Blockchain-Based Decentralized Authentication for Information-Centric 5G Networks

Muhammad Hassan, Davide Pesavento, and Lotfi Benmohamed
National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA
Email: {muhammadhassanraza.khan, davide.pesavento, lotfi.benmohamed}@nist.gov

***Abstract*—The 5G research community is increasingly leveraging the innovative features offered by Information Centric Networking (ICN). However, ICN's fundamental features, such as in-network caching, make access control enforcement more challenging in an ICN-based 5G deployment. To address this shortcoming, we propose a Blockchain-based Decentralized Authentication Protocol (BDAP) which enables efficient and secure mobile user authentication in an ICN-based 5G network. We show that BDAP is robust against a variety of attacks to which mobile networks and blockchains are particularly vulnerable. Moreover, a preliminary performance analysis suggests that BDAP can reduce the authentication delay compared to the standard 5G authentication protocols.**

I. Introduction

Information Centric Networking (ICN) has been shown to satisfy the necessities of the fifth-generation cellular system (5G) [1]. ICN follows a content-centric security model. However, the in-network caching feature of ICN makes it more challenging to enforce access control policies in 5G-ICN. This is because, unlike IP-based 5G where the content is stored at specific content producers, 5G-ICN allows the content to be cached anywhere in the network. Consequently, the user's request can be fulfilled by the cached copies at the routers on the forwarding path, while the content producers have no control over the router's behaviour. Various solutions have been presented in the literature to handle ICN access control challenges [2], [3], [4], [5]. However, some of them introduce a significant delay and a single point of failure due to their centralized nature, while others are unable to prevent unauthenticated users from exhausting network resources. Furthermore, the integration of existing IP-based authentication protocols such as 5G-AKA (5G Authentication and Key Agreement) into 5G-ICN diminishes the benefits obtained from ICN's fundamental features, e.g., in-network caching. This is due to 5G-AKA requiring a dedicated communication tunnel between the mobile User Equipment (UE) and the authentication server for each authentication session.

In recent years, Blockchain (BC) technology has gained significant interest whereby scientists from various domains have used BC to ensure security, privacy, and access control in a decentralized manner [6]. Inspired by its decentralized and tamper-proof characteristics, we make use of BC technology to address the above-mentioned issues and provide a BC-based Decentralized Authentication and re-authentication Protocol for ICN-based 5G networks (BDAP). In BDAP, we exploit the BC technology to immutably store access control data of UEs in a distributed ledger and authenticate the UEs as early as possible (i.e., at the edge nodes) in a decentralized manner, without continuous interaction among core network entities.

BDAP allows only legitimate users to access restricted content and network resources (caches, bandwidth), and does not require any additional entities or major changes to the typical 5G-ICN architecture. BDAP also reduces the authentication-related communication overhead in the core network since it does not rely on dedicated communication tunnels between UE and core functions for each authentication session. We perform a qualitative security analysis of BDAP augmented with a preliminary performance evaluation that shows the reduction in total authentication delay compared to 5G-AKA.

II. Background and Related work

Authentication and Mobile Management in 5G. In the current IP-based 5G architecture, the authentication of the UE is managed by core entities known as Security Anchor Function (SEAF) and Authentication Server Function (AUSF), while the functions related to data management during the authentication process are performed by an entity called Unified Data Management (UDM) [7]. To establish security, the 5G base station forwards the control and user plane traffic between the mobile core and UE over a private network using the tunnelling protocols SCTP/IP and GTP/UDP/IP, respectively. The complete message flow of 5G-AKA, a common 5G authentication technique, is summarized in [7]. We claim that the integration of these authentication mechanisms in 5G-ICN induces complex computations and additional authentication-related signaling overhead.

Authentication and Access Control in ICN. Most state-of-the-art authentication protocols for ICN, such as [8], target a very different use case (home IoT) that does not typically suffer from frequent mobility or scalability issues. For access control in ICN, the solutions proposed so far fall into two broad categories: authentication-based and encryption-based. In authentication-based schemes, the authentication method requires continuous interaction with the content producers [3] or an access control server [2] throughout the content retrieval phase. As a result, a significant delay is introduced due to these frequent interactions, which offsets the advantages provided by the in-network caching of ICN. Furthermore, these solutions introduce a centralized access control design with additional functions to authenticate and authorize the requesting user and unavoidably brings the issue of a single point of failure.

