Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766165

HIGHLY SECURE AUTHENTICATION AND KEY AGREEMENT PROTOCOL FOR BLOCKCHAIN ASSIMILATED 5G COMMUNICATION NETWORKS

Bhuvaneshwari G[1], Bhalaji N[2], Beulah Jayakumari R[3], Murugesan S[4], Suganya A[5], Subashini K[6]
[1,4,5,6]Assistant Professor,
[3]Professor, Department of Information Technology, Tagore Engineering College, Chennai-600 127
[2]Associate Professor, Department of Information Technology, SSN College of Engineering, Kelambakkam-603 103
[1]gbhuvaneswari@tagore-engg.ac.in, [3]hod.it@tagore-engg.ac.in, [4]muruga13@gmail.com, [5]asuganya@tagore-engg.ac.in, [6]subashini1509@gmail.com

Abstract

The evolution of every communication standard provides high connectivity among the communication devices.5G and other beyond technologies are being designed to catering diverse requirements of use cases. To realize such features of 5G and beyond technologies, we need to rethink how the current cellular networks are designed and established. Because, the radio communications and spectrum utilizations are not enough. Several technologies such as Software Defined Networking (SDN), Network Function Virtualization (NFV), Machine Learning, and Cloud Computing are currently used to establish the 5G communication technology. Also, it creates some challenges such as decentralization, transparency, interoperability, privacy, and security. To address these issues, we can integrate Blockchain into 5G. Because Blockchain has the features such as transparency, immutability, encryption and distributed environment. Even though blockchain provides a secure and reliable communication, there are some possible attacks such as Denial of Service (DoS), Eavesdropping, Man in the Middle (MitM) and jamming. We designed a secure authentication protocol which eradicates the above-mentioned attacks. It performs mining process, verify the timestamp and aggregate the transaction. It reduces the communication overhead and computation time. Our security analysis illustrates that the proposed scheme is secure and resists the known attacks such as DoS, DDoS, MitM, hijacking and compromising attacks.

Keywords: Blockchain,5G, SDN, Cloud RAN,5G, DoS, DDoS, Hijacking, Jamming, AKA, Authentication

I. Introduction

The 5G communication networks need to handle a massive amount of data and provide connectivity to billions of devices with varying degree of Quality of service (QoS). It provides the services via a combination of several technologies. It requires an open, transparent, and secure system across the overall 5G ecosystem. For example, the ultra-dense small cell networks in 5G used to give high data rates and low latencies which introduce security and reliability distresses in the network. Therefore, providing a reliable and secure connection is very important but at the same time challenging for 5G networks[1].

At present, the biggest challenge for current 5G platforms is the necessity to assure an open, transparent, and fair system within the extraordinary number of resources and several malicious users. Blockchain with its unique features such as decentralization, high level of data privacy, security, transparency and immutability become an obvious choice. Therefore, there is a need to integrate Blockchain into 5G Technology which erect 5G architecture. This architecture will work as a self-maintaining, self-servicing, and self-managing network. That network can carry out transactions, handle automatic and secure update without the need of a central broker. A Blockchain framework will contribute a new generation of distributed wireless networks by allowing seamless provisioning between heterogeneous access nodes and devices. With Blockchain, provisions and agreements between access nodes, networks, and subscribers are negotiated on-the-fly as digital smart contracts. Blockchain will allow devices on the network to negotiate the best service with the network operator which will be then executed using the smart contract [2].

The cellular standards have been evolved in each decade such as 1G in 1980,2G in 1990,3G in 2000,4G in 2010 and 5G in 2020 where each generation provides very unique services based on the market needs. The primary and most common features offered by each generation is the high throughput, large Coverage area and Capacity.

A wide range of use cases that 5G aims to provide which is broadly classified as eMB (enhanced Mobile Broadband), mMTC (massive Machine Type Communication), uRLLC (ultra– Reliable Low Latency Communication) and Secure. Figure 1 shows the use cases and the possible applications of 5G.

