A NEW AUTHENTICATION PROTOCOL FOR PORTABLE COMMUNICATION SYSTEMS

Sheng-bo Xu
Department of Mathematics and Computing Science
Eindhoven University of Technology, P.O. Box 513
5600 MB Eindhoven, the Netherlands
E-mail: sbxu@win.tue.nl

Cees Jansen
Philips Crypto B.V., De Witbogt 2
P.O.Box 218, 5600 MD Eindhoven, the Netherlands
E-mail: cja@IAEhv.nl

Henk van Tilborg
Department of Mathematics and Computing Science
Eindhoven University of Technology, P.O. Box 513
5600 MB Eindhoven, the Netherlands
E-mail: henkvt@win.tue.nl

Abstract With the global deployment of portable communication systems and the ongoing developments in this area, one expects more and more sophisticated security features to be provided such as entity authentication, robust user identity confidentiality and non-repudiation services. Motivated by these new security requirements, this article analyzes the security of authentication protocols in several mobile communication industry standards, such as DAMPS, GSM, and TETRA, and several proposals for future mobile communication systems. A new authentication protocol is presented to provide the above security services using symmetric cryptographic techniques only. The security and complexity of the new protocol are analyzed and compared with the aforementioned protocols.

B. Preneel (ed.), *Secure Information Networks*

1. INTRODUCTION

Portable communication systems (PCS) are playing a more and more important role in the telecommunication industry nowadays, and are expected to put ubiquitous wireless telephony into widespread public use. However, wireless communication is inherently more vulnerable to breach of privacy than wire-line communication because wireless communication can be intercepted without any physical tap. Also, wireless networks are more likely subjected to fraud than their wire-line counterparts for similar reasons. Therefore, it is important for PCS to provide privacy (of conversation and location) and fraud control comparable to or even better than that of the wire-line network.

Due to limitations of technology and implementation techniques, the first-generation PCS adopted non-cryptographic means to control privacy and authentication. The authentication of the telephone placing the call was implemented through a Number Assignment Module (NAM) and an Electronic Serial Number (ESN) [5]. Since ESN and phone number are transmitted in clear in these systems, it would be very easy to clone the phone and thus cause several millions of dollars loss of benefit to operators every year. Moreover, as the conversation through the wireless channel was transmitted in clear, the first generation PCS failed to provide both privacy of conversation and fraud control.

In the 80's, the communication technology, digital signal processing, computer, and VLSI techniques matured to a level, that enabled feasible introduction of cryptographic methods into the second-generation PCS. In these systems encryption mechanisms are used to protect the conversation and/or some sensitive signal information transmitted over the radio channel, whereas authentication mechanisms are employed to identify the subscriber who is requesting the service. Considerations on the portable's hardware complexity, battery power, and connection set-up time (validation delay) have restricted a mobile unit from performing computations that require expensive hardware or are time-consuming (i.e., high power consumption). Because of the ease of implementation of symmetric cryptographic methods, the encryption algorithms and authentication protocols used in existing standards in the mobile communication industry, such as, DAMPS [8], GSM [9], and TETRA [10], all are based on symmetric cryptography. The application of cryptographic methods has effectively reduced the interception of conversation and the placement of fraud calls and clearly gives the second generation PCS a substantially higher level of security than its predecessor. In addition, the 2nd generation PCS employs a mechanism to protect the user's real identity, called temporary mobile subscriber identity (TMSI).

With the further development of PCS, the third-generation PCS are expected to provide multimedia communication services and support IP access. Some additional security features are also expected to be incorporated in the third generation PCS. One of the most important new security features is mutual authentication between a mobile user and a network. In GSM and DAMPS, users cannot authenticate the network, and, as a consequence, intruders are able to masquerade as network operators or service providers. TETRA has already used two-way authentication protocols, and therefore users can be sure that they are connected to the network of a trusted operator. This becomes increasingly important as the number of competing public and private network operators and service providers grows larger. TETRA uses symmetric cryptographic methods to implement mutual authentication between user and network. Over time, several people have attempted to implement the direct mutual authentication between the portable and network using asymmetric cryptographic methods. Beller *et al.*, [2, 3], proposed several authentication protocols based on Modular Square Root (MSR) and/or ElGamal signature scheme. Carlsen, [6], proposed some enhancements to the protocols in [2]. Xu and Wang , [19], improved the protocol in [3]. In addition, it is worth noting that the ASPeCT project [1] has systematically studied the authentication framework based on the public-key cryptosystems and also discussed how to provide end-to-end services using trusted third parties in the third generation PCS.

