ESAP: Efficient and secure authentication protocol for roaming user in mobile communication networks

BALU L PARNE^{1,*}, SHUBHAM GUPTA¹ and NARENDRA S CHAUDHARI^{1,2}

¹Department of Computer Science and Engineering, Visvesvaraya National Institute of Technology (VNIT), Nagpur 440010, India

²Department of Computer Science and Engineering, Indian Institute of Technology (IIT), Indore 453552, India
e-mail: balu.parne@students.vnit.ac.in; shubham.gupta@students.vnit.ac.in; nsc0183@yahoo.com

MS received 2 March 2017; revised 27 June 2017; accepted 13 September 2017; published online 29 May 2018

Abstract. The Global System for Mobile communication (GSM) network is proposed to mitigate the security problems and vulnerabilities observed in the mobile telecommunication system. However, the GSM network is vulnerable to different kinds of attacks such as redirection attack, impersonation attack and Man in-the Middle (MiTM) attack. The possibility of these attacks makes the wireless mobile system vulnerable to fraudulent access and eavesdropping. Different authentication protocols of GSM were proposed to overcome the drawbacks but many of them lead to network signalling overload and increases the call set-up time. In this paper, an efficient and secure authentication and key agreement protocol (ESAP-AKA) is proposed to overcome the flaws of existing authentication protocol for roaming users in the GSM network. The formal verification of the proposed protocol is presented by BAN logic and the security analysis is shown using the AVISPA tool. The security analysis shows that the proposed protocol avoids the different possible attacks on the communication network. The performance analysis based on the fluid flow mobility model shows that the proposed protocol reduces the communication overhead of the network by reducing a number of messages. On an average, the protocol reduces 60% of network signalling congestion overhead as compared with other existing GSM-AKA protocols. Moreover, the protocol not only removes the drawbacks of existing protocols but also accomplishes the needs of roaming users.

Keywords. GSM; authentication; roaming user; AVISPA; BAN logic.

1. Introduction

Mobile communication is one of the fastest growing area of the wireless telecommunication networks. The Global System for Mobile Communication (GSM) is a pan-European digital cellular mobile system supporting widespread roaming and personal communication services (PCS) across the world [1, 2]. The GSM was designed to provide the authentication and data confidentiality using several authentication schemes [3–6]. It has become the global standard as it offers quality digital voice at the lowest cost. Nowadays, we are running towards 3rd or 4th generation of mobile communication networks, but still most of the services provided by the service providers are based on the 2nd generation of mobile communication networks. Also, the security architecture of the Evolved Packet System (EPS) in 4G follows the same principle as that of GSM and 3G network [7].

The GSM mobile network has been operational over the past two decades and is widespread throughout the world as several mobile equipment/devices operate on the GSM network. Yet, there are many more applications based on the GSM technology across the world [8–11]. These applications are effective and secure only after a successful authentication and key agreement (AKA) in the communication devices. Hence, there is a need to propose an efficient and secure AKA protocol for GSM network. Also, the 3rd generation partnership project (3GPP) technology, i.e., universal mobile telecommunication system (UMTS), and the long-term evolution (LTE) system are based on the GSM system. Therefore, it is possible to extend the proposed protocol for further upcoming technologies. It is expected that the proposed AKA protocol can be used in the various applications of the GSM networks.

Nowadays, UMTS and LTE mobile networks are dominating in the telecommunication market. However, the construction cost of the base station in these technologies is extremely high. Therefore, a number of telecommunication companies still adopt the GSM or integrate the GSM

*For correspondence

network with their network [7]. However, the existing GSM protocols suffer from lack of confidentiality, data integrity and authentication. To prevent the identified vulnerabilities, GSM network validates the identity of the mobile user through the challenge response scheme. In this scheme, the user authenticates himself by providing a response to a challenge sent by a network. However, extensive research on the GSM network exploits the issues of challenge response scheme such as the mutual authentication of communication entities, high bandwidth consumption and storage overhead. To improve the security of the GSM network, an improved solution needs to be designed to overcome the user authentication problems.

The architecture of GSM network consists of three subsystems as shown in figure 1 [1, 12–16]: the mobile station (MS) subsystem, base station subsystem and home subsystem. The MS and Subscriber Identity Module (SIM) card are the parts of the MS subsystem. The MSs are uniquely identified by their International Mobile Equipment Identity (IMEI). The SIM card has the International Mobile Subscriber Identity (IMSI), which is used to identify the subscriber to the system and a secret key for the authentication of MS. The Base Transceiver Station (BTS) and the Base Station Controller (BSC) are the parts of the base station subsystem. These elements are necessary in order to maintain the connectivity between the MS and the Mobile Switching Centre (MSC). The home subsystem consists of the MSC, Visitor Location Register (VLR), Home Location Register (HLR), Authentication Centre (AuC) and Equipment Identity Register (EIR) [1, 17]. The HLR works as a database that is used to store the complete local subscribers/users information and locations within the network. The VLR maintains the dynamic database and is responsible for storing the roaming user information. The AuC is a robust database that contains all the confidential and authentication information required by the VLR and HLR for each mobile user. The EIR has a database that keeps the information of all the valid MS on the communication network and prevents a stolen or fraudulent MS equipment from accessing the network. The MS communicates to the base stations via radio links that are connected to the MSC. The

Figure 1. The architecture of GSM network.

MSC is responsible for signal transmission between radio links and wired line networks [18].

1.1 Existing AKA protocol for roaming users in the GSM network

In the GSM network, authentication is necessary to ensure that the network services will not be accessed fraudulently [19]. The authentication is carried out using a challenge/response mechanism in the GSM network [20–22]. In the authentication process, it is important to maintain the secrecy of shared secret key K_i . The K_i is generated and installed into the SIM card at a secure place and a copy of the key is put into the HLR database. The security of GSM is based on the A3, A5 and A8 algorithms. A3 is a one-way function that computes the certificate to authenticate the MS, A8 is another one-way function that generates the secured session key K_c and A5 is an encryption/decryption algorithm [23, 24]. The authentication procedure follows the following steps as shown in figure 2 [1, 5, 12, 15, 25, 26]. First, the MS sends an IMSI to the network; then the network finds out the corresponding K_i of the received IMSI. Later, the network generates a RAND and forwards it to the MS over the air interface. From the generated challenge and the K_i , MS calculates the SRES by the A3 algorithm. Finally, MS sends the SRES to the network. From the received SRES, the network verifies the validity of the mobile user.

As long as the MS stays in the area covered by a particular VLR, it uses n copies of authentication parameters to verify the MS. Once the VLR uses all the n parameters, it forwards the authentication request to the HLR for another set of parameters as illustrated in figure 2. It explains the authentication process during location registration. Figure 3 illustrates the authentication procedure of the location update [16, 27]. First, the MS is registered at VLR1 to perform the location registration process. After a successful verification, VLR1 allocates the $TMSI_1$ to the MS. When the MS enters the coverage area of another VLR (VLR2), the flow of the signalling messages for location update is as follows:

- The MS transmits a $TMSI_1$ to VLR2 and VLR2 forwards it to the location area of VLR1.
- VLR1 transmits an IMSI and remaining authentication triplets to VLR2.
- VLR2 selects one of the triplet (RAND, SRES and K_c) for validating the MS and forwards RAND to the MS.
- Then the MS calculates SRES and transmits to the VLR2 and VLR2 authenticates the user information.
- After a successful verification of the MS, VLR2 transmits a location area update message to the HLR. Finally, HLR updates the location information of the MS.
- HLR sends an acknowledgment to the VLR2 and VLR2 assigns $TMSI_2$ to the MS.

Figure 2. Basic authentication protocol of GSM network.

Figure 3. Existing GSM-AKA protocol for roaming users in the network.

- Finally, HLR sends the $TMSI_1$ cancellation message to the VLR1.

Moreover, similar authentication steps will be followed as the MS moves to VLR3. If any visited VLR uses the n copies of authentication triplets then VLR must send a request to the HLR for another set of authentication parameters.

1.2 Attack analysis of the existing authentication protocol for GSM network

This subsection illustrates the security analysis of existing GSM-AKA protocol by considering the encryption scenario and various possible attacks on the GSM network.

- **Replay attack:** In this attack, first an adversary stores a copy of transmitted packets between the users and the network. Later, he/she misuses the previously captured information by re-transmitting the message in order to get access to the resources by replaying an authentication message.
- **Impersonation attack:** In this attack, an adversary eavesdrops the voice signalling and data messages of the target users. The existing protocols suffer from the impersonation attack as an adversary impersonates as a legitimate entity and sends the signalling messages to the network in order to believe that it originates from the authentic user.
- **Man in the middle attack (MiTM):** In the existing protocols, network authenticates only to the mobile equipment but vice-versa is not achieved. Hence, an adversary can launch a false BTS and impersonate himself as a legitimate one to perform MiTM attack.
- **Denial of service (DoS) attack:** In the existing protocols, an adversary sends several bogus requests to the mobile equipment that makes them inaccessible. Moreover, an adversary may keep the network busy by sending a number of unwanted authentication requests to the network.
- **Redirection attack:** In the existing protocols, an adversary locates the fake BTS in a particular area that performs as a legitimate one and broadcasts the signal over air to the mobile equipment. There is a possibility of redirection attack as the existing schemes provide unilateral authentication. The redirection attack may cause the mischarge billing problem in the communication network.
- **Interleaving attack:** In the existing protocols, an adversary collects the necessary information by compromising the network nodes and accessing the signalling messages on the network links. After intercepting the information, an adversary modifies the information to make it beneficial for him/her. Hence, there is a possibility of known plaintext and cipher-text attacks in the communication network.

