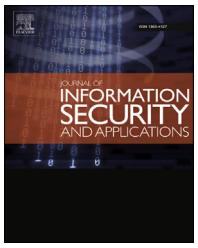
Available online at www.sciencedirect.com

ScienceDirect

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



An efficient and secure anonymous mobility network authentication scheme

Wen-Chung Kuo [a,*], Hong-Ji Wei [b], Jiin-Chiou Cheng [c]

[a] Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology, Yunlin, Taiwan

[b] Library and Information Center, University of Kang Ning, Taiwan

[c] Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology, Taiwan

Keywords:
Authentication scheme
Anonymous authentication
Mobile networks
Roaming
Elliptic curve

ABSTRACT

The demands of Internet users are steadily increasing. Many users access Internet services through mobile devices via wireless networks. To prevent disclosure of private data, researchers have proposed various anonymous roaming authentication schemes which apply different technologies to provide integral security properties, such as symmetric and asymmetric encryption, digital signature, timestamp, etc. Unfortunately, some of these schemes still exhibit security and efficiency issues. In order to provide tripartite authentication and enhance efficiency, we propose an efficient and secure anonymous authentication scheme for mobility networks. According to our performance and security analysis, we can prove that our proposed scheme is able to enhance efficiency and improve security in comparison to previous schemes.

1. Introduction

With popularization of smart phones, mobility networks are increasingly pervasive. Because mobile networks transfer information using electromagnetic waves, the message are vulnerable to interception and may expose users to privacy concerns. In order to prevent these issues, many authors proposed different anonymous roaming authentication schemes for mobile networks to protect user privacy (Chang et al., 2009a, 2009b; Kim and Kwak, 2012; Lee et al., 2006, 2009; Li et al., 2011; Li and Lee, 2012; Mun et al., 2012; Wu et al., 2008; Feng, 2009; Zeng et al., 2009; Zhou and Xu, 2011; Zhu and Ma, 2004). In 2004, Zhu and Ma first proposed an anonymous authentication scheme for wireless networks. However in 2006, Lee et al. analyzed Zhu–Ma's scheme and found a weakness where it failed to ensure user anonymity and backward secrecy of the session key. In the same work, Lee et al. also proposed an improved anonymous authentication scheme (LHL-scheme) to resolve the two weaknesses of Zhu–Ma's scheme. Unfortunately in 2008, Wu et al. pointed out that the LHL-scheme still contains the same weakness as Zhu–Ma's scheme because it only uses a one-way hash function to hide the user's real identity. An attacker could easily obtain ID_{MU} by off-line guessing attack. The session key between mobile user (*MU*) and foreign agent (*FA*) could be determined by context such as obtaining session key K_{i+1} from K_i and K_{i-1}. In order to remedy these issues, Wu et al. proposed an enhanced authentication scheme (WLT-scheme) with anonymity and modified $h(ID_{MU})$ to be $h(N||ID_{MU})$, where N is a random number, to prevent off-line guessing attack. So the WLT-scheme provided backward secrecy of the session key because the session between MU and FA could not be determined by context anymore.

* *Corresponding author.*
E-mail address: simonkuo@yuntech.edu.tw (W.-C. Kuo).
http://dx.doi.org/10.1016/j.jisa.2013.12.002

In 2009, many authors (Chang et al., 2009a; Lee et al., 2009; Feng, 2009; Zeng et al., 2009) pointed out that WLT-scheme still could not ensure anonymity of users effectively because $h(ID_{HA}||N)$ was shared with every MU in the same HA. In addition, Chang et al. (Chang et al., 2009b) also found a weakness to impersonation attack in WLT-scheme and proposed an improved scheme (CLL-scheme), which was added $h(N)$ to calculate r for each MU, to overcome these two weaknesses within the registration phase. Unfortunately, every legitimate user is privy to other users communications in the same area because they share the same secret data, such as $h(N)$ and $h(ID_{HA}||N)$, for obtaining the user's ID. Therefore, the CLL-scheme still cannot offer anonymity from other users.

Recently, Mun et al. (2012) proposed a new framework of an anonymous authentication scheme (MHLYC-scheme) to improve the security weakness in previous schemes. In order to match the computational capability of mobile devices, the MHLYC-scheme only utilizes a hash function and random nonce instead of the public-key cryptosystem and timestamp. Kim and Kwak (2012) analyzed the MHLYC-scheme and found the MHLYC-scheme cannot prevent replay and man-in-the-middle attacks. They also proposed an improved anonymous authentication scheme to overcome these security weaknesses. From our analysis, their method is susceptible to replay attack. In this paper, we propose an efficient and secure anonymous roaming authentication scheme for mobility networks. According to our security analysis, our proposed scheme not only provides several security properties but also enhances performance over mobility networks.

