Journal of Information Security and Applications 35 (2017) 160–167

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Enhanced secure mutual authentication and key agreement scheme with user anonymity in ubiquitous global mobility networks

Prosanta Gope

Department of Computer Science, National University of Singapore, 21 Lower Kent Ridge Rd, 119077, Singapore

ARTICLE INFO

Article history:
Available online 17 July 2017

Keywords:
Privacy
Anonymity
Authentication
Smart card
Global mobility networks

ABSTRACT

With the widespread use of mobile gadgets, security in mobile communication becomes an important issue. In 2011, Zhou et al. proposed a mutual authentication and key agreement scheme with the user anonymity for roaming environments. In this article, however, we reveal that the authentication protocol presented by Zhou et al. suffers from certain weaknesses which have been overlooked during design. As a consequence of these weaknesses, Zhou et al.'s scheme cannot achieve desired security. Therefore, here we propose a novel authentication scheme to overcome these weaknesses that is efficient, secure, and causes significantly less computational overhead as compared to Zhou et al.'s scheme.

1. Introduction

Wireless mobile networks take up a large mount in the contemporary communications. One can use a mobile device, e.g., a smart phone, to access wireless mobile networks distributed everywhere in anytime to obtain the data he/she needs. Global Mobility Network(GLOMONET) provides the roaming service, which is supported by the home agent(HA) in any foreign network. But unfortunately the fact that the message transmission is very dangerous in wireless environment is widely accepted by all. So before the communication, authentication is very important to make the data flow secure. When a mobile station (MS) moves into any foreign wireless network, he should contact the special foreign agent(FA) to get the information in it. However, it is necessary that the process of mutual authentication between MS and FA must be helped through the home agent(HA) where MS registers itself. After the mutual authentication, a temporary session key is constructed for the latter conversation between MS and FA and the following messages can keep secret. The other hot issue about the secure transmission is about the privacy of the MS. Malicious attackers may get valid information, such as the identity or the password of the user, if the authentication scheme is designed with security flaws. So how to protect the user's information is also an urgent task for the researchers.

For accomplishing these goals, many authentication and key agreement schemes have been proposed with anonymity for roaming services in global mobile networks [1–8]. Particularly, in 2004, Zhu et al. proposed a wireless security protocol based on smart card and featuring user anonymity [1]. Unfortunately, Lee and Hwang [2] pointed out in 2006 that Zhu and Ma's protocol's [1] does not achieve mutual authentication and is also subjected to the forgery attack. Lee et al. also proposed a slightly modified version of Zhu et al.'s protocol so as to remedy the identified shortcomings. However, in [3], it was shown that the Zhu et al.'s scheme and Lee and et al.'s scheme fails to provide user anonymity, and Wu, Lee and Tsaur proposed an enhanced scheme by providing an effective remedy. Independently, in [4], Chang et al. showed that Lee et al.'s scheme cannot provide user anonymity under the forgery attack and also proposed an enhanced authentication scheme. Unfortunately, Youn et al. found that the scheme of [4] fails to achieve user anonymity under four attack strategies [5]. In 2008, Tang et al. proposed an authentication protocol for mobile network [6], and they claimed that their scheme is immune to all known types of attacks. However, [7] showed that Teng et al.'s scheme [6] suffers from replication attack. Hereafter, in 2011, Zhou et al. proposed a mutual authentication and key agreement scheme [8], based on the Decisional Diffie-Hellman (DDH) assumption. However, in this article, we show that the scheme has some serious weaknesses which have been overlooked during design. Therefore, the contribution of this article is to disclose the weaknesses of the Zhou et al.'s scheme, which have not been revealed yet.

Apart from [1–8], there are many authentication schemes [15–21] have been proposed in recent years. For example, Gope et al. proposed two authentication protocols [10] and [15] which are the improvements of He et al. [16] and Wen et al.'s scheme [17], respectively. In [10], to easily comprehend a mobile subscriber and also for dealing with replay attack, the authors introduced the concept of a sequence number, which is randomly generated, thus may

E-mail addresses: prosanta@comp.nus.edu.sg, prosanta.nitdgp@gmail.com

http://dx.doi.org/10.1016/j.jisa.2017.07.002
2214-2126/

Table 1
Notations and cryptographic functions.

Symbol	Definition
MS	Mobile Station
FA	Foreign Agent
HA	Home Agent
ID_M	Identity of the mobile user
AID_M	One-time-alias identity of the MS
SID_M	Shadow identity of the MS assigned by the HA
ID_h	Identity of the HA
ID_f	Identity of the FA
SK	Session key between FA and MS
K_{uh}	Shared key between MS and HA
K_{fh}	Secret Key shared between the FA and HA
Ts_{uh}	Transaction sequence number (maintain both MS and HA)
E_K	Encryption using secret key K
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation

not be unique and hence this may cause difficulty at the server-side to uniquely identify a MS. On the other hand, the scheme presented in [15], is based on *Chinese Remainder Theorem* (CRT), which will cause higher computational overhead and hence is suitable for resource constrained mobile devices.

Meanwhile, Zhang et al. [18] proposed a new authentication scheme for roaming environment. However, Wang et al. [19] shown that Zhang et al.'s scheme is vulnerable to password-guessing attack. Besides, they also pointed out the security weaknesses in some existing GLOMONET authentication protocols [20,21]. Recently, some other interesting anonymous authentication protocols have introduced using public-key cryptography, where the researches have shown how to enhance the security of the anonymous authentication protocols in GLOMONET by considering various new aspects of privacy. In a nutshell, this article makes three main contributions.

