critic network, and analog action value from the action network.

Corresponding to the chain rule and error propagation equation of the backpropagation algorithm, the gradient of NN objective function to weight has been determined. It can be provided below as follows.

For the hidden layer output is represented with Eqs. (7), (8), and (9).

$$\Delta x_{d_j}^{(2)}(l) = m_d(l) \left[-\frac{\partial F_d(l)}{\partial x_{d_j}^{(2)}(l)} \right] \tag{7}$$

$$= -m_d(l) \left[\frac{\partial F_d(l)}{\partial K(l)} \frac{\partial K(l)}{\partial x_{d_j}^{(2)}(l)} \right] \tag{8}$$

$$= -m_d(l) \left[\beta f_d(l) \varepsilon_j(l) \right] \tag{9}$$

The critic parameters are updated based on prediction error of critic network. The fuzzy interference system has certain equivalence when the number of conditions are satisfied. The basis function of hidden layers aresame as that of the membership function of the input vector. In addition to that the part of each fuzzy rule is equal to the connection weight between the output layer and hidden layer. Each hidden layers are represented with fuzzy rule. For input to the hidden layer, the representation is given with Eqs. (10), (11), and (12).

$$\Delta x_{d_{jk}}^{(1)}(l) = m_d(l) \left[-\frac{\partial F_d(l)}{\partial x_{d_{jk}}^{(1)}(l)} \right] \tag{10}$$

$$= -m_d(l) \left[\frac{\partial F_d(l)}{\partial K(l)} \frac{\partial K(l)}{\partial \varepsilon_j(l)} \frac{\partial \varepsilon_j(l)}{\partial \gamma_j(k)} \frac{\partial \gamma_j(l)}{\partial x_{d_{jk}}^{(1)}(l)} \right] \tag{11}$$

$$= -\beta m_d(l) f_d(l) x_{d_i}^{(2)}(l) \; . \; \left[\frac{1}{2} \left(1 - \varepsilon_j^2(l) \right) \right] y_k(l) \tag{12}$$

where, $m_d(l) > 0$ signifies the learning rate of critic network while considring j^{th} message. Normally, this rate can reduce overtime to less value. At each iteration, critic output determines discounted total reward to resolve the issue of infinite horizon.

3.4.3 Action network

As discussed earlier, the output is pre-defined and if the outcome $S(l)$ is "0", then the output is successful. That is, the output "0" is signified as the reinforcement signal merely for success. To persuade Bellman equation as well as increase the state value function, the final learning target of the action network represented as V_d, has set to 0. While analyzing in action network, it is determined that the parameter adjustment principle is to indirectly backpropagate the error between V_d and K. The network learning can beaccomplished through prediction error function of the network. Then, the prediction error function $f_b(l)$ and objective function $F_b(l)$ of active network can be defined in Eqs. (13), and (14).

$$f_b(l) = K(l) - V_d(l) \tag{13}$$

$$F_b(l) = \frac{1}{2} f_b^2(l) \tag{14}$$

The action network accommodates the NN model, the same as that on the critic network. Then, the action network is characterized in Eqs. (15), (16), (17), and (18).

$$n_j(l) = \sum_{k=1}^{p_{in}} x_{b_{jk}}^{(1)}(l) y_k(l), \qquad j = 1, 2, 3, ..., P_i \tag{15}$$

$$a_j(l) = \frac{1 - \exp^{-n_j(l)}}{1 + \exp^{-n_j(l)}}, \qquad j = 1, 2, 3, ..., P_i \tag{16}$$

$$i(l) = \sum_{j=1}^{P_i} x_{b_j}^{(2)}(l) a_j(l) \tag{17}$$

$$v(l) = \frac{1 - \exp^{-i(l)}}{1 - \exp^{-i(l)}} \tag{18}$$

where, n_j indicate the input of j^{th} hidden node for action network, $i(l)$ resembles the input of output node, x_b resembles the weight vector, $y_k(l)$ represents the input vector,a_j represents the corresponding output. Like the critic network, the parameter updating rule of action network has provided below as:

For hidden to the output layer, the representation is given in Eqs. (19), (20), and (21).

$$\Delta x_b^{(2)}(l) = m_b(l) \left[-\frac{\partial F_b(l)}{\partial x_{b_j}^{(2)}(l)} \right] \tag{19}$$

$$= -m_b(l) \left[\frac{\partial F_b(l)}{\partial K(l)} \frac{\partial K(l)}{\partial v(l)} \frac{\partial v(l)}{\partial i(l)} \frac{\partial i(l)}{\partial x_{b_j}^2} \right] \tag{20}$$

$$= f_b(l) \left[\frac{1}{2} \left(1 - v^2(l) \right) \right] a_j(l) \sum_{j=1}^{P_i} \left[\frac{1}{2} x_{d_j}^2(l) (1 - \varepsilon^2(l)) x_{d_j, p+1}^{(1)}(l) \right] \tag{21}$$

The output layer is made up of actor and critic part in which the critic part contains the estimation for state value function. Mapping is determined from the state to expected critic value. The actor part considers as action selector which provides mapping from state space into action space. When the resolution of state space is insufficient, the variation of prediction error is high through learning value function in space converges with partial observations.

