International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Security Improvement of Authentication and Key Agreement Protocol for Subscriber Identity

Hitesh T. Loriya[1], Navinkumar T. Ganeshan[2], Rahul R. Keshwala[3]

Submitted:15/12/2023 **Revised**: 19/01/2024 **Accepted**: 28/01/2024

Abstract: Subscriber identity security is critical for wireless communication networks. Fake base stations with stronger signal strength than genuine stations attract subscribers to register with fake base stations. An attacker can try bidding down the attack. In this attack, attacker tries to persuade UE and the network entities that opposite side doesn't uphold a security features, despite the fact that the two sides as a matter of fact uphold security features. It opens the gate for various kinds of attacks by taking advantage of the security limitations of old-generation mobile networks. This paper examined security advances and issues related to wireless communication networks. In the first place, 5G architecture is examined. Second, it focuses on a framework of security-based plan for the 5G network. Third, security flaws found in wireless communication networks are examined, with a focus on key confirmation and authentication mechanism. In this paper, we present a strong authentication and key agreement protocol for the 5G network. The proposed protocol's goal is to improve security of subscriber identity against different types of attacks by sending them over channel. There is no need to modify the network's fundamental foundation for the proposed authentication and key agreement (AKA) protocol. The proposed protocol is verified using the ProVerif tool and shows that it further strengthens the security of authentication and key agreement procedure of wireless communication network.

Keywords: *5G Network, 4G Network, AKA, Security, LTE, EPS*

1. Introduction

5G System Architecture is a service-based architecture as shown in Figure 1 [1]. It provides efficiency, modularity, flexibility and consists of many essential network functions performing unique tasks in establishing and maintaining complete communication among applications, users, and devices. The primary features of the 5G Core Network are covered in this section. The functionalities like packet routing and data forwarding are handled by the User Plane Function (UPF) to ensure effective communication between external networks and services with User Equipment (UE) by ensuring reliable data delivery, low latency, and high throughput for bandwidth-hungry applications. The control functions and signaling are handled by the Control Plane Function (CPF) by authentication, mobility management, and session establishment. The CPF is an important component of the system in ensuring QoS, seamless connectivity, and network resource optimization as well as connection and mobility, and network policy handling is done by CPF by staying in communication with UE. The data flow and user session management are the key responsibilities of the Session Management Function (SMF).

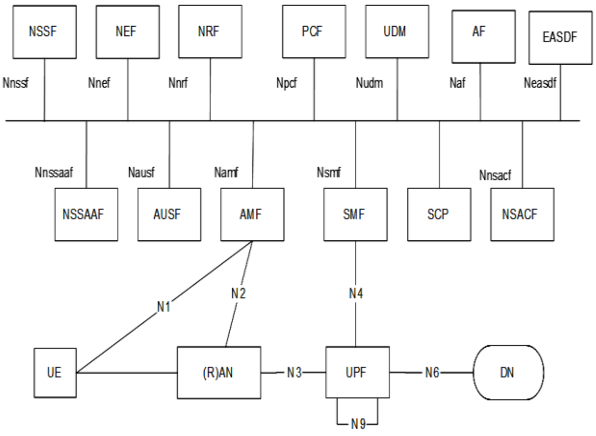


Fig 1: 5G System Architecture

Active user sessions are managed by maintaining QoS needs, session rates, and user identity details. Mobility and access-related functionalities are supervised by the Access and Mobility Management Function (AMF) which ensures seamless connectivity between the users by performing handover, registration, and authentication. The 'Middle-Man', Security Anchor Function (SEAF), residing within the serving network and closely with AMF, handles the authentication process between the Home Network and User Equipment. The SLAs (Service Level Agreements) and implementation of network policies are handled by the Policy Control Function (PCF). The PCF handles key tasks like policy enforcement, traffic management, QoS protocol handling, and dynamic resource allocation. One of the most important tasks of authenticating users by verifying user

[1] *Electronics & Comm. Engineering, L.E. College, Morbi, INDIA*
[2] *Electronics & Comm. Engineering, V.G.E.C., Chandkheda, INDIA*
[3] *Information Technology Engineering, L.E. College, Morbi, INDIA*
** Corresponding Author Email: hitesh_loriya@yahoo.co.in*

credentials is handled by the Authentication Server Function (AUSF) by storing, retrieving, and comparing the passwords, keys, and other unique user identities which ensures the security and integrity of the users. The user subscription and identity are managed by the function known as Unified Data Management (UDM) by preserving the data like user credentials for authentication, subscription details, and user profiles, to offer seamless services.