1. eMBB-enhanced Mobile Broadband-It aims to provide 10 to100x times faster data rate than 4G and 4.5G networks.
2. uRLLC-Aims to support mission critical applications which obviously need low error rate and latency.

mMTC-massive Machine Type Communication-with the rise of Internet of Things, the ubiquity of the devices has necessitated the deployment of connectivity standards that can support high density devices with less power consumption.

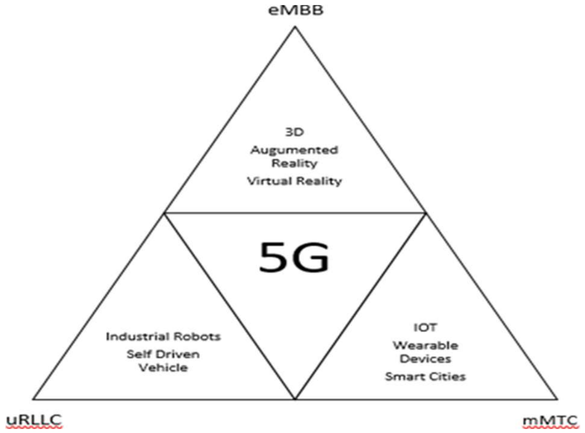

Figure1.5G Usecases

Blockchain technology has the all-probable solution to transform the way services are offered across various industries. It provides a distributed, immutable, single source of truth that everyone agrees upon without trusting on a middleman. Blockchain has the potential to be integrated with the 5G network to enable end-to-end services delivery across the entire 5G+ ecosystem. Blockchain facilitates a reliable, decentralized, secure and immutable ledger which performs Transaction between two entities without the control from central entity. All data recorded on blockchain will be visible to all participating nodes and can be verified by all nodes using consensus algorithm. It is built by linking blocks using linked list or chain of blocks [3].

2. Related work

The survey presented in [4], provides a complete coverage showing various aspects of 5G application to Blockchain. But, it does not include taxonomy and layered approach for Blockchain integration into 5G technology. In this paper, various Surveys have been conducted in relation to the application of Blockchain in several areas such as edge computing IoT [5], smart city [6], and [7]. In [8] a detailed analysis of healthcare system has been done. In [9], the authors concentrated on the application of Blockchain in 5G networks with varying degree of scope. In [10], the authors claimed that 5G AKA protocol undergoes from impersonating, DoS, and MitM attacks.

In [11], the authors introduced a secure efficient and lightweight AKA protocol for machine-type communications devices in 5G cellular network. In this scheme, the authors assumed that each UE has a unique identity, each UE shares a secret key with the HN, and the HN is fully trusted. However, this scheme has no registration procedure which is the first step of the AKA protocol. Moreover, the UE begins the authentication procedure which means that the impersonating attacks can still possible. In [12], the authors proposed a novel 5G authentication protocol to improve the battle against active attacks and malicious serving networks.

In [13], the authors proposed a security authentication scheme for 5G ultra dense networks based on blockchain. In this scheme, the authors used the blockchain to create an access point (AP) group based on the Byzantine fault tolerance in order to optimize the consensus of the mechanism. However, there is no privacy in the same group. In addition, this scheme needs to reach the HN at each frequent authentication request thus the HN could be violated with different types of attacks since the ultra-dense network access points are out of the formal network operator management.

3. Proposed Work

The proposed scheme consists of four steps; initialization, registration, mining process, and authentication and key agreement protocol as follows:

Initialization

In this, we describe the initialization process of the system that the Home Node(HN) is responsible to achieve. It is the principal entity of the network which bootstraps the system by choosing a large prime number p and generates Z_p as a finite field with order p. Let G be a cyclic additive group with generator P, whose order is p, H is hash function, where $H:\{0,1\}^{*}$□ G. $H1:\{0,1\}^{*}$□ Z_p. HN chooses a random element sk_h which is an element of Z_p and computes $PK_h= (1/ sk_h)P$ where sk_h and PK_h are the HN's private and public keys, respectively. For each node of the network y, such as UE, SN, or AP, the HN chooses a random element sk_y which is an element of Z_p as a private key and computes the corresponding public key $PK_y = (1/sk_y)$ P.