1.3 Drawbacks of the existing authentication protocol for GSM network

The existing AKA protocol for GSM network suffers from various security and performance issues as follows [5, 12, 15, 25, 27]:

- Mutual authentication between the MS and VLR is not established. Only MS is authenticated by the VLR but vice-versa is not true. Hence, there is a possibility that an adversary may impersonate as the VLR and successfully perform the MiTM and redirection attack on the communication networks.
- If the MS resides in the location area of a particular VLR and uses all the available authentication

parameters, the VLR must send a request for another set of parameters to the HLR. Hence, the network suffers from high bandwidth consumption.

- Each VLR needs to store the n copies of authentication parameters (triplets) in its database. Therefore, there is a problem of storage overhead in the VLR.
- The computational complexity of the HLR is very high as it needs to generate all the triplets used by the VLR.
- If the MS shifts frequently to another VLR, the previous VLR needs to repeatedly forward the remaining copies of n authentication parameters to the new VLR. Hence, high bandwidth consumption occurs at VLRs.
- Moreover, the existing protocols in the GSM network are vulnerable to various security attacks such as redirection attack, DoS attack and MiTM attack.

1.4 Our contribution

In this paper, we propose a new efficient and secure authentication protocol (ESAP-AKA) to avoid the drawbacks of the existing AKA protocol for roaming users in the GSM network. Our contributions of the proposed protocol are summarized as follows:

1. The protocol follows the existing architecture of the GSM network and suits the roaming scenario.
2. The protocol achieves mutual authentication between the communication entities during the authentication process.
3. The protocol maintains the key secrecy and also guarantees the freshness of the keys used in the authentication process.
4. The protocol reduces the communication and computational overhead on the network as compared with existing AKA protocols.
5. The proposed protocol eliminates the identified security attacks and performance issues in the GSM network.
6. The proposed protocol, on an average, reduces 60% of signalling congestion overhead as compared with existing GSM-AKA protocol in the authentication process.

1.5 Organization of the paper

The organization of the paper is as follows. Section 2 describes a brief review of existing GSM authentication protocols. The proposed ESAP-AKA protocol for roaming users in GSM networks is proposed in section 3. The formal verification and security analysis of the protocol is carried out in section 4. In section 5, the performance analysis of the proposed protocol with respect to bandwidth consumption is presented. Finally, section 6 concludes the paper.

2. Review of authentication protocols for GSM network

In this section, we present an overview of existing GSM authentication protocols with respect to network architecture and various issues. Many AKA protocols were designed to overcome the drawbacks of the existing GSM authentication protocol. However, some researchers modified the architecture of GSM network. Moreover, the communication entities are authenticated by additional hardware and the public key cryptosystem to mitigate these problems [4, 28]. However, none of them succeeded in overcoming all the drawbacks of existing authentication protocol for roaming user in the GSM network.

Secure communication mechanisms for GSM network were proposed by Lo and Chen [13, 29], which were comparatively more secure than the original GSM protocol. However, the mechanism follows the public key cryptosystem and the architecture of GSM network is also customized. Lee *et al* [12] introduced an authentication protocol for GSM network to avoid the drawbacks without modifying the existing architecture. The protocol reduces the computational and storage overload of the communication entities, but it is vulnerable to the security attacks. Lee *et al* [15] designed a mutual authentication protocol to fix all the afore-mentioned drawbacks. In this protocol, the HLR verifies the authenticity of the MS and issues a ticket to the VLR. Later, the MS and VLR use the ticket to verify the authenticity of each other. However, this approach works perfectly for the first MS authentication, but fails in subsequent authentications [25]. Chang *et al* [25] proposed a modified approach that overcomes the identified security vulnerabilities. The protocols maintain the existing architecture of the GSM network, but mention the roaming scenario is not considered. An anonymous channel protocol was proposed that uses the authentication tickets and a hybrid key cryptosystem [30]. The authors also modified the architecture of the GSM network. Hahn *et al* [27] proposed an authentication protocol for the roaming users in the GSM network. The protocol avoids the signalling overload in the roaming network but cannot solve the problems of GSM network.

An identity-based secure authentication scheme for GSM network is proposed by Kumar *et al* [31]. In this approach, MS and VLR mutually authenticate each other and set up a session secret key between them. The authors modified the architecture of the GSM network that is not suitable for the roaming users. An Elliptic Curve Cryptography (ECC)-based authentication protocol is proposed in [2]. The protocol achieves the mutual authentication with minimum storage space and avoids various attacks. However, the protocol suffers from high computational complexity as asymmetric key operations are performed. Kalaichelvi and Chandrasekaran [32] proposed an AKA protocol for GSM network on the basis of weak secrets such as passwords and

PINs. Fanian *et al* [14] proposed a GSM authentication protocol that provides secure mutual authentication and reduces the call set-up time and bandwidth consumption. However, the authors modified the GSM network architecture and did not address the scheme for roaming scenario. Southern *et al* [33] proposed solutions to avoid possible attacks on the UMTS network because of unification with the GSM. First, the authors modified the GSM security protocol as a standalone solution and later the modification of the UMTS security protocol was designed as a second solution. Lee *et al* [16] proposed an efficient authentication protocol without altering the GSM architecture. The protocol fails to avoid all the identified attacks on the GSM network and also does not maintain the secrecy of the signalling data on the network.

A new location-based key generation and management approach was introduced in [34]. The MS's location information is used to generate the key by geo-encryption approach. The encryption is performed on the basis of the MS's location, which is known to the GSM network. The accuracy of the encryption and decryption depends on the positioning algorithm used. Moreover, the authors modified the architecture of GSM network. Fanian *et al* [35] proposed a new approach based on symmetric polynomials for mutual authentication. In this approach, the authors allocate the share of symmetric polynomial to each MS during the initial authentication. For subsequent authentication requests, the MS and VLR use these polynomial shares and verify each other. However, the authors use the TESLA protocol in the mutual authentication, which increases the memory utilization and processing time in the MS. In addition, Saxena and Chaudhari [5] proposed the SAKA protocol, which improves the authentication of GSM and reduces the bandwidth consumption, but the roaming scenario was not considered by the authors. Also, they did not provide a mechanism to maintain the security of signalling data transmission over the network.

To resolve the security problems and accomplish all the requirements, we propose an ESAP-AKA protocol for roaming users in the GSM network. The proposed protocol prevents the GSM network from different attacks such as replay attack, MiTM attack, DoS attack, interleaving attack and redirection attack. The protocol design follows the basic architecture of GSM network and resolves the synchronization problem between the communication entities. The protocol takes the advantage of existing schemes [5, 25]. In the proposed protocol, the HLR of the MS verifies the authenticity of the visited VLR and provides the authentication token to validate the MS without knowing K_i . The visited VLR keeps only a copy of T_{key} rather than n parameters to verify the MS. Hence, it reduces the storage overload at VLR. Moreover, the protocol suits the roaming scenario in the GSM network. Whenever MS shifts to the location area of another VLR, the previous VLR transmits only the T_{key} in place of remaining copies of

Table 1. Notations/symbols and definitions.

Symbol/ abbreviation	Definition
RAND	random Number
K_i	shared secret key between the MS and HLR
S_k	shared secret session key between HLR and VLR
K_c	temporary session key
T_1	timestamp generated by the MS for the first computed authentication
MAC	message authentication code
LAI	Location Area Identity
VLR_C_1	certificate of VLR computed for the 1 st authentication
VLR_C_j	certificate of VLR computed for the j^{th} authentication, $j > 1, j \in N$
VLR_C_p	certificate of VLR computed for the p^{th} authentication, $p > 1, p \in N$
T_{key}	shared secret key between VLR and MS
SRES	signed response message
$SRES_j$	signed response for the j^{th} authentication, $j > 1, j \in N$
$SRES_p$	signed response for the p^{th} authentication, $p > 1, p \in N$
A3, A5, A8	the secure algorithms of GSM network

n authentication parameters to the new VLR. Hence, it reduces the message signalling overhead between VLRs and the computational overload at the HLR. The notations/symbols to be used throughout this paper are listed in table 1.

