Cloud Computing and Data Science
http://ojs.wiserpub.com/index.php/CCDS/

Review

Review on Authentication Algorithms in Cellular Communication Networks

Bem Sombo*, Simon Tooswem Apeh, Isi Arthur Edeoghon

Department of Computer Engineering, University of Benin, Benin City, Nigeria
E-mail: sombopeter@gmail.com

Received: 9 September 2024; **Revised:** 9 December 2024; **Accepted:** 13 December 2024

Abstract: Black market and third-party subscriber identification module (SIM) cards are often exploited by criminals, such as kidnappers, to perpetrate their nefarious activities through cellular network services while maintaining anonymity. Authentication algorithms in cellular networks are designed to ensure that only users with valid SIMs can access network services. However, vulnerabilities in these algorithms allow perpetrators to bypass security measures. This paper reviews authentication algorithms across different generations of cellular networks, including second generation (2G), third generation (3G), fourth generation (4G) and fifth generation (5G). It explains the cryptographic challenge-response mechanism fundamental to these systems and highlights the detailed authentication procedures for each network generation. The review compares these procedures in terms of computational and communication overheads and their resistance to various attacks. Furthermore, it identifies common vulnerabilities that enable perpetrators to exploit these systems while remaining anonymous. The analysis reveals that while advancements in network generations have introduced more robust cryptographic techniques, they also increase computational and communication overheads. Importantly, the authentication algorithms primarily authenticate SIM cards rather than users, leaving room for exploitation. This review offers insights for improving authentication algorithms by incorporating user-level authentication, enhancing security in existing and future network generations, including 6G and beyond.

***Keywords*:** authentication algorithms, cellular communication networks, 2G/3G/4G/5G authentication, cryptographic challenge-response mechanisms, SIM-based authentication, cellular network security, user-level authentication

1. Introduction

According to Benfarhi, Peeters, Khan & Ullah and Alezabi et al. [1-4], the authentication algorithms deployed in cellular communication networks make use of the different components of the cellular communication system to assert that a given subscription identifier indeed belongs to a particular user to prevent a fraudulent user from impersonating another user's identity, thereby not paying for the services used. The authentication process also proves that the network is indeed the network it claims to be to deny unauthorized users such as mobile subscriber identity (IMSI) catchers from engaging with the mobile station (MS)/user equipment (UE). A typical global system for mobile communication (GSM) network architecture from which other cellular network architectures evolved is depicted in Figure 1.

DOI: https://doi.org/10.37256/ccds.6120255673

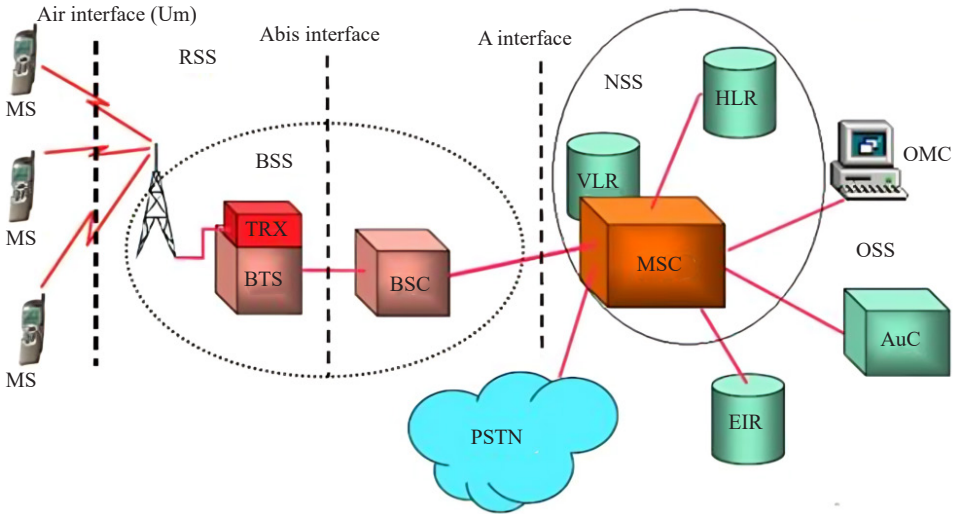

Figure 1. A typical cellular communication network [9]

According to Asplund et al., Gu and Peng, Gopikrishnan, Obaidat et al., Olsson et al. and Chinnaraji [5-10], a typical cellular communication network consists of several key components that work together to enable mobile communication. The mobile station (MS) is the user's mobile device, such as a smartphone, which contains a subscriber identification module (SIM) card. This SIM card allows the device to access the network and verifies the user's identity. The base station system (BSS) serves as a gateway between the mobile device and the main network. It includes the base transceiver station (BTS), which handles wireless communication with the mobile device, and the base station controller (BSC), which manages multiple BTSs and ensures smooth communication by coordinating their operations. The network switching system (NSS) is the core component of the network that connects mobile devices to other telecommunication networks. It interfaces with the public switched telephone network (PSTN), a global system that supports voice calls and other telecommunication services, as well as the public land mobile network (PLMN), a country-specific cellular network that uses technologies like GSM or LTE. Finally, the operation and management center (OMC) monitors and manages the network's operations. It is responsible for tasks such as fault management, which identifies and resolves network issues, and security management, which ensures the network remains secure and functions properly.

Authentication algorithms in cellular communication networks ensure that network services are accessed only by users with valid SIM cards. However, perpetrators exploit these services illegitimately by using third-party legitimate SIMs to maintain their anonymity. Therefore, this study reviews the authentication algorithms used in cellular communication networks.

The rest of the paper is organized as follows: Section 2 presents the concept of cryptographic challenge-response-based authentication. Section 3 provides a survey of authentication algorithms across generations of cellular communication networks. Section 4 presents a comparative study of authentication algorithms in cellular networks. Section 5 discusses the application of machine learning for parallel authentication enhancement in cellular networks, and Section 6 concludes the paper and highlights future trends.

