A REVIEW OF SELECTED PROPOSALS FOR IMPROVING IDENTITY PRIVACY IN UMTS

Hiten Choudhury

Department of Computer Science & Information Technology
Cotton University, Guwahati, Assam, India

ABSTRACT

Universal Mobile Telecommunication System (UMTS) is a popular 3G standard for mobile telecommunication networks. 'Vulnerability of the subscriber's identity privacy and the need to eliminate this vulnerability', is an established security issue in UMTS. This vulnerability continues to exist up to various extents in the descendent networks of UMTS, like LTE. Several solutions suggesting improvements to the identity privacy in UMTS is present in the literature. In this paper, we look into select few of these solutions, with the expectation that researcher envisioning to work in this area will get a direction in devising an efficient mechanism in improving identity privacy in UMTS, its descendants and future mobile networks.

KEYWORDS

Identity; Privacy; Authentication; Anonymity; IMSI; UMTS; LTE; Interworking

1. INTRODUCTION

3rd Generation Partnership Project (3GPP) has standardised one of the most popular third generation mobile telecommunication network called the Universal Mobile Telecommunication System (UMTS). The security architecture of UMTS (Fig. 1) involves three primary participants namely: the Home Network (HN), the Serving Network (SN) and the Mobile Station (MS) that represents the subscriber. Every MS has to be registered with a HN (with their security credentials stored at the HN's data base). The HN contains key security elements like the Home Location Register (HLR) and the Authentication Centre (AuC). The HLR stores permanent sensitive information of the subscribers such as identity, service profile, activity status, etc., where as the AuC are a protected database that stores association between subscriber identities and long-term keys. The HN extends its services to its roaming subscribers through the SNs. The SN contains elements like the Visitor Location Register (VLR) and the Mobile Switching Centre (MSC). The VLR stores temporary information about subscribers visiting a given location area of the SN and maintains temporary to permanent identity associations, where as the MSC offer circuit-switching domain services. A MS directly communicates with a Base Transceiver Station or NodeB which covers the area the MS is located in. One or more NodeBs are connected with a Radio Network Controller (RNC). The RNC manages the radio resources and is the interface between the MS and the core network. Communication between the MS and the SN happens over radio link, whereas communication between the SN and the HN happens through wired link. While the radio link is considered to be vulnerable, it is assumed that the wired links are adequately secure.

The Authentication and Key Agreement (AKA) protocol adopted by UMTS is called the UMTS-AKA. This mutual authentication is done in two stages [1][2]:

In the first stage, the MS presents its identity to the SN. The SN, with the help of this identity, obtains the security credentials of the MS in the form of a set of Authentication Vectors (AVs) from the HN.

- In the second stage, the SN utilises one of these AVs to perform mutual authentication of the MS through a challenge response mechanism. In this phase, a Cipher Key (CK) and an Integrity Key (IK) are established between the MS and the SN, so that communication over the otherwise vulnerable radio link can happen in a secured and reliable way.

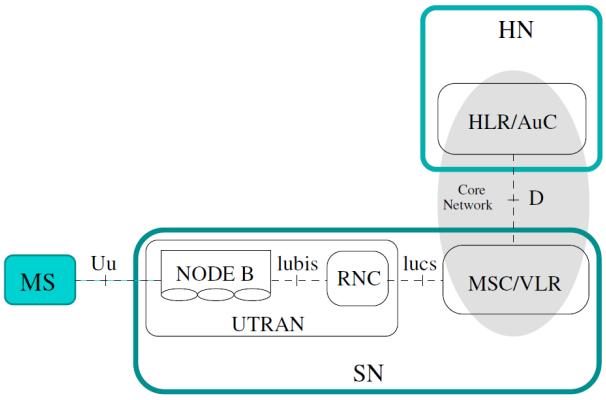

Figure 1. Simplified roaming architecture of UMTS.

Each MS is assigned a unique and a permanent identity called the International Mobile Subscriber Identity (IMSI). This identity is assigned by the HN so that an MS may be uniquely identified. The IMSI is a precious piece of information that needs to be protected. Knowledge of the IMSI of a subscriber may allow an adversary to track and amass comprehensive profiles about individuals. Such profiling may expose an individual to various kinds of unanticipated risks, and above all may deprive an individual of his privacy. Thus, transmission of the IMSI is avoided for identity presentation during an AKA. To restrict the transmission of IMSI over the wireless link, an MS is assigned a short lived Temporary Mobile Subscriber Identity (TMSI). In spite of the above security arrangement, there are situations in UMTS-AKA where the identity privacy of a user may get compromised [3].

To address the vulnerabilities described above, researchers have suggested several new schemes, algorithms and protocols. In this paper, we discuss and analyse a selection of these solutions.
The rest of the paper is organised as follows: section 2 presents a brief description of the UMTS-AKA. The problem of user identity privacy vulnerability in UMTS-AKA is discussed in section 3. In section 4, we present the desirable features of an efficient identity privacy ensuring solution. In section 5, we discuss some of the threats to which a cellular network may be vulnerable. Section 6 reviews the solutions proposed by various researchers. In section 7, we present a couple of classifications based on which the identity privacy ensuring proposals may be categorised. Section 8 presents a comparative analysis of the proposed solutions. We conclude the paper in section 9.

2. UMTS-AKA

UMTS-AKA achieves mutual authentication between the MS and the SN. In order to facilitate the authentication mechanism, each MS shares with its HN a long term secret key Ki and a set of one way hash functions viz., f0, f1 to f5, f8 and f9. In order to assure freshness of authentication data, two counters, viz., SQN_{MS} and SQN_{HN} are maintained at the MS and the HN respectively. UMTS-AKA consists of the following two stages:

A. Distribution of Authentication Data

1. The MS presents its identity to the SN by transmitting it through the radio channel.
2. If the presented identity is a temporary identity, SN locates the corresponding IMSI using the TMSI-IMSI mapping maintained in its local database. The SN then sends an authentication data request to the HN along with the IMSI.
3. Upon receipt of the message, HN generates an authentication vector denoted by AV.
   Each AV consisting of five elements, viz.: a Random Number (RAND), an Expected Response (XRES), a Cipher Key (CK), an Integrity Key (IK), and an Authentication Token (AUTH). An AV is generated according to the following steps (Figure 2):

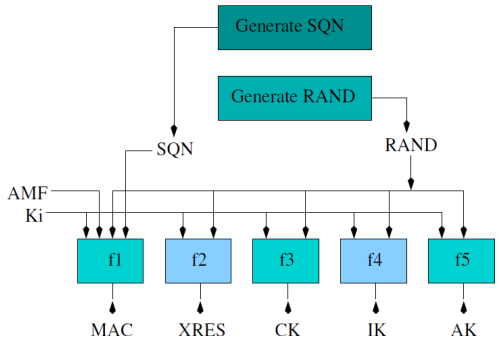

Figure 2. Generation of AV.