3. The proposed ESAP-AKA protocol for roaming users in GSM network

In this section, we propose a new ESAP-AKA for roaming user in the GSM network. The protocol increases the authentication efficiency with less signalling congestion and reduces the computational delay. According to the basic architecture of GSM network, the channel between VLR and HLR is secure using the D interface. The mobile application part (MAP/D) protocol is used to exchange the message between them [36, 37]. The proposed protocol strictly follows the basic architecture of GSM network, so that the channel between VLR and HLR is assumed to be secure. The proposed protocol consists of three phases: (i) 1st authentication of MS with VLR, (ii) j^{th} authentication of MS with the same VLR, where $j > 1$ and $j \in N$ and iii) authentication of MS in roaming phase. The first phase is carried out when the MS enters into the coverage area of new VLR and requests the authentication. In the first phase, the HLR sends the T_{key} to VLR for verification of MS

without the knowledge of K_i as shown in figure 4. The second phase is executed when the MS halts the VLR and requests the j^{th} authentication. The roaming phase is executed when the MS traverses to the coverage area of the new VLR. Hence, the first phase is compiled only when the MS joins the network. The second and third phases are executed each time whenever the MS needs the services of the network. The request and response packet formats of the transmitted message in the authentication process of the proposed protocol are as shown in figures 5 and 6, respectively [38, 39].

3.1 Phase-1: The 1st authentication of MS with the visited VLR

- Whenever MS joins VLR, MS establishes a connection with VLR by forwarding the request message packet (TMSI, T_1 and MAC_1) to VLR. The message ID is the identity number assigned to the request message. The last field is time to live (TTL), which records a timer that controls how long the message is allowed to remain in the network.
- VLR identifies the corresponding IMSI from the previous VLR and transfers it together with T_1 , LAI and MAC_1 to the HLR. If the previous VLR is not available in the corresponding network, the MS can directly transmit the IMSI to the current VLR.
- After collecting the information, HLR verifies whether the VLR is valid or not. It calculates MAC'_1 and compares it to the received MAC_1 . If it is verified, MS is a legitimate user.
- After the validation of the MS and VLR, HLR generates the the response message packet (T_{key} and VLR_{Cert}). Then the HLR sends response message packet along with received T_1 to the VLR. The transmission of the pair (T_{key}, VLR_{Cert}) is encrypted with session key S_k of the HLR to protect from eavesdropping.
- After getting the authentication parameters, the VLR retains the T_{key} , VLR_{Cert} and T_1 in its database. Then it computes MAC_2 and VLR_C_1 . In addition, VLR maintains a counter for timestamp that increments after each transmission of VLR_C_i to the MS. VLR_C_i consists of MAC_2 and timestamp T_i .
- After receiving the VLR_C_1 , the MS verifies the validity of T_1 . If the result is positive, MS computes the MAC'_2 and compares it to the received MAC_2 . If $MAC_2 = MAC'_2$, MS generates T_{key} and SRES. Otherwise, the request is discarded.
- MS sends the computed SRES to the VLR. VLR computes SRES' and verifies with the acquired SRES. If $SRES = SRES'$, the MS is authenticated; otherwise, the request is discarded.

Figure 4. The proposed ESAP-AKA protocol for the 1st authentication in the network.

Message ID	IMSI/TMSI	T_1	MAC	TTL
1 Bytes	16 Bytes	8 Bytes	8 Bytes	1 Bytes

Figure 5. The request message packet format in ESAP-AKA protocol.

Message ID	VLR_Cert	T_1	T_{key}	TTL
1 Bytes	8 Bytes	8 Bytes	16 Bytes	1 Bytes

Figure 6. The response message packet format in ESAP-AKA protocol.

3.2 Phase-2: The j^{th} authentication of MS with the same VLR, $j > 1$ and $j \in N$

If MS halts/stays in the same VLR for a long time, to accomplish the objective of mutual authentication the second phase is executed. As long as the MS halts in the same VLR, the VLR uses the T_{key} to validate the MS for each call. Hence, the VLR does not need another set of authentication parameters from HLR. Different from the first phase, the $SRES_j/SRES_j'$ is calculated using T_{j-1} , $||T_j$ and T_{key} as the inputs of A8 algorithm as shown in figure 7.

While MS halts in the same VLR and needs a new communication, the MS generates $SRES_j$ and forwards an authentication request message to the VLR. The request message consists of TMSI, $SRES_j$ and T_j . After collecting the request from MS, the VLR verifies whether T_j is legitimate or not. If it is found to be valid, VLR calculates the $SRES_j'$ and compares it to the acquired $SRES_j$. Otherwise, the authentication request is discarded. If $SRES_j' = SRES_j$, MS is authenticated and the value of stored

Figure 7. The proposed ESAP-AKA protocol for the j^{th} authentication in the network.

timestamp to T_j is updated. Otherwise, the authentication process is terminated. Then VLR calculates VLR_C_j and transmits to MS along with T_j . Once the MS collects the message, it verifies the validity of T_j . If it is verified, the MS extracts the MAC_2 from VLR_C_j and computes $MAC_2' = A_8(VLR_{Cert} || T_1, T_{key})$. If $MAC_2 = MAC_2'$, VLR is validated and MS accumulates T_j in its database. Otherwise, the authentication process is terminated.

3.3 Phase-3: Roaming MS

When MS shifts to another VLR, the roaming MS performs either the location registration or the location updation as illustrated in figure 8. The flow of signalling messages is as follows:

- When MS moves to the coverage area of VLR2, MS computes $SRES_p = A_8(T_p, T_{key})$ and sends a $TMSI_1$, T_p and $SRES_p$ to VLR2.
- Upon receiving the message from MS, VLR2 sends the $TMSI_1$ to the coverage area of VLR1.

Figure 8. The proposed ESAP-AKA protocol for roaming user in the network.

- After receiving the $TMSI_1$ from VLR2, VLR1 forwards the IMSI and T_{key} through a secure channel to the VLR2.
- Then VLR2 computes $SRES'_p = A8(T_p, T_{key})$ and compares it to the received $SRES_p$. If $SRES_p = SRES'_p$, MS is verified; otherwise, the authentication process is terminated.
- Once the authenticity of MS is verified by VLR2, VLR2 computes $VLR_C_p = (MAC_2 \parallel T_p)$ and transmits it to the MS along with T_p .
- Later, MS verifies the validity of T_p . If it is verified, the MS extracts the MAC_2 from VLR_C_p and calculates $MAC'_2 = A8(VLR_Cert \parallel T_p, T_{key})$. If $MAC_2 = MAC'_2$, VLR is the legitimate one. Otherwise, the process is terminated.
- VLR2 transmits location update message to the HLR. HLR updates the current location of the MS accordingly and transmits an acknowledgement to the VLR.
- VLR2 assigns $TMSI_2$ to the MS.
- Finally, $TMSI_1$ cancellation message is transmitted from HLR to VLR1.

If the MS connects to VLR3, a similar authentication procedure will be executed. For security reasons, an interval of T_{key} validity should be set, or it must be effective before a certain number of message forwardings is accomplished.

4. Formal verification and security analysis of the proposed ESAP-AKA protocol

4.1 Formal verification of the proposed ESAP-AKA protocol

In this subsection, we formally demonstrate the authentication process of the proposed ESAP-AKA protocol

using the BAN Logic. The statements of our analysis are formally verified using BAN logic. The BAN logic was formulated by Burrows, Abadi and Needham in 1989 [40]. It is a methodology of logical verification of authentication protocol that formally states the knowledge of information. It formally verifies the information exchanged and the trust among communicating parties at each step in the authentication protocol. It is defined to formalize the description and analysis of the authentication protocols [40–42].

The formalism is based on several sorted model logic. In the logic there are various objects such as principals, encryption keys and statements (also called as formulas). The symbols P, Q and S denote principals; K_{ab} , K_{as} and K_{bs} denote shared keys; K_a , K_b and K_s denote public keys and $K_{a^{-1}}$, $K_{b^{-1}}$ and $K_{s^{-1}}$ denote the corresponding secret keys; N_a , N_b and N_s denotes the specific statements. The symbols P, Q and R range over principals; X and Y range over statements; K ranges over encryption keys. The most often used constructs in BAN logic are listed as follows [40, 41, 43]:

1. $P \equiv X$: P believes X. The principal P acts as if X is true. P knows that X is indeed true or the truth of X is justified by some evidence.
2. $P \triangleleft X$: P sees X. Someone has sent a message including X to P, who can read and repeat X.
3. $P \mid \sim X$: P once said X. The principal P at some time sent a message containing the statement X. It is known that P believed X when it sent the message.
4. $P \Rightarrow X$: P has jurisdiction over X. P controls X. This construct is used when a principal has delegated authority over some statement.

5. $\#(X)$: The formula X is fresh, i.e., X has not sent a message before the current run of the protocol.
6. $P \xleftrightarrow{k} Q$: P and Q may use the shared secret key k to communicate. The k is secure, in that it will never be discovered by any principal except P or Q , or a principal trusted by one of them.
7. $\xrightarrow{k} P$: P has K as a public key. The matching secret key, K^{-1} , will never be discovered by any principal except P , or a principal trusted by P .
8. $P \xleftrightarrow{X} Q$: P and Q share a secret X . It is known only by them, and possible principals trusted by them. An example of a shared secret is a password.
9. $(X)_k$: It represents that the formula X is encrypted under the key k .

