

Blockchain-enabled Authentication Handover with Efficient Privacy Protection in SDN-based 5G Networks

Abbas Yazdinejad, Reza M. Parizi, *Senior Member, IEEE*, Ali Dehghantanha, *Senior Member, IEEE*, and Kim-Kwang Raymond Choo, *Senior Member, IEEE*

Abstract—5G mobile networks provide additional benefits in terms of lower latency, higher data rates, and more coverage, in comparison to 4G networks, and they are also coming close to standardization. For example, 5G has a new level of data transfer and processing speed that assures users are not disconnected when they move from one cell to another; thus, supporting faster connection. However, it comes with its own technical challenges relating to resource management, authentication handover and user privacy protection. In 5G, the frequent displacement of the users among the cells as a result of repeated authentication handovers often lead to a delay, contradicting the 5G objectives. In this paper, we propose a new authentication approach that utilizes blockchain and software defined networking (SDN) techniques to remove the re-authentication in repeated handover among heterogeneous cells. The proposed approach is designed to assure the low delay, appropriate for the 5G network in which users can be replaced with the least delay among heterogeneous cells using their public and private keys provided by the devised blockchain component while protecting their privacy. In our comparison between Proof-of-Work (POW)-based and network-based models, the delay of our authentication handover was shown to be less than 1ms. Also, our approach demonstrated less signaling overhead and energy consumption compared to peer models.

Index Terms—Blockchain, Authentication handover, 5G, Privacy protection, SDN.

1 INTRODUCTION

THE rapid growth of mobile devices and applications along with their processing needs have led to the emergence of the fifth generation (5G) networks. The 5G networks have been introduced with properties like higher bit rate than 10 Gb/s, low latency and increased network coverage compared to 4G [1]. The 5G networks operate through heterogeneous cells and expand overlay coverage [2], [3]. The 5G users, like Internet of Thing (IoT) devices, vehicles, and mobile nodes, when moving from one cell to another, make the handover process activated and if this handover is frequently run, it could lead to a delay in the 5G network [4]. Following a frequent handover, the authentication mechanisms become more involved and may increase the delay time, which contradicts the 5G objectives. Using inefficient authentication handover could cause performance degradation among heterogeneous 5G cells and increases the delay. The power and resource constraints among the Access Points (APs) in cells require low complexity and highly efficient handover authentication procedures

among heterogeneous and homogeneous cells in 5G [5]. The 5G architecture offers technical advantages in communication but has associated technical challenges including, authentication handover, the existence of heterogeneous cells, and privacy protection [5], [6]. Providing network management and security services inside heterogeneous cells can be challenging since mobile users (MU) may leave one cell for another frequently, and specifically when they are dealing with financial and data-sensitive applications.

5G requires taking into account the acceptable level of security in application scenarios and network architecture, especially in validating the facilities and providing their access level to 4G. Also, reducing the delay is one of the objectives and characteristics of 5G. An approach to validate and protect privacy, which is faster, safer and more effective, is essential for the advancement of the 5G networks. For 5G, the security requirements are higher in comparison with previous networks (2G, 3G, and LTE) for which new solutions are required to provide intelligent control across heterogeneous cells for reliable mechanisms and further adoption of the 5G network [3], [5]. Recent advanced technologies like SDN/NFV and blockchain [7], [8] have recently received a lot of attention for the advancement of the next generation of wireless networks.

In SDN, the control plane is separated from the data plane, and its controlling part can meet the controlling needs in 5G, as the SDN is a new architecture of the network, with properties like programmability and flexibility in networks management for testing new ideas [9], [10]. The infusion of SDN in 5G is beneficial because, in the future, mobile networks would be going towards more scalability requiring

- A. Yazdinejad, was with the Faculty of Computer Engineering, University of Isfahan, Iran. Email: abbasyazdinejad@yahoo.com.
- R.M. Parizi is with the Department of Software Engineering and Game Development, Kennesaw State University, GA 30060, USA. Email: rparizi1@kennesaw.edu.
- A. Dehghantanha is with the Cyber Science Lab, School of Computer Science, and University of Guelph, Ontario, Canada. Email: adehghan@uoguelph.ca
- *K.K.R. Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio Texas, USA. Email: raymond.choo@fulbrightmail.org (Corresponding author)

better management and flexibility [9]. SDN flexibility could potentially benefit 5G applications, in terms of quality of service (QoS), machine to machine (M2M) and human to human (H2H) communications [9]. Applying blockchain, on the other hand, can also allow us to better respond to some of the security challenges in 5G [7]. Specifically, a blockchain is a fraud-resilience, distributed ledger that records all transactions in a 2P2 network. The blockchain has a decentralized architecture, and its popularity in cryptocurrency world in securing distributed communication has been remarkable [11]. Blockchain can play an important role in facilitating secure communication between mobile users in 5G, for example by removing intermediaries for authentication, reduction in transaction cost, and global accessibility for all users [12]. In other words, we posit that SDN and blockchain can be combined to facilitate us to provide enhanced privacy protection and security in 5G. Blockchain technology is more widely known in financial [13] and supply chain applications [14], but its adoption is limited on 5G mobile networks and mobile services because of its resource-intensive consensus and validation protocols, mainly Proof of Work (POW) [15]. POW requires significant energy and processing time, which is not appropriate for mobile users, especially on the 5G network [15]. Having said that, the blockchain should be compatible with the 5G specification to be effective, and thus, we use an upgraded Delegated Proof of Stake (DPOS) algorithm in this work.

In this paper, a blockchain-enabled authentication handover approach with effective privacy protection is proposed for the 5G within SDN platform. In the proposed approach, users obtain a quick and secure connection by eliminating re-authentication among handovers operators between heterogeneous cells with a low delay. Demonstrated in experimental results, the comparison between authentication delay with POW-based and network-based models, and the delay of our authentication handover shown to be less than 1 ms, making the proposed approach well suited for 5G. In addition, our approach showed to have less signaling overhead with better energy consumption in compared with POW-based and network-based models. This was achieved by applying the upgraded DPOS algorithm, which has been shown to be scalable and energy-optimized and effective in reducing latency as opposed to POW.

The rest of the paper is organized as follows: The proposed architecture of 5G with a heterogeneous cell of SDN and blockchain on the 5G is described in Section 2. The blockchain-enabled authentication handover mechanism for 5G is presented in Section 3. The effective privacy protection in SDN based 5G network is discussed in Section 4. Section 5 defines the DPOS algorithm used in blockchain component. The simulations results and evaluation are presented in Section 6. Section 7 presents the related work and finally, Section 8 gives the concluding remarks.

2 THE PROPOSED ARCHITECTURE OF 5G WITH A HETEROGENEOUS CELL

In the proposed architecture, the blockchain and SDN are introduced into the 5G network to simplify and eliminate the frequent handover authentication into small cells and heterogeneous networks. The overall model of architecture

is shown in Fig. 1. The blockchain center (BC) is located in an environment outside and near the cells or heterogeneous cells and is applied as a space for storing and producing an encryption of parameters like the device identification, certification, and unique data related to the device under the alias. Encryption materials are applied to protect privacy and security. BC is involved in this architecture as follows: 1) the initial registration, the new devices require initial registration when they first want to enter a cell or heterogeneous network, 2) changing identity information, devices may change their alias when passing through a cell to another, thus their encrypts, therefore, BC generates new encryption for identification and validation in other cells, and 3) Hostile cancelation, in BC, malicious behaviors are detected by using blockchain lookup. The identity of the adversary is publicized once the malicious behaviors have been confirmed by BC among Cells. The BC is a public ledger that any MU can register into it, which is approved and recognized by mobile operators. Only MU who are known to mobile operators have permission to register in BC. In our architecture, we used a public blockchain to facilitate collaboration among various mobile operators who can select and approve associated MU with the chain in BC. In the blockchain, any MU can be part of the network and can have their own private and public keys. Moreover, all SDN controller candidates can be involved in consensus mechanism and can also check and validate all transactions within the 5G network.