2. 5G Security architecture

The 3GPP board serves as a demonstration of 5G security architecture [2] as shown in Figure 2.

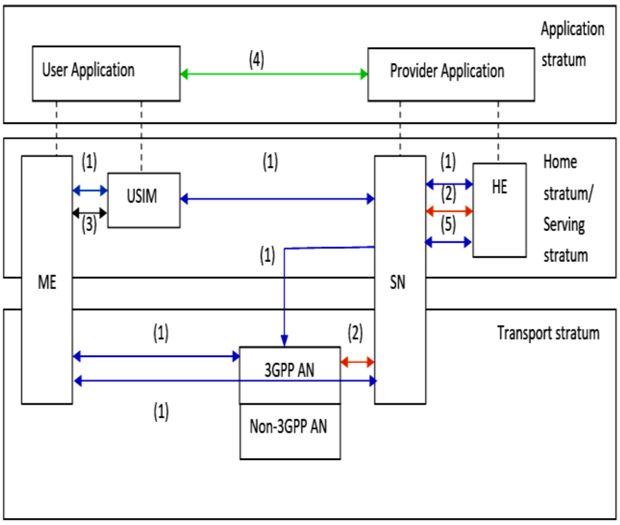


Fig 2: 5G security architecture

The five head security levels are in architecture. (1) Network access security: At this level, UEs are granted secure access to the core network and are protected from radio association attacks. (2) Network domain security: This level provides protection against different wireline network attacks and allows entities to safely exchange user and signaling data (both within and between AN and SN). (3) User domain security: At this stage, ME and USIM have mutual approval. (4) Application region security: This level allows for the safe exchange of messages between applications running in the client and provider spaces. (5) Service based architecture (SBA) space security: which is the set of security features in regards to SBA. These incorporate the network component enrolment, revelation, and approval security viewpoints, as likewise the security for the service-based interfaces. Visibility and configurability: This level permits client to check whether a security highlight is in active or not and whether the utilization and arrangement of services ought to rely upon the security highlight. This security level isn't displayed in the figure.

3. Security vulnerabilities and related work

As soon as a subscriber enrols for first time, unique verification cycle known as authentication and key agreement (AKA) procedure is triggered. This occurs by sending subscriber unique identity over a radio channel, such as an airport where all new customers turn on their phones. Fake base stations have the potential to register users by having a stronger grounded signal than real base stations. An attacker may attempt to bidding down attack. Attacker attempts to persuade UE and the network elements that the opposite side doesn't uphold a security feature, despite the fact that the two sides as a matter of fact uphold that security feature. It opens the door for different sorts of attacks by exploiting the security restrictions of old-generation mobile networks. 5G-AKA has upgrades over the 4G-AKA yet at the same time, there are some security weaknesses present in the 5G-AKA in light of direct advancement from the 4G-AKA convention. Security threats like subscriber privacy, DoS assaults, location protection, counterfeit base station assaults, and impersonation assaults on 5G networks and 4G networks have been introduced in many research papers [3-12]. 5G-AKA convention is vulnerable and the aggressor can impersonate other subscriber in a serving network [13]. Security properties of 5G AKA convention are checked based Tamarin model and a few significant issues including location protection [14-15]. Another type of attack that 5G-AKA cannot withstand is the sequence number (SQN) under specific replay attacks because of exclusive-OR (XOR) and an irregularity shortfall [16]. The 5G-AKA demonstration uses important security components (such as UE, SN, and HN) and discovers an attack that takes advantage of a possible race condition. They argued that resolving the racial condition for a just case does not guarantee that the attack will be impeded [17]. The Bana-Comon reasoning was used to analyse the privacy properties in the 5G-AKA show [18–20]. They demonstrated how the suggested show guarantees privacy properties and disclosed a novel de-synchronization attack. To hide UE and sendoff DoS assaults, aggressors can acquire partner data, collect user data, and infrequently even discussion data. Along these lines, it gives admittance to a man-in-the-centre assault [21]. A viable attack model for obtaining IMSI has been put forth in [22], according to which an effective attacker can truly reveal the IMSI and the 4G-AKA framework is unable to repel such formidable assaults. Attacker can pose as legitimate clients in order to send fictitious IMSIs repeatedly and overwhelm the HSS. HSS needs to employ its processing power to generate UE-specific irrational authentication vectors. DoS assaults can be sent off against 4G-AKA. DoS assaults have been seen to excessively annoy the substances in E-UTRAN during the NAS system [23]. Moreover, on the grounds that minimal expense base stations are presently effectively gotten by aggressors, they can use base station into a 4G network with the comfort of a base station. Voice and information transmission from the UE can be hindered by the fomenter base station, which can likewise reflect man in the middle attack. The attacker can likewise latently tune in or redirect client traffic to an alternate network by utilizing a nonconformist base station [24]. This enables aggressors to send off a man-in-the-middle attack or track the client's compact region. Although the 5G-AKA convention is intended to prevent active attacks and provide protection against risky serving networks, it may not be able to fend off a man-in-the-center attack due to the possibility of an SN impersonation [25]. Though it faces protection conservation, a modified 5G-AKA convention is suggested. Gadget personalities are sent into the air, which leads to various security breaches [26].

