

SEAI: Secrecy and Efficiency Aware Inter-gNB Handover Authentication and Key Agreement Protocol in 5G Communication Network

Shubham Gupta (✉ shubham.gupta@students.vnit.ac.in)

Norwegian University of Science and Technology: Norges teknisk-naturvitenskapelige universitet
<https://orcid.org/0000-0002-9915-3183>

Balu L. Parne

Sardar Vallabhbhai National Institute of Technology

Narendra S. Chaudhari

IIT Indore: Indian Institute of Technology Indore

Sandeep Saxena

GCET: Galgotias College of Engineering and Technology

Research Article

Keywords: 5G communication, Key-secrecy, Security attacks, Computation overhead, Random oracle model.

Posted Date: March 16th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-262554/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Version of Record: A version of this preprint was published at Wireless Personal Communications on August 27th, 2021. See the published version at <https://doi.org/10.1007/s11277-021-09036-4>.

SEAI: Secrecy and Efficiency Aware Inter-gNB Handover Authentication and Key Agreement Protocol in 5G Communication Network

Shubham Gupta¹ · Balu L. Parne² ·
Narendra S. Chaudhari³ · Sandeep Saxena⁴

Received: date / Accepted: date

Abstract Recently, the Third Generation Partnership Project (3GPP) has initiated to work in the Fifth Generation (5G) network to fulfill the security characteristics of IoT-based services. 3GPP has proposed the 5G handover key structure and framework in a recently published technical report. In this paper, we evaluate the handover authentication methodologies available in the literature and identify the security vulnerabilities such as violation of global base-station, failure of key forward/backward secrecy, de-synchronization attack, and huge network congestion. Also, these protocols suffer from high bandwidth consumption that doesn't suit for energy efficient mobile devices in 5G network. To overcome these concerns, we introduce Secrecy and Efficiency Aware Inter-gNB (SEAI) handover Authentication and Key Agreement (AKA) protocol. The formal security proof of the protocol is carried out by random oracle model to achieve the session key secrecy, confidentiality, and integrity. For the protocol correctness and achieve the mutual authentication property, simulation is performed using the AVISPA tool. Also, the informal security evaluation represents that the protocol defeats all

✉ Shubham Gupta
guptashubham396@gmail.com
· Balu L. Parne
blparne@coed.svnit.ac.in
· Narendra S. Chaudhari
nsc0183@yahoo.com
· Sandeep Saxena
saxena.s.in@ieee.org

¹Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), Trondheim, 7491, Norway.

² Computer Engineering Department, Sardar Vallabhbhai National Institute of Technology (SVNIT), Surat, 395007, India.

³Department of Computer Science and Engineering, Indian Institute of Technology (IIT), Indore, Madhya Pradesh (M.P.), 453552, India.

⁴Department of Information Technology, Galgotias College of Engineering and Technology (GCET), Greater Noida, 201306, India.

the possible attacks and achieves the necessary security properties. Moreover, the performance evaluation of the earlier 5G handover protocols and proposed SEAI protocol is carried out. From the evaluations, the significant results are obtained based on computation, transmission, and communication overhead.

Keywords 5G communication · Key-secrecy · Security attacks · Computation overhead · Random oracle model.

1 Introduction

With the advancement of IoT-based services and applications, the academicians and researchers of 3GPP have recommended 5G communication technology of the cellular network from the recent past [1–3]. The 5G technology suggests advanced aspects related to LTE-A network as non-3GPP inter-working, the formative arrangement of User Plane (UP) operations which are described as logical networks (user and control plane operations) with different potentials [4]. Further, User Equipment (UE) may broadcast Non-Access Stratum (NAS) information to core network of 5G for session and mobility administration, that hasn't been attained in preceding cellular network technologies [5; 6]. Moreover, these attributes associate discrete aspects in the security structure of the 5G handover network. There are different handover services and applications as vehicular management system, e-health care, and multimedia services, etc. because of the portability of numerous IoT devices/ equipment in 5G network [7–10]. To gain the secrecy of these services, it is prescribed to execute a secure and cost efficient handover mechanism in 5G communication network.

Although, a key structure of 5G handover suffers from authentication complications and different security susceptibilities [11]. In handover key structure, an attacker can breach the secret session keys from genuine base-stations. Nonetheless, the segregation of secret keys among base-stations averts the raised issues at the time of handover. However, this approach overlooks the negotiated key in one particular gNB from the other one. The source Next Generation (5G) Base-Station Node (gNB_s) broadcasts session key to the target Next Generation (5G) Base-Station Node (gNB_t). The gNB_s obtains a fresh session key by adopting a one-way operation and attains key backward secrecy (KBS). The KBS restrains gNB's from generating the preceding keys from the established key. Contrarily, the gNB's might learn entire keys used in earlier sessions of handover. Correspondingly, the KFS (forward secrecy) is preserved to provide that the communicating participants install different specifications in obtaining the new key for subsequent gNB. Moreover, the current gNB doesn't form subsequent keys. The structure of 5G handover key declines to form KFS if an attacker negotiates an honest base-station. In this situation, gNB_t doesn't provide fresh session keys because of desynchronization. Hence, it exhibits the security deficiencies in the key structure of handover, and attacker can negotiate entire prior keys between gNB and UE. The potential attacks may be protracted before the aforesaid modifications of current key as the specifications of the key are obtained from preceding keys [12]. Furthermore, inter-gNB handover in 5G networks deteriorates from transmission overhead because of numerous rounds of information transfer among the communicating participants. Hence, it is recommended to introduce a cost efficient and attack resilient inter-gNB handover protocol in the 5G network.

1.1 Fundamental Security Properties of Handover Protocol

The security properties of the 5G handover are required to establish the mutual authentication and shared secret key compliance between the communicating participants to satisfy the integrity for subsequent handover. The proposed 5G inter-gNB handover protocol must conclude the following properties.

- The protocol should maintain the privacy of the communicating participants during the authentication process. Only the home network can obtain the permanent identity of mobile devices.
- The protocol should maintain forward/backward secrecy with key re-freshness in each new handover authentication connection even if an attacker knows the private keys.
- The protocol must establish robust secrecy during the authentication to curtail the possible attacks in the 5G network.
- It is known that the UE is a limited power resource equipment and the network channel has controlled frequency. Therefore, the protocol must be structured in a form that it mandates the reduced overhead.

To achieve the necessary security properties during the handover process, 3GPP has introduced the handover methodology [11]. However, the protocol incurs security vulnerabilities such as 1) several messages correspondence are needed to communicate with the AMF (serving network). Therefore, the 5G network diminishes transmission efficiency. 2) The 5G handover key derivation structure proposed by 3GPP brings out various gNB keys based on horizontal/vertical key approach. Hence, the researchers have proposed various handover protocols in 5G communication network [13–17]. Unfortunately, an authentication complexity, high communication, and computation overhead are noticed in these protocols. In addition, these protocols are susceptible to several security attacks. Hence, these handover protocols are not much suitable for efficient handover authentication in 5G communication network.

In the prospect of these issues, we introduce Secrecy and Efficiency Aware Inter-gNB (SEAI) handover AKA protocol in 5G network. The proposed protocol avoids the problem of key escrow without involving any third party in establishing the secret keys. Also, the UE/gNB presents a secret correspondence of their identity by collision avoidance hash function and chooses secret keys in the handover initialization stage. The protocol doesn't execute the time consuming exponentiation operations and shows less overhead. Moreover, the protocol doesn't send the secret keys over the public channel to preserve the handover key compliance.

1.2 Core Technical Improvements

To avert the above-raised issues, we propose the inter-gNB handover protocol in 5G network. The main improvements of this article compared to previous ones are:

1. Essentially, we investigate the current 5G handover key structure and describe its security deficiencies as bogus base-station attack and de-synchronization problem.

2. We introduce an inter-gNB handover protocol to dodge the security deficiencies from the current handover protocol of 5G network. In proposed protocol, gNB_t and UE realize mutual authentication at the time of handover formation without broadcasting the secret keys in the air. Moreover, the protocol mandates the KFS/KBS.
3. The confidentiality, integrity, and session key secrecy in the protocol are proven secure by using ROM. Also, the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool presents correctness and verification. Moreover, the attack and security analysis are inclined with respect to numerous security specifications. The analysis represents that the protocol averts the potential attacks.
4. The performance estimation of current and proposed handover protocols is concluded on the basis of communication, computation, and transmission overhead. The estimation results represent that the SEAI protocol is far efficient and secure than the current one.

The rest of the article is formed as follows: Section 2 illustrates the 5G handover framework, handover key hierarchy, and evaluates the key structure. The existing handover methodologies are illustrated in section 3. The security susceptibilities of the 5G handover protocol are discussed in section 4. Section 5 discusses the proposed SEAI handover protocol in 5G network. The formal security proof using ROM, correctness and informal analysis of the protocol are presented in section 6. Section 7 demonstrates the performance estimation of 5G handover AKA protocols. Lastly, section 8 concludes the article.

2 Framework, Hierarchy and Structure

The 5G network derives a fundamental security architecture of the LTE-A network. 3GPP has done some security design contributions in 5G network after the performance and practical operations. Although, a novel handover authentication framework is required in order to mandate these modifications for 5G network. In this section, we demonstrate the 5G handover framework, handover key structure, and key hierarchy.

2.1 5G Network Framework

The communication in 5G network framework is established by following participants as Access and Mobility Management Function (AMF)/Security Anchor Function (SEAF), Authentication Credential Repository and Processing Function (ARPF), Session Management Function (SMF), Policy Control Function (PCF), and Authentication Server Function (AUSF) as shown in Fig. 1 [18–20]. In this framework, UE establishes the connection with various gNBs and AMF maintains secure communication using Key_{AMF} . Further, UE verifies the AUSF while subscription information is kept by the ARPF. For the authentication with UE, the ARPF stores the secure symmetric key S_{key} . Also, ARPF computes the authentication vectors (AVs) by executing the cryptographic operations with the security parameters. The Security Policy Control Function (SPCF) consists of security to

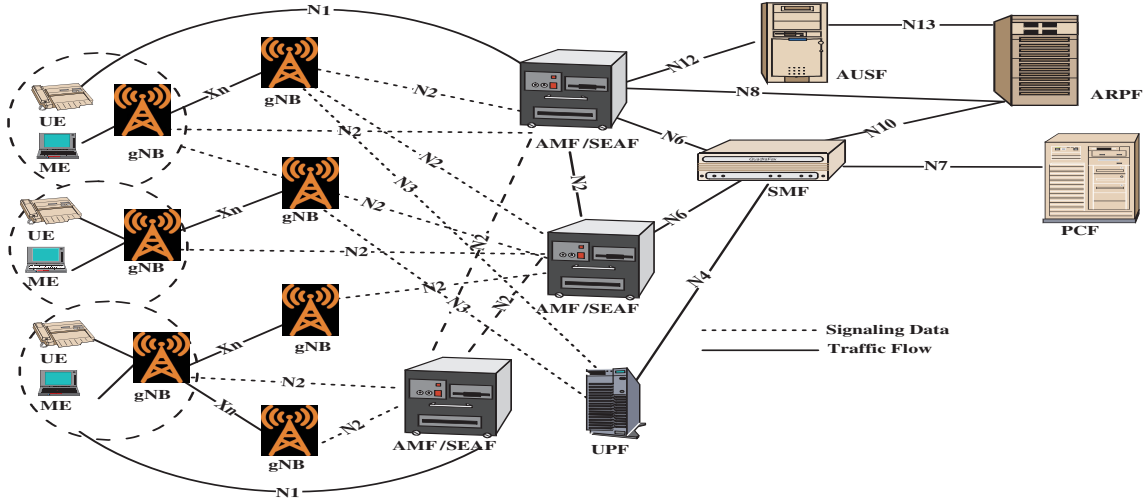


Fig. 1 A handover framework of 5G communication network

the SMF and AMF. The security credentials hold the key length, integrity and confidentiality algorithm, and AUSF information. The Non-access Stratum (NAS) and AS layers conserve their communication traffic to establish gNB security [21]. Whenever UE communicates in the 5G network, the AS layer establishes the secrecy between the UE, NAS layer, and gNB. In addition, the N3-UP (path of user plane signaling) and N2-CP (path of control plane signaling) are established between UE & User Plane Function (UPF) and UE & AMF respectively [22]. These new updates are the absolute paths for user/control planes and key algorithms (integrity and encryption).

