國立中山大學資訊工程學系

碩士論文

可運用於行動網路環境中具公平隱私且可計費之

匿名認證協定

An Anonymous Authentication Protocol with Chargeability and Fair Privacy for Mobile Network Environments

研究生：黃士銘　撰

指導教授：范俊逸

中華民國 九十五 年 七 月

致謝

首先要感謝我的指導教授范俊逸老師對我的諄諄教誨，不論是在待人處事或研究心得上，都給了我細心的指導，還要感謝三位口試委員官大智教授、林俊宏教授與林葭華教授對我的指正，讓我最後完成的的論文能更加完美。

接著要感謝實驗室的學長姐、同學與學弟妹，有了這一群好伙伴，讓我在研究上有困難時，可以與我悉心討論，讓我成長了許多。

最後，僅以此論文獻給所有支持我的師長與同學，有了你們的指導與協助，才能讓我能順利的完成碩士學業。

學年度：94

學期：2

校院：國立中山大學

系所：資訊工程學系

論文名稱(中)：可運用於行動網路環境中具公平隱私且可計費之匿名認證協定

論文名稱(英)：An Anonymous Authentication Protocol with Chargeability and Fair Privacy for Mobile Network Environments

學位類別：碩士

學號：M933040058

語文別：English

提要開收使用：是

頁數：56

研究生(中)姓：黃

研究生(中)名：士銘

研究生(英)姓：Huang

研究生(英)名：Shi-Ming

指導教授(中) 姓名：范俊逸

指導教授(英) 姓名：Chun-I Fan

關鍵字(中)：雙向認證、匿名性、公平隱私、密碼系統、行動網路、無所不在的運算

算鍵字(英)：Mutual authentication, Anonymity, Fair privacy, Cryptography, Mobile networks, Ubiquitous computing

中文摘要

近幾年來行動通訊設備越來越普及，其計算能力與通訊能力也不斷的提升，而行動通訊網路服務也不斷的推陳出新，從 2G、3G 的 GSM 系統甚至是目前正在極積規畫與建設的第四代行動通訊網路(4G)，行動通訊網路的服務將越來越完善。未來對行動用戶而言，盡情的使用行動通訊網路來從事工作或娛樂將不再只是夢想。然而，就如已經非常普及的有線網路一樣，在行動通訊網路上仍然存在著許多安全上的威脅，由於行動通訊網路的特性，行動用戶可以隨身攜帶著個人資料、重要的檔案或是文件，並隨時隨地的藉由行動通訊網路的服務而與外界取得聯繫。一但行動用戶進入了行動通訊網路，便開始接受來自各方的威脅，惡意的行動用戶可能藉由行動通訊網路設計上的漏洞而取得他人的重要資料。

為了保證行動通訊服務的品質，行動用戶的隱私與安全性將會是個非常重要的議題。在這篇論文裡，我們將提出一個保護行動用戶隱私與確保行動用戶通訊安全的匿名認證協定。在我們的論文裡，行動用戶不僅僅對其他行動用戶匿名，對於系統業者也具有匿名的特性，然而系統業者仍然可以對匿名的行動用戶進行計費。除此之外，我們維持著隱私權的公平性，任何行動用戶並無法藉由隱私之便而行使違法的行為，任何違規的行動用戶都會被法院或警察單位監督著，甚至撤銷其隱私權。

關鍵字：雙向認證，匿名性，公平隱私，密碼系統，行動網路，無所不在運算。

Table of Contents

List of Figures

List of Tables

Abstract

Mobile network equipments are widely popularized and advanced mobile communication services are provided increasingly such that ubiquitous computing environments will come true soon. It is a pleasure for mobile users to work or get recreations in the mobile network environments. However, just as the cases in wireline environments, there are a lot of security threats to mobile network systems and their impact on the security is more serious than that in wireline environments owing to the feature of wireless transmissions and the ubiquity property in mobile network systems. The secret personal information, important data, or classified missives which mobile users carry may be stolen by malicious entities. In order to guarantee the quality of the advanced communication services, the security and privacy would be the important issues when mobile users roam to the mobile networks. In this thesis, an anonymous authentication protocol will be proposed to protect both the security of the mobile network system and the privacy of mobile users. Not only does the proposed scheme provide mutual authentication between each user and the system, but also the identity of each user can be kept secret against anyone else including the system. Although the users are anonymously authenticated by the system, it can still make correct bills to charge these anonymous users. Finally, our protocol also achieves the goal of fair privacy which allows the judge to be able to revoke the anonymity and trace the illegal users when they misused the anonymity property such

as they committed crimes.

Keywords: Mutual authentication, Anonymity, Fair privacy, Cryptography, Mobile networks, Ubiquitous computing

Chapter 1

Introduction

Recently, the mobile network is becoming more and more popular. There are a lot of applications and services provided in the mobile network environments. Even many countries are planning to construct new wireless network architectures of 4G (4th Generation) mobile networks. There are also more and more mobile equipments produced for the people to enjoy the mobile life. PDAs, notebook computers, cellphones, and etceteras are all the mobile equipments which support the people to roam over the mobile networks at anywhere and anytime. The mobile equipments are designed to be quite powerful such that they can carry more batteries and have more powerful computing capability, much faster transmitting rate, and etc. It is obvious that mobile computing will penetrate the people's life in the near future. The convenient mobile network environments and the powerful mobile equipments will make the people all around the world be willing to join the society of mobile communications.

In the mobile computing environments, mobile users can use mobile equip-

ments to process their secret data everywhere and anytime. The mobile users may handle important missives, documents, or secret personal information in their mobile equipments. Once the mobile users carry their mobile equipments and enter the mobile networks, they are beginning to face the threats from malicious entities. Mobile users would worry about whether it is secure for them to carry their important data and enter the mobile networks. When mobile users exchange messages in the public mobile networks, they may face a lot of security threats. The eavesdroppers may try to obtain their communicating messages, their real identities, and even their locations where they are roaming around. The more information the eavesdroppers know, the less security and privacy the mobile users have. In addition to the eavesdroppers, mobile users also need to get privacy from the system operator. Sometimes the vicious insiders of the system operator would betray the classified information of mobile users. A system without maintaining user privacy will not be popular in the future since most users always care about their personal privacy.

The mobile network has been constructed in our life for several years, but its security and user privacy is still not enough. In the future, the hackers' intruding ability will be more and more powerful. They may steal personal information and gain benefits from the mobile users because of the defects of the security designs. Many authentication protocols for the mobile network have been proposed [1][2][3][5][7][8][9][11]. Usually, an authentication protocol is used to verify a mobile user. Only the valid users can use the network services. An illegal user cannot obtain any benefit from the system operator because that she/he cannot pass the authentication phase. In

other words, an illegal user cannot impersonate a legal user and use the services. Therefore, the authentication protocol is to protect the rights and interests of the system operator. However, many scholars think that such an authentication protocol is not enough. Hackers may harm mobile users or gain benefits from them by stealing their personal information during the authentication or communication phase. The scholars also suggest that an authentication protocol must protect the rights of the system operator and protect the privacy of mobile users at the same time.

In the existent 2G mobile network system, there exist some weaknesses in user privacy. Each mobile user's alias or TMSI can be linked to her/his real identity or IMSI by attackers when the VLR requests her/him to retransmit her/his IMSI. The 2G mobile network also has no design for satisfying mutual authentication and protecting the users' privacy against the system operator. A mobile user may be cheated by some fake base stations in a mobile network system due to lack of mutual authentication. Although the newer 3G system has provided mutual authentication, the privacy or anonymity of mobile users has not been sufficiently considered yet.

Most of the proposed authentication schemes which emphasize the privacy of mobile users usually assign an anonymous identity to each user. A mobile user will get an anonymous identity after she/he is authenticated by the system operator successfully, and she/he will take this valid alias to roam over the mobile networks. Certainly, an anonymous authentication protocol must ensure that eavesdroppers cannot know the relation between an alias and the real identity corresponding to the alias. We hope that even the system operator cannot derive such relations either. The technique of **blind**

signatures can help us with realizing complete anonymity for mobile users. A mobile user sends a blinded message to the system and then the system signs it. After the mobile user unblinds the blind signature, she/he obtains a valid anonymous identity which can conceal her/his real identity from the system operator and eavesdroppers. Another problem is that once a mobile user gets anonymity, how can the system operator charge her/him when she/he requests the mobile network services via an anonymous identity? Besides, if there is some mobile user who misused the anonymity property, how can the judge handle it? Most of the current solutions cannot cope with all of the above problems at the same time.

In our solution, every mobile user is anonymous from any other one's point of view when she/he is accepting the mobile network services. Furthermore, the system operator can charge the mobile user according to the time the user consumed. Moreover, we also consider the issue of fair privacy. The privacy of the mobile users who misused the anonymity property can be revoked by the judge. We simultaneously realize the anonymity, chargeability, and fair privacy in our proposed authentication protocol for mobile communications.

The rest of the thesis is organized as follows. In Chapter 2, we introduce the related works about this reasearch. In Chapter 3, we describe some privacy requirements in mobile network environments. We present our scheme in Chapter 4 and make some security analysis in Chapter 5. In Chapter 6, we make a comparison between our scheme and the others. In Chapter 7, we discuss some additional issues on the proposed scheme. Finally, a concluding remark is given in Chapter 8.

Chapter 2

Related Works

In this chapter we will review several mobile authentication schemes [2][7][8][9][11] that focus on the privacy or anonymity for mobile users. They will be briefly described in the following sections, respectively.

2.1 He et al.'s Scheme: Basic User Privacy

In 2004, He et al. proposed a scheme to protect the location privacy for mobile users [7]. The scheme contains the *registration* protocol and the *controlled connection* protocol. In the *registration* protocol shown in Figure 2.1, each mobile user can obtain an alias from the system through the technique of blind signatures.

