Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient Anonymity Authentication and a Fast Revocation Process in WMN

Sindhuja A, Sasidevi J, Aarthy R
Computer Science & Dhanlakshmi Srinivasan Engineering College
Tamil Nadu, India

Abstract— In secure roaming service, the foreign server must authenticate the roaming user, who originally subscribed to the home server. Hence, an authentication mechanism is currently important requirement for providing secure roaming services and protects the location privacy of users on unidentified authentication. The unidentified authentication will process without participating the home server on efficiency communication for existing work. The process of authentication increases high computation costs and huge revocation lists. The novel three-round anonymous (unidentified) roaming protocol uses a pseudo-identity-based signcryption scheme and using CK-model to perform efficient revocation with a short revocation list and efficient authentication. The use of a signcryption algorithm minimizes the storage in a Subscriber Identification Module (SIM) card with limited storage capacity. The authentication efficiency is also higher than that of existing protocols.

Keywords— Quorum Sensing Protocol, Signcryption, Efficient Anonymity.

I. INTRODUCTION

Mobile computing is human computer by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications.

Several categories of portable computing devices can run on batteries but are not usually classified as laptops: portable computers, PDAs, ultra mobile PCs (UMPCs), tablets and smart phones. A portable computer (discontinued) is a general-purpose computer that can be easily moved from place to place, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source. Portable computers are also called a "transportable" or a "luggable" PC.A personal digital (PDA) (discontinued) is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and to synchronize with a desktop computer, giving access to contacts, address book, notes, e-mail and other features.

A tablet computer that lacks a keyboard (also known as a non-convertible tablet) is shaped like a slate or a paper notebook. Instead a physical keyboard it has a touch screen with some combination of virtual keyboard, stylus and/or hand writing recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most of the tasks of an ordinary laptop. A smart phone has a wide range of features and install-able applications. A carpeted is installed in an automobile. It operates as a wireless computer, sound system, GPS, and DVD player. It also contains word processing software and is Bluetooth compatible. A Pen top (discontinued) is a computing device the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device, and calculator

Boundaries that separate these categories are blurry at times. For example, the OQO UMPC is also a PDA-sized tablet PC; the Applegate had the clamshell form factor of a laptop, but ran PDA software. The book line of laptops included some devices small more enough to be called ultra mobile PCs. The hardware of the Nokia770 internet tablet is essentially the same as that of a PDA such as the Azures , both the 770 and the Azures can run some desktop Linux software, usually with modifications.

Wireless data connections used in mobile computing take three general forms so. Cellular data service uses technologies such as GSM, CDMA or GPRS, 3G networks such as EDGE or CDMA2000. And more recently 4G networks such as LTE, LTE-Advanced. These networks are usually available within range of commercial towers. Wi-Fi connections offer higher performance, may be either on a private business network or accessed through public hotspots, and have a typical range of 100 feet indoors and up to 1000 feet outdoors.

II. RELATED WORK

Roaming services should be secure, i.e., provide authentication to identify legal roaming users. As well as security, location privacy should be provided to protect trajectories of roaming users. In particular, various anonymous authentication methods have been proposed to achieve secure authentication and location privacy simultaneously.

According to, anonymous authentication could be classified into two types: weak user anonymity authentication and strong user anonymity authentication. Roaming protocols could be divided into two types: three-party protocols involving a home server and two party protocols that do not involve a home server. In recent years, various three-party protocols have been proposed for anonymous authentication.

The past days various types of algorithm proposed in secure roaming Services. Anonymous authentication only secure provides the user hide the information only third party, which means neighbor nodes. The later days developed in foreign domains. Next past days used Tree-party protocols involving a home server. The protocols for four round communication. Occur bottleneck & single point failure and then this system for open communication. Pseudo-identity based roaming protocols not protect both private key and session key. Light-weight three party protocols also involve home server. This protocol Used also occur the security problems. Compare with some protocols drawback clear in two-party protocols. But the existing two-party protocols based on group signature with backward unlinkability. So each roaming user with N secret keys. So increase the revocation cost & revocation list.

