SAKA: a secure authentication and key agreement protocol for GSM networks

Neetesh Saxena · Narendra S. Chaudhari

Received: 17 July 2013 / Accepted: 20 October 2013 / Published online: 21 November 2013
© CSI Publications 2013

Abstract Although nowadays we are running in the 3rd generation of cellular networks but most of the service providers are also providing the services of 2nd generation cellular networks. The Global System for Mobile Communication (GSM) protocol is proposed to solve the security issues and vulnerabilities found in first generation of cellular communication which was based on analog communication system. GSM system is still vulnerable to redirection attack, man-in-the-middle attack and impersonation attack. An intruder can apply these attacks to impersonate the network or bill mischarge the users. In this paper, we propose a new secure GSM protocol called “SAKA” to prevent GSM networks from various security issues and attacks. This proposed protocol improves the drawbacks of the original GSM authentication protocol including: not supporting mutual authentication; large bandwidth consumption between VLR and HLR; storage space overhead in VLR; and overloaded HLR with authentication of mobile stations. This protocol also eliminates the need of synchronization between a mobile station MS and its home network HLR. The SAKA protocol generates minimum communication overhead as compare to all other existing and proposed GSM protocols. Authors claim that on an average the SAKA protocol has reduced 56 % of the bandwidth consumption during the authentication process which is the maximum reduction of bandwidth by any GSM protocol.

Keywords GSM · Bandwidth · Man-in-the-middle attack · Replay attack · Impersonation attack

1 Introduction

Security issues were not properly addressed in the first generation (1G) analog systems. An intruder can eavesdrop user traffic or even change the identity of mobile phones to gain the unauthorized service with the equipments available in the market. Given this background, security measures were taken into account in the design of second-generation (2G) digital cellular systems. The Global System for Mobile Communications (GSM) was designed from the very beginning to resolve the security issues and has adopted several schemes to provide the authentication and data confidentiality to the subscribers. To prevent the fraudulent use, the GSM network normally authenticates the identity of a subscriber through a challenge-response scheme where the subscriber proves its identity by providing a response to a challenge with time constraint asked by the network. When the user roams into a foreign network, the home network transfers a set of authentication data (called triplets) to the foreign network. Based on each triplet, the foreign network can authenticate the subscriber without the involvement of the home network [1].

However, the weaknesses of the GSM challenge response scheme have been uncovered over time in [2–4] where the authentication is only unidirectional and the subscriber cannot authenticate the serving network. The lack of authentication of serving network allows the redirection or false base station attack [5]. Furthermore, the triplets generated at HLR (home location register) can be reused indefinitely. There is no evidence which ensures to the user that authentication information and cipher keys are

N. Saxena (✉) · N. S. Chaudhari
Indian Institute of Technology Indore, Indore, India
e-mail: neetesh.saxena@gmail.com

N. S. Chaudhari
e-mail: narendra@iiti.ac.in

not being reused. It also allows an adversary to use the authentication tokens corrupted from one network to impersonate other networks [1].

1.1 Limitations of existing GSM protocols

Several drawbacks related to security and performance issues have been found in the original GSM authentication protocol, which are as follows:

1. Mutual authentication between mobile station (MS) and visitor location register (VLR) is not provided in the original GSM architecture. Only VLR authenticates the MS, but the VLR is not authenticated by the MS.
2. When the MS is in the foreign network, there are 'n' copies of triplet authenticating tokens transmit from HLR to VLR which normally store in VLR's database. This approach generates a huge storage space overhead.
3. If any MS resides in a VLR for long time duration and consumes all the available authenticating tokens, the VLR will request the HLR again to send 'n' copies of next authenticating tokens. Additionally, it may be the case for the MS to move frequently from one foreign network to another in a short span of time. Then in such cases, each VLR will request the HLR to send 'n' copies of triplet authentication tokens which then results in the huge bandwidth consumption between VLR's and HLR.
4. The HLR is also overloaded with authentication of mobile stations because all triplets are generated at HLR;
5. Problem of synchronization between mobile station MS and its home network HLR;

The readers please note that the authentication is required at the time of connection establishment as well as when the connection is required to release. Since a mobile subscriber is charges after every connection, the base station should be able to provide him the required services efficiently. It is also required to prevent the MS from repudiation attack and furthermore, the integrity of the service request message should be preserved. The security architecture of the GSM consists of three tiers. In the first tier, the A3 algorithm uses the challenge response scheme for user authentication. In the second tier, the A8 algorithm uses the output from the A3 algorithm to generate the key. In the last and third tier, the A5 algorithm uses an algorithm for message encryption/decryption which varies according to the mobile operators. However, this architecture has some problems which are as follows: challenge-response is a

simple authentication method, but doesn't seem to be very secure. Additionally, the length of the key generated by the A8 algorithm is fixed so the key might be disclosed by the analysis. As the A3, A8 and A5 algorithms are proprietary, thus their security can't be easily verified. The user authentication depends on a shared secret key between SIM card (mobile station) and the HLR called Ki. This secret key is embedded into the SIM card at the time of manufacturing, which is also securely copied into the HLR/AuC.

