Available online at www.sciencedirect.com
ScienceDirect
Applied Mathematics and Computation 192 (2007) 487–495
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

A simple mobile communication billing system among charged parties

Hsia-Hung Ou [a], Min-Shiang Hwang [b,*], Jinn-Ke Jan [a]

[a] Department of Computer Science, National Chung Hsing University, Taichung 402, Taiwan, ROC
[b] Department of Management Information Systems, National Chung Hsing University, 250, Kuo Kuong Road, Taichung 402, Taiwan, ROC

Abstract

Mobile communication is a milestone technology that has brought people a kind of universal convenience otherwise unattainable. From GSM to UMTS, the mobile communication technologies, like all the other great inventions in human history, have gone through such fast-paced advancements since the very first day it came to existence that each day we seem to be using a newer, more powerful device than before to talk to people close by or far away. We are so used to this convenience that it is hard to imagine how life could carry on without cell phones. However, when cell phone users roam from city to city crossing different system facilitators' domains of services, besides the conveyance of the signals, some charging problems may also arise between or among the service providers. In this paper, we shall present a simple mobile communication billing system that can help solve roaming-related charging problems. Our new system can be used in a wide variety of applications without having to modify the standard UMTS protocol, and it only causes slight, readily ignorable traffic increase. As we can expect, the new mobile communication billing system will be a friendly design that comes in handy for both service providers and users.

Keywords: Mobile communication; Billing; Charging; UMTS

1. Introduction

In the last couple of decades, mobile communication systems have thrived and become a dominant trend of advanced technologies and a significant part of modern people's lives. Since the earlier times of the history of mobile communication, global system for mobile communications (GSM), has long been the thing that dominates the market, but now the even more powerful universal mobile telecommunication system (UMTS)[1], has just developed to offer yet wider varieties of state-of-the-art services. GSM often referred to as the 2G (second generation) mobile service technology, is a common international standard for the cell phone issued by European Telecommunication Standards Institute (ETSI) [8] that has offered unbelievable convenience to hundreds

* Corresponding author.
E-mail address: mshwang@nchu.edu.tw (M.-S. Hwang).
[1] http://www.3gpp.org.

0096-3003/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.amc.2007.03.034

of millions of people in every part of the world. However, GSM only has a limited bandwidth of 9600bps and can hardly meet the needs of future, and UMTS or the 3G (third generation) mobile service technology, has come out to take its place. In the design of UMTS, time division multiple access (TDMA) is replaced with code division multiple access (CDMA), supporting a maximum bandwidth of 2 Mbps, which is assumed enough for the mobile communication loads in the future.

In 3GPP, the following assumptions have been brought up that have an impact on the design of UMTS-based charging and billing systems [3]:

- support the generation of standardized charging records;
- support on-line billing;
- support the billing of third party value-added services.

The major requirements a UMTS charging and accounting system should live up to are [1]:

- It should provide charging information for all charges so that disputes can be settled between different parties if any.
- It should support the home environment and the serving network with fraud control.
- It should support the charged party with cost control.
- It should provide a notice for the charged party at the beginning of a chargeable event.
- It should support itemized billing for all services offered by home environments.
- It should provide prepay services.
- It should support inter-operator charging.
- It should allow network operator to 3rd party supplier charging.
- It should provide details required for customer care purposes.
- It should support shared network architecture.

The paying methods developed on the basis of UMTS can be classified as follows [1]:

- Prepay service: The prepay service allows a subscriber to pay in advance for the use of specific services.
- Real time: The real time is an on-line mechanism that charging by time.
- Session: Logical connection between parties normally used for a connection over conventional systems.

Different entities involved play different roles, and therefore they should be charged differently. For example, regular users are usually retail charged by the mobile network operators or 3rd party service providers, and 3rd party service providers are wholesale charged by mobile network operators. Besides, there are interconnect charging between mobile network operators and circuit-switched network operators for call traffic carried, usage charging between mobile network operators and IP-based network operators for session traffic carried, and roaming charging between mobile operators. These different charging requirements explain the need for different mechanisms due to the change from the traditional circuit-switched way of communication to the IP-based way. Also, where mobile operators need to pass traffic to one another, there will be both interconnect charging for the non-IP, circuit-switched type of communication and usage charging for the IP-based type.