2.2 5G Key Hierarchy

The 5G network key hierarchy is designed for the efficient structure of numerous keys among the participating entities in the communication [11]. The first transition key Key_{AUSF} is computed by the ARPF to maintain secret communication between UE and ARPF. From this key, another transition key Key_{SEAF} is computed between UE and AUSF to determine Key_{AMF} . In addition, the key Key_{gNB} is retrieved at AMF and sent to the gNB. The UE establishes the authentication compliance with AMF in support of AUSF/ARPF. The AMF and UE compute the Key_{AMF} using Key_{SEAF}/Key_{AUSF} after obtaining the mutual authentication. The Key_{AMF} is valid for the certain period computed for the successive AKA process and generates four sub-keys from it. The two sub-keys Key_{NASenc} and Key_{NASint} are computed for encryption verification and integrity respectively. UE and AMF derive the third sub-key Non-3GPP access Inter-working Function (Key_{N3IWF}) from Key_{AMF} for non-3GPP access. Moreover, UE and gNB generate the fourth sub-key Key_{gNB} that computes another four keys. Firstly, two keys Key_{RRCenc} and Key_{RRCint} are required to authenticate the Radio Resource

Control (RRC) signaling encryption and its integrity respectively. In addition, the keys $Key_{UP_{enc}}$ and $Key_{UP_{int}}$ are required to verify the UP data traffic encryption and integrity respectively. Also, Key_{gNB} is renewed during handover whenever the UE enters into the coverage area of another gNB.

2.3 Handover Structure of 5G

In this section, we will demonstrate the Xn-based (inter-gNB) 5G handover structure. In the inter-gNB handover, AMF and UE attain the authentication and key compliance process to achieve the security properties. For secure communication during handover, gNB_s generates the $Key_{NG-RAN'}$ (preceding Key_{gNB}) for gNB_t . Also, Key_{gNB} is concatenated at handover key chaining before the subsequent AKA process [11]. By using the one-way hash, gNB_s generates the next Key_{gNB} from the present gNB and applies the current key from AMF. Then, AMF transmits these information to gNB_t after accomplishing the inter-gNB handover and apply it for subsequent handover. NH Chaining Counter (NCC) and Next Hop (NH) are the key parameters in handover key chaining. AMF setups the next NH parameters generated from Key_{AMF} for respective handover repeatedly. The communication mechanism of 5G inter-gNB handover is shown in Figure 2 [11]. It is analyzed that the gNB_s obtains the specific key parameters $\{NH_{NCC}, NCC\}$ from the preceding handover. The counter of NH key update is NH_{NCC} . The gNB_s computes $Key_{NG-RAN'}$ from NH key and Key_{gNB} by performing horizontal and vertical key operations respectively for gNB_t . The horizontal and vertical key operations are $Key_{NG-RAN'} = KDF(\eta || NH_{NCC})$ and $Key_{NG-RAN'} = KDF(\eta || Key_{gNB})$ respectively, where $\eta = ARFC-DL || PCIA$, $NH_{NCC'} = KDF(Key_{gNB} || Key_{AMF})$ (original value of NH), $NH_{NCC} = KDF(NH_{NCC-1} || Key_{AMF})$, NH_{NCC-1} (preceding value of NH), absolute radio frequency channel-down link (ARFC-DL), and physical cell identity allocation (PCIA). In the horizontal handover, gNB_s doesn't achieve the specific NH key, and $\{NH_{NCC}, NCC\}$ are appeared before the completion of inter-gNB 5G handover. On the other hand in vertical handover, gNB_s has specific NH key derived in 5G inter-gNB handover, and AMF and UE could fetch the NH only.

The gNB_s transmits $\{NCC, Key_{NG-RAN'}\}$ to gNB_t in inter-gNB handover. It is analyzed that the gNB_s executes the vertical operation and future keys between gNB_t and UE. In this handover, the AMF and gNB_t transmit their handover request/response to UE. Later, UE verifies the acknowledged NCC from the equipped NCC. If it authenticates, UE performs vertical operation from the current Key_{gNB} to generate $Key_{NG-RAN'}$. Or, UE tries to integrate the NCC by generating NH key regularly, until it authenticates and executes the horizontal key operation to derive $Key_{NG-RAN'}$. Moreover, the gNB_t transmits the path change inquiry to AMF in inter-gNB 5G handover after the handover accomplishment with UE. Then, AMF increases NCC value by one and derives the specific NH key. Also, AMF transmits the $\{NH_{NCC+1}, NCC + 1\}$ to gNB_t for further handover.

3 Existing Methodologies

In order to obtain mutual authentication and overcome the bandwidth consumption from 5G network, researchers and academicians have introduced numerous handover methodologies. In this section, we illustrate these protocols based on their security features and issues.

Cao et al. [13] discussed the privacy-preserving handover authentication protocol for 5G HetNets using the Software Defined Network (SDN). The protocol obtains the mutual authentication and key agreement between base-stations and mobile devices without any other entities. Also, the protocol overcomes the system authentication complexity and minimizes bandwidth consumption. However, similar to 3GPP-5G handover AKA protocol, the protocol fails to avoid the desynchronization of communicating entities that lead to DoS attack because of sequence number (SQN) mismatch. In the protocol, it is considered that the SQN is maintained between base-station and UE. In one registration, the value of SQN is used for entire the n connections and increases the value by one at UE/ base-station. An adversary may attempt a bogus registration attempt by using previous messages and SQN value got inconsistent. If the genuine UE attempts to create the connection with the target base-station, the session keys and message authentication code are not matched. Therefore, the genuine UE will be unauthorized to access the network during handover.

To avoid the above issues, Sharma et al. [14] proposed the handover authentication protocol that maintains the privacy-preservation and key secrecy. Also, the protocol avoids all the security susceptibilities and withstands the security attacks. However, numerous message correspondence with the base-station and terminal (UE) carries handover disruption and increases the overhead because the serving network is very far from base-station. Hence, the protocol incurs authentication complexity. Also, the source base-station computes numerous keys for target base-stations that enhances the probability of dodging the secret keys.

Zhang. et al. [15] introduced the Elliptic Curve Cryptography (ECC)-based handover authentication protocol by using chameleon hash function key pairs to avoid the authentication complexity. However, the protocol obtains all the security characteristics but suffer from identity privacy preservation and MitM attack. Also, the protocol exhibits a huge network and transmission overhead due to additional use of point multiplication key operations. Han et al. [16] designed the efficient handover AKA to enhance security properties and maintain the mutual authentication. Also, the protocol incurs less overhead and establishes the key secrecy. However, the protocol suffers from DoS attack similar to Cao's protocol. Due to the use of Extensible Authentication Protocol (EAP)-AKA [23], the proposed protocol suffers from the identity privacy preservation and security vulnerabilities such as redirection and MitM attack.

Recently, Kumar et al. [17] designed the ECC-based handover authentication protocol for 5G-wireless LAN networks. The protocol exhibits the mutual authentication and most of the security properties such as key forward/ backward secrecy, anonymity. However, the protocol fails to preserve the identity of the communicating participants and suffers from redirection, MitM attack. In addition, the protocol incurs huge communication and computational overhead due to additional use of point multiplication functions during the handover authentication process.

From the existing handover methodologies, it is noticed that these protocols are susceptible to various known attacks and exhibit huge network overhead. Also, the protocols fail to provide the key secrecy and suffer authentication complexity. Therefore, the above-discussed protocols are not well suited for efficient handover development in 5G communication network. In order to avoid these problems, we introduce the SEAI handover AKA protocol in the 5G network to obtain necessary security requirements. The SEAI protocol is free from the problem of key escrow as there is no entanglement of any third party in establishing the secret keys. Also, the communicating participants send their identity securely in handover process and don't transmit the secret keys in the public channel during handover agreement. The protocol operates the key operations using the point multiplication functions and enhances its efficiency compared to the existing protocols. Moreover, the protocol averts from the potential attacks and provides all the security properties.

4 Security Susceptibilities

This section illustrates the security susceptibilities in 5G handover mechanisms proposed by the 3GPP and other various researchers. These security problems represent various adversities in the steady communication of the 5G handover network. Let consider, an attacker \mathcal{ATT} impersonates the genuine base-station (gNB) and implants the forged base-station $gNB_{\mathcal{ATT}}$ in the communication network. \mathcal{ATT} may approach its stored parameters by massive intrusion as gNB is implanted very far to the AMF.

4.1 De-synchronization Attack

\mathcal{ATT} can install the $gNB_{\mathcal{ATT}}$ that performs the Denial-of-Service(Dos) and leads to de-synchronization during the 5G handover. The prime target of $gNB_{\mathcal{ATT}}$ is to build the bogus information of NCC and dodge the imminent keys. The \mathcal{ATT} can impose to gNB_t to disturb the key forward secrecy by performing horizontal key operations. The value of NCC can be compromised by manipulating the information between gNB_s and gNB_t in 5G handover mechanism. The $gNB_{\mathcal{ATT}}$ chooses a large prime number to impersonate the NCC and transmits to gNB_t during second handover response as shown in Figure 2.

\mathcal{ATT} sends the original and false NCC to UE for maintaining the synchronization. The NCC value in path shifting information is trivial than that obtained by $gNB_{\mathcal{ATT}}$. In addition, the gNB_t and UE generate future handover keys on the basis of present Key_{gNB} in place of NH_{NCC+1} . Therefore, $gNB_{\mathcal{ATT}}$ may not obtain the following Key_{gNB} because of forward secrecy failure. The gNB acquires the following key of Key_{NG-RAN}' from Key_{gNB} because \mathcal{ATT} can have the knowledge of ARFC-DL and PCIA. Moreover, \mathcal{ATT} impersonates the UE by sending the original value of NCC and executes de-synchronization. \mathcal{ATT} can decimate the NCC by disguising the information AMF to gNB_t . The gNB_t fails to conform to the fresh value of NCC because bogus information has a lesser value of NCC compared to the initial one. To overcome above security concerns,

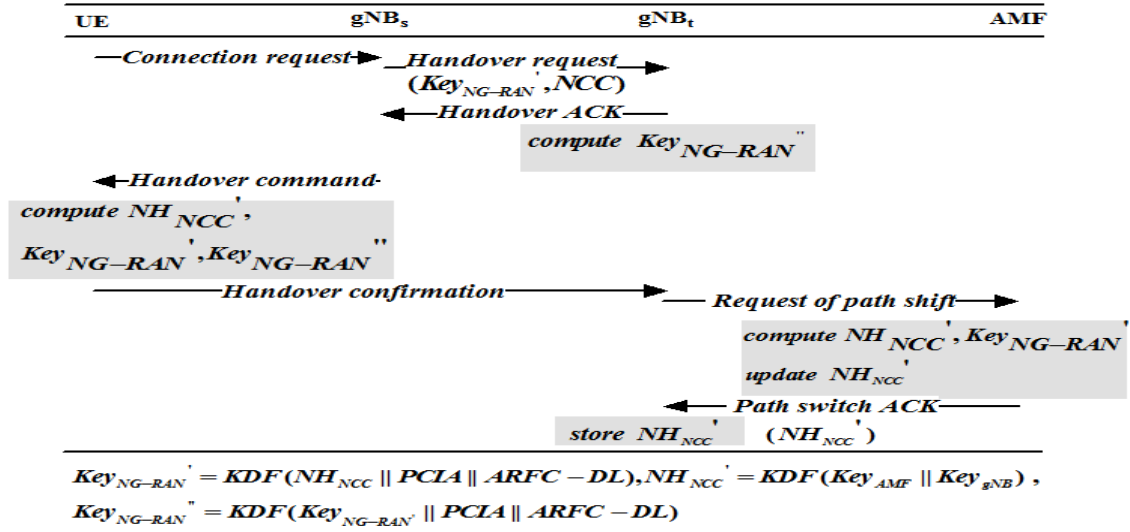


Fig. 2 Inter-gNB 5G Handover Mechanism

the Internet Protocol Security scheme is applied in path shifting and its confirmation message. Although, numerous links of IPSec with $gNBs$ are prescribed to establish in these transmitted messages with AMF. ATT may deploy the de-synchronization by information flooding/drop to block the gNB_t from recovering the NCC . Accordingly, the gNB_t may not modify the NCC and synchronization of the keys is not established. ATT may know the secret handover information from the communicating parties from gNB_{ATT} and degrades the network efficiency.

4.2 Verification Failure

The 5G inter-gNB handover mechanism needs various request/response message communication rounds with the AMF and gNB_s/gNB_t that suffers from handover explosion. Also, it increases the overhead because the AMF is installed far from gNB . Hence, the 5G handover network endures the authentication complexity/verification failure. The gNB_s generates legitimate keys for numerous gNB_t from the current one by using required specifications in 5G handover mechanism. For explanation, gNB_s may obtain the $Key_{NG-RAN}^{''}$ between the UE and gNB_t from $Key_{NG-RAN}^{'}$. Once the gNB_s is attacked, the ATT knows all the subsequent keys. Therefore, the key backward secrecy is not obtained in current 5G handover communication.