For input to the hidden layer, the representation is given with Eqs. (22), (23), and (24).

$$\Delta x_b^{(1)}(l) = m_b(l) \left[-\frac{\partial F_b(l)}{\partial x_{b_{jk}}^{(1)}(l)} \right] \tag{22}$$

$$= -m_b(l) \left[\frac{\partial F_b(l)}{\partial K(l)} \frac{\partial K(l)}{\partial v(l)} \frac{\partial v(l)}{\partial i(l)} \frac{\partial i(l)}{\partial a_j(l)} \frac{\partial a_j(l)}{\partial n_j(l)} \frac{\partial n_j(l)}{\partial x_{b_{jk}}^{(1)}(l)} \right] \tag{23}$$

$$= -m_b(l) f_b(l) \left[\frac{1}{2} \left(1 - v^2(l) \right) \right] x_{b_j}^2(l) \left[\frac{1}{2} \left(1 - a_j^2(l) \right) \right] y_k(l) . \sum_{j=1}^{P_i} \left[\frac{1}{2} x_{d_j}^2(l) (1 - \varepsilon^2(l)) x_{d_j, p+1}^{(1)}(l) \right] \tag{24}$$

where, $m_b(l) > 0$ defines that the learning rate for action network is considered with j^{th} message. Subsequently, a list PU and PG is defined to record nodes where s_t is 1 or -1. The list PU accumulates where s_t is 1 whereas the list PG accumulates where s_t is -1. If the number of nodes in PU is equal to or greater than $2G$, then the consensus is confirmed. On the other hand, if the number of nodes PG is equal to or greater than $2G$, the SN does not trust the MN respectively.

4 Result and discussion

In this part, the outcomes of the proposed method have been discussed. The performance of RLAC-FNN can be determined based on different metrics and compared with existing algorithms to evaluate its effectiveness. The implementation of RLAC-FNN is carried out using the Python platform. Then, the result of the RLAC-FNN is compared with recent existing methods. The network consisting of 30 heterogeneous cells with a distance of 200 m between two APs are selected to determine the comparability of the consensus approach based on RLAC-FNN among 5G heterogeneous cells. Table 3 illustrates the network parameters used for simulation. All the values of the parameters are selected from the previos research as well the performance of the proposed approach with possible parameter values. By using this parameter values better performance is obtained in the exiting researches [28] and our proposed work.

Table 3 Simulation parameters employed for evaluation

Parameters	Values
Number of cell	30
Number of transaction	1200
Cell radius	100 m
Distance between two AP	200 m
Number of users	600
User mobility direction	Random
Receiving power	1340 mW
Transmit power	1726 mW
Block size	4 byte

While testing the performance, the rules to adjust the credit value can be shown below as follows:

- Initially, the credit of all nodes indicated as D_{BASE}, which is assigned to 3.The reliability of consescus nodes are measured with credit value. The node with higher credit can be participate in the consensus. Hence, the value D_{BASE} is set as lower than than the possible credit value of non malicious node from the previous iteration.
- The credit value of a MN is maximized by 0.2 if it finishes a consensus. The credit value of the SN is reduced by 0.1 if the verification type of the SN is *false*. Whereas the credit value of the SN is maximized by 0.1 if the verification type of SN is *true*. In addition, the credit is minimized by 0.1 to a SN, which is not responding over time. These values are selected from the possible credit maximization or minimization values which are applied to the proposed algorithm. From the possible values the best one is selected based on the performance of proposed algorithm.
- The credit of the MN is set to 2 when the SN guess that the MN is successful.
- The MN will be reduced by 1 if it has not finished the consensus process within the timeout.

Subsequently, some of the specific settings of NN have been illustrated as follows:

- The internal cycle of the action network P_b is set to 100.
- The internal cycle of the critic network P_d is set to 50.
- The initial learning rate of the action network $m_b(0)$ is set to 0.3.
- The initial learning rate of the critic network $m_d(0)$ is set to 0.3.
- The learning rate of the action network $m_b(u)$ at time u is minimized by 0.05 until it attains 0.005.
- The learning rate of the critic network $m_d(u)$ at time u is minimized by 0.05 until it attains 0.005.
- The number of hidden nodes P_i is considered as 6.
- For an action network, the internal training error threshold U_b is set as 0.005 (the threshold of $F_b(l)$).
- For a critic network, the internal training error threshold U_d is set as 0.05 (the threshold of $F_d(l)$).

Moreover, in this evaluation, the proposed method has considered 10 consensus, and the value G is set to 3 and P to 13. The outcomes of the simulation are depicted in Fig. 4.

4.1 Performance metrics

This section discusses various performance metrics that were considered to determine the simulated results of RLAC-FNN. RLAC-FNN considered various metrics such as consensus delay, consensus time, signalling overhead, handover authentication delay and energy consumption for evaluation.