Fig.2 illustrates the proposed block contents that the APs create and manage in the proposed scheme. AP's pool initiates a new block in the blockchain with the following contents

Block header BID	Hash of Previous Block	Time Stamp TS	Nonce	Transactions

Figure 2. Contents of a Block

1) Block header (BID): It is a field used to index the block.
2) Hash of the previous block: It is a field to determine the integrity of the block.
3) Timestamp (TS): It is a timestamp for each block to ensure the validity of the block.
4) Nonce (Nonce): It shows a hash calculation of the number of transactions included in the block.
5) Transactions: It stores the transactions of the network entities. It consists of the following fields such as transaction number of the UE (Tue), public key of the UE (PKue), timestamp of UE (TSue), transaction number of the AP that services the UE (Tap), status of the node public key (status).

Registration

The registration process occurs between the network entities at the first time they communicate such as, it may be done between UE and AP or AP and SN. Therefore, we describe the first communication between UE and AP and the same protocol will be valid between AP and SN, with respect to the AP may need to update its location in the case of mobile relay node (MRN). When the UE accesses to the new AP, the AP sends to the new coming UE a registration message and thus a registration protocol starts.

1) Once the UE receives a registration notification message from the corresponding AP, itchooses a random number N_{ue} which is an element of Zp and creates a timestamp, TS_{ue} and sends a registration request to the corresponding AP, RegReq(Tue,Nue,,P,TSue,σue), where T_{ue} is the latesttransaction number of the UE, and σ_{ue} is the signature of the UE computed by the UE as

$\sigma ue = (1/sk_{ue})H(Tue, Nue.P, TSue)$.

2) The AP verifies the freshness of the message by the timestamp, and verifies the signatureσue as ê(σue,P)=ê(H(Tue,Nue,P, TSue), PKue); the proof of signature verification is illustrated in Eq. 1.Moreover, AP verifies the identity of the UE by using the received block index and transaction number, if the verification is correct, the AP chooses a random number N_{ap} which is an element ofZp and computes the shared key $K_{ueap} = H1(N_{ap}.N_{ue}.P)$, computes the challenge H (K_{ueap}, 1), and sends a registration response to the UE as RegRes(Tap,Nap,P,TSue,H(Kueap,1)σp).

$$\hat{e}(\sigma ue, P) = \hat{e}((1/sk_{ue})H(Tue,Nue,P,TSue), P)$$
$$= \hat{e}(H(Tue,Nue,P,TSue), (1/sk_{ue})P)$$
$$= \hat{e}(H(Tue,Nue,P,TSue),PK_{ue})$$

(Eq.1)

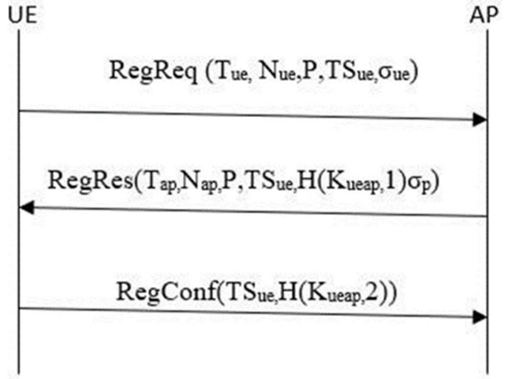
UE
AP
RegReq ($T_{ue,}$ N_{ue},P,$TS_{ue,}\sigma_{ue}$)
RegRes($T_{ap,}N_{ap,}$P,$TS_{ue,}$H($K_{ueap,}$1)σ_{p})
RegConf($TS_{ue,}$H($K_{ueap,}$2))

Figure.3:UE – AP Authentication Procedure

3. When the UE receives the response from the corresponding AP, it verifies the freshness of the messages and the signature of the AP. If the verification is correct, the UE computes the shared key as Kueap=Nue.Nap.P and computes H(Kueap,1) to verify the received one. If the verification is correct, the UE computes H(Kueap,2) and sends a confirmation message to the AP as RegConf (TSue,H(Kueap,2)). Otherwise, the UE restarts the registration procedure.

4. Once the AP receives the confirmation message from the UE, it sends a location update message to the HN in order to create new transaction to the UE and ends the registration procedure.