5 Proposed SEAI Handover Protocol

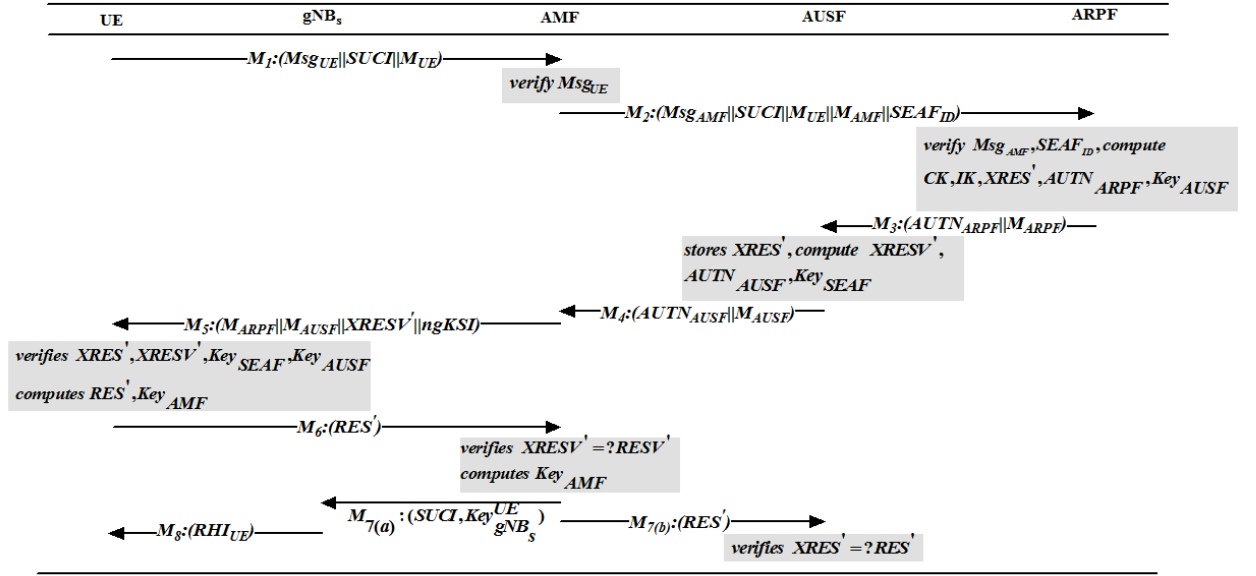
In this section, we discuss the novel SEAI handover AKA protocol to avoid the security deficiencies from the previously proposed handover protocols. The proposed protocol has three stages: a) establishment stage; b) handover initialization stage, and c) handover authentication stage. The security premises and methodology of Elliptic Curve Cryptography (ECC) are illustrated in the establishment stage. UE is authenticated at AMF and gNB_s formulates the handover request/ response information to UE for preceding communication in the initial authentication stage. Moreover, the gNB_t and UE executes the handover authentication stage when UE arrives in the area of gNB_t . The used notations and their meaning in the proposed protocol are reported in Table 1.

Table 1 Used notations and their meaning in the proposed SEAI protocol

Notation	Meaning
$m_{AMF}/m_{UE,n_{UE}/n_{gNB_t}/m_{ARPF}/x_{AUSF}$	Secret key of AMF/UE/ gNB_t /ARPF/ AUSF
$M_{AMF}/M_{UE,n_{UE}/n_{gNB_t}/M_{ARPF}/X_{AUSF}$	Public key of AMF/UE/ gNB_t /ARPF/ AUSF
$XRESV'/RESV'$	Expected response/actual expected response at AMF/ UE
$XRES'/RES'$	Expected response/actual response at AUSF/UE
$Key_{AMF}, Key_{SEAF}, Key_{AUSF}$	Generated key at AMF/UE, AUSF, and ARPF respectively
$IKey/CKey$	Integrity/ cipher key
$ID_{gNB_t}/ID_{gNB_s}/SEAF_{ID}$	Identity of gNB_t / gNB_s /SEAF
$ngKSI$	Key set identifier function of 5G communication network
$AUTN$	Authentication token value
RHI_{UE}	Received handover information by UE from gNB_s
T_{exp}	Time of expiration of RHI_{UE}
$Key_{gNB_s}^{UE}/Key_{gNB_t}^{UE}$	Computed session key between gNB_s / gNB_t and UE
$MAC_{gNB_t}/MAC_{UE}, MAC_{cfm}$	Message authentication information of gNB_t / UE, confirmation of handover
$inau_i$	Information of authentication of entity i

5.1 Establishment Stage

In order to achieve the authentication between gNB_t and UE in the proposed 5G handover protocol, we are applying ECC [24]. Consider, a prime number w and an elliptic curve $E(F_w)$ over F_w with w elements. Here, two elements a, b are designated in E over F_w of an equation $b^2 + x_1ab + x_3b = a^3 + x_2a^2 + x_4a + x_5$, where $x_1, x_2, x_3, x_4, x_5 \in F_w$. Suppose, q is a prime order in $E(F_w)$ with point P , where $q \nmid \#E(F_w)$. Moreover, finite field of integers modulo prime q is the Z_q and Z_q^* is multiplicative sub-group of Z_q . Also, the cyclic group C has the generator P . In the protocol, one way collision resistant hash functions are used as $H_j : \{0, 1\}^* \times C \rightarrow Z_q^*$, where $j = 1, 2, 3, 4, 5$. ARPF distributes system specifications $\{KDF, P, C, w, q, H_1, H_2, H_3, H_4, H_5\}$ and establishes the private key during handover authentication. As the protocol believes in the elliptic curve discrete logarithmic problem (ECDLP) assumption [25; 26]. It is admitted that the ECDLP



$$\begin{aligned}
Msg_{UE} &= H_1(SUCI \parallel M_{AMF} \cdot m_{UE}), Msg_{AMF} = H_1(SUCI \parallel m_{AMF} \cdot M_{ARPF} \parallel SEAF_{ID}), CK_{Key} = H_2(SUCI \parallel M_{UE} \cdot m_{ARPF}), \\
XRES' &= H_4(SUCI \parallel M_{UE} \cdot m_{ARPF} \parallel M_{AUSF}), RES' = H_4(SUCI \parallel m_{UE} \cdot M_{ARPF} \parallel M_{AUSF}), Key_{AUSF} = KDF(SUCI \parallel CK_{Key} \parallel IK_{Key} \parallel M_{ARPF}), \\
AUTN_{ARPF} &= (XRES' \parallel Key_{AUSF} \parallel M_{AMF}), Key_{SEAF} = (SUCI \parallel Key_{AUSF} \parallel M_{AUSF}), XRESV' = H_5(RESV' \parallel M_{AMF} \cdot m_{AUSF} \parallel M_{ARPF}), \\
RESV' &= H_5(RES' \parallel m_{AMF} \cdot M_{AUSF} \parallel M_{ARPF}), AUTN_{AUSF} = (XRESV' \parallel Key_{SEAF} \parallel M_{ARPF}), Key_{AMF} = (SUCI \parallel Key_{SEAF} \parallel M_{UE}), \\
Key_{gNBs}^{UE} &= KDF(ID_{gNBs} \parallel Key_{AMF} \parallel rspec), RHI_{UE} = E\{SUCI \parallel ID_{gNBs} \parallel Key_{gNBs}^{UE} \parallel T_{exp}\}, IK_{Key} = H_3(SUCI \parallel M_{UE} \cdot m_{ARPF})
\end{aligned}$$

Fig. 3 Handover Initialization Stage

computation is not feasible in polynomial-time and the key of ECC (size: 256 bits) obtains the same secrecy as RSA (size: 3072 bits).

- *Assertion-(a)*: Let, C be a group of q prime order and point P . $xP \in C$ is an element, where $x \in \mathbb{Z}_q^*$. It is computationally difficult to derive x from xP and P .
- *Assertion-(b)*: Let, C be a group of q prime order and point P . $P, xP, yP \in C$ are the elements where $x, y \in \mathbb{Z}_q^*$. It is computationally difficult to derive the xyP by using any polynomial time algorithm.

5.2 Handover Initialization Stage

In this stage, UE is verified at AUSF and AMF followed by ARPF [4]. During the verification process, some handover specifications are confined in message authentication request/response of original 5G-AKA protocol. These specifications in 5G-AKA don't mitigate the efficiency of network. In the SEAI protocol, the AMF sends the secret keys to gNB_s and gNB_s broadcasts the information to UE for subsequent handover after accomplishing the verification of UE. The descrip-

tive presentation of the handover initialization is exhibited in Fig. 3 and step-wise discussion is as follows:

- **Step-1:** $m_{UE} \in Z_q^*$ is private key chosen by the UE and computes $M_{UE} = m_{UE}.P$. Then, UE sends the message $SUCI, M_{UE}, Msg_{UE}, M_{AMF}$ to AMF and initiate the authentication mechanism with ARPF. The Subscription Permanent Identifier (SUPI) is never broadcasted in the communication channel of 5G handover. Therefore, the Subscription Concealed identifier (SUCI) function is created to obtain it. ARPF uses the Subscriber Identity De-concealing Function (SIDF) only and decrypts the SUCI to achieve the original SUPI.
- **Step-2:** AMF authenticates the message from UE and verifies Msg_{UE} . After this, it chooses $m_{AMF} \in Z_q^*$ (private key) and derives public key $M_{AMF} = m_{AMF}.P$. Finally, AMF sends the $SUCI, M_{ARPF}, M_{AMF}, M_{UE}, Msg_{AMF}, SEAF_{ID}$ to ARPF.
- **Step-3:** The Msg_{AMF} is verified at ARPF and authentication of UE is accomplished. Then, ARPF authenticates $SEAF_{ID}$ and checks the $SEAF_{ID}$ of UE. The $SEAF_{ID}$ is verified if they are same; Or, ARPF rejects an authentication request. Moreover, the ARPF choses $m_{ARPF} \in Z_q^*$ and derives $M_{ARPF} = m_{ARPF}.P$. It generates the $IKey, CKey, Key_{AUSF}, AUTN_{ARPF}, XRES'$ and transmits the $M_{ARPF}, AUTN_{ARPF}$ to the AUSF.
- **Step-4:** AUSF keeps $XRES'$ and generates the $Key_{SEAF}, AUTN_{AUSF}, XRESV'$. Then, it transmits the $M_{AUSF}, AUTN_{AUSF}$ to AMF.
- **Step-5:** AMF sends the $M_{ARPF}, M_{AUSF}, ngKSI, XRESV'$ to UE. Then, UE generates the $XRES', XRESV', Key_{AMF}, Key_{AUSF}, Key_{SEAF}$. It analyzes these derived values with the obtained ones. UE verifies the AUSF and ARPF, if they match. Moreover, UE computes RES' and sends to AMF.
- **Step-6:** AMF obtains $RESV'$ and checks with $XRESV'$. If it verifies, AMF confirms the UE's verification and generates Key_{AMF} . Further, AMF transmits RES' to AUSF and $Key_{gNB_s}^{UE}, SUCI$ to gNB_s .
- **Step-7:** The AUSF achieves the RES' and checks with $XRES'$. If the relation is legitimate, authentication of the UE is accomplished at AUSF. Moreover, gNB_s retrieves the RHI_{UE} from $Key_{gNB_s}^{UE}$ and sends to UE for subsequent handover. Here, $rspec$ is the related specifications of gNB_s as $ID_{gNB_s}, ECI, frequency, PCI$. Then, UE retrieves $Key_{gNB_s}^{UE}$ and securely stores RHI_{UE} .

5.3 Authentication Stage of Handover

When UE moves into the range of gNB_t , the gNB_t and UE initiate the mutual authentication and key compliance mechanism. Here, UE uses the RHI_{UE} which is retrieved in the handover initialization stage. The inter-gNB handover follows the traditional handover authentication mechanism. Fig. 4 represents the authentication steps in SEAI handover mechanism. The illustration of the steps is shown below:

- **Step-1:** When UE is in the area of gNB_t , it takes public parameters of associated gNBs and another specifications such as cell ID (ECI), PLMN-ID,

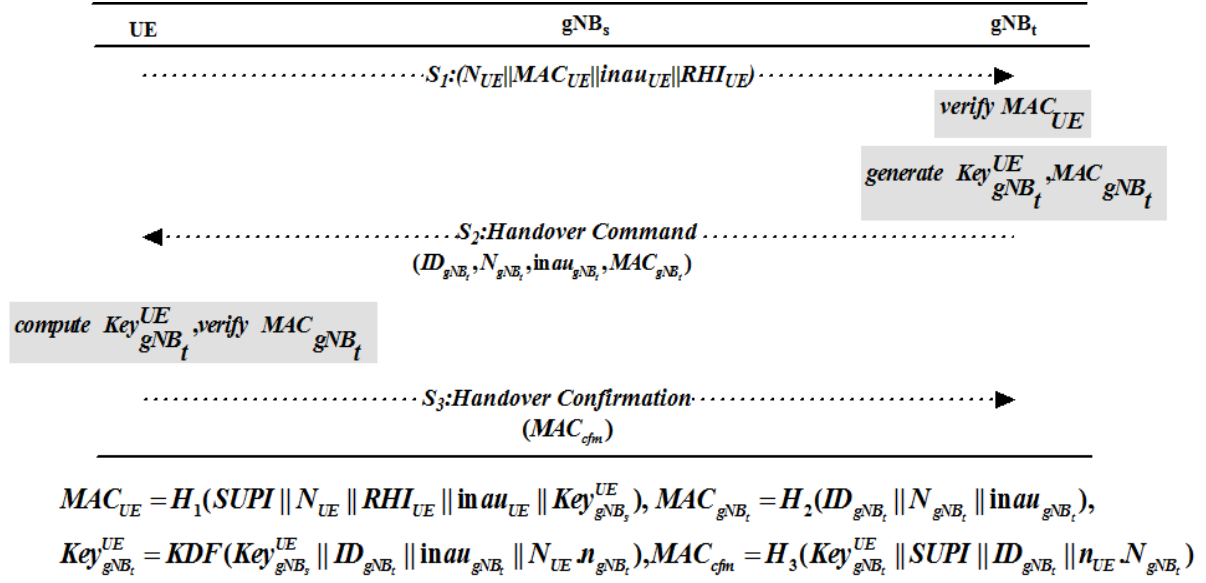


Fig. 4 Handover Authentication Stage

location area identity (LAI), PCI of gNB_t . After this, UE chooses a random nonce $n_{UE} \in Z_q^*$ and generates $N_{UE} = n_{UE} \cdot P$. Then, UE retrieves MAC_{UE} and sends the $N_{UE} || RHI_{UE} || MAC_{UE} || inau_{UE}$ to gNB_t ; where, the $inau_{UE}$ has the related specifications as $ECI, PLMN_{ID}, PCI$ of gNB_t and targeted LAI.