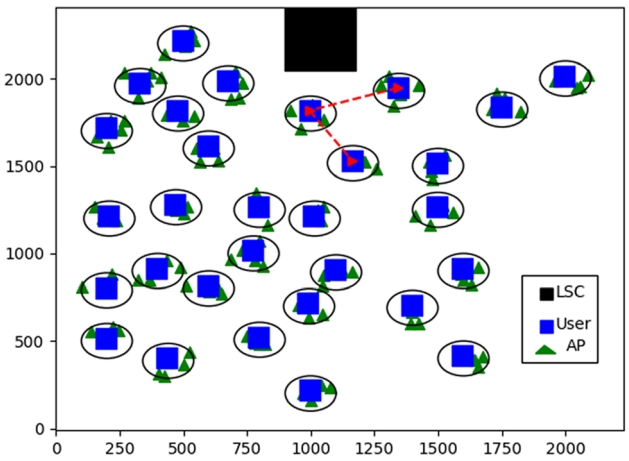


Fig. 4 Output of simulation

a. ***Consensus delay***

Consensus delay is considered a significant metric to compute the speed of the consensus process. The minimum consensus delay can quickly confirm the transaction, making blockchain outcomes more practical and stable. Indeed, the consensus delay U_e evaluated in the proposed method is the consensus completion time, and it is expressed in Eq. (25).

$$U_e = U_{ud} - U_{us} \tag{25}$$

where, U_{ud} resembles the transaction's start time and U_{ts} indicates the completion time of consensus. Here, the value of G has set to 1, 2, and 3, and the value of P has set to 4, 7, 10, considerably.

b. ***Consensus time***

It is a taken between the UE, AP and AUC to authenticate the particular UE for accomplishing handover. It depends on the organization of network structure and the rules of interaction for measuring the system reliability.

c. ***Authentication delay***

After sending request to access the duration taken for getting authentication response is refered as authentication delay. It includes the process of request generation, validation with AUC, getting response from AUC and sending authentication message to the UE. Normally, when the network load is low then the authentication delay is negligible. With increasing the network load, data transmission operation and mobility among cells, the authentication delay is increased.

d. ***Energy consumption***

If the received rate D_{RX} is the received rate and D_{TX} is the transmit rate, the energy consumption can be computed in Eq. (26).

$$F = [D_{TX} \times Q_U \times T1] + [D_{RX} \times S_Y \times T1] + [Q_R \times (T - T1)] \tag{26}$$

where, Q_U indicates the transmit power, S_Y resembles the receiving power, Q_R signifies the received power, T represents the initial time, and $T1$ represents the connection time.

e. ***Signalling overhead***

Signalling overhead comprised additional or pattern information to improve the performance of wireless communication. This overhead relates to the register UE in LSC. The signalling overhead is compared to network-based, POW-based and BAHEPP models. Then, the signalling overhead can be expressed in Eq. (27).

$$W_{OH} = \left(\frac{C \times N}{T}\right) + \frac{Z}{T} \tag{27}$$

where, W_{OH} indicates the signalling overhead, T represents the time, C represents the steps count between UE and LSC. Z resembles the length of packets forwarded to LSC and N signifies the length of packets registered in LSC.

4.2 Performance evaluation

Besides, the result of RLAC-FNN is demonstrated and compared with recent existing algorithms such as PBFT, Credit Reinforcement Byzantine Fault Tolerance (CRBFT) algorithm, network-based model, POW-based model, blockchain-enabled Authentication Handover with Efficient Privacy Protection (BAHEPP) model Fast and Universal Inter-Slice (FUIS) [19] and Lightweight and Secure Handover Authentication (LSHA) [29] considerably.

The working principle of proposed fast authentication process is given as follows. Initially all the parameters are initialised for the proposed 5G UDHN network model. After network deployment and parameter initialization, the request is send for APG generation at initial phase. After granting the access request of UE, the AP accept and send it to LSC. LSC interacts with the AUC for generating the parameters such as APG key and APG ID. UE is registered with LSC which provides private and public key to the UE. The join request for UE is forwarded to the LSC for entering into the specific cell. This request is acknowledged with AUC and the confirmation is sent to the UE. The authentication control is applied for finding the UE information as well as private and public key management. During the process of authentication, the block chain based approach with SHA-256 is utilized for fast and efficient authentication. For authentication LSC sends consensus computing to all AP with the proposed algorithm RLAC-FNN.

Then, the consensus delay attained by the proposed method has depicted in Fig. 5.

In Fig. 5, it is determined that when the number of nodes maximizes, the consensus delay of the proposed, PBFT and CRBFT algorithm can also be maximized. However, the maximization of PBFT and CRBFT is more than proposed RLAC-FNN. So increasing the consensus node contains a major impact on PBFT and CRBFT algorithms. Moreover, for varying numbers of nodes, the consensus delay of RLAC-FNN is considerably less than PBFT and CRBFT algorithms. Thus, the proposed method is superior to existing algorithms.