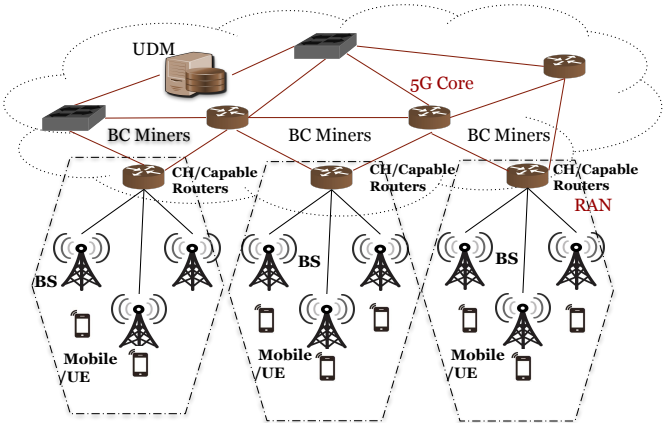

Fig. 1. BDAP system architecture.

By contrast, encryption-based schemes manage access control by encrypting the content and limiting the distribution of the decryption key to authorized consumers only [4], [5]. In such schemes, unauthorized users cannot decrypt the content, but they can still retrieve it from the network. This is because the network routers are unable to distinguish between authenticated and unauthenticated requests. Consequently, the router's resources, such as the cache space and the Pending Interest Table (PIT), can easily be exhausted by flooding fake requests.

III. Blockchain-based Authentication and Re-authentication Protocol for 5G-ICN

A. System and Adversary Model

The design of BDAP consists of two main layers, namely the core network and the clusters [9]. In our model, every cluster includes a number of radio access nodes (BS or gNodeB) and a Cluster Head (CH), as illustrated in Figure 1. For the selection of the CH, we utilize a *weighted clustering algorithm* (WCA) [10]. To simplify the system model, we consider all core network nodes except the UDM as ICN routing entities. In addition, we assume that the complete network forms a single autonomous system. The CHs manage their respective cluster members (i.e., BSs) and all the UEs connected to those BSs. A subset of core entities are responsible for managing the global blockchain, while each cluster manages its own local immutable ledger (see Section IV). Each UE is in possession of its credentials to access the 5G network, i.e., it has an operator-provided SIM card, which includes a private key. In BDAP, the authorization server runs at the UDM, which is responsible for initiating the genesis transaction for the BC and the initial registration of each UE. The other 5G core entities (e.g., SEAF, AUSF) are not included in BDAP's framework.

In our threat model, the adversary controls an arbitrary number of unauthorized UEs and uses them to attempt to connect to the 5G network. The malicious UEs may access the content stored in the ICN routers to get unauthenticated access or may perform a cache poisoning attack [11]. Further attack scenarios exist, such as: (i) the attacker can flood false (new or replayed) authentication requests in the network, which can result in a denial of service (DoS); (ii) the attacker can affect the caches and PITs of routers by sending out unauthorized content requests which, even though the adversary is not able to decrypt the content, can still exhaust the routers' resources. Finally, we assume that any subset of BSs, CHs, and core routers can be compromised, while the UDM is assumed to be a trusted entity that cannot be compromised.

B. Modeling Data through Blockchain

The BC provides a database of transactions that is disseminated to all participating nodes of the BC network, i.e., BSs, CHs and a subset of core nodes that are elected as miners, including the UDM. BDAP leverages the BC as an application that provides a distributed repository of authentication data and utilizes this data to authenticate access requests. In particular, the two fundamental primitives in BDAP are as follows.

Retrieving a transaction. All routers contain a local copy of the BC. Thus, any BS can retrieve BC data to validate authentication requests from UEs. Specifically, the BS, after receiving an authentication request (which we call a *transaction*, or T_x) from a UE, recovers the previous transaction of the same UE from the BC ledger.

Adding a transaction. Once the transaction is validated following the procedure outlined in Sections III-C and III-D, it is included in the BC. Instead of adding individual transactions to the BC, a predefined set of transactions (called a *block*) are mined together and added by the miners. Mining is the process where all miners begin competing to develop the next block (see Section IV). The miner who first mines a new block appends it to its local BC copy and later broadcasts it to all other routers. The other routers, when receiving the new block, first verify it and then revise their own BC copies. In this way, every router in the network eventually contains the same (i.e., most recent) copy of the BC.

