Mobile Privacy in Wireless Networks - Revisited

Caimu Tang, *Member, IEEE,* and Dapeng Oliver Wu, *Senior Member, IEEE*

***Abstract*— With the widespread use of mobile devices, the privacy of mobile location information becomes an important issue. In this paper, we present the requirements on protecting mobile privacy in wireless networks, and identify the privacy weakness of the third generation partnership project - authentication and key agreement (3GPP-AKA) by showing a practical attack to it. We then propose a scheme that meets these requirements, and this scheme does not introduce security vulnerability to the underlying authentication scheme. Another feature of the proposed scheme is that on each use of wireless channel, it uses a one-time alias to conceal the real identity of the mobile station with respect to both eavesdroppers and visited (honest or false) location registers. Moreover, the proposed scheme achieves this goal of identity concealment without sacrificing authentication efficiency.**

***Index Terms*— mobile privacy, mobile authentication, user untraceability, one-time alias, 3GPP-AKA, elliptic curve cryptosystems.**

I. Introduction

Mobile handheld devices in wireless networks are gradually changing the way we live our life. Privacy is a serious concern for many emerging applications in wireless networks whereas mobile privacy protection is a complicate issue. On one hand, location tracking capability provided by modern technologies makes mobile users uncomfortable. On the other hand, location management for mobile devices, which helps direct incoming calls and supports mandatory location service required by governments in the case of emergency (e.g., enhanced 911 location mandate by U.S. Federal Communications Commission), makes mobile terminals vulnerable to revelation of location information. Any mobile privacy protection mechanism has to address these seemingly contradictory requirements.

A mobile station (MS) or a mobile user (they are used interchangeably in this paper) can expose its location at the mobile-station authentication stage or during actual data communication. At the authentication stage, an adversary in a serving network, or the visitor location register (VLR) of a mobile switching center [1], [2] (we simply refer a mobile switching center as a VLR if the MS is a visitor of it), might be able to identify the MS and then its location. Moreover, an adversary may be able to track an MS while the MS is hopping among VLRs and authenticating itself to VLRs. If the identity of MS is required in order for the home network, which is simply referred by home location register (HLR) in this paper, to authenticate an MS, HLR and/or an eavesdropper may be able to track the MS at least at the granularity of VLRs that an MS has visited. Only when the identity privacy is protected at the authentication stage, can the protection of mobile user's location privacy in wireless services be possible.

The mobile privacy issue in the Third Generation Partnership Project - Authentication and Key Agreement (3GPP-AKA) [3], [4] is addressed via a so-called anonymity key. That method on privacy is also used in some other 3GPP-AKA related work, e.g., [5]. In Ref. [6], a proposed privacy protection scheme for mobile terminals uses blind signature, and it is able to support MS authentication and access authorization functionalities. In Ref. [7], [8], content privacy, location privacy and sender-receiver unlinkability issues were investigated, and a MIX-network based technique was exploited for privacy protection. In Ref. [9], a technique using a pseudonym for a subscriber to conceal its real identity and a digital mix was proposed to disassociate a user from its real identity, where the pseudonym acts as a temporary identity of a mobile terminal to the external users and a digital mix is used for data scrambling. These approaches suffer from an insider attack, e.g., the false base station attack, as pseudonym is made only for an external interface. Adversary on those scheme can track the unique pseudonym. This problem can be alleviated to a certain degree by a frequent change of pseudonyms. In Ref. [10], [11], [12], a one-time alias (or pseudonym) approach is proposed to address the anonymity issue of mobile station. In this paper, a similar one-time alias technique is exploited and seamlessly integrated with a mobile authentication scheme for location privacy protection. The proposed scheme adds little overhead to an MS for privacy protection, and a moderate overhead is added on the fixed network part (i.e., the network of location registers).

The anonymity-key approach taken in 3GPP-AKA requires encryption of MS sequence numbers during mobile authentication and key agreement to conceal MS's identity and location, and hence this approach is not efficient. Furthermore, 3GPP-AKA is able to provide MS anonymity only when all VLRs (not only the currently serving VLR) are not compromised. This is a strong assumption for privacy protection. We shall show an example in Section III where the privacy of an MS is compromised as long as one VLR is corrupted. To address the limitation of 3GPP-AKA and help devise sound privacy protect method, we will identify important design principles for wireless mobile privacy. The mobile privacy provision should start at the mobile authentication stage. A privacy protection solution should not compromise the underlying authentication, and at the same time it should be flexible so that a location service can be provided whenever necessary, and most importantly, a solution should be efficient for mobile devices in terms of communications and computation overhead.

Manuscript received xx xx, xxxx; revised xx xx, xxxx; accepted October, 5, 2007. The editor coordinating the review of this paper and approving it for publication is Prof. Yi-Bing Lin. The authors are in alphabetical order.

C. Tang is with Pathfinder Energy Services at Houston, TX 77041 (e-mail: caimu.tang@pathfinderlwd.com).

D. O. Wu is with the Department of Electrical and Computer Engineering at the University of Florida, Gainesville, FL 32611-6130, USA (e-mail: wu@ece.ufl.edu).

Public key cryptosystems have been used for mobile authentication and privacy in wireless networks [11], [13], [14], [6], [15]. In Ref. [14], a scheme called EMAS is proposed. In EMAS, an MS, which is registered to an HLR, proves its registration to a VLR via the trust delegation mechanism, which was first exploited for mobile authentication in Ref. [15]. The EMAS scheme requires only two messages to mutually authenticate MS and VLR, and it is also invulnerable to the denial of service attack. Previous work on mobile privacy [11], [3], [4] assumes that there is no false base station in a network. One focus in this paper is to analyze the existing mobile privacy schemes in wireless networks under a more generic condition, for example, not all base station are assumed to be honest, and then to devise a privacy protection soultion for EMAS under this more generic assumption without sacrificing its security and efficiency properties.