Table 4 illustrates the consensus delay performance comparison with RLAC-FNN and existing PBFT and CRBFT algorithms. The consensus is determined for varying the number of nodes to 4, 7, and 10. The RLAC-FNN has attained better outcomes of 191.94 ms for 4 nodes, 239.143 ms for 7 nodes, 0.21 s for 270.32 ms for 10 nodes, compared with existing algorithms considerably.

The performance of consensus delay is compared with the exiting approaches such as CRBFT, PBFT, FUIS and LSHA in Fig. 5 and Table 4. When compared with the exiting approaches, the performance of the proposed approach is lower in terms of delay. For the proposed approach, the delay is in the range of 200 ms. It is due to the fast consensus process of proposed RLAC-FNN. It computes the consensus with minimal time duration by effectively learning the parameters used for the process. Efficient parameters are chosen with the RLAC based

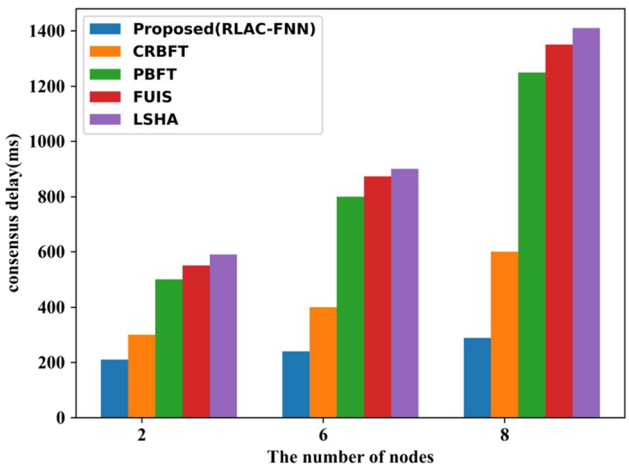


Fig. 5 Performance evaluation of consensus delay with proposed and existing algorithms

Table 4 Comparative analysis of consensus delay

Number of nodes	Consensus delay (ms)				
	PBFT	CRBFT	FUIS	LSHA	RLAC-FNN (Proposed)
7	800	400	550	590	239.143
10	1250	600	873	900	270.32
4	500	300	1350	1410	191.94

approach which provides better weight value with minimal computational complexity. Hence, the FNN accomplishes the weight updating process within short duration and it enhances the computation process of FNN. Meanwhile, the consensus confirmation efficiency is improved with fast computation of consensus information.

The performance evaluation of the single consensus time is given in Fig. 6. In the figure, it is evidently seen that the proposed method takes more time in the first consensus, and with the learning of NN, the consensus time minimizes till the learning finish., For the first consensus, RLAC-FNN has taken 1606.76 s followed by 670.78, 655.18, 608.38, 389.99, 389.99, 358.79, 358.79, 343.19, and 311.99, considerably.

The handover authentication delay of the proposed method is related with existing network-based, POW-based and the BAHEPP model [22]. In the existing POW-based model, the users should register in the blockchain and upon continuous displacement of the cells, it becomes re-authentication in the cell. Both network-based as well as POW-based schemes separate protocol and re-approval amid heterogeneous cells for the authentication process. In RLAC-FNN, the user cannot require to be re-authenticated if being placed in the heterogeneous cells since they are valid in neighbour cells as well as handover simply by eliminating the re-authentication delay.

In Fig. 7, the handover authentication delay is shown with varying rate of network utilization in 5G heterogeneous network. The proposed delay is compared with the existing POW based, Network based, BAHEPP approaches. With low network utilization, the handover authentication delay is in the range below 0.2 ms. If the network utilization is increased to 0.6, then the delay is slightly increased for the existing approaches. For the proposed approach, it is below 0.2 upto the network utilization rate 0.8. When it is increased above 0.8, the handover authentication delay is slightly increased. Authentication delay is in the range between 0.5 and 3 when the network utilization is 1. FUIS and LSHA performance is lower when compared to that of the proposed approach. When compared with the existing approaches, the handover authentication delay is lower for the proposed approach.

Table 5 compares handover authentication delay performance with RLAC-FNN and existing network-based model, POW-based model and BAHEPP. The table clearly shows that the proposed consensus mechanism based on RLAC-FNN has minimized the handover authentication delay more than the existing models due to eliminating the re-authentication process. The handover authentication delay given in Table 5 is lower for the proposed approach and it is higher for the existing approaches. Upto the network utilization is 0.3 is 0.1 for all the approaches. By increasing the network utilization, the handover authentication delay is increased heavily for the existing