4. 5G security and key hierarchy

5G-AKA is developed upon 4G-AKA with the addition of newly developed security features like Serving Network Name (SNN), Non-Access Layer (NAS) and Access Layer (AS) used for different security function, as well as fresh key hierarchy to secure user and signalling information traffic. The option of integrity protection of the user plane could be seen as one of the main differences between 4G and 5G architecture. The 5G system architecture has an integration of major four security features: SEAF (SEcurity Anchor Function), AUSF (AUthentication Server Function), SIDE (Subscription Identifier De-Concealing Function) and ARPF (Authentication credential Repository and Processing Function). Mutual authentication among the user and the network is handled by AKA protocol, in which user and network agree to use a secured session key. AS and NAS, Integrity keys and cipher Keys of stratum (AS and NAS) are generated using KAUCF. gNB is the termination place for confidentiality protection, Radio network AS signalling and integrity whereas AUSF is the destination for termination of integrity, confidentiality protection NAS signaling. HN helps authenticating UE by providing subscription details. Figure 3 shows the novel key hierarchy used to derive sub-keys used in 5G architecture.

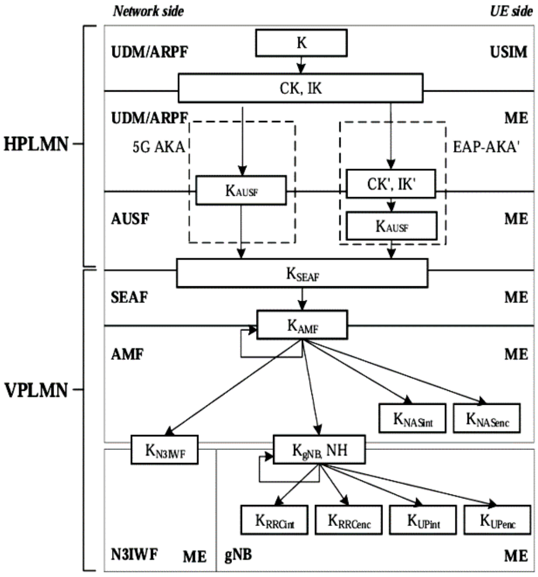


Fig 3: 5G Key Hierarchy

K and CK/IK keys are included for authentication. CK, IK helps fetching CK', and IK' in case of EAP-AKA'. K$_{UPenc}$, K$_{gNB}$, K$_{RRCenc,}$ K$_{SEAF}$, K$_{NASint}$, K$_{N3IWF}$, K$_{AMF}$, K$_{RRCint}$, K$_{UPint}$, K$_{NASenc}$ and K$_{AUSF}$ are the keys inclusions of authentication hierarchy. ME and ARPF derives the K$_{AUSF}$ key used for AUSF from CK, IK in the case of 5G-AKA and K$_{AUSF}$ is fetched by AUSF as a segment of 5G HE AV from ARPF. ME and AUSF fetches K$_{AUSF}$ from CK', IK', in EAP-AKA', which are fetched by AUSF from ARPF. ME and AUSF derives the K$_{SEAF}$ anchor key using K$_{AUSF}$, which is supplied by AUSF to the SEAF. ME and SEAF derives a K$_{AMF}$ key for AMF from K$_{SEAF,}$ which is fetched by ME and source AMF. AS and NAS security context protect the signaling and user data traffic once 5G AKA is performed and the UE and HN agree on a common session key. Four lower-level keys such as K$_{NASint}$, K$_{NASenc}$, K$_{gNB,}$ and K$_{N3IWF}$ are derived using K$_{AMF}$ among which K$_{NASint}$ and K$_{NASenc}$ protects the NAS signaling data. Integrity protection between UE and SN is handled by K$_{NASint}$. Four lower-level keys such as K$_{UPint}$, K$_{UPenc}$, K$_{RRCint}$, and K$_{RRCenc}$ are generated using K$_{gNB}$ which are used to protect AS data. K$_{UPint}$ protects integrity of user data exchange between UE and gNB. K$_{UPenc}$ is used for encryption of user data traffic between UE and gNB. K$_{RRCint}$ and K$_{RRCenc}$ maintains integrity and encryption of radio resource control traffic between UE and gNB. For forward security, Intermediate key NH and for non-3GPP access, K$_{N3IWF}$ key is derived by ME and AMF and from K$_{AMF}$. K$_{N3IWF}$ is not forwarded among N3IWFs. Key derivation is using one way function from top to bottom in downward direction. High key is never derived from low key. It protects fundamental keys and also reduces the need for periodic regeneration and transmission of fundamental keys. It speed up re-authentication process. It also protects network from effect of compromised low-key.