The formal analysis of the proposed ESAP-AKA protocol is performed as follows [40, 41, 43–45]:

- idealize the protocol by replacing conventional message with idealize message;
- state the initial assumption in the language of BAN logic;
- attach the logical formulas to the statements of the protocol to annotate the idealized protocol with logical formulas;
- apply the inference rules to the assumptions and the assertions in order to identify the beliefs held by the parties in the protocol.

4.1a The conventional/formal messages in proposed protocols:

- $M_1: MS \rightarrow VLR: TMSI, Na, MAC_1$.
- $M_2: VLR \rightarrow HLR: IMSI, Na, LAI, MAC_1$.
- $M_3: HLR \rightarrow VLR: Na, (T_{key}, VLR_{Cert})_{S_k}$.
- $M_4: VLR \rightarrow MS: VLR_{C1}$.
- $M_5: MS \rightarrow VLR: SRES$.

4.1b Transform messages into idealized logical form:

- $M_1: MS \rightarrow VLR: Na, A3(Na, LAI)_{K_i}, MS \xleftrightarrow{K_i} HLR$
- $M_2: VLR \rightarrow HLR: Na, A3(Na, LAI)_{K_i}$
- $M_3: HLR \rightarrow VLR: (A3(Na)_{K_i}, A3(A3(Na, LAI)_{K_i})_{K_i})_{S_k}, X$
where, $X = HLR \xleftrightarrow{T_{key}} VLR, HLR \xleftrightarrow{S_k} VLR$
- $M_4: VLR \rightarrow MS: Nb, A8(A3(A3(LAI, Na)_{K_i})_{K_i}, Nb)_{T_{key}}$
- $M_5: MS \rightarrow VLR: A3(Na)_{K_i}, A8(Nb)_{T_{key}}$

4.1c *Security assumption about the original messages:* In this subsection, we have listed out the assumptions while designing the protocol.

- It is pretended that K_i is a shared secret key between the MS and HLR.

- MS has a secure key K_i and MS believes K_i is a shared secret key between the MS and HLR. $MS \models MS \xleftrightarrow{K_i} HLR$
- HLR has a secure key K_i and HLR believes K_i is a shared secret key between the MS and HLR. $HLR \models MS \xleftrightarrow{K_i} HLR$

- It is pretended that VLR trusts the HLR.

- $VLR \models HLR \mid \Rightarrow MS \xleftrightarrow{K_i} HLR$
VLR believes that HLR has a control over shared secret key K_i between MS and HLR
- $\frac{VLR \mid \sim P, HLR \triangleleft P}{HLR \models VLR \models P}$
VLR once said principal P ; as VLR sent P it is known that VLR believes P ; also HLR sees P implies that HLR believes VLR believes P
- $\frac{HLR \mid \sim P, VLR \triangleleft P}{VLR \models HLR \models P}$
HLR once said principal P ; as HLR sent P it is known that HLR believes P ; also VLR sees P implies that VLR believes HLR believes P

- assumed that communication channel between the HLR and the VLR is safe

- $HLR \models HLR \xleftrightarrow{S_k} VLR$
- $VLR \models VLR \xleftrightarrow{S_k} HLR$
where S_k is a shared secret session key between VLR and HLR.
- $HLR \models VLR \xleftrightarrow{X} HLR$
- $VLR \models VLR \xleftrightarrow{X} HLR$,
where X is the conveyance message between VLR and HLR.

4.1d Annotated statements of protocol analysis:

- $M_1: MS \rightarrow VLR: MS \models \#(Na) \wedge VLR \models \#(Na); VLR \triangleleft Na, A3(Na, LAI)_{K_i}$
- $M_2: VLR \rightarrow HLR: HLR \triangleleft Na, LAI, A3(Na, LAI)_{K_i}$,
after receiving check $A3(Na, LAI)_{K_i}$
- $M_3: HLR \rightarrow VLR: VLR \triangleleft A3(A3(Na, LAI)_{K_i})_{K_i}, A3(Na, LAI)_{K_i} HLR \models \forall (VLR \xleftrightarrow{T_{key}} MS)$
- $M_4: VLR \rightarrow MS: MS \models \#(Na) \wedge VLR \models \#(Nb), MS \triangleleft Nb, A8(A3(A3(LAI, Na)_{K_i})_{K_i}, Nb)_{T_{key}}$
- $M_5: MS \rightarrow VLR: VLR \triangleleft A8(Nb)_{T_{key}}, MS \models A3(Na)_{K_i}$,
after receiving check $A8(Nb)_{T_{key}}$

4.1e *Inference rules:* In this subsection, we present the inference rules of the proposed protocol, which is useful in the formal proof to identify the beliefs held by the parties in the protocol.

- Message meaning rule

$$\frac{MS \models (MS \xleftrightarrow{K_i} HLR) \wedge (VLR \xleftrightarrow{T_{key}} MS), MS \triangleleft A3(Na, LAI)_{K_i}}{MS \models HLR \mid \sim A3(Na, LAI)_{K_i}}$$

validates the authenticity of the MS by verifying SRES. The VLR needs to keep a replica of T_{key} as a substitute of n copies of authentication parameters. Hence, this

$$\frac{VLR \models (VLR \xleftrightarrow{S_k} HLR) VLR \triangleleft (A3(Na)_{K_i}, A3(A3(Na, LAI)_{K_i})_{K_i})_{S_k}}{VLR \models HLR \mid \sim (A3(Na)_{K_i}, A3(A3(Na, LAI)_{K_i})_{K_i})_{S_k}}$$

$$\frac{VLR \models A3(Na)_{K_i} \wedge (VLR \xleftrightarrow{T_{key}} MS), VLR \triangleleft (A8(A3(A3(Na, LAI)_{K_i})_{K_i}), Nb)_{T_{key}}}{VLR \models HLR \mid \sim (A8(A3(A3(Na, LAI)_{K_i})_{K_i}), Nb)_{T_{key}}}$$

- Nonce verification rule

$$\frac{MS \models \#(Na) \wedge \#(Nb), MS \models HLR \mid \sim A3(Na, LAI)_{K_i}}{MS \models HLR \models A3(Na, LAI)_{K_i}}$$

$$\frac{VLR \models \#(Na) \wedge \#(Nb), VLR \models HLR \mid \sim A8(A3(A3(Na, LAI)_{K_i})_{K_i}, Nb)_{T_{key}}}{VLR \models HLR \models A8(A3(A3(Na, LAI)_{K_i})_{K_i}, Nb)_{T_{key}}}$$

- Jurisdiction rule

$$\frac{MS \models HLR \mid \Rightarrow A3(Na, LAI)_{K_i}, MS \models HLR \models A3(Na, LAI)_{K_i}}{MS \models A3(Na, LAI)_{K_i}}$$

$$\frac{VLR \models HLR \mid \Rightarrow A8(A3(A3(Na, LAI)_{K_i})_{K_i}, Nb)_{T_{key}}, VLR \models HLR \models A8(A3(A3(Na, LAI)_{K_i})_{K_i}, Nb)_{T_{key}}}{VLR \models HLR \models A8(A3(A3(Na, LAI)_{K_i})_{K_i}, Nb)_{T_{key}}}$$

4.1f Goal analysis: The communication overhead among the VLRs increases as the MS roams frequently. In the proposed protocol, the VLR passes only the T_{key} instead of n authentication parameters to reduce the overhead. Thus, it is suitable for roaming users and minimizes the communication overload. The mutual authentication between MS and VLR/HLR is ensured in the proposed protocol as $MS \models HLR \models VLR \wedge VLR \models HLR \models MS \longrightarrow MS \models VLR \wedge VLR \models MS$. For successive authentications, even if the HLR is not physically involved, the MS still authenticates the HLR with the participation of T_{key} . T_{key} is the agreement key between MS and VLR as $MS \models \#(Na), MS \models T_{key} \wedge \#(Nb)$, since $T_{key} = A3(Na)_{K_i}$. $VLR \models \#(Na), VLR \models T_{key} \wedge \#(Nb)$, since $HLR \rightarrow VLR \mid \sim T_{key}$. The VLR

approach diminishes the storage overhead in VLR compared with original authentication protocol. The HLR validates VLR and grants a temporary secret key T_{key} to authenticate MS. As long as the MS halts in the same VLR or moves across the VLRs, the VLR can use T_{key} to validate the authenticity of MS for each call. Hence, in the proposed protocol, VLR does not need another set of authentication parameters from HLR. Hence, the communication overload between the VLR and HLR is reduced. Also, the computational overload of the HLR can be reduced as the HLR need not generate n authentication parameters. The key freshness between the MS and the VLR holds as $MS \models \#(Na) \wedge VLR \models \#(Na), VLR \models \#(Nb) \wedge MS \models \#(Nb), T_{key} = A3(Na)_{K_i}$.