Generally speaking, charging information is collected by the service network to record lists of chargeable users, mobile station activities, and inter-carrier connections. Some of the information is provided to the users, other information is only available to the elements of the serving network. Basic information provided to the users may include [1]: user identity for authentication, home environment identity, terminal identity and terminal class, destination endpoint identifier for service(s) requested, resource(s) requested, QoS parameters, and IP multimedia capability requested.

Besides those listed above, the serving network must provide some extra information to its own elements [1]: serving network identity, recording network element identity, universal time at which the service request was initiated, universal time at which the resource was allocated to the user, quantity of data transferred both to and from the user, QoS provided to the user, location of the user in the standard format used for 3GPP

location based services, whether GSM optimal routing was applied, the service parameters and the actually used destination number and calling party number identification, time duration covered by this charging information to an accuracy of at least 1 s, unique identity of the chargeable event which allows the billing system to correlate all charging information belonging to the same chargeable event, unique charging information identity, IP multimedia capability provided to the user, VAS information, identifier of third party accessed by the user, presence information, service identification, supplementary services used, as well as prepay account identifier and related information.

When the above charging information is collected over a serving network and is transferred to the home network, the integrity and secrecy of the information have to be ensured. The home environment should be able to validate the sources and integrity of the charging information provided by the serving network, and the serving network should also be able to validate the sources and integrity of the charging information provided by the user, and the most important thing is that the serving network should have proof that due services were provided to specified users.

2. Overview of the charging and billing related protocols

In the 3GPP design, the UMTS charging and billing protocol can vary in accordance with the subscriber's choice of charging information collection period. The service provider can keep track of the charging time from the instant at which the service request was initiated to when the service provision was completed, the service type and other necessary data. The service provider collects and processes such charging data generated by its network elements. The record of each individual transaction is reported to the home environment within short time intervals in order to allow further processing by the billing system in the home environment. With the itemized bill providing, any charging dispute between or among the user, the visited network and the home environment can be easily settled. Each entity involved in this system has the responsibility to provide true charging data to each other, and the subscribers must trust in the bills generated by the home service provider. In other words, authentication is the key to a successful charging and billing system. During the authentication process, the subscriber and service provider verify each other and then establish a new pair of cipher and integrity key between them. This is the mutual authentication required by the 3GPP specification [3]. In fact, mutual authentication is not included in the GSM standards, but it is a part of UMTS.

Fig. 1 [4] shows the UMTS protocol of authentication and key agreement. When a subscriber (MS, mobile station) roams through visitor local register (VLR, visitor service provider), the international mobile

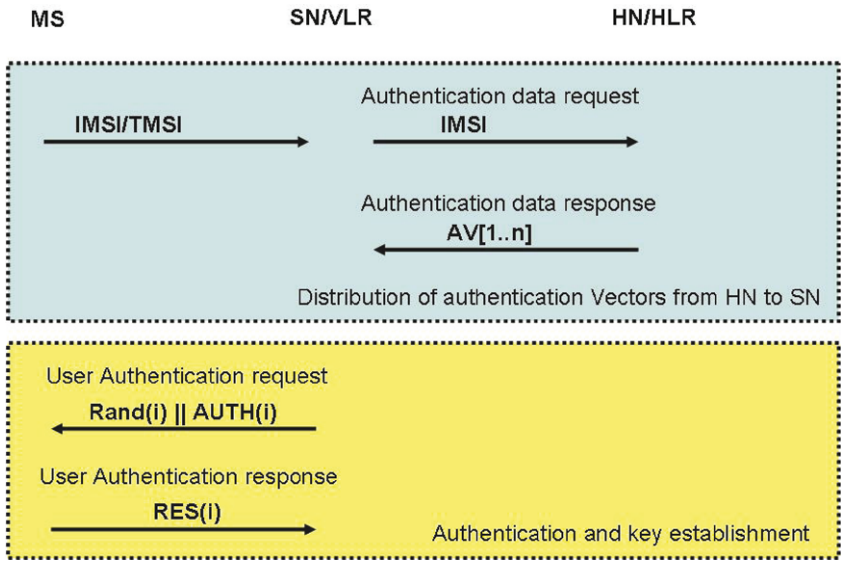

Fig. 1. Authentication and key agreement on UMTS.