Proposed Mining Process

In the proposed scheme, mining is the process of finding and adding new transaction records that is happening as a 5G entity registration records to the blockchain. The blockchain confirms the transaction to the whole network nodes. The network nodes in the network use the blockchain to verify the correctness of the transaction. The proposed mining process depends on the APs computation capabilities. There is a mining pool which consists of all APs in the 5G network.

Whenever the AP receives a registration request, it broadcasts a mining request over the entire network. The HN maintains its own criteria to add a new block to the blockchain. The HN checks the freshness of the packet using the timestamps. If the packet is fresh, then the blockchain requires to add the packet as a new block. Once the criterion is satisfied, blockchain collects all the confirmed transactions and adds a new block to the blockchain.

Authentication and Key Agreement Protocol

Whenever the UE requests a service from the network, it should execute AKA protocol with the corresponding SN through the AP. We can prove that the proposed AKA protocol by using blockchain as follows.

1) The UE sends authentication request to the corresponding AP as AuthReq(Tue,TSue,Nue,P,σue).

2) Once the AP receives the message, it verifies the freshness of the message using the timestamp, verifies the UE’s signature. If all verification is correct then the AP calculates the aggregated signature σue+ σap and forwards the authentication request as AuthReq(Tue,TSue,Nue,P,σueap) to the SN.

1) The Servicing Network(SN) verifies the freshness of the message and the aggregated signature as $\hat{e}$ (σ_{ueap}, P) = $\hat{e}(H(T_{ue},TS_{ue},N_{ue},P),PK_{ue}+PK_{ap})$.If all verification is correct, it chooses a random number M_m which is an element of Z_q and computes the secret key $K_{uem}=H1(M_m\ r_{ue}\ P)$, computes the challenge $ch_k=H(k_{uem},1)$ creates a signed authentication response message AuthRes($T_m,TS_{ue},M_m,P,ch_k,\sigma_m$) and sends the message to the AP.

$$\begin{aligned}\hat{e}(\sigma_{ueap},P) &= \hat{e}(\sigma_{ueap},P)\\ &= \hat{e}(\sigma_{ue},P)\ \hat{e}(\sigma_{ap},P)\\ &= \hat{e}((1/sk_{ue})H(T_{ue},N_{ue}.P,TS_{ue}),P)\ \hat{e}((1/sk_{ap})H(T_{ue},N_{ue}.P,TS_{ue}),P)\\ &= \hat{e}(H(T_{ue},N_{ue}.P,TS_{ue}),\ (1/sk_{ue})P)\ \hat{e}(H(T_{ue},N_{ue}.P,TS_{ue}),\ (1/sk_{ap})P)\\ &= \hat{e}(H(T_{ue},N_{ue}.P,TS_{ue}),\ PK_{ue})\ \hat{e}(H(T_{ue},N_{ue}.P,TS_{ue}),PK_{ap})\\ &= \hat{e}(H(T_{ue},N_{ue}.P,TS_{ue}),\ PK_{ue}+PK_{ap}) \qquad \text{(Eq.2)}\end{aligned}$$

4) Once the AP receives the message, it verifies the freshness of the message and the aggregated signature of the SN. If the verification is correct, the AP computes an aggregated signature, σmp and forwards the signed message to UE as AuthRes (Tm, TSue, Mm.P, chk, σmp).

5) When the UE receives the message, it verifies the freshness of the message and the aggregated signature. If all verification is correct, the UE computes the shared key

Kuem = H1(Nue M mP) and verifies the challenge chk. If it is correct, then the UE computes new challenge chue = H(kuem, 2) and sends an authentication confirmation message to the SN via the AP, AuthConf (TSue, chue).