The confidentiality between the MS and the VLR is maintained as

$$\frac{MS \models (MS \xleftrightarrow{T_{key}} VLR), MS \triangleleft A5(Message)_{T_{key}}}{MS \models VLR \mid \sim Message} \wedge$$

$$\frac{VLR \models (VLR \xleftrightarrow{T_{key}} MS), VLR \triangleleft (Message)_{T_{key}}}{VLR \models MS \mid \sim Message}.$$

If an adversary gets Na from M_1 , he/she is unable to forge message M_1 and M_2 as an adversary has no clue of K_i . If an adversary gets Nb from message M_4 , he/she does not have knowledge of T_{key} . Hence, an adversary

not possible to redirect the traffic in communication network. According to the jurisdiction rule, the MAC is computed at MS and verified at HLR. It prevents the impersonation of the MS. Moreover, the integrity of MAC between the MS and HLR will be violated if the adversary impersonates to the legitimate VLR. This prevents the impersonation of the VLR. The timestamps Na and Nb act as the counter values and these values are incremented for each authentication request. Hence, the server can easily verify the repeated requests from the counter values and ignore them. The nonce verification rule illustrates that the proposed protocol maintains the freshness of the timestamp values between the communication entities

$$\frac{VLR \models \#(Na) \wedge \#(Nb), VLR \models MS \mid \sim A8(A3(A3(Na, LAI)_{K_i})_{K_i}, Nb)_{T_{key}}}{VLR \models MS \models A8(A3(A3(Na, LAI)_{K_i})_{K_i}, Nb)_{T_{key}}}$$

will never succeed in forging message M_4 and M_5 . For every authentication request, the values of Na and Nb are updated. Therefore, the communication network is free from the replay attack in the proposed protocol. An adversary has knowledge of neither T_{key} nor A5 encryption algorithm; hence, he/she never succeeds in eavesdropping the traffic between communication entities. The message meaning rule clearly shows that the proposed protocol maintains the secrecy of T_{key} in the communication network. It secures the communication network from the MiTM attack. The integrity of the base station is preserved using $MAC = A3(LAI \parallel Na)_{K_i}$. Hence, it is

and

$$\frac{MS \models \#(Na) \wedge \#(Nb), MS \models VLR \mid \sim A8(Nb)_{T_{key}}}{MS \models VLR \models A8(Nb)_{T_{key}}}.$$

Hence, DoS attack is avoided by the proposed protocol.

In table 2, a comparative analysis of the identified goals for proposed ESAP-AKA protocol with existing authentication protocols of GSM network is illustrated. It is observed that the proposed protocol achieves all the goals defined in section 2. The existing protocols fail to fulfill all

Table 2. Comparison among the GSM authentication protocols on various parameters.

Parameters to compare	AKA protocols											ESAP-AKA
	Original GSM	[1]	[29]	[26]	[12]	[15]	[27]	[25]	[14]	[16]	[5]	
ROU	No	No	No	No	No	No	Yes	No	No	Yes	No	Yes
TOC	SYM	ASYMM	ASYMM	ASYMM	SYM	SYM	SYM	SYM	Hybrid	SYM	SYM	SYM
SBC	No	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
RSOVLR	No	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
RCOHLR	No	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
STOSD	No	No	No	No	No	No	No	No	No	No	No	Yes
NSCA	No	No	No	No	No	No	No	No	Yes	No	No	Yes
MAUTH1	No	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes
MAUTH2	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes
FGSMA	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

ROU: suitable for roaming users; TOC: type of cryptosystem used; SBC: solves the problem of bandwidth consumption; RSOVLR: reduces the storage overload of VLR database; RCOHLR: reduces the computational overload of HLR; STOSD: secure transmission of signalling data; NSCA: network signalling congestion avoidance; MAUTH1: mutual authentication at the time of location; registration; MAUTH2: mutual authentication at the time of location update; FGSMA: follows the basic architecture of GSM network; SYM: symmetric key cryptosystem; ASYMM: asymmetric key cryptosystem

```

goal

  secrecy_of sec_key1, sec_sk1
  authentication_on hlr_ms
  authentication_on ms_vlr
  authentication_on vlr_hlr

end goal

```

Figure 9. Goals of the proposed protocol.

Figure 10. Results summarized by OFMC.

the goals and do not suit for roaming scenario. Hence, the proposed ESAP-AKA protocol is comparatively superior to existing protocols for GSM network.

4.2 Security verification using AVISPA tool

To provide the key agreement and mutual authentication between communication entities is the main objective of the proposed ESAP-AKA protocol. In this section, the formal verification of the protocol using Automated Validation of Internet Security Protocol and Applications (AVISPA) tool is carried out and coded in High Level Protocol Specifications Language (HLPSL) for the analysis of network security protocols [46–48]. AVISPA consists of the verification back-end servers such as OFMC (On-the-Fly-Model-checker), CL-ATSE (CL-based attack searcher) and SATMC (SAT-based Model-Checker) [49, 50]. The goals of the proposed ESAP-AKA protocol are shown in figure 9. The figure 10 presents the output of the OFMC model analysis results. In figure 10, SAFE keyword represents that ESAP-AKA protocol achieves the specified goals as shown in figure 9. In addition, the simulation of the protocol is demonstrated in figure 11. Hence, it is observed that the proposed protocol obtains the security requirements and avoids all the identified attacks.

The primary goals of the proposed ESAP-AKA protocol are to provide mutual AKA between the MS and VLR because all the keys used among these communication entities (K_i , T_{key}) are computed on either ends, without being transmitted over any communication channels. In the proposed protocol, there are three participants such as MS, VLR and HLR. The basic role of these participants is described in the HLPSL code. In this paper, we present the authentication analysis among MS, VLR and HLR. The basic role of MS, VLR and HLR is shown in Appendix I..

Figure 11. Simulation of the proposed ESAP-AKA protocol.

Table 3. Prevention of GSM-AKA protocols from various security attacks.

Prevention from attacks	AKA protocols											ESAP-AKA
	Original GSM	[1]	[29]	[26]	[12]	[15]	[27]	[25]	[14]	[16]	[5]	
Replay attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Impersonation attack	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Man in-the Middle (MiTM) attack	Yes	No	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes
Denial of service (DoS) attack	No	No	No	No	No	No	No	Yes	No	Yes	Yes	Yes
Redirection attack	No	No	No	No	Yes	No	No	No	No	No	Yes	Yes
Interleaving attack	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protection of signalling message	No	No	No	No	No	No	No	No	No	No	No	Yes

4.3 Security analysis

Table 3 illustrates the prevention of GSM network from various attacks such as reply attack, impersonation attack, MiTM attack, DoS attack, redirection attack and interleaving attack. In literature, there are a number of protocols designed to overcome the security vulnerabilities but none of them succeed in defeating all the identified attacks. Different from existing GSM-AKA protocols, the proposed ESAP-AKA protocol avoids all the potential attacks and obtains secure data communication on the network. Hence, the protocol is comparatively superior to existing AKA protocol. We clarify that the proposed ESAP-AKA protocol prevents the communication network from all these identified attacks.

- **Replay attack:** A unique random number/timestamp is used to avoid the network from replay attack. As the timestamp T_i is embedded with the authentication parameters it is merely impossible to compute the messages and reply them without the knowledge of k_i and T_{key} . Hence, the replay attack is not possible in the proposed protocol.
- **Impersonation attack:** There is a possibility that an adversary attempts to impersonate the MS but the impersonation of the MS will be declined because the HLR verifies whether MAC_1 is computed by the authorized MS or not. Moreover, an adversary needs to reply with a legitimate $A8(Nb)_{T_{key}}$, but he/she cannot compute the T_{key} . HLR assigns the T_{key} to the VLR as a temporary shared secret key between MS and VLR. If an adversary attempts to impersonate the VLR, the impersonation will fail as MS verifies whether VLR_C_i is computed by the legitimate VLR or not.
- **MiTM attack:** In the proposed protocol, bilateral authentication is established between communication entities that help resist the MiTM attack. The MS verifies VLR from received VLR_C_i . An adversary never computes the VLR_C_i unless he/she has the knowledge of K_i . On the other hand, the VLR verifies the MS received by SRES. Also, the SRES cannot be computed unless an adversary knows T_{key} . Since an adversary neither knows T_{key} nor the A5 algorithm, the eavesdropping of communication is not possible in the proposed protocol.
- **DoS attack:** In the proposed protocol, MS and network both use the timestamp as a counter. The value of the

counter is incremented each time whenever communication is carried out between them. With the help of counter value, one can easily identify the repeated request and ignore them. For each authentication process between the MS and network a unique RAND is used. The communication entities analyse the same information received by MS/network and reject the authentication request. Hence, the protocol avoids the DoS attack.

