ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 5, March 2017

National Conference on Advanced Computing, Communication and Electrical Systems - (NCACCES'17)

24th - 25th March 2017

Organized by

C. H. Mohammed Koya
KMEA Engineering College, Kerala- 683561, India

Review of Authentication in Roaming Service

Jasna K Y[1], Raseya K Y[2,] Shijinaz K B[3] ,Suhana Yunes[4]

U.G. Student, Department of Computer Engineering, KMEA Engineering College, Edathala, Kerala, India[1]

U.G. Student, Department of Computer Engineering, KMEA Engineering College, Edathala, Kerala, India[2]

U.G. Student, Department of Computer Engineering, KMEA Engineering College, Edathala, Kerala, India[3]

U.G. Student, Department of Computer Engineering, KMEA Engineering College, Edathala, Kerala, India[4]

ABSTRACT: In mobile communications, roaming means a device going from its home location to different location where it will connect to a foreign network for services. Secure authentication in roaming services is being designed to allow legal users to get access to wireless network services when they are away from their home location. Recently, to protect the location privacy of the user s there have been researches on anonymous authentication .In particular, anonymous authentication without the participation of home server has attracted considerable interest owing to its influence on the communication efficiency. This paper proposes a novel three-round anonymous roaming protocol that does not require the participation of home servers. These protocols propose an anonymous authentication protocol that supports time-bound credentials for an efficient revocation. No expired key can be used to authenticate, and hence naturally revoked users are not required to be put into the revocation list .This makes our protocol much faster than previous roaming protocols in terms of revocation checking, which is a main part in verification.

KEYWORDS: Roaming, Authentication, Group signature, Revocation.

I. INTRODUCTION

In wireless telecommunications, roaming is a general term referring to the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using a visited network. roaming is technically supported by mobility management, authentication and authorization. Now a days mobile computing is getting much priority since the number of portable computers is increasing and also due to the desire to have continuous network connectivity to the internet irrespective of the physical location of the node. Through roaming services mobile device users can use their network services while they are in foreign area. Roaming services should be secure, i.e., provide authentication to identify legal roaming user's[2]. To achieve secure authentication and location privacy simultaneously anonymous authentication methods are used. There are two types of anonymous authentication: weak user anonymity authentication and strong user anonymity authentication. The weak user anonymous authentication hides the user's identity only from third parties, whereas the strong user anonymous authentication hides the users identity even from foreign servers. The basic roaming services involves a home server, a foreign server, and a roaming user. For secure roaming services, the foreign server must authenticate the roaming user, who originally subscribe to the home server. Hence, and authentication mechanism is an important requirement for providing secure roaming services.

User revocation is of great importance to roaming protocols. If the subscription period of a user has expired, the foreign server needs to find out whether a roaming user is revoked. Any revoked user should not be allowed to enter the foreign network. It is quite difficult to achieve efficient user revocation because of the difficulty in taking back the electronic credential. There are two main steps in the verification phase of authentication: validity check and revocation check. Validity check is performed to find whether the authentication token is from a valid user and revocation check checks whether the user has been revoked. Revocation can either be natural or premature. Natural user revocation occurs when the user's access rights has expired. Premature revocation can occur before the expiry time due to the compromise of the credential[2]. D He.et al. [3] proposed a privacy-preserving universal authentication protcocol,

called priauth, which provides strong user anonymity against both eavesdroppers and foreign servers, session key establishment, and achieves efficiency. Hyojinjo et al. [1] proposed a privacy preserving anonymous authentication for mobile networks where user authentication is done without involving a home server. Pseudo identity-based signcryption scheme is used by the protocol to perform efficient revocation with a short revocation list and efficient authentication. Chen et al. [4] proposed a VLR group signatures with indisputable exculability and efficient revocation. Security of scheme is based on the strong Diffie-Hellman assumption and the decisional diffie-hellman assumption in the random oracle model. Similar to many existing anonymous authentication primitives(e.g., [5], [6], [7], [8], [9], [10], [11], [12]) which support revocation , either all unrevoked users need to update their credentials regularly, or the server needs to perform extra steps in verification to check each member against a revocation list. As time goes by, the list will just become larger since the authentication is anonymous. All kind of users to be revoked, including those who were authorized for a limited time period, will be added to the revocation list.