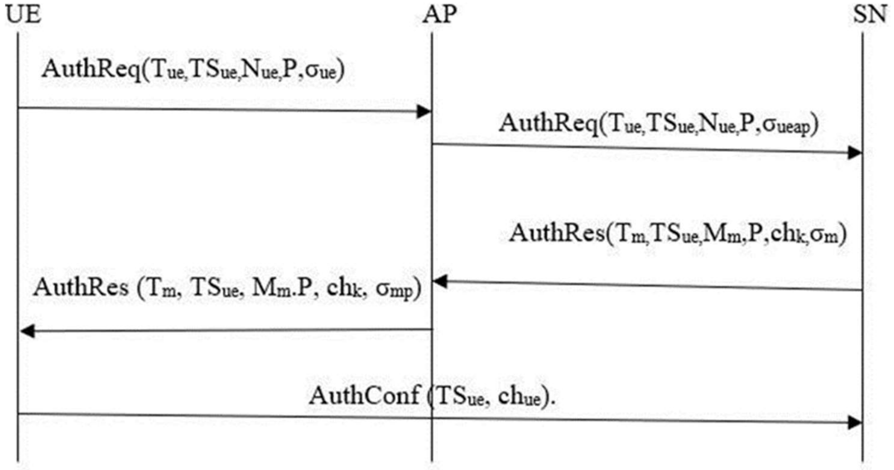
UE
AP
SN
AuthReq($T_{ue},TS_{ue},N_{ue},P,\sigma_{ue}$)
AuthReq($T_{ue},TS_{ue},N_{ue},P,\sigma_{ueap}$)
AuthRes($T_m,TS_{ue},M_m,P,ch_k,\sigma_m$)
AuthRes (T_m, TS_{ue}, M_m.P, ch_k, σ_{mp})
AuthConf (TS_{ue}, ch_{ue}).

Figure .4: UE-AP-SN Authentication Procedure

4. SECURITY ANALYSIS

This section shows the robustness of the proposed scheme against well-known attacks that threaten 5G networks.

Security level 1: Blockchain-based security

In the proposed scheme, the blockchain provides the 5G network with a security capability against hijacking attacks because the blockchain is distributed over all the network. The public key is completely registered, validated, and verified; therefore, hijacking attacks have no capability to gain information from one node to use it in another one. Besides, the blockchain ensures the integrity of the distributed data since no one can modify or remove the block or transaction from the blockchain.

Security level 2: Signature-based security

In the proposed scheme, each node in the network UE, AP, or SN, has a public and private key generated from the HN. HN already registers the public key in the blockchain, therefore, as we mentioned, there is no chance to fake the public key. The security of the signatures is based on the well-known discrete logarithm. The proposed scheme can secure the registration and authentication protocol without involving the HN, which is important to improve scalability, efficiency, and resiliency. In addition, impersonating any node in the network is infeasible because all messages are signed and forging signatures is infeasible, and computing the private key 1/ skue from the public key (1/ skue) P is infeasible because of the discrete logarithm difficulty. Each node in the network can verify the packet's integrity because they are signed and any modification to the packet will result in failure of the signature verification. Therefore, the proposed scheme countermeasures the MitM, DoS, DDoS, impersonating, and malicious attacks.

Security level 3: Timestamp-based security

In this scheme, the timestamps are used to prevent the packets from replay attacks. Each node will verify the timestamps to make sure that the packet is fresh. The timestamps are used to declare the packet is a stale packet or fresh packet. If any stale packet arrives means that will be dropped. If the nodes are not able to identify the stale packet, attackers can launch attacks to exhaust the network resources.

5. Performance Evaluation

We can analyze the performance based on the communication overhead and computation overhead.

Communication overhead

It is based on the amount of data exchanged and number of exchanged messages. The existing Registration protocol uses fixed number of messages between source and destination. Our scheme is also uses fixed number of messages between the source and destination. The main difference is that the existing protocol involves HN for each transaction. But the proposed scheme does not involve HN for a transaction. The proposed authentication protocol uses very less number of communication messages. So, it reduces the communication overhead. In our scheme, 15bytes for prime number p,15 bytes for elliptic curve,15bytes for signature and 5 bytes for timestamp has been allotted.