Another new security requirement is non-repudiation of services. For a network operator, it is desirable that mobile users cannot deny the charges over the services they requested. Similarly, mobile users should not be wrongly charged due to any billing error or security breach by the serving network. This requirement is motivated by the observation that the service of mobile communication systems is provided by multiple regional networks, each operating under a different administration. Therefore, it is necessary to provide undeniable evidence to resolve possible disputes on billing. There have been some articles discussing how to provide non-repudiation services in PCS [13, 15, 16, 20]. Preneel *et al.*, [13, 16], suggest to adopt public-key digital signatures to provide the non-repudiation service whereas the other articles, [15, 20], describe how to implement non-repudiation through public/private-key hybrid techniques. Also, a more robust user identity confidentiality can easily be provided if public-key cryptographic methods are employed. In addition, Y. Mu and V. Varadharajan [18] proposed the *subliminal identity* concept to provide users' identity confidentiality, which is different from TMSI in GSM.

In this paper, we discuss how to implement the aforementioned security requirements based on symmetric cryptographic techniques. In the second section, we give a brief introduction of PCS. In the third section, the security of authentication protocols in DAMPS, GSM, and TETRA, and several proposals for future mobile communication systems are analyzed. In the forth section, we introduce a new authentication protocol using symmetric cryptographic methods only. In the fifth section, we analyze the security and complexity of the new protocol.

2. A SIMPLE MODEL FOR PCS

The service of PCS is usually provided by multiple regional networks, each operating under a different administration. In the discussion of security in PCS, we use a simple model with four entities, and follow the terminologies of GSM [9]. Mobile Station (MS) stands for a user who is authorized to use particular network services. A Visitor Location Register (VLR) is an entity providing network capabilities to support particular services, and allowing MSs to use network services. A Home Location Register (HLR) is an entity responsible for the provision of particular services to MSs through VLRs. VLRs and HLRs typically cooperate by means of contractual relationships. An intruder is an entity that abuses the network infrastructure or services on the network. In the following, we will exemplify GSM to explain the relationship among MS, VLR and HLR.

In GSM, each MS registers with a HLR. The HLR issues MS an identity number, called International Mobile Subscriber Identity (IMSI), and a secret key K_i by means of MS' Subscriber Identity Module (SIM) card. SIM card is a kind of smart card, which can execute the authentication algorithm (also called A3 algorithm) and key generation algorithm (also called A8 algorithm) when MS authenticates itself to a VLR. Usually HLR produces the authentication triplet ($RAND$, $SRES$, K_c), where $RAND$ is a random number, $SRES = A3(RAND, K_i)$ is the authentication response, and $K_c = A8(RAND, K_i)$ is the session key. When VLR authenticates MS, it loads MS' authentication triplet ($RAND$, $SRES$, K_c) from HLR. The authentication protocol is listed in Table 1.

When MS has access to network services for the first time, MS needs to transmit IMSI in clear to VLR. If the first authentication succeeds, VLR will issue TMSI to MS. Since then, MS will transmit TMSI to VLR.

Encryption of the conversation on a radio channel is optional in GSM. When MS wants to use the encryption mode, it needs to calculate the session key K_c and inform VLR. Since MS and HLR use the same key

Table 1 Table 1. Authentication protocol in GSM

1.	$MS \rightarrow VLR$	:	TMSI(IMSI)
2.	$VLR \rightarrow MS$	:	RAND
3.	$MS \rightarrow VLR$	:	SRES

generation algorithm and parameters, $RAND$ and K_i, the generated session keys must be same.

DAMPS and TETRA also adopt simple challenge-response authentication protocols like GSM. The difference is that VLR may authenticate MS directly using SSD in DAMPS [8] and K_s in TETRA [10]. These are derived from MS' secret key by HLR and sent to VLR. Mitchell and Chen also adopt this authentication mode in their symmetric techniques based authentication protocol proposed for the future mobile communication systems [17].

3. SECURITY ANALYSIS OF THE ABOVE AUTHENTICATION PROTOCOLS

In this section, we analyze the security of authentication protocols in DAMPS, GSM, TETRA, and several proposals for future mobile communication systems.