II. RELATED WORKS

The main issue in group signature is revoking a group member's signing capability to solve this this issue, the message can send by only the group manager and he can also have the capability to revoke message only to signature known as group signature with protocol verifier-local revocation. In existing VLR design, the cost of revocation check grows rapidly in accordance with the size of revocation message. Here analyses only the authentication and key agreement protocol that adopted by universal mobile system, an emerging standard for third generation (3G) wireless communications. The protocol, known as 3Gpp aka, is based on the security in GSM and provides significant enhancement to address and correct real and weakness in GSM and other wireless communication systems. In this paper, we first show that the 3Gpp aka protocol is vulnerable to a variant of the so called false base station attack. The protocol retains the framework of the GSM aka and provides significant enhancement to achieve additional goal such as mutual authentication, key exchanging between the user and the serving network, and freshness assurance of agreed cipher key and integrity key. The revocation checking construction done in large scaled networks. Here public key infrastructure in order to support global roaming networks. There are also concerns on the processing power of mobile station and the bandwidth consumption in exchanging public keys of large scale size. Dynamic k-times anonymous authentication schemes allow member of a group to be authenticated schemes allow member of a group to be authenticated anonymously. Application providers can independently and dynamically allow or revoke access right to members in their own group. We also describe some trade –off issues between different system characteristics. Anonymous authentication allows users communicate without reveal their identity. Here also uses the strong diffie hell man assumption. Its main advantage is to maintain constant size in both private and public key. Vehicular ad-hoc networks (vanets) allow wireless communications vehicles and roadside infrastructures. This scheme resolves the issues of non-repudiation and distinguish ability of origin which were previously unresolved in the scheme, thereby enabling a reliable and auditable to service while preserving user privacy against both authorized parties and adversaries. One important criterion in assessing to schemes is performance. In cryptography only verifiers are involved in the revocation mechanism; here signers have no involvement. Although boneh and shacham recently proposed a VLR group signature scheme from bilinear maps, this scheme does not satisfy the backward unlinkability. It means that even after a member is revoked they produced by the member before the revocation remains anonymous. A group manager controls the membership of members. Then, often the anonymity of signature a third party can cancel by tracing. If we compare the protocols we get better efficiency and supports user anonymity to an extent comparable to that provided by current mobile.

III. AUTHENTICATION IN ROAMING

A. SECURITY

In the security analysis, we require an anonymous roaming protocol which satisfy the following properties[4][6]:

1. Subscription Validation: the foreign server should know the identity of the home server of the user;
2. User Anonymity: besides the user and the home server,no one including the foreign server can tell the identityof the user
3. User Untracability: besides the user and the HS, no one including the FS is able toidentify any previous protocol runs which have the sameuser involved.
4. Provision of User Revocation Mechanism [4], [5]:due to various reasons (e.g., the subscription period of a user has expired), the FS should be able to find out whether a roaming user is revoked;
5. Server Authentication: the user should know about the identity of the foreign server;
6. Key Establishment: the user and the FS determines a random session key which is known only toFS and user and is derived from contributions of both of them such that the home server cannot predict the value of it.

B. REQUIREMENT ANALYSIS

In this protocol, we require a group signature scheme as a primitive for both anonymous authentication of user and premature revocation. Group signature allows a member of a group to sign messages on behalf of the group without reveal his/her identity. There is a concept of group manager who has some trapdoor information which allows him to recover the identity of the signer from any valid group signature. A normal group signature cannot achieve our goal since the signature itself does not bear with any time-related information. Traditional revocation approach is inefficient since it either checks every entry in the revocation list or requires the manager to open all signatures.