C. Initial Mobile Authentication

BDAP reuses the concept of Subscription Permanent Identifier (SUPI) from the 5G standards. In our proposal, each UE maintains a pair of public (pk) and private (sk) keys associated to the SUPI. In particular, sk is securely embedded in the USIM card; moreover, the UDM keeps a copy of pk and is responsible for registering the sk with its associated pk. When the UE first attaches to the network, the UDM directly verifies the authentication request T_x issued by the UE. The authentication request includes the identity (SUPI) and pk, and also carries a digital signature that the UE generates by signing its identity and some additional information with its sk, as shown in Figure 2. The additional information contains the ID of the current network and several BC-specific fields, such as the current and previous transaction identifiers (T_xID).

When the UDM receives the initial authentication request issued by the UE, it confirms the request by validating the attached digital signature. Once the verification is successful, the UDM generates the first transaction for that particular UE and broadcasts the transaction in the BC network. The miners receive this transaction and add it to their next block to

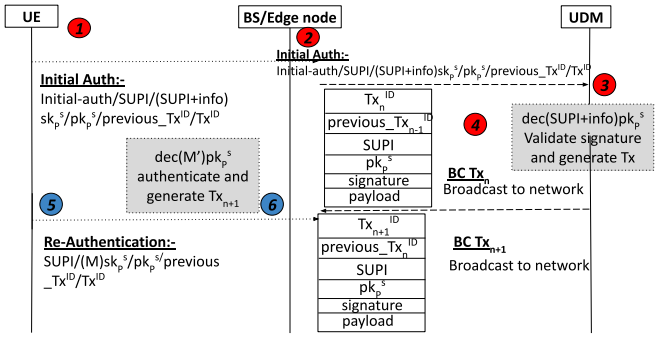

Fig. 2. Initial authentication (red) and re-authentication (blue) of UE.

mine. In particular, the first validated T_x of a UE includes the following fields: 1) the current transaction identifier T_xID_{curr}, which becomes the output of this particular T_x; 2) the previous transaction identifier T_xID_{prev}; 3) the public key pk associated with the SUPI; 4) the digital signature created by the UE for authentication; 5) additional payload that is utilized to increase the efficiency and scalability of the BC (described in Section IV).

D. Efficient Re-Authentication of UE during Handover

Similar to the initial authentication, the UE sends an authentication request to the network during the re-authentication phase as well. In particular, at each handover event when a UE attaches to a new BS, it issues a re-authentication request which includes the following fields: 1) the SUPI provided by the network operator; 2) a digital signature generated by signing SUPI and additional information with the private key sk, formally: $sig = encrypt(sk,\ hash(SUPI \mid\mid info))$; the signature ensures the UE's request authenticity and immutability with its previous authentication event; 3) the public key pk associated with the UE's identity, which is required for the signature verification; 4) the T_xID_{prev} needed to retrieve any previously stored authentication data of that specific UE from the BC; 5) T_xID_{curr}, computed as the cryptographic hash of the complete authentication request message, formally: $T_xID_{curr} = hash(auth\_req)$.

When a BS receives an authentication request from a UE, it first retrieves the previous T_x of the same UE utilizing the T_xID_{prev}. In order to authenticate the UE's request and verify the signature, the BS fetches the pk of the earlier transaction from the BC and utilizes it to verify the digital signature in the current (pending) transaction. Once the signature is successfully verified, the BS authenticates the UE and forwards the T_x to the CH. The CH, after receiving T_x, verifies it and broadcasts it to the network in order to make it part of the blockchain. In our illustration, we describe the authentication steps executed at one instance, i.e., at the BS. However, each node participating in the network carries out similar verification steps upon receiving the authentication request. At each authentication event, a unique value of BS/CH ID is signed along with the SUPI. Although the SUPI remains the same at each instance, the protocol takes advantage of the BS/CH ID to generate different signatures for each instance. The procedure guarantees that the present authentication request was indeed received from the same UE that had previously completed a successful authentication process. Linking each authentication request of the UE with its previous authentication event in an immutable way, thanks to the BC, eventually leads to the root transaction, i.e., the initial authentication of the UE validated by the UDM. Figure 2 summarizes BDAP's message flow for the initial authentication and re-authentication mechanisms.