5. NTRU Cryptosystem

The NTRU public key cryptosystem is used by the suggested AKA protocol to secure subscriber identity. Joseph H. Silverman, Daniel Lieman, Jill Pipher and Jeffrey Hoffstein founded NTRU Cryptosystems. It is common to refer to the NTRU Public Key Cryptosystem (PKC) as NTRUEncrypt. The NTRUEncrypt public key cryptosystem, introduced by NTRU Cryptosystems Inc. at Crypto '96, is presently associated with the IEEE P1363 standard. N-th degree truncated polynomial ring is referred to as NTRU. The polynomial computation, which occurs far quicker than other fanning out encryption systems like RSA, El Gamal, and elliptic curve cryptography, is the most puzzling development during encryption and decryption. NTRU public-key computation uses the ring of polynomials.

$$R = Z[X]/(X^N - 1) \qquad \text{………………..(i)}$$

The polynomials conforming R have integer coefficients: $a(X) = a_0 + a_1X + a_2X^2 + ….... + a_{N-1}X^{N-1,}$ which are multiplied together using the extra rule $X^N \equiv 1$. The product c(X) = a(X) * b(X) is given by

$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_N b_{k+1} = \sum_{i+j \equiv k \bmod N} (a_i b_j)$ ……………….(ii)

In particular, if we write a(X), b(X), and c(X) as vectors a = [a_0, a_{1},... ,a_{N-1}], b = [b_0, b1,…. , b_{N-1}], c = [c_0, c_1,….. , c_{N-1}]

then the convolution product of two vectors with c sizes of N positions is c = a * b.

The more significant properties of NTRU PKC are the going with:

1. P and q must meet gcd(p, q) = 1 and the bounds (N, p, q) are public.

2. Polynomial coefficients are limited both mod p and mod q.

3. The polynomial A(X) 2 R that satisfies a(X) *A(X) = 1 mod q is the inverse of a(X) mod q.

5.1 Key generation

The key generation of the public key h and the secret key (f, fp) together make up the key generation. Select two irregular polynomials with "little" coefficients, f and g, from R. Denoting "little" is far less than q; typically, f {-1,0,1} for p = 3. Next, calculate fp, such as the reciprocal of f (mod p), which may be expressed as f * fp = 1 (mod p).

Process fq, which is inverse of f (mod q) and thus satisfies the following requirement:

f * fq = 1 (mod q) ……………………… (iii)

The polynomial h = g * p fq can be found.

The set (f, fp) is the secret key, while h is the public key.

5.2 Encryption

A polynomial with coefficients taken mod p is the plaintext m. It should be noted that the NTRU public-key computation does not depend on the message m being entirely converted to a polynomial structure. Randomly select a blinding message r from R with small coefficients. The encrypted text is

e = r * h + m (mod q) ……..……………….(iv)

5.3 Decoding

Using the secret key (f, fp), the decoding extracts the message m from the coded message e.

calculate a = e * f (mod q)

picking the coefficients of a to fulfill - q/2 <a_i < q/2.

Lessen a modulo p

b = a (mod p) :

Figure

c = b * fp (mod p) ……………………(v)

Then, at that point, c mod p is equivalent to the plaintext m. Detail description of NTRU cryptosystem is given by authors [27].

NTRU and ECC cryptosystem is compare in view of time necessities for key creation, encryption and decryption for security levels and based on it plots are shown in Figure 4, Figure 5 and Figure 6 [28].