Heterogeneous network management and flexibility of the SDN structure is applied in the proposed architecture to increase programmability. The SDN controller is prescribed for the overall control cell or heterogeneous network. The SDN switch deals with the data transfer and behavior change in the network by following the controller commands. By separating the data plane and the control plane in the SDN, defining the protocol, functions, and policy on the 5G network becomes possible [9,10]. The SDN controllers in this proposed approach are one network and can communicate with each other and BC, and like Bitcoin, the information inside secure messages is exchanged as encapsulated transactions among them. Transactions and messages from BC can be shared through the dedicated transfer keys to the controller. Each SDN controller has a dedicated transfer key received from BC and is applied to transfer and receive information. Scalability is an important problem in SDN, and we have solved it through a hierarchical structure between SDN controller and BC in our architecture. Not only the SDN controllers are one network that can communicate with each other (as another layer) but also they are being managed via BC (as a higher layer). If any SDN controller becomes down in a cell, the system will then manage this cell via another SDN controller in the network between SDN controllers. In this architecture, it is assumed that the data center of the mobile operator has the information of BC and SDN controllers can be controlled by mobile operators. The objective is to achieve an effective, secure and fast mechanism for authentication handover among the 5G network. In our BC, we have applied the optimal DPOS algorithm [16] for energy consumption and speed boosting during transactions.

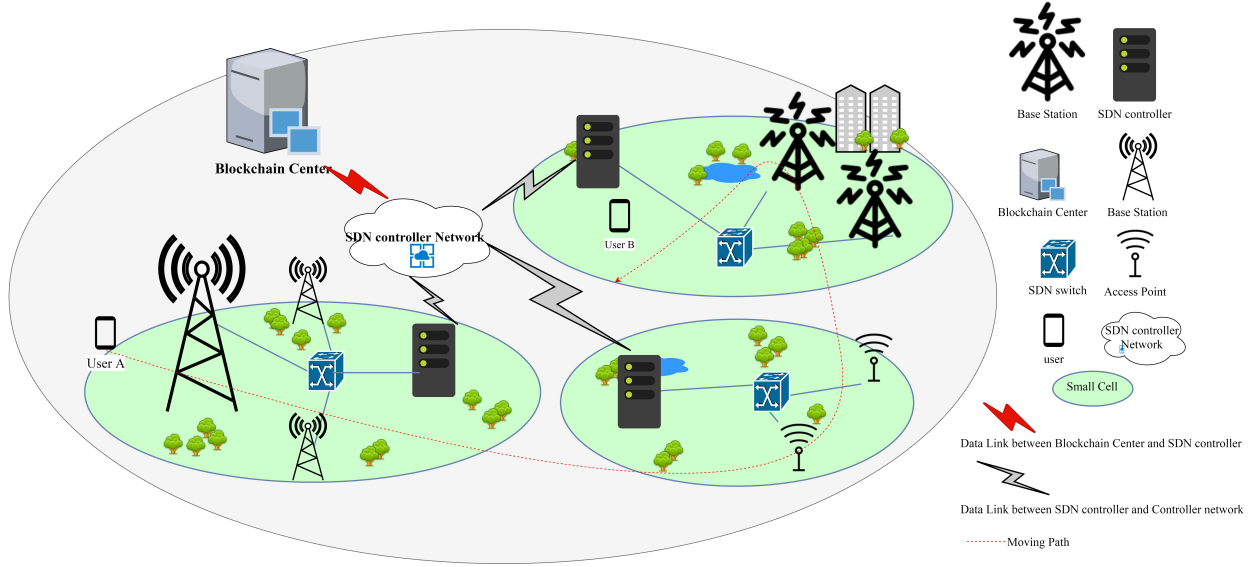


Fig. 1. The proposed architecture of blockchain-enabled handover in SDN-based 5G networks with heterogeneous cell

3 BLOCKCHAIN-ENABLED AUTHENTICATION HANDOVER MECHANISM FOR 5G

By applying BC and SDN, a handover mechanism is designed for transmitting the key for authentication in the 5G with eliminating re-authentication among handovers between cells. Fig. 2 shows the relationship between BC, SDN, and AP/BS in our approach, and gives the main components forming BC including a ledger (to store and maintain data), Auth_Control and Sec_info units.

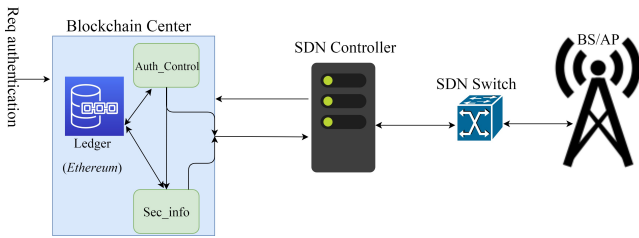


Fig. 2. Relationship among BC and SDN and AP/BS structure in the proposed 5G network

Initially, the mobile users (MU) are registered in BC to generate encryption material based on their properties and then receive the key and encryption properties, and BC sends a vector containing the MU information to the SDN of that cell in a simultaneous manner. BC assigns two public and private keys to each users mobile. As shown in Fig. 3, the mutual authentication between user and BC occurs in procedure 1. The MU sends the request of joining the BC to enter the given cell or domain. This request is received by the *Auth_Control* unit in BC and sent to the MU after it is confirmed; meanwhile, another unit in BC named *sec_info* sends the data of this MU to the SDN controller in that domain or cell.

In this context, the *Auth_Control* inside BC is applied to identify the unique MU information like identity, location, direction, physical layer properties, RTT, and public and private key assignment.

Through the *sec_info* unit, the messages are sent to the SDN controller safely in capsuled packages. Specifically, a set of information from the registered user in BC like the public key is sent to the SDN controller of that and other cells.

The SDN controller is responsible for MU management and defines the invoices for the SDN switch tables in a cell. It also stores the APs in the cell to validate the key, and the MU, and then the MU joins the cell. If for any reason the MU wants to handover from the existing AP to another AP in the same cell, the existing AP makes the SDN controller arena and the MU sends the associate request to the target AP and then becomes disconnected with the existing AP. In general, the unique characteristics of MU are shared among current and adjacent cells, thus, there will be no need for re-authentication when passing through heterogeneous cells. As to direction and speed, the SDN controller can recognize the next cell, which in turn informs the BC. The BC checks the *sec_info* unit to ensure that the MU is a trusted cell. A handover process between the two heterogeneous cells for the 5G network is presented in Fig. 3 (Procedure 2). After registering the MU, BC sends its information to the SDN controller of the cell and its adjacent cells, which can be heterogeneous. The SDN controllers in each cell run MU validation operations on APs. The MU is registered in the available cell and intends to go to the neighboring heterogeneous cell that sends the request to the AP of the same cell. The AP then communicates to the controller and accepts the MU request as BC has already considered it as a valid SDN controller in that cell.

The SDN controller informs BC of its position and, after disconnecting from the current AP, the controller of that cell is notified. The public key P is known between the MU and the AP, and it is capable of switching between the APs of a cell. The private key Q is applied in signing transactions and decoding data for privacy protection.