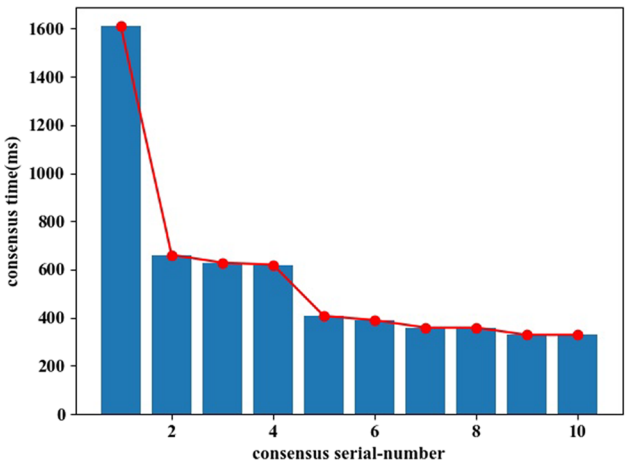


Fig. 6 Performance evaluation of single consensus time with proposed and existing algorithms

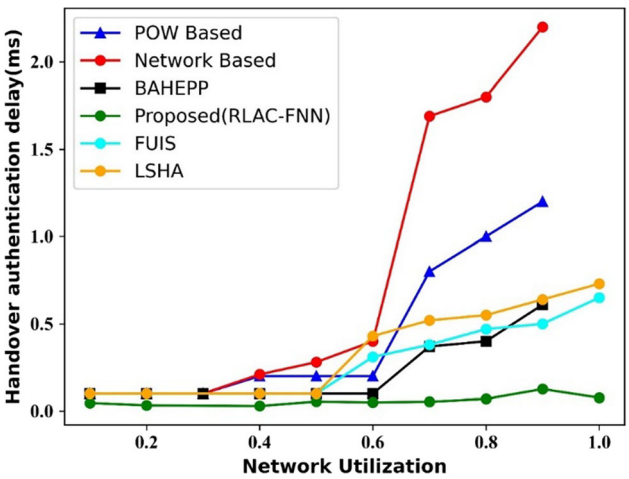


Fig. 7 Performance evaluation of handover authentication delay with proposed and existing models

Table 5 Comparative analysis of handover authentication delay

Network utilization	Handover authentication delay (ms)					
	Network-based model	POW-based model	BAHEPP	FUIS	LSHA	Proposed
0.1	0.1	0.1	0.1	0.1	0.1	0.052
0.2	0.1	0.1	0.1	0.1	0.1	0.036
0.3	0.1	0.1	0.1	0.1	0.1	0.03
0.4	0.21	0.2	0.1	0.1	0.1	0.057
0.5	0.28	0.2	0.1	0.31	0.43	0.05
0.6	0.4	0.2	0.1	0.38	0.52	0.057
0.7	1.69	0.8	0.37	0.47	0.55	0.074
0.8	1.8	0.1	0.4	0.5	0.64	0.13
0.9	2.2	0.2	0.61	0.65	0.73	0.081

approaches. But for the proposed approach all the values are below 0.6. This deviation is due to the proposed fast handover algorithm which utilizes the weight optimization process for FNN. Hence efficient weight updating process is accomplished with minimal duration. During handover process the consensus confirmation can be accomplished with the proposed algorithm which provides fast confirmation process and it minimizes the time required for authentication.

Figure 8 signifies the performance evaluation of energy consumption with proposed and existing models. According to Fig. 8, the proposed method has attained minimum energy consumption than existing models. In contrast with the existing models, the network-based model has increased energy consumption due to the frequent re-authentication process.

The performance comparison of energy consumption with RLAC-FNN and existing network-based model, POW-based model and BAHEPP are illustrated in Table 6. The initial energy level is considered as 0.1×10^4 and by increasing the time duration the energy consumption is

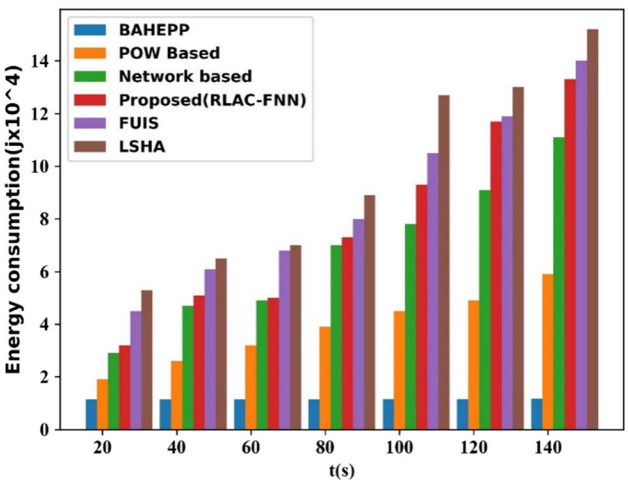


Fig. 8 Performance evaluation of energy consumption with proposed and existing models

increased for all approaches. The comparison shows that the proposed method has obtained less energy consumption than existing models. Moreover, BAHEPP has consumed less energy close to the proposed method, and the network-based model reached higher energy consumption among all existing models. The time represents the processing time of request registration and authentication among cells.