The ciphering key generating algorithm A8 is used to produce the 64-bit ciphering key (KC). The ciphering key (KC) is used to encrypt and decrypt the data between the MS and the BTS by the use of the encryption algorithm A5 [6, 7]. This encryption provides the data confidentiality but not the total security solution because only cipher cannot provide the data integrity and non-repudiation. Hence, the digital signal concept may be incorporated along with ciphering [8]. The A5 algorithm includes A5/1 and A5/2 variant algorithms. A5/1 [9] was commonly used in western countries and was deemed strong encryption [10] but it was reverse engineered some time ago and proved vulnerable. A5/2 [11] has been cracked by Wagner and Goldberg, used the methodology which required five clock cycles and made A5/2 almost useless. All these problems with the A5 encryption algorithms prove that eavesdropping between mobile station MS and BSS is still possible. Thus, there is a need to investigate these algorithms and results in a secure GSM architecture.

1.2 Our contribution

In this paper, we propose a new AKA protocol named SAKA (Secure Authentication and Key Agreement Protocol) for the GSM network. The highlights of the proposed SAKA protocol are as follows:

1. The SAKA protocol eliminates the security and performance issues listed in points 1–4 (above subsection).
2. This protocol also eliminates the need of synchronization between the MS and its HLR.
3. The SAKA protocol generates minimum communication overhead as compare to all other existing and proposed GSM protocols.
4. On an average the SAKA protocol reduces 56 % of the bandwidth consumption in the authentication process which is the maximum reduction of bandwidth by any GSM protocol found in the literature.

The only drawback is that the generated computation overhead by SAKA protocol is only better than [20] compared with all the existing protocols discussed in the paper.

Table 1 Symbols and abbreviation

Symbol	Definition	Bits
IMSI	International mobile subscriber identity	128
Service request	location update request/call attempt	8
User profile	User mobile number/reference number	40
VLR_ID	Identification of VLR	28
Count	Integer number	24
KC	Temporary session key	64
LAI	Location area identity	40
VLR_C	Certificate of VLR	Variable
Ki	Secret key shared b/w MS and HLR	128
DK/TK	Delegation key/shared secret key b/w MS and VLR	128
SK	Session key	128
RAND	Random number	128
MAC	Message authentication code	64
SRES/AUTR/AUTHR	Signed results	32
T	Timestamp	64

1.3 Organization of paper

This paper is organized into five Sections. Section 2 represents the review of various GSM protocols. Section 3 states a proposed protocol called SAKA for GSM networks. Section 4 describes the security analysis of the proposed protocol with respect to various issues and prevention from various attacks. Finally, Section 5 summarizes the conclusion of this work.

2 Review of GSM protocols

This section represents the review of various proposed GSM protocols with respect to their architecture and their issues. Many authentication protocols have been proposed to improve the existing GSM authentication protocol. However, most of them couldn't solve all the drawbacks mentioned in Sect. 1 and some of them even change the architecture of the original GSM. In this subsection, we define the symbols and abbreviation used with their sizes in Table 1. Next, Table 2 lists various cryptographic algorithms and their roles. In the year of 1999, Lo and Chen [12, 13] proposed a secure communication protocol for GSM which was more secure than the existing GSM. However, the architecture proposed in these papers were changed and based on public-key cryptography. Unfortunately this protocol couldn't solve the drawbacks discussed in Sect. 1. Afterward, Lee et al. [3] proposed an enhanced privacy and authentication method for GSM that can solve

Table 2 Cryptographic algorithms

Functions	Definition
A3	Authentication algorithm
A8	Key agreement algorithm
A5	Specified for data encryption and decryption
	Concatenation

some drawbacks. Now, we have a brief look of recent technological advancement in GSM architecture and its networks. In [14], a new location depended key generation management mechanism is introduced, and its applicability in GSM is evaluated. Here, authors have used MS's location information to generate this key by geo-encryption algorithm idea. Encrypted data only in the MS's location, that just GSM network is aware of it, can be decrypted and its accuracy depends on used positioning algorithm. The paper [15] proposed an idea about catching the GSM/UMTS Phone Number over the air by man-in-the-middle attack. Unlike other terminal detectors or interceptors which only can catch the IMSI/IMEI of the phone number, this concept do the phone number catching by a man in-the-middle attack between the victim's mobile station and the operator's GSM network. Authors proposed a novel mutual entity authentication using the TESLA protocol in [16]. The proposed solution not only provides secure bilateral authentication, but also decreases the call setup time and the required connection bandwidth.

The paper [17] proposes simple and effective solutions to reduce the possible attacks on the UMTS systems due to the integration with GSM. First authors propose a subtle modification to the GSM security protocols as a standalone solution, and then a modification to the UMTS security protocols is proposed as a second solution. In [18], authors propose a new approach to mutual entity authentication based on symmetric polynomials. In the proposed protocol, each MS is allocated a share of the symmetric polynomial during initial authentication and in subsequent authentication requests the MS and VLR authenticate each other using the polynomial share. Authors claim that the proposed solution not only provides secure bilateral authentication, but also decreases the memory overhead in the VLR and the required connection bandwidth. However, using the TESLA protocol in the proposed mutual authentication protocol does increase memory usage and processing time in the MS. Unfortunately, all these recent protocols have proposed with change in GSM architecture. Next, we have some old proposed protocols based on the GSM architecture. Lee et al. [19] proposed a mutual authentication technique for the GSM network. The main idea is that the HLR issues a ticket for the new VLR the first time the MS is authenticated in a new location. The VLR and MS