- HN generates a Random Number RAND using the function f0, and a Sequence Number SQN from the counter SQN_{HN}.
- HN then calculates the following values:
  $XRES = f2_{Ki}(RAND)$
  $CK = f3_{Ki}(RAND)$
  $IK = f4_{Ki}(RAND)$
  $AK = f5_{Ki}(RAND)$
  $MAC = f1_{Ki}(SQN \| RAND \| AMF)$
  Where AK: Anonymity Key, MAC: Message Authentication Code, AMF: Authentication and Key Management Field, and '||' denote concatenation. AK is used to conceal the sequence number, as the later may expose the location of the user. If no concealment is needed, AK is set to zero.

4. HN assembles the Authentication Token $AUTH = SQN \oplus AK \| AMF \| MAC$ and the Authentication Vector AV = (RAND, XRES, CK, IK, AUTH), where, '$\oplus$' is bit wise Exclusive OR operation.
5. HN increments SQN_{HN} by 1.
6. Finally, HN sends AV back to the SN.

B. Authentication and Key Agreement

1. SN selects extracts RAND and AUTH from AV and sends it to the MS as a challenge.
2. MS calculates $AK = f5_{Ki}(RAND)$. Using the calculated AK, the sequence number $SQN = AUTH \oplus AK$ is calculated. SQN is then compared with SQN_{MS} in order to verify freshness of the challenge. MS then computes $MAC = f1_{Ki}(SQN \| RAND \| AMF)$ and compares this value with the MAC included in AUTH. If they are different, MS rejects the connection procedure, otherwise it accepts it.
3. Finally MS computes $RES = f2_{Ki}(RAND)$ and sends it back to SN.

4. Upon receipt of the RES, SN compares it with XRES. If these values match, the authentication process is considered successful. CK and IK, calculated at either end are used to secure further communications between the SN and MS.

The mutual authentication and key agreement process is schematically expressed in Fig. 3.

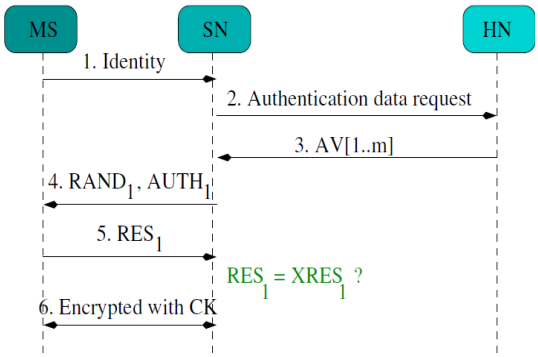

Figure 3. Authentication and Key Agreement.

3. IDENTITY PRIVACY IN UMTS-AKA

To achieve identity privacy during UMTS-AKA, a subscriber is identified within the SN by a TMSI. A TMSI has a local significance and therefore in order to avoid ambiguities, outside the SN, a TMSI should be appended with the Location Area Identification (LAI) of the SN. To avoid compromise of identity privacy, a subscriber should not be identified by means of the same temporary identity for a long period. The allocation of a new temporary identity is initiated by the SN. The SN generates a temporary identity (TMSIn) and stores the association of TMSIn and the IMSI in its local database. The SN then sends this new TMSIn and (if necessary) the new location area identity LAIn to the user through a ciphered channel. This channel is secured using the CK and the IK established at either end. In spite of the above security mechanism, there are situations when the identity privacy of a subscriber may get compromised due to the transmission of its IMSI in clear-text. Some of the situations when the IMSI of an MS becomes vulnerable are as follows (Figure 4):

- MS attaches for the first time with the SN and has not yet received a TMSI: In such a situation, the MS has to present its identity to the SN by transmitting its IMSI in clear-text through the wireless link.
- A database failure at the SN prevents retrieval of IMSI from the TMSI: In such a situation the SN will be forced to request the MS for its IMSI. The later will then have to be transmitted in clear-text through the wireless link.
- After roaming into a new SN's region, the old SN cannot be contacted for the TMSI-IMSI mapping: When an MS moves into the region of a new SN (SNn), it will present its identity to SNn through the TMSI allocated to it by the previous SN (SNo). In order to request for a new set of authentication vectors from HN, SNn will need to have the knowledge of the IMSI. Normally this will be obtained by presenting the TMSI to SNo. However, in case SNo cannot be contacted, SNn will be forced to ask the MS for its IMSI. The later will then have to be transmitted in clear-text over the radio link by the MS. This vulnerability can in fact be exploited by an attacker who can masquerade as a new SN.
- UMTS-AKA assumes full trust relationship within the wired intermediary service network components, and hence the IMSI is transmitted freely amongst them. The possibility of an intermediary agent (like a third party SN) turning hostile and misusing or compromising the IMSI is ruled out.

Thus, ensuring complete identity privacy still remains elusive in UMTS. Several works has been carried out to device enhanced identity privacy in UMTS. Each of these follows different approach and has different characteristics.

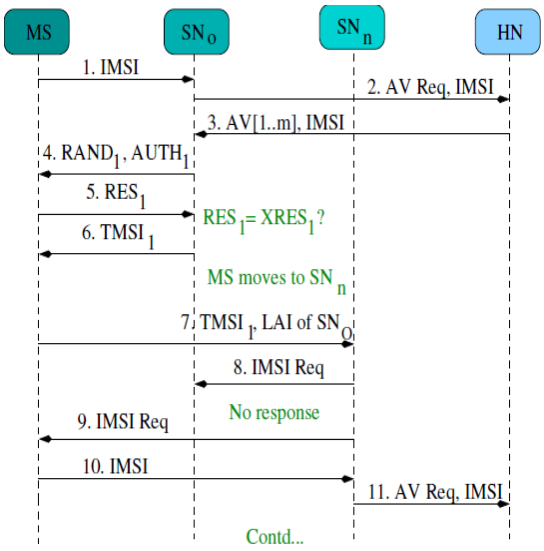

Figure 4. Identity privacy in UMTS-AKA.

4. DESIRABLE FEATURES OF AN IDENTITY PRIVACY ENSURING SOLUTION

In this section, we discuss some of the characteristics that we believe are desirable in an efficient identity privacy ensuring solution for UMTS:

- *Less computational overhead at the MS*: Computationally intensive algorithms must be avoided at the MS, as they are limited by low battery power and computational capability. Symmetric key based computations that are less processor intensive are more suitable compared to public key based computations for the MS.
- *Less computational overhead at the HN*: Since the HN needs to cater to a large number of subscribers; it should avoid computationally intensive algorithms, because such algorithms may increase the overall processing time of the subscriber's requests. Thus, symmetric key based computations are more desirable compared to public key based computations, at the SN.
- *No impact at the SN*: A migration to a new solution should be transparent to the SN. This would make adoption of the protocol easy for service providers who have to rely on third party SNs for providing services to its own subscribers.
- *End to end identity privacy*: An ideal identity privacy ensuring solution should provide end to end identity privacy to the subscribers by restricting the transmission of IMSI in clear text throughout the entire path (wired and wireless) between the MS and the HN. Even key intermediary element like the SN should not have any knowledge about the IMSI of the MS. This would relax the trust requirement which otherwise is a prerequisite for roaming agreements between the HN and the SN. Such a relaxation would specifically be helpful in cases where the same service provider does not own both the HN and the SN.
- *Communication efficiency*: Any kind of security mechanism introduces extra traffic as well as delay into a regular communication. An efficient identity privacy ensuring solution should achieve its objectives with as few signaling message exchanges as possible. This would ensure better performance in terms of traffic overhead and overall latency introduced in the communication. We consider a solution to have communication efficiency if the number of message exchanges involved in it is not more than the number of message exchanges involved in UMTS-AKA.