subscriber identity (IMSI) or temporary mobile subscriber identity (TMSI) this MS has must be transmitted to the VLR before the MS can request services. The VLR, upon receiving a request by the MS, then transmits the MS's IMSI and an authentication request to the home local register (HLR). Having received these, the HLR generates a series of authentication vectors (AV) and sends them to the VLR in return. Here, each authentication vector consists of five components: a random number (RAND), an expected response (XRES), a cipher key (CK), an integrity key (IK), and an authentication token (AUTH). The HLR has generated these authentication vectors by using a pre-shared secret key with the contacted MS. The VLR receives the n copies of authentication data response $\mathrm{AV}(1 \ldots n)$ and stores them.

Those n copies of authentication vectors can be used to do authentication the next n times without the MS's contacting the HLR. If the MS roams into another VLR, the remaining authentication vectors can also be used to pass the mutual authentication between the MS and the new VLR. Here, the VLR selects a string of AV_i, and sends $\{(\mathrm{RAND}_i, \mathrm{AUTH}_i)\}$ to the MS. The MS verifies the validity of AUTH_i in terms of RAND_i and that of the pre-shared secret key with the HLR. If accurate, the MS generates and transmits the correct SRES_i to the VLR. The VLR then checks the SRES_i on its own AV_i and accepts the connection request of the MS if the SRES_i is equal to that one from the MS.

In the literature concerned, several papers such as [13,9] mention the term "billing program" but have not gone any further than that. Billing programs in those papers are classified as non-repudiation programs. In fact, although an enhanced authentication protocol has been designed to strengthen mutual authentication, the focus has not been placed on the charging and billing program but rather on the authentication and key agreement (AKA) protocol.

Chen and Hsueh [6] proposed a light-weight authentication and billing protocol for GSM based on Krypto-Knight cryptography [10,5]. They even proposed a billing protocol solution to mobile users roaming into foreign networks by using value-added services (VASs). However, their protocol has only the prepay mode for when the mobile user desires to access VASs. When the authentication has been passed but the connection gets interrupted for one reason or another, in their protocol, there is no way the mobile user can get a refund.

Chen et al. [7] claim to have put together a fair and secure mobile billing system for GSM that satisfies five requirements including fairness, non-repudiation, non-usurpation, simplicity, and practicability. They introduce the "observer" concept into the mobile billing system. Observer is a piece of hardware installed to help subscribers sign the charging data. It is a fresh concept capable of ensuring fair and secure billing; unfortunately, additional installation loads are needed to put it to work.

3. The proposed scheme

Through the UMTS AKA protocol, members of UMTS verify the legality of each other and then provide services and/or record charging data. When a chargeable event occurs, the charging information is transferred between the serving network and the home environment. In this paper, we offer to present a new protocol that deals with the part of charging and billing where a third party is involved. With the new protocol, it is easy for network operators and third parties to charge each other for the use of their resources. Here, a third party may be a content/application provider or a portal, or the term can even mean another service network. When an MS is roaming around in the realm of another service network or is using VAS provided by another service network, this particular service network (called the third party) will charge the MS, or, to be more precise, it is the home network where the MS belongs that pays the bill to the third party for the roaming of the MS, and later the MS is charged by its home network for this event.

The question here is whether or not the third party is truly worthy of all trust. After all, the correctness of the bill is a key element of the whole business. Therefore, in this paper, we shall propose a simple mobile communication billing system that takes care of the charges among all parties involved. The new system can work smoothly on the basis of the well-accepted UMTS environment, and so there is no need to modify the original UMTS AKA protocol. All we have to do is simply append some charging parameters. To have a clear overview of our new system, please take a look at the framework of our new method illustrated by Fig. 2.