Trust delegation has been studied in the context of proxy signature. Since the seminal work of Ref. [16] where delegation is built upon the intractability of discrete logarithm problem (DLP), a smart-card version of that scheme is presented in Ref. [17], and that scheme was proven to be reducible to DLP when impersonation attack is concerned. Further results on vulnerability and security analysis related to DLP based delegation are presented in Ref. [18], [19], [20].

Our contribution in this paper includes analytic results on weakness on existing mobile authentication/privacy schemes including 3GPP-AKA with concretely constructed attacks. We have also devised a one-time alias mechanism for various levels of privacy protection. This derived privacy protection scheme based on a provable secure trust delegation building block fulfills all practical requirements of mobile stations in wireless networks under a more generic threat model.

The rest of the paper is organized as follows. In Section II, we first give the notation and assumptions used in this paper. In Section III, requirements on mobile privacy are investigated. A mobile privacy solution to EMAS is proposed in Section IV. Conclusions are drawn in Section VI.

II. Notations and Assumptions

Before we proceed, we next make some assumptions and define some notation for use throughout this paper. We denote by F a Galois field which is either a prime field or an extension field of a prime field, and by E an elliptic curve over F, and by T a point on E. Further assume that the order of T is a large prime p or has a large prime factor p, and this prime number p and the ground field F are proper for the cryptographic purpose. The additive group derived from T over F for a cryptographic use is denoted by E/F. We refer to Ref. [21] for the parameter selection on elliptic curve cryptosystem (ECC) setup. Notations and assumptions are shown in Table I with comments for their use in the paper, and additional explanations of their uses are given in Section III and Section IV.

Due to progresses on sub-exponential algorithms on discrete logarithm over Galois field [22] and integer factoring [23], the intractability of elliptic curve discrete logarithm problem (ECDLP) has been instead exploited for building many secure protocols. Let a point $Q = xT$ for $x \in Z_p^*$, the ECDLP refers to obtaining the unknown x from $Q \in E/F$. When cares are exercised on the selection of the curve E, the point T on E, its prime order or a prime factor of T (i.e. p) and the ground field F, the only known available algorithms to solve this well formed ECDLP will be some extensions of these square-root-type algorithms for the discrete logarithm problem over a Galois field [24]. These algorithms in general have exponential complexity with regard to the key bit length. ECC is built upon the intractability of ECDLP. The significant advantages ECC brings much shorter key length (163 bits vs. 1024 bits), hence reductions on communication cost and memory requirement as these are crucial for low-power embedded mobile terminals.

We have considered a threat model to EMAS including message en route threat, fase base station threat. Attacks from the threat model include message relay/redirect attacks, impersonation attacks, collusion attacks. We refer to Ref. [14] for details. The same threat model is assumed in this paper.

III. A Taxonomy of Wireless Mobile Privacy: An Analytic Perspective

We consider four levels of mobile privacy, namely, privacy against eavesdropper (PAE), privacy against false base station (PAFB), privacy against genuine base station (PAGB), and privacy against home base station (PAHB). PAE is the lowest level of mobile privacy, and PAHB and PAGB are the highest level and the second highest level, respectively. PAHB may not be practical due to location management for incoming connections and mandatory emergency services. All state-of-the-art mobile authentication schemes require a static or semi-static shared secret between MS and its HLR in one way or another. As long as this shared secret and the VLR identity are used during the authentication process, the mobile location privacy is violated under PAHB. It seems contradictory to authenticate VLR from HLR without knowing VLR's identity. Approaches taken in Ref. [11] on PAHB assumes that a chain of trust from HLR to successively visited VLRs exists, and such assumption might be too strong in practice. Additional comments on this issue are presented in Section V. In Ref. [11], a classification on mobile identity and location privacy was presented. In this paper, we address this instead focusing on privacy implications from antenna beamforming techniques and recent development on mobile attacks, and ignore relatively well studied content-privacy.

We further differentiate the granularity of privacy violation of each level by two categories, namely, itinerary privacy (IP) and location privacy (LP). Itinerary privacy of an MS is defined by the privacy of the information about the moving trajectory of the MS, while location privacy of an MS is defined by the privacy of the information about the current location of the MS. In addition, IP has two levels of granularity, namely, inter-VLR IP and intra-VLR IP, where inter-VLR IP refers to the case that an MS's itinerary can be traced at the resolution of radius of a VLR coverage area, and intra-VLR IP refers to the case that an MS's itinerary can be traced at a finer-grained level with a distance resolution smaller than the radius of VLR coverage area. For example, an adversary may be able to know