5. THREATS

An identity privacy ensuring solution should be robust against perceived threats like: eavesdropping, denial of service attack, corrupt serving network, and fake serving network. Each of these threats is briefly discussed below:

1. *Eavesdropping*: Eavesdropping is the act of secretly listening to the private conversation of others without their consent or knowledge. The IMSI is a concatenation of the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscriber Identification Number (MSIN). The MCC and the MNC combined constitutes the IMSI prefix that identifies the MS's HN, whereas the MSIN uniquely identifies an MS within the HN's subscriber base. If the MSIN gets disclosed to an eavesdropper in the radio link, the user's identity gets compromised. And, if the MCC and the MNC gets disclosed to an eavesdropper in the radio link, the MS's HN identity gets compromised [4].
2. *Corrupt Serving Network*: A corrupt serving network is a genuine SN having legitimate service agreement with the HN, but with malicious intention. Such a serving network may clandestinely share precious identity privacy related information entrusted to it by the MS and the HN [5].
3. *Fake Serving Network (Impersonation)*: A fake serving network is an impersonated SN that drowns the signals of a legitimate SN with its own signals and presents itself to the MS as a genuine SN [6].
4. *Denial of Service*: A Denial-of-Service attack (DoS attack) is an attempt to make a computer resource or a service unavailable to its intended users. One common method of the attack involves inundating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be considered effectively unavailable [7][8].

6. SOLUTIONS

In this section, we present brief and simplified interpretation of a select few solutions that are proposed by various researchers to achieve enhanced user identity privacy in UMTS. While, different authors have used different naming conventions, for clarity and uniformity, we follow a common naming convention for the various components involved in the AKA procedure.

A. **Coupon Based Solution (CBS)**

This scheme proposes one time coupons to be transmitted instead of the IMSI [9]. Since, a coupon is used only once, no correlation between the coupon and the corresponding IMSI can be found by an adversary. These onetime coupons are generated at the HN and provided to the MS. During an authentication process, these onetime coupons are transmitted by the MS prefixed with the MCC and the MNC. The association between the coupons and the IMSI is maintained at the home network's local database. For every new connection, the MS uses a new one time coupon to communicate with the SN. This coupon is then forwarded to the appropriate HN along with the request for authentication data. HN in turn, sends to the MS a new set of one time coupons C1...Cn for future connections along with the authentication data.

B. **PKI Based Solution (PBS)**

A Public Key Infrastructure (PKI) based solution is also proposed in [9]. In this solution, the MS generates a random value and builds the following bit sequence:

Seq=00001<random value>00<IMSI>

This bit sequence is then encrypted with the HN's public key and is sent to the HN through the SN. The encrypted bit sequence is used as an alias and is prefixed with the MCC and the MNC. Each time the alias needs to be renewed, a new random value is generated by the MS, and the aforementioned procedure is repeated. At the HN's end, the IMSI is recovered from the alias.

C. Anonymous Number Based Solution (ANBS)

Another technique that is proposed in [9] is an extension of UMTS-AKA, where both the HN and the MS independently derive one time aliases called the International Mobile Anonymous Number (IMAN). An IMAN is derived from the AK that is generated as a part of UMTS-AKA, as follows:

$$IMAN = MD5 (AK \| SQN \| RAND)$$

where MD5 is a hash function and '||' denotes concatenation. The concatenation of the SQN and RAND ensures the freshness of the result. During the protocol flow an IMAN is used to identify a given MS, instead of the IMSI. A mapping between the most recent IMAN and the IMSI is maintained at the MS. At the end of a successful mutual authentication process, the MS updates its IMAN. Like the other protocols proposed in **[8]**, this protocol also needs MCC and MNC to be prefixed to an IMAN.

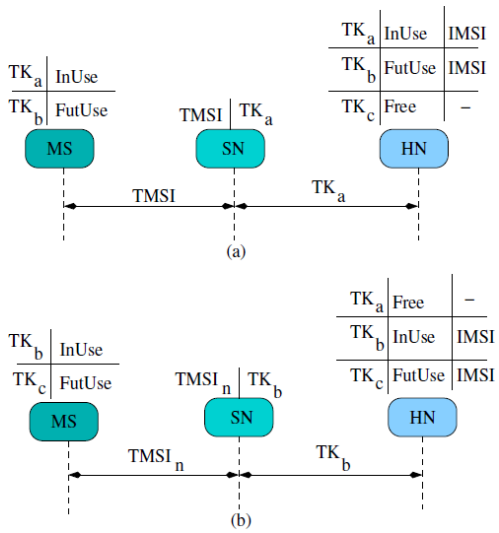

Figure 5. States of the system: (a) initial (b) final

D. IUIC

A mechanism called the Improved User Identity Confidentiality (IUIC) is proposed in [10]. In this mechanism, anonymous tickets are employed as aliases for the IMSI. The IMSI is never exposed over any interface including the wired path. The TMSI plays the same role as in UMTS-AKA. IUIC uses UMTS symmetric cryptography algorithms to ensure anonymity of tickets.

- A separate module called Anonymous Ticket Manager Module (ATMM) is introduced at the HN to handle ticket related functions. The ATMM manages some of the key ticket management operations such as:
- Mapping tickets and their corresponding IMSI.
- Generating new tickets for the MS and releasing already used tickets.
- The assigned tickets should be unique, and hence a single ticket should not be allocated to more than one MS at a particular instance of time. Also, there should not be any logical relationship between the anonymous tickets and the IMSI of an MS.

Two tickets, viz., TKa with in-use status and TKb with future-use status are stored at both the MS and the HN along with the IMSI (Figure 5.a). The SN knows only the ticket with in-use status (TKa), and keeps the relation between TMSI and TKa in its database. A TMSI identifies the MS for the SN, whereas a TKa identifies the MS for the HN. While sending a request for authentication data, SN sends TKa to the HN instead of the IMSI. On receipt of such a request, HN first retrieves IMSI from TKa and then continues with its normal operations.