2. Concept of cryptographic challenge response based authentication

Cryptographic challenge response based authentication is a type of authentication algorithm employed in cellular communication networks for verifying the legitimacy of a SIM in the device requesting access to the network resources [11]. Cryptographic challenge-response based authentication operates on a simple yet secure principle. In this authentication method, the server first sends a random challenge, which is a piece of data, to the client. The client then uses a cryptographic key or algorithm to generate a response based on this challenge and sends the response back to the

server. The server verifies the response by comparing it with the expected result. If the response is correct, it confirms that the client possesses the secret key and is authenticated. This process ensures secure authentication by confirming the client's identity without transmitting the secret key over the network. This method offers several advantages, including enhanced security as the shared secret is not transmitted over the network, flexibility in choosing cryptographic algorithms, and relative efficiency depending on the specific implementation.

The cryptographic challenge-response based authentication in cellular communication networks has evolved over the years, from one-way authentication to two-way authentication. In a one-way authentication process, the mobile subscriber (user) is authenticated by the cellular network, whereas in a two-way authentication process, both the mobile subscriber (user) and the cellular network authenticate each other before establishing a secure communication channel [4, 12]. The specifics of authentication algorithms vary in different network generations depending on the cellular technology being used. However, authentication algorithms employed in different cellular technologies have a common goal of verifying the legitimacy of a SIM card requesting access to the network services.

3. A survey of authentication protocols in cellular communication networks

Authentication protocols are sets of rules and procedures used to verify the identity of users, devices, or entities attempting to gain access to a system, network, or service [13]. The primary purpose of authentication protocols is to ensure that only authorized individuals or entities are granted access, while unauthorized users are denied entry.

Authentication protocols in cellular communication networks play a crucial role in ensuring the security and privacy of mobile users [3]. These protocols are designed to verify the legitimacy of SIM cards within the cellular network before granting users access to network services [14]. Without proper authentication, users with illegitimate SIM cards could gain access to network services and potentially exploit these services unlawfully.

According to Nakarmi [12], Mishra and Modi, Al-Tawil et al., Mobarhan et al., Xenakis and Merakos [15-18], Alezabi et al. [4], Ekene et al., Gupta et al. [19-20], Huang et al. and Jiang and Han [13, 21], the various authentication algorithms employed across different generations of cellular communication networks are reviewed in subsections 3.1 through 3.4.

3.1 *Authentication algorithm in 2G/GSM/GPRS/EDGE cellular network*

The authentication algorithm in second-generation (2G) cellular networks uses the mobile station (MS) and core network components to verify the legitimacy of the subscriber identity module (SIM) in the user's MS when requesting access to the network. The mobile services switching centre (MSC), serving the GPRS support node (SGSN) and visitor location register (VLR) represent the 2G roaming core network (roaming CN). The authentication centre (AuC) and home location register (HLR) represent the 2G home core network (home CN). When the MS requests access to the network, it sends the SIM identity, the international mobile subscriber identity (IMSI), to the roaming CN. The roaming CN forwards the IMSI and an authentication request to the AuC/HLR at the home CN. The HLR checks the IMSI in the database to ensure that it is valid and belongs to the network. After validation, the secret key (K) associated with the IMSI is extracted, and the AuC generates a random number (RAND). The authentication algorithm (A3) in the AuC uses RAND and K as inputs to generate an expected signed response (XRES). The AuC forwards the generated RAND and XRES to the roaming CN, which forwards only the RAND to the MS and keeps the XRES. The MS uses the RAND and the K stored in the SIM card as inputs to the A3 algorithm in the SIM card to generate a signed response (RES). The MS forwards the generated RES to the roaming CN, which compares the signed responses from the AuC and the MS. Thus, the roaming CN authenticates the UE by checking the 32-bit RES and XRES. Authentication in 2G is one-sided, where the roaming CN authenticates the UE, but the UE does not authenticate the network. After successful authentication, both the mobile station and the network generate session keys (CK) using the shared secret (K) and the RAND. The 64-bit CK is shared between the UE and the roaming CN, which enables encryption. The authentication flow in 2G cellular networks is shown in Figure 2.

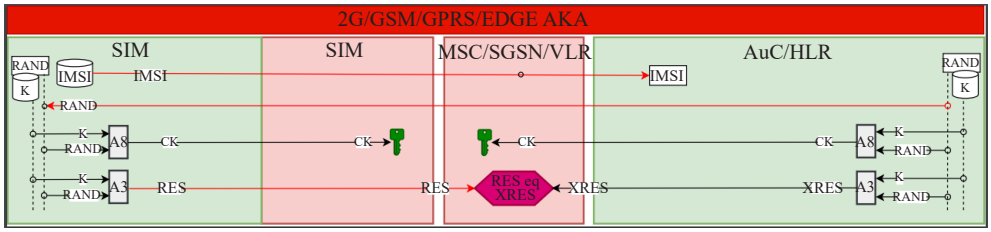

Figure 2. Authentication flow in GSM system [12]

The authentication algorithm in 2G cellular networks utilizes SIM card security, authentication vector, and IMSI validation to ensure secure subscriber authentication. However, 2G authentication is limited to one-way verification, where the network verifies the device's identity but not vice versa. While this was sufficient for early mobile networks, it is vulnerable to attacks like IMSI catchers. To address these issues, 3G and 4G cellular networks introduced mutual authentication.