An SDN controller in a cell has already validated this public key among AP or BS. The BC sends messages to other adjacent public key cells, to eliminate the need for repeated

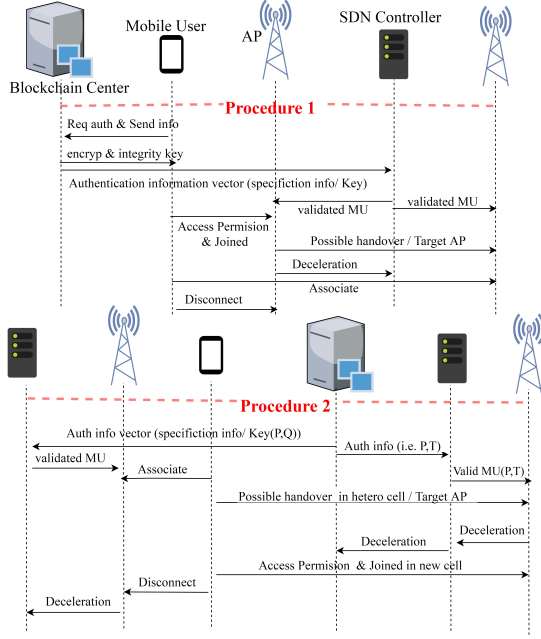


Fig. 3. Registration procedures and behavior in a cell

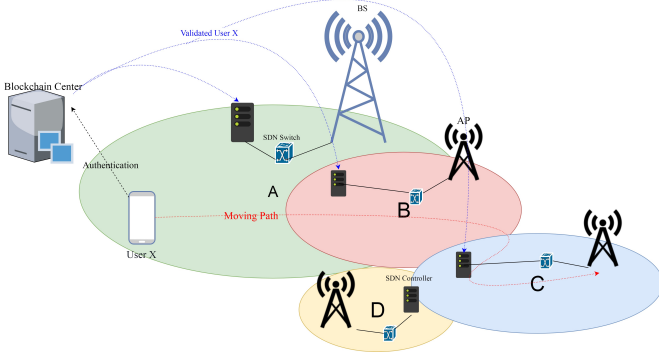


Fig. 4. The process of entering and moving among heterogeneous cells in the proposed 5G network structure

re-authentication in these heterogeneous cells. This mechanism accelerates the authentication process when passing through few heterogeneous networks and APs, and reduces latency. In general, cells receive sensitive information for this mechanism from *sec_info*. The *sec_info*, depending on the speed, the direction of travel and the position considers timeout named T and makes the cell controller aware of this. The AP based on this T waits for the MU entry or its displacement among the APs. If T is over and there is no effect on its request to the AP, there is a probability of compromise behavior of which the BC becomes aware, and this follows the assessment of the status of its transactions and even the possibility of blocking, where this blockages will be reported to other SDN controllers. Specific user information like IP, physical layer properties, position, velocity, and direction of movement within the cell are collected and the SDN configures the flow controller tables according to the given policy, in a sense that it identifies the location of the next cell controller, which accelerates the authentication process and removes the re-authentication process in entering into other cells, as shown in Fig. 4. An

authentication procedure is applied between the user X and BC, then, user X join the cell A, which is implemented by BC-enabled based on the base SDN structure described in Algorithm 1. Handover authentication does not require any change in user authentication hardware and, similarly, after being registered in BC in other adjacent cells in the direction of the MU, it is run to eliminate the need for repeated authentication when entering cells B and C, which reduces the latency, by removing re-authentication. By predicting the MU route, the SDN controller is ready to serve the MU.

Algorithm 1 User X authentication handover

```

1: Initial register : User X // in Blockchain Center (BC)
2: User X → Req authentication and Send info
3: BC → Send(auth_User X info(spec_info/ Key))
4: User X: receive (encryption & integrity key)
5: BC → Send(User X vector to Predicted Cell) // SDN controller in near cells
   receive info
6: SDN Controller: validated User X // in APs
7: User X → Associate (State A)
8: SDN Controller → Monitor User X
9: SDN Controller: Message (BC) // send info to BC
10: BC: Message (SDN controller Net) // send info to SDN controllers
11: if (Mobility or migration)
12:   if (Possible handover (Target AP)) // in same cell
13:     SDN Controller: Message (BC) // send to BC
14:     Update(Switch Flow Table)
15:     User X → Handoff (current AP, Target AP)
16:   else
17:     SDN Controller: Message (BC) // send to BC
18:     Update(Switch Flow Table)
19:     User X → Handover (current AP, Target AP) // in other cell
20: end

```

3.1 Managing BC Keys in Handover

The structure and content of BC provide an approach to managing the key in the 5G heterogeneous cells and networks, which in turn reduces key transfer time among cells for users handover. The focus here is on the BC on the management of keys in heterogeneous cells to achieve a scalable and light-weight transfer mechanism through the BC. The duty of the BC is to remove a third party (intermediary) in transactions. Key transportation handshake can be eliminated by applying the BC mining method, that is, the messages are approved by the BC instead of the third party.

The BC structure the excess additional units in the handshake process for validating and authenticating the authenticity of the previous and traditional methods. The handshake process according our approach is shown in Fig. 5. The collection period (CP) allows multiple transactions to be broadcasted to BC, where T_{cp} is the transactions time to BC. Signatures are processed in transactions to assure whether the information in transactions are trusted or not. By applying the public key, the messages are exchanged between the user and BC and only the cryptographic transaction remains to reach the destination and be opened with the users private key. As observed in Fig. 5, $T_p + T_m$ contain the delay emission time and the mining process. T_k is the transmission and distribution time of the public key among controllers and the attributed controller key.

In Fig. 5, T_i is the time to send the user's unique information and features to the controller. T_{cb} is the time to send data from the controller to BC. The key processing time (T_{total_key}) during handover in 5G heterogeneous cells, which includes public/private key emission for the user and

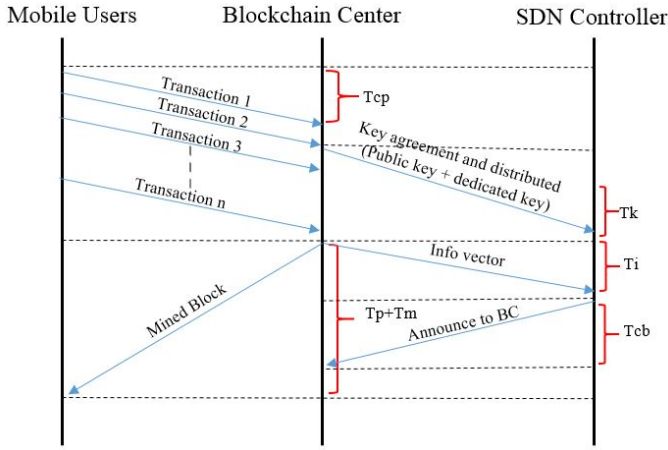


Fig. 5. The key transmission for BC structure

the attributed key to the controller in the BC structure to support the handover in heterogeneous cells, is obtained through Eq. (1).

$$T_{total_key} = [Nt \times Tcp] + Tk + (Tp + Tm) \quad (1)$$

where Nt is the transaction count obtained through Eq. (2). Ncp is the transmitters' theories count n is the requisitions count registered in BC at every m minute. Nt is expressed in Eq. (2).

$$Nt = \frac{(n \times m)}{60s} \times Ncp \quad (2)$$

In T_{total_key} , Ti and Tcb are not contributive in transmitting keys, and are implemented in a co-procedural manner in the key transfer process. Transactions time collection is optimized with a minimum of key transfer time.

3.2 Dynamic Key Management in Handover

We should be able to manage keys attributes within BC in a way that is compatible with 5G goals by the transaction collection period (Tcp). Dynamic key management in handover in 5G cell is achieved by using our dynamic Tcp . To decrement the side effect of variables, the approach of detection variable is engaged in our scheme.