- **Step-2:** Now, gNB_t retrieves the $Key_{gNB_s}^{UE}$ by using RHI_{UE} . It also confirms the potency of RHI_{UE} from T_{exp} . If it is not verified, gNB_t rejects the handover inquiry. After this, gNB_t computes and checks the MAC_{UE} by using $Key_{gNB_s}^{UE}$. If it verifies, gNB_t accepts the acknowledged MAC_{UE} that is transferred from genuine UE. Or, authentication will be rejected.
- **Step-3:** After this, gNB_t chooses a random nonce $n_{gNB_t} \in Z_q^*$ and retrieves $n_{gNB_t} \cdot P = N_{gNB_t}$. Moreover, it generates the MAC_{gNB_t} for UE and session key $Key_{gNB_t}^{UE}$. Also, it sends the handover message $MAC_{gNB_t} || N_{gNB_t} || ID_{gNB_t} || inau_{gNB_t}$ to the UE. The $inau_{gNB_t}$ has the specifications as $ID_{AMF}, ECI, PLMN_{ID}$, and PCI .
- **Step-4:** Now, UE calculates the $Key_{gNB_t}^{UE}$ and checks the MAC_{gNB_t} . If it is incorrect, UE transmits the authentication failure response to gNB_t . On the other hand, UE accepts the gNB_t and transmits successful handover acknowledgement (MAC_{cfm}) to gNB_t with the $Key_{gNB_t}^{UE}$. After this, gNB_t approves the handover realization with the UE.

6 Security Analysis

This section discusses that the proposed protocol meets the security requirements in the ROM. The used assumptions and security model are shown in this proof. The

correctness of the protocol is obtained from the AVISPA tool. Also, the informal analysis of protocol is discussed with respect to various security attacks.

6.1 Security model

For the resistance of identified attacks in the SEAI protocol, we are using a provable security mechanism. We are showing the security proof based on the modeling introduced by [27].

6.1.1 Participants

The protocol Π executes with numerous number of associated participants in 5G network where the participant could be a client $W \in \omega$ or server $N \in \eta$. The set η is considered that only a single server is involved at one time. Every participants could have numerous instances (oracles) in distinct executions of Π . We indicate the i_{th} instance of W and N in sessions as Π_W^i and Π_N^i respectively. Each instance Π_W^i/Π_N^j has its session identity sid_W^i/sid_N^j (set of identities that shows the message flow sending/ receiving in this instance), partner identity pid_W^i/pid_N^j (set of identities which are executed in this instance), and session key as sk_W^i/sk_N^j . The instances Π_W^i, Π_N^j can be accepted if it maintains the $sid_W^i/sid_N^j, sk_W^i/sk_N^j$, and pid_W^i/pid_N^j . $\Pi_{W_1}^i/\Pi_{W_2}^j$ are acknowledged as a partner if (i) both are successfully accepted; (ii) $sid_{W_1}^i=sid_{W_2}^j$; (iii) $sk_{W_1}^i=sk_{W_2}^j$; (iv) $pid_{W_1}^i=pid_{W_2}^j$.

6.1.2 Attacker model

It is considered that the attacker \mathcal{ATT} completely controls the network, which initiates the communication sessions among the participants [28]. The \mathcal{ATT} can execute following queries as:

Execute($\Pi_{W_1}^i, \Pi_{W_2}^j, \Pi_N^k$): The query forms passive attacks where an adversary dodges the legitimate operations among the instances of client $\Pi_{W_1}^i, \Pi_{W_2}^j, \Pi_N^k$. The result of the query is the exchange of messages at the time of the genuine operation of Π .

Send_Client(Π_W^i, m): The attacker may use this query to trace the message and update it or forward to the client Π_W^i . The result of the query is the information that the client Π_W^i might compute upon acceptance of message m . Moreover, an attacker is granted to start the protocol by appealing to **Send_Client**($\Pi_{W_1}^i, (W_1, Start)$).

Send_Server(Π_N^i, m): The query builds active attacks counter to server. The result of the query is the information that the server Π_N^i might compute upon acceptance of message m .

Reveal(Π_W^i): The query builds identified session key attack. An attacker executes the query to achieve the secret keys of instance Π_W^i .

Corrupt(W): The query sends the long-term secret/ private keys to an attacker for participant W .

Test(Π_W^i): An attacker can build this type of query only one time to a fresh instance. On the response of the query, random number $e \in 0, 1$ is chosen. If $e = 1$,

session key obtained by Π_W^i is send. Or, return the consistently chosen random number.

6.1.3 Fresh instances

An instance Π_W^i is fresh if following condition satisfies: (i) Π_W^i is accepted; (ii) Π_W^i or its corresponding partner hasn't run the **Reveal** query after acceptance; (iii) client's corresponding partner with Π_W^i , hasn't run the **Corrupt** query.

6.1.4 Protocol security

The security of proposed protocol Π is formed by game $Game^{protocol}(\Pi, \mathcal{ATT})$. As running this game, \mathcal{ATT} can execute several queries to Π_W^i and Π_N^j . If \mathcal{ATT} asks a **Test**(Π_W^i) query, and Π_W^i is fresh and accepted, \mathcal{ATT} generates the e' . The objective of \mathcal{ATT} is know e correctly in test query. The advantage of \mathcal{ATT} can be written as:

$$Adv_{\Pi}^{protocol}(\mathcal{ATT}) = |2Pr[e = e'] - 1| \quad (1)$$

The protocol Π is secure if $Adv_{\Pi}^{protocol}(\mathcal{ATT})$ is negligibly higher than $O(q_{se})$, where q_{se} is the number of **Send** queries.

6.1.5 Assumption

The CDH assumption can be stated by two experiments, $Exp1_q^{CDH-real}(\Phi)$ and $Exp2_q^{CDH-rand}(\Phi)$. Adversary Φ is obtained with xP, yP, xyP in the $Exp1_q^{CDH-real}(\Phi)$; and xP, yP, zP in the $Exp2_q^{CDH-rand}(\Phi)$, where $x, y, z \in Z_q^*$. The advantage of Φ in breaching the CDH assumption, $Adv_q^{CDH}(\Phi) = \max\{|Pr(Exp1_q^{CDH-real}(\Phi) = 1) - Pr(Exp2_q^{CDH-rand}(\Phi) = 1)|\}$

6.2 Security Proof

Theorem: Let proposed protocol Π runs the q_{se} number of **Send** queries, q_{ex} number of **Execute** queries, and q_{hash} number of hash queries. Then CDH assumption holds the following

$$Adv_{\Pi}^{protocol}(\mathcal{ATT}) \leq \frac{(q_{se} + q_{ex}^2)}{q} + \frac{q_{hash}}{2^l} + 2q_{ex}Adv_q^{CDH}(\Phi) + 4\max\{\frac{q_{se} + q_{ex}}{2^l}, \frac{q_{hash}}{l}\}.$$

Proof: The proof has a combination of games, initiating from real attack G_1 and finishing at game G_5 where an attacker has no power. In each game, we set $Succ_i$ as event that \mathcal{ATT} knows e correctly in test query.

Game G_1 : This is the real attack by \mathcal{ATT} in protocol. In this game, the entire instances of participants are formed as real run/ execution in ROM. As per the definition of $Succ_i$, we have

$$Adv_{\Pi}^{protocol}(\mathcal{ATT}) = |2Pr[Succ_1] - \frac{1}{2}| \quad (2)$$

Game G_2 : This is very similar game to *Game G_1* except the simulation of hash oracles h by constructing hash records h_{rec} with input/ output entries. By executing *hinp* query, the output result is generated from the h_{rec} , otherwise randomly select the *Output* $\in \{0, 1\}^l$ and transmit to the \mathcal{ATT} with storing new entry of input/ output in h_{rec} . Moreover, we simulate the oracles of the entire queries. As per the knowledge of \mathcal{ATT} , the game G_2 is indistinguishable from real attack (game G_1). Therefore,

$$Pr[Succ_2] = Pr[Succ_1] \quad (3)$$

Game G_3 : Here, we simulate the entire instances of game G_2 , except we omit the game by which collisions may appear on transcripts as (Msg_{UE}, Msg_{AMF}) , (MAC_{UE}, MAC_{gNB_t}) , and hash values in the protocol. As per the definition of birthday paradox, in the result of h instances, the probability of collisions is $\frac{q_{hash}}{2^{l+1}}$.

Also, collisions probability in the transcripts is no more than $\frac{(q_{se} + q_{ex}^2)}{2q}$. Therefore,

$$|Pr[Succ_3] - Pr[Succ_2]| \leq \frac{(q_{se} + q_{ex}^2)}{2q} + \frac{q_{hash}}{2^{l+1}} \quad (4)$$

Game G_4 : Here, we change queries to the *Send_Client* instances. Also, select a random session initiated by legitimate clients UE and gNB_t for partner oracles Π_{UE}^i and $\Pi_{gNB_t}^j$.

- **Send_Client**($\Pi_{UE}^i, (gNB_t, Start)$) is requested and send output $SUCI, MAC_{UE}, RHI_{UE}$ to the \mathcal{ATT} .
- **Send_Client**($\Pi_{UE}^i, (AUTN_{AUSF}, XRESV')$) is requested, randomly select $x \in Z_q^*$ and generates $N_{UE} = x.P$. Then, UE computes $MAC_{UE} = H_1(SUPI||x||RHI_{UE}||inau_{UE}||K_{gNB_s}^{UE})$ and $RHI_{UE} = E\{SUCI||ID_{gNB_s}||K_{gNB_s}^{UE}||T_{exp}\}$ as real protocol. Then, send the output as $N_{UE}||RHI_{UE}||MAC_{UE}||SUCI||inau_{UE}$ to \mathcal{ATT} .
- **Send_Client**($\Pi_{gNB_t}^j, (N_{UE}||RHI_{UE}||MAC_{UE}||SUCI||inau_{UE})$) is requested and randomly select $y \in Z_q^*$ and generates $y.P = N_{gNB_t}$. Also, computes $MAC_{gNB_t} = H_2(ID_{gNB_t}||y||inau_{gNB_t})$ and $Key_{gNB_t}^{UE} = Key_{gNB_t} = KDF(Key_{gNB_s}^{UE}||ID_{gNB_t}||inau_{gNB_t}||N_{UE}.y) = xy.P$. Then, it sends the output $MAC_{gNB_t}||N_{gNB_t}||ID_{gNB_t}||inau_{gNB_t}$ to \mathcal{ATT} .
- **Send_Client**($\Pi_{UE}^i, (MAC_{gNB_t}||N_{gNB_t}||ID_{gNB_t}||inau_{gNB_t})$) is requested, compute $Key_{UE} = xy.P$, $MAC_{cfm} = H_3(Key_{gNB_t}^{UE}||SUPI||ID_{gNB_t}||x.N_{gNB_t})$ and session key $Key_{gNB_t}^{UE}$ in real protocol. Then it send MAC_{cfm} to \mathcal{ATT} .

