Undeniable Mobile Billing Schemes*

Shiqun Li[1,2], Guilin Wang[2], Jianying Zhou[2], and Kefei Chen[1]

[1] Dep. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China
[2] Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613.

Abstract. An undeniable mobile billing system allows a mobile network service provider to bill its subscribers with trustworthy evidences. Chen, Jan and Chen proposed such a billing system by introducing a trusted third party – Observer and exploiting a hash chain mechanism. In their system, the Observer provides call time evidence to both cellular carriers and subscribers for billing. In this paper, we first identify some vulnerabilities in their mobile billing system. Then, we propose an undeniable billing scheme based on a proper combination of digital signature and hash chain mechanism. The proposed scheme can achieve authentication, non-repudiation, and fairness, which are desirable security requirements for an undeniable mobile billing system.

1 Introduction

In the traditional GSM billing system, both the billing management and the billing information are processed by the Mobile Network Service Provider (MNSP) alone. From the subscribers' point of view, the above method may be not a good solution. Therefore, Chen et al. [3] proposed a mobile billing scheme (CJC scheme, for short) to provide undeniable billing evidences for call services in GSM. They introduced a TTP – Observer and used hash chain to provide billing information. The Observer is in charge of authentication and evidence provision.

In this paper, we first identify some vulnerabilities in the CJC system. Then we propose a new undeniable billing scheme, which is based on a proper combination of digital signature and a hash chain mechanism. It is very lightweight and suitable for the GSM mobile phone users.

The rest of the paper is organized as follows. Section 2 briefly introduces existing mobile billing systems. Section 3 reviews the CJC scheme and analyzes its security. Section 4 presents the proposed mobile billing systems which is based on hash chain technique and digital signatures. Section 5 evaluates the proposed scheme in aspects of security and efficiency. Section 6 draws a conclusion.

* Project supported by the National Nature Science Foundation of China key project(No.90104005) and Specialized Research Fund for the Doctoral Program of Higher Education(No. 20050248043). The primary author's work was done during his attachment to the Institute for Infocomm Research under its sponsorship.

2 Mobile Billing Systems

To provide undeniable evidences for mobile network services, several schemes were proposed. The undeniable billing system in mobile communication [6] proposed an efficient solution to undeniable billing when a mobile user roams into foreign networks. This scheme adopted public key cryptographic algorithm to provide authentication and non-repudiation evidences, which is complicated for the current GSM mobile terminals. The Secure Billing for Mobile Information Services [2, 4], provided a secure billing scheme for value-added information services using micropayment mechanism. It also requires public key operations for the mobile terminal which is applicable for UMTS mobile users but not the current GSM mobile users.

The CJC scheme [3] introduced an Observer as the TTP and used hash chain mechanism to provide billing information. It is a very efficient for mobile users, since the MSU is not required to perform any asymmetric cryptographic operation. However, our analysis shows that the CJC mobile billing system has some vulnerabilities so that it is not applicable in practice.

Our main purpose in this paper is to propose a new mobile billing scheme such that it is secure and as efficient as the CJC scheme. That is, we do not require the user's MSU do any public key operation (so our work is different from [2, 4, 6]). On the other hand, as in [6] we also employ the hash chain technique to determine the duration of a call service.

3 CJC Scheme and Its Vulnerabilities

3.1 Review of the CJC Scheme

The CJC mobile billing system [3] is illustrated in Fig. 1. As shown in Fig. 1, the Observer acts as the agent of a subscriber's MSU and shares a hash chain with it. To generate the bill evidence for a call, the MSU will first be authenticated by the MNSP and the Observer. Then the MNSP and the Observer sign the start time and end time of a valid call. Thus, by exploiting the hash chain technique and digital signature mechanism, both the MNSP and the subscriber cannot forge or deny the valid billing records. Note that here the Observer acts as a TTP and is in charge of providing call evidences to both the mobile subscriber and the MNSP. For more details about the CJC scheme, please refer to [3].

The authors claimed that their system satisfies the requirements of a fair mobile billing system. However, our analysis below will show that the CJC scheme cannot provide practicability and non-repudiation as supposed.