We consider 1ms for pattern metric to measure the efficiency of different collection periods. Thus T_{total_All} is a sum up number of transactions in BC. $Nt-1$ is the average processing time in 1ms under different collection periods. Basing on the Equation (1) and (2), we can derive the number of transactions on n cells as Equation (3).

$$T_{total_All} = [(Nt \times Tcp) + Tk + (Tp + Tm)] \times n \quad (3)$$

Estimated key transfer time is calculated apply different collection periods. The optimized Tcp time is elected according to the minimum key transfer time. The Tcp is presented in Algorithm 2, where it is applied in the BC for key transfer.

4 EFFICIENT PRIVACY PROTECTION IN SDN BASED 5G NETWORK

Data privacy implies the right to separate network users from threats and retaliations against their data. By reducing

Algorithm 2 Optimize TCP

```

1: BC (Received (TCPi)) // TCP1, TCP2.. TCPn
2: BC = Accounting(mining)
3: BC → initialize (SDN Controller)
4: SDN controller → Announce to BC // Path traffic
5: For (i=0; i=n; i++) // n is number of transactions
6:   Call Equation0 // Calculate the number of transactions (Equation 3)
7:   Calculate (Ti)
8:   Call Traffic cell (Pi)
9:   Tcp[i] → Tcp
10: End for
11:  $Tcp^M = \min(Tcp)$ 
12: Return  $Tcp^M$ 
13: end

```

the size of the 5G heterogeneous cells and networks, users may move among many cells before the communication session is completed, and may be trapped in non-trust APs or become compromised during handover. Privacy protection is a challenge in 5G. The available approaches [5], [17] for privacy protection apply a complex key agreement, mutual interaction, by adding signs to protect data, which could lead to latency, and introduce computational load encryption and complexity to the AP [18], something not appropriate for small and low power 5G cells. The multiple requirements and the existence of the third party as are considered as a bottleneck in privacy protection, not fit for 5G. By applying the encrypted keys in BC during the communication process, if reading a record is sought, the private key associated with it should be known. In any situation where the attackers do not have the key, and what they get is useless.

In our approach, SDN controllers can select multiple paths for transmitting different parts of the data stream, according to heterogeneous network coverage. Based on the applications, some of the network paths are more sensitive and should be selected. As long as the user is authenticated and be in the networks coverage, the stream is routed through the controller of that cell, and decrypts the user data based on his private key, and then reorganizes the stream received from multiple paths. The proposed approach is capable of determining free traffic and network paths through the SDN controllers, something suitable for the 5G network. By choosing multiple routes between APs or femtocells in data transfer, the traffic on the 5G network would be reduced. The privacy protection mechanism where SDN and BC are presented in Algorithm 3. In this algorithm, K

Algorithm 3 Blockchain-enabled Privacy Protection using SDN in 5G

```

1: User A → Announce to SDN controller // User A wants to send information to User B
2: If (user A == authentic in BC && trust in cell)
3:   SDN controller → Announce to other
4:   SDN controller (Check other traffic cells)
5:   SDN controller → calculate (optimize (path))
6:   SDN switch → update flow table()
7:   User A = Allocate (WK) // allocate bandwidth to user form SDN controller
8:   User A → Encrypt (send data (dK)) // encrypt and send data parts to SDN switch through AP
9:   VK = min (Ts, tr) // size in bytes to be transferred with TS
10:  SDN switch → forward data // base policy
11:  SDN Controller = monitordatatransient(User B)
12:  User B → Received (data)
13:  User B = Decrypt (data) // using private key and re-organize data
14: else
15:   Add to block()
16: end

```

is the count of the network paths that the SDN controller selects for data transfer. The symbol dk is a different data section that can be sent in K directions in a simultaneous manner. The symbol tr is the time of data transfer inside the involved cells. T_s is the delay threshold for 5G applications. For example, some services like transferring email that can withstand a long delay or online games with a slight threshold of delay before T_s is required. WK is the bandwidth allocated by the SDN controller in accordance with the traffic situation of different networks, and VK is the transmitted data volume in multiple paths with the delay of the delay threshold application. The count of K paths here is through the balance between the privacy level and the complexity of the adjustable system through the SDN controller. Privacy protection for users is programmable through the SDN controller, and the advantages of BC are essential for future requirements.

5 CONSENSUS ALGORITHM USED IN OUR BC

In order to verify and record every transaction in open blockchains, it has to go through consensus process. POW [18] has been mainly the consensus protocol used in a many decentralized platforms including Bitcoin and Ethereum, which could be problematic in 5G environments due its high computational power and latency [15], [16].

Also, the original DPOS has the limitations of vulnerability to centralization as the number of evidences is limited, and being exposed to fault of real-life voting. To address this issues in our approach, we have solved the DPOS limitations [16] in our upgraded DPOS algorithm with the help of SDN controllers in any cells and the network between them in the our proposed 5G architecture.

Our mechanism acts like a board of directors where SDN controllers in the cells vote on a number of SDN controller candidates, in a sense that they would be responsible for verification and billing. In general, for constructing each block, SDN controllers are applied for electing representatives who would produce blocks based on collaboration. Representatives monitor each others performance, and when one is out of line is either omitted or does not get votes. DPOS can reduce the count of the nodes associated with the authentication and accounting process in a significant manner.

In our context, the SDN controllers perform transaction processing and the addition of a new block to the BC. When the SDN controllers miners succeed, they can receive a certain volume of information of their interest as a reward, indicating that the miner is the processor of the information he/she is interested in. Miners are nodes that control a large amount of information on the network, because in each cell the controller monitors users. It is possible that someone else would be interested in this information, in this situation, the user can request from the miner for this information, in a sense that the miner verifies the access control policy in the BC and then shares the data. Here, the advantage is that the user will delete the decryption process after the verification. The benefits of DPOS include cheap, scalable, energy-efficient transactions. A partial centralization in devising creation of the blocks makes this algorithms functionality better than its counterparts. Devising a new block in Bitcoin

takes only 10 minutes, while the EOS, by applying DPOS, do the same in less than one second [16]. Algorithm 4 shows the mining procedure in our approach.

Algorithm 4 upgraded DPOS Algorithm

```

1: BC = Get_info (H, VB, HPre, tstamp, S, Trans) // BC strat updating and get
   require info like, ( H: Block Header, VB: Block Version, HPre: Previous Block Hash,
   tstamp: Timestamp, S: number of SDN controllers, Trans: transactions Trans = [T1;
   T2:::Tn] )
2: Group_Agent = Voting() // select group of agents for mining
3: BC → Announce (Candidate mining) // sending require info to agent
4: Initialize bool variable K = False
5: Integer P = 0;
6: While (NOR K) do
7:   transaction order = random(n) // range [1:n]
8:   Calculate (Merkle tree root (Root_P))
9:   Root_P → basing on the transactions in payload
10:  Create hashed block header ( Hn = VB||HPre||tstamp||S||Trans)
11:  while (NOR K & NOT got DPOS) do
12:    Group_Agent → mining(block);
13:    Create header: Hverify= VB||HPre||tstamp||S||Trans;
14:    The string to Hn= Hverify||nonce;
15:    Result = hash(Hn || nonce)
16:    Cooperate (Group_Agent)
17:    Extract nonce = getNonce(Hn);
18:    RootP basing on the transactions in Bpayload
19:    nonce ++ ;
20:    if (NOT got DPOS) then
21:      Group_Agent → mining(block);
22:      P= (nonce - 1) into nonce field
23:      Return (nonce - 1);
24:      K= true;
25:    else if (receive DPOS) then
26:      Group_Agent → mining(block);
27:      K= true;
28:    return NULL;
29:  end if
30: end while
31: end while
32: If (Miner == success) then
33:   Miner (i) = Resive_data_interest ();
34:   Share_data (Miner(i));
35: } }
36: end

```

6 EVALUATION AND RESULTS

Experiments are run to evaluate the delay, efficiency, and comparability of the proposed approach. The results are obtained through OMNeT ++ 5.1 [19] with the INET 3.6.4 framework. The INET framework, which is involved in the implementation of the SDN switch and controller, can support the SDN [20] and the BC function [21]. The BC encompasses the consensus algorithm (DPOS) for users in the 5G network. We define certain categories of messages among BC and cells to help achieve a common view of the blockchain among all participating MU.