- First, this article shows some security weaknesses on an existing authentication protocol proposed by Zhou et al.
- Second, we propose a new mutual authentication and key agreement scheme based on symmetric key crypto-system.
- Finally, through security and performance analyses we show that our proposed scheme can ensure several imperative security properties (like privacy against eavesdropper, security against any forgery attacks) and hence can guarantee a secure and expeditious roaming service in GLOMONET with the reasonable computational overhead.

The remainder of this article is organized as follows. Section 2 reviews the protocol of [8] and whose weaknesses are pinpointed in Section 3. Thereafter, we present our proposed scheme in Section 4, whose security and performance are analyzed in Sections 5 and 6 respectively. The formal analysis of the proposed scheme is presented in Section 7. Finally, a concluding remark is given in Section 8. The abbreviations and cryptographic functions used in this article are defined in Table 1.

2. Review of Zhou et al.'s scheme

In this section, we briefly describe Zhou et al.'s scheme, which consists of two phases. In Phase I, the home agent (HA) securely issues a smart card to a mobile user MS. In Phase II, both the MS and foreign agent (FA) mutually authenticate each other under the supervision of the MS's home agent and eventually establish a session key between them.

2.1. Phase I: registration phase

When a mobile user desires to register at the home agent, the user needs to request to the home agent, and then the home agent will issue a smart card with related information to the user. In this regard, MS at first submits his/her identity ID_M and the password PSW_M to the HA. After receiving the request from MS, the HA selects two large prime number p, q, where $p = 2q + 1$ and a multiplicative group generator g of order q. Then, the home agent also chooses its secret key $b \in Z_q^*$ and computes $B = g^b \bmod p$, $u = h(ID_M \| b) \oplus PSW_M$. Hereafter HA issues a smart card containing $\{p, g, B, h(.), u\}$ and delivers it to MS through a secure channel.

2.2. Phase II: mutual authentication and key agreement phase

Once enrolled by HA, when MS visits a foreign network managed by the FA, then he/she needs to authenticate himself/herself to FA. In this case, they take assistance of the HA, who issued the smart card to MS. The steps of this phase are outlined in Fig. 1. and explained as follows.

Step 1 M_{A_1} : MS → FA : $\{AID_M, N_m, A, V_1, ID_h\}$.
MS submits his/her identity and password to the smart card. Then the device generates two random numbers a and N_m, and computes $A = g^a \bmod p$, $D = B^a \bmod p$, $C = u \oplus PSW_M$, $AID_M = ID_M \oplus h(D \| N_m)$, and $V_1 = h(C \| D)$. Where AID_M denotes the one-time alias identity of the MS. Finally, MS forms the request message M_{A_1} and sends it to FA.

Step 2 M_{A_2} : $FA \rightarrow HA$: $\{AID_M, N_m, A, V_1, N_f, ID_f, V_2\}$.
Upon receiving the request message from MS, FA at first generates a random number N_f, then computes $V_2 = h(N_f \| K_{fh} \| V_1 \| ID_f \| A \| AID_M \| N_m)$ and sends a message $M_{A_2} = \{AID_M, N_m, A, V_1, N_f, ID_f, V_2\}$ to the HA.

Step 3 M_{A_3} : $HA \rightarrow FA$: $\{K_1, V_3, V_4\}$.
After receiving M_{A_2}, HA computes and verifies whether V_2 is equal to $h(N_f \| K_{fh} \| V_1 \| ID_f \| A \| AID_M \| N_m)$ or not. If so, HA computes $D = A^b \bmod p$, $ID_M^* = AID_M \oplus h(D \| N_m)$, $V_1^* = h(h(ID_M^* \| b) \| D)$ and checks legitimacy of the user where the relation $V_1^* = V_1$ must satisfy. After successful verification, HA continues to compute $SK = h(D \| ID_M \| N_m \| ID_f \| N_f)$, $K_1 = SK \oplus h(K_{fh} \| N_f)$, $V_4 = h(D \| N_m \| ID_f)$, $V_3 = h(K_{fh} \| N_f \| K_1 \| V_4)$ and sends a response message M_{A_3} to the foreign agent (FA).

Step 4 M_{A_4} : $FA \rightarrow MS$: $\{ID_f, N_f, V_4\}$.
After receiving M_{A_3}, FA verifies whether V_3 is equal to $h(K_{fh} \| N_f \| K_1 \| V_4)$ or not. If so, then the system computes the session key $SK = K_1 \oplus h(K_{fh} \| N_f)$ and forms a message M_{A_4} and sends it to MS. After receiving the message M_{A_4}, MS at first verifies V_4 is equal to $h(D \| N_m \| ID_f)$ or not. If so, MS believes that the foreign agent is a legitimate one and based on that, computes the agreed session key $SK = h(D \| ID_M \| N_m \| N_f \| ID_f)$.

3. Security weaknesses in Zhou et al.'s protocol

In this section, we present the several weaknesses of the Zhou et al.'s protocol, which certainly cause an insecure mobile communication.

3.1. Unsuccessful key-agreement (forgery attacks)

Assume that a malicious adversary A who does not want that FA and MS successfully establish the session key SK between them. In this regard, A just eavesdrops the communication between FA and MS (intercepts M_{A_4}) and replaces the nonce $N_f$with N'_f. Unfortunately, MS does not verify it and even cannot