3.2 *Authentication algorithm in 3G/UTMS cellular network*

The third-generation (3G) cellular network utilizes user equipment (UE) and core network components, as illustrated in Figure 3, for authentication. This authentication process in the 3G network enables two-way verification of both the user equipment (UE) and the home core network (home CN). The authentication process is initiated when the UE requests access to the network. The roaming network then sends an authentication data request to the HLR/AuC in the subscriber's home network. The home network (AuC/HLR) generates a random number (RAND). It also generates an authentication token (AUTN) using the f1 message authentication function, the f5 key generating function, AMF, and SQN, as well as an expected signed response (XRES) using the f2 authentication function. These authentication vectors are transmitted to the roaming network, which forwards the AUTN and RAND to the UE and keeps the XRES. The AUTN and RAND are then used to challenge the UE requesting access to the network. The UE deduces the message authentication code (MAC) from the AUTN received from the network, computes the expected message authentication code (XMAC) using the f1 function for computing MAC, and compares the deduced MAC with the computed XMAC. Thus, the UE authenticates the home CN by checking the 64-bit MAC and XMAC and by verifying that the 48-bit SQN is within the acceptable range. The UE generates a signed response (RES) and forwards it to the roaming network, which compares the RES with the expected signed response (XRES) stored there. Thus, the roaming CN authenticates the UE by checking 32- to 128-bits RES and XRES. The mobile station and the network generate security keys for encryption (CK) and integrity protection (IK) using the f3 and f4 functions, which use K and RAND. The 128-bit CK and IK are shared between the UE and the Roaming CN. This enables both encryption and integrity protection. Figure 3 illustrates the authentication flow in the 3G cellular network.

The authentication algorithm in the 3G network offers two-way authentication, ensuring both the user equipment (UE) and the serving network (SN) are authenticated. It uses a private key (K), International Mobile Subscriber Identity (IMSI), and a randomly generated number (RAND) to generate unique authentication vectors, preventing replay attacks. The challenge-response mechanism with authentication tokens (AUTN) and message authentication codes (MAC) enhances security by incorporating sequence number (SQN) validation to prevent replay attacks. Mutual authentication offers security against IMSI catchers, and the integrity protection provided by the integrity key (IK) enhances this security.

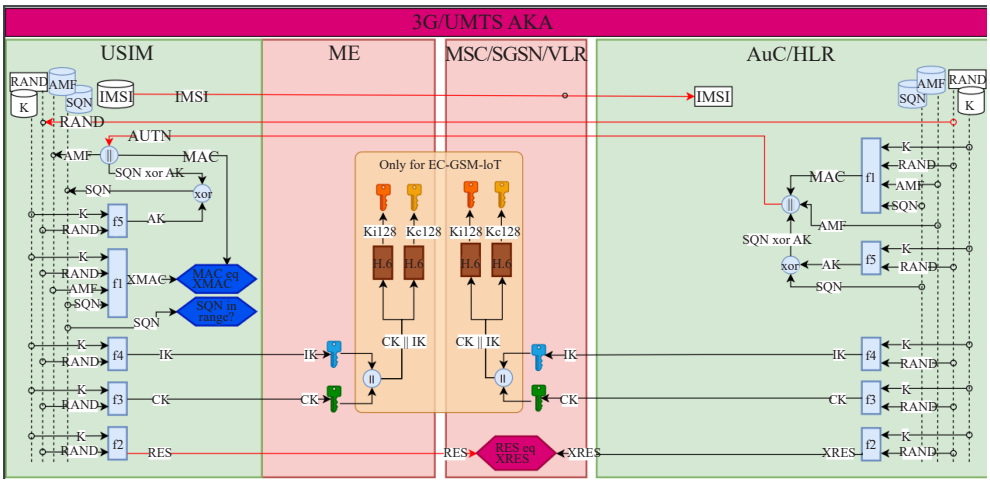

Figure 3. Authentication flow in UTMS network system [12]

3.3 *Authentication algorithm in 4G/LTE cellular network*

In 4G networks, the AKA (authentication and key agreement) process ensures that the user equipment (UE) and the network are authenticated based on the type of network the UE uses to access the mobile operator's core infrastructure. When a UE connects to a 3GPP access network, the authentication process for authenticating the UE and the network is illustrated in Figure 4. The Mobility Management Entity (MME) and AuC/HSS in Figure 4 represent the roaming core network (roaming CN) and home core network (home CN), respectively. The home CN generates and sends authentication vectors to the roaming CN, which forwards the AUTN and RAND to the UE and keeps the expected signed response (XRES). The UE derives a message authentication code (MAC) from the authentication token (AUTN), and also computes a signed response (RES) using RAND and the subscriber key (K) stored in the UE. The RES is sent to the roaming CN, which compares it with the expected signed response (XRES) stored in the roaming CN. If the signed responses match, the roaming network has successfully authenticated the UE by checking the 32-to-128 bits of RES and XRES. The UE computes an expected message authentication code (XMAC) and uses the MAC derived from the AUTN to authenticate the home CN by checking the 64-bit MAC and XMAC, and verifying that the 48-bit SQN is within the acceptable range. The UE authenticates the roaming CN by binding the 24-bit serving network identity (SNID) to KASME. This enables serving network binding, so that session keys generated for one roaming network cannot be used in another. The UE checks the service type by verifying that the Authentication Management Field (AMF) bit 0 is 1. The 256-bit KASME is shared between the UE and the Roaming CN, from which encryption and integrity protection keys are derived. The authentication flow in 4G networks for 3GPP access is shown in Figure 4 below.

When a mobile device (UE) connects to an untrusted non-3GPP network, the authentication and key agreement (AKA) process ensures authentication using the Extensible Authentication Protocol (EAP)-AKA, as specified in IETF RFC 4,187. The 3GPP AAA server and the AuC/HLR/HSS in Figure 5 represent the home core network (home CN). The process begins with the home CN generating the authentication vectors. The authentication token (AUTN) and a random number (RAND) from the vectors are sent to the UE, while the expected signed response (XRES) is retained in the home CN. The UE computes RES using RAND and the subscriber key (K) stored in the UE and sends the RES to the home CN; the Home CN authenticates the UE by checking the 32- to 128-bit RES and XRES. The UE extracts the message authentication code (MAC) from the AUTN and computes the expected message authentication code (XMAC); the UE authenticates the Home CN by checking the 64-bit MAC and XMAC and by verifying that the 48-bit SQN is within an acceptable range. The 512-bit Master Session Key (MSK) and 512-bit Extended Master Session Key (EMSK) are shared between the UE and the Roaming CN, and between the UE and the Home CN respectively. These keys are used to establish encryption and integrity protection, ensuring that data exchanged between the UE and the network is securely protected against unauthorized access. The mutual authentication and key exchange process prevents potential security threats, ensuring the legitimacy of both the device and the network in untrusted non-3GPP environments. The authentication flow in 4G networks for untrusted non-3GPP network access is shown in Figure 5.