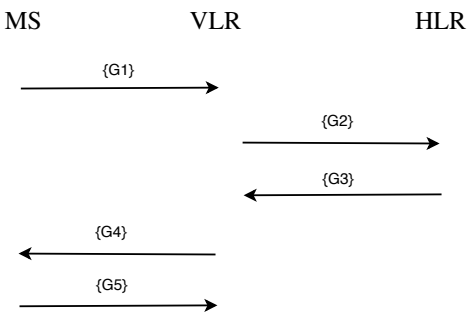
TABLE I
NOTATIONS

p	: the largest prime factor of the order of T, non-smooth, of length ≥ 163
Z_x^*	: the cyclic group of order $x-1$ for prime number x
$\uplus$	: the point addition in E/F
$\oplus$	: binary bit-wise exclusive OR operator
xT	: the point scalar multiplication of $x \in Z_p^*$ to T in E/F
$h(.)$	: a collision resistant one-way hash function from $Z_p^* \mapsto Z_p^*$
m_w	: a warrant containing its generator's identification, imposed restrictions
$\|$ or ','	: the concatenation operator of two bit strings whenever the context is clear
$K_{(V,H)}$	: the session key between VLR and HLR
K_V	: the secret key of VLR
K_H	: the secret key of HLR
IDV	: identity (a number in Z_p^*) of VLR
IDH	: identity (a number in Z_p^*) of HLR
IDM	: identity (a number in Z_p^*) of MS
IDMA	: identity (a number in Z_p^*) of an alias of MS
$\{x\}$	: a message labelled by x
'ts'	: time-stamp for key timing
'ck'	: symmetric communication key used for message encryption and decryption
'nonce'	: a random number not being used more than once for countermeasure of replay attack
T_{exp}	: expiration time of a session key
$[m]_K$	: a message 'm' enciphered under symmetric key K
$\Pi(.)$	: a point representation function: $E/F \mapsto Z_p^*$
$[x \mapsto y, \{z\}]$	: x sends y Message $\{z\}$

if an MS is located within a given VLR coverage area, then this MS's LP is violated. Furthermore, if the MS can be tracked within a VLR coverage area, then this MS's intra-VLR IP is violated. Likewise, if the MS can be tracked among VLRs, then this MS's inter-VLR IP is violated.

PAE is relatively easier to achieve. However, encryption or simple randomization may not be sufficient noting that an eavesdropper can recognize the pattern of encrypted data using some traffic analysis tool, and it can then infer a mobile user's movement and whereabouts from this information. For example, in Ref. [15], each MS is associated with a static unique K which is derived from an exponent of a random number, and this same K is used to authenticate itself to different VLRs until HLR updates the shared secret with the MS. An eavesdropper can certainly track an MS using this unique K. Therefore, the protocol in Ref. [15] cannot achieve LP or intra-VLR IP of PAE. One-time alias has been shown to be an effective approach for PAE [12], where a new alias is assigned to an MS after each authentication, and the alias mapping (merely two random numbers to an eavesdropper) is tracked by HLR and made available to MS. Furthermore, if VLR can be kept off the one-time alias mapping, this approach is able to achieve both PAFB and PAGB. This will be examined in details in Section IV.

We next analyze mobile privacy in 3GPP-AKA with regard to these three privacy levels as defined above. 3GPP-AKA consists of three components, namely, (1) distribution of authentication vectors, (2) challenge-response message exchanges between VLR and MS, and (3) resynchronization between MS and HLR. HLR generates a quintet as an authentication vector which comprises a random number, an expected response, a cipher key, an integrity key, and an authentication token. Cipher key and integrity key are for data communications between VLR and MS when the authentication process is completed successfully. The random number is generated by



$\{$G1$\}$:IMSI, IDH
$\{$G2$\}$:IMSI
$\{$G3$\}$:$AC = [$RAND, XRES, $CK, IK,$ AUTN$]$
$\{$G4$\}$:RAND, AUTN
$\{$G5$\}$:RES

Fig. 1. Message Exchange in 3GPP AKA

HLR for the purposes of key generation, challenge-response message exchanges and resynchronization if to be needed. The expected response and authentication tokens are used by VLR to check if an MS indeed possesses the secret key shared with HLR, and if it is properly synchronized with HLR.

In 3GPP-AKA, both HLR and MS maintain a counter of sequence numbers as denoted by SQN_{HLR} and SQN_{MS}, respectively, and in addition, MS and HLR share a secret key denoted by K. Let $f_K^i(.)(i = 1, 2, 3, 4, 5)$, $f_K^{1*}(.)$ and $f_K^{5*}(.)$ be collision-resistant hash functions using K, and denote AC as the authentication vector and AMF as the authentication key management field. Referring to Fig. 1, HLR performs the following tasks (H1), (H2) and (H3) on receipt of a connection request:

(H1) HLR generates a random number RAND

(H2) HLR computes $CK, IK, AK, \text{XRES}, \text{MAC}, \text{AUTN}, \text{AC}$ using (1) to (7) below, respectively:

$$CK = f_K^3(\text{RAND}) \quad (1)$$
$$IK = f_K^4(\text{RAND}) \quad (2)$$
$$AK = f_K^5(\text{RAND}) \quad (3)$$
$$\text{XRES} = f_K^2(\text{RAND}) \quad (4)$$
$$\text{MAC} = f_K^1(\text{SQN}_{HLR}, \text{RAND}, \text{AMF}) \quad (5)$$
$$\text{AUTN} = (\text{SQN}_{HLR} \oplus AK)|\text{AMF}|\text{MAC} \quad (6)$$
$$\text{AC} = (\text{RAND}, \text{XRES}, CK, IK, \text{AUTN}) \quad (7)$$

(H3) HLR increases SQN_{HLR} by 1 after each AC

Upon a service request from an MS and the availability of authentication vectors, VLR performs the following tasks (V1), (V2) and (V3):

(V1) VLR selects an authentication vector corresponding to MS

(V2) VLR sends MS a challenge comprising RAND and AUTN

(V3) VLR verifies the response from MS with XRES

Upon a challenge from VLR, the MS extracts RAND, and performs the following tasks (M1), (M2) and (M3):

(M1) MS computes AK using (3) and SQN using (8), then it verifies if SQN is larger than SQN_{MS}

$$\text{SQN} = (\text{SQN} \oplus AK) \oplus AK \quad (8)$$

(M2) MS computes MAC using (5) and verifies if it is consistent from what retrieved from AUTN

(M3) MS computes XRES using (4) and sends it as the response to the challenge from VLR

Refer to Ref. [3], [4] for details of 3GPP-AKA.

