Ad Hoc Networks 44 (2016) 19–31

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Provably secure anonymous authentication with batch verification for mobile roaming services

Jia-Lun Tsai*, Nai-Wei Lo

Department of Information Management, National Taiwan University of Science and Technology, Taipei 106, Taiwan

ARTICLE INFO

Article history:
Received 16 September 2015
Revised 4 February 2016
Accepted 5 February 2016
Available online 23 February 2016

Keyword:
Anonymous authentication
Mobile roaming service
Formal proof
Batch verification

ABSTRACT

Recently, multiple secure authentication schemes with user anonymity feature for mobile roaming services have been proposed to address general user privacy concern from mobile device users. As mobile devices usually have limited computing resources, it is difficult to develop an anonymous authentication scheme which possesses performance efficiency and security robustness at the same time. In this paper, a new anonymous authentication scheme for mobile roaming services is proposed to support fast authentication and preserve security strength and user privacy. The proposed authentication mechanism adopts identity-based encryption scheme and identity-based batch signature scheme to further reduce the total computation cost during one authentication session in comparison with existing authentication schemes. In addition, our scheme eliminates the requirement of storing a lot of pseudo-identities in user's SIM card and supports batch verification feature at the server side to further enhance authentication efficiency. User revocation mechanism is also developed in the proposed scheme for occasions when it is necessary for a home server to revoke individual users. To evaluate security strength of the proposed scheme, the scheme has conducted security analysis through formal proof under Jakobsson et al.'s security model. In comparison with existing authentication schemes, our scheme provides faster authentication along with lower storage consumption in user's SIM card. Hence, the proposed scheme is a very competitive candidate on secure anonymous authentication for mobile roaming services.

1. Introduction

Since handheld mobile devices have been massively purchased and used by people in modern societies, various wireless mobile services have been developed to support instant information, social networking and convenient online services for people's daily life. Roaming service is a wireless technology for a mobile user to gain access to the Internet when the user does not locate at the signal coverage area of his corresponding mobile operator. In general, there are three roles in a mobile roaming service [1–3]: a home server (HS), multiple foreign servers (FSs), and multiple roaming mobile users (RUs). A mobile user needs to register itself on its home server in advance before connecting to a FS. When a mobile user tries to access wireless services through a FS, the mobile user has to authenticate itself with the FS. Therefore, secure authentication schemes play a very important role for the successful deployment of mobile roaming services.

Authentication schemes [4–10] are basic elements of security protection for wireless mobile networks. A secure authentication scheme for mobile roaming services should prevent illegal access from malicious adversaries through mutual authentication. With raising concern on user privacy, authentication schemes for mobile roaming services also need to consider user privacy protection in terms of transmitted messages during authenticating process [11–14]. Since mobile devices usually have less computing

* Corresponding author. Tel.: +886 3 3685557.
E-mail address: crousekimo@yahoo.com.tw (J.-L. Tsai).

http://dx.doi.org/10.1016/j.adhoc.2016.02.011
1570-8705/© 2016 Elsevier B.V. All rights reserved.

capability and less storage capacity in comparison with personal computers, traditional public key cryptosystems such as public key infrastructure (PKI) requiring storage space for certificates and computing resources for certificate verification have practical difficulties to be implemented on mobile devices. In consequence, it is necessary to develop new design for authentication schemes to preserve the quality of mobile roaming services [15].

Recently, Yang et al. [16] first categorized anonymous authentication schemes into weak user anonymity authentication and strong user anonymity authentication, and then proposed two corresponding anonymous authentication schemes based on those two different types. Their first scheme for weak user anonymity authentication environment utilizes an identity-based signature scheme. Their second scheme for strong user anonymity authentication environment adopts a group signature scheme. In their first scheme, a FS knows the user identity during user authentication. In their second scheme, a FS does not know the user identity during user authentication since only a group signature sent from the user is verified by the receiving FS. Obviously, the strong user anonymity authentication environment provides better security hardness than the other one. However, authentication schemes complying with the strong user anonymity authentication environment may not be able to support personalized services that require user identities to access authorized resources and services.

