available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

An efficient and non-interactive hierarchical key agreement protocol

Hua Guo[a,*], Yi Mu[b], Zhoujun Li[c,*], Xiyong Zhang[d]

[a] School of Computer Science & Engineering, Beihang University, Beijing, PR China
[b] School of Computer Science Software Engineering, University of Wollongong, Australia
[c] Beijing Key Laboratory of Network Technology, Beihang University, Beijing, PR China
[d] Zhengzhou Information Science and Technology Institute, Zhengzhou, PR China

ARTICLE INFO

Article history:
Received 16 June 2010
Received in revised form
4 September 2010
Accepted 10 October 2010

Keywords:
Key agreement
Hierarchical systems
Mobile ad-hoc networks

ABSTRACT

The non-interactive identity-based key agreement schemes are believed to be applicable to mobile ad-hoc networks (MANETs) that have a hierarchical structure such as hierarchical military MANETs. It was observed by Gennaro et al. (2008) that there is still an open problem on the security of the existing schemes, i.e., how to achieve the desirable security against corrupted nodes in the higher levels of a hierarchy? In this paper, we propose a novel and very efficient non-interactive hierarchical identity-based key agreement scheme that solves the open problem and outperforms all existing schemes in terms of computational efficiency and data storage.

1. Introduction

Mobile ad-hoc networks (MANETs) and tactical networks are very dynamic and have significant bandwidth and energy constraints. In these networks, many nodes are vulnerable to attacks. Establishing shared cryptographic keys for MANETs is an important step for secure communications. Authenticated key agreement (AKA) protocols play an important role in authentication and secure channel establishment. However, it is observed that AKA protocols (especially, a hierarchical AKA) add considerable computation and bandwidth overheads to the network, thus they are not suitable for MANETs which usually have significant bandwidth and energy constraints.

An authenticated key agreement protocol for MANETs and tactical networks should have the following properties (Gennaro et al., 2008):

- *Non-interactive*: any two nodes can compute a unique shared secret key without an interaction. This property is used to save bandwidth.
- *Identity-based* (Shamir, 1984): each node computes the shared secret key only using its own secret key and the identity of its peer. This property is used to avoid coordination and therefore support ad-hoc communication.
- *Hierarchical*: the scheme is decentralized through a hierarchy where intermediate nodes in the hierarchy can derive the secret keys for each of its children. This property is used to allow flexible provisioning of nodes.
- *Resilient*: the scheme is fully resilient against any number of malicious nodes.

A non-interactive identity-based AKA demonstrates some elegant features in saving bandwidth and providing the convenience in identity management. Despite these features,

* *Corresponding authors*. Tel.: +86 61 2 4221 4327; fax: +86 61 2 4221 4170.
E-mail addresses: hguo.xyz@163.com (H. Guo), lizj@buaa.edu.cn (Z. Li).

0167-4048/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2010.10.003

how to construct a sound non-interactive identity-based AKA is still an open challenge.

There are some nice attempts to provide efficient and provably secure key agreement schemes for hierarchical MANETs. One of such attempts is due to Blundo et al. (1998) who used the earlier work of Blom (1984) based on the polynomials. Later, Eschenauer and Gligor (2002) presented an alternative by using a randomized key-predistribution schemes. Since their schemes are threshold-based, the security of their schemes is assumed when the corrupted nodes in the hierarchy are less than the pre-defined threshold.

The first hierarchical identity-based encryption was proposed by Horwitz and Lynn (2002). Their scheme is only two level where a pairing-based scheme is placed at the top level and a polynomial-based scheme is at the second level. Although their scheme supports key agreement, such arrangement requires user interaction. To propose a non-interactive key agreement, Gennaro et al. (2008) reversed the order, i.e., using the polynomial scheme for all the top levels and the pairing-based scheme only for the leaves. They proposed two non-interactive hierarchical key agreement protocols by making use of two existing hierarchical schemes (Blundo et al., 1998; Ramkumar et al., 2005) along with the work due to Sakai et al. (2000). These protocols are indeed well motivated in terms of their applicability in hierarchical MANETs and are secure against the corruption of any leaves. Unfortunately, their scheme is not designed against the corruption of the nodes of the higher levels in the hierarchy. Thus, in Gennaro et al. (2008) pointed out that "it would be interesting to have a hierarchical non-interactive key-agreement scheme where resilience is achieved not only against any number of corruptions in the leaves but also against any number of corruptions in the higher levels of the hierarchy". They left it as an open problem.