The part of 3GPP-AKA that is closely related to mobile privacy is the use of an international mobile subscriber identity (IMSI) and the sequence number. We next give a detailed account on these. IMSI is used by VLR and HLR in service request and authentication vector request to identify the MS. The sequence number in 3GPP-AKA is used to form the authentication token AUTN which further prevents an adversary to replay an old authentication vector. When an MS detects an SQN and it is smaller than the largest sequence number SQN_{MS} that this MS maintains (note that this could happen for reasons like out-of-order AC delivery), MS has to resynchronize with HLR. Referring to Fig. 2, on detection of a smaller sequence number from HLR, MS performs the following tasks ($\overline{M1}$) and ($\overline{M2}$):

($\overline{M1}$) MS computes S_{MAC}, AUTS using (9) and (10) below, respectively:

$$S_{MAC} = f_K^{1*}(\text{SQN}_{MS}, \text{RAND}, \text{AMF}) \quad (9)$$
$$\text{AUTS} = (\text{SQN}_{MS} \oplus f_K^{5*}(\text{RAND}))|S_{MAC} \quad (10)$$

($\overline{M2}$) MS sends AUTS to VLR

Upon receipt of the resynchronization request from MS, VLR performs the following task ($\overline{V1}$):

($\overline{V1}$) VLR forwards to HLR a message $(\text{AUTS}, \text{RAND})$

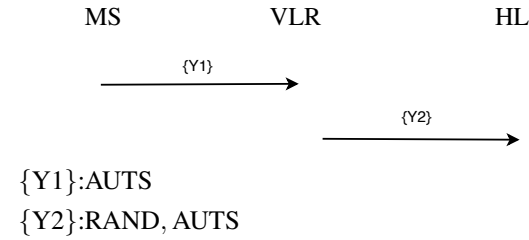


Fig. 2. Resynchronization of MS and HLR in 3GPP AKA

HLR then performs the following tasks ($\overline{H1}$), ($\overline{H2}$) and ($\overline{H3}$) to actually synchronize itself with MS on the sequence number:

($\overline{H1}$) HLR computes $f_K^{5*}(\text{RAND})$, then it recovers SQN_{MS} using (11) as follows:

$$\text{SQN}_{MS} = (\text{SQN}_{MS} \oplus f_K^{5*}(\text{RAND})) \oplus f_K^{5*}(\text{RAND}) \quad (11)$$

($\overline{H2}$) HLR computes S_{MAC} as in (9) and verifies if it is consistent with what extracted from AUTS

($\overline{H3}$) HLR sets $\text{SQN}_{HLR} = \max\{\text{SQN}_{MS}, \text{SQN}_{HLR}\}$

In 3GPP-AKA, once an enough number of authentication vectors is distributed to a VLR, the VLR does not need to talk with HLR while it continuously serves the MS, i.e., in an offline mode. Since VLR has to authenticate the MS for each session, the sequence number could put the MS in danger of intra-VLR IP violation of PAE. Due to the use of the anonymity key in 3GPP-AKA, these sequence numbers are concealed from an eavesdropper.

Since VLR knows the IMSI of an MS that it serves in 3GPP-AKA, it is clearly not able to achieve PAGB including LP and inter-VLR IP. Since IMSI is forced to be exchanged between MS and VLR, and the allocated temporary mobile subscriber identity (TMSI) by VLR can be correlated with the corresponding IMSI using a traffic analysis tool, an eavesdropper can infer if an MS is located in a given VLR. In the case of lost of synchronization, IMSI has to be sent unencrypted for resynchronization, and this may directly expose the unique IMSI. Therefore, 3GPP-AKA is not able to achieve LP or inter-VLR IP of PAE.

For the case of PAFB, although direct inference of MS's location seems not possible due to the use of anonymity keys on sequence numbers during authentication and resynchronization processes, an adversary at a false station can redirect an MS to an impersonated HLR via modifying IDH in the service request message $\{\text{G1}\}$ (as shown in Fig. 1). The impersonated HLR then acts as a legitimate VLR for the MS to send a $\{\text{G2}\}$ (as shown in Fig. 1) to the real HLR to obtain the cipher key and integrity key of the MS. Denote by IDF the identity of the false station with a false location register (FLR), this attack is detailed in Attack 1.

Attack 1: False base station attack to 3GPP-AKA

The attack follows these steps (F1) to (F6):

(F1) Adversary replaces IDH with IDF in $\{\text{G1}\}$

(F2) VLR sends $\{\text{G2}\}$ to FLR by following 3GPP-AKA

(F3) On receipt of {G2}, FLR acts as a legitimate VLR and sends a newly composed {G2} with a return address IDF set to HLR
(F4) On receipt of {G2}, HLR sends back FLR an array of authentication vectors
(F5) FLR extracts CK and IK from the authentication vectors and forwards these vectors to VLR
(F6) VLR then authenticates MS following the same steps taken by 3GPP-AKA ■

Remark 1: By Attack 1, FLR can obtain the exactly same information that a VLR can, and with CK and IK in possession, the adversary can decode the messages between MS and VLR.