Whenever a TMSI cannot identify its owner MS, or the relation between the TMSI and an associated ticket is lost, a process called Anonymous Ticket Exchange procedure (ATEP) is invoked. During ATEP, the MS sends TKb to the SN. The SN temporarily stores TKb and forwards a copy of it to the HN. Taking TKb as the parameter, the HN obtains the next free ticket TKc and the corresponding IMSI from the Anonymous Ticket Manager Module (ATMM). The ATMM then frees TKa and sets TKb to in-use status and TKc to future-use status (Figure. b). HN then generates the next AV in the same way as in UMTS-AKA, except that TKc is XORed with the AK instead of the SQN. The HN then forwards the AV to the SN. The SN in turn sends the challenge extracted from the AV to the MS; in the process TKc reaches the MS. MS then sets TKb to in-use and TKc to future-use status. Next time, when TMSI fails to identify an MS, TKc can be used in place of the IMSI as explained above.

E. PP3WAKA

A privacy preserving 3-way authentication and key agreement (PP3WAKA) protocol is proposed in [11] that protects user identity and location data from eavesdropping. It also provides location privacy with respect to the HN. This protocol is devised to deal with the following privacy related security issues:

- Long Term Security Context: These security contexts are based on roaming agreements (SN-HN) and service subscriptions (MS-HN).
- Medium Term Security Context: This context is established dynamically on the basis of long term contexts, and it includes the MS, SN and HN. The validity is restricted according to area, time and usage patterns.
- Short Term Security Context: This context is derived from the medium term context. It encompasses session key material. These contexts are short lived and will only have local validity (MS-SN).
- Spatial home control: HN may need to know if the MS is located within some Validity Area (VA), but no other information should be disclosed to the HN. To get spatial home control, the HN must define a VA for the roaming MS.

In this scheme, the long term shared secret key between the MS and the HN forms a part of the long term security context. The PP3WAKA is an MS initiated scheme. The MS initiates by choosing a pseudorandom value called the Context Reference Identity (CRID). CRID is chosen such that it has no correlation with the user's permanent identity IMSI. The CRID acts as common (authenticated) reference to the three party medium term security context and is valid for exactly one medium-term 3-way security context. Since the HN should be able to forward data to the MS, the HN is allowed to learn the IMSI-CRID association. The CRID-IMSI association is forwarded to the HN without disclosing the same to the SN. SN shall not learn permanent identity (IMSI), but will know that HN acknowledges CRID.

For short term security context, a local Temporary Alias Identity (TAID) is assigned by a SN during a confidentiality protected session. The TAID is used for paging and access request purposes. The TAID should ideally be assigned for one time use. There should be no correlation

between CRID and TAID and amongst TAIDs. SN and MS know TAID-CRID association. The following cryptographic algorithms are used for implementation of the PP3WAKA protocol:

- Secure Multi-party Computation (SMC): With the help of this algorithm, the SN is enabled to transfer the MS's location (x, y) in protected form to the HN. The HN will not be able to learn the (x, y) location, but will be able to determine whether the MS is within the validity area by running a point inclusion algorithm.
- Identity Based Encryption (IBE): This is an unconventional asymmetrical cryptographic method in which there is no need for a prior distribution of digital certificates, the MS can enter a new area and immediately construct and use the public id key. This allows for fast set-up and for improved flexibility in the context binding.
- Deffie-Hellman Exchange: Deffie-Hellman Exchange is used between the SN and the HN to derive the medium term-security context shared secret. It may be noted that the DH-secret is actually used between the SN and the MS.

F. GSZV ALGORITHM

The GSZV algorithm proposed in [12][13] uses public key infrastructure, public key certificates and sequence numbers for its protocol flow. Public keys are used for secured communication of the messages, certificates are used for mutual authentication, and sequence numbers are used to avoid replay attacks. The algorithm proceeds as follows:

- MS sends the following message to the SN:
  $msg1=E_{SN}$ (CERT, E_{HN} (SQN_{MS}))
  where CERT is the certificate issued to the MS by the HN:
  CERT = E_{HN} ((IMSI, Kp) C_{HN})
  E_{SN}(M) and E_{HN} (M) indicates encryption of a value M with the public key of SN and HN respectively; (M)C_{SN} and (M)C_{HN} indicates encryption of M with the private certification key of SN and HN respectively; SQN_{MS} is the most recent sequence number at the MS; Kp is the public key of the MS.

- SN decrypts msg1 and discovers the home address of the MS from the CERT. It then generates the following message, which is certified by its private certification key and encrypted with the HN's public key.
  $msg2=E_{HN}$ {CERT, E_{HN} (SQN_{MS}), TMSI, SQN_{SN}, C_{SN}}
  Here TMSI is the temporary mobile subscriber identity generated by the SN and SQN_{SN} is the sequence number maintained at the SN. msg2 is then forwarded to the HN.

- HN extracts the IMSI from the message and hence authenticates the MS. It then composes the following reply:
  $msg3=E_{SN}$ {SQN_{MS}, TMSI} C_{HN}, {SQN_{HN}, KP} C_{HN}
  The public key of the MS (KP) is recovered from the CERT.
- SN checks for the authenticity of the HN's signature. The SN then sends the following message to the MS.
  $msg4=E_{KP}$ {SQN_{MS}, TMSI} C_{HN})

- MS decrypts the message and validates the digital certificate of the HN. MS then forwards the following message back to the SN for mutual authentication purpose.
  $msg5=E_{SN}$ (SQN_{MS})

G. AIRAM ALGORITHM

AIRAM, presented in [14] is based on GSZV algorithm and is proposed as an improvement over GSZV (in terms of reduced execution time). Like GSZV, this protocol uses symmetric keys, digital certificates and sequence numbers, and its protocol flow is almost the same as GSZV, except minor changes. Unlike GSZV, where the public key of the MS is shared with the SN, in AIRAM, this message transmits the long term secret key Ki to SN. Though the improvement of AIRAM over GSZV is established in the paper by replacing a computationally intensive public key based calculation with a computationally light symmetric key based calculation, the very idea of compromising the long term shared secret key Ki with a third party (SN) goes against the basic 3GPP specifications.

H. HAAP

A scheme called the Hybrid Approach of Authentication Protocol (HAAP) is presented in [15]. This scheme is divided into two procedures. The first one is named Initial Authentication Procedure (IAP), which flow between MS ↔ SN ↔ HN. The second one is limited between MS ↔ SN and is called the Subsequent Authentication Procedure (SAP). The IAP is invoked by the MS when it needs to authenticate itself to all the entities of the network. The SAP enables subsequent authentications between the MS and the SN.

In this scheme, both symmetric and asymmetric keys are used. Authentication between the MS and the HN relies on the long term shared secret key Ki, whereas, authentication between the MS and the SN depends on a public/private key pair and a session key K_{VM}.

The MS invokes the initial authentication procedure by generating a Cipher Key (CK), an Integrity Key (IK) and a session key (K_{VM}). It then encrypts its IMSI and the IK with the secret key Ki. These two encrypted values are forwarded along with a TMSI (that is allocated to the MS during the previous successful IAP) and the identity of the home network to the SN. The SN in turn, forwards the message towards the respective HN.