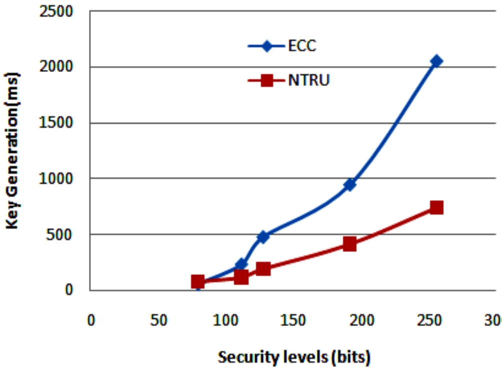


Fig 4: Security levels (bits) V/s Key creation (ms) plot of ECC & NTRU

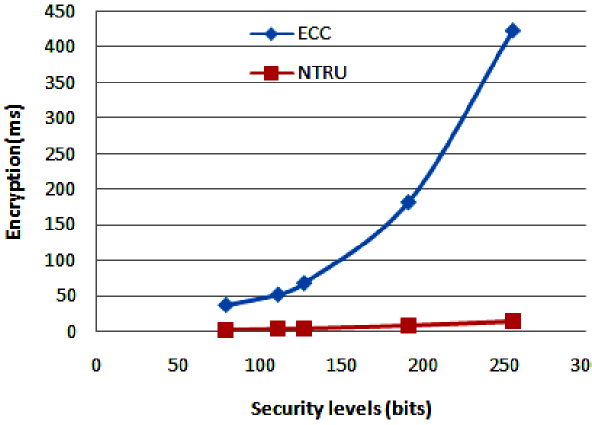


Fig 5: Security levels (bits) V/s Encryption (ms) plot of ECC & NTRU

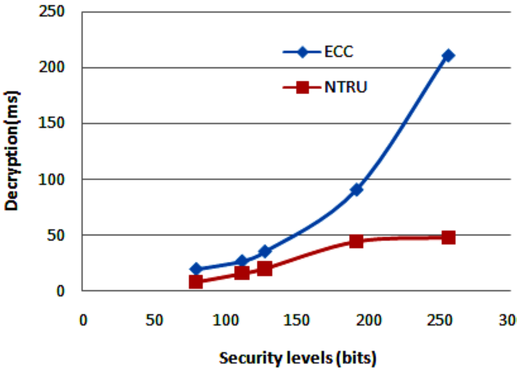


Fig 6: Security levels (bits) V/s Decryption (ms) plot of ECC & NTRU

ECC timings are provided for each and every heading structure as the min-max of the characteristics. For all security levels, NTRU is far quicker than the ECC. We can finish up from Figures 4, 5, and 6 that the performance of NTRU is better than ECC min timings. The relationship between the RSA, ECC, and NTRU implementations in terms of key generation time, encoding & decoding time is shown in Table 1[29].

Table 1: Performance comparison of RSA, ECC, and NTRU

	RSA-1024	ECC-168	NTRU-263
Public key size (bits)	1024	168	1841
Key Generation (ms)	1432	65	19.8
Encryption (ms)	4.32	140	1.9
Decryption (ms)	48.5	67	3.5

Table 1 above shows that NTRU is the quickest cryptosystem for a comparative degree of security. The NTRU block encryption is quite often quicker than the ECC block encryption. NTRU utilizes negligeable battery and central processor power. NTRU functions admirably with required gadgets where code size is a significant limitation. NTRU, by and large, brings down server usage. With regards to equipment and programming execution, NTRU is more advantageous than inspected public key cryptosystems. Moreover, it is found that discrete logarithms can be determined in polynomial time utilizing quantum PCs. Thusly, a quantum PC will break cryptosystems like RSA, ECC, and others. NTRU cryptosystem is very secure against quantum-based attacks because of hard problem in lattice reduction.

6. Proposed AKA protocol

Proposed-AKA protocol comprises the entities i.e. UE, SEAF, AUSF, and UDM/ARPF. The SEAF is positioned in the SN and the AUSF and ARPF are configured in the HN. Proposed-AKA protocol exchange messages as shown in Figure 7. UE transmit enrolment request to SEAF through gNB to start communication. SEAF stats an authentication procedure by asking for subscriber identity. In response to request, UE sends its subscriber identity in message-M1 to SEAF which is encoded with NTRU public key of UDM/ARPF. SEAF has its personal identity known as SNN (serving network identity). SEAF directs request containing subscriber identity to the AUSF and sends SNN in message-M2 which is encoded with NTRU public key of UDM/ARPF. AUSF forwarded the received message as AV_REQ message-M3 to UDM/ARPF.