After obtaining an alias, the mobile user will use the alias in the *controlled connection* protocol such that the system and eavesdroppers cannot know who the mobile user is. Once the mobile user can perserve the identity privacy, her/his location privacy is also guaranteed. Figure 2.2 illustrates

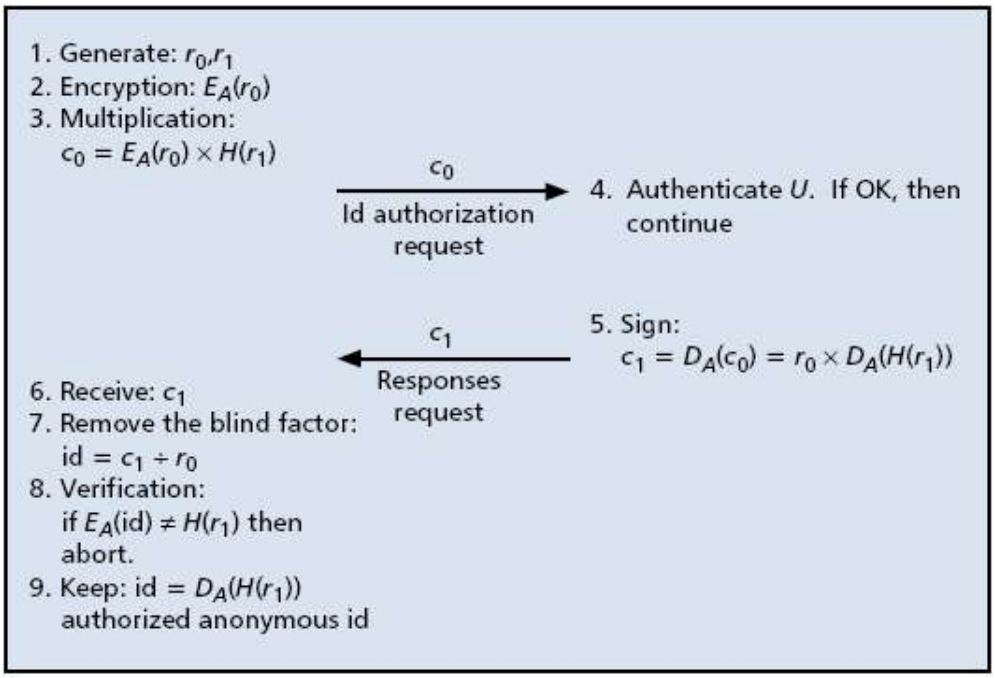

Figure 2.1: The registration protocol

the details of the protocol.

In He et al.'s scheme, the authors did not mention the problem of billing. Most of the researches on anonymity in mobile communication did not consider the billing issue, either. In an anonymous authentication protocol, the system operator does not know the real identities of anonymous mobile users. In [1], the authors pointed out that it will conflict with the need for billing if the system operator cannot know the anonymous users' real identities.

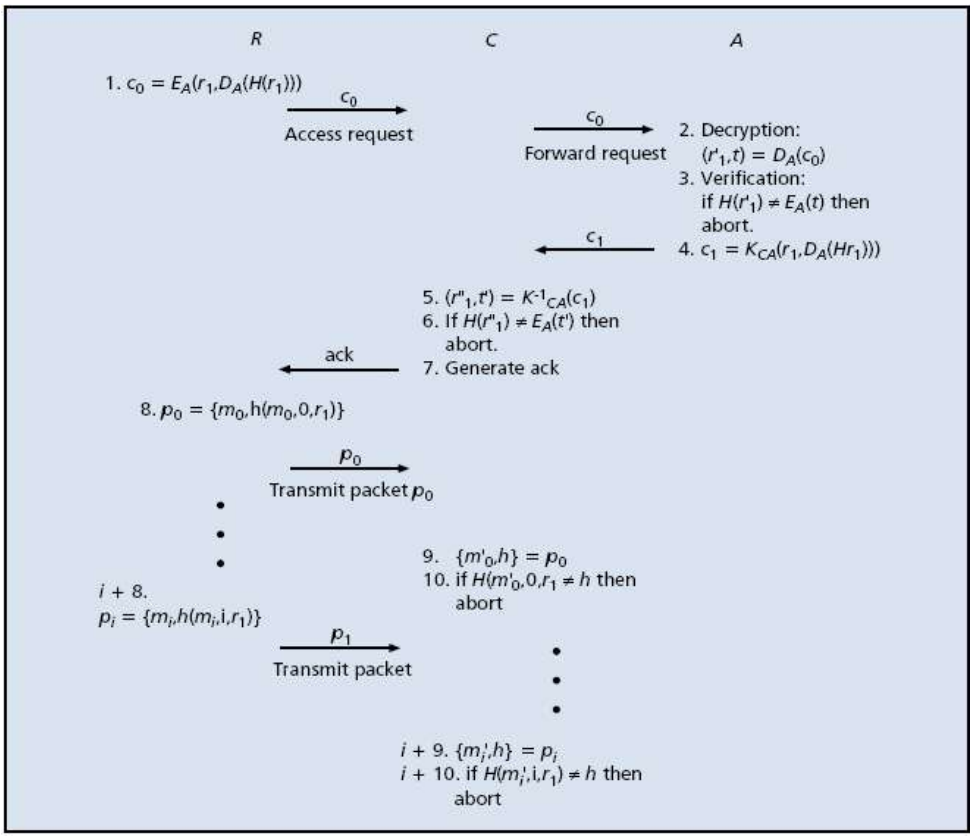

Figure 2.2: Controlled connection protocol

2.2 Tracz et al.'s Scheme: A Conceptual Schema for Charging Anoymous Users

In 2001, Robert Tracz and Konrad Wrona proposed an electronic cash withdrawal and change return protocols for wireless networks [13]. The scheme is merely a conceptual schema and the detailed design was not addressed. Figure 2.3 illustrates the *Withdrawal* protocol.

After the payer got a certificate, she/he can take it to access communication resources via the *change return* protocol shown in Figure 2.4.

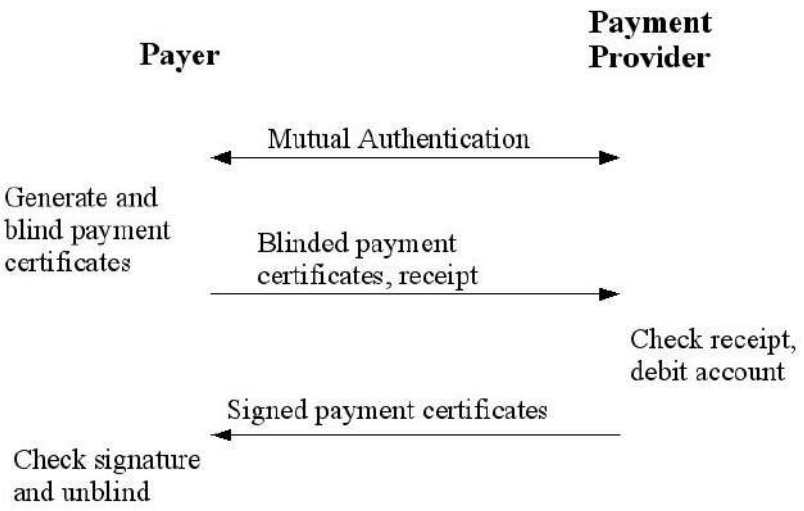

Figure 2.3: Withdrawal protocol

This is a pre-charging method. The payer must pay a fixed amount of money to the payment provider to purchase a certificate with the same value of the money from the provider. The payer can obtain the communication services by consuming the value of her/his certificate. However, there exists a problem that the payer may overspend the value of her/his certificate or the services will be terminated by the system when the value of the certificate has been used up.

If the network service is a time-period[1] service, before the payer terminates her/his using of network service, the payee or payment provider do not know how many values the payer will spend. Hence, the payment provider need to care about the extra issue of payer's overspending.

This scheme guarantees the anonymity for users. However, a perfect anonymity is not suitable for real world. In mobile network environments,

[1]The service provider must charge the payer according to her/his using time.

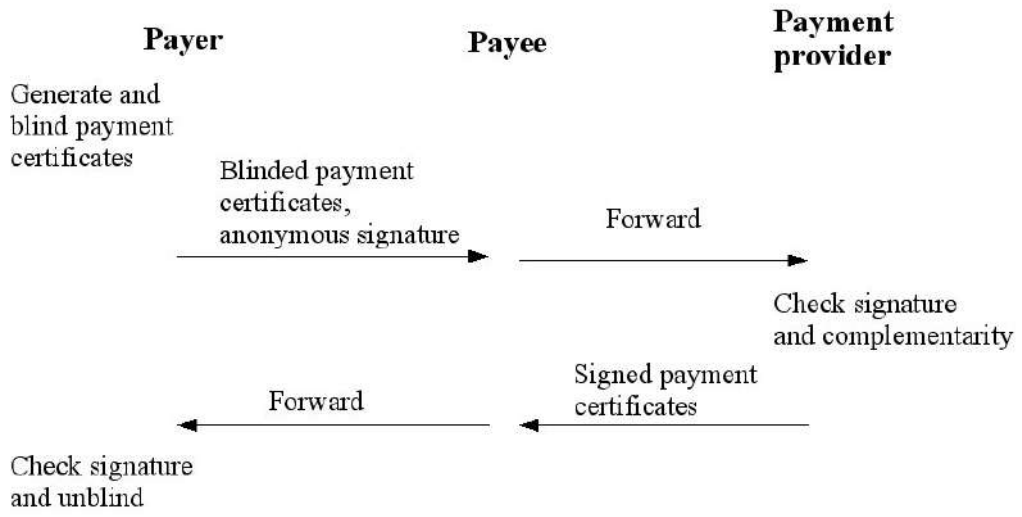

Figure 2.4: Change return protocol

a malicious mobile user like swindle bloc will exploit the privacy facilitation to illicitly obtain behoof from other mobile users. If every mobile user has perfect privacy, malicious parties may misuse the property to commit crimes. Hence, we need a mechanism to prevent the irregularities. If any mobile user transgresses the law, the judge can revoke her/his anonymity at any time. We call it **Fair Privacy**.