authenticate each other using the ticket without any need to refer to the HLR. Detailed analysis shows that this technique only works correctly for the first MS authentication, and cannot subsequently verify the network [20]. Chang et al. [20] developed a modified version of the approach in [19] which overcomes this security flaw. After the MS joins a new visiting area, in the MS request, a timestamp is added to the initial message. After obtaining the corresponding IMSI from the received TMSI, the new VLR forwards the MS request to the HLR. Afterwards, to authenticate the VLR by the MS, the HLR generates a certificate for the VLR. The HLR also generates a random number and a secret key for future MS authentication. The secret key must be of at least 64 bits because an adversary can easily compromise the 32 bit secret key simply by listening to the wireless channel and using brute force attack [21].

2.1 Review of original authentication protocol for GSM

The security of GSM is based on algorithms A3, A5 and A8. The outputs of SRES and KC are computed, using Ki, and RAND through algorithms A3 and A8 as inputs respectively, where Ki, is the mobile station's secret key shared between the mobile station and the home system (HLR) and saved in the SIM card, and RAND is generated by HLR. SRES is a certificate or signed result to authenticate mobile stations and Ki is the session key between mobile stations and HLR. An algorithm A5 is used to encrypt/decrypt the transmitted messages with confidentiality. Here, an overview of the original GSM authentication protocol is summarized as follows:

While MS moves into a new visiting network and asks for new communication service, an authentication request is sent to VLR first, where the request includes TMSI and LAI. After receiving the request, the new VLR uses the received TMSI to get the IMSI from the old VLR and then sends IMSI to HLR. Then, HLR generates n distinct sets of authenticating parameters $\{SRES_i, RAND_i, KC_i\}$ and sends them to VLR. After receiving those sets of authenticating parameters, VLR keeps them in its own database and selects one set of them to authenticate the mobile station for each call. Next, VLR sends the selected $RAND_i$ to MS. Once MS receives $RAND_i$ from VLR, it computes $SRES' = A3(RAND_i, Ki)$ and the temporary session key $KC' = A8(RAND_i, Ki)$, respectively, where KC' is kept secret for communication. Then the $SRES'$ is sent back to VLR. Upon receiving $SRES'$ from MS, VLR compares it with the selected SRES kept in its own database. If they are not the same, the authentication is failure; otherwise, VLR can make sure that MS is legal. Harn and Lin's approach [2] eliminated the stored information in VLR and stores

only the one-way result. This modification also reduces the amount of information to some extents. Nonetheless, the overhead occurs in the computation of $f^n(SRES)$ and $g^{n-1}(KC)$ by each subscriber in each session is huge. The Lee et al. illustrate the approach described in [3]. The parameters are transmitted from HLR to VLR in an encrypted mode that protects the signaling data from eavesdropping. Furthermore, the authentication of MS is done by VLR itself, and no more aid from HLR is required. This eliminates the bandwidth consumption for transmitting the authentication parameters.

Lee et al. [19] proposed a new authentication protocol in which the HLR makes the visiting VLR and MS share a temporary secret key TKi which is computed through A3 by HLR using Ki and RAND as the inputs. In addition, the HLR also computes the certificate $VLR_Ci = A3(T, Ki)$ for the visiting VLR of MS which then is used for authenticating the validity of VLR. Another protocol had presented by Chang et al. [20] and can be divided into two phases. The first phase is the authentication in the visiting VLR which generates $(T||RAND)$ instead of RAND as the inputs through A5 to compute the authentication pattern SRES. Second phase is ith authentication between the same visiting VLR and the MS in order to achieve the goal of mutual authentication anytime. Different from Phase 1, the signed result $SRES_i$ is computed by using $(Ti||Ti)$ and TK as the inputs through A5. Al-Tawil et al. [22] are interested in reducing the authentication delay and the network signaling overhead by reducing the number of messages which lead to decreasing the call setup time without compromising GSM security. However, unfortunately the original GSM protocol even doesn't have sufficient security. Note: 'count' is sent from the HLR to the AuC. Computations take place at the AuC and results return to HLR. Although the sizes of some parameters are mentioned in the paper by Khalid et al. but we have considered all the parameters used in this paper as globally for all proposed and existing GSM protocols. We assumed the user profile as user mobile number/reference number which is a 10 digit number (between 0 and 9 numbers in each and is of 40 bits in size). Authors of [13] and [23] proposed the changed architecture of GSM system. For this reason, we have not included these two protocols while calculating the computation and communication overheads.

2.2 Attack model

This subsection reviews the security analysis of GSM protocol by considering the various attacks in this network scenario like replay attack, impersonation attack, man-in-the-middle attack and redirection attack.

2.2.1 Replay attack

An intruder delays the transmitted packet or later can misuse the captured information by retransmitting the message to the original destination. This attack is applied to gain access to resources by replaying an authentication message.