Hence, it is observed that the game is indistinguishable from game G_3 . So,

$$Pr[Succ_4] = Pr[Succ_3] \quad (5)$$

Game G_5 : Here, we update the simulation queries of *Send_Client* instances for randomly chosen session in G_3 . In this game, we choose another way for computing the value of Key_{gNB_t}, Key_{UE} so it will be autonomous for handover acknowledgment value and keys. When

Send_Client($\Pi_{gNB_t}^j, (N_{UE} || RHI_{UE} || MAC_{UE} || SUCI || inau_{UE}))$ and **Send_Client**($\Pi_{UE}^i, (MAC_{gNB_t} || N_{gNB_t} || ID_{gNB_t} || inau_{gNB_t}))$ are requested $Key_{gNB_t} = Key_{UE} = T_z(\psi)$ (for UE and gNB_t), where $z \in Z_q^*$. The difference between game G_5 and G_4 is:

$$|Pr[Succ_5] - Pr[Succ_4]| \leq q_{ex} Adv_{\psi, q}^{CDH}(\Phi) \quad (6)$$

By considering a successful attacker \mathcal{ATT} to analyze G_5 and G_4 , we make the CDH fixer Φ . The difference between G_5 and G_4 is the way of calculation of Key_{gNB_t}, Key_{UE} for chosen session. Firstly, Φ obtains the CDH value (xP, yP, Z) . As G_5 and G_4 , the fixer Φ chooses a verifying session for Π_{UE}^i and $\Pi_{gNB_t}^j$ initiated legitimate clients UE and gNB_t respectively. When **Send_Client**($\Pi_{UE}^i, (AUTN_{AUSF}, XRESV')$) is requested, the Φ sets $N_{UE} = x.P$. In addition, when, **Send_Client**($\Pi_{gNB_t}^j, (N_{UE} || RHI_{UE} || MAC_{UE} || SUCI || inau_{UE}))$ and **Send_Client**($\Pi_{UE}^i, (MAC_{gNB_t} || N_{gNB_t} || ID_{gNB_t} || inau_{gNB_t}))$ are requested, Φ sets $y.P = N_{gNB_t}$ and $Key_{gNB_t}^{UE} = Z$.

The analyzer \mathcal{ATT} selects a random session for the test queries (**Test**(Π_{UE}^i), **Test**($\Pi_{gNB_t}^j$)), then the probability is $\frac{1}{q_{ex}}$. Hence, the Φ simulates all instances query without having information of x, y . From this, analyzer \mathcal{ATT} may generate $N_{UE} = x.P, y.P = N_{gNB_t}$ but not the correct Key_{gNB_t}, Key_{UE} . In case, $Z = xyP$, this setting for the analyzer is similar to G_4 . In case, $Z = zP$, this setting for the analyzer is similar to G_5 .

Lastly, if analyzer \mathcal{ATT} interacts with G_4 , the fixer Φ decides that $Z = xyP$. And, if \mathcal{ATT} interacts with G_5 , the fixer Φ decides that $Z \neq xyP$. Hence, eq. (6) holds. In this game, the keys Key_{gNB_t}, Key_{UE} are independent and random with secret keys. Therefore, three possibilities can be arises where an attacker analyzes the random and secret session keys as:

Case-1: Attacker queries $(zP, SUCI, ID_{gNB_t})$ to h . Then, this event obtains in $\frac{2q_{hash}}{l}$.

Case-2: Attacker requests **Send_Client** query excepting **Send_Client**($\Pi_{gNB_t}^j, m$) and impersonates UE to gNB_t . If an attacker, tries to impersonate UE in random session by generating MAC_{UE} and got success, it will make the discrepancy but the probability is less than to $\frac{1}{2^l}$. As there are maximum $2(q_{se} + q_{ex})$ sessions, then the total probability that this event is obtained will be less than to $\frac{2(q_{se} + q_{ex})}{2^l}$.

Case-3: Attacker requests **Send_Client** query excepting **Send_Client**(Π_{UE}^i, m) and masquerades the gNB_t to UE. Similar to *Case-2*;, the probability of this event is obtained less than to $\frac{2(q_{se} + q_{ex})}{2^l}$. Therefore, from above three cases;

$$|Pr[Succ_5]| = \frac{1}{2} + 2maxima\{\frac{q_{se} + q_{ex}}{2^l}, \frac{q_{hash}}{l}\} \quad (7)$$

By combining the eq. from (1) to (7), the results are:

$$\begin{aligned}
Adv_{\Pi}^{protocol}(\mathcal{ATT}) &= 2Pr[Succ_1] - \frac{1}{2} \\
&\leq (|Pr[Succ_2] - Pr[Succ_3]| + \\
&\quad |Pr[Succ_4] - Pr[Succ_5]| + \\
&\quad 2maxima\{\frac{q_{se} + q_{ex}}{2^l}, \frac{q_{hash}}{l}\}) \\
&\leq \frac{(q_{se} + q_{ex}^2)}{q} + \frac{q_{hash}}{2^l} + \\
&\quad 2q_{ex}Adv_q^{CDH}(\Phi) + \\
&\quad 4maxima\{\frac{q_{se} + q_{ex}}{2^l}, \frac{q_{hash}}{l}\}
\end{aligned}$$

6.3 Correctness of the Protocol

The proposed SEAI-AKA handover protocol is simulated using the AVISPA tool to prove its correctness. The protocol is programmed coded in classic High-Level Protocol Specification Language (HLPSL) to define its characteristics [29]. AVISPA tool simulates the protocol in numerous backends as On-the-Fly Model Checker (OFMC) and SAT-based Model-Checker (SATMC). There are two participants titled gNB and UE in the protocol. We have programmed the fundamental role of these participants in HLPSL and simulated the mechanism by adopting the AVISPA tool. The HLPSL program of the communicating participants is demonstrated in the *Appendix-A*. Also, the objectives of protocol are described in Fig. 5.

```

goal
  secrecy_of sec_ue_nuei, sec_gnb_ngnbi, sec_kuei_gnbs, sec_kuei_gnbt
  authentication_on gnb_uei
  authentication_on ue_gnbi
end goal

```

Fig. 5 Objectives of the SEAI Handover protocol

The simulation of the protocol is implemented by applying the OFMC back-end with a restricted number of terms. Essentially, the OFMC simulates handover protocol, and then attacker fetches the information from preceding executions. Therefore, OFMC attains the session complexity and averts replay attack without executing different sessions between communicating participants. Also, OFMC checks whether the genuine participants can execute the protocol by seeking the passive attacker and broadcasts the instructions of a few sessions to the attacker between genuine participants [30]. The test outputs show that the protocol dodges replay attack. The output of OFMC back-end model is represented in Fig. 6. The keyword **SAFE** in result proves the preciseness of protocol. Moreover, the protocol averts from the MitM attack by adopting the tests of OFMC back-end. Therefore, we achieve that the SEAI-AKA handover protocol gains the essential security characteristics and dodges the known attacks from the 5G network.

```

akshay@ubuntu: ~/Desktop/avispa-1.1
akshay@ubuntu:~/Desktop/avispa-1.1$ avispa testsuite/hlpsl/5gaka.hlpsl --ofmc
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/akshay/Desktop/avispa-1.1/testsuite/results/5gaka.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.05s
visitedNodes: 40 nodes
depth: 6 plies
akshay@ubuntu:~/Desktop/avispa-1.1$

```

Fig. 6 Output of OFMC back-end

6.4 Informal Analysis

In this section, we discuss various malicious attacks to show that the SEAI handover protocol is not vulnerable to the probable attacks.

- **KFS/KBS:** To preserve the KFS/KBS, the secret keys must not be acknowledged in the preceding and successive sessions even if it is compromised. In the protocol, UE achieves the RHI_{UE} and $Key_{gNB_s}^{UE}$ from gNB_s and AMF respectively in a secure communication even if ATT generates the required public keys. Moreover, ATT aims to achieve MAC_{UE}/MAC_{gNB_t} for self-verification at any participant. However, ATT can't obtain these authentication values as n_{UE} and n_{gNB_t} are random values at unique communication of handover. ATT needs the information of private keys to generate the preceding and following session keys of $Key_{gNB_t}^{UE}$. However, it fails to obtain these values as ECDLP is computationally hard. Also, the protocol doesn't follow the key chain framework and interaction with gNB_s . Therefore, ATT will never have the information of earlier/subsequent private keys.
- **Key Escrow Problem:** The UE or gNB_t select the secret keys in each handover authentication. To compute these secret keys, there is no association of third party such as a key generation center (KGC)/private key generator (PKG). Therefore, the protocol avoids the key escrow problem.
- **DoS Attack:** The ATT may transmit a large number of false handover requests to UE or gNB_t in the authentication stage to drain its network bandwidth. In the protocol, gNB_t obtains the $Key_{gNB_t}^{UE}$, MAC_{gNB_t} , and transfers the sequence message S_2 to the UE (as presented in Fig. 4). UE generates $Key_{gNB_t}^{UE}$ and authenticates MAC_{gNB_t} . After this, it sends the MAC_{cfm} to gNB_t . If the authentication is not successful, an authentication reject information is send to UE. As per the ECDLP infeasibility assumption, it is impractical for ATT to obtain the secret keys of the communicating participants. Hence, the proposed protocol avoids the DoS attack.
- **Privacy-Preservation:** In proposed protocol, UE transmits the SUCI to the ARPF followed by AMF as SUPI can't be transmitted over the communica-

tion channel and SUCI is applied to form this. The ARPF decrypts SUCI value by SIDA. Hence, the identity of the UE is achieved in the proposed protocol. In addition, the ID_{gNB_s} is never transmitted from AMF to UE for computing the $Key_{gNB_s}^{UE}$, RHI_{UE} . Suppose, ATT computes the ID_{gNB_t} transmitted from gNB_t to UE and attempts to compute the bogus MAC_{gNB_t} . However, an attacker can't derive the private keys due to computationally infeasibility assumption of ECDLP. Therefore, only legitimate UE can accept the ID_{gNB_t} from gNB_t .

- **Replay Attack:** In the authentication stage of handover mechanism, replay attack couldn't be initiated as each corresponding message has the chosen private keys. Let consider, ATT transmits duplicate informations to gNB_t/UE . Then, the communicating participants instantly verify that the information is achieved previously by them as secret/random keys are unique in every communication of handover. Also, ATT couldn't obtain the genuine $Key_{gNB_t}^{UE}$. Therefore, the protocol dodges the replay attack.
- **Redirection Attack:** The ATT can initiate redirection attack if it masquerade/impersonates UE or maintains the bogus gNB correctly. Moreover, no ATT could decrypt the identity of UE excluding the ARPF. Therefore, it can't obtain the original identity of the UE. Also, ATT fails to obtain identity of gNB_t and compute MAC_{gNB_t} . gNB_s sends LAI to gNB_t when the UE arrives in the range of gNB_t . Hence, protocol averts the redirection attack from the 5G network.
- **MitM Attack:** ATT can't implant the MitM attack at the authentication stage of protocol. It is noted that the $Key_{gNB_t}^{UE}$ is verified at UE and gNB_t successfully. Suppose, ATT corrupts the N_{UE} , N_{gNB_t} and generates the N_{UEATT} , N_{gNB_tATT} , where $N_{UEATT} = n_{UEATT}.P$ and $N_{gNB_tATT} = n_{gNB_tATT}.P$. Therefore, ATT generates the N_{UEATT} at gNB_t but, the $Key_{gNB_tATT}^{UE}$ is not generated rightly as $Key_{gNB_tATT}^{UE} = KDF(Key_{gNB_s}^{UE} || ID_{gNB_t} || inau_{gNB_t} || N_{UEATT}.n_{gNB_t})$. Similarly, ATT obtains N_{gNB_tATT} at UE but, the $Key_{gNB_tATT}^{UE}$ is not generated correctly as $Key_{gNB_tATT}^{UE} = KDF(Key_{gNB_s}^{UE} || ID_{gNB_t} || inau_{gNB_t} || n_{UE}.N_{gNB_tATT})$. As, the ATT doesn't have the information of UE's/ gNB_t secret key, so it is not possible for to obtain valid MAC_{UE}/MAC_{gNB_t} . Hence, ATT can't achieve the authentic handover message to execute MitM attack in the network.
- **Eavesdropping Attack:** In the handover establishment stage, the UE and AMF authenticate to each other. AMF transmits the $Key_{gNB_s}^{UE}$ to gNB_s and then gNB_s broadcasts RHI_{UE} to the UE. The chosen secret keys are private in all over the handover operations. Hence, ATT couldn't compute the secret session keys even though he/she calculates the universal/public specifications of the UE and gNB_s . In the handover authentication stage, the universal and handover specifications are transmitted between gNB_t and UE in the public channel.

The analysis of SEAI handover protocol and existing 5G protocols is presented in Table 2 based on numerous security characteristics. It can be defined that the current 5G handover protocol achieves the mutual authentication between the communicating participants in the authentication mechanism. Although, the protocol doesn't obtain the KFS/KBS and deteriorates from authentication complication. Also, the protocol fails to avoid DoS attack. The Cao's-AKA protocol doesn't

obtain the KFS/KBS and defeats from DoS, redirection, and eavesdropping attack. Also, Sharma's-AKA protocol fails to achieve the key secrecy and avoid system complexity. Additionally, the protocol is vulnerable to redirection attack. Zhang's-AKA protocol can't preserve the identity during the handover authentication; hence, it is susceptible to several security attacks. Similar to Zhang's protocol, Han's-AKA protocol has numerous security weaknesses and can't establish identity privacy preservation. Furthermore, Kumar's-AKA protocol obtains most of the security characteristics but can't prevent the MitM and eavesdropping attack from the communication network. Different from the current protocols, the proposed SEAI handover protocol executes the key procedures adopting the ECC. The protocol accomplishes the KFS/KBS in the authentication mechanism. Moreover, the protocol confronts all the potential attacks and free from the authentication complication. Therefore, the proposed protocol is relatively better compared to the existing protocols as it gains all the crucial security characteristics.