3.2 Vulnerabilities in the CJC Scheme

In this part, we show some vulnerabilities in the CJC mobile billing scheme [3]. Some of them are security flaws, and others are about implementation weaknesses.

First of all, the CJC scheme is *not fair* for both the MNSP and the mobile users. We now show two attacks on the fairness of the CJC scheme.

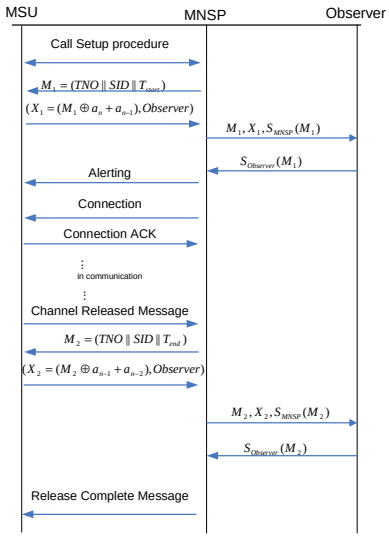

Fig. 1. The CJC Mobile Billing System.

– **Attack 1**. In the CJC scheme, if the call is set up successfully but terminated abnormally later, then the MNSP cannot get the signature on T_{end}. In practice, a call may be terminated abnormally because of power failure, operation error or the caller's deliberate cheating (e.g., shutting down the device or unplugging the battery suddenly).

According to the specification in [3], if such abnormal interruptions in Attack 1 happen, the MNSP and the user's MSU cannot exchange M_2) and X_2. However, without proper X_2 the MNSP cannot get $S_{Observer}(M_2)$ from the Observer. So, the MNSP only has $S_{MNSP}(M_1)$ but does not have $S_{MNSP}(M_2)$. Consequently, with just one piece of non-repudiation evidence the MNSP cannot charge the users properly according to the CJC scheme. Moreover, if a called party does not pick up or deny the caller's call request, the connection would not be set up. According to Fig. 1, however, the MNSP and the Observer already calculated and exchanged $S_{MNSP}(M_1)$ and $S_{Observer}(M_1)$, although the *Alerting*, *Connection* and *Connection ACK* messages are not exchanged between the MSU and the MNSP.

Naturally, a subscriber should pay in the first case but needs not to pay in the second case. However, the Observer cannot tell which of those two cases occurred. So the MSU can deny a successful call if an abnormal termination happens. Thus, the CJC mobile billing system is unfair for the MNSP.

On the other hand, the following Attack 2 shows that the CJC scheme is nor fair for the mobile users, since the MNSP can maliciously overcharge them.

– **Attack 2**. At some time T_{start}, a mobile user wants to make a call, so proper messages M_1 and X_1 are exchanged between the user's MSU and

the MNSP. Then, the MNSP gets $S_{Observer}(M_1)$ from the Observer but it tells the user's MSU that this call cannot be set up due to some reason. In this scenario, the user may wait and re-call at T'_{start}. Now, the MNSP uses the same transaction number TNO used in M_1 to generate M'_1, i.e., $M'_1 = (TNO \| SID \| T'_{start})$. Upon receiving X'_1 from the user's MSU, the MNSP directly makes a connection for this MSU without contacting the Observer. Once the MSU ends its call, the MNSP can properly get $S_{Observer}(M_2)$ from the Observer, where $M_2 = (TNO \| SID \| T_{end})$. Therefore, the MNSP can charge the user on this call over the time interval of $T_{end} - T_{start}$, instead of the correct one $T_{end} - T'_{start}$.

The second problem of the CJC scheme is about *synchronization*. It employs the hash chain to realize the mutual authentication between the user's MSU and the Observer. However, the authors of do not provide how to maintain the synchronization of the hash chain between the MSU and the Observer. If a connection is terminated due to any abnormal reason, the MSU and the Observer may lose synchronization of the current state of hash value a_i, and then it would be impossible for the Observer to authenticate later valid calls.