The MS also encrypts the CK, the IK and the K_{VM}, using the public key of the SN. These three encrypted values are forwarded to the SN. The SN can easily decrypt these values using its private key.

After the HN receives the message from MS, it locates the corresponding Ki using the TMSI-IMSI mapping stored in its local database. It then decrypts the message using Ki to find the correct IMSI and hence authenticates MS. The HN then passes IK+1, and some other protocol related information back to the SN. HN also generates a new TMSI (TMSI') and after encrypting it with Ki sends it back to the MS. The SN in turn, authenticates the HN by checking the value of IK.

At the end of an IAP, three shared keys are established between the MS and the SN, viz., IK, CK, K_{VM}. Where, CK and IK serve the purpose of ciphering and integrity protection of communications between the MS and the SN. And, K_{VM} serves as a long term shared secret key that enables the MS and the SN to carry out successive authentications following the successive authentication procedure by themselves.

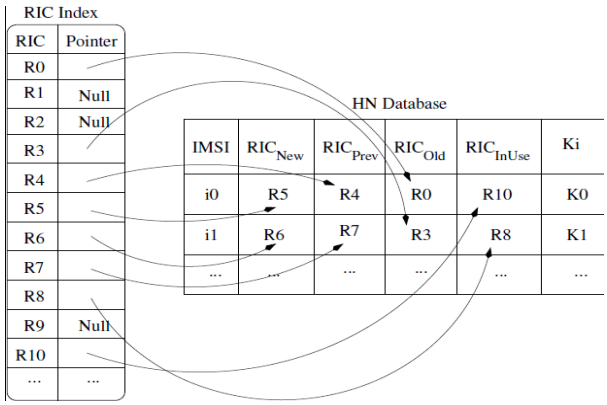

Fig. 6 RIC-Index for HN's database

I. E2EUIC

An extension to UMTS-AKA called the End to End User Identity Confidentiality (E2EUIC) is proposed in [16][17]. In this solution, the IMSI is never transmitted at any stage of the protocol flow; a new dynamic identity called the Dynamic Mobile Subscriber Identity (DMSI) is transmitted instead. The TMSI that is issued by the SN plays the same role as in UMTS-AKA.

A DMSI constitutes of a random number called the Random number for Identity Confidentiality (RIC). A RIC uniquely identifies an MS within a particular HN. Every time a new array of Authentication Vector (AV [1..m]) is generated at the HN, a new value of RIC (say RICn) is also generated. RICn is then cryptographically embedded into the RAND of each and every AV in AV[1..m]. Only the MS, having knowledge of the key Ki, is capable of extracting this embedded RIC from the RAND. Through this technique, it is ensured that RICn reaches the MS in a safe and a secured way during an AKA procedure. A copy of RICn is also stored against the IMSI of the MS in the HN's local database.

DMSI is calculated dynamically as and when its need arises. Its value keeps on changing based on the most recent RIC value received by the MS during the last AKA procedure. DMSI is a concatenation of the Mobile Country Code (MCC), the Mobile Network Code (MNC) and the most recent RIC received by the MS:

$$DMSI = MCC \parallel MNC \parallel RIC$$

where '||' indicates concatenation. Since DMSI is calculated using short-lived RIC values, knowledge of the former does not compromise the actual identity of the MS.

HN stores the current and few previous values of RIC (RIC_{New}, RIC_{Prev}, RIC_{Old}, etc.) against the IMSI of an MS in its local database (Fig. 10). These values ensure that the mapping between the RIC that the MS currently possesses and the RIC that is stored against the IMSI in the HN's database is never lost. To assist in speedy identification of IMSI through the RIC value, a RIC-Index is maintained at HN. The E2EUIC protocol flow is as follows:

While setting up a connection, MS transmits its DMSI to SN, which the latter forwards to corresponding HN.

- Receiving this request, HN extracts RIC from the DMSI to trace the IMSI of MS using the RIC-index. It then generates a fresh RIC and embeds it into the elements of a fresh AV[1..m];

and sends AV[1..m] along with original DMSI, the latter required by the SN to uniquely identifying the MS.

- Receiving this AV[1..m], SN continues the authentication procedure by extracting RAND (with embedded RIC) and AUTH from the first unused AV from AV[1..m], and completes authentication procedure following the same steps as in UMTS-AKA.
- The latest value of RAND (with the embedded RIC) is stored at MS's memory. This embedded RIC will be useful in generating a fresh DMSI if the current TMSI fails to serve its purpose in the next authentication.

J. 3GPP-AKA WITH IDENTITY PROTECTION

In this scheme, random numbers, message authentication codes and one way hash functions are used instead of authentication vectors [18]. The MS and the HN share a long term shared secret key K. HN has another master secret key x with which a secret token Wi is computed as follows:

$$Wi=H(x||ri)$$

where, H is a hashing algorithm and ri is the i^{th} random number generated by the HN for identity protection. Wi and ri are distributed to the MS during an authentication and key agreement procedure via a secure channel. The MS stores these received values for later use.

Since an active location privacy attack may occur only at the time of receiving an identity request at the MS, the proposed scheme is divided into two cases. One is a normal case, where a mutual authentication is performed between the SN and the MS. The other case is during location updating, where the MS receives an identity request.

In a normal case, the MS presents its identity by sending a TMSI that was allocated to it by the SN during a previous run of the scheme. In case the MS has entered a new SN, it sends its TMSI and the Location Area Identity (LAI) of the previous SN to the new SN. The new SN finds the permanent identity (i.e., the IMSI) of the MS from the previously visited SN. The IMSI is then forwarded to the HN for further authentications and key agreements involved in the scheme. During location updating, the MS presents its identity in the following way:

- The MS does not transmit its IMSI in plain text through the radio link. Instead, it generates a token Pi using the secret token Wi and the random number ri that it received from the HN during the previous run of the scheme.
  $Pi=Wi \oplus IMSI$
  Pi is then sent along with the HN's identity and the random number ri to the SN. The SN in turn forwards Pi and ri to the respective HN.
- The HN uses the master key x, the random number ri and the hash function H to generate Wi. It then performs a XOR operation of Wi with Pi to obtain the IMSI and the corresponding shared secret key K of the MS from the local database.
  $IMSI=Wi \oplus Pi$
  K is then used for further processing necessary for authentications and key agreements involved in the scheme. A fresh Wi+1 and ri+1 is also generated at the HN and passed on to the MS in a secured way as a part of the authentication process for identity presentation during the next location updating request.