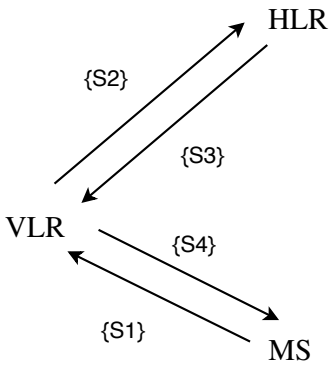
Using Attack 1, the adversary can then employ some directional beam-forming algorithm based on radio frequency signals received at multiple antennae spaced around half wavelength apart in a false base station [25], [26] to locate and track the MS, and it can resolve the distance with a precision within a hundred meter as long as the MS is within the coverage area of a given VLR. The adversary can follow the MS to adjacent VLR and apply Attack 1 there as well. Therefore, 3GPP-AKA does not have LP, inter-VLR IP, or intra-VLR IP of PAFB.

The association (in the view of an eavesdropper or VLR) of an MS to its HLR is also a piece of important privacy information, so does the association (in the view of the HLR) of an MS to its visited registers. Proxy to HLR or a similar approach using a Home Trusted Device (HTD) taken in Ref. [9] may not be practical to address this association privacy issue due to the scalability and additional security implication of an HTD. In specific, if a static HLR proxy is used, the association between the proxy and an MS is also vulnerable to a trace or traffic analysis attack, while non-static HLR proxy may lead to the exposure of the shared secret of mobile stations since this nomadic HTD needs the shared secret to perform authentication task. In practice, it seems that this problem is preferred to be addressed by protocol design on authentication. In Ref. [11], this association problem has been solved under the assumption that previously visited register must ensure the solvency of currently being visited register. If this chain of trust is broken (e.g. at a false base station), that protocol then cannot guarantee the location privacy of an MS. However, those techniques increase the complexity of location management services as an incoming connection may not be efficiently established. We shall add some more comments on this issue in Section V.

IV. Providing Strong Mobile Privacy with Efficient Authentication

We first give a brief review on EMAS [14]. Let Y be the certified public key of HLR whose private key is $x \in Z_p^*$ and $Y = xT \in E/F$. The additional public information Γ and the shared secret σ is generated and verified by following TDI as defined in Protocol 1 (cf. Appendix A).

Referring to Fig. 3, when the session key $K_{(V,H)}$ is created in advance before the authentication process, the proposed protocol consists of four messages as {S1}, {S2}, {S3}, {S4}. Message {S1} is for the request to communicating with VLR, as well as for the MS's authentication to VLR via trust delegation. Message {S2} is a request to HLR for the communication key with MS. Message {S3} is used to deliver the communication key back to VLR. Message {S4} authenticates VLR to MS. The authentication part of EMAS is called EMA and presented in Appendix B as Protocol 2. EMAS can provide mutual authentication between MS and HLR provided that VLR and HLR are mutually authenticated in advance (cf. Proposition 2 of Ref. [14]). There are one transmission and one reception needed on MS in EMAS and each message length is in $O(\log(p))$. MS needs to perform only one point scalar multiplication in actual authentication process. Hence a low-power MS can efficiently perform the authentication process.



$\mathcal{T}_{V,M} = \text{IDV}, \text{nonce}$
{S1}:$m_w, R, s, \text{IDH}, [ck, ts, T_{exp}, \text{nonce}]_\sigma, \text{nonce}$
{S2}:$\text{IDM}, [ck, ts, T_{exp}, \text{nonce}]_\sigma$
{S3}:$[\text{IDM}, T_{exp}, ts, ck, \text{nonce}]_{K_{(V,H)}}, [\mathcal{T}_{V,M}]_\sigma$
{S4}:$\text{IDH}, [\text{nonce}, \text{IDV}, [\mathcal{T}_{V,M}]_\sigma]_{ck}$

Fig. 3. Messages in EMAS

In EMAS, MS's identity IDM is put in the certificate by HLR to facilitate verification by any VLR, and the same public information Γ of MS is also displayed in the certificate. However, in order to use a one-time alias on MS, this information has to be replaced and made one-time use only. Due to the fact that Γ depends on IDM, once IDM is replaced by an alias, IDMA, Γ is automatically made one-time use.

For this one-time alias approach to work for EMAS, IDM from a legitimate MS needs to be made indistinguishable from an IDMA of any legitimate MS in the view of an eavesdropper or a VLR (honest or false). The above holds as long as IDMA and IDM is made indistinguishable to an eavesdropper and a VLR during the TDI execution of EMAS since EMA only depends on a newly shared secret σ', and a given pair of verifying information $(\Gamma', \text{IDX}, m_w)$, where IDX denotes an alias. In other words, all security properties of EMA (under a minor change) are intact when this pair of data replace the original σ and $(\Gamma, \text{IDM}, m_w)$, respectively. Here we have assumed that the probability to derive mobile identity information from its associated proxy constraint information

m_w is negligible.

To enable the one-time alias on MS, it seems desirable from an implementation standpoint to keep the shared secret σ intact and alter the public information Γ. However, we shall show in Section V that it may introduce security vulnerability to the underlying authentication scheme, and it has some other drawback as well. Instead, we work out a solution by performing these three different tasks, namely, (T1) generating alias, (T2) randomizing public information and corresponding shared secret, and (T3) securely delivering the newly shared secret to an MS.