We are going to design a group signature schema which consists of a tuple of probabilistic polynomial-time algorithms (Gp.Kg, Gp.Join, Gp.Sign,Gp.Ver, Gp.Trace). During Gp.Kg, the group manager producea master public key gpk and a master secret key msk.gpk is published while msk is kept secret. During Gp.Join,the group manager uses msk to generate a user secret key gski for user Ui and a revocation token grti which is used to trace user Ui. During Gp.Sign, a user Ui uses his secret key gski to generate a signature σ for a message m at time t. Gp.Ver takes mpk, t,m, σ and returns valid or invalid. Gp.Trace takes mpk, grti and a valid message-signature pair (m, σ) and returns true or false. Each server chooses a symmetric encryption scheme,

$$ENC = (Enc, Dec) \quad (1)$$

The phases of group signature schmea includes:

a. Master Key Generation Phase

The system structure is similar to the group signature scheme from Bringer and Patey construction.

1. Group manager chooses bilinear groups G1,G2 of prime order p
2. H is the hash function with range Zp
3. Group manager randomely chooses some values which belongs to G1,G2 and Zp
4. Generate public key and master key for group
5. Group manager publishes public key and keeps master key secret
6. He also maintains a revocation list which initially empty

b. User Joining Phase

User can send a request to join the group by selecting the group from the created group. User can randomly chooses some secret values and generate the encrypted values with the foreign server key. It is used to proves the knowledge of the foreign server to the manager. As a result of this user can get the secret key after approving the user by the group manager.

1. User randomly chooses a random value
2. User computes some values and send it to the group manager
3. Group manager checks the values
4. Group manager also computes some values with the user expiry time and sends it to user
5. User gets the secret key and the group manager keeps the revocation token

c. Signing Phase

User can send message as another request to use the roaming system. This action is only possible if and only if the user can approved by the group manager. There are many computations and operations in this phase. Finally user outputs the signature for message m and time.

1. User can send message as another request to use the roaming system.
2. This action is only possible if and only if the user can approved by the group manager.
3. There are many computations and operations in this phase.
4. Finally user outputs the signature for message m and time.

d.Verification Phase

The two servers HS and FS are responsible for performing the verification phase. There are two operations:

Validity check and verification check. These two steps used together to find whether a user is revoked or not.

Upon receiving the signature for specific message and the signing time, the verifier verifies the validity of the signature and ensures that it is not generated by a revoked user.It includes two checks: Validity check and Verification check

Validity Check

1. Recomputes the values as signing phase

2. Check values are equal or not

3. If it is not equal, output is invalid

4. Otherwise continue for revocation check

Verification Check

1. Check for grt

2. If validity check is passed and the user is not revoked, output is valid

3. Otherwise output is invalid

e. Tracing Phase

1. The group manager can open the signature to trace the signer.

2. Group manager only has the permission to trace the user.

3. He can get the full details of the users who are revoked.

4. For each GRT the group manager performs some operations and get the personal details of the user.

The major notations that used in our description are summarized in this table.

TABLE 1 NOTATIONS

$\mathcal{U}_i$	User i
$\mathcal{V}$	Foreign server
$\mathcal{H}$	Home server
gpk	Public parameter of the group signature scheme
msk	Master secret key
gsk_i	User secret key of user $\mathcal{U}_i$, kept by the user
grt_i	Revocation token of user $\mathcal{U}_i$, kept by the group manager
σ	Signature generated by the user
RL	Revocation list
ID	temporary identity chosen by the user
$\mathcal{SIG}$	Signature scheme chosen by each server
$\mathcal{ENC}$	Symmetric encryption scheme chosen by each server

C. AUTHENTICATION AND REVOCATION

Data confidentiality and authenticity are usually needed to protect communications between users and the FS. However, a full personal authentication may not be desirable especially when privacy is a concern. In the roaming

scenario, it is desirable to keep mobile phone users anonymous from other persons as well as the FS unless the identity information becomes critical. It is often sufficient to verify whether a user is among a group of subscribers.