Figure 9 depicts the performance evaluation of the signalling overhead with proposed and existing models such as network-based, POW-based and BAHEPP models. In the graph, it is observed that the proposed method achieved less overhead than all existing models. However, the POW-based model has applied consists of more overhead. Besides, the network-based model can need different authentication servers and third parties in communication among heterogeneous cells. BAHEPP attained minimum overhead closed to the proposed method since it has registered directly on the blockchain centre and interacts with the cell without communicating with other APs. When comparing the energy consumption of the proposed approach, it is higher for the existing approaches. It is due to the fast computing process which requires less energy. Since the time required for the authentication process is low and the authentication delay is minimal, the energy consumption is lower with the proposed approach. Efficient computation process involved in the block chain process with SHA-256 minimizes the energy consumption of the process.

The performance comparison of energy consumption with RLAC-FNN and existing network-based model, POW-based model and BAHEPP are stated in Table 7. The new consensus mechanism based on RLAC-FNN has considerably achieved minimum overhead than all other existing models such as network-based, POW-based, and BAHEPP. It is noted in the table that increasing the time maximizes overhead due to more requests for authentication and registration among the heterogeneous cells.

Table 6 Comparative analysis of energy consumption

Time (sec)	Energy Consumption ($j \times 10^4$)					
	Network-based model	POW-based model	BAHEPP	FUIS	LSHA	RLAC-FNN (Proposed)
20	3.2	2.9	1.9	4.5	5.3	1.213
40	5.1	4.7	2.6	6.1	6.5	1.216
60	5	4.9	3.2	6.8	7	1.217
80	7.3	7	3.9	8	8.9	1.217
100	9.3	7.8	4.5	10.5	12.7	1.219
120	11.7	9.1	4.9	11.9	13	1.22

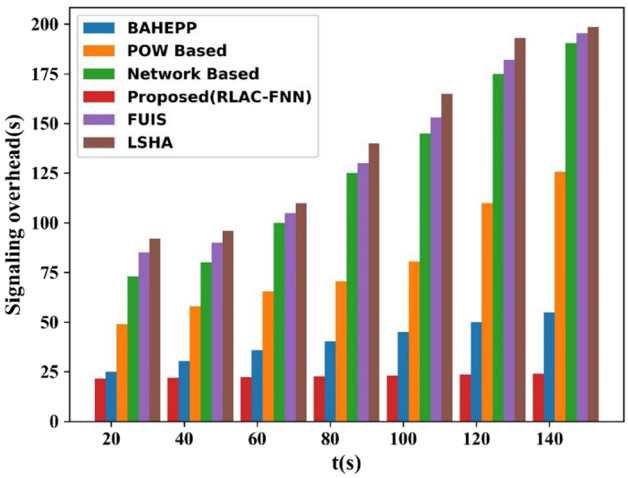


Fig. 9 Performance evaluation of signalling overhead with proposed and existing models

However, the proposed method achieved a minimum overhead than existing models respectively.

The comparison of signaling overhead was given in Fig. 9 and Table 7. When compared with network based, BOW based, FUIS, BAHEPP and LSHA models, the performance is lower for the exisitng approaches. For the existing approaches, the signaling overhead is higher than 21 bytes for all approaches. But in case of RLAC-FNN, it is on or below 20 and it is not increased with increasing the time duration. With the utilization of proposed block chain based approach, the input information is divided into several blocks and the fast encryption process is accomplished with SHA-256. Hence the size for the message send for each communication is lower for the existing approaches. It can be possible with the proposed weight updating process and fast consensus confirmation process. The proposed algorithm minimizes the number of bits send and by minimizing the number of bytes, the overhead is also minimized.

Subsequently, from the overall analysis, it is observed that the new consensus mechanism based on RLAC-FNN is superior to existing methods and suitable for fast authentication and reducing the handover delay in 5G heterogeneous networks.

4.3 Computational complexity analysis

The complexity of the proposed algorithm is based on the handover procedure, authentication algorithm such as block chain based and SHA-256 encryption, and the

Table 7 Comparative analysis of signalling overhead

Time (sec)	Signalling overhead (bytes)					
	Network-based model	POW-based model	BAHEPP	FUIS	LSHA	RLAC-FNN (Proposed)
20	73	49	20	85	92	18.48
40	80	58	30.5	90	96	18.79
60	100	65.3	35.8	105	110	19.12
80	125	70.5	40.3	130	140	19.45
100	145	80.5	45	153	165	19.8
120	175	110	50	182	193	20.16
140	190.5	125.5	55	195	198	20.53

proposed consensus confirmation process. Based on the number of AP and the UE and the amount of registration process the computation complexity of the handover process is $O(n^2)$. Then the process of authenticating the UE during the handover process has the complexity $O(n)$. It is assumed that the random variable is represented with J which denotes the amount of invalid blocks generated between the consecutive blocks. In addition to the estimated value the complete histogram of J is generated with its properties in block chain process. The time required for each block creation is T_l and the length of block chain is h_l in which l represents each block. Due to the complexity of time and matrix with number of iterations has the complexity $O(nm)$. Where, m and n is associated with time and block length. By adding SHA-256 to the proposed block chain model, the complexity becomes $O(nm + m^2)$. Then the consensus confirmation can be verified with the proposed model RLAC-FNN in which the complexity required is $O(u, N^2) + O(m^2n^2)$. Where, u denotes the number of layers,N is the complexity of fuzzification process, and actor and critic network complexity is represented with m and n.