2.3 Jakobsson and Yung's scheme: Fair Privacy

A well electronic cash scheme usually supports chargeability and anonymity. Hence, We think that an electronic cash scheme can be adopted to mobile network environments. In this section we review a farther electronic scheme which support fair privacy. In 1996, Markus Jakobsson and Moti Yung pro-

posed an off-line electronic cash scheme [14], which provides the traceability and revokability of electronic cash when the anonymity is misused. The scheme contains the three protocols: withdrawing a coin, spending a coin, and depositing a coin. Here, we focus on the withdrawing protocol and the *limiting privacy* proposed in this paper. The withdrawing protocol is described below.

Withdrawing a Coin: Alice will withdraw a coin by engaging in the following 3-party protocol:

1. Alice picks

$$\begin{cases} K_B \in_u \mathcal{K}_B \\ K_O \in_u \mathcal{K}_O \\ x \in \mathcal{X}_C oin \end{cases}$$

and calculates

$$\begin{cases} \overline{K}_B = E_{Bank}(K_B) \\ \overline{K}_O = E_{Ombudsman}(K_O) \\ y = f(x) \\ \overline{y} = E_{K_O}(y) \\ \overline{id} = E_{Bank}(id) \\ \overline{\overline{id}} = E_{K_O}(\overline{id}) \end{cases}$$

where id is Alice's identity. She sends $(\overline{K}_B, \overline{K}_O, \overline{y}, \overline{\overline{id}})$ to the Bank and identifies herself to the bank.

2. The bank sends the ombudsman the quadruple $(\overline{K}_O, \overline{y}, \overline{\overline{id}}, n))$, where n is a unique withdrawal session number.

3. The ombudsman calculates

$$\begin{cases} K_B = D_{Ombudsman}(\overline{K}_O) \\ y = D_{K_O}(\overline{y}) \\ \overline{id} = D_{K_O}(\overline{\overline{id}}) \\ \sigma = S_{Ombudsman}(y) \end{cases}$$

and send $\overline{id}$ to the Bank, who verifies that $D_{Bank}(\overline{id}) = id$. Interacting with each other, and using a normal blinded signature protocol, the ombudsman and the bank produce $s = S_{Bank}(\sigma)$ in a way so that y and σ are blinded from the bank. The ombudsman verifies that $V_{Bank}(\sigma, s) = 1$, sends $\overline{s} = E_{K_O}(s)$ to the bank, and enters $(n, y, K_O, \overline{id})$ in its database.

4. The bank sends $\overline{s}$ to Alice , and stores $(n, id, \overline{s}, \overline{\overline{id}})$ in its database. The bank subtracts the value of the coin from Alice's balance.

5. Alice calculates the value $s = D_{K_O}(\overline{s})$, and then verifies that $V_{Bank,Ombudsman}(y, s) = 1$, and then saves (x, s).

After a user withdraws a coin, she/he may spend her/his coin and the shop would deposit this coin to the bank. This scheme also limit the user's behavior by limiting the privacy of the user. The following is a description of limiting the privacy by revoking the anonymity.

Limiting the Privacy by Revoking the Anonymity: If somebody is sus-

pected of a serious crime, the bank can obtain a court order allowing it to have the privacy removed for some specific withdrawal session n or some coin serial number y. The bank sends this court order to the ombudsman, along with either the specified n or y. The ombudsman searches its database and responds with the $(n, y, K_O, \overline{id})$ used for the withdrawal. The bank looks up $(n, id, \overline{s}, \overline{\overline{id}})$ in the database and verifies that

$$\begin{cases} s = D_{K_O}(\overline{s}) \\ V_{Bank,Ombudsman}(y, s) = 1 \\ \overline{id} = D_{Bank}(\overline{\overline{id}}) \\ id = D_{K_O}(\overline{id}) \end{cases}$$

The bank now know the triple (id, y, s), so that the coin has been traced.

Chapter 3

Privacy Requirement in Mobile Network Environments

Before designing a protocol for user privacy, we need to discuss some important privacy issues which will happen in the mobile network environment. According to the analysis on these issues and the mobile network environment, we can excogitate some privacy requirements for our scheme.

3.1 The Mobile Network Environment

There are several kinds of mobile networks nowadays, like 2G/3G GSM systems, WLAN, and so forth. The mobile network architecture is usually composed by a home network, several visiting networks, and many mobile stations, just as the case of the 2G GSM system. Even though a payment system is implemented in wireless LAN which uses the wireless EAP dialog [5] or other kinds of network, it also usually adopts such network architec-

ture. We call it **Distributed Architecture**, shown in Figure 3.1. In the Distributed Architecture, there are authorities in the home network and every visiting networks. The visiting networks are used to reduce and share the overload of the home network. They are like remote agents of the home network. In a GSM system, the authorities are called Home Location Register (HLR) and Visiting Location Network (VLR). The connecting lines between visiting networks and home network are called system core networks. Every mobile user can roam between the visiting networks but does not need to attach to the home network directly. A mobile user cannot access the system core network directly but she/he can communicate with home authentication server via the attaching server of the visiting network. Our protocol is based on the network of distributed architecture.

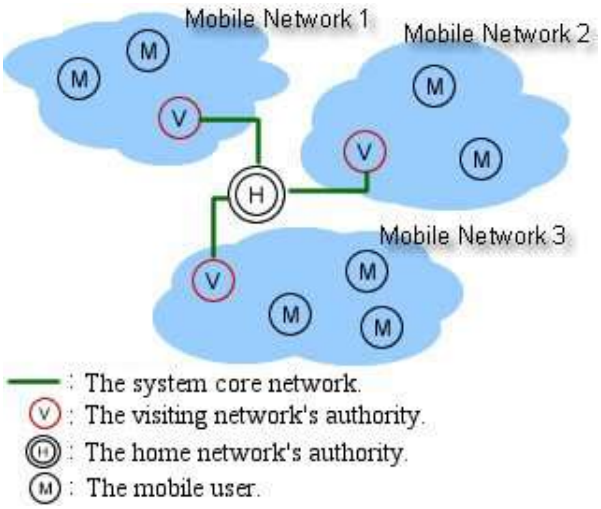

Figure 3.1: Mobile network environment

3.2 Privacy Overview

In this section, we review some important definitions about privacy. In [4], the authors proposed three different privacy requirements:

(1) Content privacy:

A message with content privacy is a protected message against eavesdroppers. Any eavesdropper cannot determine the exact meaning of the messages with content privacy. Usually, a sender and a receiver will communicate with each other by using a shared secret key to encrypt their exchanging messages. In order to achieve the content privacy, the sender and the receiver must share a secret key and the encryption algorithm in advance. In general, the shared secret key is established in an authentication phase. Before the parties begin to communicate, they will authenticate with each other and establish the secret key in passing. The shared secret key cannot be revealed to anyone else in the authentication phase. Besides, the security of the encryption algorithm determines the confidentiality of the exchanged messages. Hence, a standard encryption algorithm is recommended such that the encrypted messages cannot be decrypted by the eavesdroppers.

(2) Identity privacy:

Identity privacy means that mobile users will not reveal their identities to other parties such as other users, eavesdroppers, and even the system operator. Sometimes mobile users may need to access some sensitive resources, and hence they do not hope to reveal their identities in the

situations. To cope with the problem, a straight-forward solution is alias. Mobile users usually use alias when they were roaming in the mobile computing environment. However, there is a serious problem that the system operator may not charge anonymous mobile users if they do not reveal their real identities to the system operator. Basically, mobile users can hide their real identities from eavesdroppers only.

(3) Location privacy:

Mobile users' locations are also sensitive information. If mobile users get identity privacy, they may have location privacy. But there also exist routing problems for the system operator. The system operator must know mobile users' locations in order to make correctly and efficient routing to transmit messages to the users when they are being receivers. Hence, mobile users may not have location privacy against the system operator.

Ideally, most mobile users hope to possess full privacy, i.e., they can hide their communication messages, identities, and locations from the system operator and eavesdroppers. In [1], the authors defined five levels on untraceability, which are described as follows.

- C_1**: Hiding User Identity from Eavesdroppers.** In this case, the system usually assigns an alias for every mobile user. When the mobile user uses the alias to roam over the mobile network, the foreign authorities can authenticate her/him and know who she/he is, but the eavesdroppers cannot know her/his real identity.

- C_2: **Hiding User Identity from Foreign Authorities.** Mobile users just need to prove their qualification for receiving the services from foreign authorities but they does not show their real identities to the foreign authorities.

- C_3: **Hiding Relationship Between the User and Authorities.** A mobile user hides her/his home authority from the eavesdroppers. In this case, there are less information of the mobile user which will be known by the eavesdroppers.

- C_4: **Hiding the Identity of the Home Authority from Foreign Authorities.** Sometimes, a mobile user may roam into the service area of a less trusted foreign authority. She/He may also need to hide the identity of her/his home authority.

- C_5: **Hiding User Behavior from the Home Authority.** In this case, a mobile user not only hides her/his identity from the home authority but also hides her/his location. This case indicates perfect user privacy, where any other entity cannot know any personal information of a mobile user when she/he roams over the mobile network.

The basic requirements of privacy should satisfy C_1, C_2, and C_3, just as the case in the current GSM systems. Level C_5 is the perfect privacy for mobile users. In the next generation of mobile communications, the user privacy must be at level C_4 or C_5.