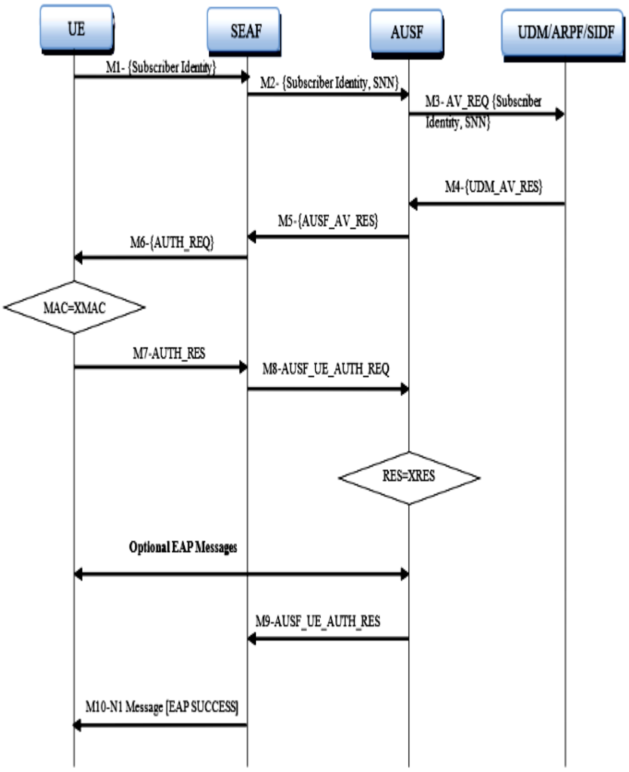
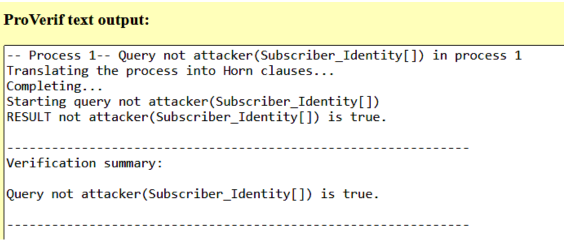


Fig 7: Proposed AKA Protocol.

First of all, UDM/ARPF decrypts authentication data requests using the NTRU private key of UDM/ARPF. UDM/ARPF uses a secret-key K common with UE. Message authentication functions and key generation functions are used to generate AV (authentication vector) in UDM/ARPF. To start with, it produces random nonce (RAND) and rise sequence number (SQN) for each vector. Using K, subscriber identity, RAND, and SQN it computes Message Verification Code, Anticipated Reaction, Code Key, Integrity Key, token, and Confirmation vector i.e. MAC, XRES, CK, IK, AUTH and AV. A validation information reaction message, designated as UDM_AV_RES in message-M4 (AVs), is sent by UDM/ARPF to AUSF. This message is encoded using AUSF's NTRU public key, granting AUSF permission to confirm the mentioning UE. AUSF saves the obtained cluster of validation vectors (AVs) and uses the NTRU public key of SEAF as AUSF_AV_RES in message-M5 to send RAND and AUTN from the selected AV to SEAF. With the help of its NTRU private key, SEAF decodes received messages. It then transmits RAND and AUTN to UE in message-M6, which is encoded with UE's NTRU public key. UE compares the MAC transmitted in AUTN with the messages it decodes using its own NTRU private key, XMAC. On the off chance that both are equivalent, UE works out and returns the RES to SEAF as AUTH_RES in message-M7. UE also calculates CK and IK same way as derived in UDM/ARPF. SEAF sends the received message to AUSF as AUTH_UE_AUTH_REQ in message-M8. After receiving RES from UE, AUSF verifies it with XRES which is available in the AV. If it is equal then the authentication process is successful and AUSF calculates the corresponding K_{AUSF} from CK and IK as the session key to protect wireless communication with the UE. It also calculates K_{SEAF} from K_{AUSF} and sends it to SEAF as AUSF_UE_AUTH_RES in message-M9. UE also calculates its K_{AUSF} and K_{SEAF}. In this way (i) UE and AUSF both agree on the common session key K_{AUSF} (ii) UE and SEAF both agree on the common session key K_{SEAF}. Optional EAP messages procedure is initiated after message-M8. SEAF sends N1 Message (EAP Success) to UE with K_{gNB} in message-M10. We have examined the security of our protocol using the ProVerif tool. ProVerif is a cryptographic verifier in Dolev-Yao model. 1) Astounding cryptography (no information without key) is what we hope to achieve in the model. 2) The communication medium is entirely under the attacker's control. 3) The attacker has access to every message and is able to forward, drop, or replay previous ones. ProVerif displays accuracy independent of run count. The ProVerif language is a modified of pi-calculus made. The ProVerif is used to examine secrecy and authentication properties. Thought is given to a limitless number of gatherings and an endless message space while assessing a protocol. If the protocol isn't protected, an attack could be carried out. The proposed-AKA makes use of encoded subscriber identity among network entities (UE, SEAF, AUSF, and UDM/ARPF) in order to provide subscriber security. In Figure 8, the ProVerif result is displayed.