In this paper, we answer this open problem by presenting an efficient hierarchical non-interactive identity-based key-agreement protocol based on the pairing cryptography. Our protocol satisfies all of the four properties defined by Gennaro et al. (2008). Different from Gennaro et al.'s (2008) scheme, which is based on a threshold-based hierarchical scheme and a non-interactive scheme of Sakai et al. (2000), our new scheme is pairing-based. The major advantage of our new solution is that it can resist against any corrupted nodes in the entire hierarchy. This is not possible in Gennaro et al.'s scheme. Moreover, our scheme captures the dynamic property as in Gennaro et al.'s scheme, i.e., nodes can be added to the hierarchy without requiring any further coordination with other nodes and without changing the information held by other nodes.

In addition, when the number of leaves is arbitrarily large and the depth of the hierarchy is relatively small, our scheme offers much better performance in terms of computation, bandwidth, and data storage.

The rest of this paper is arranged as follows. In Section 2, we introduce the relevant background on identity-based cryptography (e.g. bilinear pairings, the complexity assumptions and non-interactive identity-based key agreement protocol). In Section 3, we present our hierarchical non-interactive identity-based key agreement protocol, whose security analysis is presented in Section 4. In Section 5, we compare our protocol with the other protocols in terms of the computation costs and data storage. We conclude this paper in Section 6.

2. Preliminaries

In this section, we introduce the background knowledge that will be used for our scheme. We give the basic definition and properties of bilinear pairings, the computational problems to which our scheme can be reduced to, and Sakai et al.'s (2000) non-interactive identity-based key agreement protocol.

2.1. *Bilinear map and security assumption*

We first revisit the basic definition of the "admissible bilinear map" which plays a central roles in our scheme. More details can be found in Boneh and Franklin (2001).

The admissible bilinear map $\hat{e}$ is defined over two groups of the same prime order q denoted by $\mathbb{G}$ and $\mathbb{G}_T$ in which the Computational Diffie-Hellman problem is hard. More formally, we have the following definition:

Definition 1. (Bilinear Map)

Let $\mathbb{G}$ is an additive group of prime order q and $\mathbb{G}_T$ a multiplicative group of the same order. Let P denote a generator of $\mathbb{G}$. An admissible pairing is a bilinear map $\hat{e}$: $\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$ which has the following properties:

- *Bilinear: given* Q, $R\in\mathbb{G}$ and $a,b\in\mathbb{Z}_q^*$, *we have* $\hat{e}(aQ,bR) = \hat{e}(Q,R)^{ab}$
- *Non-degenerate:* $\hat{e}(P,P)\neq 1_{\mathbb{G}_T}$.
- *Computable:* $\hat{e}$ *is efficiently computable.*

$\mathbb{G}$ is a subgroup of the group of points on an elliptic curve over a finite field. $\mathbb{G}_T$ is a subgroup of a multiplicative group of a related finite field. Typically, the map $\hat{e}$ can be derived from either the Weil pairing or Tate pairing on an elliptic curve over a finite field. The computational effort of the Tate pairing is less than the Weil pairing. A more comprehensive description of how these groups, pairings, and other parameters should be selected in practice for efficiency and security can be found in Boneh and Franklin (2001), Galbraith et al. (2003) and Menezes et al. (1993).

Throughout this paper, we will simply use the term "bilinear map" to refer to the admissible bilinear map.

2.2. *Computational problems*

Bilinear map captures an important cryptographic problem, i.e., the Bilinear Diffie-Hellman (BDH) problem, which was introduced by Boneh and Franklin (2001). The security of our scheme relies on a variant of the BDH assumption.

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two groups of a prime order q. Let $P\in\mathbb{G}^*$ be a generator of $\mathbb{G}$. Suppose that there exists a bilinear map $\hat{e}:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_T$. We consider the following computational assumptions:

- Bilinear Diffie-Hellman (BDH): For $a,b,c\in_R\mathbb{Z}_q^*$. Given aP,bP,cP, computing $\hat{e}(P,P)^{abc}$ is hard.