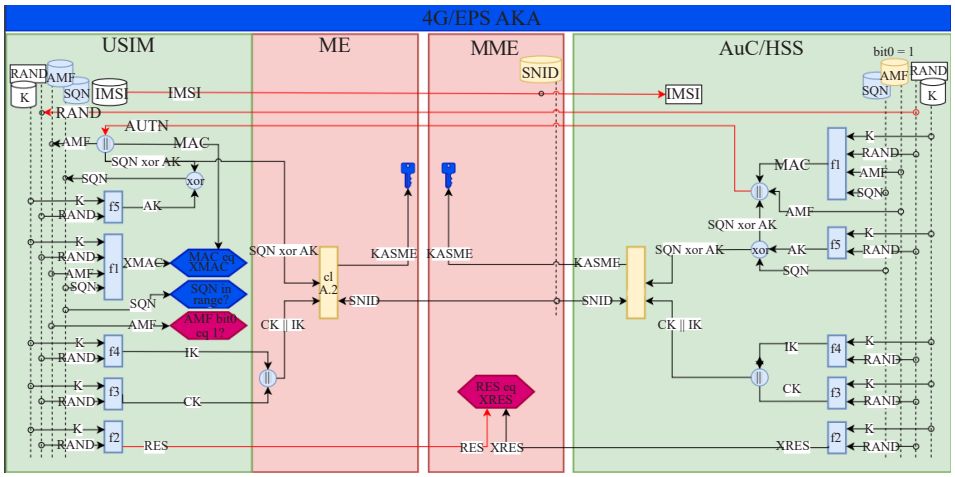

Figure 4. AKA flow in a 4G cellular network when the UE connects to a 3GPP access network [12]

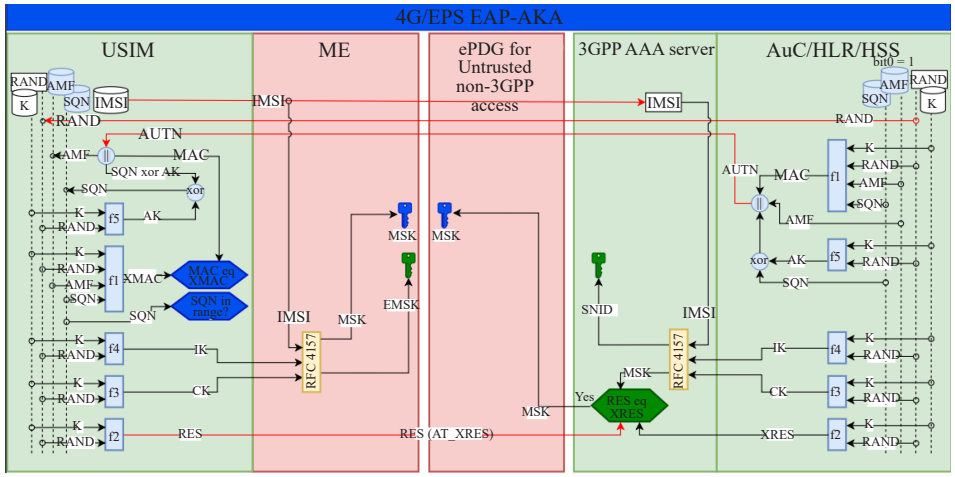

Figure 5. AKA flow in a 4G cellular network when the UE connects to an untrusted non-3GPP access network [12]

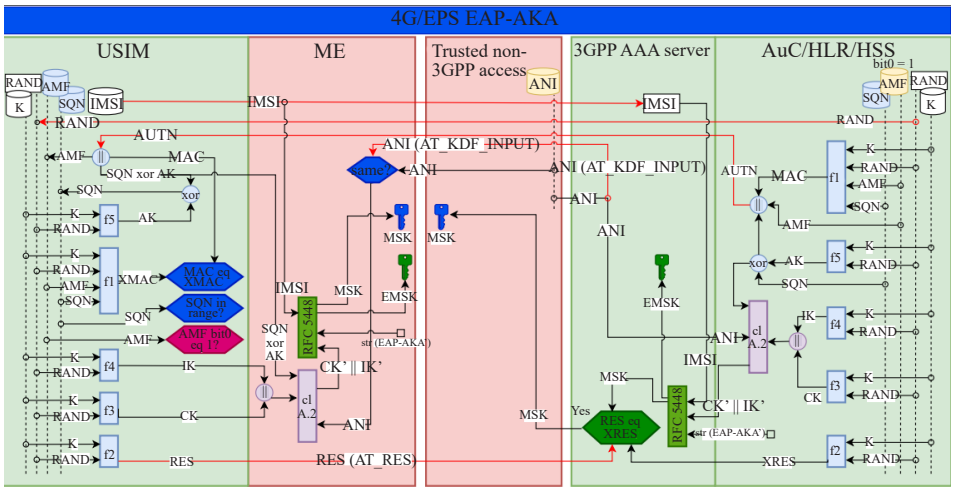

Figure 6. AKA flow in a 4G cellular network when the UE connects to a trusted non-3GPP access network [12]