3.3 Privacy Requirement

In order to simplify the analysis on the privacy from the mobile users' points of view, we regard the home domain authority and the visiting domain authorities as an unitary system. We hope that every mobile user can obtain the user privacy protection at level C_4 or C_5 which are introduced in section 3.2. For basic user privacy, it is necessary to hide the identity of every mobile user from the system operator, eavesdroppers, and any other mobile user. We think that the location of a mobile user must be known by the system because of the communication routing problem. The system operator has to take the responsibility for routing, so that it can transmit messages to the designated mobile user. Here, we give a modified privacy requirement and C_5 in Figure 3.2. In the Figure 3.2 the f is a full identity of a mobile user, h is the identity of the home domain, r is the identity of the remote/visiting domain, H is the home domain authority, R is a remote domain authority, L is a legitimate mobile user, E is an eavesdropper, and 1/0 expresses knowing/unknowing. In our modification, the remote domain authorities know the identity of the home authority of mobile users, and the home authority knows where the mobile user is. These are the differences between our proposed privacy requirement and the perfect privacy case C_5.

Besides, we must protect the privacy of the contents of the transmitted messages. Hence, for the requirement of content privacy, we have to establish a secure channel for every communication session.

	H	R	L	E
f	0	0	0	0
h	1	1	0	0
r	1	1	1	1

C_5

	H	R	L	E
f	0	0	0	0
h	1	0	0	0
r	0	1	1	1

Figure 3.2: Modified privacy requirement

3.4 Anonymity Issues

In addition to the above privacy requirements, we also have to pay attention to several anonymity issues.

1. **Dynamic anonymous identity**: When an anonymous user uses the same anonymous identity to roam over the mobile network, it may be traced by linking all of the communication sessions with the same anonymous identity together. We think that an anonymous user should use different anonymous identities in different sessions when she/he roams over the mobile network.

2. **No relation between aliases**: Relations between aliases of a user will break the privacy of the user even if they do not reveal the user's real identity. It would let eavesdroppers have more information to analyze the user's secret data.

3. **No checking list of real identities and anonymous identities in the system operator**: The system operator can authenticate an anonymous user directly when she/he is about to access the network

services. This will preserve the user's privacy since the system operator does not know the user's real identity.

4. **Non-misappropriation**: When the system operator authenticates an anonymous user directly, we must assure that any eavesdropper cannot utilize the mobile network services successfully by embezzeling any other mobile user's anonymous identity. An anonymous authentication protocol must ensure that only the real owner of the ticket can use it to roam over the mobile networks. An anonymous ticket just can be used for one time i.e. an anonymous identity cannot be re-used.

5. **An agreed session key**: If an anonymous user shared a session key with the system operator in advance, she/he might be traced by the system operator. This does not maintain the feature of user privacy. We hope that an anonymous mobile user does not share a session key with the system operator in advance. When an anonymous mobile user performs a mutual authentication operation with the system operator, they also establish a session key at the same time. After an anonymous user has been authenticated, she/he can communicate with the system operator by this session key.

6. **Traceability in some situations**: Because of the fairness principle, we need a mechanism to revoke users' anonymity if necessary.

7. **Chargeability**: An authentication protocol for mobile communications should allow the system operator to be able to charge anonymous mobile users without revealing their identities.

Before we design an anonymous authentication protocol for mobile networks, we must consider several problems. How can a mobile user get a valid anonymous identity which provides anonymity against the system operator and eavesdroppers? How can the system operator charge an anonymous mobile user without knowing her/his real identity? How can the judge trace the mobile user's behavior? When the anonymous mobile user transgress the law, the judge can revoke the anonymity of the illegal user. Most of the papers do not discuss the billing issue since it is difficult to reach both privacy and billing at the same time. However, ubiquitous computing environments will be provided by some businesses, which need chargeable mechanisms to charge the anonymous mobile users. Therefore, it is urgent to design an efficient authentication scheme with user anonymity and chargeability.

Chapter 4

Our Anonymous Ticket-Based Protocol

In this thesis, we focus on how to buy and use an anonymous ticket in the mobile network environments. We will apply an existent mutual authentication protocol in the proposed scheme. Each mobile user and the system operator must run a secure authentication protocol to authenticate with each other first. Then the authenticated mobile user can run our protocols to buy and use an anonymous ticket for mobile networks. We discuss them in Section 4.2.1 and Section 4.2.2.

In the buying phase, a mobile user must reveal her/his real identity to the system operator, and the system operator will record that she/he has ever bought a ticket. The mobile user must return her/his used ticket to the system operator at the due date of the ticket. If there is any mobile user does not return her/his used ticket at the due date, the system operator will know because the mobile users have been recorded at the buying phase.

After the mobile user bought a ticket successfully, the system operator can not trace her/him anymore. The mobile user can make use of her/his ticket to utilize the network services by an alias. Whenever the mobile user uses her/his ticket for requesting network services, she/he will get a new ticket which is returned from the system operator. The new returned ticket records that how much value the mobile user spent for the network services.

4.1 The Framework of Our Protocol

Our protocol is tailored for mobile network environments, like GSM or WLAN [5]. Before running our protocol, the user and the system must perform an existing secure **three-parties** mutual authentication protocol first, such as [2]. The authentication protocol must designed by using a hybrid solution which utilizes **Shared Key Cryptosystem(SKCS)** and **Public Key Cryptosystems(PKCS)**. A hybrid solution can guarantee that the identities of the users will not be revealed to eavesdroppers in the authentication phase [3]. Besides, the adopted authentication protocol must provide three secure channels between MS with V, between V with H, and between MS and H. In Figure 4.1, we can see that after MS mutually authenticated with V and H, she/he can run our protocol to buy an anonymous ticket via the secure channel and use the ticket to obtain services from the mobile networks.

Once an mobile user is authenticated by running an existing authentication protocol, H will know the identity of the user who wants to buy an anonymous ticket. Thus, H can record the identity of the user correctly at

the buying phase. The mobile user and H will perform the buying ticket protocol over a secure channel with their session key.

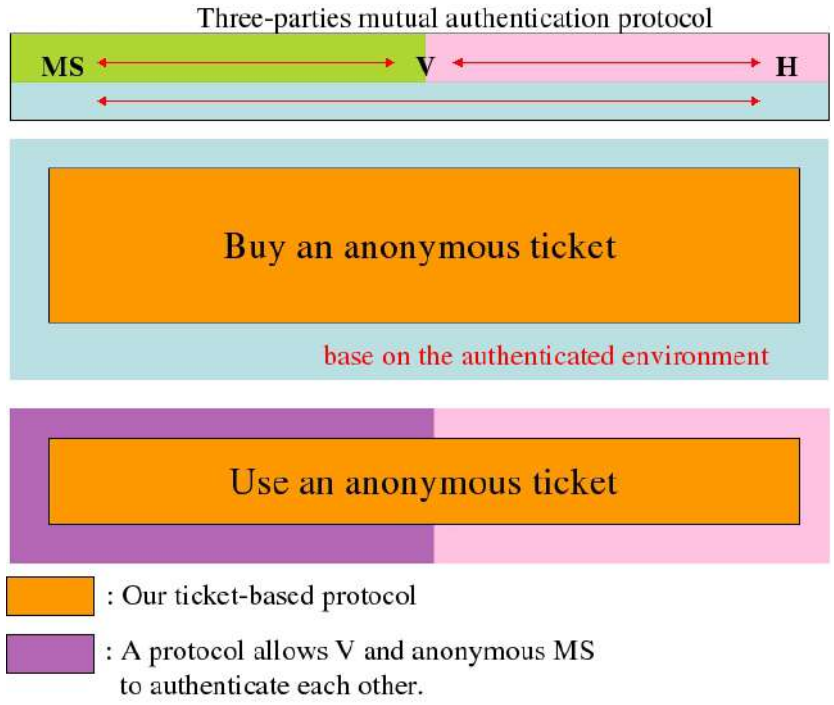

Figure 4.1: The framework of our protocol

4.2 Our Protocol

Before describing our authentication protocol, we define and explain some notations as follows:

1. $E_x(...)$: This is an encrypting function. If x is a symmetric session key, it is a symmetric encryption. If x is a public key, it will be a public-key encryption function. In general, a shared session key between entities A and B will be expressed as k_{A_B} and the encryption operation with

key $E_{A\_B}(...)$ is $E_{A\_B}(...)$. A public key of entity C will be denoted as pk_C and the encryption with the key is E_{pk_C}.

2. $F(...)$ **and** $h(...)$: These are two secure one-way hash functions. Given $m' = F(m)$ or $m' = h(m)$, it is computationally infeasible to derive m.

3. **A judge's device**: In our protocol, we adopt a judge's device which is issued by the judge. Before the device is issued, the judge can perform a public-testing for the functionality proof of the functions embedded in the device such that All of the entities can be convinced that the device is fair. The device is just a function box, and it cannot transfer any information out of the system operator by wire or wireless networks. The system operator must request a judge's device before it constructs mobile network services. The judge's device contains {a random number/string generator, a symmetric-key encrypting/decrypting function, a public-key encryption/decryption function, the public-secret key pair of the judge, two hash functions F and h, a secret seed z}. The judge's device will help the system operator with embedding some necessary information into a ticket.

4. $||$: This is the concatenating operator. For example, if $a = \{1234\}$, $b = \{5678\}$, and $c = a||b$, then $c = \{12345678\}$.

