Information Sciences 321 (2015) 224–237

Contents lists available at ScienceDirect

Information Sciences

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

# A provable authenticated group key agreement protocol for mobile environment

Hung-Min Sun [a,*], Bing-Zhe He [a], Chien-Ming Chen [b], Tsu-Yang Wu [b], Chia-Hsien Lin [a], Huaxiong Wang [c]

[a] Department of Computer Science, National Tsing Hua University, Taiwan
[b] Innovative Information Industry Research Center, Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China
[c] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

ARTICLE INFO

*Article history:*
Received 31 March 2014
Received in revised form 21 January 2015
Accepted 30 January 2015
Available online 11 February 2015

*Keywords:*
Group key agreement protocol
Semi-trusted third party
Certificateless
Mobile computing

ABSTRACT

Secure group communication over an untrusted open network is a continuing problem, especially in mobile environments. With the development of 3G networks and mobile computing technology, the number of group-oriented applications is increasing rapidly. Although these applications are convenient, achieving secure group communication to protect user privacy is a major concern. This study presents an authenticated group key agreement protocol for mobile environments. By using certificateless public key cryptography, the protocol reduces the cost of managing the certificates and avoids the key escrow problem. Instead of a fully-trusted server, the protocol uses a semi-trusted server, which helps users communicate but does not learn about the group key. The analytical results indicate that the proposed protocol provides good security in mobile environments.



## 1. Introduction

Secure information exchange over an untrusted network is a widely discussed issue in mobile computing. As 3G wireless networks grow in popularity, people can use mobile devices to connect to the Internet from almost anywhere, which has made life easier. The increasing computing power of mobile devices also increases user productivity. Some mobile computing applications enable a user in a coffee bar to hold online meetings and transfer important documents to other users. However, the document must be protected since most public networks are unsafe. One solution is to protect the communication with a group key, which only group members can compute. The group key can prevent attackers from eavesdropping or tampering with messages, even if they are sent over public and untrusted networks.

A major challenge when using a group key agreement protocol is ensuring that each member can securely derive the same group key. If all group members can meet with each other to establish a group key, this problem is easily solved. However, users typically communicate with each other through a third-party server under mobile environment. Additionally, mobile devices usually connect to the Internet through public networks (e.g., public access point). Therefore, group key agreement protocols for mobile environments must ensure that users can agree to a group key through insecure networks and each member obtains the same group key in the end of the protocol.

* Corresponding author.
*E-mail addresses:* hmsun@cs.nthu.edu.tw (H.-M. Sun), ckshjerho@is.cs.nthu.edu.tw (B.-Z. He), chienming.taiwan@gmail.com (C.-M. Chen), wutsuyang@gmail.com (T.-Y. Wu), kyonkun@is.cs.nthu.edu.tw (C.-H. Lin), hxwang@ntu.edu.sg (H. Wang).

http://dx.doi.org/10.1016/j.ins.2015.01.037
0020-0255/

Servers have a key role in mobile environments since direct communication between low-power devices or mobile devices in 3G networks is difficult. When a group key agreement protocol is used in a mobile environment, the main function of the server is to help mobile devices compute, communicate, and, ultimately, establish a group key. In most proposed protocols [7,20,21,25,26], the server learns the group key at the end of a protocol. Therefore, the server can access secret information encrypted by the group key. These protocols all assume that the server is fully trusted and will not use the group key to eavesdrop or tamper with the information. However, these servers are vulnerable to attacks that can result in financial losses. An adversary who successfully compromises the server can obtain the session keys and decrypt all the protected data. One way to increase the security of group keys is to prevent the server from learning the group key in the end of protocol. This discussion refers to these servers as semi-trusted servers.