In the proposed authentication protocol, two parties, a roaming user and a foreign server, perform an initial exchange, bootstrapping from the initial trusted information that they possess about each other. The proposed system uses efficient two-party protocol. Then the user have to propose the novel three-round anonymous roaming protocol that does not require the participation of home server. The proposed protocol uses pseudo-identity-based signcryption scheme to perform efficient revocation with a short revocation list and efficient authentication. Novel three-round anonymous protocol based on the Canetti-Krawczyk (CK) model. The model widely used as an analyzing key agreement protocols. Compare with existing the proposed protocol backward unlink ability of user's past pseudo-identities are not linked. Signcryption based revocation process require only a few hash operations. The user use a keyed hash chain to revoke malicious users. In this protocol the user minimize the number of pseudo-identities to be stored on the SIM card by using signcryption.

A. Canetti-Krawczyk (CK) model

In the proposed authentication protocol, two parties roaming user and a foreign server, perform an initial exchange, bootstrapping from the initial trusted information that they possess about each other. This protocol is formally proved in the CK model, which is widely used as a formal method for analyzing key agreement protocols.

B. Revocation cost

The revocation process requires only a few hash operations. The user use a keyed hash chain to revoke malicious users.

C. Authentication cost

The authentication cost for roaming services can be divided into two parts: cost at the roaming user and cost at the roaming server. Taking the roaming authentication cost of a foreign server into account, our protocol, which supports a fast revocation process, is more cost efficient.

D. Three-Round anonymous Roaming Protocol

HS first performs the initial process phase which is composed of an HS setup step, a roaming agreement step and a registration of RU step for preparation of roaming service. In the HS setup step, HS generates its own public parameters and secret values. Upon completing the HS setup step, the roaming agreement step and the registration of RU step are conducted to issue secret values of FSs and RUs. The anonymous roaming system phase consists of a roaming protocol step and a revocation step. In the meantime, the revocation step supports the roaming protocol step to exclude malicious RUs from the proposed roaming system.

III. SYSTEM DESIGN

The roaming service allows mobile device users to use network services even when they reside in foreign domains. For secure roaming service, the foreign server must authenticate the roaming user, who originally subscribed to the home server. Roaming services should be secure, i.e., provide authentication and identify legal roaming users. As well as security, location privacy should be provided to protect trajectories of roaming users. Existing system using various types of algorithm for secure roaming Services. Anonymous authentication only secure provides the user hide the information only third party, which means neighbor nodes. The later days developed in foreign domains. Next past days used Tree-party protocols involving a home server. The protocols are having four round communication. Existing method are using different algorithms but doesn't avoid occurring bottleneck & single point failure and then this system for open communication. Pseudo-identity based roaming protocols not protect both private key and session key.

Light-weight three party protocols also involve home server. This protocol Used also occur the security problems. Compare with some protocols drawback clear in two-party protocols. But the existing two-party protocols based on group signature with backward unlinkability. So each roaming user with N secret keys. So increase the revocation cost & revocation list. Existing methods are don't provide security Authentication and location privacy for the mobile user, High communication cost and large size of Revocation list has been maintained and Roaming charges also has been very high cost. In the proposed authentication protocol, two parties, a roaming user and a foreign server, perform an initial exchange, bootstrapping from the initial trusted information that they possess about each other. The proposed system uses an efficient two-party protocol used.

The proposed protocol uses pseudo-identity-based signcryption scheme to perform efficient revocation with a short revocation list and efficient authentication. Novel three-round anonymous protocol based on the Canetti-Krawczyk (CK) model. The model widely used as an analyzing key agreement protocols. Compare with existing protocol, the proposed protocol has backward unlinkability of user. Signcryption based revocation process require only a few hash operations. This is used to minimize the number of pseudo-identities to be stored on the SIM card by using signcryption. The proposed methods are having two techniques those are Update Revocation List and Revocation check

If RUiis revoked by the HS, all FSs have to quit the roaming service of RU*i*. Thus, the HS periodically sends a revocation list to all FSs to check whether RU*i* has been revoked. In the revocation process, two algorithms are used. Update Revocation List is used to updates the revocation list by using a new revocation list sent by the HS. The revocation list containing the revocation information followed revocation information of roaming user and revocation value of user. The information sends all foreign servers. After receiving revocation list of home server, all foreign servers update. Revocation check performs the revocation checking process when RU*i sends* requests for roaming services to FSs. The FS checks user the revocation list to determine whether the signature of roaming user pseudo-identities is a revoked state.