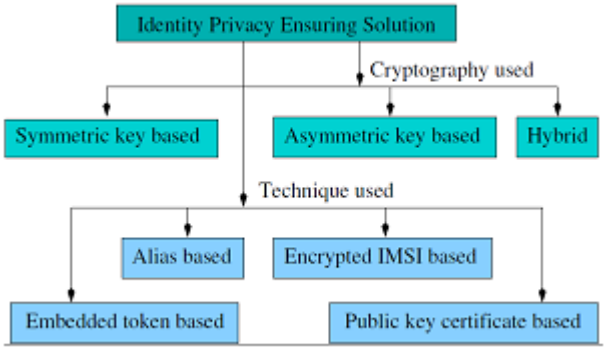

Figure. 7 Classification of identity privacy ensuring solutions

7. CLASSIFICATION

The approaches taken by the different researchers to ensure identity privacy are quite varied. In this section, we attempt to make a classification of these proposed schemes (Fig. 7).

K. CLASSIFICATION BASED ON KIND OF CRYPTOGRAPHIC ALGORITHMS USED

An important factor in the success of an identity privacy ensuring solution is the type of cryptographic algorithm used in it. Different cryptographic algorithms have different computational efficiency. Cryptographic algorithms that are robust against various kinds of attacks and at the same time are computationally efficient are more suitable for resource limited mobile devices. Based on the kind of cryptographic algorithms used, identity privacy ensuring solutions for UMTS may be classified into the following categories:

- *Symmetric key based approach (SK)*: In symmetric key based approach, a long term shared secret key is established among the communicating parties for encryption and decryption [18]. The main concern behind symmetric encryption is: how to share the secret key securely between the two peers. If the key gets compromised for any reason, the whole system collapses. Symmetric key based approach is suitable for mobile equipments because of their low computational and power requirements; and because of the ease at which the secret key can be shared securely between the MS and the HN during the Universal Subscribers Identification Module (USIM) distribution process.
- *Asymmetric key based approach (AK)*: Asymmetric encryption, also known as Public Key Cryptography is the other type of encryption where two keys are used: the public key known to the public, and the private key known only to the user [19]. Asymmetric cryptography algorithms are slow because they are designed to work through computationally intensive mathematical functions, like factoring of large prime numbers, etc. They are almost 1000 times slower than symmetric techniques [20][21]. People still use asymmetric keys as part of an encryption scheme because they provide for non-repudiation of data and make key management easier than strictly symmetric keys.
- *Hybrid approach (HB)*: In this approach, advantages of both symmetric and asymmetric cryptographic algorithms are exploited.

L. CLASSIFICATION BASED ON TECHNIQUE USED

Based on the techniques used to achieve improved identity privacy, the proposed solutions may be broadly classified into the following:

- *Alias based (AB)*: In this technique, one time aliases are used to provide identity privacy. In order to identify an MS, one time aliases are transmitted instead of the IMSI. For every new connection a fresh one time alias has to be used. An alias should be generated such that: 1) there is no correlation between two aliases and 2) there is no correlation between an alias and its corresponding IMSI. Aliases may be generated by any of the agents, viz., MS, SN or the HN. For synchronisation, aliases may have to be transferred from the agent/agents where they are generated to the other agents. The aliases have to be transferred through secured channels or they have to be encrypted before transferring.
- *Embedded token based (ET)*: In this technique, unique tokens whose value keeps changing time to time are used to identify an MS. The mapping between a token and the IMSI of an MS is maintained at the HN. The tokens should be maintained such that: 1) there is no correlation between two tokens and 2) there is no correlation between a token and its corresponding IMSI. A token is generated at the HN and transmitted securely to the MS by embedding it into the messages that are exchanged during an authentication and key agreement procedure.
- *Public key certificate based (PKC)*: In this technique, public key certificates are employed to achieve enhanced identity privacy.
- *Encrypted IMSI based (EI)*: In this technique, an encrypted version of the *IMSI* is transmitted instead of the *IMSI*.

In Table 1, we present a categorisation of the solutions based on the above classifications.

Table 1 Classification of Identity Privacy Enhancing Solutions

Solution	SK	AK	HB	AB	PKC	EI	ET
CBS	√	×	×	√	×	×	×
PBS	×	√	×	√	×	×	×
ANBS	√	×	×	√	×	×	×
IUIC	√	×	×	√	×	×	×
PP3WAKA	×	√	×	√	×	×	×
GSZV	×	√	×	×	√	×	×
AIRAM	×	×	√	×	√	×	×
HAAP	×	×	√	×	×	√	×
E2EUIC	×	×	×	×	×	×	√
3GPP-AKA with IP	×	×	×	×	×	√	×

8. COMPARATIVE ANALYSIS

In this section, we analyse all the solutions, with respect to the desirable features and with respect to the threats. Summary of the analysis are presented in Table II and Table III.

M. COUPON BASED TECHNIQUE

Coupon based technique vis-a-vis desirable features:

- No extra computation is introduced at the MS; as its only responsibility is to store the received coupons and forward them at a later time.

- Although the HN has the added burden of generating and maintenance of extra coupons, considering its computational capability, we consider this overhead to be insignificant.
- In order to accommodate the coupons, the format of message that is used to transmit authentication data from the HN to the MS has to be modified. This would impact the functioning of the SN (that is placed in between the HN and the MS), as it will have to make necessary adjustments to cope with this format change.

In this scheme, coupons are used for identity presentation instead of the IMSI. The IMSI is not shared with any intermediary element including the SN, thereby ensuring end-to-end identity privacy. Coupon based technique does not add any extra communication overhead compared to UMTS-AKA.

Coupon based technique vis-a-vis threats:

- As every coupon is prefixed with the MCC and the MNC, the home network identity is vulnerable to an eavesdropper on the radio link.
- This scheme may invite the following kind of DoS Attack: An impersonator of the SN may send many consecutive requests for the permanent identity to the MS. For every such request the MS will respond by sending an unused one time coupon. Because of the onetime nature of the coupons, very soon the coupons will get exhausted and the MS will have no other way to present its credentials to the SN. This may end up denying service to the MS.
- A corrupt SN does not have much to explore, as the IMSI is not shared with the SN.
- In this scheme, the IMSI is never transmitted. Thus, a fake SN cannot compromise the permanent identity; however, there is an opening for a fake SN to launch a DoS attack as explained above.

Table II. Identity privacy ensuring solutions with respect to fulfilment of desirable features.

Solution	Less Overhead on MS	Less Overhead on HN	No Impact on SN	End to End IP	Communication Efficiency
CBS	√	√	×	√	√
PBS	×	×	×	√	√
ANBS	√	×	×	√	√
IUIC	×	×	×	√	√
PP3WAKA	×	×	×	√	×
GSZV	×	×	×	√	√
AIRAM	×	×	×	√	√
HAAP	×	√	×	√	√
E2EUIC	√	√	√	√	√
3GPP-AKA with IP	√	√		×	×

N. PKI BASED TECHNIQUE

PKI based technique vis-a-vis desirable features:

- This scheme is based on computationally intensive public key cryptography and hence will add extra computational overhead at the MS and the HN.

- The functioning of the SN will be significantly influenced, as format of message used for identity presentation is different from UMTS-AKA.
- Since a bit sequence is presented to the SN in lieu of the IMSI, end to end identity privacy is ensured in this scheme.
- Since the number of messages exchanged between the agents in this protocol is same as 3GPP-AKA, it ensures communication efficiency.