Table 2 Comparative scrutiny of the handover protocols

Handover Protocols	Security Characteristics									
	SC_1	SC_2	SC_3	SC_4	SC_5	SC_6	SC_7	SC_8	SC_9	SC_{10}
5G Handover [11]	Yes	No	Yes	No	Yes	No	No	Yes	No	No
Cao's-protocol [13]	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	No
Sharma's-protocol [14]	Yes	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes
Zhang's-protocol [15]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No
Han's-protocol [16]	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No
Kumar's-protocol [17]	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No
SEAI protocol	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

SC_1 : Establish mutual authentication; SC_2 : Retain KFS/KBS; SC_3 : Overcomes the key escrow problem; SC_4 : Defeats the DoS attack; SC_5 : Privacy-Preservation of the identity; SC_6 : Defeats the MitM attack; SC_7 : Avoids the authentication complexity; SC_8 : Defeats replay attack; SC_9 : Defeats the redirection attack; SC_{10} : Avoids the eavesdropping attack.

7 Performance Estimation

The performance of proposed SEAI handover protocol is estimated with respect to current 5G handover protocols in terms of computation, communication, and transmission overhead. The analysis represents that the proposed protocol gains all security objectives with adequate competence.

7.1 Computation Overhead

For the estimation of computation overhead of handover protocols at the authentication and initialization stage, elapsed time of various security functions is executed at OpenSSL written in C library [31] operating on 4 GB memory machine with Intel Core i5-7200U 4 GHz processor for gNB and 2.50 GHz processor for UE. Hence, the elapsed time (in ms) is: point multiplication (T_{pmul})= 0.441, hash (T_{hh})=0.0087, AES encryption/ decryption (T_{aes})=0.071, modular exponentiation (T_{moe})=0.629, arithmetic operation (T_{art})=0.0021, multiplication operation (T_{mul})=0.0033 (for gNB); T_{pmul} : 1.023, T_{hh} =0.0194, T_{aes} =0.109 ms, modular exponentiation (T_{moe})=1.277 ms, arithmetic operation (T_{art})=0.0074 ms, multiplication operation (T_{mul})=0.0091 ms (for UE). The computational overhead of current and proposed handover protocols is presented in Table 3.

The current 3GPP-5G handover protocol accepts the hash operations and symmetric cryptography that generates the overhead at each communicating participant in inter-gNB handover. However, the protocol fails to avoid the desynchronization that derives the DoS attack and complicated handover process. In the Cao's-AKA protocol, UE and base-station execute the hash operation for integrity and AES for encryption/decryption operations. However, the protocol shows less overhead compared to the proposed one but Cao's handover protocol is not secure against eavesdropping and redirection attacks. Also, the Han's-AKA protocol presents less computation overhead compared to the SEAI handover protocol as it executes only hash operations during handover operations but suffers from DoS and MitM attack. Both the Zhang's-AKA and Kumar's-AKA protocol operate the handover authentication using point multiplication, arithmetic, and multiplication operations. Moreover, the Sharma's-AKA protocol accesses the handover authentication by time-consuming modular exponentiation operations. Hence, these protocols aren't recommended for the development of efficient handover authentication protocol in the 5G network. Different from above ones, the proposed handover protocol forms the mutual authentication and key compliance between the gNB_i and UE by adopting point multiplication operation. Moreover, the protocol manages the key secrecy and overcomes the potential security susceptibilities. Hence, it obtains a significant security level compared to the current ones with competing overhead.

Table 3 Estimated analysis of handover protocols

Handover Protocols	Computation and communication overhead						
	$COMM^{UE}$ (in bits)	$COMM^{gNB_s}$ (in bits)	$COMM^\alpha$ (in bits)	$COMP^{UE}$ (in ms)	$COMP^{gNB_s}$ (in ms)	$COMP^\beta$ (in ms)	$COMP^\lambda$ (in ms)
5G han- dover [11]	-	-	1152	-	-	$4T_{hh}$	$2T_{hh}$
Cao's-AKA protocol [13]	384	640	1884	$3T_{aes} + 3T_{hh}$	$3T_{aes} + 4T_{hh}$	$3T_{aes} + 4T_{hh}$	$3T_{aes} + 3T_{hh}$
Sharma's- AKA protocol [14]	1044	832	2978	$3T_{moe} + 3T_{hh}$	$2T_{moe} + 4T_{hh}$	$3T_{moe} + 3T_{hh}$	$3T_{moe} + 4T_{hh}$
Zhang's- AKA protocol [15]	1124	1124	2658	$4T_{pmul} + 3T_{hh} + 3T_{art} + 3T_{mul}$	$4T_{pmul} + 2T_{hh} + 2T_{art} + 3T_{mul}$	$2T_{pmul} + 3T_{hh} + 2T_{art} + 3T_{mul}$	$2T_{pmul} + 3T_{hh} + 3T_{art} + 3T_{mul}$
Han's- AKA protocol [16]	636	448	1392	$4T_{hh}$	$3T_{hh}$	$3T_{hh}$	$3T_{hh}$
Kumar's- AKA protocol [17]	1048	1048	2412	$3T_{pmul} + 2T_{hh} + 2T_{art} + 2T_{mul}$	$3T_{pmul} + 2T_{hh} + 2T_{art} + 2T_{mul}$	$4T_{pmul} + 4T_{hh} + 4T_{art} + 3T_{mul}$	$2T_{pmul} + 4T_{hh} + 2T_{art} + 2T_{mul}$
SEAI Pro- tocol	832	512	1736	$T_{pmul} + 2T_{hh}$	$2T_{hh}$	$T_{pmul} + 3T_{hh}$	$T_{pmul} + 2T_{hh}$

$COMM^{UE}$: UE's communication overhead in initial authentication stage; $COMM^{gNB_s}$: gNB_s 's communication overhead in initial authentication stage; α : Communication overhead at inter-gNB handover; $COMP^{UE}$: UE's computation overhead in initial authentication stage; $COMP^{gNB_s}$: gNB_s 's computation overhead in initial authentication stage; β : UE's computation overhead in inter-gNB handover; λ : gNB_s 's computation overhead in inter-gNB handover.

Table 4 Specifications for communication overhead

Specifications	Cost(in bits)
$SUCI/PLMN_{ID}/ID_{gNB}/ECI/PCI$	128
$Key_{NG-RAN}^*/Key_{NG-RAN}^{**}$	256
$Key_{gNB_s}^{UE}/Key_{gNB_t}^{UE}$	128
$Key_{AUSF}/Key_{SEAF}/NH_{NCC}/Key_{AMF}$	256
RES/XRES	160
$N_{re}/\text{Timestamp } (T_{cur}/T_{exp})$	64
LAI/POS/NAI	40
MAC/CMAC/Hash	256

7.2 Communication Overhead

In order to measure the communication overhead of the current and proposed protocols, we fix $|p| = 1024$ and $|q| = 256$ because the ECC key indicates identical secrecy. The $|n| = |\#E(F_n)| = 256$ and $E(F_n): \#E(F_n) = 256$ bits prime order q . Moreover, Table 4 represents the specification list and their contents [32]. To estimate the overhead, we measure the contents of the broadcasted information between the communicating participants in the current and proposed handover protocols. In Table 3, the overhead of the protocols is measured. Although, the overhead of the SEAI handover protocol is larger than the 3GPP-5G handover mechanism. However, the 3GPP-5G protocol deteriorates from key negotiation issue, DoS attack, and authenticity complication. In the Cao's-AKA protocol, UE communicates to the target and future base-station for accomplishing mutual authentication respectively. The UE and base-stations share the message authentication codes, capability messages, and handover tickets in 1884 bits. Although, the protocol incurs less communication overhead during the handover initialization stage compared to proposed one because keys and identity are generated directly from the handover module. Also, the protocol suffers from key secrecy and DoS attack. In Sharma's-AKA protocol, the terminal and new/previous hub communicate with each other during handover authentication. The terminal transmits the sequence number, message authentication code, and various handover request/response. At the same time, the authentication server communicates with new and previous hubs in 2978 bits. Han's-AKA protocol follows the EAP-AKA during the initial authentication of UE and base-station. In the handover stage, the UE, base-station obtains the authentication parameters and use additional counter hash values. Also, the protocol fails to preserve the identity during the authentication process.

The Zhang's-AKA protocol establishes mutual authentication between the communicating participants. Firstly, UE transmits its one-time trapdoor hash key, secret, public keys, expiration time, and identity. Then, the target base-station sends its handover specifications to the UE with a shared secret key, and UE approves handover acknowledgment with base-station by transmitting the secret key. Similar to Zhang's-AKA protocol, Kumar's-AKA protocol accomplishes the mutual authentication between the communicating participants. Firstly, UE trans-

mits its secret, public keys, passwords, and pseudo-identity. Then, the target base-station sends its random number, secret keys, and public parameters to UE with a shared secret key, and UE accepts the handover message successfully.

The prime objective of the proposed SEAI handover protocol is to avoid the overhead at the communicating participants and evolve the security capabilities at the time of handover. Hence, we designed the handover protocol by adopting the ECC procedure. Our protocol setups the session key secrecy and $Key_{gNB_t}^{UE}$ is attained between gNB_t and UE without any ambiguous handover system. The UE and gNB_t maintain the secure mutual authentication in the protocol and there is no transmission of the secure session key in the public channel. Thus, the protocol is very efficient and secure compared to the current handover protocols.

Table 5 Transmission Overhead of Protocols

	5G Handover [11]	Cao's-AKA Protocol [13]	Sharma's-AKA Protocol [14]	Zhang's-AKA Protocol [15]	Han's-AKA Protocol [16]	Kumar's-AKA Protocol [17]	SEAI Protocol
$TO_{gNB_s/gNB_t-AMF/SN}^u$	2ρ	5ρ	4ρ	3ρ	3ρ	2ρ	2ρ
TO_{UE-gNB_s/gNB_t}^v	3σ	6σ	12σ	3σ	3σ	3σ	4σ
$TO_{gNB_s-gNB_t}^z$	2Δ	2Δ	2Δ	0	0	0	0

u : Transmission overhead between $gNB_s/gNB_t-AMF/SN$; v : Transmission overhead between gNB_s/gNB_t and UE; z : Transmission overhead between gNB_s and gNB_t .

7.3 Transmission Overhead

It is studied that the conventional cost of the message authentication between i) gNB_s/gNB_t and UE is ρ unit; ii) gNB_s and gNB_t is σ unit; and iii) AMF and gNB_s/gNB_t is Δ unit to measure transmission overhead of the proposed and current handover protocols. As the gNB is implanted a very long distance from AMF; hence the overhead of σ unit has the scope as $0 < \sigma < \rho$. Also, the overhead of ρ is greater than the cost of Δ . The transmission overhead of proposed and existing handover AKA protocols is demonstrated in Table 5. Hence, it is noticed that the overhead of proposed SEAI protocol is less compared to most of the existing protocols. Although, Kumars scheme has less transmission overhead but suffers from huge communication and computation overhead because of additional point multiplication operations during handover.

In the handover authentication stage of proposed protocol, 3 communication messages are required between gNB_t and UE. Although, only 2 messages are tolerable to form the mutual authentication between gNB_t and UE. The third correspondence message is broadcasted from the UE to approve the handover key agreement with gNB_t .

8 Conclusion

In this article, we introduced the secrecy and efficiency aware inter-gNB handover AKA protocol in 5G communication network to avoid the potential security susceptibilities as key negotiation, DoS & bogus base-station attack, and huge authentication complexity. In the proposed SEAI handover protocol, mutual authentication is accomplished with a secret key between gNB and UE. Also, the protocol forms the forward/backward secrecy and averts the network complications. In addition, simulation of the protocol is presented by AVISPA tool to prove the correctness. To obtain the session key secrecy, confidentiality, and integrity, the formal security proof of the protocol is carried out by the ROM. The security analysis is examined with corresponding numerous security specifications and obtains the security across potential attacks. The performance estimation clarifies that the SEAI protocol is far valuable compared to the current 5G handover protocols on the basis of various overhead analysis. Hence, we expect that the proposed protocol will enhance the performance and security of the 5G communication network in numerous handover systems.