We next show how (T1) and (T3) can be efficiently performed in EMAS followed by (T2). To perform (T1), let IDX be the previous used alias or IDM, the new alias is simply IDMA $= h(\text{IDX}) \in Z_p^*$. To perform (T3), note that there is a one-time secure simplex channel enabled by EMAS from HLR to MS during each authentication process in the form of $[\mathcal{T}_{V,M}]_\sigma$ as shown in Fig. 3, this secure channel is used to deliver the next round shared secret σ' by a simple piggyback of σ' inside $\mathcal{T}_{V,M}$ during the EMA protocol message exchanges. This message on piggyback also automatically synchronizes the HLR with MS on the new shared secret σ'. To finish (T3), MS needs to verify the correctness of σ' by checking (12), and the correctness of σ' follows the same argument as that presented in those comments in Ref. [14] following the protocol TDI.

$$h(\text{IDM}'|m_w)T = (\sigma' T) \uplus (h(\Pi(\Gamma'))Y) \uplus \Gamma' \tag{12}$$

To show how to generate σ' and the new associated public information for verification purpose by VLRs, the following formulae (13) and (14) are used, and they are essentially the same as (17) and (18) in Appendix A with κ' as another random number in Z_p^*, and x in (14) is also the same private key of HLR as that for EMAS.

$$\Gamma' = (h(\text{IDMA}|m_w)T) \uplus (\kappa' T) \tag{13}$$

$$\sigma' = (-x)h(\Pi(\Gamma')) - \kappa' \tag{14}$$

To finish (T2), after each authentication of MS, HLR updates the public entry for IDM as $(\Gamma', \text{IDMA}, m_w)$.

With the aforementioned change to TDI and EMA, the revised scheme (we still simply call it EMAS) can achieve PAE and PAGB at all levels of granularity due to the approach leading to the true disassociation of MS to its real identity. For PAFB, notice the fact that EMAS is invulnerable to false base station attack [14], with the above modification to TDI and EMA, the revised scheme can also achieve PAFB since an adversary which controls a false base station does not gain additional information. We next address some practical issues and discuss some drawback of EMAS and enhancement to EMAS with regard to privacy.

V. Discussions

It is tempting to make the shared secret intact for a new alias. In fact, this could be performed under the scheme presented in Ref. [15]. The steps are as follows. In order to maintain the same shared secret for each new alias, the delegation algorithm in TDI has to be changed in such a way that the shared secret σ linearly depends on the public information Γ as the approach taken in Ref. [15]. If this holds, then the problem turns into solving the following two equations (15) and (16) with two unknowns as κ' and Γ'. In general, these Γ' and κ' will correspond to the exactly same shared secret σ as before.

$$\kappa\Pi(\Gamma) = \kappa'\Pi(\Gamma') \tag{15}$$

$$\Gamma' = (h(\text{IDMA}|m_w)T) \uplus (\kappa' T) \tag{16}$$

However, such change would make the authentication scheme vulnerable to new cryptographic attacks as detailed analysis has been given in Ref. [19].

Since a VLR knows an MS's HLR to serve the MS, the association of an anonymous MS via its alias to its home register is still exposed in EMAS to a VLR as well as an eavesdropper. We refer this as the home association exposure (HAE) in the following discussion. Another privacy violation lies in the fact that HLR also knows for whom a VLR contacts the HLR. That is the MS's inter-VLR IP privacy is violated by its own HLR, i.e., inter-VLR PAHB.

For HAE, in Ref. [11], an alias for IDH is used when contacting HLR for authentication. However, this may render heavy burden on routing services as a destination address search (in the form of broadcast query message in the whole network) may be needed. In general, this may deserve more investigation, and it is out of the scope of this paper. When HLR completely lost tracking of its MS's, this could result in other problems. For example, to serve an incoming connection request (from other MS or from another type of terminals outside of the network), the location management service may not be able to route the data. In Ref. [11], nevertheless one partial solution is provided for inter-VLR PAHB. In EMAS, when the assumption that a chain of trust from HLR to successive VLRs holds, the alias generation, update of $(\Gamma', \text{IDMA}, m_w)$ and delivery of σ' can be instead performed by a trusted VLR. This is possible when VLR's private key replaces HLR's x in (14). In essence, a trusted VLR now serves as the new HLR for the MS. Since there is no false VLR under EMAS, such solution for PAHB in EMAS is viable as well. With this solution, the HAE problem is automatically solved as any HLR is now on a temporary basis. Another note is that the above technique would not be applicable if the shared secret σ had been maintained intact for each new alias.

Next, we analyze overhead on privacy protection of EMAS on HLR, VLR and MS in terms of communications and computation. First, there is no added message for privacy support in EMAS on MS and HLR. Only messages S3 and S4 contain a piggyback σ' in the EMA protocol of EMAS. The induced memory increase and communication overhead is small (roughly estimated being less than 1% for both). Second, the main overhead paid for privacy protection is on HLR on computation. Essentially, the previous long-term shared secret σ has to be updated per each authentication. The computation overhead on HLR has a cost in tantamount to TDI for each authentication process. This main cost consists of two point scalar multiplications, one point addition, and one multiplication in Z_p^* and one modular operations. The added

computation overhead on MS consists of two point scalar multiplications and two point additions for verification on σ' which takes time, for example, less than 25 microseconds in total on ARM SC200 (at 110 MHz clock rate) when an NIST B-163 anomalous binary curve curve is used. The cost added to a VLR is due to the need to query for the public certificate of IDMA per authentication process. As added overhead to an MS is low, and it is generally believed that HLR and VLR are not constrained on resources, the proposed privacy protection is viable in a mobile wireless network environment.