PKI based technique vis-a-vis threats:

- In this protocol, every bit sequence is prefixed with the MCC and the MNC. This will enable an eavesdropper to determine the home network identity of a subscriber.
- A corrupt SN does not have a chance, as the IMSI is not shared with it.
- A Fake SN may frequently request the MS its permanent identity. This will make the MS generate a random value every time, which is then encrypted with the HN's public key. Since public key cryptography is resource intensive, the MS will be kept engaged with this cryptographic computation rather than the actual service, resulting in Denial of Service.

O. ANONYMOUS NUMBER BASED TECHNIQUE

Anonymous number based technique vis-a-vis desirable features.

- Calculation of a new IMAN value at the MS is not computationally intensive, since MD5 algorithm having low computational requirement is used in this process [22][23].
- The above is not true for the HN where extra computational cycles are introduced to check for IMAN collisions.
- Since an IMAN is transmitted instead of the IMSI, the SN has to make adjustments to accommodate the same.
- This scheme ensures end to end identity privacy, since the MSIN is never transmitted at any stage of the communication between the MS and the HN.
- No extra message is introduced in this scheme compared to UMTS-AKA, thereby ensuring communication efficiency.

Anonymous number based technique vis-a-vis threats.

- An IMAN is prefixed with the MCC and the MNC, this may enable an eavesdropper to discover the home network identity of a subscriber.
- Since the IMSI is not shared with the SN, a corrupt and a fake serving network cannot compromise the permanent identity.

P. IUIC

IUIC vis-a-vis desirable features:

- In this scheme, the MS's additional responsibility is to store the token that is received from the previous ticket exchange procedure and to transmit it in place of the IMSI when required. Thus, very little computational overhead is imposed on the MS.
- Although considerable computational overhead is imposed at the HN due to introduction of the ATMM, the same may be considered to be insignificant considering the computational capability of the HN.
- The protocol introduces adjustments on all the agents including the SN
- End to end identity privacy is ensured in this protocol, as the permanent identity is never transmitted at any stage of the protocol flow.
- The number of message exchange involved in this solution is same as that of UMTS-AKA. Thus, we infer that this solution achieves communication efficiency.

IUIC vis-a-vis threats.

- In this protocol, every token should be prefixed with the MCC and the MNC. This provides scope for an eavesdropper to compromise the home network identity of a subscriber.
- Since tokens are transmitted instead of the IMSI, a corrupt and a fake serving network cannot compromise the permanent identity.

Q. PP3WAKA

PP3WAKA vis-a-vis desirable features.

- Due to the use of processor intensive cryptographic algorithms, the computational overhead introduced at the MS and the HN is very high.
- The solution is totally different from the state of the art security architecture. Thus, the SN will have full impact if the solution has to be adopted in place of the current security protocol.
- End to end identity privacy is achieved in this solution, as the IMSI is not shared with any intermediary elements including the SN.
- The numbers of messages exchanged in this solution is more than that of UMTS-AKA. Thus, we infer that this solution is not as efficient as UMTS-AKA in terms of communication.

PP3WAKA vis-a-vis threats.

- In the first message of the authentication procedure, the MS sends the home networks identity to the SN through the radio link in clear text. This leaves scope for adversaries to eavesdrop and compromise the home network identity of the MS.
- A corrupt and a fake serving network do not have any chance, as the permanent identity is never transmitted by the MS.
- A Fake SN may request the MS to initiate an authentication process. The MS in reply generates a message that is secured with the public key, and forwards it to the SN. Through this exercise the Fake SN cannot achieve much in terms of compromised information, but can easily generate many such requests for the MS that will be enough to keep the MS busy with computationally intensive cryptographic calculations. This may result in denial of regular cellular services that the MS has subscribed to.

R. GSZV

GSZV vis-a-vis desirable features:

- Being a public key infrastructure based algorithm, the MS and the HN are imposed with extra overhead.
- The SN is also expected to participate in the protocol implementation.
- End to end identity privacy is achieved by this protocol as IMSI is not transmitted throughout the entire path between the MS and the HN.
- The number of message exchange in this solution is same as that of UMTS-AKA. Thus, we conclude that it achieves communication efficiency.

GSZV vis-a-vis threats:

- This protocol protects the home network identity form eavesdroppers in the radio path by protecting the IMSI through the use of public key cryptography.
- As the IMSI is not shared with the SN, a corrupt SN does not have any chance.

- A Fake SN may request the MS to initiate an authentication process. The MS in reply generates a message that is secured with the public key, and forwards it to the SN. Through this exercise the Fake SN cannot achieve much in terms of compromised information, but can easily generate many such requests for the MS that will be enough to keep the MS busy with computationally intensive cryptographic calculations. This may result in denial of regular cellular services that the MS has subscribed to.

Table III. Identity privacy ensuring solutions in terms of robustness against threats.

Solution	Eavesdropping	DoS	Corrupt SN	Fake SN
CBS	×	×	√	×
PBS	×	×	√	×
ANBS	×	√	√	√
IUIC	×	√	√	√
PP3WAKA	×	×	√	×
GSZV	√	×	×	×
AIRAM	√	×	×	×
HAAP	×	√	√	√
E2EUIC	×	√	√	√
3GPP-AKA with IP	×	√	×	√

S. AIRAM

Since this algorithm is proposed as an improvement over GSZV, most of its features are same as GSZV. The only difference being the fact that the SN is confided with the long term shared secret key between the MS and the HN by the HN. Such a level of trust shown on the SN is not practical and may be considered as a serious security loophole.

T. HAAP

HAAP vis-a-vis desirable features:

- In this scheme, public key cryptography is used for communication between the MS and the SN. Thus extra computational overhead will be imposed at the MS.
- Communication between the MS and the HN relies on symmetric key. Thus the cryptographic calculations imposed at the HN may be considered negligible.
- The protocol flow is different from UMTS-AKA and thus needs considerable change at the SN.
- The IMSI is not transmitted in clear text in the entire path between the MS and the HN. Thus end to end identity privacy is ensured.
- This protocol achieves its objectives with less number of messages compared to UMTS-AKA and thus, we consider it to be an efficient solution in terms of communication.

HAAP vis-a-vis threats:

- During authentication, the MS sends the home network identity (IDH) in plain text to the SN. This leaves scope for adversaries to eavesdrop and compromise the home network identity of the MS (Type II vulnerability).

- As the transmission of the permanent identity is replaced by temporary identities, this protocol is robust against corrupt and fake SNs.

U. E2EUIC

E2EUIC vis-a-vis desirable features:

- Minimal overhead of storage and transmission of the RIC at a later time is imposed at the MS.
- The burden of generation and maintenance of RIC is introduced at the HN. Considering the sound processing capability of the HN, this may be considered insignificant.
- Since the format of the messages does not change compared to UMTS-AKA, there is no impact on the functionality of the SN.
- End to end identity privacy is achieved, as the knowledge of the IMSI is not shared with anyone except the MS and the HN.
- Since the number of messages exchanged in this protocol is same as UMTS-AKA we may infer that the protocol ensures communication efficiency.