3.1 ENTITY AUTHENTICATION

In the aforementioned authentication protocols, VLR authenticates MS using a random number as challenge. Only the legal MS can calculate the correct response using its K_i in GSM, SSD in DAMPS and K_s in TETRA. VLR authenticates MS by checking if the response is fresh and correct, which may defeat effectively intruders abusing the network services and their impersonation attacks.

However, the authentication protocols in GSM and DAMPS are one-way: VLR can authenticate MS, but MS cannot authenticate VLR. Thus there exists some possibility for intruders masquerading a VLR to cheat MS and obtain authentication parameters from MS. Then the intruder may use the obtained valid authentication parameters to pass the check of VLR. In TETRA, an independent protocol is provided for MS to verify the serving network. Invoking this protocol is optional.

In addition, the above authentication protocols don't consider the mutual authentication between HLR and VLR. There are possible threats to VLR and HLR from intruders, such as, intercepting communication between VLR and HLR, impersonating HLR to VLR, and impersonating VLR to HLR. Mitchell and Chen have studied these threats in detail [17]. If one of these threats is carried out, the security of the network will be completely lost.

3.2 IDENTITY CONFIDENTIALITY

Users' identity privacy may protect users against tracing their physical location by illegal means. DAMPS adopted the same temporary identity method as GSM to provide users' identity and location confidentiality. However, as illustrated in Section 2, an MS in GSM has to send its IMSI in clear to VLR when it has access to a VLR for the first time. Also, when a roaming MS has lost connection with VLR or when VLR has lost MS' TMSI, MS will need to send its IMSI to register with the VLR again.

Current GSM and DAMPS networks may provide a level of users' identity and location confidentiality. However, the above mechanism is less appropriate for future networks because of the multi-operator environment likely to prevail. New mechanisms have been studied based on public-key cryptographic techniques [2, 3, 15]. In addition, Y. Mu and V. Varadharajan proposed *subliminal identity* concept [18], which is issued by HLR instead of VLR.

3.3 NON-REPUDIATION OF SERVICES

The current authentication protocols in GSM, DAMPS, and TETRA cannot resolve possible disputes on billing if users claim wrong bills resulting from a network security breach. Also, there do exist some potential threats in these systems. In GSM, HLR might transfer a user's secret key K_i to VLR in some special situations, such as, a communication link between VLR and HLR isn't available for some time. In DAMPS and TETRA, authentication keys are derived by HLR from MS' secret key and sent to the VLR which MS is visiting. In the multi-operator environment, each VLR might be operated under a different administration with a different level of protection. Some networks are more vulnerable than others to attacks from intruders. Once authentication triplets or authentication keys are compromised by an intruder, fraudulent calls can always happen.

Secure billing has drawn the attention of some researchers and standardization organizations. Preneel *et al.,* [13, 16], studied how to integrate micropayment systems into authentication protocols based on public-key cryptographic techniques. In their protocols, a digital signature is used to provide the non-repudiation of service. Lin and Harn [15] proposed to achieve non-repudiation of services in authentication protocols using one-way hash functions and public-key cryptographic techniques. However, their non-repudiation mechanism cannot provide enough evidence to resolve the following dispute: MS has used network services but claims that communication is disrupted after it has submitted the non-repudiation response. Zhou and Lam [20] proposed to use Lamport's hash-chain [14] and digital signature to improve the above protocol. However, their *Service Request Protocol* cannot defeat a *replay attack*: intruders intercept MS' responses and replay it to VLR to pass VLR's check. This is because there is no fresh element in MS' signature except for MS' temporary identity U_F. To avoid several services requests being linked to the same temporary identity, they suggested to update U_F according to the following method

$$U_F^{new} = H(K_{UF}, U_F^{old}),$$

where $H(X)$ is a one-way hash function of message X and K_{UF} is the authentication key shared by MS and VLR. However, they just update U_F after *completion* of the service. Hence, intruders may proceed the replay attack when MS is using network services.

4. NEW AUTHENTICATION PROTOCOL

The new protocol aims to implement the following security features: entity authentication, users' identity confidentiality, non-repudiation of services, and secret session key establishment. To keep the new protocol light-weighted regarding the computation complexity, only symmetric cryptographic techniques, such as the Message Authentication Code (MAC) and one-way hash function, are used.