In general, researches on anonymous roaming authentication schemes are classified into two types: three-party schemes with a home server [17–22] and two-party schemes without using a home server [16,23–27]. In the three-party authentication type, the home server participates in the authentication process when a mobile user connects to a foreign server. At least four rounds of communication are required for existing schemes to authenticate a user, since these schemes usually require two extra rounds of message communication for a foreign server to learn authenticating information from the home server during an authentication session. The home server will take heavy computation load when a lot of mobile users registered in this home server activate their mobile roaming services. In addition, those schemes require a communication connection between a foreign server and a home server. If this connection is interfered and broken by an adversary, corresponding mobile users associated with the foreign server cannot get successful access of their roaming services. In recent years, two-party roaming authentication schemes without the assistance of a home server have been proposed. The concept of a two-party roaming authentication scheme was introduced by Yang et al. [16]. In 2012, He et al. [23] proposed a pseudo-identity-based roaming authentication scheme based on the schemes of Yang et al. [16]. Unfortunately, Tsai et al. [24] found that the authentication scheme of He et al. is vulnerable to a private key reveal attack. In addition, the scheme of He et al. has heavy computation load at the mobile device side. In consequence, the scheme of He et al. is not a very efficient one. Tsai et al. [24] proposed a handover authentication scheme based on identity-based batch signature scheme [28–30]. Since the identity-based batch signature scheme is used in their scheme, a group of login requests can be verified at the same time. In 2015, He et al. [27] proposed an enhanced authentication scheme to overcome security weakness found in [23]. However, this enhanced scheme does not support bath verification and requires substantial amount of storage space in user's SIM card. Consequently, how to minimize the usage of storage space in user's SIM card has become an interesting research topic on roaming authentication schemes.

In 2014, Jo et al. [25] proposed an efficient pseudo-identity two-party roaming authentication scheme supporting anonymity and backward unlinkability. Their approach is different from traditional authentication schemes. Their scheme employs a signcryption scheme to minimize the number of pseudo-identities stored on user's SIM card while authenticating mobile users. Since their scheme does not require any pairing computation on user's mobile device, it has better performance than previously published schemes. However, this study found that there are some shortcomings in the authentication scheme proposed by Jo et al. First of all, RU requires a huge storage capacity to store all corresponding public keys of FSs, since their scheme employs an ECDSA [31] scheme to help users authenticate the FSs. As ECDSA belongs to traditional cryptosystems, the RUs in their scheme need to store all public keys of FSs and their corresponding certificates in advance. Without knowing these public keys of FSs, the RU cannot verify the ECDSA signatures generated by a FS during authentication. Secondly, the user revocation process of their authentication scheme requires only a few hash operations to generate a revocation list and each record of a revocation list contains one hash value and a revocation key of the targeted user. In addition, a FS in their scheme requires downloading and updating its whole revocation list from the HS periodically. Thirdly, their scheme employs signcryption scheme to minimize the number of pseudo-identities stored in user's SIM card. There may exist a better way to achieve the same goal. In addition, their scheme requires a special inefficient hash function, called MapToPoint, and does not support batch verification. It motivates us to propose a new authentication scheme to overcome these weaknesses.

1.1. Contributions

In this paper, we adopt an identity-based ECC signature scheme and an identity-based pairings encryption scheme to develop a new efficient authentication scheme for mobile roaming services. By utilizing the identity-based encryption scheme and the identity-based batch signature scheme, the proposed scheme reduces the total number of pseudo-identities stored in a SIM card and supports batch verification at the server side to enhance authentication efficiency. In addition, the proposed scheme supports user anonymity and user revocation mechanisms. We also give a formal proof to show that the proposed scheme is secure. In comparison with other related works, our scheme requires less computing resource and less storage consumption while providing efficient user revocation feature. As a result, our scheme is a very competitive candidate