E2EUIC vis-a-vis threats:

- The Dynamic Mobile Subscriber Identity that is transmitted in place of the International Mobile Subscriber Identity is prefixed with the MCC and the MNC of the HN. This provides scope for adversaries to eavesdrop and compromise the home network identity of the MS.
- A corrupt/fake SN does not have a chance as the IMSI is not transmitted in any situation.

V. 3GPP-AKA WITH IDENTITY PROTECTION

3GPP-AKA with Identity Protection vis-a-vis desirable features:

- As simple one way hash functions are used for encryption/decryption of the IMSI, minimal overhead is imposed at the MS and the HN.
- The effect of migration to this protocol will impact the SN, since new message formats and protocol flow is introduced.
- Since IMSI is transmitted freely between the SN and the HN and as such we may conclude that end to end identity privacy feature is not satisfied.
- The number of messages exchanged in this protocol is more compared to UMTS-AKA.

3GPP-AKA with Identity Protection vis-a-vis threats:

- Since the home network identity of the MS is transmitted over the radio link in clear text, an eavesdropper may easily compromise the home network identity of the MS.
- In this protocol the IMSI of a MS is shared with the SN. This makes the permanent identity of a MS vulnerable to Corrupt Serving Networks.

9. CONCLUSION AND FUTURE WORK

Identity privacy is a crucial security issue in cellular networks. The current authentication and key agreement protocol adopted by UMTS does not assure perfect identity privacy. A selection of proposed solutions towards strengthening identity privacy in UMTS were analysed in this paper. The same could be useful in providing a background in formulating a strong identity privacy ensuring solution. Though many schemes and protocols have been proposed to strengthen identity privacy, each of them is inept in fulfilling all the identity privacy related requirements at the same time. Thus, none of the proposed strategies could be adopted convincingly to strengthen the

condition of identity privacy in cellular networks. As a result, the status of identity privacy remains as it earlier used to be in UMTS. Even next generation cellular network technologies like 3GPP-WLAN interworking, LTE and non 3GPP to EPS interworking are unable to achieve any major breakthrough. Therefore, an open issue is to develop a single scheme that fulfils majority of the identity privacy related requirements. While designing such a solution adherence to some of the important features like less overhead on the network components, end to end user identity privacy, leaving out the serving network from migration, etc., will be vital for its success. It is also imperative that while trying to address the issue of identity privacy, the solutions should steer clear of introducing any additional vulnerability. A failure to do so would provide opportunities to adversaries, which in the first place such solutions are trying to nullify.

REFERENCES

[1] G. Koien, "An introduction to access security in umts", IEEE Wireless Communications, Vol. 11, Issue. 1, pp. 8–18, 2014.

[2] C. Xenakis, L. Merakos, "Security in third generation mobile networks", Computer communications, Vol. 27, Issue. 7, pp. 638–650, 2014

[3] M. Khan, A Ahmed, A Cheema, "Vulnerabilities of umts access domain security architecture" In the proceedings of Ninth IEEE ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 350–355, 2008

[4] Y. Zhang, J. Zheng, M. Ma, "Handbook of research on wireless security", Information Science Reference-Imprint of: IGI Publishing, 2008.

[5] M. Zhang, "Adaptive protocol for entity authentication and key agreement in mobile networks". In the proceedings of Information Security and Cryptology, pp. 166–183, 2004

[6] M. Zhang, Y. Fang, "Security analysis and enhancements of 3gpp authentication and key agreement protocol", IEEE Transactions Wireless Communications, Vol. 4, Issue. 2, pp. 734-742, 2005

[7] G. Carl, G Kesidis, R Brooks, S Rai, "Denial-of-service attack-detection techniques", IEEE Internet Computing, Vol. 10, Issue. 1, pp. 82–89, 2006

[8] S.A.Arunmozhi, Y.Venkataramani, "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.3, Issue.3, pp. 182-187, 2011

[9] M. Barbeau, J. Robert, "Perfect identity concealment in umts over radio access links", In the proceedings of IEEE Wireless And Mobile Computing, Networking And Communications, vol. 2, pp. 72-77, 2005

[10] B. Sattarzadeh, M. Asadpour, R. Jalili, "Improved user identity confidentiality for umts mobile networks", In the proceedings of IEEE fourth European Conference on Universal Multiservice Networks, pp. 401-409, 2007

[11] G. Køien, V. Oleshchuk, "Location privacy for cellular systems; analysis and solution", Privacy Enhancing Technologies, Springer, pp. 40-58, 2006

[12] G. Godor, B Varadi, S. Imre, "Novel authentication algorithm of future networks". In proceedings of IEEE International Conference on Mobile Communications and Learning Technologies, pp. 80-80, 2006

[13] G. Godor, S. Imre, "Novel authentication algorithm – public key based cryptography in mobile phone systems", IJCSNS, Vol. 6, Issue. 2B, pp. 126, 2006

[14] M. Naveed, A. Minhas, J. Ahmad, "Improved authentication algorithm for umts", In the proceedings of the International Conference on Hybrid Information Technology, ACM, pp. 327-332, 2009

[15] M. Al-Fayoumi, S Nashwan, S. Yousef, A. Alzoubaidi, "A new hybrid approach of symmetric/asymmetric authentication protocol for future mobile networks", In the proceedings of third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2007, pp. 29-29, 2007

[16] H. Choudhury, B. Roychoudhury, D. Saikia, "End-toend user identity confidentiality for umts networks" In the proceedings of 3rd IEEE International Conference on Computer Science and Information Technology, Vol. 2, pp. 46-50, 2010

[17] H. Choudhury, B. Roychoudhury, D. Saikia, "Umts user identity confidentiality: An end-to-end solution", In the proceedings of eighth IEEE International Conference on Wireless and Optical Communications Networks, pp. 1-6, 2011

[18] W. Juang, J. Wu, "Efficient 3gpp authentication and key agreement with robust user privacy protection" In the proceedings of IEEE Wireless Communications and Networking Conference, pp. 2720-2725, 2007

[19] B. Schneier, P. Sutherland, "Applied cryptography: protocols, algorithms, and source code in C", John Wiley & Sons, Inc., 1995.

[20] J. Edney, W. Arbaugh,. "Real 802.11 security: Wi-Fi protected access and 802.11 i", Addison-Wesley Professional, 2004

[21] T. Hardjono, L. Dondeti, "Security in wireless lans & mans", Artech House Computer Security, 2005

[22] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, M. Sichitiu, "Analyzing and modelling encryption overhead for sensor network nodes", In proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, ACM, pp. 151-159, 2003

[23] W. Freeman, E. Miller. "An experimental analysis of cryptographic overhead in performance-critical Systems", In the proceedings of 7th IEEE International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems, pp. 348-357, 1999