5 Conclusion

This paper proposes a new consensus mechanism based on RLAC-FNN and an authentication handover model to improve the user authentication and handover delay in 5G heterogeneous Networks. The credit value has been set to all APs and RL adjusts it in the proposed approach. RLAC-FNN can detect the failure AP and the illegal AP in the consensus network, thereby enhancing consensus delay, consensus network security, energy-saving etc. Finally, in contrast with existing PBFT, CRBFT, network-based model, POW-based model and BAHEPP, the proposed consensus mechanism based on RLAC-FNN has achieved minimum consensus delay, minimum signaling overhead, less energy consumption, less consensus time, and minimum handover authentication delay, considerably.

In the future, a new solution will be determined to enhance the stability of NN and increase the learning process, along with security enhancement to apply in various kinds of blockchain. The proposed handover authentication process is fast and efficient but slightly far away from complete and perfect. It requires several essential consideration for making the system robust and practicable. The proposed approach is affected with noises and channel conditions and hence higher authentication is required with the estimation of better channel conditions. The future work of this research focuses on authentication performance, resource consumption and time latency in unconstrained environment. In addition to that energy efficient protocols will be modelled with mobility management for enhancing the handover authentication through better mobility prediction.

Author contributions All authors have made equal contributions to this work.

Funding No funding is provided for the preparation of manuscript.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest Authors have declared that they have no conflict of interest.

Ethical approval This article does not contain any studies of human participants or animals performed by any of the authors.

Consent to participate All the authors involved have agreed to participate in this submitted article.

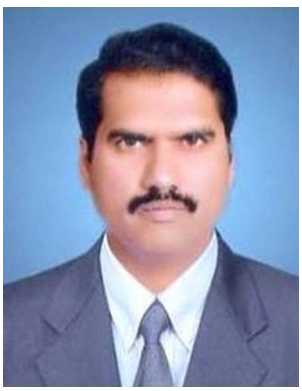
Consent to publish All the authors involved in this manuscript give full consent for publication of this submitted article.

References

1. Alezabi, K. A., Hashim, F., Hashim, S. J., Ali, B. M., & Jamalipour, A. (2020). Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks. *EURASIP Journal on Wireless Communications and Networking, 2020*, 1–34.
2. Zhou, Z., Chen, X., Zhang, Y., & Mumtaz, S. (2020). Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks. *IEEE Network, 34*(1), 24–31.
3. Kumar, A., & Om, H. (2018). Handover authentication scheme for device-to-device outband communication in 5G-WLAN next generation heterogeneous networks. *Arabian Journal for Science & Engineering (Springer Science & Business Media BV), 43*(12), 7961–7977.
4. Zhang, Y., Deng, R., Bertino, E., & Zheng, D. (2019). Robust and universal seamless handover authentication in 5G HetNets. *IEEE Transactions on Dependable and Secure Computing, 18*, 858–874.
5. Alquhayz, H., Alalwan, N., Alzahrani, A. I., Al-Bayatti, A. H., & Sharif, M. S. (2019). Policy-based security management system for 5g heterogeneous networks. *Wireless Communications and Mobile Computing, 2019*, 1–14.
6. Nyangaresi, V. O., Rodrigues, A. J., & Abeka, S. O. (2020). ANN-FL secure handover protocol for 5G and beyond networks. In *International Conference on e-Infrastructure and e-Services for Developing Countries, Springer, Cham*, 99–118.
7. Yang, H., Liang, Y., Yuan, J., Yao, Q., Yu, A., & Zhang, J. (2020). Distributed blockchain-based trusted multidomain collaboration for mobile edge computing in 5G and beyond. *IEEE Transactions on Industrial Informatics, 16*(11), 7094–7104.
8. Mafakheri, B., Subramanya, T., Goratti, L., & Riggio, R. (2018). Blockchain-based infrastructure sharing in 5G small cell networks. In *2018 14th international conference on network and service management (CNSM), IEEE*, 313–317.