- **Redirection attack:** To preserve the integrity of the LAI, the proposed protocol needs to generate the message authentication codes ($MAC = A3(Na, LAI)_{K_i}$). It prevents the network from the redirection attack. Here, the MS associates the LAI of the BTS/BSS in MAC_1 and forwards it to the VLR. The HLR verifies the LAI transmitted by the VLR embedded in MAC_1 . If the match is not successful, HLR discards the authentication request.
- **Interleaving attack:** An intruder never succeeds in compromising the authentication information of the proposed protocol as integrity of the messages is maintained with MAC. In the proposed protocol, A5 algorithm is used to generate the cipher text from a particular plain text, which generates the different cipher texts. Hence, it is not possible to perform the chosen cipher-text attack and known plain-text attack in the proposed protocol.
- **Protection of signalling data:** There is a possibility of attack on the signalling messages transmitted in the communication network. In the proposed protocol, to protect the signalling messages from eavesdropping, the secure session key S_k is used between the communication entities. It also maintains the key secrecy and guarantees the freshness of keys used in the authentication process.

5. Performance analysis of the proposed ESAP-AKA protocol

The proposed ESAP-AKA protocol follows the network architecture of the existing GSM authentication protocol. As a result, the proposed protocol maintains integrity to be the same as the original GSM. The basic GSM authentication protocol requires producing n copies of

Table 4. The combinations of A3–A8 algorithm compiled by each communication entity in ESAP-AKA protocol.

Algorithm	Phase-1			Phase-2			Roaming phase		
	MS	VLR	HLR	MS	VLR	HLR	MS	VLR	HLR
A3	2	0	3	0	0	0	0	0	0
A8	2	2	0	2	2	0	2	2	0

authentication triplets. Hence, A3 needs to compile at least n times in the HLR. However, A3 needs to be executed only three times to generate the VLR_{Cert} and T_{key} in the ESAP-AKA protocol. Thus, the protocol needs to compile the security algorithms A3 and A8 for MS authentication. The number of combinations of A3–A8 algorithm executed by each communication entities is shown in table 4. In the proposed ESAP-AKA protocol, the HLR needs to execute A3 three times in phase-1. The computational overhead of the HLR is very less compared with existing protocols. Furthermore, the protocol need not generate a random token for each communication request as in [15]. Rather than generating a RAND for each communication request, VLR requires storing only the T_{key} and timestamp. Thus, the ESAP-AKA protocol is more efficient compared with existing authentication protocols for GSM network.

The authentication efficiency means the execution of authentication process by reducing the number of cryptographic functions executed and also minimizing the overhead from the communication entities without compromising the security. The authentication efficiency of proposed scheme is evaluated on the basis of the number of functions executed, the communication and computational overhead and the network signalling traffic in the communication network. To analyse the impact of the proposed protocol on traffic, a simple estimation model is employed [1, 7, 14, 26]. The model assumes that the mobility of MS is at an average velocity v with the direction of movement uniformly scattered over the interval $[0, 2\pi]$. Mobile users are systematically populated with the density ρ and the boundary of the registration coverage area is of length $L = 30.3$ km. The serving area (SA)/HLR contains 128 registration areas (RA)/VLR. The rate R of crossing RA is given by the relation

$$R = \frac{\rho \times v \times L}{\pi}.$$

The fluid flow mobility model is used with the following assumptions captured from actual GSM scenario to figure out the traffic involved in the authentication procedure:

- There is only one HLR for the entire network SA and every location area is served with one VLR.
- 128 RAs (128 VLRs).
- The size of RA = 57.4 km^2 .
- Border length $L = 30.3$ km.
- We assume a fluid flow with local balance within RAs, i.e., call origination rate = call termination rate = $1.4 / h$ / handset.

- Mean density of MS = $\rho = 390/\text{km}^2$.
- Average velocity of MS, $v = 5.6 \text{ km/h}$.
- Here, we assume a distinct velocity and call origination rate to conclude on its impact for an assessment of total network traffic.

The MS entering into a new RA generates the traffic as a result of registration process. In the reliable condition, the rate at which MS moves into the RA is equal to the rate at which MS moves out of that RA. Since every RA is controlled by one VLR, the rate of RA crossing is

$$R_{reg,RA} = \frac{390 \times 5.6 \times 30.3}{3600 \times \pi} = 5.85 \text{ per second.}$$

The rate of registration $R_{reg,RA}$ must be equal to the number of de-registrations (registration cancellations). Hence, $R_{de-reg,RA}$ is also 5.85 per second. The total number of registration messages arriving per second at the SA/HLR is equal to

$$R_{reg,SA} = R_{reg,RA} \times \text{total number of RA's per second.}$$

$$R_{reg,SA} = 5.85 \times 128 = 749 \text{ per second.}$$

We have 5.85 and 749/s authentication requests for every VLR and HLR, respectively. The total number of authentication requests as a result of call origination and call termination for the complete SA is computed as follows:

$$R_{callorig,SA} = \frac{\text{call origination rate} \times \rho \times 57.4 \times 128}{3600} \text{ per second.}$$

$$R_{callorig,SA} = \frac{1.4 \times 390 \times 57.4 \times 128}{3600} = 1114.32 \text{ per second.}$$

Similarly, the total number of authentication requests as a result of call termination will be 1114.32 per second. The number of calls originated per RA is

Table 5. The number of authentication requests generated per VLR and HLR.

Activity	VLR/s	HLR/s
Registration	5.85	749
Call origination	8.70	1114.32
Call termination	8.70	1114.32
Total/network	23.25	2977.64

Table 6. Number of control messages exchanged per authentication request in existing GSM-AKA and proposed ESAP-AKA protocols.

GSM-AKA protocols	Communication entities	Activity		
		Registration	Call origination	Call termination
Original GSM-AKA protocol	VLR	5	5	5
	HLR	4	4	4
	AuC	2	2	2
	Old VLR	1	0	0
Hahn <i>et al</i> [27] protocol	VLR	5	5	5
	HLR	4	0	0
	AuC	2	0	0
	Old VLR	1	0	0
Lee <i>et al</i> [16] protocol	VLR	5	1	1
	HLR	4	0	0
	AuC	2	0	0
	Old VLR	1	0	0
ESAP-AKA protocol	VLR	5	1	1
	HLR	4	0	0
	AuC	2	0	0
	Old VLR	1	0	0

Table 7. Total control signalling messages exchanged per authentication request in existing and proposed ESAP-AKA protocols.

GSM-AKA protocols	Communication entities	Activity			
		Registration	Call origination	Call termination	Total/network
Original GSM-AKA protocol	VLR	29.25	43.50	43.50	116.25
	HLR	2996	4457.28	4457.28	11910.56
Hahn <i>et al</i> [27] protocol	VLR	29.25	43.50	43.50	116.25
	HLR	2996	0	0	2996
Lee <i>et al</i> [16] protocol	VLR	29.25	8.70	8.70	46.65
	HLR	2996	0	0	2996
ESAP-AKA protocol	VLR	29.25	8.70	8.70	46.65
	HLR	2996	0	0	2996

Table 8. Comparative analysis of total network signalling traffic of existing and proposed ESAP-AKA protocols.

Communication entities	GSM-AKA protocol				% Improvement
	GSM	Hahn <i>et al</i> [27] protocol	Lee <i>et al</i> [16] protocol	ESAP-AKA	
VLR	116.25	116.25	46.65	46.65	60
HLR	11910.56	2996	2996	2996	75
Total signalling messages	12026.81	3112.25	3042.65	3042.65	75

$$R_{callorig.,RA} = \frac{1114.32}{128} = 8.70 \text{ per second.}$$

Similarly, the total number of calls terminated or delivered per RA will be equal to 8.70/s. The total number of authentication requests per VLR and HLR for each activity is shown in table 5.

In this paper, a performance analysis of the existing GSM-AKA and proposed ESAP-AKA protocol for roaming user in the communication network is carried out. All the

existing GSM-AKA protocols that do not support the roaming scenario are not considered in the comparative study of performance analysis. The number of control messages per authentication request for the registration, call origination and termination activities (figures 2 and 3) are shown in table 6. Table 7 shows the total number of signalling messages generated per VLR and HLR for each type of activity. For example, in the registration process there are 5.85/s authentication requests for the VLR and 749/s for the HLR. For each authentication request, there

are 5 messages handled by the VLR and 4 messages by the HLR as shown in figure 2. The total signalling messages for the registration activities for VLR and HLR is as follows:

$$VLR = 5.85 \times 5 = 29.25 \text{ signalling messages/s,}$$

$$HLR = 749 \times 4 = 2996 \text{ signalling messages/s.}$$

As illustrated in figures 4, 7 and 8, the ESAP-AKA protocol needs less number of control signalling messages in comparison with the existing GSM-AKA protocols. Only one signalling message is required to authenticate a subscriber provided that the subscriber halts in the RA for a long time (figure 7). The number of control signalling messages per authentication request for the registration, call origination and call termination activities are shown in table 6. Table 7 summarizes the total number of signalling messages for each VLR and HLR of the proposed protocol.