When a user equipment (UE) connects to a cellular network via a trusted non-3GPP network, the authentication and key agreement (AKA) process provides authentication using EAP-AKA', a protocol specified in IETF RFC 5,448. The home core network (home CN) responds to the UE's request for network access by generating authentication vectors, from which the authentication token (AUTN) and a random number (RAND) are sent to the UE, while the expected signed response (XRES) is retained in the home CN. The UE computes a signed response (RES) using RAND and the subscriber key (K) stored in the UE. The RES is sent to the home CN, which then authenticates the UE by comparing the 32- to 128-bit RES and XRES. The UE extracts the message authentication code (MAC) from the AUTN and computes the expected message authentication code (XMAC). It authenticates the home CN by comparing the 64-bit MAC and XMAC and verifying that the 48-bit SQN is within the acceptable range. The UE authenticates the roaming CN by explicitly checking the access network identity (ANI) sent by the home CN and binding the variable-length ANI to CK' || IK'. This ensures that session keys generated for one roaming network cannot be used in another. The UE checks the service type by verifying that the AMF bit 0 is 1. The service type is also bound to CK' || IK' because the ANI contains the service code. MSK (Master Session Key) and EMSK (Extended Master Session Key) are also bound to the IMSI. MSK and EMSK are also bound to the authentication method because of the 'EAP-AKA' input string. The 512-bit MSK and 512-bit extended master session key (EMSK) are shared between the UE and the Roaming CN, and between the UE and the Home CN respectively. These keys are used to provide encryption and integrity protection for secured data exchanged between the UE and the network. The authentication flow in 4G networks for trusted non-3GPP network access is shown in Figure 6.

3.4 *Authentication algorithm in 5G cellular network*

5G AKA and 5G EAP-AKA are variants of the 5G authentication and key agreement (AKA) process. The 5G AKAs are used for all accesses. The security anchor function (SEAF) and access mobility management function (AMF) represent roaming CN. The authentication server function (AUSF), subscription identifier de-concealing function (SIDF), unified data management (UDM), the authentication credential repository and processing function (ARPF) represent home CN. In 5G AKA, the UE first identifies itself with a subscription concealed identifier (SUCI), which can only be decrypted by the home core network (home CN), thus safeguarding the user's identity. During the authentication process, the home CN generates the authentication token (AUTN), random number (RAND), and expected signed response (XRES*). The XRES* is stored in the home CN, and it is also used with the RAND to compute HXRES*, which is sent to the roaming CN. The AUTN and RAND are sent to the UE, which derives MAC from the AUTN and compares the derived MAC with its computed XMAC to authenticate the Home CN by checking the 64-bit MAC and XMAC and by verifying that the 48-bit SQN is within an acceptable range. The UE also computes RES using K and RAND, the computed RES is used with RAND to generate RES*, which is sent to the roaming CN, where the RES* is used with RAND to compute HRES*. The roaming CN authenticates the UE by checking 128-bit HRES* and HXRES*. The RES* in the UE is also sent to the home CN. The home CN authenticates the UE by checking 128-bit RES* and XRES*. The UE authenticates the Roaming CN by binding the variable length Serving Network Name (SNN) to KAUSF, and KSEAF. The SNN is also bound to RES* and XRES*. This provides serving network binding. The UE checks service type by verifying that the AMF bit 0 is 1. Service type is also bound to KAUSF, KSEAF, RES*, and XRES* because SNN contains the service code string "5G". The anti-bidding down between architectures (ABBA) is achieved by binding the ABBA value to KAMF. The user identifier binding is achieved by binding SUPI to KAMF. The 256-bit KAMF and 256-bit KAUFS are shared between the UE and the roaming CN, and between the UE and the home CN respectively. The authentication flow in 5G AKA is shown in Figure 7.

The 5G EAP-AKA' protocol enables mutual authentication between the user equipment (UE) and the core networks. The UE identifies itself with a subscription concealed identifier (SUCI), which can only be de-concealed by the home CN, protecting user privacy. The authentication is based on EAP-AKA' specified in IETF RFC 5448. During the authentication process, the home CN generates the authentication vectors: AUTN and RAND. The AUTN and RAND are sent to the UE, while XRES is kept in the home CN. The UE uses RAND and K stored in the UE to generate RES, which is sent to the home CN. The home CN authenticates the UE by checking the 32- to 128-bit RES and XRES.

The UE extracts MAC from the AUTN it received from the network; it compares its computed XMAC and MAC. The UE then authenticates the Home CN by checking 64-bits MAC and XMAC and by verifying that 48-bits SQN is within acceptable range. The UE authenticates the roaming CN by explicitly checking the SNN sent by the home CN and binding the variable length SNN to CK' || IK', KAUSF, and KSEAF. This ensures that session keys generated for one roaming network cannot be used in another. The UE checks the service type by verifying that the AMF bit 0 is 1. The service type is also bound to CK' || IK', KAUSF, and KSEAF because the SNN contains the service code string "5G". KAUSF (and implicitly KSEAF) is bound to the authentication method because of "EAP-AKA" input as a string. The anti-bidding down between architectures (ABBA) is achieved by binding the ABBA value to KAMF. The user identifier binding is achieved by binding SUPI to KAMF. The 256-bits KAMF and 256-bits KAUSF are shared between the UE and the Roaming CN, and between the UE and the Home CN respectively. The authentication flow in 5G EAP-AKA' is shown in Figure 8.

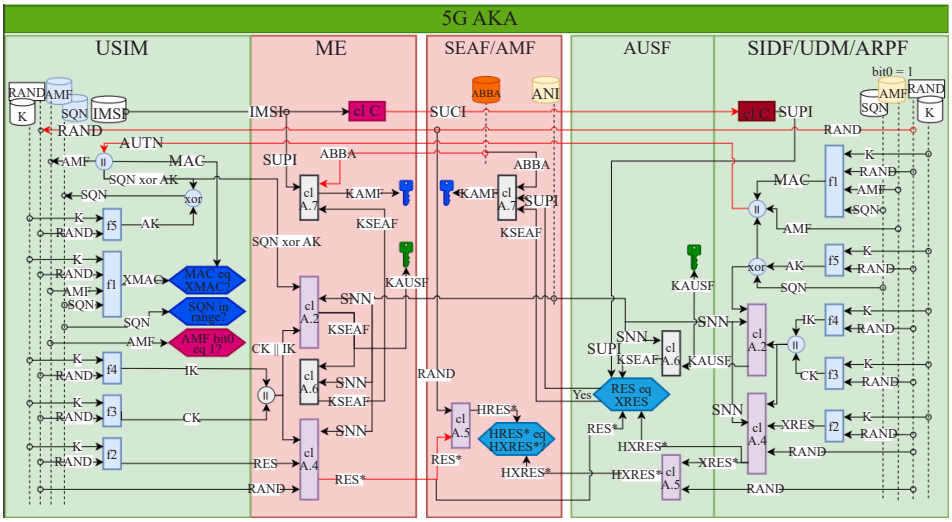

Figure 7. Authentication flow in 5G AKA [12]