2.2.2 Impersonation attack

In this attack, the intruder eavesdrops signaling and data connections associated with other users. Moreover, in the impersonation of a user, the intruder sends signaling and/or user data to the network, in order to make the network believe that originate from the authentic user. Additionally, impersonation of the network is the capability whereby the intruder sends signaling and/or user data to the target user, in order to make the target user believe that originate from a genuine network.

2.2.3 Man-in-the-middle attack

In the Man-in-the-middle attack, the adversary or the intruder puts itself in between the target user and a genuine network and can capture, modify, eavesdrop, and spoof signaling and data exchanged between the both the parties. Nowadays, due to access availability of phone number catcher in the market, it becomes easy to catch the GSM/UMTS phone number over the air by this attack.

2.2.4 Compromising authentication information in the network

The adversary possesses compromised authentication information, which may include challenge and response pairs. The adversary can obtain the necessary information by compromising network nodes or by intercepting signaling messages on network links.

2.2.5 Redirection attack

These attacks can be easily launched with fake BTS equipments. A fake BTS equipment is normally located in a bounded area that can act as a real BTS functions and broadcast the BTS signal over the air to the mobile phones. As the 2G communication system only provides unilateral authentication mechanism which authenticates the identity of a mobile user. Earlier, developing a BTS device was often a costly business, while only the government can have such devices for the security purposes.

Normally the encryption of data doesn't need in every network, while the integrity of data is mandatory in all networks. The adversary may redirect the user traffic to a

network in which the ciphering of data is not provided or provided very limited. The redirection attack causes the billing problem while the user is in their home network and charged as visitor at a foreign network on a higher rate. However, all the attacks described above can only catch the IMSI, IMEI or TMSI over the air. So for the individual privacy protection, the phone numbers of the users are stored in operator's core network. The MSC or HLR/VLR in the core network will translate the IMSI/IMEI to the phone number.

3 SAKA: proposed AKA protocol for GSM

To resolve the security issues associated with GSM authentication protocol, we propose and present a new authentication and key agreement protocol, called SAKA, which can prevent the GSM network from various attacks like redirection attack, replay attack, man-in-the-middle attack, and impersonation attack. This SAKA protocol strictly follows the framework of the original GSM architecture protocol and solves the problem of synchronization between the mobile station MS and home network HLR. In SAKA protocol, each MS and its HLR share a secret authentication key K_i . Some cryptographic algorithms A3, A8 and A5 used in this protocol are same as in the original GSM protocol. A3 algorithm is shared between MS and HLR while A8 and A5 algorithms are shared between MS and VLR. The cryptographic algorithms A3, A8 and A5 have already been proved as weak algorithms exist in the original GSM architecture. Thus, there is a strongly need to replace these algorithms with new secure algorithms. A3 and A8 algorithm can be replaced by a strong hash or MAC functions (like SHA or HMAC) while A5 algorithm is replaced by a variant of symmetric key algorithm (like AES or Blowfish); however details of these new algorithms are out of the scope of this paper. Here, we assume that all three A3, A8 and A5 algorithms are secure enough and are very difficult to break. This SAKA protocol is shown in the Fig. 1 which is described as follows:

In step 1, mobile station MS makes a request to VLR to create a connection for authentication by sending IMSI, a timestamp T_1 and a calculated MAC_1 to VLR where $MAC_1 = A_3(T_1 || LAI, K_i)$, and K_i is the secret key shared between MS and HLR. VLR passes IMSI, T_1 , MAC_1 and LAI to the home network HLR where LAI is the location area identity of MS, as VLR knows the location of MS and sends this information to HLR. After receiving such information HLR calculates MAC_1' ($MAC_1' = A_3(T_1 || LAI, K_i)$) and compare it with the received MAC_1 . If both are equal then MS is a legitimate user. HLR generates DK and VLR_C. Now, HLR passes DK and VLR_C to VLR.

Fig. 1 Proposed SAKA authentication protocol

VLR maintains a counter ‘count’ which gets incremented after every transmission of VLR_Ci to MS which consists of MAC2 and count. Please note, it doesn’t require synchronization at both ends because count increment is only used to generate a unique number, every time is sent from VLR to the MS. These MAC2 and count are updated and calculated every time an authentication is requested by MS. After receiving the VLR_Ci, MS verify ‘count’. If the received count is greater than the previous count then MS calculates MAC2’ and compare it with the received MAC2 otherwise request is discarded and connection is terminated. Now, MS generates DK and compute SRES. MS sends this SRES to VLR. VLR calculates SRES’ and compare it with the received SRES. If SRES’ and SRES are equal then authentication is successful otherwise terminates the connection. Afterwards, the message information is encrypted using the A5 algorithm and the communication between the MS and the VLR takes place.

4 Security analysis of the proposed protocol

4.1 Mutual authentication between MS and HLR/VLR

In the SAKA protocol, the HLR authenticates the MS by verifying MAC1. To authenticate the HLR, the MS checks the received VLR_Ci. The MS can acquire the expected authentication codes of the VLR as MAC2’ where $MAC2' = A8(VLR_C || count, DK)$. If MAC2’ is equal to MAC2, both HLR and VLR are authenticated and this ensures the mutual authentication between the MS and the HLR. For subsequent authentications, even it may be the case where HLR is not involved; the MS can still authenticate the HLR with the involvement of DK. Next, the VLR authenticates the MS by verifying SRES. After receiving the message, VLR calculates SRES’ and checks whether $SRES = SRES'$ where $SRES' = A8(count, DK)$. The MS is verified authenticated if this equality holds. The same

procedure takes place in authenticating the MS when the VLR receives SRES while communicating with only VLR. Now, on receiving MAC2, the MS computes MAC2’ to authenticate the VLR if $MAC2 = MAC2'$ holds. This all ensures the mutual authentication between the MS and HLR/VLR.