4.2.1 Buying a New Ticket

As mentioned in Figure 4.1, before a mobile user buys a ticket, she/he must run an authentication protocol to mutually authenticate with V and H. The

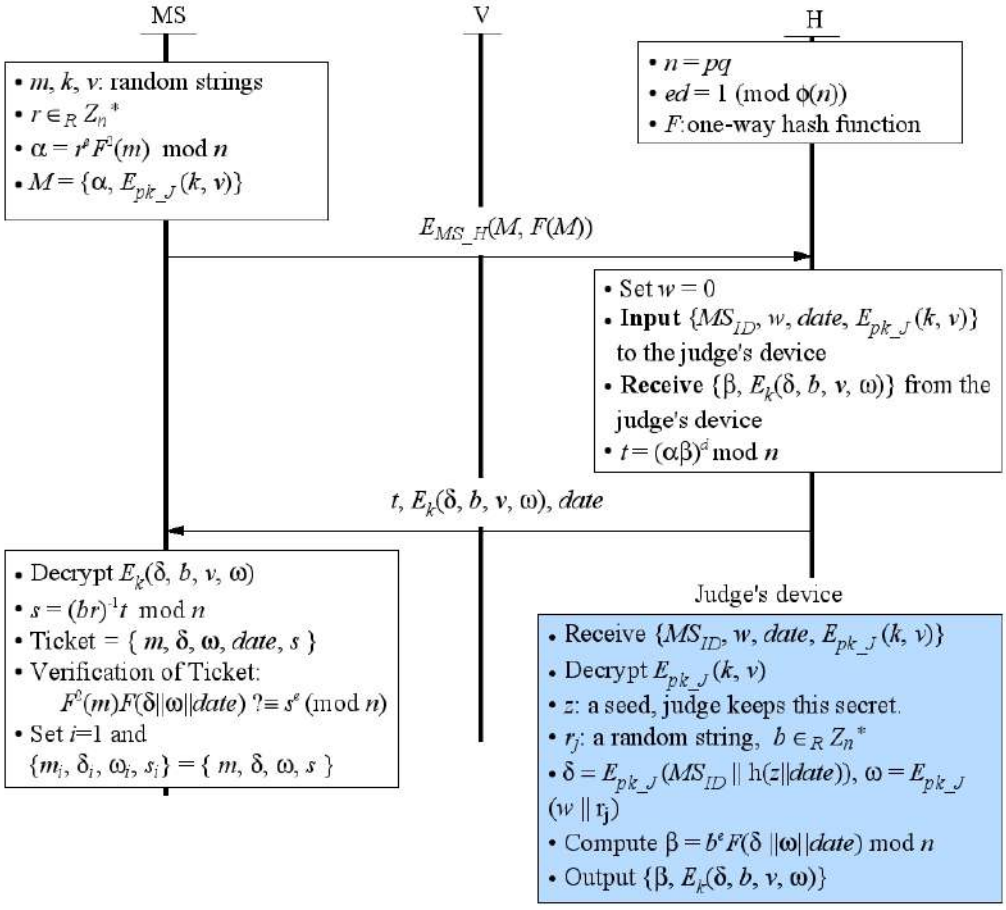

Figure 4.2: Description of our ticket-based protocol

authentication protocol will establish three shared session keys which are MS_H, MS_V, and V_H. Then the mobile user can run our ticket-based protocol to buy an anonymous ticket under the secure channel between MS and H. Our protocol contains the following steps:

1. **Initialization**: First, H chooses two distinct large primes p and q and computes $n = pq$. H also chooses its public key e and computes its secret key d as $ed = 1 \bmod \phi(n)$. Finally, H prepares a one-way hash

function F and publishes $\{n, e, F\}$. The variables p, q, and d will be kept secret by H.

2. $MS \rightarrow H : \{E_{MS\_H}(M, F(M))\}$. Before submitting $\{E_{MS\_H}(M, F(M))\}$ to H, MS generates three random strings $\{m, k, v\}$ and a random number $r \in_R Z_n^*$. Then MS computes $\alpha = r^e F^2(m) \bmod n$ and encrypts (k, v) as $E_{pk\_J}(k, v)$ by the judge's public key. Finally, MS arranges $M = \{\alpha, E_{pk\_J}(k, v)\}$ and computes the hashed value of M.

3. $H \rightarrow$ the judge's device : $\{MS_{ID}, w, date, E_{pk\_J}(k, v)\}$. In this phase, H knows that MS_{ID} wants to buy a ticket. H gives a due date $date$ for this ticket and sets $w = 0$. H then inputs $\{MS_{ID}, w, date, E_{pk\_J}(k, v)\}$ to the judge's device. The judge's device will help H with embedding MS_{ID}, w, and $date$ into the ticket where $date$ is the due date of this ticket.

4. The judge's device $\rightarrow H : \{\beta, E_k(\delta, b, v, \omega\}$. After receiving $\{MS_{ID}, w, date, E_{pk\_J}(k, v)\}$ from H, the judge's device generates random string r_j and random number $b \in_R Z_n^*$. Then it computes $\omega = E_{pk\_J}(w||r_j)$ and $\delta = E_{pk\_J}(MS_{ID}||h(z||date))$ first. H also computes $\beta = b^e F(\delta||\omega||date) \bmod n$. H decrypts $E_{pk\_J}(k, v)$ and uses k to encrypt δ, b, v and ω.

5. $H \rightarrow MS : \{t, E_k(\delta, b, v, \omega), date\}$. t is a blind signature which be signed by H. H computes $t = (\alpha\beta)^d \bmod n$

6. **Unblinding**: After receiving $\{t, E_k(\delta, b, v, \omega), date\}$, MS decrypts it by session key k and gets signature s by computing $s = (br)^{-1}t \bmod$

n. Then MS gets a valid ticket $\{m, \delta, \omega, date, s\}$. MS can verify the received ticket by checking if the following formula is true.

$$F^2(m)F(\delta||\omega||date) \equiv s^e \pmod{n} \tag{4.1}$$

Finally, MS sets $i = 1$ and $\{m_i, \delta_i, \omega_i, s_i\} = \{m, \delta, \omega, s\}$ and then goes to the i-round to use the ticket for obtaining services. When MS uses the ticket to request the network services, the system operator, H or V, will also verify the ticket via (4.1).

When a mobile user buys a ticket successfully, she/he gets a passport which allows her/him to use the network services. Each ticket can just be used once. While MS uses her/his ticket for network services, H will return a new one to her/him. Besides, H will maintain a flag to record that MS has ever bought a ticket. MS must return her/his used ticket to H at the due date to cancel the flag.

4.2.2 Using the Ticket for Network Services at i-th Round

In Figure 4.1, we have known that when an anonymous MS uses her/his ticket for network services, V and the anonymous MS have no secure channel for communicating. We have to design an authentication protocol for the anonymous MS and V. This protocol will also establish a secure channel for the anonymous MS and V. And since MS is anonymous, V cannot authenticate MS directly but it can verify that if MS is the real owner of

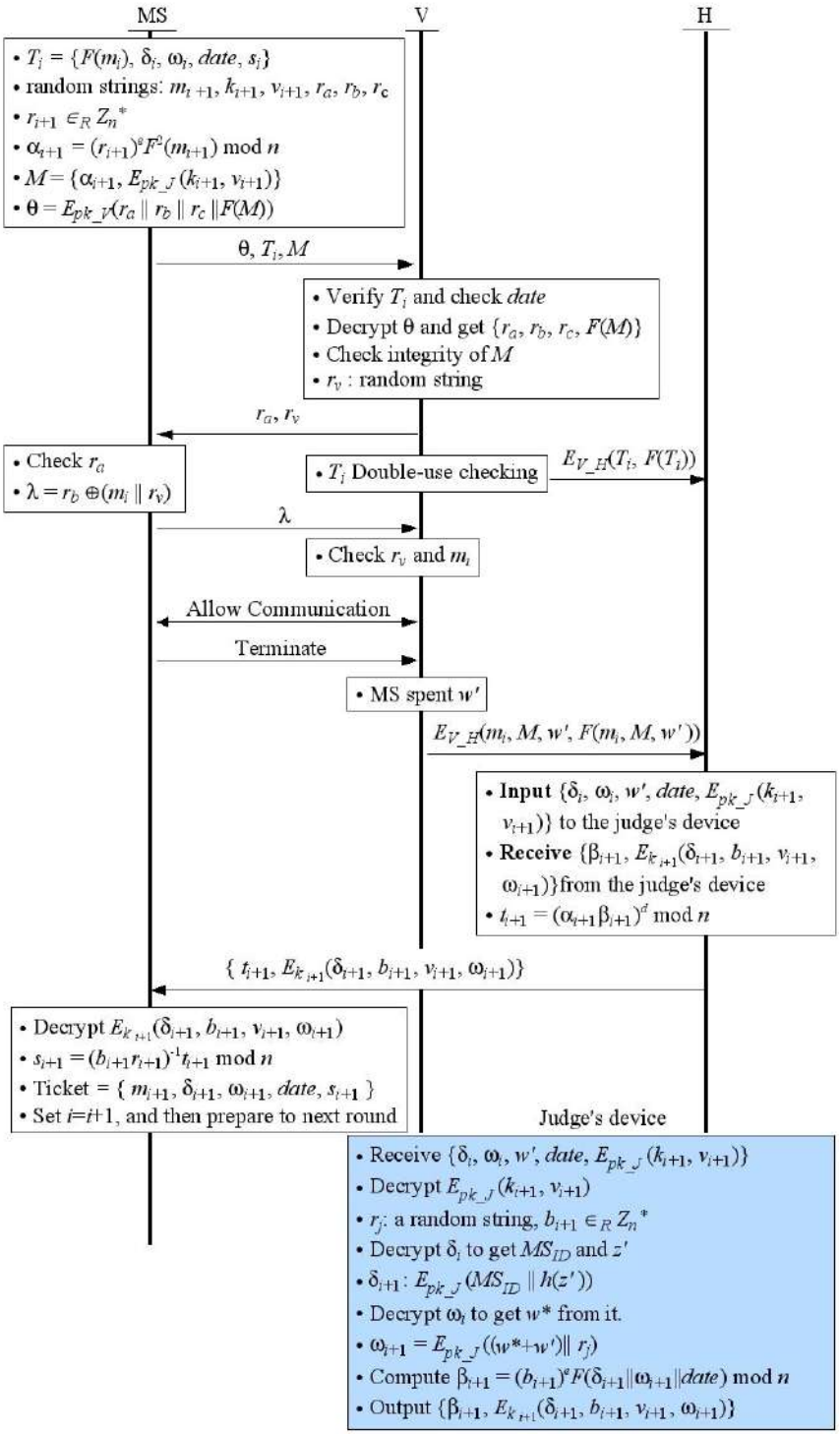

Figure 4.3: Anonymous MS uses his ticket for network services at the i-th round.

the shown ticket. We illustrate the protocol in Figure 4.3.