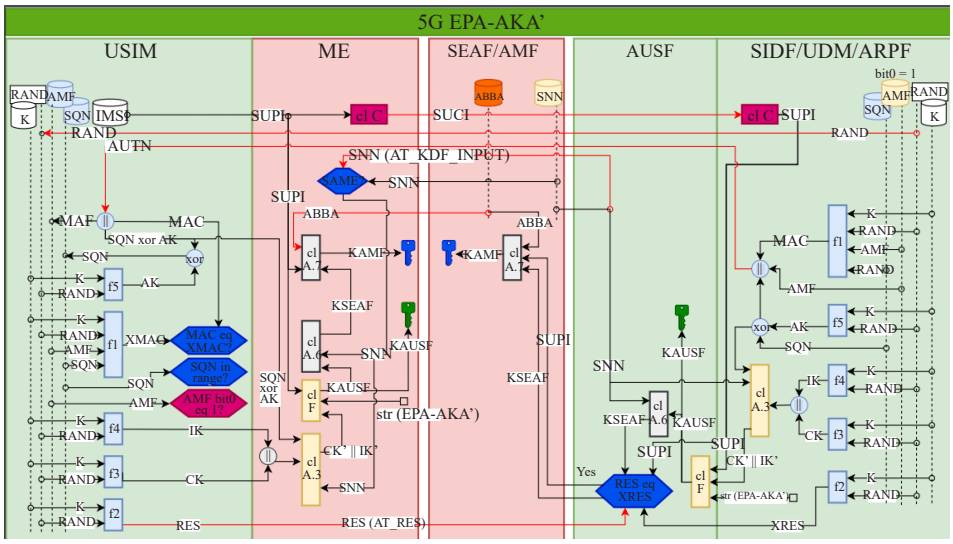

Figure 8. Authentication flow in 5G EAP-AKA [12]

4. Comparative review of the authentication in cellular communication networks

Authentication algorithms in different generations of cellular communication networks vary in their protocols. Each generation of cellular technology (e.g., 2G, 3G, 4G, 5G) has introduced advancements in security, including improvements in the authentication process. As cellular networks have evolved, authentication protocols have advanced to provide stronger security, better privacy protection, and improved mutual authentication between devices and networks. Table 1 presents a comparative study of authentication protocols in cellular communication networks based on various criteria. The criteria include:

i: computation overhead: This refers to the amount of processing power and time required by a device or network to perform the authentication process. Lower computation overhead means the authentication is faster and uses fewer resources.

ii: communication overhead: This involves the amount of data that needs to be exchanged between devices and the network during authentication. Lower communication overhead means less data is transmitted, which can lead to faster and more efficient authentication.

iii: Resistance to attacks (such as replay, man-in-the-middle, and brute-force attacks): This measures how well the authentication protocols can defend against various types of cyber attacks, such as replay attacks (where an attacker reuses old data), man-in-the-middle attacks (where an attacker intercepts and possibly alters communication), and brute-force attacks (where an attacker tries many combinations to break in).

iv: SIM user verification: This assesses how effectively the authentication protocols can verify that the person using the SIM card is a legitimate user. This is important for preventing unauthorized users from exploiting to the network the network services.

The computational and communication overhead in AKA protocols across different generations of cellular networks are measured by analyzing the number of signaling exchanges, data exchanges, and individual steps involved in each authentication process. These metrics provide a comparative basis for understanding the processing requirements and data transmission load in each protocol.

The resistance to attacks is determined for AKA protocols across cellular network generations by using comparative measures for each attack type. Replay attack resistance is assessed by evaluating whether a protocol can detect and reject any reused (or "replayed") authentication requests; protocols that use changing sequence numbers or unique nonces validated by both the UE and the network tend to be more resistant. Man-in-the-middle (MITM) attack resistance is measured by the robustness of mutual authentication mechanisms in each protocol, as stronger mutual authentication significantly reduces vulnerability to MITM attacks. Brute force attack resistance is evaluated based on the cryptographic key length; protocols with longer keys offer higher resistance against brute force attempts. Together, these measures provide a basis for comparing the attack resistance capabilities of AKA protocols across different cellular network generations. The SIM user verification in an AKA protocol is determined by analyzing the protocol's ability to verify the actual SIM user in the cellular communication network.

The comparison of authentication and key agreement (AKA) protocols across various generations of cellular communication networks in terms of computational overhead, communication overhead, resistance to attacks, and user verification is shown in Table 1.

Table 1. A comparative evaluation of the authentication protocols in cellular communication network

Generation	Authentication protocol	Computation overhead	Communication overhead	Resistance to attacks (Replay, MITM, Brute force)	SIM user verification
2G (GSM)	A3/A8	Low	Low	Low	Indirect
3G (UMTS)	UMTS AKA	Moderate	Moderate	Moderate to High	Indirect
4G (LTE)	EPS-AKA	Moderate	Moderate	High	Indirect
5G	5G-AKA, EAP-AKA'	High	High	Very High	Indirect

The attributes compare the authentication protocols across 2G, 3G, 4G, and 5G cellular networks in terms of computation and communication overhead, as well as resistance to various attacks. 2G (GSM) has low computation and communication overhead due to simple algorithms but offers weak resistance to replay, man-in-the-middle (MITM), and brute-force attacks. 3G (UMTS) introduces moderate computation and communication overhead with improved security, providing better resistance to replay attacks and moderate protection against MITM and brute-force attacks. 4G (LTE) maintains moderate overhead while enhancing resistance to all types of attacks with stronger encryption and mutual authentication. 5G incurs high overhead due to advanced cryptographic techniques, offering very high resistance to replay, MITM, and brute-force attacks, making it the most secure generation. The authentication protocols in all generations of cellular communication networks do not verify the SIM user but rather verify the legitimacy of the SIM card through which a user requests network services.