ProVerif text output:

```
-- Process 1-- Query not attacker(Subscriber_Identity[]) in process 1
Translating the process into Horn clauses...
Completing...
Starting query not attacker(Subscriber_Identity[])
RESULT not attacker(Subscriber_Identity[]) is true.

--------------------------------------------------------------
Verification summary:

Query not attacker(Subscriber_Identity[]) is true.

--------------------------------------------------------------
```

Fig 8: ProVerif Result

It demonstrates that subscriber identity can be safely transferred across insecure channels between network entities. Even if the attacker controls the channel, it is expected to receive subscriber identity securely. Table 2 displays the evaluation between 2G-AKA, 3G-AKA, 4G-AKA, and the suggested 5G-AKA.

Table 2: Comparison of 2G-AKA, 3G-AKA, 4G-AKA and proposed 5G-AKA

AKA	Subscriber identity Secrecy
2G-AKA	NO
3G-AKA	NO
4G-AKA	NO
Proposed 5G-AKA	YES

The proposed-AKA provides secrecy of subscriber identity and mutual authentication. To receive these advantages, there is a price that must be paid. Cryptosystems are always associated with a high computational cost. Generally speaking, we anticipate an optimal cryptosystem that ignores computation during proposed plan. In order to set up the protocol, we really want to select a cryptosystem that makes sense for wireless communication networks and uses less processing power. The NTRU encryption system may be the fastest open key cryptosystem currently available, providing varying degrees of security quickly, even with severely constrained assets, such as PDAs and mobile phones. Contrasted with other cryptosystems, NTRU is more worthwhile regarding equipment and software execution. The NTRU cryptosystem is suitable to use in a proposed-AKA for wireless correspondence networks.

7. Conclusion

This paper examines security concerns in wireless communication networks, focusing on authentication and key access mechanisms in fifth-generation network. The 5G network's security is still being thoroughly investigated. We used perfect cryptosystem to safeguard the subscriber identity in the proposed-AKA protocol, and we used the ProVerif tool to verify it. The proposed-AKA protocol shows how subscriber identity secrecy is protected. The proposed-AKA protocol easily fits in current network. Tradeoff between security and computation overhead is invariably. In light of this, we can state that, though the proposed method has more delay than the current one, the proposed-AKA can provide better security than the current protocol.

ACKNOWLEDGEMENT

We would like to convey our sincere thanks to Dr. K R Parmar and Dr. A. Kulshreshta for their guidance and support.

Conflicts of interest

"The authors declare that there is no conflict of interest regarding the publication of this paper."

References

[1] 3GPP, "System Architecture for 5G System", 3GPP TS 23.501 version 19.0.0. Technical Report, The 3rd Generation Partnership Project.

[2] 3GPP, "Security Architecture and Procedures for the 5G System", 3GPP TS 33.501 version 15.2.0. Technical Report, The 3rd Generation Partnership Project.

[3] A. Ferrag, L. Maglaras, A Argyriou, D. Kosmano, H. Janicke. "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-

preserving schemes", J. Netw. Comput. Appl. 2018, 101, 55–82.

[4] Jover R P, Marojevic V, "Security and protocol exploit analysis of the 5G specifications", IEEE Access 2019, 7, 24956–24963.

[5] Ahmad I, Shahabuddin S, Kumar T, Okwuibe, J, Ylianttila M, "Security for 5G and beyond", IEEE Commun. Surv. Tutor. 2019, 21, 3682–3722.

[6] Khan R, Kumar P, Jayakody D, Liyanage M, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions", IEEE Commun. Surv. Tutor. 2019, 22, 196–248.

[7] Hussain S.R., Echeverria M., Chowdhury O., Li N., Bertino E., "Privacy attacks to the 4G and 5G cellular paging protocols using side-channel information", In Proceedings of the 26th Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24–27 February 2019; pp. 1–15.