- *Ini_reg (net id, Loc, Dire, from, phys_ly, Rtt, to), Ini_reg_ack (peer list)*: Allows the users to discover BC and broadcast their information among near cells.
- *Get_block_list ()*: Request from BC, the list of blocks available with number of SDN controllers for mining.
- *Get_tran_list()*: Request for transactions in the cells (not yet mined into a block).
- *block(block_header, tran_list)*
- *block header(hash, timestamp, miner, merkle root)*
- *tran(in_list, out_list)*: Transactions have a list of inputs in each cell which it is spending, and a list of outputs which it creates in that cell.

In order to warrant that all MU have a uniform view of the blockchain, we define and consider the rules followed

by the BC so as to get consensus. We define a MU in the 5G cell by the tuple $(Ini_reg, P, Q, T, firmware)$, where (P, Q) is the public and private key pair for the MU, firmware is a function use defined algorithm in our approach. To evaluate the feasibility and performance of our proposed model, we define the following metrics to measure the feasibility of our proposed model:

- T_{tran} : Transactions added to the blockchain.
- T_{block} : Blocks added to the blockchain per second by SDN controllers via DPOS algorithm.

To evaluate the comparability of the proposed approach among heterogeneous 5G cells, a network containing 30 heterogeneous cells with a distance of 200 meters between the two APs in two cells and the MU with 5KM /h speed change and direction of every 3 seconds were selected. In each cell, the controller updates the flow tables of each cell, based on the parameters of the users who register in BC. The details of the simulations are presented in Table I.

TABLE 1
Stimulation parameters

Simulation Parameters	Values
Simulator	OMNeT++ 5.1 with INET 3.6.4
Number of Cell	30
Number of request/response to BC	2000
Number of Transactions	1200
Number of SDN Switch	90
Number of SDN controllers	30
Cell radius	100 m
User mobility speed	5 Km/h
User mobility direction	Random
Total number of users	600
distance between two AP	200
Length of packets registered in BC (M)	32 byte
Length of packets from BC to the controller(N)	16 byte
Transmit power (Pt)	1726 mW
Receiving power (Rx)	1340 mW
The influence of the number of miners	$N = (\mu_t = 1500, \sigma^2 = 4)$
Block Size	4 byte
Transaction Counter	1-9 byte
Block Header	80 byte
Prev_block_hash	32 byte

Signaling overhead: it contains a pattern or additional information to enhance performance of the wireless communications. It is related to registering the MU in BC. This is to be compared with the network-based signaling overhead and POW-based models, which use POW [22]. This method is similar to that of [22]. Here, Eq. (4) is applied for this analysis.

$$Signalingoverhead(Sover) = \frac{(B \times M)}{t} + \frac{(N)}{t} \quad (4)$$

where t is the time and B is the count of steps between MU and BC. M is the length of packets registered in BC and N is the length of packets sent from BC to the controller. As results indicated in Fig 6, our proposed approach has less overhead than the network-based and POW-based models because the DPOS algorithm was applied in our work together with the SDN controllers for managing each cell.

In the POW-based model where POW is applied it has extra overhead and does not allow the SDN controllers to be

applied in mining the handover. The network based method requires the third party in communications and a variety of authentication servers among heterogeneous cells in a 5G network. As observed in Fig. 6, an increase in time increases the signaling overhead because there are more requests for registration and authentication among cells. Our approach has less overhead than its counterparts because it is directly registered in the BC and joins the cell with no need to interact with other nodes.

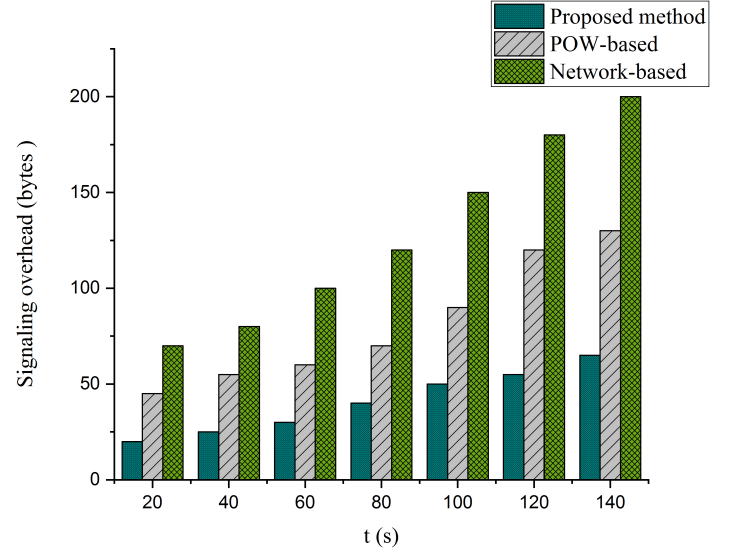


Fig. 6. Comparison of signaling overhead of our approach with the network-based and POW-based models

Energy Consumption: In all subject models, if the transmit rate Ctx is the transmit rate and Crx is the received rate, the energy consumption is calculated through Eq. (5).

$$E = (Ctx \times Pt \times t1) + (Crx \times Rx \times t1) + (Pr \times (t - t1)) \quad (5)$$

where Pt is the transmit power, Rx is receiving power, $t1$ is the connection time, and Pr is the received power. The energy consumption for the whole network is calculated through Eq. (6), where the signaling overhead must be applied as well:

$$En = (n \times c) \times \left[\left(\left(\frac{Sover}{B} \times a1 \right) + a2 \right) \right] \times Pt \times (Ctx \times Crx) + (Pr \times (t - t1)) \quad (6)$$

where n is the count of heterogeneous cells, c is the count of the controllers and $a1$ and $a2$ are power constants. The comparison results of the energy consumption of this analysis presented in Fig. 7. According to the figure, in the network-based model, the MU reaches to the third part that is responsible for authentication and needs three handshakes in a few steps. In the POW-based, more energy is consumed on POW in comparison with our proposed approach.

The influence of the number of miners in our approach: Here, it is assumed that the mined blocks size through the

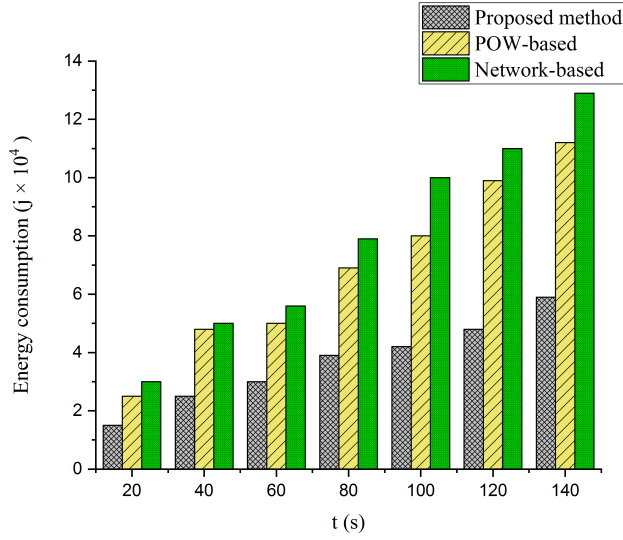


Fig. 7. Comparison of the energy consumption of our approach with the network-based and POW-based models

miners are of the normal distribution, $N = (\mu_t, \sigma^2)$ and its function is expressed through Eq. (7).