The remainder of this paper is organized as follows: In Section 2, we propose an efficient and secure anonymous authentication scheme and analyze the security of our proposed scheme in Section 3. In Section 4, we compare our proposed scheme with previous schemes regarding security and performance. Finally, conclusions are provided in Section 5.

2. The proposed anonymous mobile authentication scheme

The notations and symbols used in the proposed scheme are shown in Table. 1. There are four main phases in our proposed scheme: the registration phase, the authentication and establishment of the session key phase, the update session key phase and the password change phase. The procedure of proposed scheme is described below.

Table 1 – Notations.

Symbol	Explain
MU	The mobile user
FA	The foreign agent
HA	The home agent
PW_{MU}	The password of mobile user
ID_A	The identity of an entity A
$h(.)$	A collision free one-way hash function
p_{MU}	The secret key selected by MU
$\oplus$	The exclusive-OR operation
$\|\|$	The concatenation operation
N_A	A random nonce selected by an entity A
P	A point on the elliptic curve $Ep(a, b)$
$P.x$	The x-axis value of the point P
$p_{HA\text{-}MUi}$	The secret key of HA for MU_i

2.1. Registration phase

In this phase, MU needs to register with HA before using FA's roaming service. The steps of the registration phase are depicted in Fig. 1.

Step 1. MU chooses a secret key p_{MU} and ID_{MU} and computes $PW_{MU} = h(ID_{MU}||p_{MU})$.

Step 2. Sends ID_{MU} and PW_{MU} to HA through a secure channel.

Step 3. After receiving PW_{MU} and ID_{MU} from MU, HA checks whether ID_{MU} already exists. If it does not exist, HA generates a random nonce N_{MU_i} and p_{HA-MU_i} and then computes $U = h(p_{HA-MU_i}||N_{MU_i})$, $W_i = PW_{MU} \oplus N_{MU_i}$ and $V_i = N_{MU_i} \oplus p_{HA-MU_i}$. Then, HA delivers ID_{HA},W_i,V_i and $h(.)$ on smart cardto MU through a secure channel before storing U,PW_{MU} and p_{HA-MU_i} into its database.

2.2. Authentication and establishment of the session key phase

MU can achieve anonymous authentication via FA while roaming after registering with HA. The procedure of the authentication and establishment of the session key phase is shown as follows and illustrated in Fig. 2.

Step 1. $MU \rightarrow FA$:ID_{HA},S_1,S_2,S_3,S_4

MU inserts the smart card and inputs ID_{MU} andp_{MU}. Then, the smart card generates $N_{MU_{i+1}}$ and computes $N_{MU_i} = PW_{MU} \oplus W_i$, $p_{HA-MU_i} = N_{MU_i} \oplus V_i$, $S_1 = h(p_{HA-MU_i}||N_{MU_i})$, $S_2 = PW_{MU} \oplus N_{MU_{i+1}}$, $S_3 = h(N_{MU_{i+1}}||ID_{FA})$ and $S_4 = h(PW_{MU}||h(p_{HA-MU_i}||N_{MU_{i+1}}))$. Finally, MU stores $N_{MU_{i+1}}$ and sends ID_{HA},S_1,S_2,S_3 and S_4 to FA.

Step 2. $FA \rightarrow HA$:ID_{FA},S_1,S_2,S_3,S_4,aP

FA chooses a new random nonce a and calculates aP. Then, FA stores ID_{HA},a and aP and transmits ID_{FA},S_1,S_2,S_3,S_4 and aP to HA.

Step 3. $HA \rightarrow FA$:ID_{HA},S_6,S_7

HA extracts the corresponding PW_{MU} and p_{HA-MU_i} from its database using S_1 and computes the following steps to authenticate MU and FA.

1. Calculate $N_{MU_{i+1}} = S_2 \oplus PW_{MU}$, $S'_3 = h(N_{MU_{i+1}}||ID_{FA})$ and $S'_4 = h(PW_{MU} \oplus h(p_{HA-MU_i}||N_{MU_{i+1}}))$.
2. Check whether S'_3 equals to S_3 and S'_4 equals to S_4. If they exist, then HA authenticates MU and FA. HA computes $S_5 = h(PW_{MU}||N_{MU_{i+1}})$, $S_6 = h(ID_{FA}||ID_{HA}||S_5)$ and $S_7 = h(aP.x||S_5)$ and replaces S_1 in its database with $h(p_{HA-MU_i}||N_{MU_{i+1}})$. Otherwise, if they are not equal, HA identifies MU as an illegal user and refuses the communication request.