4.1 NOTATION

Suppose MS has registered with a HLR. HLR assigns MS a secret key K_{mh} and a temporary identity TID. Suppose HLR and VLR have signed a roaming agreement and they share a secret key K_{hv}. Following is a list of other notations used in the new protocol.

- K_{mv}: a temporary authentication key distributed by HLR for MS and VLR.

- NID: MS' temporary network identity issued by VLR after successful registration authentication, and updated by VLR after every successful call authentication.

- R_v: a random number chosen by VLR and broadcasted to MS through Base Station (BS).
- $E_K(x)$: a conventional encryption operation on message x using key K.
- $RES_{M,V}$: a response calculated by M using V's secret key K and challenges x from M and V by means of a secure MAC algorithm, denoted as $MAC_K(x)$.
- $H(x)$: a one-way hash function of message x.
- $x|y$: concatenation of messages x and y.

4.2 AUTHENTICATION MODEL

The new protocol includes two parts: Registration Authentication Protocol (RAP) and Call Authentication Protocol (CAP). The RAP will be executed among MS, VLR and HLR when MS is registering at a VLR. After successful registration at VLR, MS will execute the CAP when it wants to use network services.

According to security assumptions in Section 4.1, both MS and VLR trust HLR. With the help of HLR, MS and VLR may establish a trust relationship and share a temporary authentication key K_{mv} after executing the RAP. On account of the link connection situation in PCS, RAP will adopt the pull authentication mode in [4]. In the CAP, MS and VLR can authenticate each other using K_{mv}.

As for the non-repudiation of services, MS can use K_{mh} to produce an undeniable response and insert it into the request of services. VLR can check the response with the aid of HLR, but VLR cannot produce it. This is the basic idea of undeniable billing mechanism. We adopt Lamport's hash-chain [14] to implement the above mechanism.

Lamport's hash-chain can be constructed by recursively applying an input string to a one-way hash function, which can be denoted as $H^i(X) = H(H^{i-1}(X))$ ($i = 1, 2, \cdots$,c) where $H^0(X) = X$. According to the feature of one-way hash function, if X is chosen randomly and the hash chain is kept secret, given $H^i(X)$ it is computationally infeasible to find the input $H^{i-1}(X)$ except the originator of the hash chain.

Lamport's hash-chain has been adopted by several authentication protocols [12, 20]. The new protocol uses it to implement the undeniable billing in the following way. In the RAP, HLR chooses c, and performs the following calculations:

$$S_0 = H(K_{mh} \oplus TID'), S_1 = H(S_0), \cdots, S_C = H(S_{c-1})$$

where TID' is MS' new temporary identity. HLR sends S_c to VLR and sends TID' and c to MS. MS may do the same calculation as HLR, but VLR cannot. When MS begins to use network services in the CAP, it sends a request including S_{c-1} to VLR with the help of temporary authentication key K_{mv}. VLR can check the authenticity of MS' request by calculating and comparing $S_c = H(S_{c-1})$. Next time, MS may use S_{c-2}, S_{c-3}, and so on. Since VLR cannot produce S_i $(i = 1, 2, \cdots, c-1)$ and cannot obtain S_{i-1} from S_i, VLR may submit MS' request including the hash-chain value to HLR as bill's evidence.

4.3 REGISTRATION AUTHENTICATION PROTOCOL

The main goals of the RAP include entity authenticating, provision of necessary parameters for undeniable billing, and distribution of the temporary authentication key for MS and VLR. The concise authentication protocol is listed in Table 2.

Table 2 Table 2. Registration authentication protocol

1.	$MS \rightarrow VLR$	:	TID, HLR, R_v, RES_{mh}
2.	$VLR \rightarrow HLR$	:	$VLR, TID, R_v, RES_{mh}, RES_{vh}$
3.	$HLR \rightarrow VLR$	:	$E_{K_{mh}}(R_v \mid c \mid TID' \mid K_{mv}), E_{K_{hv}}(R_v \mid S_c \mid K_{mv})$
4.	$VLR \rightarrow MS$	:	$E_{K_{mh}}(R_v \mid c \mid TID' \mid K_{mv}), E_{K_{mv}}(TID \mid NID)$

Step 1. MS calculates a response $RES_{mh} = MAC_{K_{mh}}(R_v|TID)$, and transmits it with TID, HLR, and R_v as a request to VLR.

Step 2. VLR calculates a response $RES_{vh} = MAC_{K_{hv}}(R_v|TID)$, and transmits it with TID, R_v, and RES_{mh} to HLR.