We use a fundamental technology, **Challenge-Response**, to design the authentication protocol. Challenge-Response is a common authentication technique. In a two-parties mutual authentication protocol, each of both parties is prompted a *challenge* and then provides a specific information called the *response* to the opposite side.

Before describing the authentication protocol, we assume that all the remote authorities V's have an identical public key. When the home authority emits identity cards, SIM cards, or other cards which are used to record users' private personal information, to MS's, it also stores the public key into the cards. Besides, the home authority will inform all remote authorities the identical public key and sends the corresponding secret key to them. The home authority must assure that the remote authorities are legitimate before it sends the secret key to the remote authorities. If the system operator wants to change this public key, it can send all MS's a new one via mobile networks and informs all related remote authorities. MS spends her/his ticket at the i-th round by performing the following steps:

1. **Preparation**: Before running the i-th round, MS prepares $T_i = \{F(m_i),$ δ_i, w_i, $date_i$, $s_i\}$ and generates random strings $\{m_{i+1}$, k_{i+1}, v_{i+1}, r_a, r_b, $r_c\}$ and random number $r_{i+1} \in_R Z_n^*$. Besides, MS computes $\alpha_{i+1} = (r_{i+1})^e F^2(m_{i+1}) \bmod (n)$. Then MS prepares M which contains α_{i+1} and $E_{pk\_J}(k_{i+1}, v_{i+1})$. Finally, she/he prepares $\theta = E_{pk\_V}(r_a||r_b||r_c||$ $F(M))$.

2. $MS \rightarrow V : \{\theta, T_i, M\}$. MS divides her/his ticket into two parts. T_i is

the first part and MS sends T_i to V at this time. The string θ contains some information which will be used in this session, and M contains some ticket information which will be signed by H in the next round.

3. $V \rightarrow MS : \{r_a, r_v\}$. After receiving T_i, V will verify it via (4.1) and check if the due date *date* is expired. If T_i and *date* are valid, V decrypts θ to get $\{r_a, r_b, r_c, F(M)\}$. V checks if the hash value of M equals to $F(M)$ and generates a random string r_v. V answers r_a and sends r_v to MS.

4. $MS \rightarrow V : \{\lambda\}$. After receiving r_a and r_v, MS checks if r_a is the same as the one which is chosen by herself/himself previously. Then MS computes $\lambda = r_b \oplus (m_i || r_v)$ and sends $\lambda$to V. At the same time, V sends T_i to H and H performs the double-use checking of T_i. If the ticket is doubly used, the authentication will be terminated by H.

5. **Allowing Communication**: H performs the double-use checking, and V verifies if r_v equals to the one that is chosen by itself previously and checks whether the hashed value of m_i is the same as $F(m_i)$ of ticket T_i. Then V ensures that the ticket T_i is valid and MS is the real owner of T_i. Therefore, V allows MS to communicate. During the communication, MS encrypts her/his transmission messages by session key r_c.

6. $V \rightarrow H : \{E_{V\_H}(m_i, M, w'), F(m_i, M, w')\}$. After MS terminated the communication, V computes the expense w' of MS according to MS's communicating time or utilized services. Once H receives the spent

value w' of MS, H stores $\{T_i, w'\}$ into database. The record indicates that MS spent w' units via T_i.

7. $H \rightarrow$ The judge's device: $\{\delta_i, w', date,\ E_{pk\_J}(k_{i+1},\ v_{i+1})\}$. H extracts δ_i and $date$ from the ticket T_i. The string δ_i is the identity factor where the real identity of MS is embedded in it.

8. The judge's device $\rightarrow H : \{\beta_{i+1},\ E_{k_{i+1}}(\delta_{i+1}, b_{i+1},\ v_{i+1},\ \omega_{i+1})\}$. δ_{i+1} is the identity factor for the next round. The judge's device prepares δ_{i+1} by decrypting δ_i to get MS_{ID} and z'. Then it computes δ_{i+1} as $E_{pk\_J}(MS_{ID}||h(z'))$. Besides, ω_{i+1} is the amount of spent value, the judge's device gets $w*$ by decrypting ω_i and computes $\omega_{i+1} = E_{pk\_J}(w* +w')||r_j)$ where r_j is a random string. Finally, the judge's device randomly chooses $b_{i+1} \in_R Z_n^*$ and computes $\beta_{i+1} = (b_{i+1})^e F(\delta_{i+1}||\omega_{i+1}||$ $date) \bmod n$.

9. $H \rightarrow MS : \{t_{i+1},\ E_{k_{i+1}}(\delta_{i+1},\ b_{i+1},\ v_{i+1},\ \omega_{i+1})\}$. H computes a blind signature $t_{i+1} = (\alpha_{i+1}\beta_{i+1})^d \bmod n$ and returns it to MS.

10. **Unblinding**: After receiving the information in step 9, MS decrypts $E_{k_{i+1}}(\delta_{i+1},\ b_{i+1},\ v_{i+1},\ \omega_{i+1})$ to get $\{\delta_{i+1},\ b_{i+1},\ v_{i+1},\ \omega_{i+1}\}$. Then MS unblinds t_{i+1} by computing $s_{i+1} = (b_{i+1}r_{i+1})^{-1}t_{i+1} \bmod n$. MS gets a new ticket $\{m_{i+1}, \delta_{i+1}, \omega_{i+1}, date_{i+1}, s_{i+1}\}$ and MS can verify her/his ticket at the i-th round by the following formula:

$$F^2(m_i)F(\delta_i||\omega_i||date_i) \equiv s_i^e \pmod{n} \tag{4.2}$$

If (4.2) is true, MS sets $i = i + 1$, and she/he can use the new ticket in the next round of authentication.

4.2.3 Charging Mobile Users

Before the due date, MS can use her/his ticket for unlimited times. Whenever she/he uses her/his ticket for requesting services, H will returns her/him a new one which contains new value. The new value equals to the value of the previous ticket plus the value of his spending at this time. At the due date, H will charge MS through the following steps:

1. MS submits her/his identity and the used ticket T_i to H on the due date.

2. H checks that T_i does not exist in its database, and then extracts ω_i from T_i and sends it to the judge's device.

3. The judge's device decrypts ω_i and returns the spent value to H.

4. H adds the spent value to the bill of MS.

About the charging method, our scheme is different from the others which provided approaches of charging a mobile user before she/he uses mobile network services. In our method, the system operator charges a mobile user after she/he makes use of the mobile network services. What are the differences between charging mobile users in advance and charging them later? The followings are the reasons why we design our scheme to charge a mobile user after she/he makes use of the network services:

1. **Reducing the relations between any two rounds of communication**. There are two possible ways to charge a mobile user in advance, which are described as follows:

   Case 1: The mobile user purchases a set of payment tokens from the system previously where each of the tokens is with a unit value. In each round of communication, the mobile user sends a proper number of tokens to the system for payment. In this case, there is no relation between any two rounds of communication in some situations because each token is independent. However, this will consume a lot of storages for recording these tokens.

   Case 2: The mobile user purchases only one payment token from the system previously where the token is with a specific value w. In the following round of communication, the mobile user sends the token to the system for payment and then the system will return a token with value $w-w_1$ if the user consumes w_1 value of that token in the round of communication. The mobile user just needs one storage to store the token. But this will cause defective privacy. For example, if a mobile user carries a token with value 100 dollars to use the mobile network services and spends 30 dollars, the system will return her/his a new token with value 70 dollars. Next time, when the mobile user shows the token with value 70 dollars, the system may be able to learn that the two rounds of communication are initiated by the same user.

   In our scheme, we greatly reduce the relations between any two rounds

of communication from the system's point of view with one-token storeage only.

2. **Free from the problem of overspending**. When a mobile user shows her/his token to the system for communicating, the communication will be terminated if the token's value is used up. It will cause inconvenience for the mobile user. If the system does not terminate the communication, the mobile user will overspend the token and the system must perform extra procedures to deal with the situation.

   In our scheme, the above situation can be avoided.

4.2.4 Privacy Revoking

In some special situations, H or the judge needs to disclose the identity of an anonymous mobile user. For example, an anonymous mobile user commits a crime; the police wants to trace some criminals; or some mobile users who do something harmful for H. Our protocol supports two ways to trace illegal anonymous mobile users.

1. **Tracing the mobile user by a designated ticket**: When a mobile user uses her/his ticket to commit a crime, her/his ticket will be reported to the judge. Assume that the ticket is $T_i = \{F(m), \delta, \omega, date, s\}$. The judge will extract δ from the ticket and decrypt δ to get MS_{ID}.

2. **Tracing the tickets by a designated mobile user**: When the police wants to trace a criminal, the police will ask the judge to disclose the privacy of the criminal. In this case, the judge will compute

$$\delta_1 = E_{pk\_J}(MS_{ID}||h^1(z||date))$$
$$\delta_2 = E_{pk\_J}(MS_{ID}||h^2(z||date))$$
$$\delta_3 = E_{pk\_J}(MS_{ID}||h^3(z||date))$$
$$\vdots$$
$$\delta_i = E_{pk\_J}(MS_{ID}||h^i(z||date))$$

and send $\delta_1, \delta_2, \delta_3, \ldots, \delta_i$ to the system, and the system will help the police to trace the mobile user. In our protocol, the mobile user will use T_1 with δ_1 for the first round, T_2 with δ_2 for the second round, and so forth. According to this order, the system can trace the criminal from the first round to the i-th round via $\delta_1, \delta_2, \delta_3, \ldots$, and δ_i.

