Commun Nonlinear Sci Numer Simulat 17 (2012) 2969–2977

Contents lists available at SciVerse ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Security improvement on an anonymous key agreement protocol based on chaotic maps

Kaiping Xue *, Peilin Hong

The Information Network Lab of EEIS Department, USTC, Hefei 230027, China

ARTICLE INFO

Article history:
Received 13 May 2011
Received in revised form 12 October 2011
Accepted 22 November 2011
Available online 8 December 2011

Keywords:
Key agreement
Chaotic maps
User anonymity
Contributory property
Protocol security

ABSTRACT

In 2009, Tseng et al. proposed a password sharing and chaotic map based key agreement protocol (Tseng et al.'s protocol). They claimed that the protocol provided mutual authentication between a server and a user, and allowed the user to anonymously interact with the server to establish a shared session key. However, in 2011, Niu et al. have proved that Tseng et al.'s protocol cannot guarantee user anonymity and protocol security when there is an internal adversary who is a legitimate user. Also it cannot provide perfect forward secrecy. Then Niu et al. introduced a trust third party (TTP) into their protocol designing (Niu et al.'s protocol). But according to our research, Niu et al.'s protocol is found to have several unsatisfactory drawbacks. Based on reconsidering Tseng et al.'s protocol without introducing TTP, we give some improvements to meet the original security and performance requirements. Meanwhile our proposed protocol overcomes the security flaws of Tseng et al.'s protocol.

1. Introduction

In a key agreement protocol, a shared secret key is derived by two or more parties as a function of information contributed by each of these parties. Ideally no party can predetermine the agreed session key. Diffie–Hellman (D–H) key exchanging protocol [1] is the first key agreement protocol, in which two parties jointly exponentiate a generator with random numbers, in such way that an eavesdropper has no way of guessing the key. However D–H protocol cannot provide authentication between the two parties, which can launch man-in-the-middle attacks. Then some mutual authentication added D–H key agreement schemes have been proposed, which are usually based on public key encryption protocols. Mutual authentication methods in these schemes are secure and reliable, but have much computational overhead and storage overhead.

In the passed few years, cryptography systems based on chaos theory [2,3] have been studied widely. Much work has been done by introducing chaotic maps into the design of cryptography algorithms, such as symmetric encryption [4,5], asymmetric encryption [13], hash functions [6,7,17], and so on. For the sake of security improvement and overhead reduction, some chaotic map based key agreement protocols [8–11] have been proposed. But none of these schemes can protect users' identities while establishing a shared session key.

In another way, password sharing based key agreement protocols have been proposed to provide authentication and reduce overhead. The first password sharing based schemes was proposed by Bellovin and Merritt [12], which was a two-party password authenticated key exchange protocol. Two party password authenticated key exchange protocols allow a user and a server to establish a session key over an insecure channel, where each user only shares an easy-to-remember password with the trusted server. Then many other password authentication based key agreement schemes and chaotic

* Corresponding author.
E-mail address: kpxue@ustc.edu.cn (K. Xue).

1007-5704/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.cnsns.2011.11.025

maps based security schemes are proposed for two-party or multi-party secure communication. In most of these schemes, the server needs to search the shard password or extension values of the password for verify a user. User's identity needs to be set as the searching key. All these schemes have some storage overhead, and they are lack of anonymity support.

Currently, very few schemes provide key agreement protocols with the property of both protocol security and user anonymity. In [14], Tseng et al. firstly proposed a password sharing and chaotic maps based key agreement protocol (named Tseng et al.'s protocol in this paper) which preserved both users' anonymity and security. However, in [15] Niu and Wang have proved that Tseng et al.'s protocol cannot guarantee user anonymity and protocol security when there is an internal adversary who is a legitimate user. And it cannot provide perfect forward secrecy. In [15], Niu and Wang introduced a trust third party (TTP), which was assumed to be trusted as the same as the server. TTP is introduced to provide assistance in establishing the session key between the user and the server, where the anonymity of the user needs to be guaranteed. But based on our research, Niu et al.'s protocol is found to have several unsatisfactory drawbacks: (1) TTP is another performance and security bottleneck; (2) TTP needs to know user's identity to search the session key, which destroys the anonymity of the user; (3) two more steps will bring more delay caused by more communication overhead and more computation overhead.

Based on reconsidering Tseng et al.'s protocol without introducing TTP, we give some improvements to meet the security and performance requirements: (1) having no additional storage; (2) providing protocol security and user anonymity. Meanwhile our proposed scheme overcomes the security flaws of Tseng et al.'s protocol.

The rest of this paper is organized as follows. Section 2 reviews the Chebyshev chaotic map [16] with the semigroup property, and then introduces a hash function based on Chebyshev chaotic map. Section 3 gives the brief analysis of Tseng et al.'s protocol. Section 4 reviews and analyzes Niu et al.'s protocol. Section 5 describes our proposed key agreement protocol in details. Performance and security analysis of our proposed scheme are given in Section 6 and Section 7. At last, Section 8 presents the overall conclusion.

2. Chebyshev chaotic map with semi-group property

In this section we first describe the Chebyshev chaotic map [16]. Then we introduce the hash function based on Chebyshev chaotic map [17].

2.1. Chebyshev chaotic map

The Chebyshev polynomial of degree n is defined as

$$T_n(x) = cos(n * arccosx), \quad -1 \leqslant x \leqslant 1 \tag{1}$$

where $n \geqslant 2$, $T_0(x) = 1$, $T_1(x) = x$, the recurrent formulas are

$$\begin{aligned} &T_2(x) = 2x^2 - 1 \\ &T_3(x) = 4x^3 - 3x \\ &T_4(x) = 8x^4 - 8x^2 + 1 \\ &\dots \\ &T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x), \quad n = 1, 2, \dots \end{aligned} \tag{2}$$

Chebyshev polynomial can be proved to have the following two important properties. The first is **semi-group property**, which can be used in designing key agreement protocols and public key encryption schemes:

$$T_r(T_s(x)) = cos(r * arccos(cos(s * arccosx))) = cos(rs * arccos(x)) = T_{sr}(x) = T_s(T_r(x)) \tag{3}$$

The second is **chaotic property**: When n > 1, Chebyshev polynomial map $T_n : [-1, 1] \to [-1, 1]$ of degree n is a chaotic map with its invariant density

$$f^*(x) = 1/(\pi\sqrt{1 - x^2})$$

for Lyaounov exponent $\lambda = \ln n > 0$

2.2. One-way hash function construction based on the chaotic map

A one-dimension piecewise linear chaotic system is defined as:

$$X(t+1) = F(X(t), P) = \begin{cases} X(t)/P, & X(t) \in [0, P) \\ (X(t) - P)/(0.5 - P), & X(t) \in [P, 0.5) \\ (1 - X(t) - P)/(0.5 - P), & X(t) \in [0.5, 1 - P) \\ (1 - X(t))/P, & X(t) \in [1 - P, 1] \end{cases} \tag{4}$$