Our scheme uses a one-way hash function [11] to generate a hash chain, which we take for the proof of an MS's payment. The SN collects the proof of service usage that the MS provides so that it can prove the correctness of the charge to the HN. As Fig. 2 illustrates, in the phase where the authentication vectors are

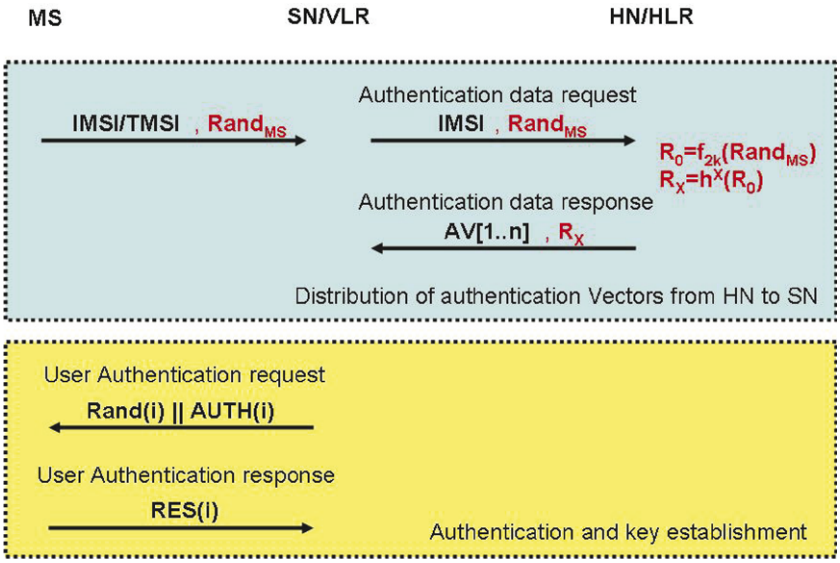

Fig. 2. Our charging protocol.

distributed from the HN to the SN, to begin with, the MS generates a random number $\mathrm{Rand}_{\mathrm{MS}}$ and then sends IMSI/TMSI and $\mathrm{Rand}_{\mathrm{MS}}$ to the HN through the SN. The HN then uses the secret key shared with the MS and the $f2$ function to generate R_0 as the seed of the hash chain. The $f2$ function is the authentication and key generation function established by UMTS [4]. This way, we can make sure that the seed R_0 is perfectly kept in secrecy and only the MS and the HN own it. The SN, on the other hand, has no access to it. Secondly, the HN takes R_0 as an initial value to calculate the HASH at time x and then gets R_x. The HN returns R_x and the authentication vectors $\mathrm{AV}[1 \ldots n]$ to the SN, and now the SN can do mutual authentication with the MS and check the validity of the MS payment.

Lastly, the MS and the SN use the standard UMTS AKA protocol to complete mutual authentication. Just like what the HN does, the MS uses the secret key shared with the HN and the $f2$ function to generate R_0 as the seed of the hash chain and takes R_0 as an initial value to calculate and record the HASH at time x and then gets R_0, R_1, R_2, …, R_x, where $R_m = h^m(R_0)$, $m = 1, 2, \ldots, x$. When the MS desires to access the services provided by the SN, the MS has to deliver the same R_m to the SN. The MS charging sequence is $R_{x-1}, R_{x-2}, R_{x-3}, \ldots, R_1$. The SN receives R_{x-1} from the MS and then checks to see whether or not $h(R_{x-1})$ equals R_x. If yes, it provides due service and records R_{x-1} for the verification and charging next time. The SN must keep track of the latest R_m as a proof of the consumption records of the MS.

As we mentioned earlier in the last section, ways of payment under the UMTS framework include prepay service, real time and session [1]. In our protocol, however, we categorize the above three ways of payment into two methods: prepay service and real time service.

- Prepay service:
  The prepay service allows a subscriber to pay in advance for the use of specific services. Each time the subscriber accesses service, the MS transmits R_{m-c} to the SN to indicate the change, where c is the equivalent of the hash chain value. For example, suppose one hash value represents the currency of a unit value. In case the service is worth c units this time. The MS delivers R_{m-c} to the SN when the service starts. Here, R_m is the last hash chain for the MS last time, and R_{m-c} is the c-th hash chain in back of R_m. Then the SN checks to see whether R_m equals $h^c(R_{m-c})$ or not. If yes, then the SN collects and saves R_{m-c} in place of R_m to prove the correctness of the charge.
- Real time:
  Typically in number of seconds or minutes, real time charging is the main stream of on-line communication/connection charging mechanisms. Since the charging unit is time, one hash chain is stands for one time

unit. That is to say, the MS keeps delivering hash chains to the SN as time units add up. For example, if the MS is charged by the second, while using the service, the MS has to send out a hash value to the SN each second. Just as it goes with the prepay service, the SN checks whether the hash value R_n equals the hash value R_m at last. If positive, then the SN collects and saves R_n in place of R_m to prove the correctness of the charge. Otherwise, there must be a problem somewhere, and in this case the SN can refuse to provide service to the MS.