4 The Proposed Scheme

In this section, we propose a secure undeniable mobile billing scheme that satisfies the security and practicability requirements described in Section 1. In our new scheme, the MNSP and the Observer sign the start time of a call. Those signatures serve the first evidence for the non-repudiation of billing. Then, the MSU periodically releases chained hash values during the call. Finally, the MNSP retains the last chained hash value from the MSU as the second non-repudiation evidences for billing.

In the proposed scheme, we assume that the MSU and the Observer share a secret key K_{MO} in advance. A keyed hash $H(M, K_{MO})$ is an ideal "one-time MAC" [1] known by the MSU and the Observer. A charge unit L is a value agreed by the MSU and the MNSP. L can also be a variable value set as a system parameter that can be chosen by the MSU in each call. The proposed scheme with five steps is illustrated in Fig. 2, and explained in detail below.

- *Step 1.* The MSU and the MNSP pass the authentication and begin a call connection. Once the connection is established, the MNSP sends $M_1 = (TNO \| SID \| T_{start} \| L \| etc)$ to the MSU, where L is the pre-defined time unit and *etc* contains some related information.
- *Step 2.* Upon receiving message M_1, the MSU checks its validity, such as the validity of T_{start} and L etc. If the check passes, the MSU generates a random number a and calculates m chained one-way hash values according to equation (1).

$$H^i(a) = H(H^{i-1}(a)), \quad i = 1, 2, ..., m. \tag{1}$$

  Then, the MSU computes a keyed-hash $MAC = H(M_1, m, H^m(a), K_{MO})$ and sends $(M_1, m, H^m(a), Observer, MAC)$ to the MNSP.

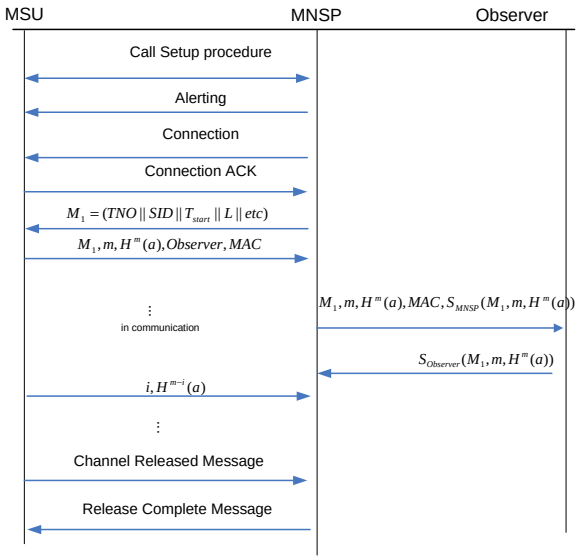

Fig. 2. The Proposed Mobile Billing Scheme.

- *Step 3.* Upon obtaining $(M_1, m, H^m(a), Observer, MAC)$ from the MSU, the MNSP signs $(M_1, m, H^m(a))$ and sends $(M_1, m, H^m(a), MAC, S_{MNSP}(M_1, m, H^m(a)))$ to the Observer.
- *Step 4.* After the Observer receives the message from the MNSP, it verifies the keyed-hash MAC by checking $MAC = H(M_1, m, H^m(a), K_{MO})$, where K_{MO} is the shared key between the Observer and the user with identity SID that is specified in M_1. If this is correct, the Observer signs $(M_1, m, H^m(a))$ and sends $S_{Observer}(M_1, m, H^m(a)))$ to the MNSP as the evidence of making a call.
- *Step 5.* The MSU can continue the call by releasing $(i, H^{m-i}(a))$ to the MNSP at the pre-defined interval L during the service. The MNSP will check

$$H^{m-(i-1)}(a) \stackrel{?}{=} H(H^{m-i}(a)), \quad i = 1, 2, ..., m.$$

  If it is true, the MNSP overwrites the former pair $(i-1, H^{m-(i-1)}(a))$ with $(i, H^{m-i}(a))$ in its cache. If it is false, it will send a warning and then cut off the call connection. The MNSP retains $(M_1, m, H^m(a), S_{Observer}(M_1, m, H^m(a))$ and the last chained hash value $(i, H^{m-i}(a))$ as *non-repudiation evidences* of a call.