4.2 Resistance to attacks

In this subsection, we justify that the proposed SAKA protocol is free from various attacks.

4.2.1 Replay attack

To detect such an attack, unique random numbers are often used to prevent the system from replayed message attack. Sequence number, timestamp, and the challenge response are three different types of random number or nonce. However, each one of it has its own boundaries to use. The SAKA protocol is free from this attack by sending timestamp T1 and counter ‘count’ with the information while the transmitting the information over the network.

4.2.2 Impersonation attack

In the original GSM protocol, the corruption of a network VLR/HLR affects the security of whole system. In this subsection we discuss the impact of network corruption on SAKA protocol. There are two possible cases for communication between MS and VLR/HLR and each of which is described as follows:

4.2.2.1 When the adversary tries to impersonate the MS

At the beginning of the SAKA protocol, MAC1 is computed at MS and has sent to the HLR. The HLR then compute MAC1’ through A3 by passing the inputs timestamp T1, and location area identity LAI of MS (notified and sent by VLR to HLR) with the key Ki. Additionally, if

the adversary is able to eavesdrop all the messages that can be sent to the other network then the adversary must reply with a valid response SRES to VLR in order to impersonate MS. However, the adversary can't obtain correct SRES.

4.2.2.2 The adversary tries to impersonate the VLR If the adversary tries to impersonate the VLR, the attempt to impersonate the VLR will be failed as the MS can verify that the authentication was not requested by VLR (if MS receives the VLR_Ci at any point of time while previously MS has not sent any request to VLR). Thus, the impact of network corruption in terms of impersonation is drastically reduced with SAKA protocol compare to original GSM protocol.

4.2.3 Man-in-the-middle attack

A man-in-the-middle attack can occur when a MS try to connect to a BTS/BSS. In the SAKA protocol, a new algorithm of A5 is conversed between MS and VLR. The message contents are encrypted with key DK through A5 algorithm. Thus this system prevents the communication from being eavesdropped.

4.2.4 Redirection attack

In the original GSM protocol, the location of the BTS/BSS (LAI) is not protected and can be changed by an adversary with some redirection attack. The SAKA protocol uses message authentication codes (MACs) to maintain the integrity of LAI. This concept thereby prevents the network from the redirection attack. This attack is easily possible when the adversary gets the correct user's MS information. In SAKA protocol, the MS involves the LAI of the BTS/BSS in MAC1 and transmits MAC1 to the VLR. The authentication request is discarded when the HLR fails to match the LAI sent by the VLR and embedded in MAC1. Such a technique solves the mischarged billing also.

4.2.5 Compromising authentication information in the network

The adversary can not compromise the authentication information in the proposed protocol. The adversary can not obtain any information because the integrity is properly maintained in the proposed protocol.

4.3 Performance analysis

This subsection provides the performance analysis of new proposed SAKA protocol in terms of VLR storage overhead, reduction in bandwidth consumption, and the efficiency of the new system with respect to the various parameters.

4.3.1 The VLR storage overhead

Obviously, VLR only needs to store DK and count in its database instead of 'n' sets of the authentication parameters {SRES, RAND, KC}n. Therefore, the proposed SAKA protocol is certainly uses less memory space of VLR as compare to the original GSM.

4.3.2 Bandwidth consumption between HLR and VLR

Instead of generating 'n' sets of the authentication parameters for VLR to authenticate MS, HLR computes a session delegation key DK and sends it to VLR. Therefore, VLR can use DK to compute the signed result to authenticate MS when MS sends the authentication request. Thus, the SAKA proposed scheme can greatly reduce the bandwidth consumption between HLR and VLR.

4.3.3 Efficiency of SAKA protocol

Since the original GSM authentication protocol needs to generate 'n' copies of the authentication parameters, A3 has to be execute at least 'n' times in HLR. Thus, the proposed protocol SAKA is more efficient than the current GSM authentication protocol. Furthermore, instead of generating a random number for each communication request, VLR only needs to keep a key DK and counter 'count' which feed as the inputs through A8 to compute SRES.