When the SN bills the HN for the MS later, the SN shows the last hash value R_m collected. The HN computes the hash value R_n by $h^s(R_0)$, where s is the bill number. The HN compares R_m with R_n to decide whether or not to take this bill. Fig. 3 shows our billing protocol.

The hash values delivered between the MS and the SN are encrypted by the cipher key CK generated by the authentication and key generation function $f3$ established by UMTS [2]. This way, the secrecy of the charging data can be ensured.

Fig. 4 shows the enhanced protocol we propose. The major difference this enhanced protocol makes is that it uses public key infrastructure (PKI) [12] to achieve non-repudiation. PKI is an asymmetric key cryptographic technique where there is a key pair composed of a private key and a public key. Only the authenticated user owns the private key with which messages can be signed, while the public key can be used by other users

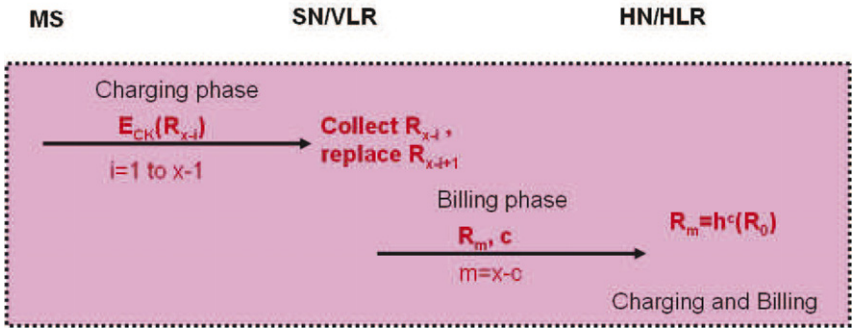

Fig. 3. Our billing protocol.

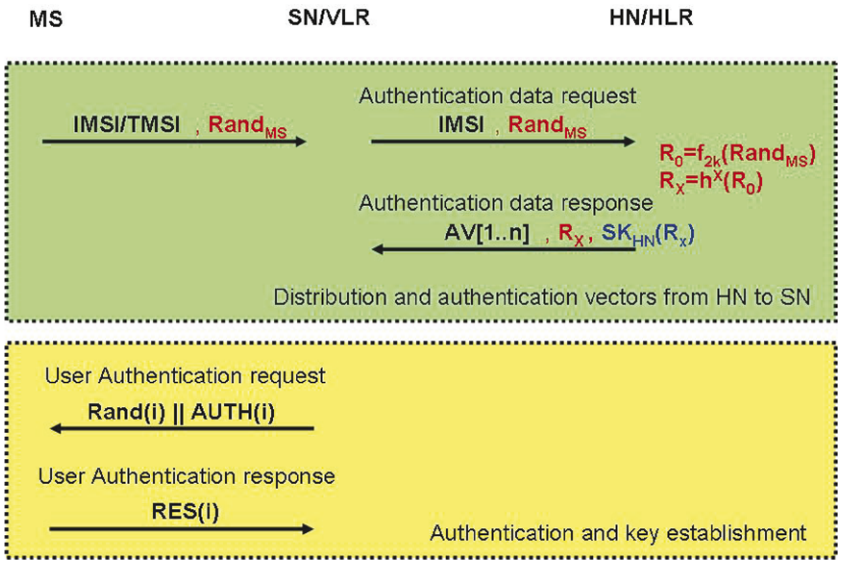

Fig. 4. The enhance protocol of our propose.

to verify the messages signed by the authenticated private key owner. In our method, we have a parameter $SK_{HN}(R_x)$ in the authentication phase. $SK_{HN}(R_x)$ indicates that R_x is signed with the private key of the HN.

Together with the hash chain value, it proves that the hash value the SN receives from the MS later is correct. The other purpose of it is to prevent the HN from denying the hash value. This way, although the use of PKI causes a little extra load on the HN and the SN (which hardly mean any trouble at all because both the HN and the SN are generally fixed facilities equipped with high computation capabilities), the MS remains uninfluenced. Moreover, for both the HN and the SN, to deal with each MS, only one time of signing or verification has to be done in the authentication and key distribution phase.