For a given period, the MNSP submits the billing information (including all non-repudiation evidences of those calls) to the Observer and gets the payment from a mobile user through the Observer.

If a user has doubts over a bill provided by the MNSP, she can get the related non-repudiation evidences from the Observer or the MNSP and then

check if each call is correctly charged. For a call with non-repudiation evidences $(M_1, S_{Observer}(M_1, m, H^m(a)), m, H^m(a), i, H^{m-i}(a))$, the user re-calculates the corresponding fee as follows.

- Check the format of M_1: whether the SID and L etc are correct.
- Checks $S_{Observer}(M_1, m, H^m(a))$ is a valid signature of the Observer on message $(M_1, m, H^m(a))$.
- Validate the hash chained values by checking whether $H^m(a) \equiv H^i(H^{m-i}(a))$.
- If all of above checks pass, compute the corresponding fee according to the call time $(m-i) \times L$ and the charge rate. Otherwise, this call should not be charged to the user.

5 Analysis of the Proposed Scheme

In this section, we evaluate the proposed scheme in terms of security and efficiency. The security properties include authentication, non-repudiation, and fairness as discussed in Section 1.

5.1 Security

Firstly, the authentication between the MSU and the MNSP is completed in the call setup phase provided by the GSM system itself. The authentication of the MSU to the Observer is achieved via the keyed hash $MAC = H(M_1, m, H^m(a), K_{MO})$ by using the shared key K_{MO}, which is known by the user and the Observer only. Before a call connection is established, the Observer calculates the value of MAC and checks whether it is the same as that one forwarded by the MNSP. According to the results of keyed hash authentication given in [1], only the right MSU with the key K_{MO} can properly calculate the value of MAC. Therefore, the authentication property is satisfied.

For the non-repudiation property, as described in Section 4, the billing information collected by the MNSP retains sufficient evidences which make a bill undeniable and clear. Namely, the MNSP keeps $S_{Observer}(M_1, m, H^m(a))$ and the last chained hash value $(i, H^{m-i}(a))$ as the non-repudiation evidences of a call. We naturally require the Observer employs an existentially unforgeable signature scheme, so a valid signature $S_{Observer}(M_1, m, H^m(a))$ must be signed by the Observer itself. Moreover, we assume that the Observer is a trusted party, so it issues this signature if and only if it received a message $(M_1, m, H^m(a))$ authenticated by MAC from someone else. However, only the user or the Observer can generate correct MAC, since a secret key K_{MO} is needed. Once more, due to the Observer is a trusted party, it is concluded that $(M_1, m, H^m(a))$ must be approved by the user. Consequently, this implies that the user requested a call that is indexed by message M_1 and hash chain $(m, H^m(a))$. Therefore, the user cannot deny the fact that she made a call defined by non-repudiation evidence $(M_1, m, H^m(a), S_{Observer}(M_1, m, H^m(a)), i, H^{m-i}(a))$.

After receiving $S_{Observer}(M_1, m, H^m(a))$ from the Observer, the MNSP is ensured that the call request is from a specific MSU, since the Observer is a

trusted party. During a call session, the MSU has to release a pair $(i, H^{m-i}(a))$ to the MNSP in each time interval L, while the MNSP can check the validity of such a pair timely. The billing information collected by the MNSP is bounded by the Observer's signature and a hash value released by the MSU. Neither the MNSP nor the MSU can forge or deny a bill record. If any dispute happens later, the user or any third party can check whether a call is correctly charged according to the procedure specified in Section **??**. Both evidences cannot be forged, so the scheme satisfies the non-repudiation requirement.