Table 8 summarizes the comparison between the GSM-AKA protocol and the proposed ESAP-AKA protocol in terms of total network signalling traffic. In the proposed protocol, the HLR of MS provides authorization to the visited VLR for the authentication of MS without knowing the secret key between MS and HLR. It reduces the authentication delay and the network signalling overload, which is proven through detailed performance analysis. The VLR has 116.25 signalling messages per second in the GSM protocol and 46.65 in the proposed protocol. In the GSM-AKA protocol, the HLR needs to handle around 11910 signalling messages per second. Moreover, only 2996 messages per second need to be handled by the HLR when the proposed protocol is executed. There is more than 60% improvement in the communication overhead required for the authentication process using the proposed protocol. Table 9 shows that the proposed protocol maintains the same level of improvement for varying velocity and call origination rate in terms of total network signalling messages compared with the conventional GSM approach. The proposed protocol generates the minimum communication overhead compared with that of existing GSM-AKA protocols.

In addition, a graph is presented to compare the total network signalling overhead of original GSM-AKA protocol and the proposed ESAP-AKA protocol as shown in figure 12. The graph is plotted among the call origination rate, velocity and the total signalling message overhead. It clearly shows that the proposed ESAP-AKA protocol reduces the signalling communication overhead as compared with the existing GSM-AKA protocol. Although Lee *et al* [16] and Hahn *et al* [27] protocols require equal amount of total network signalling communication overhead in the authentication process as that of the proposed protocol, they do not achieve all the identified objectives. Also, these protocols do not maintain a secure mechanism to transmit the network signalling message between the communication entities. Hence, there is a possibility of

Table 9. Network signalling traffic with varying velocity and call origination rate.

Mobility rate		GSM-AKA protocols											
		GSM			Hahn <i>et al</i> [27] protocol			Lee <i>et al</i> [16] protocol			ESAP-AKA		
Velocity (V)	Call origination rate	VLR	HLR	Total signalling message	VLR	HLR	Total signalling message	VLR	HLR	Total signalling message	VLR	HLR	Total signalling message
4.2	1.0	84.05	8615.20	8699.25	84.05	2248.00	2332.05	34.37	2247.68	2282.05	34.37	2247.68	2282.05
5.6	1.4	116.25	11910.56	12026.81	116.25	2997.28	3113.53	46.65	2996.00	3042.65	46.65	2996.00	3042.65
11.2	2.8	232.60	23819.60	24052.20	232.60	5990.40	6223.00	93.32	5990.40	6083.72	93.32	5990.40	6083.72
24.6	4.6	414.55	42454.32	42868.87	414.55	13166.76	13581.31	185.75	13163.52	13349.27	185.75	13163.52	13349.27
44.8	6.2	619.65	63455.84	64075.49	619.65	23976.96	24596.61	311.25	23976.96	24288.21	311.25	23976.96	24288.21

Figure 12. Signalling messages:existing GSM-AKA and proposed ESAP-AKA protocol.

eavesdropping the network signalling data. Hence, it is observed that the proposed ESAP-AKA protocol is significantly more secure and incurs less network signalling overhead than the existing protocols.

6. Conclusion

To improve the existing authentication protocols of the GSM network, many protocols were proposed but most of them modified the GSM architecture and did not address the roaming scenario. In this paper, we proposed an ESAP-AKA protocol for roaming users in the GSM network. The protocol achieves mutual authentication between communication entities and reduces the bandwidth consumption. It also minimizes the computational overload at HLR and the storage overhead at VLR. The ESAP-AKA protocol not only inherits the advantages of existing protocols but also offers an improved roaming service. The proposed protocol reduces more than 60% signalling congestion overhead as compared with other existing protocols for roaming users. Moreover, the proposed protocol avoids various attacks from the GSM network. It is expected that the proposed AKA protocol will strengthen the authentication process of roaming scenario in GSM network and can be applied to various mobile communication systems.

In the mobile communication network, whenever a group of mobile devices are moving, the authentication process of the protocol will face new security challenges. In this mobility scenario, a long delay and high computational overload is generated during handover. Therefore, the AKA protocol for the handover scenario in the mobile communication network will be further explored in future work.

Appendix I. HLP SL code defining the role of MS, VLR and HLR

See Figures 13, 14 and 15.

```

role ms (M, V, H:agent,
        SND, RCV: channel(dy), Key1, SK1: symmetric_key,
        Ti, Tmsi, Tmsi, Tkey : text, A3, A8: function)
played_by M
def=
  local
    State : nat,
    LAI : text

  const ms_vlr, vlr_hlr, hlr_ms, sec_key1 : protocol_id,
        success : text

  init State := 0
  transition
  1. State = 0 /\ RCV(start) =|>
    State' := 1 /\ LAI' := new()
    /\ SND (Tmsi.Ti.({A3(LAI'.Ti)}_Key1))
    /\ secret(Ti, Tmsi, sec_key1, {M, V, H})
    /\ witness(M, V, ms_vlr, LAI')

  2. State = 1 /\ RCV (({A8({A3({A3(LAI'.Ti)}_Key1)}_Key1).Ti})_Tkey).Ti) =|>
    State' := 2 /\ SND (A8({A3(Ti)}_Key1).Ti)
    /\ secret(Tkey, sec_key1, {M, V, H})
    /\ request(M, V, H, vlr_hlr, LAI')
    /\ witness(M, V, ms_vlr, LAI')

  3. State = 2 /\ RCV (success) =|>

  State' := 3
end role

```

Figure 13. Role of MS.

```

role vlr (V, H, M:agent,
        SND, RCV: channel(dy), Key1, SK1: symmetric_key,
        Ti, Tmsi, Tmsi, Tkey : text, A3, A8: function)
played_by V
def=
  local
    State : nat,
    LAI : text

  const ms_vlr, vlr_hlr, hlr_ms, sec_key1 : protocol_id,
        success : text
  init State := 0
  transition
  1. State = 0 /\ RCV (Tmsi.Ti.({A3(LAI'.Ti)}_Key1)) =|>
    State' := 1
    /\ SND (Tmsi.Ti. LAI'.({A3(LAI'.Ti)}_Key1))
    /\ secret(Ti, Tmsi, sec_key1, {V, H, M})
    /\ witness(V, H, vlr_hlr, LAI')
    /\ request (V, H, M, hlr_ms, LAI')

  2. State = 1 /\ RCV ((({A3(Ti)}_Key1).({A3({A3(LAI'.Ti)}_Key1)}_Key1)}_SK1).Ti) =|>
    State' := 2
    /\ SND ((({A8({A3({A3(LAI'.Ti)}_Key1)}_Key1).Ti})_Tkey).Ti)
    /\ secret(Tkey, sec_key1, {V, H, M})
    /\ witness(V, H, vlr_hlr, LAI')
    /\ request (V, H, M, ms_vlr, LAI')

  3. State = 2 /\ RCV (A8({A3(Ti)}_Key1).Ti) =|>
    State' := 3
    /\ SND(success)
    /\ request(V, H, M, vlr_hlr, LAI')

end role

```

Figure 14. Role of VLR.

```

role hlr (H, V, M:agent,
          SND, RCV: channel(dy), Key1, SK1: symmetric_key,
          Ti, Imsi, Tkey : text, A3, A8: function)

played_by H
def=
  local
    State :nat,
    LAI :text

  const ms_vlr, vlr_hlr, hlr_ms, sec_sk1 :protocol_id,
    success: text

  init State := 0
  transition

  1. State = 0 /\ RCV (Imsi.Ti. LAI'.({A3(LAI'.Ti)}_Key1)) =>

    State' := 1
    /\ SND ((({A3(Ti)}_Key1).({A3({A3(LAI'.Ti)}_Key1)}_SK1).Ti)
    /\ secret(Ti,Imsi,sec_sk1,{H,V,M})
    /\ request(H,V,vlr_hlr, LAI')
    /\ witness (H, V, hlr_ms, LAI')

end role

```

Figure 15. Role of HLR.