[8] Khan H., Martin K.M., "A survey of subscription privacy on the 5G radio interface-the past, present and future", J. Inf. Secure. Appl. 2020, 53, 102537.

[9] C.B. Sankaran," Network Access Security in Next-generation 3GPP Systems: A Tutorial," IEEE Commun. Mag., Vol.47, No.2, February 2009, pp.84-91.

[10] N. Seddigh, B. Nandy, R. Makkar, and J.F. Beaumont," Security Advances and Challenges in 4G Wireless Networks," Proc. Eighth Annual International Conference on Privacy Security and Trust (PST), August 2010, pp.62-71.

[11] J. Zheng, "Research on the Security of 4G Mobile System in the IPv6 Network," Recent Advances in Computer Science and Information Engineering, Vol. 126, 2012, pp. 829-834.

[12] Li Zhu, Hang Qin, Huaqing Mao, Zhiwen Hu, "Research on 3GPP LTE Security Architecture", International Conference on WiCOM, IEEE Conference publications-2012

[13] Dehnel-Wild M., Cremers C., "Security Vulnerability in 5G-AKA Draft", Department of Computer Science, University of Oxford, Oxford, UK, 2018.

[14] Meier S., Schmidt B., Cremers C., Basin D., "The Tamarin prover for the symbolic analysis of security protocols", In Proceedings of the 25th International Conference on Computer Aided Verification, Saint Petersburg, Russia, 13–19 July 2013; pp. 696–701.

[15] Basin D., Dreier J., Hirschi L., Radomirovic S., Sasse R., Stettler V, "A formal analysis of 5G authentication". In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 1383–1396.

[16] Borgaonkar R., Hirschi L., Park S., Shaik A., "New privacy threat on 3G, 4G, and upcoming 5G AKA Protocols". Proc. Priv. Enhancing Technol. 2019, 3, 108–127.

[17] Cremers C., Dehnel-Wild M., "Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion", In Proceedings of the 26th Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24–27 February 2019; pp. 1–15.

[18] Koutsos A., "The 5G-AKA authentication protocol privacy", In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 464–479.

[19] Bana G., Comon-Lundh H., "Towards unconditional soundness: Computationally complete symbolic attacker", In Proceedings of the First International Conference on Principles of Security and Trust (ETAPS), Tallinn, Estonia, 24 March–1 April 2012; pp. 189–208.

[20] Bana G., Comon-Lundh H., "A computationally complete symbolic attacker for equivalence properties", In Proceedings of the 2014 ACMSIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 609–620

[21] C. Vintila, V. Patriciu, and I. Bica, "Security Analysis of LTE Access Network", Proceedings of the Tenth International Conference on Networks (ICN 2011), January 2011, pp. 29-34.

[22] D. Forsberg, L. Huang, K. Tsuyoshi, and S. Alanara, "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface," Proc. Personal,

[23] D. Yu and W. Wen, "Non-access-stratum Request Attack in E-UTRAN," Proc. Computing, Communications and Applications Conference (Com-ComAp), January 2012, pp.48-53.

[24] Y. Park, T. Park, "A Survey of Security Threats on 4G Networks," in GLOBECOM-07.

[25] Braeken A., Liyanage M., Kumar P., Murphy J., "Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks", IEEE Access 2019, 7, 64040–64052.

[26] Gharsallah I., Smaoui S., Zarai F., "A secure efficient and lightweight authentication protocol for 5G cellular networks: SEL-AKA". In Proceedings of the 2019

15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 1311–1316.

[27] Jeff Hoffstein Daniel Lieman Jill Pipher Joseph H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem" Available online on www.ntru.org.

[28] Hien Ba Nguyen, Thesis on "An Overview of the NTRU Cryptographic system", San Diego State University, 2014.

[29] Priit Karu, "Practical Comparison of Fast Public-key Cryptosystems" Proceedings of the Helsinki University of Technology Seminar on Network Security fall 2000.

[30] Hu X., Liu C., Liu S., Li J., Cheng X., "A vulnerability in 5G authentication protocols and its Countermeasure", IEICE Trans. Inf. Syst. 2020, 103, 1806–1809.

[31] Xiao Y., Wu Y., "5G-IPAKA: An Improved Primary Authentication and Key Agreement Protocol for 5G Networks", Information 2022, 13, 125.

[32] Blanchet, B.; Smyth, B.; Cheval, V.; Sylvestre, M. "ProVerif 2.05: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial". Proverif User Manual, 2023. https://bblanche.gitlabpages.inria.fr/proverif/