Computer Networks 56 (2012) 2994–3006

Contents lists available at SciVerse ScienceDirect

Computer Networks

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

A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants

Tsu-Yang Wu [a], Yuh-Min Tseng [b,*], Tung-Tso Tsai [b]

[a] School of Computer Science and Technology, Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen 518055, PR China
[b] Department of Mathematics, National Changhua University of Education, Jin-De Campus, Chang-Hua City 500, Taiwan, ROC

ARTICLE INFO

Article history:
Received 31 October 2011
Received in revised form 14 March 2012
Accepted 28 May 2012
Available online 5 June 2012

Keywords:
Authenticated group key exchange
Identity-based
Revocation
Malicious participant
Bilinear pairing

ABSTRACT

Authenticated group key exchange (AGKE) protocol provides secure group communications for participants in cooperative and distributed applications over open network environments such as the Internet and wireless networks. In the past, a number of AGKE protocols based on the identity (ID)-based public key system (IDPKS) have been proposed, called ID-AGKE protocols. In the IDPKS system, users' identities are viewed as the public keys to eliminate certificate management of the traditional certificate-based public key system. Nevertheless, any certificate-based public key systems or IDPKS systems must provide a revocation mechanism to revoke misbehaving/compromised users from the public key systems. However, there was little work on studying the revocation problem of the IDPKS system. Quite recently, Tseng and Tsai presented a new ID-based encryption scheme and its associated revocation mechanism to solve the revocation problem efficiently, called revocable ID-based public key system (R-IDPKS). In this paper, we follow Tseng and Tsai's R-IDPKS system to propose the first revocable ID-AGKE (RID-AGKE) protocol. Security analysis is made to demonstrate that the proposed RID-AGKE protocol is a provably secure AGKE protocol and can resist malicious participants. As compared to the recently proposed ID-AGKE protocols, the proposed RID-AGKE protocol is provably secure and has better performance while providing an efficient revocation mechanism.

1. Introduction

Due to many group-oriented applications such as teleconference and collaborative work are popularly and widely used in the recent years, secure group communication technique has become an important research issue for protecting communication security between participants. Authenticated group key establishment protocol is an important security mechanism which provides secure group communications and mutual authentication for participants in cooperative and distributed applications over open network environments such as the Internet and wireless networks. There are two categories for authenticated group key establishment: authenticated group key distribution and authenticated group key exchange (AGKE). In the authenticated group key distribution protocol, there is a trusted chairman who is responsible to generate a common key and then securely distribute the common key to the other participants. In the AGKE protocol, group participants cooperatively compute a common key. The point is that in the AGKE protocol no participant can predict or predetermine the common key and no trusted chairman is involved in the key construction. In the past, numerous authenticated group key establishment protocols based on the traditional certificate-based or ID (identity)-based public key systems (IDPKS) have been published in the literatures [1–10].

In the traditional certificate-based public key system, certificates are used to make publicly available the mapping between identities and public keys. A public key certificate is a signature produced by a trusted certificate

* Corresponding author. Tel.: +886 4 723 2105; fax: +886 4 721 1192.
E-mail address: ymtseng@cc.ncue.edu.tw (Y.-M. Tseng).

1389-1286/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comnet.2012.05.011

authority (CA) that securely binds together several quantities which usually include the identity of a user, its associated public key, the issuing date and the expiration date. When a public key is used, the associated certificate must be checked to ensure its validity (revoked or non-revoked). In general, Certificate revocation list (CRL) [11] is used to revoke the users' public keys. Users can check these revoked users' public keys by querying the CRL. Actually, efficient revocation is a well-studied problem in the certificate-based public key system, e.g. [12–16].

In 1984, Shamir [17] first proposed the concept of the IDPKS system. In this system, each user's identity (e.g. e-mail address, name, or social security number) can be viewed as the public key and the user's private key is computed by a trusted private key generation center (PKG). Thus, it can eliminate the need of certificates to simplify certificate management of the certificate-based public key system. In 2001, Boneh and Franklin [18] followed Shamir's concept to propose a practical ID-based encryption (IBE) scheme from the Weil pairing. Later on, the design of ID-based cryptographic mechanisms using bilinear pairings has received much attention from researchers and numerous literatures have been presented such as ID-AGKE protocols [4,7,10], IBE schemes [19–21], ID-based signature schemes [22–24], ID-based key agreement protocols [25–27], and ID-based user authentication schemes [28,29].