A Appendix: Fundamental role of the communicating participants

Listing 1: HLPSSL code for UE

```
role ue(U, G:agent,
        SND, RCV: channel(dy),
        U_NUE, G_NgNB: public_key,
        P, RHI_UE, K_UE_GNBs, K_UE_GNBt: text,
        H1, H2, H3, KDF : function)
played_by U def=
```

```

local
  State : nat,
  IDgNBs, IDgNBt, SUCI, Inau_ue, Inau_gNBt,
  N_ue, N_gNBt : text

const sec_ue_nuei, sec_gnb_ngnbi,
sec_kuei_gnbs, sec_kuei_gnbt,
uei_gnb, gnb_ue : protocol_id,
success : text

init State := 0

transition

1. State = 0 /\ RCV(start) =|>
  State' := 1 /\ N_ue' := new()
  /\ SND({SUCI.N_ue'.P.H1(SUCI.
    N_ue'.Inau_ue.RH1UE.
    K_UE_GNBs).Inau_ue.RH1UE} -
    (inv(U_NUE)))
  /\ secret(N_ue', sec_kuei_gnbs,
    {U,G})
  /\ witness(G, SUCI, ue_gnb,
    RH1UE)

2. State = 1 /\ RCV({IDgNBt.N_gNBt'.P.
  Inau_gNBt.H2(IDgNBt.N_gNBt'.
  Inau_gNBt}) - (inv(G_NgNB))) =|>
  State' := 2
  /\ SND(H3(K_UE_GNBt.SUCI.IDgNBt.
    N_ue'.N_gNBt.P))
  /\ secret(K_UE_GNBt,
    sec_gnb_ngnbi, {U,G})
  /\ secret(N_ue', sec_kuei_gnbt,
    {U,G})
  /\ witness(G, U, gnb_uei, N_gNBt')

3. State = 2
  /\ RCV(success) =|>
  State' := 3
end role

```

Listing 2: HLPSTL code for gNB

```

role gnb(G, U:agent,
  SND, RCV: channel(dy),
  U_NUE, G_NgNB: public_key,
  P, RH1UE, K_UE_GNBs, K_UE_GNBt: text,
  H1, H2, H3, KDF: function)
played_by G def=

local
  State : nat,
  IDgNBs, IDgNBt, SUCI, Inau_ue, Inau_gNBt,
  N_ue, N_gNBt : text

const sec_ue_nuei, sec_gnb_ngnbi, sec_kuei_gnbs,
sec_kuei_gnbt, ue_gnb, gnb_uei : protocol_id,
success : text

```

```

init   State := 0
transition

1.State = 0 /\RCV({SUCI.N_ue'.P.H1(SUCI.N_ue'.
                Inau_ue.RHI_UE.K_UE_GNBs).
                Inau_ue.RHI_UE}-(inv(U_NUE)))=|>
State' := 1 /\N_gNBt' := new()
          /\SND({IDgNBt.N_gNBt'.P.Inau_gNBt.
                H2(IDgNBt.N_gNBt'.Inau_gNBt)}-
                (inv(GNgNB)))
          /\secret(N_gNBt',sec_gnb_ngnbi,
                {G,U})
          /\secret(IDgNBt,sec_kuei_gnbt,
                {G,U})
          /\witness(G,U,gnb_uei,K_UE_GNBt)

2.State = 1 /\RCV (H3(K_UE_GNBt.SUCI.IDgNBt.
                N_ue'.N_gNBt.P)) =|>
State' := 2 /\SND(success)
          /\request(G,U,gnb_uei,N_ue')
end role

```

References

- Shancang Li, Li Da Xu, and Shanshan Zhao. 5g internet of things: A survey. *Journal of Industrial Information Integration*, 10:1–9, 2018.
- Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong. A survey on security aspects for 3gpp 5g networks. *IEEE Communications Surveys & Tutorials*, 22(1):181–186, 2019.
- Shunliang Zhang, Yongming Wang, and Weihua Zhou. Towards secure 5g networks: A survey. *Computer Networks*, 162:106871, 2019.
- 3GPP. 3gpp technical specification; security architecture and procedures for 5g system. https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf, 2018.
- Xiaowei Zhang, Andreas Kunz, and Stefan Schröder. Overview of 5g security in 3gpp. In *Standards for Communications and Networking (CSCN), 2017 IEEE Conference on*, pages 181–186. IEEE, 2017.
- Mamta Agiwal, Abhishek Roy, and Navrati Saxena. Next generation 5g wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 18(3):1617–1655, 2016.
- Abhishek Khanna and Sanmeet Kaur. Internet of things (iot), applications and challenges: A comprehensive review. *Wireless Personal Communications*, 114:1687–1762, 2020.
- Ihsan Ullah and Hee Yong Youn. Intelligent data fusion for smart iot environment: a survey. *Wireless Personal Communications*, 114(1):409–430, 2020.
- Sotirios K Goudos, Panagiotis I Dallas, Stella Chatziefthymiou, and Sofoklis Kyriazakos. A survey of iot key enabling and future technologies: 5g, mobile iot, semantic web and applications. *Wireless Personal Communications*, 97(2):1645–1675, 2017.
- Kinza Shafique, Bilal A Khawaja, Farah Sabir, Sameer Qazi, and Muhammad Mustaqim. Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios. *IEEE Access*, 8:23022–23040, 2020.
- 3GPP. 3gpp technical specification; security architecture and procedures for 5g system. https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.07.00_60/ts_133501v150700p.pdf, 2020.
- 3GPP. 3gpp technical specification; security architecture and procedures for 5g system. https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.06.00_60/ts_133501v150600p.pdf, 2020.
- Jin Cao, Maode Ma, Yulong Fu, Hui Li, and Yinghui Zhang. Cppha: Capability-based privacy-protection handover authentication mechanism for sdn-based 5g hetnets. *IEEE Transactions on Dependable and Secure Computing*, 2019.

14. Vishal Sharma, Ilsun You, Fang-Yie Leu, and Mohammed Atiquzzaman. Secure and efficient protocol for fast handover in 5g mobile xhaul networks. *Journal of Network and Computer Applications*, 102:38–57, 2018.
15. Yinghui Zhang, Robert Deng, Elisa Bertino, and Dong Zheng. Robust and universal seamless handover authentication in 5g hetnets. *IEEE Transactions on Dependable and Secure Computing*, 2019.
16. Kaihong Han, Maode Ma, Xiaohong Li, Zhiyong Feng, and Jianye Hao. An efficient handover authentication mechanism for 5g wireless network. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–8. IEEE, 2019.
17. Amit Kumar and Hari Om. Design of a usim and ecc based handover authentication scheme for 5g-wlan heterogeneous networks. *Digital Communications and Networks*, 2019.
18. Akhil Gupta and Rakesh Kumar Jha. A survey of 5g network: Architecture and emerging technologies. *IEEE access*, 3:1206–1232, 2015.
19. Hans Christian Rudolph, Andreas Kunz, Luigi Lo Iacono, and Hoai Viet Nguyen. Security challenges of the 3gpp 5g service based architecture. *IEEE Communications Standards Magazine*, 3(1):60–65, 2019.
20. Jolly Parikh and Anuradha Basu. Technologies assisting the paradigm shift from 4g to 5g. *Wireless Personal Communications*, pages 1–22, 2020.
21. 3GPP. 3gpp technical specification; digital cellular telecommunications system (phase 2+) (gsm); universal mobile telecommunications system (umts); lte; 3gpp system architecture evolution (sae); security architecture,. https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/14.06.00_60/ts_133401v140600p.pdf, 2018.
22. Junseok Kim, Dongmyoung Kim, and Sunghyun Choi. 3gpp sa2 architecture and functions for 5g mobile communication system. *ICT Express*, 3(1):1–8, 2017.
23. Jari Arkko, Vesa Lehtovirta, and Pasi Eronen. Improved extensible authentication protocol method for 3rd generation authentication and key agreement (eap-aka'). *Network Working Group Request for Comments*, 5448:1–29, 2009.
24. Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.
25. Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.
26. Suman Majumder, Sangram Ray, Dipanwita Sadhukhan, Muhammad Khurram Khan, and Mou Dasgupta. Ecc-coap: Elliptic curve cryptography based constraint application protocol for internet of things. *Wireless Personal Communications*, pages 1–30, 2020.
27. Michel Abdalla and David Pointcheval. Interactive diffie-hellman assumptions with applications to password-based authentication. In *International Conference on Financial Cryptography and Data Security*, pages 341–356. Springer, 2005.
28. Shehzad Ashraf Chaudhry, Mohammad Sabzinejad Farash, Husnain Naqvi, SK Hafizul Islam, and Taeshik Shon. A robust and efficient privacy aware handover authentication scheme for wireless networks. *Wireless Personal Communications*, 93(2):311–335, 2017.
29. AVISPA. Avispa automated validation of internet security protocols. <http://www.avispa-project.org>, 2005.
30. Bhawna Narwal and Amar Kumar Mohapatra. Seemaka: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks. *Wireless Personal Communications*, 113(4):1985–2008, 2020.
31. OPENSSL. Openssl-cryptography and ssl/tls toolkit, technical report. <https://www.openssl.org/>, 2018.
32. Shubham Gupta, Balu L Parne, and Narendra S Chaudhari. Srgh: A secure and robust group-based handover aka protocol for mtc in lte-a networks. *International Journal of Communication Systems*, 32(8):e3934, 2019.