VI. Conclusions

In this paper, we studied the problem of mobile privacy in wireless networks. The major contribution of this paper is two-fold. First, we systematically studied the problem of mobile privacy protection in wireless networks from the perspectives of security, efficiency and flexibility, and we identified the weakness of the existing schemes including 3GPP-AKA. Second, we proposed a privacy protection for EMAS, and it employs one-time alias technique with a secure trust delegation mechanism.

Our proposed scheme does not introduce security vulnerability to the underlying authentication scheme and is able to conceal the real identity of the mobile station with respect to both eavesdroppers and visited (honest or false) location registers. Moreover, our scheme achieves identity concealment without sacrificing authentication efficiency. Due to the low complexity introduced to an MS, our scheme suits well to embedded low-power mobile devices.

References

[1] V.-S. Wong and V. Leung, "Location management for next generation personal communication networks," *IEEE Network*, vol. 14, no. 5, pp. 8–14, Sept./Oct. 2000.

[2] S. Tabbane, "Location management methods for third generation mobile systems," *IEEE Commun. Mag.*, vol. 35, no. 8, pp. 72–78, 1997.

[3] (2001) TS 33.102: Security architecture, version 4.2.0, release 4. Third Generation Partnership Project - Technical Specification Group.

[4] (2000) TR 33.902: Formal analysis of the 3G authentication protocol. Third Generation Partnership Project - Authentication and Key Agreement (AKA).

[5] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 734–742, Mar. 2005.

[6] Q. He, D. Wu, and P. Khosla, "Quest for personal control over mobile location privacy," *IEEE Commun. Mag.*, vol. 42, no. 5, pp. 130–136, 2004.

[7] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, Jan. 1988.

[8] D. A. Cooper and K. P. Birman, "Preserving privacy in a network of mobile computers," in *Proc. IEEE Symposium on Research in Security and Privacy*, 1995, pp. 26–38.

[9] S. Hoff, K. Jakobs, and D. Kesdogan, "Anonymous mobility management for third generation mobile networks," in *Proc. IFIP Communications and Multimedia Security*, 1996, pp. 72–83.

[10] R. Molva, D. Samfat, and G. Tsudik, "Authentication of mobile users," *IEEE Network*, vol. 8, no. 2, pp. 26–34, Mar./Apr. 1994.

[11] D. Samfat, R. Molva, and N. Asokan, "Untraceability in mobile networks," in *Proc. of International Conference on Mobile Computing and Networking*, 1995, pp. 26–36.

[12] A. Herzberg, H. Krawczyk, and G. Tsudik, "On travelling incognito," in *Proc. of IEEE Workshop on Mobile Systems and Applications*, 1994, pp. 205–211.

[13] M. J. Beller, L.-F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE J. Select. Areas Commun.*, vol. 11, no. 6, pp. 821–829, Aug. 1993.

[14] C. Tang and D. O. Wu, "An efficient mobile authentication for wireless networks (to appear)," *IEEE Trans. Wireless Commun.*

[15] W.-B. Lee and C.-K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," *IEEE Trans. Wireless Commun.*, vol. 4, no. 1, pp. 57–64, Jan. 2005.

[16] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in *Proc. of 3rd ACM CCS*, 1996, pp. 48–57.

[17] T. Okamoto, M. Tada, and E. Okamoto, "Extended proxy signature for smart card," in *LNCS 1729*. Spinger-Verlag, 1999, pp. 247–258.

[18] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strong non-designated proxy signature," in *LNCS 2119*. Springer-Verlag, 2001, pp. 474–486.

[19] G. Wang, F. Bao, J. Zhou, and R. H. Deng, "Security analysis of some proxy signatures," in *Proc. of Information Security and Cryptology (LNCS 2971)*. Springer-Verlag, 2004, pp. 305–319.

[20] K. Zhang, "Threshold proxy signature schemes," in *Proc. 1st International Information Security Workshop*, 1997, pp. 191–197.

[21] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal on Information Security*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[22] A. M. Odlyzko, "Discrete logarithm in finite fields and their cryptographic significance," in *Proc. of Eurocrypt*. Spinger-Verlag, 1985, pp. 224–314.

[23] C. Pomerance, "Analysis and comparison of some integer factoring algorithms," in *Computational Methods in Number Theory (ed. by H. W. Lenstra, Jr. and R. Tijdeman)*. Mathematisch Centrum, Amsterdam, 1982, pp. 89–139.

[24] E. Teske, "Square-root algorithms for the discrete logarithm problem," in *Public-Key Cryptography and Computational Number Theory*. Walter de Gruyter, Berlin - New York, 2001, pp. 283–301.

[25] J. Zagami, S. Parl, J. Bussgang, and K. Melillo, "Providing universal location services using a wireless E911 location network," *IEEE Commun. Mag.*, vol. 36, no. 4, pp. 66–71, 1998.

[26] L. C. Godara, "Application of antenna arrays to mobile communications, part ii: Beam-forming and direction-of-arrival considerations," *Proceedings of the IEEE*, vol. 85, no. 8, pp. 1195–1245, Aug. 1997.