IV. Enhancing the Efficiency & Scalability of BC

To ensure adequate efficiency and scalability, BDAP exploits the concept of global BC and local immutable ledgers from [6]. In BDAP's architecture, the global BC is managed by all CHs and a subset of core routers, called Global BC Administrators (GBA). On the other hand, every cluster maintains its Local Immutable Ledger (LIL) which is managed by each respective CH, referred to as LIL Administrator (LILA). Notably, the CH performs the role of both GBA and LILA, and therefore it processes all the transactions that are coming to and from its associated cluster members towards the core. The LIL also uses a similar public-key infrastructure as the global BC. In particular, when the BS and CH accept any transaction (say x), it initially verifies if the UE that generated the transaction has changed location (i.e., point of attachment) within the same cluster or across different clusters. This is accomplished by enabling the UE to issue two distinct pairs of transaction IDs, one related to the LIL (T_xID_{local}) and one to the global BC (T_xID_{global}). If the incoming transaction matches the hash pointer for T_xID_{local} in LIL, then the BS verifies x and only LIL is updated by the CH.

In BDAP, we utilize the time-based consensus algorithm given in [6], rather than applying conventional resource-intensive algorithms such as proof-of-work and proof-of-stake. In the time-based consensus algorithm, during the process, a block generator is randomly selected among all participating nodes. Additionally, BDAP considers amplifying the throughput performance by making use of the *Distributed Throughput Management* (DTM) mechanism [6]. In the DTM, after each consensus period, the blockchain utilization is monitored and optimized. Lastly, BDAP uses a *Distributed Trust Algorithm* (DTA) to guarantee scalability [6]. Using DTA, routers in BDAP are not required to verify the entire BC instantiation at every instance. This is accomplished by creating a trust relationship between BC administrators (i.e., routers generating new blocks) by developing their reputations.

V. Evaluation

A. Security Analysis

Table I outlines the defenses and robustness of BDAP against various threat actors and attack scenarios.

B. Performance Analysis

The performance comparison studies the total delay D_{auth} that occurs in the UE authentication and re-authentication process in BDAP and in the standard 5G-AKA protocol. D_{auth}

TABLE I
SECURITY ANALYSIS AGAINST VARIOUS THREATS

Threat	Mitigation in BDAP
Impersonating UE	Each router in the network authenticates the UE's request (Sections III-C and III-D).
Compromised GBA generates false T_x	GBAs can detect a fake T_x during the verification step (Section III-D).
Denial-of-service attack	Routers verify the authentication only once (Section III-D).
Cache and PIT exhaustion	Unauthenticated requests cannot propagate since each request from UE is authenticated by the edge nodes (Section III-D).
Replay attack	One transaction output is immutably linked to only one unique hash pointer in the BC.
Packet discarding attack	Cluster members can reattach to a different CH/GBA if the transactions are not being processed.
False reputation	False increase in the reputation is detected by other GBAs during verification.

can be further split into three components: 1) the transmission time of a protocol message D_{tx}; 2) the protocol processing delay D_{proc}, this includes database access, generation of keys and tags, cryptographic operations, and various other computations; and 3) the propagation delay D_{prop}. We consider that BDAP and 5G-AKA both employ asymmetric keys with equivalent key sizes. Therefore, the processing delay is similar in both authentication protocols. According to [12], D_{tx} is insignificant compared to D_{proc} and D_{prop}; thus, we ignore it. We can conclude that the total authentication delay mainly depends on the propagation delay.