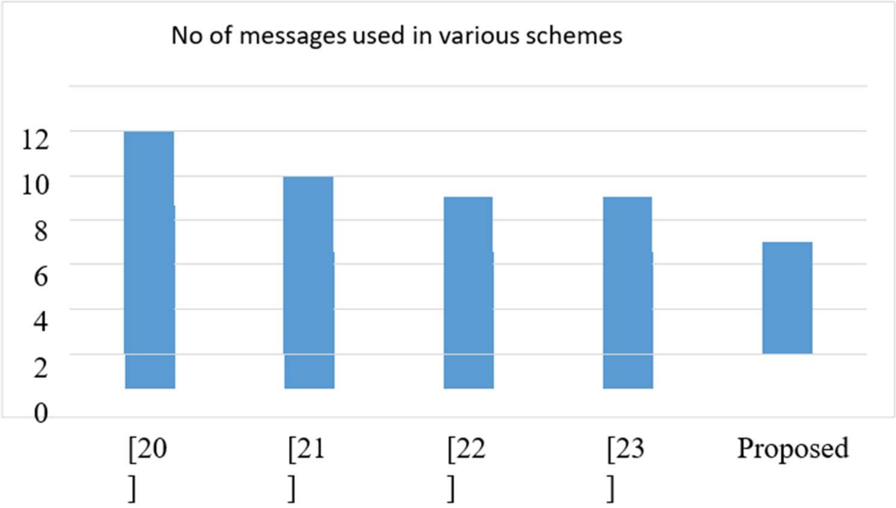

Figure 5. Number of messages used in various Schemes

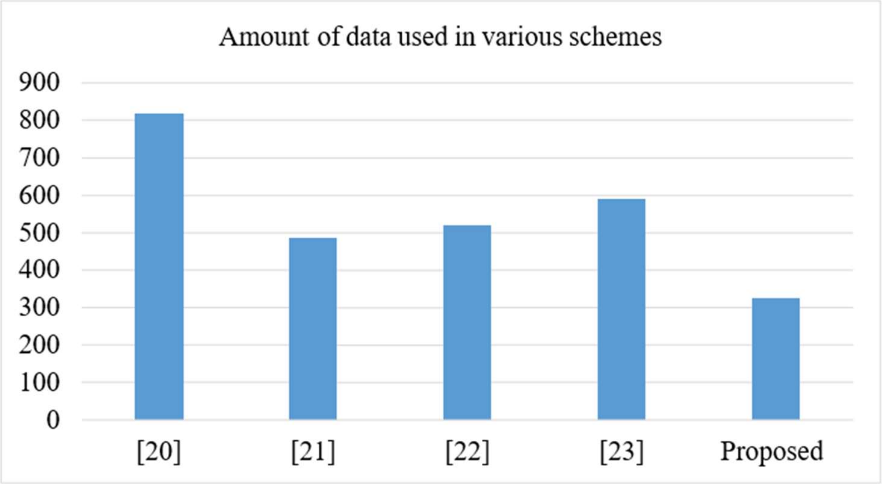

Figure 6. Amount of data used in various schemes

Computation Overhead

It is about the time needed to compute the required functions that are used in the authentication procedure. The proposed scheme needs less computations than the other schemes since it depends on the blockchain that provides the network nodes an integrated copy of the HN database. In the UE, the proposed scheme needs a computation time less than the other schemes which is very important and desirable behavior since the UE has a limited battery, therefore, the proposed scheme preserves the battery consumption of the UE. In the AP node, the other schemes consider the AP as a gateway which transfers the messages to the HN without verification which is a security issue thwarting the HN. However, our proposal gives a rule to the AP to deny attacks to access the HN, therefore, the computation overhead appears at the AP. In the SN nodes, the proposed scheme also decreases the computation overhead which enhances the quality of service. In the HN node, the proposed scheme does not involve the HN in the authentication protocol which decreases the congestion in the core network and decreases the security risks. Fig.7 shows that the authentication algorithms such as cryptographic function takes 38ms, SHA256 takes 5ms, AES takes 20ms, ECC takes 1ms and the module takes 0. 005ms.It saves the battery power. Since, the devices are highly expected to endure high battery energy, less computation time highly saves the battery.