9. Serrano, W. (2021). The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities. *Journal of Network and Computer Applications, 175*, 102909.
10. Kausar, F., Sadiq, M. A. K., & Asif, H. M. (2021). Convergence of blockchain in IoT applications for heterogeneous networks. *Real-time intelligence for heterogeneous networks* (pp. 71–86). Springer.
11. Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., & Zhang, Y. (2019). Blockchain and deep reinforcement learning empowered intelligent 5G beyond. *IEEE Network, 33*(3), 10–17.
12. Feng, C., Liu, B., Guo, Z., Yu, K., Qin, Z., & Choo, K.-K.R. (2021). Blockchain-based cross-domain authentication for intelligent 5g-enabled internet of drones. *IEEE Internet of Things Journal, 9*, 6224–6238.
13. Adat, V., Politis, I., Tselios, C., Galiotos, P., & Kotsopoulos, S. (2018). On blockchain enhanced secure network coding for 5G deployments. In *2018 IEEE global communications conference (GLOBECOM)*, 1–7.
14. Hojjati, M., Shafieinejad, A., & Yanikomeroglu, H. (2020). A blockchain-based authentication and key agreement (AKA) protocol for 5G networks. *IEEE Access, 8*, 216461–216476.
15. Abdullah, R. M., Abualkishik, A. Z., & Alwan, A. A. (2018). Improved handover decision algorithm using multiple criteria. *Procedia Computer Science, 141*, 32–39.
16. Sangeetha, D., Selvi, S., & Keerthana, A. (2022). A trust-based handover authentication in an SDN 5G heterogeneous network. *Computer networks and inventive communication technologies* (pp. 841–852). Springer.
17. Divakaran, J., Prashanth, S. K., Mohammad, G. B., Shitharth, D., Mohanty, S. N., Arvind, C., Srihari, K., Abdullah, R. Y., & Sundramurthy, V. P. (2022). Improved handover authentication in fifth-generation communication networks using fuzzy evolutionary optimization with nanocore elements in mobile healthcare applications. *Journal of Healthcare Engineering*, *2022*.
18. Chow, M. C., & Ma, M. (2021). A blockchain-enabled 5G authentication scheme against DoS attacks. *Journal of Physics: Conference Series, IOP Publishing, 1812*(1), 012030.
19. Ren, Z., Li, X., Jiang, Q., Cheng, Q., & Ma, J. (2021). Fast and universal inter-slice handover authentication with privacy protection in 5G network. *Security and Communication Networks, 2021*, 1–19.
20. Jia, X., Hu, N., Yin, S., Zhao, Y., Zhang, C., & Cheng, X. (2020). A2 chain: A blockchain-based decentralized authentication scheme for 5G-enabled IoT. *Mobile Information Systems, 2020*, 1–19.
21. Haddad, Z., Fouda, M. M., Mahmoud, M., & Abdallah, M. (2020). Blockchain-based authentication for 5G networks. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 189–194.
22. Yazdinejad, A., Parizi, R. M., Dehghantanha, A., & Choo, K.-K.R. (2019). Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. *IEEE Transactions on Network Science and Engineering., 8*, 1120–1132.
23. Gharsallah, A., Zarai, F., & Neji, M. (2019). SDN/NFV-based handover management approach for ultradense 5G mobile networks. *International Journal of Communication Systems, 32*(17), e3831.
24. Yang, J., Ji, X., Huang, K., Chen, Y., Xu, X., & Yi, M. (2019). Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet. *IET Communications, 13*(2), 144–152.
25. Chen, Z., Chen, S., Xu, H., & Hu, B. (2018). A security authentication scheme of 5G ultra-dense network based on block chain. *IEEE Access, 6*, 55372–55379.
26. Nabeel, M., Manalastas, M., Ijaz, A., Refai, H., & Imran, A. (2022). Investigating handover behavior with 5G and beyond TurboRAN Testbed. In *2022 seventh international conference on mobile and secure services (MobiSecServ), IEEE*, 1–6.
27. Goudarzi, S., Anisi, M. H., Ciuonzo, D., Soleymani, S. A., & Pescape, A. (2020). Employing unmanned aerial vehicles for improving handoff using cooperative game theory. *IEEE Transactions on Aerospace and Electronic Systems, 57*(2), 776–794.
28. Chen, P., Han, D., Weng, T.-H., Li, K.-C., & Castiglione, A. (2021). A novel Byzantine fault tolerance consensus for Green IoT with intelligence based on reinforcement. *Journal of Information Security and Applications, Elsevier, 59*, 102821.
29. Yan, X., & Ma, M. (2021). A lightweight and secure handover authentication scheme for 5G network using neighbour base stations. *Journal of Network and Computer Applications, 193*, 103204.

Shivanand V. Manjaragi is working as an Assistant Professor in Department of Computer Science and Engineering at Hirasugar Institute of Technology, Nidasoshi, Belagavi, India and he is currently pursuing Ph.D. studies at Basaveshwar Engineering College, Bagalkote Research Centre, Visvesvaraya Technological University, Belagavi, India in the Department of Computer Science and Engineering. He received his Master and Bachelor of Engineering degrees from the Visvesvaraya Technological University, Belagavi, Karnataka, India in 2011 and 2002, respectively. He has published papers in journals, International, and National conferences. His main research interests include Computer Networks, Wireless Networks, Machine Learning, Deep Learning, and Block Chain. He is a member of the CSI and ISTE association.



S. V. Saboji is working as a Professor in the Department of Computer Science and Engineering at Basaveshwar Engineering College, Bagalkote, India. He pursued his B.E. in Computer Science and Engineering from Karnataka University Dharwad in 1997, M.Tech, and Ph.D. from Visvesvaraya Technological University, Belagavi in 2005, and 2013 respectively. His research areas include Wireless Mobile Networks, Wireless Adhoc Networks, Computer Networks. He has published papers in journals, International, and National conferences. He is the reviewer for international journals and conferences. He is a Senior Member of the CSI and IEEE association.