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \quad (7)$$

The values of the parameters are $\mu_t = 150$ and $\sigma^2 = 4$. The effect of increasing the miners count on the total service demand indicates the normalized rate of the provided service. These services include consensus-building by miners through the DPOS algorithm and sharing information for users and BC. Fig. 8 shows the results of this analysis.

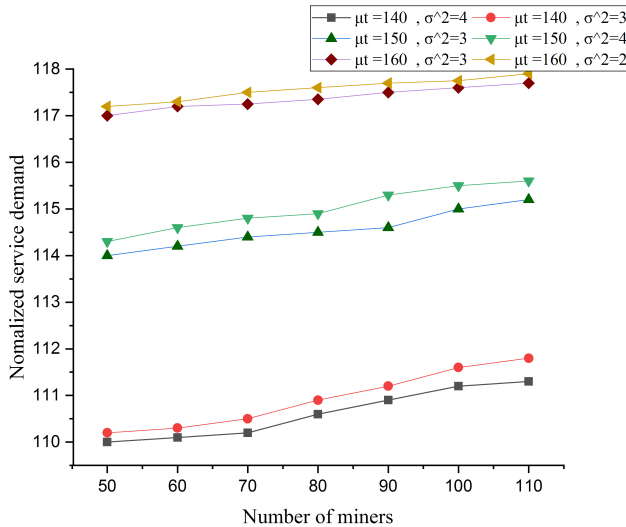


Fig. 8. The effect of the miners on the offered service rate

The reason for the increase in the miners count is the increase in the heterogeneous cells count in the 5G and the possibility of further coverage of the network that is, providing more service. The more the count, the more the miners,

indicating that more delegates will collaborate to reach a consensus, thus a reduction in the delays. An increase in μ_t rate increases the demand for service because this increase in μ_t increases the average size of a block ending in the miners rewards.

Privacy efficiency preserving: In this particular analysis, our approach was compared with the two SEMR-ABE [23] and DACC [24], as shown in Table II. T_e is the time for one exponentiation, and T_c is the constant time. S is the text code size, and f is the code attribute. In our method, something that the user does not need is a cryptographic operation but decryption, thus no overhead as applying the BC properties fits 5G with less delay.

TABLE 2
Comparison of Transmission Traffic and Calculation Time of our approach with DACC and SEMR-ABE for preserving privacy

Scheme	Size of Password text	Decryption time	Revocation message	Transfer security
DACC	$(3f + f)S$	$f \times T_e$	$f \times S$	no
SEMR-ABE	$L^2 + (f \times s) + s$	T_e	T_e	Yes
Our method	S	T_e	T_c	Yes

The efficiency of Algorithm 3 is measured in two aspects: delay and bandwidth. In case that the source and destination are not for transferring files between adjacent cells, and there are other heterogeneous cells among them, there are K paths via which a SDN controller deals with the file transfer in terms of latency, bandwidth, and data volume. Proposed algorithm has less delay than the network-based (it does not consider traffic and delay threshold). As illustrated in Fig. 9, network-based increases the delay by increasing the data size because the packets are in queue, K represents the number of different paths in our method for sending, and the SDN controller simultaneously sends data from different paths to reduce transmission delay. Also, the effect of this can cause the decrease of consuming bandwidth during transferring packets among cells. As shown in Fig. 10, with the increase of packets transferring at the path between source and destination in a cell, the proposed method is more efficient than network-based as the algorithm considers traffic of another cell and sends packets through efficient path. Here we considered an average of consumption bandwidth in the path with various $K=(2,3,4)$.

Handover execution time: The assessment of authentication handover delays in our approach is compared with both POW-based and network-based models. In POW-based method, users must be registered in the blockchain and upon repeated displacements among the cells become re-authenticated in the cell. These two methods require re-approval and separate protocols among heterogeneous cells for authentication.

In our approach, the user does not need to be re-authenticated when being replaced among the heterogeneous cells because they are valid in adjacent cells and easily handover, removing the re-authentication delay. The comparison between our authentication delay and the other two methods based on the utilization rate in the 5G network is shown in Fig. 11. In this context, network efficiency is the total data volume reached the processing rates ratio in BC and SDN controllers. The network productivity rate

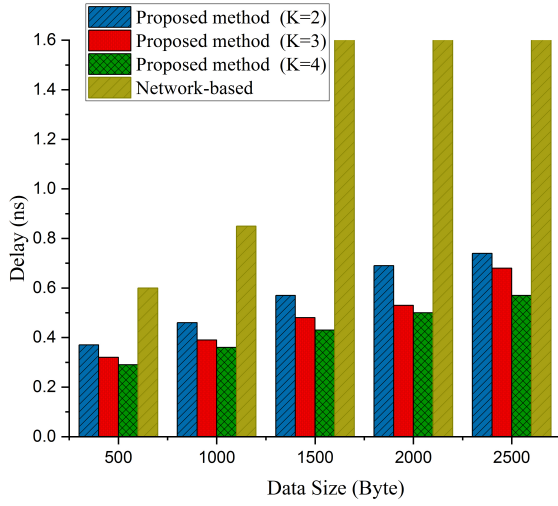


Fig. 9. The efficiency of delay measured between proposed method and network-based model

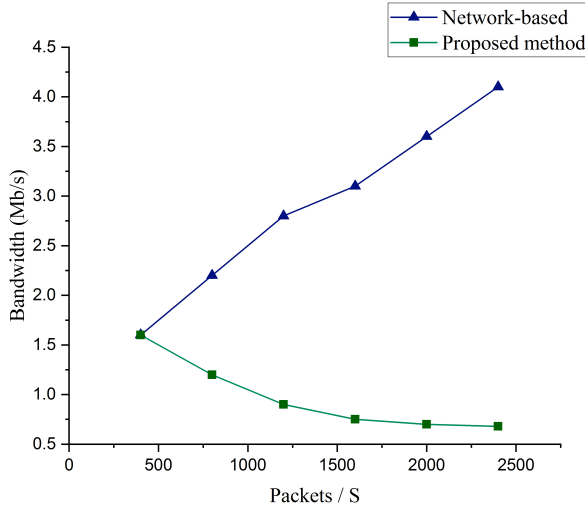


Fig. 10. The efficiency of consumption bandwidth measured in a cell between proposed method and network-based model

is defined as the different load conditions in the network. When the network load is low, the authentication delay does not have a problem in our approach and other methods. But, when the count of the users increases and there is mobility among the cells, and the data transmission operation is run, the network load increases in the other two method as opposed to our approach, which resulted in a delay less than 1ms making it suitable for 5G.