Revocation is the major part of the roaming protocol. Due to some reasons (e.g., the subscription period of a user has expired), the FS needs to find out whether a roaming user is revoked. Any revoked user should not beallowed to enter the foreign network.All kind of users to be revoked, including those who were authorized for a limited time period, will be added to the revocation list Eventually, it will include many such short-term members after their membership expiration. This will cause a serious bottleneck, as the foreign server has to check the whole revocation list for everysingle authentication process, which often involves a cryptographic mechanism to ensure the privacy of (at least other honest) users. For revocation of existing anonymous authentication protocols, we observe that the designs involve a Boolean function(for revocation checking) RCheck() within the verification algorithm which takes an authentication

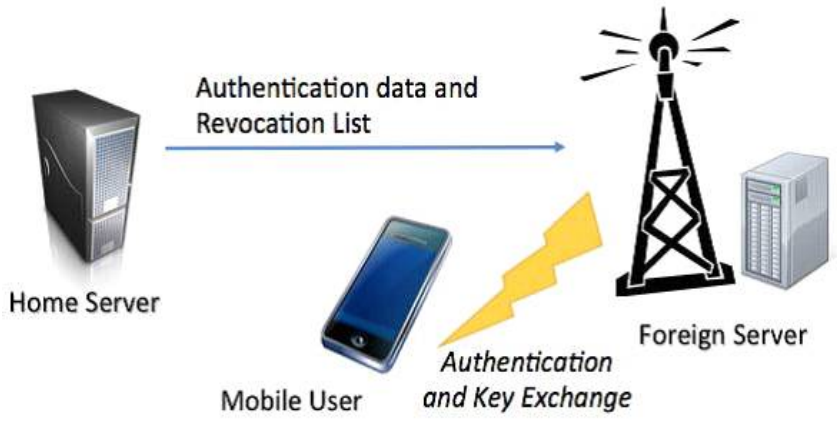

Fig. 1.Authentication in Roaming Networks.

token σ and a revocation list RL = {R1, R2, · · · , RN } as the input, where Ri is an element representing the revoked user i and N is the numberof revoked users.An anonymous authentication token σ is not generated by a revoked user if and only if for every element Ri∈ RL, RCheck(σ, Ri) = negative. In this case,

$$\text{Total Cost of Revocation Check} = C \times N \qquad (2)$$

where C is the computation cost of RCheck() which is a design-specific constant. Equation suggests two approaches to speed up the revocation check:a smaller C, i.e., more efficient designs or a smaller N, i.e., less revoked users.

User authentication is an security mechanism that allows mobile users access to roaming service. Anonymous authentication methods are used to achieve secure authentication and location privacy simultaneously. There are two types of anonymity authentication are: Weak user anonymity authentication: which hides user identity from third party and Strong user anonymity authentication which hides user identity even from foreign server.

D. ANONYMOUS ROAMING AUTHENTICATION PROTOCOL

a. HS Setup

1. Generate bilinear map groups (G1, G2, GT) witha prime order p and choose the generators Q ∈G2, P = ψ(Q) ∈ G1, and g = e(P, Q) ∈ GT (e: bilinearmap, G1 × G2 → GT, ψ: isomorphism G2 → G1).

2. Choose cryptographic hash functions H1:{0, 1}∗ →Z∗p, H2:{0, 1}∗×GT → Z∗p, H3:GT → {0, 1}n, H4:GT →{0, 1}n+w, H5:{0, 1}∗ → {0, 1}n, and H5,key:{0, 1}∗ ×key → {0, 1}n (w is a parameter representing the fixed input ofan encryption algorithm).

3. Choose a master secret key s← Z∗p and computea public key Qpub = sQ∈ G2 and a roaming key

RKHS = 1H1(IDHS)+sQ∈ G2. (RKHS is the HS's secretvalue.)The public parameters are Param: ={G1,G2, GT,e, P, Q, Qpub, ψ, H1, H2, H3, H4, H5, H5,key}.

b. Roaming Agreement

When the HS completes its setup process, it establishes a roaming agreement to generate the roaming keys of

each FS.

1. All FSs send their identity IDFS*i*to the HS.

2. The HS computes a roaming key RKFS*i*=1*H*1*(*IDFS*i)*+*sQ*∈G2 for FS*i*.

3. The HS sends *RK*FS*i*toFS*i*through a securechannel.

c. Registration of RU

RU*i*performs the following process to register in the HS:

1. RU*i*in the HS domain sends its own Id*i*to the HS via a secure channel.

2. The HS generates a random value Seed*i*and a revocation value *rvi*that is used as a key of *H*5,key, and produces keyed hash chain values. The length of the chain is KRevInfo*i,j*= *Hj*5,*rvi(*Seed*i)(*1 ≤ *j* ≤ K*)*.