4.2.5 Exceptions

In addition to the above issues, there are still two exceptions that may happen in our protocol. One is that the mobile user denies returning her/his ticket, and the other one is that the mobile user loses her/his ticket (or loses her/his mobile equiptment).

1. **The mobile user denies to return her/his ticket**: When a mobile user buys a ticket, H records some related information and knows that the mobile user must return a used ticket on the due date. If the mobile user denies to send her/his ticket back, H will ask the judge to reveal the set of δ of the mobile user. H submits MS_{ID} and *date* to the judge, and the judge returns H a set of $\{\delta_1, \delta_2, \delta_3, \ldots,$ and $\delta_i\}$. Assume that the mobile user denied to return the T_{i+1}, H will find the T_i from its database via the set of $\{\delta_1, \delta_2, \delta_3, \ldots,$ and $\delta_i\}$. The system's database

stored a lot of pairs of $\{T_i, w'\}$. When H finds T_i and w^*, the judge can help H with extracting the spent value w^* of T_i, and then H computes $w'' = w^* + w'$ and charges MS the value w''.

2. **The mobile user lost her/his ticket**: When a mobile user lost her/his ticket, she/he must ask H to freeze her/his ticket or her/his ticket may be used by another user. In our protocol, when a mobile user lost her/his ticket, she/he must reveal her/his identity to H in order to freeze her/his ticket. According to the MS_{ID} and *date*, H asks the judge to compute the set of $\{\delta_1, \delta_2, \delta_3, \ldots,$ and $\delta_i\}$. Assume that the mobile user lost T_i, H must deny the service for T_i, T_{i+1}, and so on, and H will charge the mobile user by the spent value T_i.

   In order to handle this exception, the mobile user must reveal her/his identity to H, so that she/he will lose the privacy from $T_1, T_2, T_3, \ldots,$ and T_i. If the mobile user remembered how many times she/he has used the ticket, she/he can preserve still her/his privacy. For example, a mobile user lost her/his ticket, and she/he remembers that she/he has used her/his ticket for 5 times. Then the judge just needs to compute δ_5 for H, and δ_2, δ_3, δ_4 are still be kept secret for the mobile user.

Chapter 5

Security Analysis

In our protocol, we adopts the technique of blind signature to design the protocol for a mobile user to buy a ticket, and after a mobile user used her/his ticket, the system operator returns her/him a new one. Besides, before a mobile user uses her/his ticket, she/he must mutually authenticate with the system. Hence, we analyze the security on authentication and blind signatures.

5.1 The Security Analysis on Authentication

From Figure 4.1, an authentication protocol for the anonymous MS and V is required. We examine the following attacks on the authentication protocol.

5.1.1 The Replay Attack

If an attacker replays the messages transmitted between the system and a mobile user and they cannot detect the event, the replay action will be

successful. At the i-th round, our authentication protocol for an anonymous MS and V contains three transmissions. We will demonstrate that it can be detected by the system or the user if any of these transmissions is replayed.

<**1**> $MS \rightarrow V : \{\theta, T_i, M\}$. If this message is replayed, the attacker cannot pass the authentication successfully. Because that the attacker cannot show m_i of the T_i. Only the real owner of T_i knows the corresponding m_i. If the attacker replays $\{\theta, T_i, M\}$ and $\{\lambda\}$, it will be detected by V because of the random string r_v, where V randomly chooses the string r_v in each round.

<**2**> $V \rightarrow MS : \{r_a, r_v\}$. If there is a fake V wants to cheat MS of her/his m_i, the fake V will be detected by MS because of the random string r_a. The fake V cannot decrypt θ to get r_a.

<**3**> $MS \rightarrow V : \{\lambda\}$. If an attacker replays λ directly, it will be detected by V according to random strings r_v and r_b. The variables r_v and r_b are chosen differently in each round.

5.1.2 The Impersonate Attack

It is easy to copy a T_i of any MS from the transmission. However, it is difficult to use the copied T_i to impersonate MS since it will be detected in our protocol.

<**1**> **Impersonate** MS: V authenticates MS by verifying her/his ticket T_i and checking the secret m_i. Only the real owner has the corresponding

m_i of T_i. As long as the hash function $F(\ldots)$ is secure enough and MS keeps its m_i secret, anyone else cannot obtain m_i to impersonate MS.

<2> **Impersonate** V: Similarly, the attacker cannot impersonate V. A fake V will be detected by MS since it cannot send the correct r_a to MS. As long as the public key cryptosystem is secure enough and V keeps the secret key, no one can decrypt θ and then return correct r_a to MS.

5.2 The Security Analysis on Blind Signatures

When a mobile user buys a ticket or gets a returned new ticket after using her/his ticket, she/he always follows the procedure of a blind signature protocol. In this section, we discuss possible attacks on blind signatures in our protocol to examine the security of the protocol.

5.2.1 Message Modification

If the attack works, a malicious mobile user can change an original signature to a modified one. Before sending messages to system for requesting the signatures, the malicious mobile user can choose a special message in order to change the content of the returned signature. In Figure 4.2, the message which the malicious mobile user can choose is α. We analyze the computation formula of the signature which is $(F^2(m)F(\delta||\omega||date))^d$, where the verification formula is (4.1). The variables δ and ω are unpredictable for

the malicious mobile user when she/he is choosing message α. The malicious user does not know how to choose a special α to modify the content of the signature.

5.2.2 Message Replacement

If an attacker replaces a message which is prepared for the system to sign and the replacement causes that the legal user cannot get a valid ticket, then the attack works.

<**1**> $MS \rightarrow H : \{E_{MS\_H}(M, F(M))\}$. In Figure (4.2), if the transmission is replaced, it will be detected by H after H decrypts the message and checks the hashed value of M.

<**2**> $H \rightarrow MS : \{t, E_k(\delta, b, v, \omega), date\}$. If any variable of this transmission is replaced, it will be detected by MS via the verification formula (4.1). Even if t and $E_k(\delta, b, v, \omega)$ are replaced simultaneously by valid t, δ and ω, MS can still detect it via v which is chosen by herself/himself.

<**3**> $MS \rightarrow V : \{\theta, T_i, M\}$. In Figure (4.3), M is the message which is prepared for H to sign. θ and M are combined by function F. Attackers must replace θ and M at the same time or H will detect the replacement when checking the hashed value of M. However, once an attacker replaces θ and M, it will be detected by MS because of the incorrect r_a.

<**4**> $V \rightarrow H : \{E_{V\_H}(m_i,\ M,\ w',\ F(m_i, M, w'))\}$. If the transmission is replaced by another $\{E_{V\_H}(m_i',\ M',\ w'',\ F(m_i', M', w''))\}$, H will detect

it through different hashed values of m_i and $F(m_i)$.

<**5**> $H \rightarrow MS : \{t_{i+1}, E_{k_{i+1}}(\delta_{i+1}, b_{i+1}, v_{i+1}, \omega_{i+1})\}$. If any variable of this transmission is replaced, the formula (4.2) will not be true. And MS will find that $v_{i+1}$is incorrect.

5.3 The Security Requirements for Each Entity

In this section, we discuss some security requirements for mobile users and the system, respectively. We show that why our protocol satisfies the requirements.

5.3.1 The Viewpoints of Mobile Users

From the viewpoints of a mobile user, she/he would like to ensure the following requirements:

1. **Mutual authentication**: MS and V can be mutually authenticated by each other via performing the protocol of the steps <2>, <3> and <4> of Section 4.2.2. MS authenticates V by asking it if it knows the secret key of pk_J. And MS shows the secret m_i after she/he ensures that the V is legal. Once MS shows her/his m_i to V, V is convinced that MS is a legal user.

2. **None can impersonate** MS: According to <1> and <3> in Section 5.1.1 and <1> in Section 5.1.2,none can impersonate MS via the replay

or impersonation attacks.

3. **None can impersonate the system**: According to the <2> in Section 5.1.1 and <2> in Section 5.1.2, none can impersonate V.

4. **Ticket correctness**: When MS received a ticket in step <6> of Section 4.2.1, it can verify whether the received ticket is correct or not by equation (4.1). Besides, <1>, <2>, <3>, <4>, and <5> in Section 5.2.2 shows that nobody can destroy the correctness of the ticket.

5. **Ticket would not be stolen**: In our protocol, MS sends her/his ticket T_i to V without any protection but MS does not have to worry that T_i will be stolen. Since <1> in Section 5.1.2 shows that none can impersonate her/him to get m_i. The formula <2> in Section 5.1.2 demonstrates that none can impersonate V to cheat m_i out of MS. Besides, step <4> in Section 4.2.2 shows that MS encrypts m_i by short-term key r_b.

6. **Obtain privacy**: In steps <2>, <3>, and <4> of Section 4.2.2, MS does not reveal her/his identity to the system and eavesdroppers. Furthermore, there is no relation between tickets of any two rounds, so that the system cannot trace an anonymous mobile user via the information of T_i in each round.

7. **Secure communication channel**: In step <5> of Section 4.2.2, MS communicates with V via the secure channel r_c. MS sends the session key r_c to V by the public key of V.

5.3.2 The Viewpoints of the System

From the viewpoints of the system, including H and V, it would like to ensure the following requirements:

1. **Malicious mobile users cannot cheat the system**: In steps <3> and <4> of Section 4.2.2, V makes use of the mechanism of **Challenge-Response** to authenticate MS. This can withstand the replay attack like <3> in Section 5.1.1. Hence, malicious users cannot pass the authentication process. Besides, according to Section 5.2.1, malicious users cannot cheat the system to get a modified signature.