Following the 5G specification [7], we further divide D_{prop} into three sub-components: 1) propagation delay between UE and SEAF, $D_{prop(UE-SEAF)}$; 2) propagation delay between SEAF and AUSF, $D_{prop(SEAF-AUSF)}$; and 3) propagation delay between AUSF and UDM, $D_{prop(AUSF-UDM)}$. From [7] we also derive that the total number of messages exchanged by 5G-AKA between the entities UE $\rightarrow$ SEAF, SEAF $\rightarrow$ AUSF, and AUSF $\rightarrow$ UDM is 3, 4, and 3, respectively. Hence, the unitary propagation delays are multiplied by these factors. Therefore, the total authentication delay in 5G-AKA can be expressed as:

$$D_{auth}^{5G-AKA} = 3D_{prop(UE-SEAF)} + 4D_{prop(SEAF-AUSF)} + 3D_{prop(AUSF-UDM)}$$

Based on Figure 2, we can write the total authentication delay of BDAP as:

$$D_{auth}^{BDAP} = 2D_{prop(UE-BS)} + 2D_{prop(BS-UDM)}$$

From the two equations, we can see that BDAP reduces the propagation delay between the UE and the rest of the mobile network by one, even if we conservatively assume that $D_{prop(UE-BS)} \approx D_{prop(UE-SEAF)}$. This is because BDAP requires one message fewer than 5G-AKA.

The second improvement in BDAP's authentication delay is due to the removal of the SEAF and AUSF participation in the authentication process. This drastically reduces the number of messages exchanged among the core network entities. Moreover, BDAP exchanges only two messages between the BS and the UDM, resulting in a propagation delay of $2D_{prop(BS-UDM)}$. On the other hand, the standard 5G-AKA flow requires 3 messages exchanged between UE and SEAF, 4 messages exchanged between SEAF and AUSF, and 3 messages exchanged between AUSF and UDM.

Lastly, during the re-authentication phase, our protocol directly authenticates the UE through the BS which requires one message exchanged between UE and BS. While it is intuitively expected that an authentication procedure without the participation of SEAF and AUSF would decrease the propagation delay between UE and UDM, since it requires fewer messages to propagate within the core network, this section is an attempt at quantifying the delay savings.

VI. CONCLUSION

We presented BDAP, a blockchain-based decentralized access control framework and associated authentication protocol for ICN-based 5G networks. BDAP efficiently prevents unauthorized mobile users from accessing restricted content and network resources as early as possible, with only minimal changes to the 5G-ICN architecture. Our preliminary security and performance assessment shows that BDAP significantly outperforms the standard 5G-AKA. Future work includes a proof-of-concept implementation on a 5G-ICN testbed in support of further quantitative evaluation of BDAP.

REFERENCES

[1] R. Ravindran, P. Suthar, A. Chakraborti, S. O. Amin, A. Azgin, and G. Wang, "Deploying ICN in 3GPP's 5G NextGen Core Architecture," in *2018 IEEE 5G World Forum (5GWF)*, July 2018, pp. 26–32.

[2] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Access control enforcement delegation for information-centric networking architectures," in *Proceedings of the Second Edition of the ICN Workshop on Information-Centric Networking*, ser. ICN '12, 2012, p. 85–90.

[3] N. Fotiou and G. C. Polyzos, "Securing content sharing over icn," in *Proceedings of the 3rd ACM Conference on Information-Centric Networking*, ser. ACM-ICN '16, 2016, p. 176–185.

[4] S. Misra, R. Tourani, F. Natividad, T. Mick, N. E. Majd, and H. Huang, "Accconf: An access control framework for leveraging in-network cached data in the icn-enabled wireless edge," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1, pp. 5–17, 2019.

[5] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, "Live: Lightweight integrity verification and content access control for named data networking," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 308–320, 2015.

[6] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for iot security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[7] 3GPP, "Security architecture and procedures for 5g system," 2020.

[8] D. Pesavento, J. Shi, K. McKay, and L. Benmohamed, "PION: Password-based IoT onboarding over named data networking," in *ICC 2022 - IEEE International Conference on Communications*, 2022.

[9] M. Hajjar, G. Aldabbagh, and N. Dimitriou, "Using clustering techniques to improve capacity of LTE networks," in *2015 21st Asia-Pacific Conference on Communications (APCC)*, Oct 2015, pp. 68–73.

[10] M. Chatterjee, S. K. Das, and D. Turgut, "An on-demand weighted clustering algorithm (WCA) for ad hoc networks," in *Globecom '00 - IEEE. Global Telecommunications Conference.*, vol. 3, 2000.

[11] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 566–600, 2018.

[12] Y. E. H. E. Idrissi *et al.*, "Security analysis of 3GPP (LTE) - WLAN interworking and a new local authentication method based on EAP-AKA," in *International Conference on Future Generation Communication Technologies*, 2012, pp. 137–142.