In the group key agreement protocol, authentication is essential. If a key agreement protocol does not provide authentication, the protocol is vulnerable to the man-in-the-middle (MITM) attack [11]. One solution is using signature algorithms to provide user authentication. If the signature algorithm is based on public key infrastructure (PKI), then a certificate authority (CA) is needed to manage certificates. However, in conventional PKI, the costs of certificate management, including storage, distribution, verification and revocation, are high. Therefore, Shamir [22] proposed ID-based cryptosystems in 1985, in which the identity of the user is used to derive the public key of the user. Although public keys are used as user IDs and are not generated by CA, ID-based cryptosystems still require that private keys are generated by a private key generator (PKG). Another problem in ID-based cryptosystems is the key escrow problem [19]. This study developed a certificateless public key cryptography (CL-PKC) authentication system that avoids the key escrow problem and does not require certificates to authenticate public keys. Therefore, the CL-PKC combines the advantages of PKI and ID-PKC.

This study developed an efficient group key agreement protocol for mobile environments. In mobile environments, the proposed protocol requires a semi-trusted server instead of a fully-trusted server. Although the semi-trusted server helps users to communicate, it cannot access group key information in messages sent by users. Hence, the semi-trusted server is more secure than a fully-trusted server. The proposed protocol also uses certificateless public key cryptography for user authentication. In comparison with public key cryptography and ID-based cryptography, certificateless public key cryptography reduces the cost of certificate management and avoids the key escrow problem. A formal security proof and performance analysis of the protocol is also presented. Compared to previous schemes, the proposed scheme is more secure and more suitable for mobile environments.

The rest of this paper is organized as follows. Section 2 reviews previous group key agreement protocols. Section 3 introduces the basic preliminaries, including the security assumption and adversarial model. Section 4 presents the proposed scheme. Section 5 discusses the security and performance analyses. Finally, Section 6 concludes the study.

## 2. Related work

In 1976, Diffie and Hellman [10] proposed the well-known key exchange protocol (DH protocol). In this protocol, modular exponentiation is used to allow two parties to establish a secret key. Although the DH protocol was vulnerable to MITM attack, it was highly influential. Many studies later extended the DH protocol to the group key agreement protocol [4,12,16–18,24]. Since these protocols and DH protocol are all based on modular exponentiation, they can be considered variants of the DH protocol. Another type of group key agreement protocol is based identity-based cryptosystems. In 1985, Shamir [22] first introduced an identity-based cryptosystem and signature scheme. Boneh and Franklin [2] proposed a fully functional identity-based encryption scheme in 2001. Various key agreement protocols based on ID-based cryptosystems were later proposed [8,11,23,32]. For example, Wan et al. [28] proposed an anonymous ID-based group key protocol for wireless networks in 2008. In a wired network, user identity is not very important. In a wireless network, however, the identities of group members are exposed to everyone, including the adversary. For example, the adversary can easily trace the movement pattern of a user based on the user identity. In Wan et al.'s work [28], an anonymous protocol successfully excluded outside passive and active adversaries, but the protocol cannot exclude inside attacks. Hence, Wu et al. [31] (2011) proposed an authenticated group key protocol that can resist an insider attack.

Although an ID-based cryptosystem can reduce certificate management costs, an important limitation is the key escrow problem [19]. A solution to the key escrow problem is certificateless public key cryptography (CL-PKC), which was proposed by Al-Riyami and Paterson [1] in 2003. Since then, many certificateless signature schemes have been proposed [9,13,15,27,34]. In 2007, Cao et al. [5] proposed a certificateless group key exchange protocol that uses secret sharing to construct the group key. However, Geng et al. [14] argued that the signature scheme in the Cao et al.'s protocol is insecure and proposed a secure certificateless authenticated group key agreement protocol in which a modification of the Zhang–Zhang signature scheme [34] is used for batch verification.

With the development of mobile devices, many group key agreement protocols [3,6,7,20,21,25,26] have been proposed for the mobile environment. However, since mobile devices have limited battery life and limited computing power, a normal group key agreement protocol is unsuitable for mobile environments. In 2002, Boyd and Nieto [3] proposed an efficient protocol that requires only one communication round. However, the protocol lacks forward secrecy. In 2005, Nam et al. [21] proposed a security protocol for mobile environments based on decisional Diffie–Hellman (DDH) assumption. In 2007, Tseng [26] reported that the group key in the Nam et al.'s protocol can be pre-determined by the powerful node. Additionally, the Nam et al.'s protocol is not a contributory group key agreement protocol since users cannot confirm that their contributions