Figures

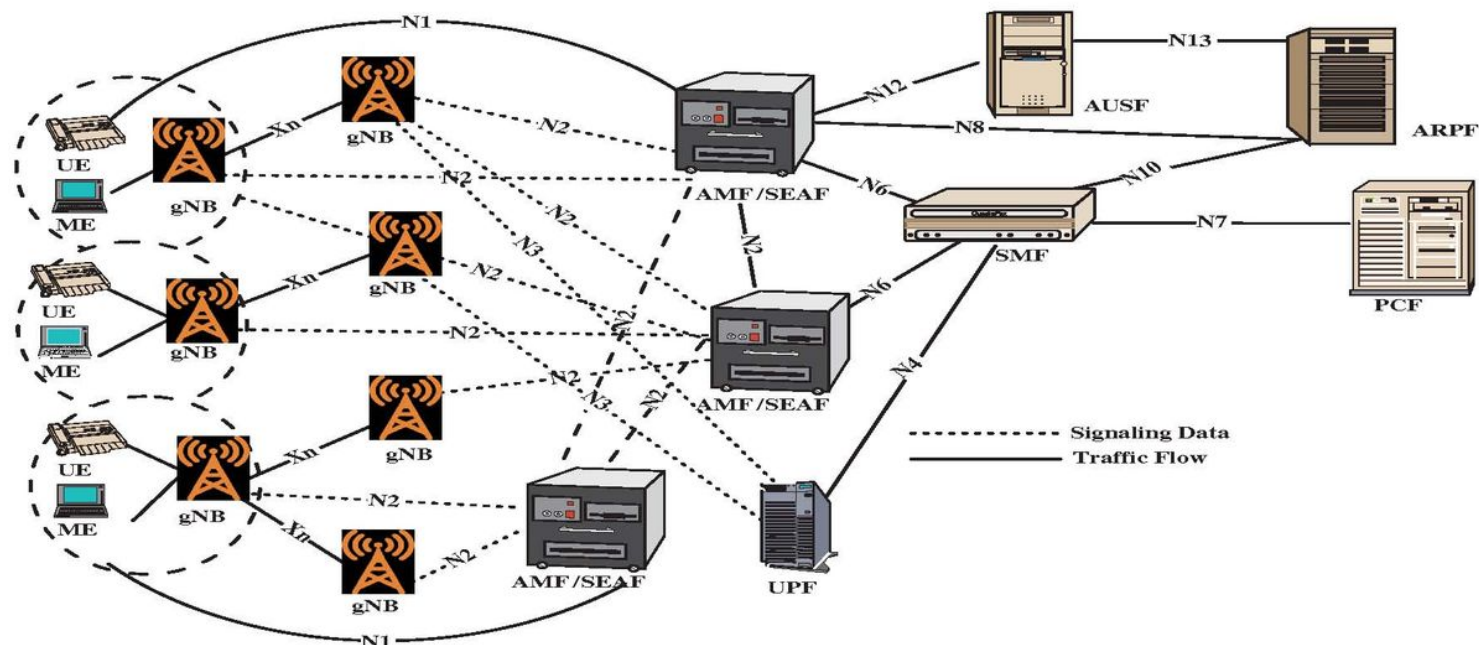


Figure 1

A handover framework of 5G communication network

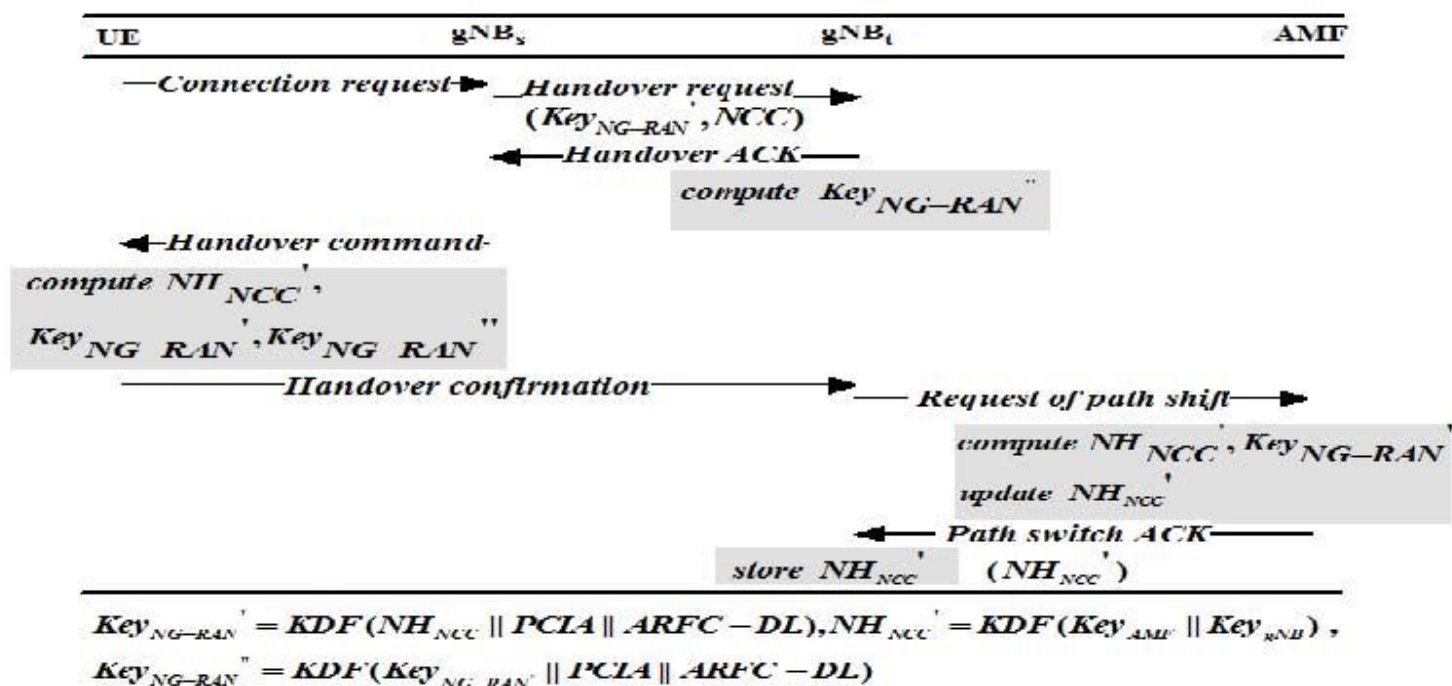


Figure 2

Inter-gNB 5G Handover Mechanism

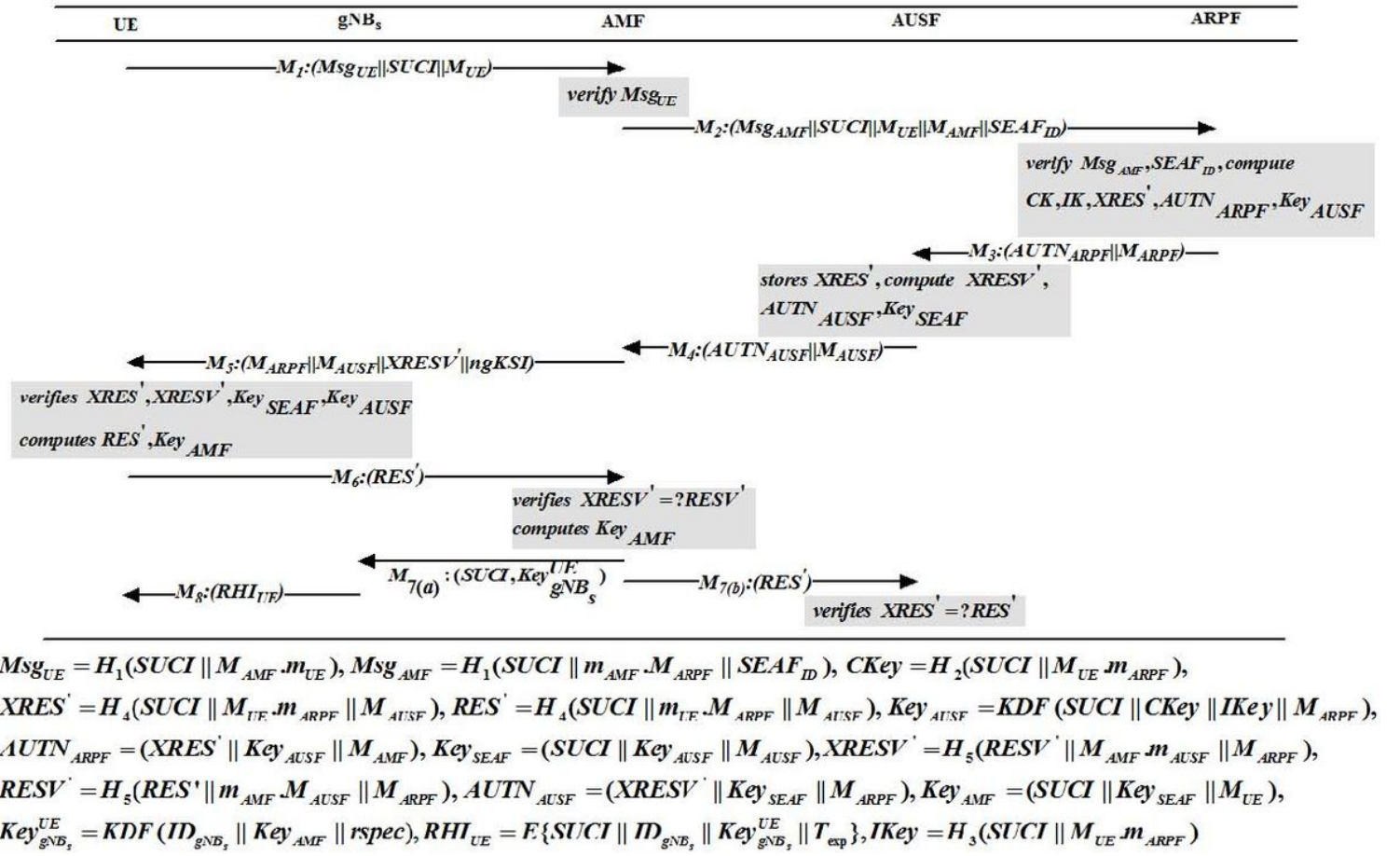


Figure 3

Handover Initialization Stage

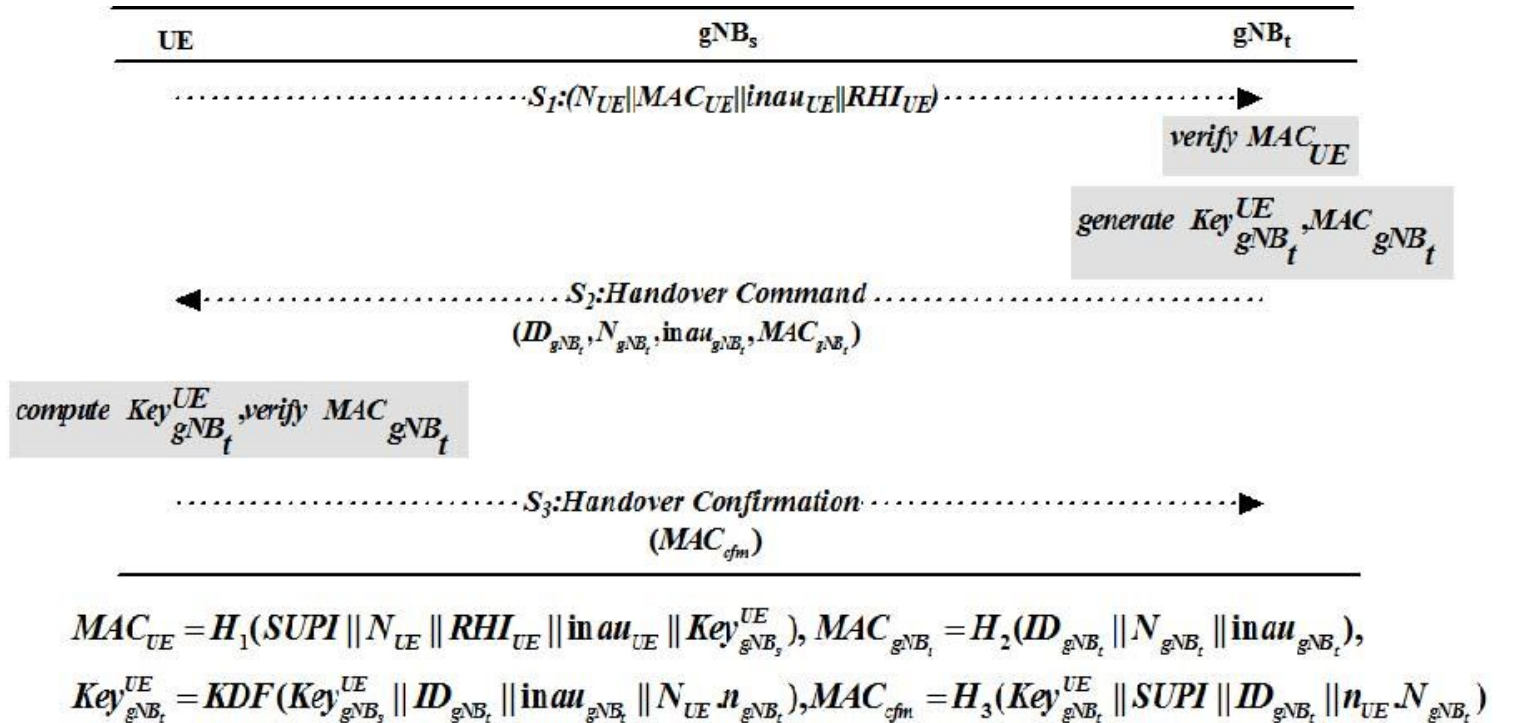


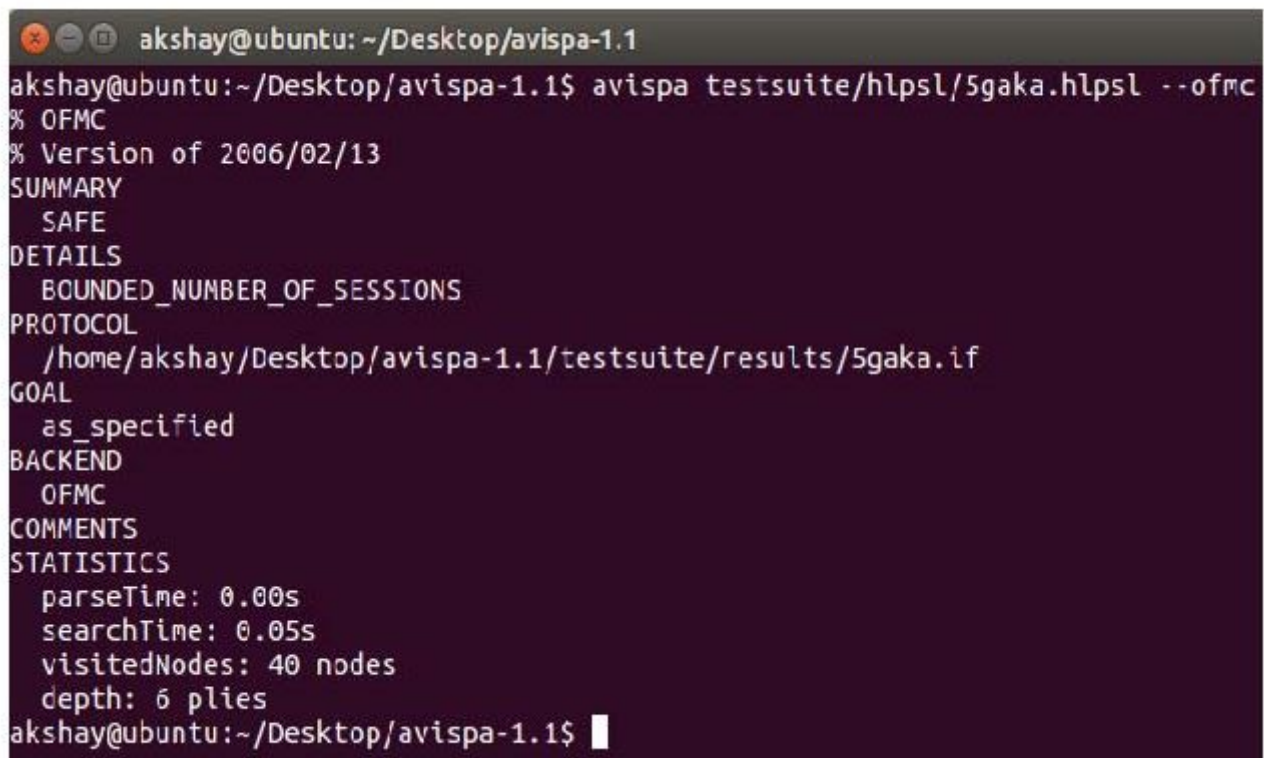
Figure 4

Handover Authentication Stage

```
goal
  secrecy_of sec_ue_nuei, sec_gnb_ngnbi, sec_kuei_gnbs, sec_kuei_gnbt
  authentication_on gnb_uei
  authentication_on ue_gnbi
end goal
```

Figure 5

Objectives of the SEAI Handover protocol



```
akshay@ubuntu: ~/Desktop/avispa-1.1
akshay@ubuntu:~/Desktop/avispa-1.1$ avispa testsuite/hlpsl/5gaka.hlpsl --ofmc
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/akshay/Desktop/avispa-1.1/testsuite/results/5gaka.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.05s
  visitedNodes: 40 nodes
  depth: 6 plies
akshay@ubuntu:~/Desktop/avispa-1.1$
```

Figure 6

Output of OFMC back-end