A comparison among various existing GSM protocols along with new proposed protocol SAKA is shown in the Table 3. The table summarized the same in terms of the computation overhead, total storage at VLR and the communication overheads. The storage space used by SAKA is S (DK, count). The computation overhead is slightly more in SAKA but the communication overheads has drastically reduced in the SAKA protocol as compared to the other mentioned protocol according to the Table 3. Table 4 represents the requirements to solve the issues of GSM networks with respect to various protocols. Some of these requirements are MAUTH: Mutual Authentication, SSVLR: Solve problem of space overhead at VLR, SBWC: Solve problem of bandwidth consumption, CGSMA: Change in GSM Architecture, and AVLRL: Authentication of MS by VLR instead of HLR. Here, we can clearly see that SAKA protocol fulfills all such requirements of GSM network. Next, Table 5 describes the prevention of GSM network from various attacks like replay attack, man-in-the-middle attack, redirection attack and impersonation attack. The SAKA protocol can prevent the GSM network from all these attacks successfully. The bandwidth consumed during the authentication process by the original GSM protocol and the new SAKA protocol is computed in

Table 3 Comparisons of authentication protocols

	Original GSM	[2]	[3]	[20]	[19]	[22]	Proposed SAKA
Computation overhead	2nT(A3)	$\left(n + \sum_{j=1}^{n-1} T(f)\right)$	2T(A3) + 2nT(A5)	$(4 + 2n)T(A3) + (2 + 2n)T(A5)$	2T(A3) + 2nT(A5)	2T(A3) + 2T(A8) + 2nT(A5)	6T(A3) + 4nT(A8)
Total storage (VLR)	nS(SRES)	$S(j^{n-1}/(SRES))$	S(TKi)	S(Ti-1, TK)	S(TKi)	S(KC, user profile)	S(DK, count)
Communication overhead	296 + 512 × n	448 + 320 × n	512 + 384 × n	1082 + 384 × n	708 + 448 × n	888 + 384 × n	784 + 176 × n

the Table 6. On an average the SAKA protocol shows 56 % reduction in bandwidth consumption as compared to the GSM protocol when $n = 5, 10, 50$, and 100 .

4.4 Formal proof of proposed SAKA protocol

In order to clear statement of our analysis, we use the BAN-Logic symbols to formally proof the authentication process of the proposed protocol.

1. $P| \equiv X$: P believes X, or P would be entitled to believe X.
2. $P \triangleleft X$: P sees X. Someone has sent a message containing X to P, who can read and repeat X.
3. $P| \sim X$: P once said X. P at some time sent a message including the statement X.
4. $P| \Rightarrow X$: P has jurisdiction over X. P is an authority on X and should be trusted on this matter.
5. $\#(X)$: The formula X is fresh, that is, X has not been sent in a message at any time before the current run of the protocol.
6. $P \stackrel{K}{\leftrightarrow} Q$: P and Q may use the shared key K to communicate.
7. $P \stackrel{X}{\leftrightarrow} Q$: The formula X is a secret known only to P and Q.
8. $(X)_y$: This represents X combined with the formula Y that Y be a secret.

4.4.1 The formally messages in SAKA protocols

Message (1): $MS \rightarrow VLR : Na, A3(Na, LAI)_{Ki}, MS \stackrel{Ki}{\leftrightarrow} HLR$

Message (2): $VLR \rightarrow HLR : Na, A3(Na, LAI)_{Ki}$

Message (3): $HLR \rightarrow VLR : A3(Na)_{Ki}, VLR \stackrel{DK}{\leftrightarrow} HLR, A3(A3(Na, LAI)_{Ki})_{Ki}$

Message (4): $VLR \rightarrow MS : Nb, A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}$

Message (5): $MS \rightarrow VLR : A3(Na)_{Ki}, A8(Nb)_{DK}$

4.4.2 Security assumptions

- a. It is assumed that K_i is a secure key which is shared between the MS and its HLR.

1. MS has the secure key K_i and $MS| \equiv MS \stackrel{Ki}{\leftrightarrow} HLR$
2. HLR has the secure key K_i and $HLR| \equiv MS \stackrel{Ki}{\leftrightarrow} HLR$

- b. It is assumed that VLR trusts the HLR.

1. $VLR| \equiv HLR| \Rightarrow MS \stackrel{Ki}{\leftrightarrow} HLR$

Table 4 Comparisons of GSM authentication protocols versus requirements

	Original GSM	[3]	[19]	[2]	[22]	[13]	[23]	[20]	Proposed SAKA
MAUTH	N	N	Y	N	N	Y	Y	Y	Y
AVLR	N	Y	Y	N	N	N	N	Y	Y
SSVLR	N	Y	Y	N	N	N	N	Y	Y
SBWC	N	Y	Y	Y	Y	N	N	Y	Y
CGSMA	–	N	N	Y	Y	Y	Y	N	N

Table 5 Prevention from various attacks

Protocol attacks	Original GSM protocol	SAKA protocol
Replay attack	Y	Y
Man-in-the-middle attack	N	Y
Redirection attack	N	Y
Impersonation attack	N	Y

2. $\frac{VLR| \sim P, HLR \triangleleft P}{HLR| \equiv VLR \equiv P}$
3. $\frac{HLR| \sim P, VLR \triangleleft P}{VLR| \equiv HLR \equiv P}$

c. It is assumed that communication between the HLR and the VLR is secure.

1. $VLR| \equiv VLR \xrightarrow{P} HLR$, P is conveyance message between VLR and HLR.
2. $HLR| \equiv VLR \xrightarrow{P} HLR$, P is conveyance message between VLR and HLR.