Step 3. HLR first authenticates MS and VLR by checking RES_{mh} and RES_{vh}. If these two responses are correct and fresh, HLR chooses a random number as K_{mv} and an initial value c for MS' call counter, refreshes MS' temporary identity with TID', and calculates hash-chain (S_0, S_1, $\cdots$, S_c) as illustrated in the subsection 4.2. Then HLR encrypts R_v, c, TID' and K_{mv} using K_{mh}, and encrypts R_v, S_c and K_{mv} using K_{hv}. Finally, HLR transmits two ciphertexts to VLR.

Step 4. VLR first decrypts $E_{K_{hv}}(R_v|S_c|K_{mv})$ using K_{hv} and authenticates HLR by checking if R_v occurs in the plaintext. If so, VLR draws S_c and K_{mv} from the plaintext. Then VLR issues MS a network identity (NID), and encrypts TID and NID using K_{mv}. Finally, VLR sends $E_{K_{mh}}(R_v|c|TID'|K_{mv})$ and $E_{K_{mv}}(TID|NID)$ to MS.

MS first decrypts $E_{K_{mh}}(R_v|c|TID'|K_{mv})$ using K_{mh}, and authenticates HLR by checking if R_v occurs in the plaintext. If so, VLR draws c, TID' and K_{mv} from the plaintext. Then MS decrypts $E_{K_{mv}}(TID|NID)$ using K_{mv}, and authenticates VLR through checking if TID occurs in the plaintext. Finally, MS calculates the hash-chain (S_0, S_1, $\cdots$, S_c) in the same way as HLR, stores its new TID', NID and hash-chain, and initializes the call counter with $c-1$.

4.4 CALL AUTHENTICATION PROTOCOL

After registration with the VLR, MS may execute CAP with VLR when it wants to use network services. Suppose the current value of the call counter is $c-i$.

Table 3 Table 3. Call authentication protocol

1.	$MS \rightarrow VLR$	:	$NID, E_{K_{mv}}(R'_v|S_{c-i})$
2.	$VLR \rightarrow MS$	:	$E_{K_s}(S_{c-i}|NID')$

Step 1. MS encrypts VLR's new challenge R'_v and S_{c-i} using K_{mv} as a request, and transmits it with NID to VLR.

Step 2. VLR loads hash-chain value S_{c-i+1} and K_{mv} according to NID, and decrypts $E_{K_{mv}}(R'_v|S_{c-i})$ using K_{mv}. VLR authenticates MS by checking if R'_v occurs in the plaintext. If so, VLR compares if $S_{c-i+1} = H(S_{c-i})$. If equality holds, VLR calculates the session key $K_s = H(S_{c-i} \oplus R'_v)$, updates MS' NID with NID', and refreshes old hash-chain value S_{c-i+1} with S_{c-i}. Then VLR encrypts S_{c-i} and NID' using K_s, and sends the ciphertext to MS.

Since MS may compute K_s in the same way as VLR, it can authenticate VLR by checking if S_{c-i} occurs in the plaintext. If so, MS will refresh its NID with NID' and decrements the counter. Then MS starts secure access to network services, and sends the new hash-chain value $S_{c-i-j} \oplus R''_v$ ($j = 1, 2, \cdots$) to VLR under the protection of K_s to VLR at a pre-defined interval T during services. VLR checks if the new hash-chain value is valid according to the same method as illustrated above. After every successful check of hash chain value, VLR will refresh the old hash-chain value with new one. If VLR hasn't received S_{c-i-j}, or received a incorrect value, VLR will cut off the service.

In the case MS has sent *message* 1 to VLR but VLR doesn't receive it, or VLR has sent *message* 2 to MS but MS doesn't receive it, MS would continue executing the CAP to send the request using the same S_{c-i} and new challenge from VLR until MS and VLR establish the synchronism. When the hash-chain has been used up, MS has to execute the RAP to get new authentication parameters.

5. ANALYSIS OF NEW PROTOCOL

5.1 SECURITY ANALYSIS

Entity authentication: Both RAP and CAP use a challenge-response authentication mechanism. Only valid MS, VLR and HLR can calculate correct responses, ciphertexts and plaintexts because only they know secret keys K_{mh}, K_{hv}, and K_{mv}. Thus the new protocol achieves the entity authentication among MS, VLR and HLR. Also, challenges R_v and R'_v are fresh random numbers, and TID is also fresh because it will be changed by HLR after every successful authentication to MS and only HLR and MS know TID. Thus the new protocol effectively defeats replay attacks. In addition, two-way authentications among MS, VLR and HLR defeat active impersonation attacks for MS, VLR and HLR.