1.1. Motivation

In spite of IDPKS's advantage with eliminating certificate management, it is a critical issue to revoke misbe having/compromised identities in the IDPKS system. Nevertheless, any IDPKS system or certificate-based public key system must provide a method to revoke misbehaving/compromised users from the public key systems. Several situations require a certificate or an ID to be revoked before its intended expiration date. For example, if an employer leaves a company and is no longer entitled to use the corresponding ID, the employer's ID must be revoked. Straightforward implementation of the CRL mechanism will not be the good solution to the IDPKS system since no certificate is required for such a system. For ID-AGKE protocol, since only the system's public parameters and the users' identities should be involved to participant authentication and the construction of the group common key, it is difficult to notify participants that a specific particular's identity has been revoked. For the revoked participants, they should not be allowed to establish a group key with the other legitimate (non-revoked) participants. However, there has been little work on studying the revocation mechanisms of the IDPKS. Meanwhile, no ID-AGKE protocol deals with the revocation problem.

1.2. Related work

The first ID-AGKE protocol using bilinear pairings was proposed by Choi et al. [4] in 2004. However, their protocol suffered from several attacks. In [30], Zhang and Chen presented an impersonation attack on Choi et al.'s protocol [4]. In 2007, Shim [31] also proved that Choi et al.'s protocol is insecure against an insider (participants) colluding attack in which three malicious participants can collude to impersonate an honest participant to the other participants in the group. Shim also presented an improvement to resist the mentioned insider colluding attack. In 2008, Choi et al. [7] demonstrated that Shim's improvement [31] still suffered from other insider colluding attacks. They then proposed an improvement to withstand the mentioned insider colluding attacks. In 2009, Wu and Tseng [32] proved that Choi et al.'s protocol [7] is also insecure against an insider colluding attack. Recently, Wu et al. [10] proposed a provably secure ID-AGKE protocol with resistant to malicious participants.

For the revocation problem of the IDPKS system, Boneh and Franklin [18] have suggested a solution. In their suggestion, the PKG can periodically generate new private keys for non-revoked users. When the PKG wants to revoke a specific user, it only stops to issue the new private key. However, this method has two disadvantages: (1) the periodical workload of computing new private keys is too heavy for the PKG; (2) secure channels must be established between non-revoked users and the PKG to transmit the new private keys for each time period.

In 2008, Boldyreva et al. [33] proposed a revocable IBE (RIBE) scheme to reduce the PKG's periodical workload required in Boneh and Franklin's IBE [18]. In their RIBE scheme, a binary tree is used to reduce the total size of key updating. However, the security of their scheme is under a weak security model, called the relaxed selective-ID model [34], in which an adversary must choose the target identity to attack before the system parameters are set. In 2009, Libert and Vergnaud [35] presented an adaptive-ID secure RIBE scheme relying on the Boldyreva et al.'s work [33]. Though both protocols [33,35] can provide the revocation functionality, there still exist several drawbacks: (1) each user must hold $3\log n$ private keys; (2) secure channel is still required to transmit new private keys; (3) the PKG must maintain a binary tree of n leaf nodes, where n denotes the total number of all users.

Very recently, Tseng and Tsai [36] proposed an efficient RIBE scheme and its associated revocation mechanism to solve the revocation problem efficiently, called revocable ID-based public key system (R-IDPKS). In the R-IDPKS system, each user's private key consists of a fixed initial secret key and a time update key, where the time update key is changed along with time period. For non-revoked users, the PKG periodically generates new time update keys and sends them to the non-revoked users via a public channel. Upon receiving the new time update keys, the non-revoked users can update own private keys by themselves. Obviously, the PKG can stop issuing the new update time keys to revoke the misbehaving or compromised users because they are unable to update their private keys. For the security and efficiency, the Tseng-Tsai RIBE scheme is semantically secure against adaptive chosen ciphertext attacks and is efficient than the previously proposed protocols [33,35].

1.3. Our contribution

Until now, no related study focuses on the design of revocable ID-AGKE (RID-AGKE) protocol. We will rely on Tseng and Tsai's R-IDPKS system [36] to present the first