Ad Hoc Networks 10 (2012) 1009–1016

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

An efficient remote user authentication and key agreement protocol for mobile client–server environment from pairings

Debiao He

School of Mathematics and Statistics, Wuhan University, Wuhan, People's Republic of China

ARTICLE INFO

Article history:
Received 30 April 2011
Received in revised form 19 September 2011
Accepted 2 January 2012
Available online 12 January 2012

Keywords:
ID-based
Mutual authentication
Key agreement
Bilinear pairing
Mobile device
Provable security

ABSTRACT

With the continue evaluation of mobile devices in terms of the capabilities and services, security concerns increase dramatically. To provide secured communication in mobile client–server environment, many user authentication protocols from pairings have been proposed. In 2009, Goriparthi et al. proposed a new user authentication scheme for mobile client–server environment. In 2010, Wu et al. demonstrated that Goriparthi et al.'s protocol fails to provide mutual authentication and key agreement between the client and the server. To improve security, Wu et al. proposed an improved protocol and demonstrated that their protocol is provably secure in random oracle model. Based on Wu et al.'s work, Yoon et al. proposed another scheme to improve performance. However, their scheme just reduces one hash function operation at the both of client side and the server side. In this paper, we present a new user authentication and key agreement protocol using bilinear pairings for mobile client–server environment. Performance analysis shows that our protocol has better performance than Wu et al.'s protocol and Yoon et al.'s protocol. Then our protocol is more suited for mobile client–server environment. Security analysis is also given to demonstrate that our proposed protocol is provably secure against previous attacks.

1. Introduction

With the rapid growth of mobile networks, handheld mobile devices (i.e. PDAs and cellular phones) are widely and popularly used in many mobile applications, such as on-line shopping, internet banking and pay-TV. As a result, security of the secure remote user authentication over insecure communication channels becomes an important issue to ensure the fair transaction. Then the remote user authentication and key agreement protocol for mobile client–server environment has been studied widely.

Generally speaking, the remote client authentication is usually implemented by the traditional public-key cryptography [1,2]. But since the computation ability and battery capacity of mobile devices are limited, traditional public-key cryptograph, in which the computation of modular exponentiation is needed, is no longer applicable in mobile devices. To solve the problem, the elliptic curve cryptosystem (ECC) [3,4] can be resorted to because it has significant advantages like smaller key sizes, faster computations. Thus, ECC-based authentication protocols are more suitable for mobile devices than other cryptosystem. However, like other public-key cryptography, ECC also needs a public key infrastructure (PKI) to maintain the certificates for users' public keys. With the increase of the user's number, PKI requires a large storage space to store users' public keys and certificates. Besides, additional computations are required to verify the other's certificate in these protocols. To solve the above problems, Shamir [5] proposed the identity (ID)-based public-key cryptosystem. Compared with the traditional certificate-based public-key systems, the ID-based public key system may simplify the certificate management. However, the disadvantage of the system lies in the fact that the user's

E-mail address: hedebiao@163.com

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2012.01.002

private key must be generated by the Key Generator Center (KGC). Because the security of Shamir's system is based on the integer factorization problem, Shamir's system is not practical. Fortunately, Boneh and Franklin [6] proposed a practical ID-based encryption protocol from the Weil pairing defined on elliptic curves in 2001. Since then, the pairing-based remote client authentication protocol was studied widely.

In 2006, Das et al. [7] proposed a pairing-based remote client authentication protocol with smart cards. However, their protocol suffered from a forgery attack [8]. Later on, two improvements [9,10] on Das et al.'s protocol were proposed. In [9], Fang and Huang proposed an improvement to overcome the mentioned forgery attack. Nevertheless, Giri and Srivastava [10] proved that the Fang et al.'s improvement is still insecure against another forgery attack (or called off-line attack). However, the Giri et al.'s improvement used a public-key encryption algorithm [11] in the smart card. In 2008, Tseng et al. [11] presented a provably secure and efficient pairing-based client authentication protocol for wireless clients with smart cards. In 2009, Goriparthi et al. [12] also proposed another efficient protocol based on Das et al.'s remote client authentication protocol. However, these protocols [7,9,10,12] do not provide mutual authentication and key agreement between the client and the server. To improve security, Wu and Tseng [13] proposed an improved protocol and demonstrated that their protocol is provably secure in random oracle model. Based on Wu et al.'s work, Yoon and Yoo [14] proposed another user authentication and key agreement protocol for mobile client–server environment to improve performance. However, their scheme just reduces one hash function operation at the both of client side and the server side. In this paper, we present a new user authentication and key agreement protocol using bilinear pairings for mobile client–server environment. Performance analysis is made to show that our protocol has better performance than Wu et al.'s protocol and Yoon et al.'s protocol. Then our protocol is more suited for mobile client–server environment. Security analysis is also given to demonstrate that our proposed protocol is provably secure against previous attacks.