Now we discuss the fairness of our mobile billing scheme. Fairness means that the billing method should provide objective evidences accepted by both the MNSP and mobile users such that neither the MNSP nor the mobile user can cheat the other. First, the duration of each call is clearly and objectively determined by $(m - i) \times L$, if the corresponding non-repudiation evidence is $(M_1, S_{Observer}(M_1, m, H^m(a)), m, H^m(a), i, H^{m-i}(a))$. Second, the MNSP cannot forge valid evidences for a call that is not made by the user since the MNSP cannot forge the Observer's signature $S_{Observer}(M_1, m, H^m(a))$; the MNSP also cannot overcharge a call to the user since beside the user nobody cannot release further pre-images of the hash chain. Finally, a mobile user cannot cheat the MNSP too. The reason is that to get the MNSP's service, a user should be first authenticated by the Observer. Otherwise, the user's call will not be connected by the MNSP. So, only legal users can be served by the MNSP via using their proper keys shared with the Observer. Moreover, during the call session the user has to periodically release new hash values to continue a call. In particular, note that the proposed new scheme is immune to the two attacks presented in Section 3.2, since we do not use two signatures to determine the duration of a call at all.

5.2 Efficiency

To design a practical mobile billing system, the limitations of the computation capability, storage capability and power capability of the mobile terminal should be considered. Generally, the efficiency of a system is mainly determined by the computation complexity and communication complexity. So, in Table 1 we make an efficiency comparison between the CJC scheme and our new solution.

Table 1. Efficiency Comparison

	Communication Steps	Public Key Operations
CJC Scheme [3]	8	8
Our Scheme	5	4

As shown in Table 1, the new scheme has fewer communication steps than the CJC scheme. For the public key operations, the CJC scheme requires 4 signature generation operations and 4 signature validation operations to generate the undeniable evidences. While in the proposed mobile billing mechanism, only 2

signature generation operations and 2 signature validation operations are needed. Thus our newly proposed scheme is more efficient. On the other hand, as same in the CJC scheme the proposed scheme also does not employ public key algorithm for the MSU and the certificate revocation issue is also avoided without using public key certificate for the MSU. Although a hash value needs to be released periodically in our scheme, the computation and communication overheads are very lightweight. Moreover, note that the hash chain can be pre-computed before a call setup to improve the efficiency. Thus the proposed undeniable billing scheme is more efficient than the CJC scheme and can be integrated into the current GSM systems.

6 Conclusion

In this paper, we first re-examined the security requirements of a secure and undeniable mobile billing system for current mobile systems. Then, we analyzed the CJC mobile billing system [3] and identified some weaknesses in the CJC mobile billing system. In particular, two attacks were demonstrated to show that the CJC scheme is not fair for both the mobile user and the service provider. Finally, we proposed a new scheme by combining digital signature mechanism and the technique of gradually releasing the chained hash values. The scheme satisfies the authentication, non-repudiation, and fairness requirements of a secure undeniable mobile billing system. In our scheme, the user's mobile device just need to perform hash operation without doing any public key operation during call procedures. Therefore, the proposed scheme is very efficient and could be applicable to the current GSM systems.

References

1. M. Bellare and P. Rogaway. Minimizing the use of random oracles in authenticated encryption schemes. In *ICICS '97: Proceedings of the First International Conference on Information and Communication Security*, pages 1–16, Beijing, China, 1997. Springer-Verlag.
2. L. Chen, H. J. Hitz, G. Horn, K. Howker, V. Kessler, L. Knudsen, and C. J. Mitchell. The use of trusted third parties and secure billing in umts. In *Proceedings of ACTS Mobile Telecommunications Summit*, pages 493–499, Granada, 1996.
3. Y.-Y. Chen, J.-K. Jan, and C.-L. Chen. A fair and secure mobile billing system. *Computer Networks*, 48(4):517–524, 2005.
4. 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. In *IS&N '98: Proceedings of the 5th International Conference on Intelligence and Services in Networks*, pages 535–548, London, UK, 1998. Springer-Verlag.
5. S. Shenker, D. Clark, D. Estrin, and S. Herzog. Pricing in computer networks: reshaping the research agenda. *SIGCOMM Comput. Commun. Rev.*, 26(2):19–43, 1996.
6. J. Zhou and K.-Y. Lam. Undeniable billing in mobile communication. In *MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pages 284–290, New York, USA, 1998. ACM Press.