4. Analysis and discussion

The new method we propose here is very suitable for mobile communication charging and billing, and the major reason for it, as we mentioned earlier, is because our protocol does not modify the original communication protocol in charge of authentication and key agreement. We use the standard AKA protocol to confirm the legitimacy of the user and obtain the communication key without causing any trouble to the original system. As a matter of fact, our charging and billing protocol is only a small attachment to the standard UMTS AKA protocol. This explains the second advantage of our new protocol: it is extremely easy to apply. Way above the limit of UMTS, our new protocol can in fact work on any mobile communication system to enhance the performance of its billing protocol because we leave the original authentication protocol untouched. Simply put, our new protocol can be viewed as just a module protocol.

The built-in charging and billing protocol on UMTS is only for billing and charging. It involves kinds of services, universal time of service request and so on. It does not have a solid dispute solution mechanism. When a subscriber leaves her/his service provider and roams into the realm of another service provider, charging problems might happen.

To achieve smooth charging and billing and to solve disputes if any, we offer the use of hash chains. Hash chains come in handy here because they are irreversible. Given a hash chain $R = \{R_0, R_1 = h(R_0), R_2 = h(R_1), \ldots, R_x = h(R_{x-1})\}$, everyone can easily figure out what the next value is on the hash chain if they get to know the current value on the chain. However, with the knowledge of a value on the hash chain, no one can trace backward and learn what the hash value in front of it is. In other words, R_2 can be derived from R_1 by $R_2 = h(R_1)$. But there is no way to derive R_1 from R_2. Our new protocol has been built up on the basis of this irreversibility. The MS reverses and takes out a hash value R_n from the hash chain and sends it to the SN. The SN then derives R_{n+1} from R_n by using the hash function and verifies the correctness of this hash value by matching it with the one received the last time. In the charging phase, the SN takes the hash value R_m last received to prove the correctness of the bill. As for the amount charged, simple $(x - m)$ multiplications can do the trick.

In addition, the original UMTS charging and billing protocol uses the universal time. However, mobile communication is not restricted to a single time zone but too often happens in the global environment, where a user can roam across service networks in different time zones and cause problems of time confusion. In our new protocol, we use the chain value to quantify the charge and let the SN hold the consumption records of the MS. We believe such a design is much more practical.

Lastly, let's shift the focus onto the generation of the hash chain. For both the SN and the HN, hash chain generation means no trouble at all because they are equipped with fixed, powerful hardware that can satisfy demanding computation and storage requirements. However, what the MS has is a light-weight, handheld moveable device whose computation and storage powers are comparatively limited. In our protocol, the SN executes the hashing operation one time whenever a charge is received from the MS, and the prior hash value is then replaced with the present hash value. This does not require much computing power, and neither is much storage space needed.

On the other hand, the MS must deliver the hash chain in reverse order to the SN for verification. There are three options to it. One is to generate the whole hash chain at a time and store it. The USIM card or the mobile device can be the location of storage. As Fig. 5a shows, this seems to be the best way of doing it since both the generation and access are the easiest. However, if the storage space is a worry, we can take the substitute method illustrated by Fig. 5b, where, instead of keeping track of all the hash values, we can skip nine