The remainder of this paper is organized as follows. Section 2 describes some preliminaries. In Section 3, we propose our efficient mutual authentication and key agreement protocol. The security analysis of the proposed protocol is presented in Section 4. In Section 5, performance analysis and some experimental results are presented. Conclusions are given in Section 6.

2. Preliminaries

Let G_1 be a cyclic additive group of prime order q, and G_2 be a cyclic multiplicative group of the same order q. We let P denote the generator of G_1. A bilinear pairing is a map $e{:}G_1 \times G_1 \rightarrow G_2$ which satisfies the following properties:

(1) Bilinearity

$$e(aQ, bR) = e(Q, R)^{ab}, \quad \text{where} \quad Q, R \in G_1, a, b \in Z_q^*.$$

(2) Non-degeneracy

$$e(P, P) \neq 1_{G_2}.$$

(3) Computability

There is an efficient algorithm to compute $e(Q, R)$ for all $Q, R \in G_1$.

The Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such admissible pairings, as in [9]. The following problems are assumed to be intractable within polynomial time.

Definition 1 (*Computational Diffie–Hellman (CDH) Problem*). Given $\{P, xP, yP \in G_1\}$, it is difficult to compute $xyP \in G_1$.

Definition 2 (*Collision Attack Assumption (k-CCA) Problem[15]*). For an integer k and $x \in Z_q^*, P \in G_1$. Given $\{P, xP, e_1, e_2, \ldots, e_k \in Z_q^*\}$ and $\left\{\frac{1}{x+e_1}P, \frac{1}{x+e_2}P, \ldots, \frac{1}{x+e_k}P\right\}$, it is difficult to compute $\frac{1}{x+e}P$ for some $e \notin \{e_1, e_2, \ldots, e_k\}$.

3. Our protocol

Our proposed protocol consists of three phases that include the setup phase, the key extract phase, and the user authentication and key agreement phase. We describe them as follows:

3.1. Setup

On input a security parameter l, this algorithm runs as follows.

(1) Selects a cyclic additive group G_1 of prime order q, a cyclic multiplicative group G_2 of the same order, a generator P of G_1, and a bilinear map $e{:}G_1 \times G_1 \rightarrow G_2$.
(2) Computes $e(P, P) = g \in G_2$.
(3) Choose a random master key $s \in Z_q^*$ and set the master public key $P_{pub} = sP$.
(4) Chooses cryptographic hash functions $H_1 : \{0,1\}^* \times G_1 \rightarrow Z_q, H_2 : G_1 \times \{0,1\}^* \times Z_q^* \times G_1 \rightarrow Z_q, H_3 : \{0,1\}^* \times Z_q^* \times G_1 \times Z_q^* \times G_1 \rightarrow Z_q, H_4 : Z_q^* \times \{0,1\}^* \times Z_q^* \times G_1 \times G_1 \rightarrow Z_q$.

The system parameters are $params = \{G_1, G_2, e, P, P_{pub}, g, H_1, H_2, H_3, H_4, l\}$. The master-key is $s \in Z_q^*$.

3.2. Key extract phase

This algorithm takes system parameters, master key and a user's identifier ID as inputs, generates the partial private key. The Schnorr's signature scheme [16] is a signature scheme based on the discrete logarithm problem, which can be proved secure against the adaptively chosen message attack in the random oracle model. We use Schnorr's signature scheme to generate the partial private key as follows.