Users' identity confidentiality: In the RAP and CAP, two different temporary identities TID and NID are issued and updated after each successful authentication by HLR and VLR, respectively. TID and NID are used only once in the RAP and CAP, which guarantees MS' identity is kept secret from eavesdroppers. Even the VLR doesn't know the MS' real identity.

Non-repudiation of services: As showed in Section 4.2 and 4.4, the billing information collected by VLR contains sufficient evidence to make a bill undeniable. On the other hand, without the knowledge of TID' and K_{mh}, VLR cannot calculate the hash-chain as MS and HLR can. Also, the one-way property of $H(X)$ makes it computationally infeasible for VLR to get S_{c-1} from the S_c.

Session key establishment: In the CAP, K_s is the hash value of a bit-wise exclusive-or of a fresh challenge R'_v and the new hash-chain value S_{c-i}. Although an intruder may intercept R'_v, it doesn't know S_{c-i}. No one but MS and VLR (and HLR) can obtain the correct K_s.

Other attacks' analysis: Although the CAP works like the S/Key user authentication scheme [12], MS doesn't need VLR to remind of the counter value and seed in the CAP. Actually VLR doesn't know these values. Thus, the CAP defeats the so-called *host-impersonation attack* [7]. In addition, the secret 64-bit key shared by user and host in the S/KEY scheme is derived from a *pass-phrase* of arbitrary length, which is vulnerable to the off-line password guessing attack. As illustrated in Section 4.2, the hash-chain is calculated from MAC value of TID' using

K_{mh}. Neither K_{mh} nor TID' is derived from any password. So the new protocol is immune from the off-line password guessing attack whereas the S/Key scheme is not.

5.2 COMPLEXITY ANALYSIS

As claimed, we have only used symmetric cryptographic techniques to design the RAP and CAP, and achieve expected security features. Obviously, the computation complexity of the new protocol is lower than authentication protocols based on public-key cryptographic techniques. In the following, we mainly compare the new protocol with authentication protocols based on private-key and/or hybrid cryptographic techniques.

The RAP needs to do a little more computation than protocols in [8, 9, 10, 17] because the it implements mutual authentications among MS, VLR and HLR. As illustrated in [17], the entity authentications of VLR and HLR are necessary to defeat the intruder's impersonations of VLR and HLR. In the new protocol, however, the RAP is executed only when MS has to register with a new VLR or hash-chain values have been used up. After registration, the CAP is executed between MS and VLR to implement the mutual authentication and distribution of a session key. In the CAP, MS only needs to do one encryption, one decryption and one hash operation.

In the new protocol, VLR only needs to fetch and store the authentication parameter S_c for MS from HLR in the RAP, not the authentication triplets $(RAND, SRES, K_c)$ in GSM. Also, VLR may refresh the authentication parameters S_i using the new valid hash-chain value from MS in the CAP. Thus VLR doesn't need to load authentication parameters from HLR after the registration. In GSM, VLR may fetch five authentication triplets each time. Thus, the new protocol reduces the number of communication between VLR and HLR to a large extent. In addition, the new protocol reduces the number of authentication parameters in the transmission and storage.

The new protocol has lower computation complexity than the protocols in [15, 20] based on public-key/private-key hybrid cryptographic techniques. Like the protocols in [15, 20], however, the new protocol needs uses to store the hash-chain values. In order to defeat the birthday attack on hash-chain values, it is better to choose a hash value of sufficient length, for instance 16 bytes. Suppose T is 6 seconds. Then MS needs 600 hash-chain values for one hour's services. Thus MS needs 9.6K bytes of memory. The average EEPROM size in current smart cards is about 4-8K bytes. A suggestion of the solution to the storage problem: MS divides the hash-chain into several sub-chains. Every subchain has 100 values. MS only stores the originator of each sub-chain. When MS needs the hash-chain values in the CAP, it will recover them from the originator of some subchain. Thus HLR may choose c large enough to provide the necessary hash-chain values for MS when it is visiting the VLR. This is an efficient method to save memory at the cost of computation time.