Processing Time of Cryptographic: In this analysis, the time spent on cryptographic is assessed with the objective to apply Eq. (1) and algorithm 2. For this purpose, the key transfer time must consider the cryptographic approach. The efficiency of the cryptographic approach where the key transfer procedure was taken into account. Except for the mining process, an increase in transactions count, the processing time increases in a linear manner. The mining

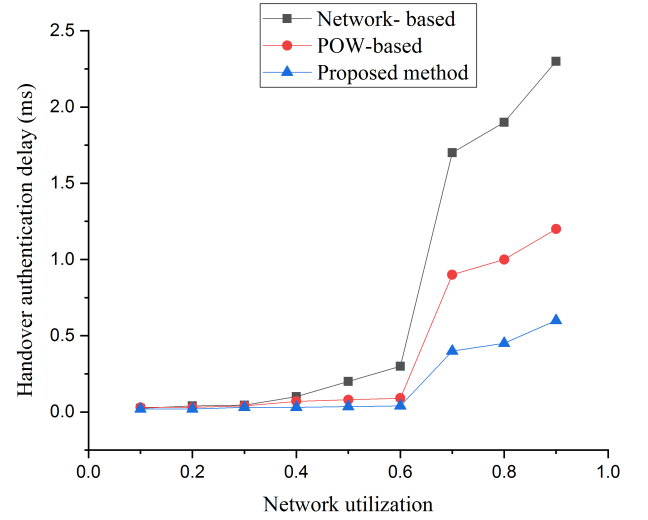


Fig. 11. Comparison of handover authentication of our approach with the network-based and POW-based models

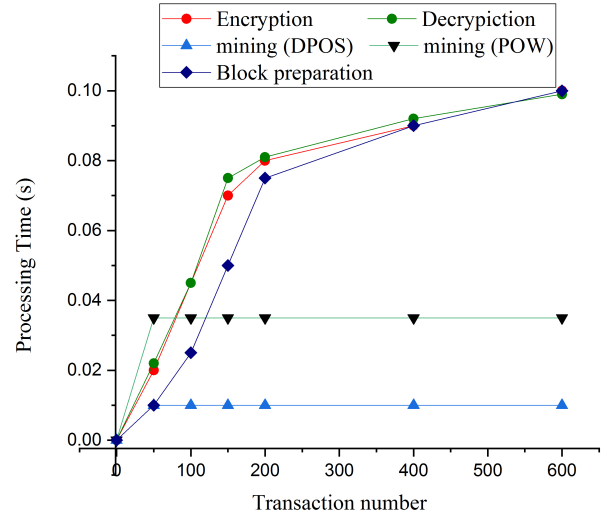


Fig. 12. Cryptographic time-out assessment through a key transfer procedure

algorithm is always a mined header, containing multiple transactions. The processing time of mining is the mean value of multiple simulations. The processing time of DPOS and POW are shown in Fig. 12. Due to the cooperation of representatives (30 representatives here), DPOS reaches a consensus in less time.

Attack model: We have considered two classes of attacks.

- *Class 1 attacks:* DOS/DDOS attacks like, UDP Flood, SYN Flood, TCP Flood which are common in the network level [25].
- *Class 2 attacks:* Those attacks that can occur when MU want to join cell or BC like, ID spoofing, Authentication attack, Link-ability attack and Numb attack

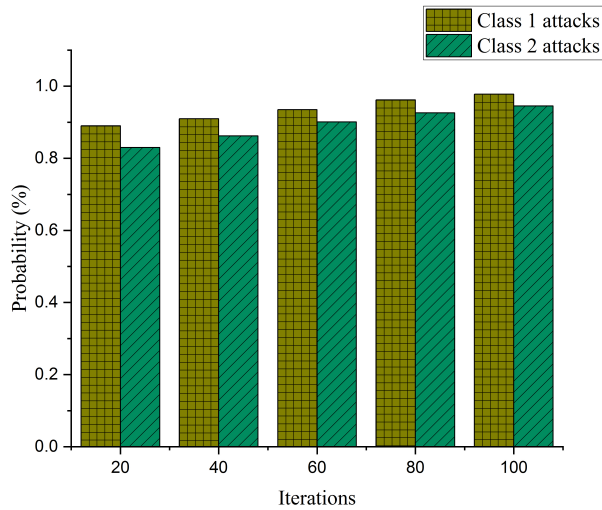


Fig. 13. Percentage of attack detection probability in the proposed architecture

[26].

Attacks in class 1 usually execute by MU in cells after joining and registering in the network for running down infrastructure in the cells. BC and SDN controllers usually face with attacks in class 2 since these attacks work with BC and SDN controller directly. For example in Authentication attack, MU frequently wants to join BC or other cells with malicious behavior, or wants to join network with fake or block ID for communication with other MUs. For assessing the attack detection capability of the proposed architecture, in the simulation we assumed that in 20 cells there were 400 MUs, 50 of which were malicious (i.e. occupying bandwidth by sending duplicate packets) and 100 AP (20 under compromise and file transfer barriers). In our scenario, if AP is compromised and the MU attacks (i.e. class 1 or class 2 attacks) inside the cell, the SDN controller is able to detect it based on traffic generated, packet type, and consumed bandwidth. The SDN controller is also able to detect the attack and notify BC and other SDN controllers based on the patterns defined by the BC or mobile operator. Also, the BC has valid ID MU (specified by mobile operators) associated with the registration which then can be used to detect malicious MU. The probability of detecting an attack in the proposed architecture during 100 times of implementation of this scenario is shown in Fig. 13. The results shows that the proposed approach easily detects attacks and blocks ID them by the SDN controllers and BC.

7 RELATED WORK

The 5G network requires high capacity and efficient security mechanisms to support data traffic [1], [27]. The concentration of heterogeneous networks and vast expansion of small base stations have led to the selection of the 5G network [27]. Many applications supported in 5G require high privacy and reliability against malicious attacks, like mobile banking and social network applications [28]. The common methods for secure communications in 3G and

subsequent wireless networks are based on the controllability and cryptographic modifications that impose constraints and challenges for 5G [5], [27].

To support the increased data traffic, 5G networks require high capacity together with strong security mechanisms. With the advent of new communication models in 5G in heterogeneous environments like vehicles [1], SDNs [5], IoTs [6], and fog computing [1], [17]. The common approaches to having a secure connection in 3G and subsequent generations are based on cryptographic exchange control [18], which requires different authentication servers and protocols to support different networks and channels. When the authentication servers are located in another location and are remotely accessible, security challenges rise which are not suitable for 5G [5]. According to [16], due to the frequent displacements among cells, the existence of repetitive authentication is inevitable which may take one-hundredths of milliseconds to identify users, something that would not be acceptable for 5G communications.

In [29], a 3rd Generation Partnership Project (3GPP) provided a specific presentation of hierarchical keys and the flow of handover messages for animated scenarios. Although there exist keys for the handovers, and different handovers are required for different scenarios, this approach increases the delay and the handovers complexity when entering into different 5G cells.

An authentication handover approach was developed by [30], including direct authentication between the user and the AP based on public cryptography. Their proposed mutual authentication and the key agreement does run authentication according to new networks through three-way handshake without having contact with a third part, like authorized and server. Although this authentication handover procedure seems simple, it increases the cost of computing and delays due to the overhead it imposes for exchanging encryption over the wireless mediators. Accordingly, the transfer of a digital signature for the 5G wireless networks is not effective in their approach because of exchanging more cryptographic in overhead.

The privacy presentation for SDN / NFV base architecture in 5G was discussed in [31] with a special focus on network architectures where the core of their mobile packets were for the SDN/NFV structure. This study was focus on the privacy in 5G scenarios like position protection, identity protection based on SDN/NFV, it does not assure the users identity; thus, a challenge for the 5G. An approach for authentication and privacy protection for the 5G small cell vehicular was proposed in [32], where the authors specifically presented the idea of a non-authorized assignment design named CLASC that reduces the low-communications overhead. This approach monitors road and vehicle systems and considers the restrictions on authentication and privacy as future tasks in the heterogeneous 5G networks.