4.4.3 Security analysis

1. $MS \rightarrow VLR : MS| \equiv \#(Na) \wedge VLR| \equiv \#(Na); VLR \triangleleft Na, A3(Na, LAI)_{Ki}$
2. $VLR \rightarrow HLR : HLR \triangleleft Na, LAI, A3(Na, LAI)_{Ki}$, on receiving check $A3(Na, LAI)_{Ki}$

3. $HLR \rightarrow VLR : VLR \triangleleft A3(A3(Na, LAI)_{Ki})_{Ki}, A3(Na, LAI)_{Ki}, HLR| \equiv \forall (VLR \xleftrightarrow{DK} MS)$
4. $VLR \rightarrow MS : MS| \equiv \#(Na) \wedge VLR| \equiv \#(Nb), MS \triangleleft Nb, A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}$
5. $MS \rightarrow VLR : VLR \triangleleft A8(Nb)_{DK}, MS| \equiv A3(Na)_{Ki}$, on receiving check $A8(Nb)_{DK}$

4.4.4 Message meaning rule

1. $\frac{MS| \equiv (MS \xleftrightarrow{Ki} HLR) \wedge (VLR \xleftrightarrow{DK} MS), MS \triangleleft A3(Na, LAI)_{Ki}}{MS| \equiv HLR| \sim A3(Na, LAI)_{Ki}}$
2. $\frac{VLR| \equiv A3(Na)_{Ki} \wedge (VLR \xleftrightarrow{DK} MS), VLR \triangleleft A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}}{VLR| \equiv HLR| \sim A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}}$

4.4.5 Nonce verification rule

1. $\frac{MS| \equiv \#(Na) \wedge \#(Nb), MS| \equiv HLR| \sim A3(Na, LAI)_{Ki}}{MS| \equiv HLR| \equiv A3(Na, LAI)_{Ki}}$
2. $\frac{VLR| \equiv \#(Na) \wedge \#(Nb), VLR| \equiv HLR| \sim A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}}{MS| \equiv HLR| \equiv A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}}$

4.4.6 Jurisdiction rule

1. $\frac{MS| \equiv HLR \Rightarrow A3(Na, LAI)_{Ki}, MS \triangleleft VLR| \sim A3(Na, LAI)_{Ki}}{MS| \equiv HLR| \equiv VLR}$

Table 6 Bandwidth consumption: existing GSM protocols versus proposed SAKA (in bits)

Authentication token (n)	Original GSM protocol	[2]	[3]	[20]	[19]	[22]	SAKA protocol
5	2,856	2,048	2,432	3,002	2,948	2,808	1,664
10	5,416	3,648	4,352	4,922	5,188	4,728	2,544
50	25,896	16,448	19,712	20,282	23,108	20,088	9,584
100	51,496	32,448	38,912	39,482	45,508	39,188	18,384
Auth. token (n)	[2]/Original GSM	[3]/Original GSM	[20]/Original GSM	[19]/Original GSM	[22]/Original GSM	SAKA/original GSM	
5	0.71	0.85	1.05	1.03	0.98	0.58	
10	0.67	0.80	0.90	0.95	0.87	0.46	
50	0.63	0.76	0.78	0.89	0.77	0.37	
100	0.63	0.75	0.76	0.88	0.76	0.35	
Average	0.66	0.79	0.87	0.93	0.84	0.44	

Bold value shows the minimum bandwidth consumption among all the protocols compared in the paper

2.

$$\frac{VLR| \equiv HLR \Rightarrow A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}, VLR \triangleleft VLR| \sim A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}}{VLR| \equiv HLR| \equiv MS}$$

4.4.7 Protocol goals

a. Mutual Authentication

$MS| \equiv HLR| \equiv VLR \wedge VLR| \equiv HLR| \equiv MS \rightarrow MS| \equiv VLR \wedge VLR| \equiv MS$, thus mutual authentication is hold.

b. Key Agreement

There is one key DK between the VLR and the MS to provide agreement.

$MS| \equiv \#(Na), MS| \equiv DK \wedge \#(Nb)$, since $DK = A3(Na)_{Ki}$

$VLR| \equiv \#(Na), VLR| \equiv DK \wedge \#(Nb)$, since $HLR \rightarrow VLR| \sim DK$

c. Key Freshness

$MS| \equiv \#(Na) \wedge VLR| \equiv \#(Na), VLR| \equiv \#(Nb) \wedge MS| \equiv \#(Nb), DK = A3(Na)_{Ki}$

Thus key freshness between the MS and the VLR holds.

d. Confidentiality between the MS and the VLR

$$\frac{MS| \equiv (MS \xleftrightarrow{DK} VLR), MS \triangleleft A5(Msg)_{DK}}{MS| \equiv VLR| \sim Msg} \wedge \frac{VLR| \equiv (VLR \xleftrightarrow{DK} MS), VLR \triangleleft (Msg)_{DK}}{VLR| \equiv MS| \sim Msg}$$

e. Resistance Replay Attack between the MS and the VLR

If the attacker gets Na from message (1), he/she is unable to forge Message (1) and (2) because he/she doesn't know Ki. If the attacker gets Nb from message (4), he/she is unable to forge Message (4) and (5) because he/she doesn't know DK. Since Na and Nb will be changed at the next time so goal of resistance Replay attack between the MS and the VLR hold.

f. Resistance Man-in-the-Middle Attack between the MS and the VLR

Since attacker neither knows DK nor A5 encryption algorithm, thus it prevents the communication from being eavesdropped.

g. Resistance Redirection Attack between the MS and the VLR

Since $A3(Na, LAI)_{Ki}$ is used to maintain the integrity of LAI, thus it prevents from the Redirection attack.

h. Resistance Impersonation Attack between the MS and the VLR

1. *Adversary tries to impersonate MS*: Since $A3(Na, LAI)_{Ki}$ is computed at MS and compared

at HLR, this prevents from the impersonation attack. Additionally, adversary must reply with a valid $A8(Nb)_{DK}$ but he/she doesn't have DK where $DK = A3(Na)_{Ki}$.