6. CONCLUSIONS

With the further development of PCS, one expects more and more sophisticated security features to be provided. This article analyzed the security of authentication protocols in DAMPS, GSM, and TETRA, and several proposals for future mobile communication systems, and pointed out their shortcomings. A new authentication protocol is presented to provide the following security features: entity authentication, users' identity confidentiality and non-repudiation services using symmetric cryptographic techniques only. Security and complexity of new protocol have been analyzed and compared with aforementioned protocols. The results show that new protocol has low computational complexity while it keeps security as high as possible.

Acknowledgments

We are very grateful to the anonymous referees for their valuable comments, and to Joris Claessens for the proper style format.

References

[1] ACTS project AC095, Advanced Security for Personal Communication Technologies. *http://www.esat.kuleuven.ac.be/cosic/aspect/.*

[2] M.J. Beller, L.-F. Chang and Y. Yacobi. Privacy and authentication on a portable communications system. *IEEE Journal on Selected Areas in Communications*, 11:821–829, 1993.

[3] M.J.Beller, and Y.Yacobi. Fully-fledged two-way public key authentication and key agreement for low-cost terminals, *Electronics Letters*, Vol.29, No.11, May 1993, pp. 999-1001.

[4] R.Bird, I.Gopal, A.Herzberg, P.Janson, S.Kutten, R.Molva, and M.Yung. The KryptoKnight family of light-weight protocols for authentication and key distribution. *IEEE Trans. On Networking*, Vol.3, No.1, pp.31-41, Feb. 1995.

[5] Dan Brown. Techniques for privacy and authentication in personal communication systems. *IEEE Personal Communications*, Vol. 2, No.4, 1995, pp.6-10.

[6] U. Carlsen. Optimal privacy and authentication on a portable communications system. *ACM Operating Systems Review*, 28(3):16–23, 1994.

[7] L. Chen and C.J. Mitchell. Comments on the Secret Key User Authentication Scheme. *Operating Systems Review*, Vol.30 No.4, 10/96.

[8] Electronic Industries Association, EIA Interim Standard IS-54, Rev B, Dual-mode mobile station- base station compatibility standard, 1992.

[9] ETSI ETS 02.09, *European Digital Cellular Telecommunications System (Phase 2): Security Aspects*, Version 4.2.4, September 1994.

[10] European Telecommunications Standards Institute (ETSI), Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security, November 1998.

[11] J.C. Francis, H. Herbrig, and N. Jefferies. Security provision of UMTS services over diverse access networks. *IEEE Communications Magazine*, 128-136, February 1998.

[12] N.Haller. The S/KEY one-time password system, Bellcore, February 1995. Internet RFC 1760.

[13] G. Horn and B. Preneel. Authentication and payment in future mobile systems. *Computer Security - ESORICS 98*, Lecture Notes in Comput. Sci., 1485:277–293, 1998.

[14] L.Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24:770–772, 1981.

[15] H.Y. Lin and L. Harn. Authentication protocols for personal communication systems. *Proceedings of ACM SIGCOMM'95*, 256–261, August 1995.

[16] K.M. Martin, B. Preneel, C.J. Mitchell, H.J. Hitz, G. Horn, A. Poliakova and P. Howard. Secure billing for mobile information services in UMTS. *5th International Conference in Services and Networks, IS&N '98*, Lecture Notes i nComput. Sci., 1430:535–548, 1998.

[17] C.J. Mitchell and L. Chen. Security in future mobile multimedia networks. Chapter 11 of *Insights into Mobile Multimedia Communications*, eds. D.R. Bull, C.N. Canagarajah and A.R. Nix, Academic Press, 1999, pp. 177-190.

[18] Y. Mu and V. Varadharajan. On the design of security protocols for mobile communications. *Information security and privacy*, Lecture Notes in Comput. Sci., 1172:134–145, 1996.

[19] S.B.Xu and X.M.Wang. Authentication and key distribution schemes based on public-key cryptosystems for portable communication systems. *Proceeding of the 2nd International Conference techniques on Personal, Mobile and Spread Spectrum Communications,* Hong Kong, Dec., 1996, pp.379-382

[20] J. Zhou and K.-Y. Lam. Undeniable billing in mobile communications. In *Proceedings of the 4th ACM/IEEE International Conference on Mobile Computing and Networking, Dallas, Texas, October 1998*, ACM Press, 1998.