In another work, an architecture named blockchain-based trusted authentication (BTA), based on the chain cell was designed for the 5G network by [33], which is being applied through the blockchain-based anonymous access (BAA) approach used in cloud radio over fiber network. Despite the proposed works advantages, this study does not discuss the handover challenges among the heterogeneous 5G networks nor their privacy protection aspects. The archi-

texture of the 5G network where the fog computing and radio access network are integrated is devised in [34]; to achieve Privacy protection, named the F-RAN architecture. Two loosely and highly coupled approaches for computing functions in 5G are devised to address several privacy attacks that identify the attack location among fog nodes in the F-RAN architecture, which does not address the Authentication and challenges and issues in the 5G.

The authentication handover and privacy protection in 5G networks have been discussed in [5], where the authors have discussed the application of SDN. In this study, by sharing users content among APs, the privacy protection and handover are discussed. Through SDN the 5G heterogeneous cells are managed but sharing the users content when a user is passing through heterogeneous networks would lead to the different content transformation of APs, which is followed by overhead and security challenges like data leakage, and a delay in SDN controllers.

8 CONCLUSION

The 5G networks with heterogeneous cells and expansion in overlay network coverage are replacing previous generations of mobile networks. A reduction in delay, which is one of the objectives and characteristics of the 5G, is of great importance that can happen with a solid architecture. In this paper, with the assistance of blockchain technology and SDN structure, a new authenticate approach was proposed to protect the privacy of users in a faster, safer and more effective manner for the advancement of the 5G network and to provide intelligent control across heterogeneous cells. As results indicated, by removing the repeated manipulations among heterogeneous cells, low latency was obtained for the 5G network. In addition, with a more lightweight blockchain, instead of applying the POW, the upgraded DPOS consensus algorithm associated with our BC demonstrated to be a better fit for scalability and optimized energy consumption.

REFERENCES

- [1] S. Li, L. Da Xu, and S. Zhao, "5g internet of things: A survey," *Journal of Industrial Information Integration*, 2018.
- [2] P. Duan, Y. Jia, L. Liang, J. Rodriguez, K. M. S. Huq, and G. Li, "Space-reserved cooperative caching in 5g heterogeneous networks for industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2715–2724, 2018.
- [3] S. Hu, B. Yu, C. Qian, Y. Xiao, Q. Xiong, C. Sun, and Y. Gao, "Nonorthogonal interleave-grid multiple access scheme for industrial internet of things in 5g network," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 12, pp. 5436–5446, 2018.
- [4] A. Mukherjee, "Energy efficiency and delay in 5g ultra-reliable low-latency communications system architectures," *IEEE Network*, vol. 32, no. 2, pp. 55–61, 2018.
- [5] X. Duan and X. Wang, "Authentication handover and privacy protection in 5g hetnets using software-defined networking," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 28–35, 2015.
- [6] M. Dohler, "The future and challenges of communication toward a world where 5g enables synchronized reality and an internet of skills," *Internet Technology Letters*, vol. 1, no. 2, p. e33, 2018.
- [7] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino, and G. Zizzo, "A technical approach to the energy blockchain in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4792–4803, 2018.
- [8] Z. Ning and L. Guo, "Fog computing enabled internet of everything," *IEEE*, 2019.
- [9] A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "Efficient design and hardware implementation of the openflow v1.3 switch on the virtex-6 fpga ml605," *The Journal of Supercomputing*, vol. 74, no. 3, pp. 1299–1320, 2018.
- [10] A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "P4 to sdnet: Automatic generation of an efficient protocol-independent packet parser on reconfigurable hardware," in *2018 8th International Conference on Computer and Knowledge Engineering (ICCKE)*, pp. 159–164, IEEE, 2018.
- [11] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contracts security testing on blockchains," in *Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering*, pp. 103–113, IBM Corp., 2018.
- [12] R. M. Parizi and A. Dehghantanha, "On the understanding of gamification in blockchain systems," in *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 214–219, IEEE, 2018.
- [13] T. Miyamae, T. Honda, M. Tamura, and M. Kawaba, "Performance improvement of the consortium blockchain for financial business applications," *Journal of Digital Banking*, vol. 2, no. 4, pp. 369–378, 2018.
- [14] M. H. Meng and Y. Qian, "A blockchain aided metric for predictive delivery performance in supply chain management," in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pp. 285–290, IEEE, 2018.
- [15] L. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1545–1550, IEEE, 2018.
- [16] G. Zyskind, O. Nathan, et al., "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW)*, 2015 IEEE, pp. 180–184, IEEE, 2015.
- [17] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.
- [18] L. Chen, J. Ji, and Z. Zhang, "Wireless security: Models, threats, and solutions," 2013.
- [19] D. Klein and M. Jarschel, "An openflow extension for the omnet++ inet framework," in *Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques*, pp. 322–329, ICST (Institute for Computer Sciences, Social-Informatics and , 2013.
- [20] N. Gray, T. Zinner, S. Gebert, and P. Tran-Gia, "Simulation framework for distributed sdn-controller architectures in omnet++," in *International Conference on Mobile Networks and Management*, pp. 3–18, Springer, 2016.
- [21] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the internet of things," in *Communication Systems & Networks (COMSNETS)*, 2018 10th International Conference on, pp. 561–564, IEEE, 2018.
- [22] J.-H. Lee, J.-M. Bonnin, P. Seite, and H. A. Chan, "Distributed ip mobility management from the perspective of the ietf: motivations, requirements, approaches, comparison, and challenges," *IEEE Wireless Communications*, vol. 20, no. 5, pp. 159–168, 2013.
- [23] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pp. 75–86, ACM, 2011.
- [24] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac-macs: Effective data access control for multiauthority cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1790–1801, 2013.
- [25] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.
- [26] N. Vladimirova, "New attacks against 4g lte mobile networks registered." <https://www.virusguides.com/new-attacks-4g-lte-mobile-networks-registered/>, 2018.
- [27] D. Marabissi, L. Mucchi, R. Fantacci, M. Spada, F. Massimiani, A. Frattini, G. Cau, J. Yunpeng, and L. Fedele, "A real case of implementation of the future 5g city," *Future Internet*, vol. 11, no. 1, p. 4, 2019.
- [28] K. Wang, L. Yuan, T. Miyazaki, Y. Chen, and Y. Zhang, "Jamming and eavesdropping defense in green cyber-physical transportation

- systems using stackelberg game," *IEEE Transactions on Industrial Informatics*, 2018.
- [29] E. U. T. R. A. Network, "3rd generation partnership project; technical specification group services and system aspects; general packet radio service (gprs) enhancements for evolved universal terrestrial radio access network (e-utran) access," *EUTRA Network*, 2011.
 - [30] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," *IEEE communications letters*, vol. 14, no. 1, 2010.
 - [31] V.-G. Nguyen, A. Brunstrom, K.-J. Grinnemo, and J. Taheri, "Sdn/nfv-based mobile packet core network architectures: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1567–1602, 2017.
 - [32] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 772–782, 2017.
 - [33] H. Yang, H. Zheng, J. Zhang, Y. Wu, Y. Lee, and Y. Ji, "Blockchain-based trusted authentication in cloud radio over fiber network for 5g," in *Optical Communications and Networks (ICOON)*, 2017 16th International Conference on, pp. 1–3, IEEE, 2017.
 - [34] Y.-J. Ku, D.-Y. Lin, C.-F. Lee, P.-J. Hsieh, H.-Y. Wei, C.-T. Chou, and A.-C. Pang, "5g radio access network design with the fog paradigm: Confluence of communications and computing," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 46–52, 2017.