3. The HS picks random values *xi,j*∈Z∗*p*andcomputes*ri,j*= *gxi,j*. Subsequently, it encrypts Id*i*andcomputes *Tij*using these values.*Eri,j (*ID*i)* = ID*i*⊕*H*3*(ri,j)*(1 ≤ *j* ≤ K)*Ti,j*= *xi,j(H*1(IDHS)*P* + *ψ(Qpub))*(1 ≤ *j* ≤ K*)*

4. The HS generates K pseudo-identities.PID*i,j*=TI*j*||*Eri,j (*ID*i)*||*Ti,j*||RevInfo*i,j(*1 ≤ *j* ≤ K*)*

5. The HS computes private keys for RU*i*, that are associated with the pseudo-identities. $s_{i,j} = 1H1(PID_{i,j}) + sQ \in G2 (1 \leq j \leq K)$

6. The HS sends PID∗*I* and *s*∗*i*generated in 4) and 5) toRU*i*via a secure channel.

IV. CONCLUSION

An anonymous authentication roaming protocol that supports efficient revocation of naturally expired credentials is proposed.it relies on the group signature scheme which can bind the expiry time to the secret key of every user. The modified signature scheme can provide efficient revocation checking. When compared the two running time and revocation checking time the most efficient checking is obtained from the modified encryption. With this new feature expired keys are no longer needed to be included in the revocation list. this results in a significant efficiency improvement for revocation checking due to the elimination of the expired keys in the revocation list.T his makes our construction more practical in the roaming network environment.

REFERENCES

[1]. Hyo JinJo,Jung Ha Paik, Dong HoonLee,-Efficient Privacy-Preserving Authentication in Wireless Mobile Network, IEEE Trans.MobileCoputing ,vol.13,no.7,July 2014
[2]. Joeph K. Liu, Cheng-Kang Chu, Sherman S. M. Chow, Xinyi Huang, Man Ho AU, Jianying Zhou –Time-Bound Anonymous Authentication for Roaming Network, IEEE Trans. Information Forensics and Security,Vol.10,no.1,January 2015
[3]. D. He,J. Bu, S. Chan , C. Chen, and M.Yin, -Privacy –Preserving Universal authentication protocol for wireless communication ,‖ IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 431–436, Feb. 2011.
[4] D. He, J. Bu, S. Chan, C. Chen , and M. Yin,‖Privacy-Preserving universal authentication protocol for wireless communication,‖ IEEE Trans. Wireless Commu, Vol.10, no.2,pp.431-436,feb.2011.
[5] C-K. Chu, J.K.Liu,X. Huang, and J.Zhou, ―Verifier- local revocation group signature wuth time bound keys,‖in Proc. 7th ACM SympInfCopmutCommun. Secur, 2012, pp.26-27.
[6] G. Yang, Q. Huang, D. S. Wong, and X. Deng, ―Universal authentication protocols for anonymous wireless communications,‖ IEEE Trans. Wireless Commun., vol. 9, no. 1, pp. 168–174,Jan. 2010.
[7]. L. Chen, S.-L. Ng, and G. Wang, ―Threshold anonymous announcement in VANETs,‖ IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 605–615, Mar. 2011.
[8]. S. S. M. Chow, W. Susilo, and T. H. Yuen, ―Escrowed linkability of ring signatures and its applications,‖ in Progress in Cryptology (Lecture Notes in Computer Science), vol. 4341. Berlin, Germany: Springer-Verlag, 2006, pp. 175–192.
[9]. B. Libert and D. Vergnaud, ―Group signatures with verifier-local revocation and backward unlinkability in the standard model,‖ in Cryptology and Network Security (Lecture Notes in Computer Science), vol. 5888. Berlin, Germany: Springer-Verlag, 2009, pp. 498–517.
[10]. D. Johnson, A. Menezes, and S. Vanstone, ―The elliptic curve digital signature algorithm (ECDSA),‖ Int. J. Inform. Security, vol. 1,no. 1, pp. 36–63, 2001.
[11]. T. Nakanishi and N. Funabiki, ―Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps,‖ in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3788. Berlin, Germany: Springer-Verlag,2005