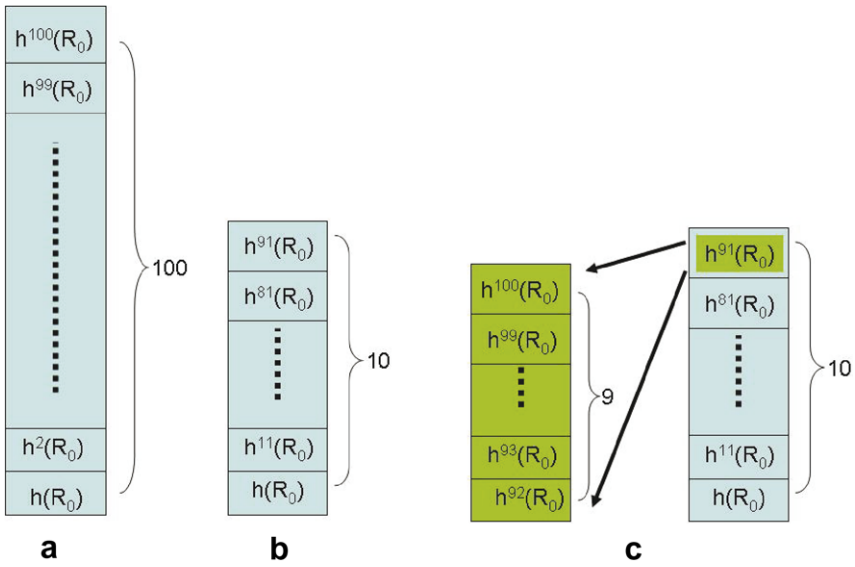

Fig. 5. The methods of hash chain generation and storage.

every time after we record one. If so, in case a certain hash value skipped is wanted, we can still take the lower, closest hash value recorded and compute the next value and then the next until the wanted value is reached.

For example, $h^{93}(R_0)$ can be derived from $h^{91}(R_0)$ by executing two hashing operations; in other words, $h(h(h^{91}(R_0)))$ comes to the result of $h^{93}(R_0)$. This method can reduce the storage space consumption, but additional time is needed for the extra operations. The third method, illustrated by Fig. 5c, makes use of two slots of storage. One slot is just like what happens in Method 2, and the other slot, where no hash value gets skipped, is for the hash values currently in use. This method can strike a balance between storage space economy and time efficiency.

5. Conclusions

In this paper, we have proposed a simple mobile communication billing protocol. Instead of authentication, our protocol focuses on charging-related affairs. When a mobile user roams out of its home network, there has to be a proper protocol that can ensure the correctness of the charges so that no disputes will trouble the parties involved. Without modifying the original standard UMTS AKA protocol, we attach our charging and billing protocol to it. This way, our new method not only is easy to apply but also is compatible with various communication systems. Besides, it can ensure the correctness of the bills, and it does not cause much computation and storage load increase.

Acknowledgement

This work is supported in part by National Science Council and Taiwan Information Security Center at NCTU, Taiwan, ROC.

References

[1] 3GPP, 3rd Generation partnership project, technical specification group services and system aspects, service aspects, charging and billing. Technical report, 3GPP TS 22.115 8.0.0 (2006–2009).
[2] 3GPP, 3rd Generation partnership project, technical specification group services and systems aspects, 3G security, security architecture. Technical report, 3GPP TS 33.102 V7.1.0 (2006–2012).
[3] 3GPP, 3rd Generation partnership project, technical specification group services and systems aspects, 3G security, security requirements. Technical report, 3GPP TS 33.21 V3.0.0 (1999–2002).

[4] 3GPP, 3rd Generation partnership project, technical specification group services and systems aspects, architectural requirements for release 1999. Technical report, 3GPP TS 23.121 V3.6.0 (2002–2006).
[5] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, M. Yung, The kryptoknight family of light-weight protocols for authentication and key distribution, IEEE/ACM Transactions on Networking 3 (2) (1995) 31–41.
[6] Hsing-Bai Chen, Sue-Chen Hsueh, Light-weight authentication and billing in mobile communications, in: IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, October 2003, pp. 245–252.
[7] Yu-Yi Chen, Jinn-Ke Jan, Chin-Ling Chen, A fair and secure mobile billing system, Computer Networks 48 (7) (2005) 517–524.
[8] European Telecommunication Standards Institute (ETSI), Recommendation GSM 03.20, security related network functions. Technical report, Technical report, June 1993.
[9] Lein Harn, Wen-Jung Hsin, On the security of wireless network access with enhancements. ACM workshop on Wireless security, 2003.
[10] P. Janson, G. Tsudik, M. Yung, Scalability and flexibility in authentication services: the kryptoknight approach, Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies 2 (4) (1997) 725–736.
[11] M. Naor, M. Yung, Universal one-way hash functions and their cryptographic applications, in: Proceedings of the twenty-first Annual ACM Symposium on Theory of Computing, Seattle, Washington, 1989, pp. 33–43.
[12] ITU/ISO Recommendation X.509, Information technology open systems interconnection – the directory: public key and attribute certificate frameworks, 1997.
[13] Muxiang Zhang, Yuguang Fang, Security analysis and enhancements of 3GPP authentication and key agreement protocol, IEEE Transactions on Wireless Communications 4 (3) (2005) 734–742.