The delays caused by computational and communication overheads in different generations of cellular networks can noticeably impact user experience. Higher computational overhead may slow down authentication and increase power consumption, which could lead to faster battery drain, especially for devices with limited resources. Similarly, higher communication overhead, such as extra signaling or data exchanges, can lead to delays in connecting calls, accessing the internet, or switching networks, which users might perceive as lag or slow service. Perpetrators exploit indirect user verification to commit crimes via the black market or third-party SIMs, remaining anonymous. In newer generations like 5G, although the technology is optimized for faster speeds and lower latency, the added complexity in security protocols may still cause some initial delays, particularly in areas with weaker network coverage. Balancing these overheads while maintaining security and efficiency is the key to ensuring a smooth and responsive experience for end users.

5. Application of machine learning for parallel authentication enhancement in cellular networks

Authentication algorithms in cellular communication networks, regardless of generation (2G, 3G, 4G, or 5G), primarily allow access to network resources only for users with valid SIM cards by verifying the legitimacy of the SIM within the network [22]. In 2G, the authentication algorithm verifies only the legitimacy of the SIM card, while in 3G, 4G, and 5G, the algorithm additionally verifies the legitimacy of the network [23, 24]. However, a critical vulnerability persists across all generations: the identity of the SIM card user is not authenticated, leaving the system susceptible to misuse. Perpetrators can exploit this gap by using black market or third-party SIM cards, accessing network services while maintaining anonymity, and potentially engaging in fraudulent or malicious activities.

Machine learning algorithms, particularly supervised learning techniques, can be trained to recognize the unique characteristics of a speaker's voice, distinguishing between individuals based on voice features such as pitch, tone, cadence, and speech patterns [25-27]. This capability of machine learning to accurately identify speakers can be leveraged to develop an algorithm for identifying SIM users in cellular communication networks. By integrating voice biometrics into the authentication process, the algorithm can verify not only the legitimacy of the SIM card but also the identity of the person using it. This adds an extra layer of security, helping to prevent perpetrators from using black market or third-party SIM cards to access network services while maintaining anonymity. The implementation of the voice biometrics-based algorithm to run in parallel with the authentication algorithm has the potential to enhance authentication in cellular networks by adding an additional layer of security through the recognition of SIM users.

5.1 *Potential of machine learning approach in parallel authentication enhancement in cellular networks*

The architecture of cellular communication networks evolves with each generation to accommodate new functionalities and meet changing technological demands [28]. All the generations of cellular networks can be broadly categorized into three main components: mobile station (MS), base station (BS), and core network (CN) [21]. In a 2G

cellular network and beyond, the authentication algorithm is hosted and run on a server in the core network (CN) [21, 23]. To enhance authentication in cellular networks, irrespective of the cellular network generation, including future cellular networks such as 6G or beyond, a machine learning-based algorithm utilizing voice biometrics for SIM user recognition can be deployed on a server within the cellular core network (CN). The deployment of the algorithm will require subscribers' voiceprints for its operation; the existing subscribers' information database, hosted on a server in the CN, will be updated with the subscribers' voiceprints, which will be utilized by the algorithm to recognize users. The algorithm will require a voice sample of a caller in real time for its operation; a customized application with over-the-air (OTA) capability will be designed to trigger a mobile station to capture and send voice data when it detects a specific signaling message. The application will be (remotely) installed on the SIM cards of the subscribers. Alternatively, the signaling messages in the cellular network can be modified so that a caller's voice, transmitted through the network, is duplicated in real time and used by the algorithm to recognize callers.

Thus, it is important to note that the algorithm will integrate seamlessly into the existing infrastructure, eliminating the need for any hardware modifications in either mobile networks or mobile phones. In the mobile network (core network, CN), the algorithm will reside on one of the existing servers typically located in data centers, ensuring no additional hardware requirements. In mobile phones, the functionality will be supported by a SIM applet within the SIM card, capable of capturing and transmitting a caller's voice samples to the CN for authentication. By utilizing existing hardware, the proposed approach ensures compatibility with current and future network generations. Additionally, no hardware or software modifications will be required in mobile phones if the caller's voice samples are captured directly from the CN as the voice data is routed through the network.

6. Conclusions and future trends

This review has highlighted the evolution of authentication algorithms across the various generations of cellular communication networks, from 2G through to 5G. Each generation has progressively enhanced the security of mobile communication by introducing more sophisticated authentication protocols, reflecting the increasing complexity and demands of modern mobile networks.

In 2G networks, the authentication process was straightforward, relying primarily on the SIM card for identity verification. While this method provided adequate security for its time, it was vulnerable to attacks due to its one-way nature, where only the mobile station was authenticated by the network. The introduction of mutual authentication in 3G networks marked a significant improvement, addressing many of the vulnerabilities inherent in 2G systems. The 3G authentication protocol provided a robust framework for authenticating both the UE and the network, significantly enhancing security.

The 4G networks were built upon the foundations laid by 3G, employing the evolved packet system authentication and key agreement (EPS AKA) mechanism, which further strengthened authentication processes. With the introduction of variant protocols like EPS EAP-AKA and EPS EAP-AKA', the 4G offered greater flexibility, especially in environments requiring non-3GPP access to the network.

5G networks have continued this trajectory of advancement, introducing more comprehensive authentication mechanisms that involve multiple network components and ensure a high level of security. The 5G authentication protocols, such as 5G-AKA and 5G EAP-TLS, not only offer mutual authentication but also enhance privacy and resistance to a wide range of attacks through the use of advanced cryptographic techniques.