References

- [1] Al-Tawil K, Akrami A and Youssef H 1998 A new authentication protocol for gsm networks. In: *Proceedings of the 23rd Annual Conference on Local Computer Networks, LCN'98*, IEEE, pp. 21–30
- [2] Ammayappan K, Saxena A and Negi A 2006 Mutual authentication and key agreement based on elliptic curve cryptography for gsm. In: *Proceedings of the International Conference on Advanced Computing and Communications*
- [3] William S and Stallings W 2006 *Cryptography and network security*, 4th ed. Pearson Education India
- [4] Chaudhry S A, Naqvi H, Sher M, Farash M S and Hassan M U 2017 An improved and provably secure privacy preserving authentication protocol for SIP. *Peer-to-Peer Netw. Appl.* 10(1): 1–15
- [5] Saxena N and Chaudhari N S 2013 SAKA: a secure authentication and key agreement protocol for gsm networks, *CSI Trans. ICT* 1(4): 331–341
- [6] Hwang T and Gope P 2014 Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets. *Wireless Pers. Commun.* 77(1): 197–224
- [7] Degefa F B, Lee D, Kim J, Choi Y and Won D 2016 Performance and security enhanced authentication and key agreement protocol for sae/lte network. *Comput. Netw.* 94: 145–163
- [8] Tan H R, Lee C and Mok V 2007 Automatic power meter reading system using GSM network. In: *Proceedings of the International Power Engineering Conference, IPEC 2007*, IEEE, pp. 465–469
- [9] Nugra H, Abad A, Fuertes W, Galarraga F, Aules H, Villacis C and Toulkeridis T 2016 A low-cost IoT application for the urban traffic of vehicles, based on wireless sensors using GSM technology. In: *Proceedings of the 20th IEEE-ACM International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, IEEE, pp. 161–169
- [10] Wightwick A and Halak B 2016 Secure communication interface design for IoT applications using the GSM network. In: *Proceedings of the 59th IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, IEEE, pp. 1–4
- [11] Rahman A M, Hossain S, Tuku I J, Hossam-E-Haider M and Amin M S 2016 Feasibility study of GSM network for tracking low altitude helicopter. In: *Proceedings of the 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, IEEE, pp. 1–5
- [12] Lee C H, Hwang M S and Yang W P 1999 Enhanced privacy and authentication for the global system for mobile communications. *Wireless Netw.* 5(4): 231–243
- [13] Lo C C and Chen Y J 1999 A secure communication architecture for GSM networks. In: *Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, IEEE, pp. 221–224
- [14] Fanian A, Berenjkoub M and Gulliver T A 2009 A new mutual authentication protocol for GSM networks. In: *Proceedings of the Canadian Conference on Electrical and Computer Engineering, CCECE'09*, IEEE, pp. 798–803
- [15] Lee C C, Hwang M S and Yang W P 2003 Extension of authentication protocol for GSM. *IEEE Proc. Commun.* 150(2): 91–95
- [16] Lee C C, Liao I E and Hwang M S 2011 An efficient authentication protocol for mobile communications. *Telecommun. Syst.* 46(1): 31–41
- [17] Rappaport T S, et al 1996 *Wireless Communications: principles and practice*, vol. 2. New Jersey: Prentice-Hall-PTR
- [18] Zamzami A A, Devara E P, Pramana J, Sudarsono A and Zainudin A 2015 Reliability analysis of GSM network using software defined radio-based system. In: *Proceedings of the International Electronics Symposium (IES)*, IEEE, pp. 274–279
- [19] Chaudhry S A, Naqvi H, Farash M S, Shon T and Sher M 2015 An improved and robust biometrics-based three factor authentication scheme for multiserver environments. *J. Supercomput.* 1–17, <https://doi.org/10.1007/s11227-015-1601-y>
- [20] Ramadan M, Li F, Xu C X, Abdalla A and Abdalla H 2016 An efficient end-to-end mutual authentication scheme for 2G-GSM system. In: *Proceedings of the IEEE International Conference on Big Data Analysis (ICBDA)*, IEEE, pp. 1–6
- [21] Heydari M, Sadough S M S, Farash M S, Chaudhry S A and Mahmood K 2016 An efficient password-based authenticated key exchange protocol with provable security for mobile client–client networks. *Wireless Pers. Commun.* 88(2): 337–356
- [22] Memon I, Mohammed M R, Akhtar R, Memon H, Memon M H and Shaikh R A 2014 Design and implementation to authentication over a GSM system using certificate-less public key cryptography (cl-pkc). *Wireless Pers. Commun.* 79(1): 661–686

- [23] Chouhan A and Singh S 2015 Real time secure end to end communication over GSM network. In: *Proceedings of the International Conference on Energy Systems and Applications*, IEEE, pp. 663–668
- [24] Anwar N, Riadi I and Luthfi A 2016 Forensic SIM card cloning using authentication algorithm. *Int. J. Electron. Inf. Eng.* 4(2): 71–81
- [25] Chang C C, Lee J S and Chang Y F 2005 Efficient authentication protocols of GSM. *Comput. Commun.* 28(8): 921–928
- [26] Stach J F, Park E K and Makki K 1999 Performance of an enhanced GSM protocol supporting non-repudiation of service. *Comput. Commun.* 22(7): 675–680
- [27] Hahn G, Kwon T, Kim S and Song J 2004 Design and analysis of improved GSM authentication protocol for roaming users. *Netw. Parallel Comput.* In: *Proceedings of NPC 2004*, pp. 451–458
- [28] Kumari S, Chaudhry S A, Wu F, Li X, Farash M S and Khan M K 2017 An improved smart card based authentication scheme for session initiation protocol. *Peer-to-Peer Netw. Appl.* 10(1): 92–105
- [29] Lo C C and Chen Y J 1999 Secure communication mechanisms for GSM networks. *IEEE Trans. Consumer Electron.* 45(4): 1074–1080
- [30] Hwang M S, Lee C C and Lee J Z 2004 A new anonymous channel protocol in wireless communications. *Int. J. Electron. Commun.* 58(3): 218–222
- [31] Kumar K P, Shailaja G, Kavitha A and Saxena A 2006 Mutual authentication and key agreement for GSM. In: *Proceedings of the International Conference on Mobile Business, ICMB'06*, IEEE, pp. 25–25
- [32] Kalaichelvi V and Chandrasekaran R 2008 Secure authentication protocol for mobile. In: *Proceedings of the International Conference on Computing, Communication and Networking*
- [33] Southern E, Ouda A and Shami A 2011 Solutions to security issues with legacy integration of GSM into UMTS. In: *Proceedings of the International Conference on Internet Technology and Secured Transactions (ICITST)*, IEEE, pp. 614–619
- [34] Firoozjaei M D and Vahidi J 2012 Implementing geo-encryption in GSM cellular network. In: *Proceedings of the 9th International Conference on Communications (COMM)*, IEEE, pp. 299–302
- [35] Fanian A, Berenjkoub M and Gulliver T A 2012 A symmetric polynomial-based mutual authentication protocol for GSM networks. *Int. J. Security Netw.* 7(3): 161–173
- [36] Mehrotra A and Golding L S 1998 Mobility and security management in the GSM system and some proposed future improvements. *Proc. IEEE* 86(7): 1480–1497
- [37] Ghosh R 2017 *Wireless networking and mobile data management*, pp. 1–546
- [38] Huang J L, Yeh L Y and Chien H Y 2011 ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* 60(1): 248–262
- [39] Lin X, Sun X, Ho P H and Shen X 2007 GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Trans Veh. Technol.* 56(6): 3442–3456
- [40] Burrows M, Abadi M and Needham R M 1989 A logic of authentication *Proc. R. Soc. London A: Math. Phys. Eng. Sci.* 426: 233–271
- [41] Burrows M, Abadi M and Needham R 1988 Authentication: a practical study in belief and action. In: *Proceedings of the 2nd Conference on Theoretical Aspects of Reasoning About Knowledge*, Morgan Kaufmann Publishers Inc., pp. 325–342
- [42] Gaarder K and Sneekenes E 1990 On the formal analysis of PKCS authentication protocols. In: *Proceedings of the Advances in Cryptology, AUSCRYPT'90*. Berlin, Heidelberg: Springer, pp. 105–121
- [43] Kytäjä T 1995 A logic of authentication by Burrows, Abadi and Needham. Tehran: Helsinki University of Technology, <http://www.tml.tkk.fi/Opinnot/Tik-110.501/1995/ban.html>
- [44] Ou H H, Hwang M S and Jan J K 2010 A cocktail protocol with the authentication and key agreement on the UMTS. *J. Syst. Softw.* 83(2): 316–325
- [45] Saxena N, Thomas J and Chaudhari N S 2015 ES-AKA: an efficient and secure authentication and key agreement protocol for UMTS networks. *Wireless Pers. Commun.* 84(3): 1981–2012
- [46] Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuéllar J, Drielsma P H, Héam P C, Kouchnarenko O, Mantovani J, et al 2005 The AVISPA tool for the automated validation of internet security protocols and applications. In: *Proceedings of the International Conference on Computer Aided Verification*. Berlin, Heidelberg: Springer, pp. 281–285
- [47] AVISPA 2003 Automated validation of internet security protocols, <http://www.avispa-project.org>
- [48] Lai C, Li H, Li X and Cao J 2015 A novel group access authentication and key agreement protocol for machine-type communication. *Trans. Emerg. Telecommun. Technol.* 26(3): 414–431
- [49] Jiang R, Lai C, Luo J, Wang X and Wang H 2013 EAP-based group authentication and key agreement protocol for machine-type communications. *Int J. Distrib. Sens. Netw.* 2013: <https://doi.org/10.1155/2013/304601>
- [50] Lai C, Li H, Lu R and Shen X S 2013 SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks. *Comput. Netw.* 57(17): 3492–3510