2. **None can impersonate the system**: According to <2> in Section 5.1.1 and <2> in Section 5.1.2, none can impersonate the system to cheat a mobile user to pass the authentication. And according to <2> and <5> in Section 5.2.2, none can impersonate the system to emit tickets.

3. **Charge anonymous mobile users correctly**: From the description in Section 4.2.3, the system can charge mobile users in general cases. Even in exception cases, the system can still charge mobile users as described in Section 4.2.5.

5.3.3 The Viewpoints of the Judge

For the judge, it needs a mechanism to revoke the privacy of the mobile users who misused the anonymity property. It also needs the capability of tracing a criminal who roams over the mobile networks. In our protocol, the

judge can supervise the illegal mobile users and criminals by <1> and <2> in Section 4.2.4.

Chapter 6

Comparisons

Before we design a protocol for user privacy, we focus on several features. In this section, we make comparisons of these features between our protocol and others which have discussed the issue of user privacy. First, we describe these features as follows.

1. **No relation**: It means that there is no relation between any two rounds of authentication actions performed by a mobile user and the system. If there is any relation information between any two rounds, this will bate the user privacy. For example, a mobile user always uses the same alias or session key to roam over the network. Even the value of ticket will reveal a mobile user's privacy. If the system gives a ticket with value $100 to a mobile user and then the mobile user uses this ticket for requesting the network services, the system can guess that the mobile user is the previous one with great probability.

2. **Secure channel**: After performing mutual authentication between

a mobile user and the system, they must establish a session key for the following secure communication activities. If the mobile user does not encrypt her/his messages during transmission, the contents of the messages may be revealed.

3. **Fair privacy**: Fair privacy contains **traceability** and **revokability**. If a crime happens, the police can trace the identities of related anonymous mobile users, or the judge can revoke the privacy of a criminal mobile user.

4. **Chargeability**: The system must have ability to charge anonymous mobile users, and it must charge these users according to the time of communication or the types of services they used.

When a mobile user is obtaining the network services, she/he would like to hide her/his identity from the system operator, H and V, and eavesdroppers for privacy consideration. This is the basic privacy requirement for a mobile user. Besides, a mobile user also cares about if there is any relation between any two rounds of authentication actions, which will reveal the privacy of her/his behaviors. The contents of transferred messages may also contain the mobile user's privacy. Hence, a mobile user needs to encrypt her/his transmitted messages with a session key after being authenticated. The system operator needs to charge the anonymous mobile users for the services it provided. And in order to uphold the law, we need fair anonymity where the anonymity will be revoked when a mobile user transgress the law. Hence, we also make comparisons about this property.

	Privacy					**Property**			
	Hide Identity			NoR	S	Fair		C	L
	H	V	E			T	R		
ours	◯	◯	◯	◯	◯	◯	◯	◯	◯
[5]	◯	◯	◯	×	◯	⋆	⋆	◯	×
[7]	◯	◯	◯	×	×	×	×	×	×
[8]	×	◯	◯	◯	◯	×	×	×	×
[9]	×	×	◯	◯	◯	×	×	×	×
[10]	×	◯	◯	×	◯	×	×	◯	◯
[11]	◯	◯	◯	◯	×	×	×	×	×
[13]	◯	◯	◯	×	×	×	×	◯	×

NoR: No relation between any two rounds.
S: Secure Channel.
T: Traceability. Trace the criminal user.
R: Revokability. Revoke the user's privacy.
C: Chargeability. Charge anonymous users.
H: Home domain. **V**: Visiting domain. **E**: Eavesdropper.
L: Charge a mobile user after she/he uses services.

Table 6.1: Comparison

Table 6.1 summarizes the comparisons between our protocol and the others.

In Table 6.1, the authors of [5] also mentioned untraceability revoking, but they did not realize it in their scheme. We think that untraceability revoking is not easily realized. Besides, the chargeability is achieved in [5] through an e-cash division method. However, the e-cash division method is much less efficient than ours, which adopted the change-return mechanism [13].

Chapter 7

Discussions

7.1 The Double-Use Checking of Tickets

Basically, when a user submits a one-time-use ticket to the system for requesting communication services, the system must immediately perform the double-use checking on the ticket. Because of the mechanism of privacy revoking in our protocol, the double-use checking can be off-line. Since our protocol guarantees that the user's ticket cannot be used by any other user, it must be spent by the real owner of this ticket if the system finds that a ticket was doubly spent. The system can extract the real owner's identity from the double-spending ticket and then charge the owner. The system will not get any loss whenever a ticket is doubly spent. The off-line double-spending checking will cause less latency when running our protocol.

7.2 The Judge's Device

Mobile users would like to preserve their privacy. The system operator hopes to make profits and the judicial entities want the users to obey the law. We adopt a judge's device to involve a fair third party into the proposed protocol. The judge should take the responsibility for punishing criminals, so that it must have enough capability to revoke the untraceability of any anonymous user who misused the property. In our protocol, the judge's device engages in embedding a mobile user's identity, a spent value, and a due date into her/his ticket. Embedding the mobile user's identity into her/his ticket is the responsibility of the judge's device for the purpose of anonymity revoking. Nevertheless, embedding the spent value and the due date into the ticket may be extra works of the device. Is it suitable for the judge's device to do the extra works?

We discuss two extreme cases. Is it suitable to transfer all works of the system operator to the judge's device? If we do this, the judge's device will know the secret signing key of the system operator because the judge's device needs to help the system operator to sign messages. This is not secure since the signing key of the system is supposed to be kept secret by itself for non-repudiation. On the other hand, if we let the system operator take over all of the works, it is hard to achieve both user privacy and anonymity revokability without the assistance of a trusted third party. Hence, these two extreme cases are not suitable for the design of our protocol.

Instead, under the considerations of security, privacy, and performance, we properly distribute the works to the system and the judge's device such

that the benefits of the system and the rights of the judge will not be affected in the proposed protocol.

Chapter 8

Conclusions

We have proposed a mobile authentication scheme which can authenticate mobile users anonymously. When a mobile user enters the anonymity mode, she/he can perform a mutual authentication operation with the system operator. The system operator can charge the anonymous user correctly according to the time she/he consumed. Furthermore, if some mobile user misuses the anonymity property, the judge will revoke her/his privacy and trace her/him.

In the proposed scheme, we adopt Chaum's blind signatures to realize our method. Hence, the mobile equipments might not have enough computation capabilities to handle the RSA encryption/decryption operations. In the future, we will attempt to implement our protocol by making use of a low-computation blind signature scheme and other user efficient cryptographic primitives. Besides, the privacy of a honest mobile user might be broken by the system operator if the mobile user lost her/his ticket since the system operator needs to trace her/his used tickets in order to find the spending value of her/him. It will be interesting to find an efficient solution to cope

with the above problem. Finally, how to achieve the anonymity of receivers is another interesting research problem. However, it seems to be a hard problem because that the system does not know how to transmit messages to a receiver if the receiver is anonymous to the system.

Bibliography

[1] Didier Samfat, Refik Molva and N. Asokan, "Untraceability in mobile networks," *International Conference on Mobile Computing and Networking.*, pp. 26-36, 1995.

[2] Kuo-Feng Hwang and Chin-Chen Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Transactions.*, vol. 2 pp. 400-407, Mar 2003.

[3] N. Asokan, "Anonymity in a mobile computing environment," *Mobile Computing System and Applications.*, pp. 200-204, Dec 1994.

[4] Celal Ozturk, Yanyong Zhang, Wade Trappe and Max Ott, "Source-location privacy for networks of energy-constrained sensors," *Software Technologies for Future Embedded and Ubiquitous Systems, 2004. Proceedings. Second IEEE Workshop on.*, pp. 68-72, May 2004.

[5] A. Karygiannis, Aggelos Kiayias and Yiannis Tsiounis, "A solution for wireless privacy and payments based on e-cash," *Security and Privacy for Emerging Areas in Communications Networks, 2005.*, pp. 206-218, Sept. 2005.

[6] C.I. Fan, "Improved low-computation partially blind signatures," *Applied Mathematics and Computation.*, vol. 145 pp. 853-867, 25 Dec 2003.

[7] Q. He, D. Wu, and P. Khosla, "The quest for personal control over mobile location privacy," *Communications Magazine, IEEE*, pp. 130-136, May 2004.

[8] Sang Yun Park, Moon Seoq Han, and Young Ik Eom, "An Efficient Authentication Protocol Supporting Privacy in Mobile Computing Environments," *High Speed Networks and Multimedia Communications 5th IEEE International*, pp. 332-334, July 2002.

[9] Jianming Zhu and Jianfeng Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, pp. 231-235, Feb 2004.

[10] D. Kesdogan and X. Fouletier, "Secure location information management in cellular radio systems," *Wireless Communication System Symposium, IEEE*, pp. 35-40, Nov 1995.

[11] Whe Dar Lin and Jinn-Ke Jan, ".A Wireless-based Authentication and Anonymous Channels for Large Scale Area," *Computers and Communictions, 2001. proceedings. Sixth IEEE Symposium*, pp. 36-41, July 2001.

[12] Bruce Schneier, "Applied Cryptography Second Edition: protocols, algorithms, and source code in C," *Professional, Reference and Trade Group*, 1996.

[13] Robert Tracz and Konrad Wrona, "Fair Electronic Cash Withdrawal and Change Return for Wireless Networks," *International Workshop on Mobile Commerce*, pp. 14-19, 2001.

[14] Markus Jakobsson and Moti Yung, "Revokable and Versatile Electronic Money," *Conference on Computer and Communications Security*, pp. 76-87, 1996.