Across all generations, the balance between computation and communication overhead, and resistance to various attacks, has been a key consideration in the design of authentication protocols. While 5G represents the pinnacle of security with its robust authentication mechanisms, it also incurs higher overhead due to its complexity. This trade-off highlights the continuous challenge of designing authentication protocols that are both secure and efficient.

The review underscores that, while authentication protocols across cellular network generations have significantly evolved, they still focus on validating the SIM card rather than verifying the SIM user directly. This highlights an area for future improvement, where user-level verification could be incorporated to enhance the security of mobile communications. A practical solution addressing this area would involve developing a voiceprint neural network-based model to create an artificial neural network-based caller authentication algorithm in cellular networks. This

algorithm would authenticate the legitimate owner of a first-time SIM user and identify third-party SIM users to prevent perpetrators from using black market and third-party SIMs to commit crimes anonymously. This approach would enhance security within cellular communication networks.

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Benfarhi Z. *Evaluation of a New Authentication and Key Agreement Protocol for 5G Network*. Final International University; 2024.

[2] Peeters C. *Developing End-To-End Security Solutions for Redirection Attacks in Legacy Telecommunications Infrastructure*. University of Florida; 2022.

[3] Khan W, Ullah H. Authentication and secure communication in GSM, GPRS, and UMTS using asymmetric cryptography. *International Journal of Computer Science Issues (IJCSI)*. 2010; 7(3): 10.

[4] Alezabi KA, Hashim F, Hashim SJ, Ali BM. An efficient authentication and key agreement protocol for 4G (LTE) networks. In: *2014 IEEE Region 10 Symposium*. IEEE; 2014. p.502-507.

[5] Asplund H, Karlsson J, Kronestedt F, Larsson E, Astely D, von Butovitsch P, et al. *Advanced Antenna Systems for 5G Network Deployments: Bridging the Gap Between Theory and Practice*. Academic Press; 2020.

[6] Gu G, Peng G. The survey of GSM wireless communication system. In: *2010 International Conference on Computer and Information Application*. IEEE; 2010. p.121-124.

[7] Gopikrishnan K. *Architecture of a General Cellular Communication System*. Technobyte; 2020.

[8] Zarai F, Nicopolitidis P. *Modeling and Simulation of Computer Networks and Systems: Methodologies and Applications*. Morgan Kaufmann; 2015.

[9] Chinnaraji A. *Wireless and Cellular-Mobile Communication Architecture*. Zenodo; 2023

[10] Olsson M, Mulligan C. *Epc and 4G Packet Networks: Driving the Mobile Broadband Revolution*. Academic Press; 2012.

[11] Bakaul M, Islam M, Ahad H, Rahman S. Security in gsm networks. *International Journal of Computer Applications*. 2020; 177: 36-39.

[12] Nakarmi PK. Cheatsheets for Authentication and Key Agreements in 2G, 3G, 4G, and 5G. *arXiv: 2107.07416*. 2021. Available from: https://arxiv.org/abs/2107.07416.

[13] Huang X, Yoshizawa T, Baskaran SBM. Authentication mechanisms in the 5G system. *Journal of ICT Standardization*. 2021; 9(2): 61-78.

[14] Kazmi SHA, Hassan R, Qamar F, Nisar K, Ibrahim AAA. Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. *Symmetry*. 2023; 15(6): 1147.

[15] Mishra S, Modi N. GSM Mobile Authentication Based on User SIM. *International Journal of Computer Science Trends and Technology*. 2014; 2(6): 121-125.

[16] Al-Tawil K, Akrami A, Youssef H. A new authentication protocol for GSM networks. In: *Proceedings 23rd Annual Conference on Local Computer Networks*. IEEE; 1998. p.21-30.

[17] Mobarhan MA, Mobarhan MA, Shahbahrami A. Evaluation of security attacks on UMTS authentication mechanism. *International Journal of Network Security & Its Applications*. 2012; 4(4): 37.

[18] Xenakis C, Merakos L. Security in third generation mobile networks. *Computer Communications*. 2004; 27(7): 638-650.

[19] Ekene OE, Ruhl R, Zavarsky P. Enhanced user security and privacy protection in 4G LTE network. In: *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*. IEEE; 2016. p.443-448.

[20] Gupta S, Parne BL, Chaudhari NS. Security vulnerabilities in handover authentication mechanism of 5G network. In: *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*. IEEE; 2018. p.369-374.

[21] Jiang W, Han B. *Cellular Communication Networks and Standards: The Evolution from 1G to 6G*. Textbooks in Telecommunication Engineering. Springer; 2024.

[22] Ahmed AS. *Advancing Authentication for Cellular Networks and Mobile Users*. Aalto University Publication

Series; 2023.
[23] Benfarhi Z, Gemikonakli O, Mobarhan MA. Evaluation of authentication and key agreement approaches of 5g networks. In: *The International Conference on Artificial Intelligence and Applied Mathematics in Engineering*. Cham: Springer Nature Switzerland; 2023. p.194-221.
[24] Zukarnain ZA, Muneer A, Ab Aziz MK. Authentication securing methods for mobile identity: Issues, solutions and challenges. *Symmetry*. 2022; 14(4): 821.
[25] Kane J, Johnstone MN, Szewczyk P. Voice synthesis improvement by machine learning of natural prosody. *Sensors*. 2024; 24(5): 1624.
[26] Dhakal P, Damacharla P, Javaid AY, Devabhaktuni V. A near real-time automatic speaker recognition architecture for voice-based user interface. *Machine Learning and Knowledge Extraction*. 2019; 1(1): 504-520.
[27] Ahmad R, Iqbal A, Jadoon MM, Ahmad N, Javed Y. XEmoAccent: Embracing diversity in cross-accent emotion recognition using deep learning. *IEEE Access*. 2024; 12: 41125-41142.
[28] Rost P, Banchs A, Berberana I, Breitbach M, Doll M, Droste H, et al. Mobile network architecture evolution toward 5G. *IEEE Communications Magazine*. 2016; 54(5): 84-91.