A. Home Server Setup Phase

The home server setup phase is the initial process.It is the cryptographic hash function used to find the key, a keyed hash chain is used to revoke malicious users. Next compute the secret key of Home server. The roaming key of home server is the Home Server secret value.

B. Roaming Agreement Phase

The Home Server after completes its setup process, it establishes a roaming agreement to generate the roaming keys of each foreign server. All foreign servers send their identity as request to the home server for secret agreement. Then home server computes a roaming key for foreign server. And the next process is that home server sends roaming key to all requested foreign server through a secure channel.

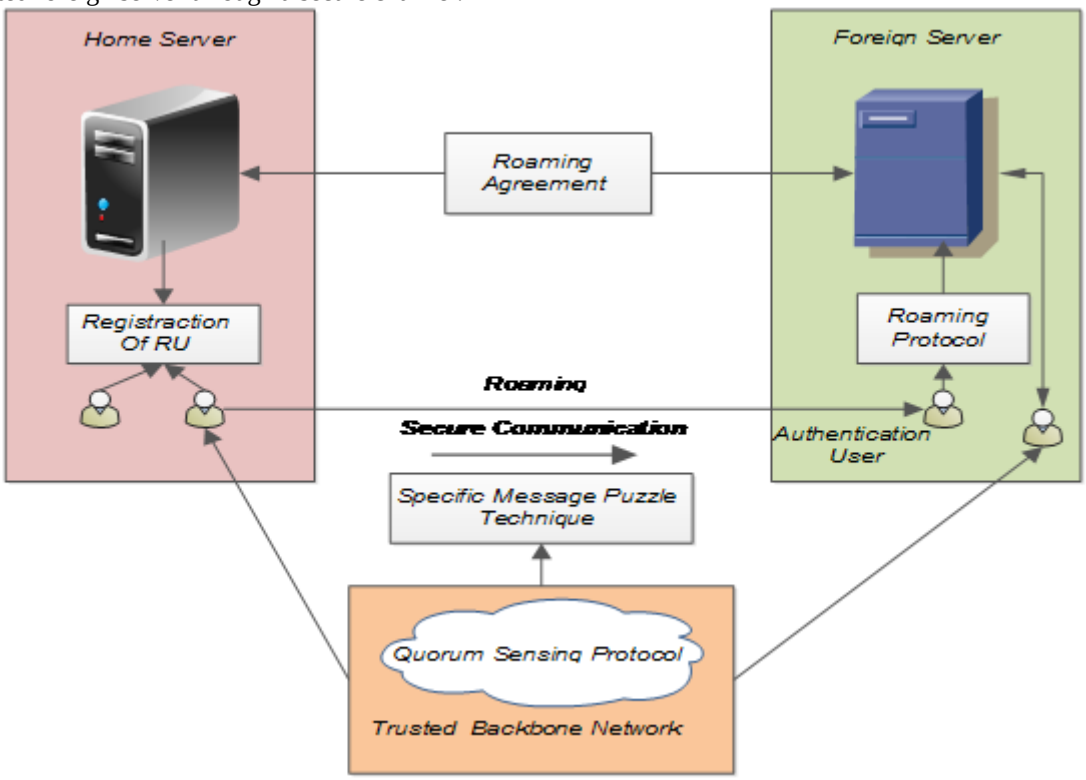

Fig 1 Architecture Diagram

C. Registration Of Roaming User In Home Server Phase

Roaming user going to register their details such as own identity in the home server using secure channel. Home server get the roaming user identity compute the roaming user pseudo-identities and roaming user secret value and then sending it to roaming user. Then secret value is saved as roaming user's private key.

D. Anonymous Roaming System

Roaming user send request containing identity of HS and newly generated Random values and so on by signcrypt. Then foreign server accepting the request by unsigncryption. The revocation check process is also carry out. After successful completion, it sends response with identity of FS and Signature .Roaming user finally sends the MAC address for requesting connection then allows them after verification .Hence this proposed scheme known as an anonymous roaming protocol.