2. *Adversary tries to impersonate VLR*: The integrity value $A3(Na, LAI)_{Ki}$ at the Ms and the HLR will be violated. Additionally, if the MS receives $A8(A3(A3(Na, LAI)_{Ki})_{Ki}, Nb)_{DK}$ at any time, then the connection will be terminated because the MS has not sent any request to VLR.

5 Conclusion

We can conclude with the remarks that the proposed SAKA protocol offers a better service while the mobile subscribers are in roaming and it is able to prevent replay attack, man-in-the-middle attack, redirection attack and impersonation attack. The SAKA protocol generates minimum communication overhead as compare to the other GSM protocols. The proposed protocol is also better in terms of bandwidth utilization compared with all the existing and proposed GSM protocols. One can clearly observe that on an average the SAKA protocol is able to reduce 56 % of the total bandwidth used in the GSM protocol for authentication.

Acknowledgments This research work is supported by Tata Consultancy Services (TCS), India.

References

1. Zhang M, Fang Y (2005) Security analysis and enhancements of 3GPP authentication and key agreement protocol. IEEE Trans Wireless Commun 4(2):734–742
2. Harn L, Lin H (1995) Modifications to enhance the security of GSM. In: Proceedings of 5th national conference on information security, Taipei, Taiwan, ROC, pp 74–76.
3. Lee CH, Hwang MS, Yang WP (1999) Enhanced privacy and authentication for the global system for mobile communications. Wirel Netw 1999:231–243
4. Lin H, Harn L (1995) Authentication protocols for personal communication system. In: Proceedings of ACM Special Interest Group on data communications (SIGCOMM'95), pp 256–261
5. Mitchell C (2001) The security of the GSM air interface protocol. Technical report RHUL-MA-2001-3, University of London, Royal Holloway

6. Recommendation GSM 02.09. Security aspects. European Telecommunications Standards Institute
7. Recommendation GSM 03.20. Security related network functions. European Telecommunications Standards Institute
8. Amani N (2009) Using SMS as a business communication tools for SMES. In: 6th Regional innovation system and innovation clusters in Africa Tanzania.
9. Biryukov A, Shamir A, Wagner D (2000) Real time: cryptanalysis of A5/1 on a PC. Springer, Heidelberg
10. Wagner D (2009) GSM cloning. Smartcard Developer Association and ISAAC security research group.
11. Barkan E, Biham E, Keller N (2003). Instant ciphertext-only cryptanalysis of GSM encrypted communication. CRYPTO 2003. Lecture notes on computer science, vol 2729, pp 600–616
12. Lo CC, Chen YJ (1999) A secure communication architecture for GSM networks. In: Proceedings of IEEE Pacific Rim conference on communication, computers and signal processing
13. Lo CC, Chen YJ (1999) Secure communication mechanisms for GSM networks. IEEE Trans Consumer Electron 45(4):1074–1080
14. Firoozjaei MD, Vahidi J (2012) Implementing geo-encryption in GSM cellular network. In: 9th International conference on communications (COMM), June 2012, pp 299–302
15. Yubo S, Xili H, Zhiling L (2011) The GSM/UMTS phone number catcher. In: Third international conference on multimedia information networking and security, pp 520–523
16. Fanian A, Berenjkoub M, Gulliver TA (2009) A new mutual authentication protocol for GSM networks. In: Canadian conference on electrical and computer engineering, CCECE '09, pp 798–803
17. Southern E, Ouda A, Shami A (2011) Solutions to security issues with legacy integration of GSM into UMTS. In: 6th International conference on internet technology & secured transactions, Abu Dhabi, pp 614–619
18. Fanian A, Berenjkoub M, Gulliver TA (2010) A symmetric polynomial based mutual authentication protocol for GSM networks. In: IEEE wireless communications and networking conference (WCNC), pp 1–6
19. Lee CC, Hwang MS, Yang WP (2003) Extension of authentication protocol for GSM. IEE Proc Commun 150(2):91–95
20. Chang CC, Lee JS, Chang YF (2005) Efficient authentication protocols of GSM. Comput Commun 28(8):921–928
21. Bocan V, Cretu V (2006) Threats and countermeasures in GSM networks. J Netw 1(6):18–27
22. Al-tawil K, Akrami A, Youssef H (1998) A new authentication protocol for GSM network. In: Proceedings of 23rd IEEE annual conference on local computer network, pp 21–30
23. Stach JF, Park EK, Makki K (1999) Performance of an enhanced GSM protocol supporting non-repudiation of service. Computer Commun 22:675–680