Appendix A: TDI - Trust Delegation Initialization of EMAS

Protocol 1: TDI

1. [at HLR] HLR performs the following steps:
   - sets key usage restrictions on IDM in m_w
   - converts $(\text{IDM}|m_w)$ to an element in Z_p^*, and computes $h(\text{IDM}|m_w)$
   - selects a random number $\kappa \in Z_p^*$, and produces (Γ, σ) (where $\Gamma \in E/F$ and $\sigma \in Z_p^*$) as follows:

$$\Gamma = (h(\text{IDM}|m_w)T) \uplus (\kappa T) \text{ (in } E/F) \quad (17)$$

$$\sigma = -xh(\Pi(\Gamma)) - \kappa \text{ (in } Z_p^*) \quad (18)$$

     where, $h(\Pi(\Gamma))$ in (18) is performed in Z_p^* after the mapping on an appropriate point representation of Γ.
   - puts $(\Gamma, \text{IDM}, m_w)$ in public.
   - delivers (σ, m_w) to MS securely.
2. [at MS] MS accepts the delegation key σ if (19) holds.

$$h(\text{IDM}|m_w)T = (\sigma T) \uplus (h(\Pi(\Gamma))Y) \uplus \Gamma \quad (19)$$

where, (19) is evaluated in E/F. ■

Appendix B: EMA - Efficient Mobile Authentication of EMAS

Protocol 2: EMA

1. [at MS]: MS picks two random numbers $k, \mathcal{N} \in Z_p^*$, and generates the communication key ck (upon one session use or timing based invalidation), then computes R and s as in (20) and (21), respectively.

$$R = kT \qquad \text{(in } E/F\text{)} \qquad (20)$$

$$s = \sigma - kh(\Pi(R)|\mathcal{N}) \qquad \text{(in } Z_p^*\text{)} \qquad (21)$$

   - MS generates a certificate $[ck, ts, T_{exp}, \mathcal{N}]_\sigma$ and then composes $\{\text{S1}\}$ as shown in Fig. 3.
   - [MS $\mapsto$ VLR, $\{\text{S1}\}$]: MS initiates the protocol by sending $\{\text{S1}\}$.
   - [VLR $\mapsto$ MS, $\{\text{S4}\}$]: MS decodes $\{\text{S4}\}$ for IDV, $\mathcal{N}$, and checks if nonce is consistent.

2. [at VLR]: on receipt of message $\{\text{S1}\}$, VLR checks warrant m_w for restrictions and verifies if (22) holds

$$(sT) \uplus \Gamma \uplus (h(\Pi(\Gamma))Y) \uplus (h(\Pi(R)|\mathcal{N})R) = h(\text{IDM}|m_w)T \qquad (22)$$

   - VLR composes $\{\text{S2}\}$ on receipt of $\{\text{S1}\}$, and composes $\{\text{S4}\}$ on receipt of $\{\text{S3}\}$.
   - [VLR $\mapsto$ HLR, $\{\text{S2}\}$]: VLR requests to HLR for a communication key with MS.
   - [HLR $\mapsto$ VLR, $\{\text{S3}\}$]: VLR decodes $\{\text{S3}\}$ for ck, and checks expiration timestamp and consistence of nonce.
   - [VLR $\mapsto$ MS, $\{\text{S4}\}$]: VLR authenticates to MS via sending $\{\text{S4}\}$ which is encrypted by the communication key ck which can be decrypted by MS.

3. [at HLR]:
   - [VLR $\mapsto$ HLR, $\{\text{S2}\}$]: HLR processes $\{\text{S2}\}$ using σ, then retrieves $K_{(V,H)}$ and validates restrictions on m_w (saved copy at HLR for IDM during parameter generation phase) of IDM.
   - HLR composes $\{\text{S3}\}$ using σ and $K_{(V,H)}$.
   - [HLR $\mapsto$ VLR, $\{\text{S3}\}$]: HLR forwards the communication key. ■

Caimu Tang (S'97–M'05) received B.S. in Applied Mathematics from Xi'an Jiaotong University, Xi'an, China, in 1990, M.S. in Computer Science from Wayne State University, Detroit, Michigan, in 1997, and Ph.D. in Computer Science from University of Southern California, in 2005. From Aug. 2005 to April 2006, He was with Rockwell Scientific Company at Thousand Oaks, CA, as a research scientist. From Aug. 2006 to June 2007, he was with Tut Systems, Lake Oswego, OR, as a staff engineer. Since June 2007, he has been with Pathfinder Energy Services, Houston, TX, as a DSP engineer. His research interests are in the areas of source coding, network security, signal processing for real-time measurement/logging-while-drilling, video coding/transcoding, and wireless communications.

Dapeng Oliver Wu (S'98–M'04–SM'06) received B.E. in Electrical Engineering from Huazhong University of Science and Technology, Wuhan, China, in 1990, M.E. in Electrical Engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1997, and Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University, Pittsburgh, PA, in 2003.

Since August 2003, he has been with Electrical and Computer Engineering Department at University of Florida, Gainesville, FL, as an Assistant Professor. His research interests are in the areas of networking, communications, multimedia, signal processing, and information and network security. He received NSF CAREER award in 2007, the IEEE Circuits and Systems for Video Technology (CSVT) Transactions Best Paper Award for Year 2001, and the Best Paper Award in International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine) 2006.

Currently, he serves as the Editor-in-Chief of Journal of Advances in Multimedia, and an Associate Editor for IEEE Transactions on Wireless Communications, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transactions on Vehicular Technology, and International Journal of Ad Hoc and Ubiquitous Computing. He is also a guest-editor for IEEE Journal on Selected Areas in Communications (JSAC), Special Issue on Cross-layer Optimized Wireless Multimedia Communications. He has served as Program Chair for IEEE International Conference on Communications (ICC 2008), Signal Processing for Communications Symposium, and as a member of executive committee and/or technical program committee of over 50 conferences. He is Vice Chair of Mobile and wireless multimedia Interest Group (MobIG), Technical Committee on Multimedia Communications, IEEE Communications Society. He is a member of the Best Paper Award Committee, Technical Committee on Multimedia Communications, IEEE Communications Society.