IV. CONCLUSION

An anonymous roaming protocol uses signcryption. Existing three-party roaming protocols require the assistance of home servers, while two party. Roaming protocols have weak security features (weak anonymity, insecurity in the CK model, backward linkability and leakage of the session key) or inefficient operations (high authentication and revocation costs). However, unlike these protocols, our protocol does not need the support of the home server, and includes an efficient anonymity authentication process and a fast revocation process. Furthermore, our protocol is secure in the CK model and it provides roaming users with strong user anonymity and backward unlinkability. We evaluated the efficiency of our protocol by comparing it with existing protocols and by implementing a prototype of our protocol. If any anonymous third party (Unauthenticated user) disturbs the Home server and foreign server communication, there is a chance to make delay in communication. So it may severely affect the Roaming users to connect. To enhance the model by using Trusted Third party sensing node. The main responsibility of this node are monitoring the servers operation and controlling the time delay in presence of interference. Specifically this third party uses a Quorum Sensing Protocol to efficiently carry out above process.

REFERENCES

[1] C. Y. Chow, M. F. Mokbel, and T. He(2011), "A privacy-preserving loca- tion monitoring system for wireless sensor networks," IEEE Trans. Mobile Comput., vol. 10, no. 1, pp. 94–107, Jan.

[2] B. Gedik and L. Liu(2008), "Protecting location privacy with person- alized k-anonymity: Architecture and algorithms," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 1–18, Jan.

[3] D. He, J. Bu, S. Chan, C. Chen, and M. Yin(2011), "Privacy-preserving universal authentication protocol for wireless communications," IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 431–436, Feb.

[4] Hyo Jin sssJo, Jung Ha Paik, and Dong Hoon Lee(2014), Fellow, IEEE "Efficient Privacy-Preserving Authentication in Wireless Mobile Networks", VOL. 13, NO. 7, JULY.

[5] K. Mehta, D. Liu, and M. Wright(2011), "Protecting location privacy in sensor networks against a global eavesdropper," IEEE Trans. Mobile Comput., vol. 11, no. 2, pp. 320–336, Feb.

[6] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi(2012), "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," Math. Comput. Model., vol. 55, no. 1–2, pp. 214–222.

[7] A. Shen, S. Guo, D. Zeng, and G. Mohsen(2012), "A lightweight privacy- preserving protocol using chameleon hashing for secure vehicular communications," in Proc. IEEE WCNC, Shanghai, China, 2012, pp. 2543–2548.

[8] Security Aspects(1993), ETSI GSM 02.09.

[9] Y. Sun, T. La Porta, and P. Kermani(2009), "A flexible privacy enhanced location-based services system framework and practice," IEEE Trans. Mobile Comput., vol. 8, no. 3, pp. 304–321, Mar.

[10] 3rd Generation Partnership Project(2003); Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP Network Layer Security, 3GPP TS 33.210 V5.5.0.

[11] G. Yang, D. S. Wong, and X. Deng(2007), "Anonymous and authenti- cated key exchange for roaming networks," IEEE Trans. Wireless Commun., vol. 6, no. 9, pp. 3461–3472, Sept.

[12] G. Yang, D. S. Wong, and X. Deng(2008), "Formal security definition and efficient construction for roaming with a privacy-preserving extension," J. Universal Comput. Sci., vol. 14, no. 3, pp. 441–462.

[13] H. Zhu, X. Lin, M. Shi, P.-H. Ho, and X. Shen(2009), "PPAB: A privacy preserving authentication and billing architecture for metropoli- tan area sharing networks," IEEE Trans. Veh. Technol., vol. 58, no. 5, pp. 2529–2543, Jun.

[14] H. Zhu, W. Pan, B. Liu, and H. Li(2012), "A lightweight anonymous authentication scheme for VANET based on bilinear pairing," in Proc. 4th Int. Conf. INCoS Bucharest, Romania, 2012, pp. 222–228.

[15] D. He, C. Chen, S. Chan, and J. Bu(2012), "Secure and efficient handover authentication based on bilinear pairing functions," IEEE Trans. Wireless Commun., vol. 11, no. 1, pp. 48–53, Jan.