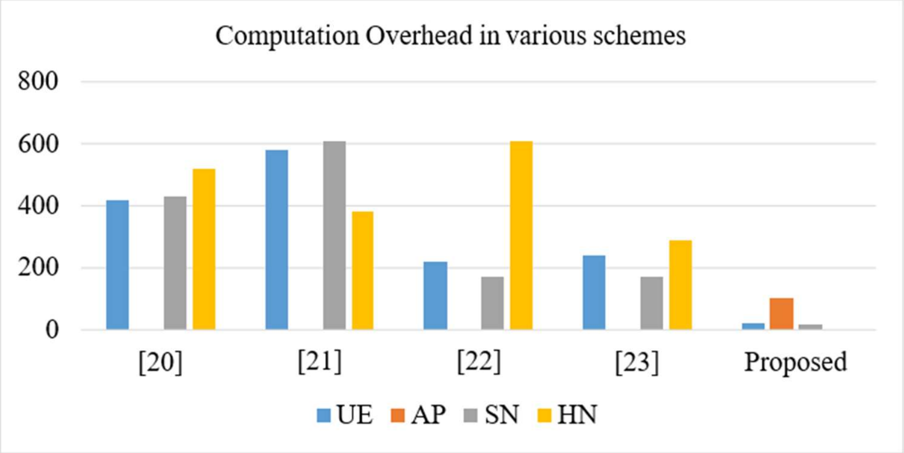

Figure 7. Computation overhead in various schemes

6. Conclusion

In this paper, we proposed a novel blockchain based authentication protocol. We reviewed the possibilities and benefits of integrating blockchain in to the 5G network. The blockchain ensures the integrity of the distributed data since no one can modify or remove the block or transaction from the blockchain. A new procedure for authentication has been proposed to improve the security. The HN is the capital entity of the network which is responsible for initiating the bootstrapping of the network. Each and every node should be registered as a transaction in a block. Mining procedure ensures the newly added transaction records in to the network. Whenever a new node is entered in to the network, the registration and authentication procedure shall be executed between the UE and the SN. The public and private keys have been chosen randomly which avoids the hijacking attacks. These keys are completely registered, validated and verified. Timestamps have been checked each and every node to ensure the freshness of the data packet. The security analysis shows that the proposed scheme is secure. It provides high throughput. Results are showing that the proposed scheme is definitely ensures the integrity and freshness of the message. Definitely, the proposed scheme reduces the overhead and computation time.

References

[1] A. Gupta and R. K. Jha, “A survey of 5G network: Architecture and emerging technologies,” IEEE access, vol. 3, pp. 1206–1232, 2015.

[2] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016.

[3] A. Chaer, K. Salah, C. Lima, P. Ray, and T. Sheltami, “Blockchain for5g: opportunities and challenges,” in Proceedings of the IEEE GlobalCommunications Conference (GLOBECOM), 2019.

[4] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for 5g and beyond networks: A state of the art survey,” arXiv preprintarXiv:1912.05062, 2019.

[5] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, “Blockchain for 5genabled iot for industrial automation: A systematic review, solutions, and challenges,” Mechanical Systems and Signal Processing, vol. 135,p. 106382, 2020.

[6] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A survey of blockchain technology applied to smart cities: Research issues and challenges,” IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2794–2830, 2019.

[7] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: A survey, some research issues and challenges,”IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp.1508–1532, 2019.

[8] D. Lin, S. Hu, Y. Gao, and Y. Tang, “Optimizing mec networks for healthcare applications in 5g communications with the authenticity of users’ priorities,” IEEE Access, vol. 7, pp. 88 592–88 600, 2019.

[9] E. Hossain and M. Hasan, “5g cellular: key enabling technologies and research challenges,”

IEEE Instrumentation & Measurement Magazine,vol. 18, no. 3, pp. 11–21, 2015. Software: Practice and Experience, 2019.

[10] I. Gharsallah, S. Smaoui, and F. Zarai, “A secure efficient and lightweight authentication protocol for 5G cellular networks: Sel-aka,” in 2019 15th International Wireless Communications Mobile Computing Conference (IWCMC), Jun. 2019, pp. 1311–1316.

[11] F. Liu, J. Peng, and M. Zuo, “Toward a secure access to 5G network,” in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Aug. 2018, pp. 1121–1128.

[12] Z. Chen, S. Chen, H. Xu, and B. Hu, “A security authentication scheme of 5G ultra-dense network based on blockchain,” IEEE Access, vol. 6, pp. 55 372–55 379, Sep. 2018.