ITC 2/46

Journal of Information Technology and Control
Vol. 46 / No. 2 / 2017
pp. 205-218
DOI 10.5755/j01.itc.46.2.12118
© Kaunas University of Technology

Security Vulnerabilities and Improvements of SPAM: a Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks

Received 2015/09/02 | Accepted after revision 2017/04/05

crossref http://dx.doi.org/10.5755/j01.itc.46.2.12118

Security Vulnerabilities and Improvements of SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks

Mohammad Sabzinejad Farash

Faculty of Mathematical Sciences and Computer, Kharazmi University, Tehran, Iran e-mail: sabzinejad@khu.ac.ir

Shehzad Ashraf Chaudhry

Department of Computer Science & Software Engineering, International Islamic university, Islamabad, Pakistan, e-mail: shahzad@iiu.edu.pk

SK Hafizul Islam

Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan, India. e-mail: hafizul@pilani.bitspilani.ac.in

Muazzam A. Khan Khattak

Department of Computer Engineering, CE&ME National University of Science & Technology (NUST), Islamabad. Pakistan, e-mail: muazzamak@ce.ceme.edu.pk

Aiiad Albeshri

Department of Computer Science, King Abdulaziz University, Jeddah, Saudi Arabia, e-mail: aaalbeshri@kau.edu.sa

Corresponding author: sabzinejad@khu.ac.ir

The main contribution of this paper is to analyze a secure password authentication mechanism (SPAM), proposed by Chuang et al. in 2013 (IEEE Syst J.). The SPAM was used for designing a secure handover in Proxy Mobile IPv6 (PMIPv6) networks. Chuang et al. in the original paper claimed that SPAM provides high security properties and can resist various attacks. However, in this paper we point out that SPAM is vulnerable to the critical attacks, such as stolen smart card and off-line dictionary attack, replay attack and impersonation attack. In addition, we show that the identity of mobile nodes (MNs) and the session key between MNs and mobile access gateway (MAG) can be disclosed by an insider attacker; resultantly, anonymity and confidentiality between MNs and MAG will be completely broken in SPAM. In-order to counter these problems, an improved scheme is offered which also reduces the computational cost. Moreover, the scheme delivers the anonymity/untraceability and secure session key agreement. Finally, the security of the scheme is proved in the random oracle model.

KEYWORDS: Proxy Mobile IPv6, password authentication mechanism, Impersonation attack, Dictionary attack, Seamless handover.

Introduction

Wireless and mobile communication connectivity systems have recently been increasingly developed. A human-like who carry small mobile devices is able to access real-time and multimedia services, such as the Internet services, VoIP, video conferencing, and multimedia applications in much more convenient and pleasurable ways. Hence, the wireless connectivity performance is affected with the emergence of such services especially when the tendency of Mobile Node's (MN) mobility is extraordinary. The issue becomes critical when MN roams across the networks. Therefore, the Internet Engineering Task Force (IETF) developed Mobile IPv6 (MIPv6) [10] along with its optimized enhancement Fast MIPv6 (FMIPv6) [15], and Hierarchical MIPv6 (HMIPv6) [23] in order to enable an MN to maintain continuous communication service. Additionally, a host-based mobility approach is maintained by these protocols [5, 8, 9]. However, all of these suffer by numerous weaknesses, which include: signaling overhead, data loss, high power requirements, latency during handover and extensive mobility signaling functionality [1].

To counter the performance challenges of such protocols, Proxy Mobile IPv6 (PMIPv6) protocol [6] has been recently standardized by the Network-based Localized Mobility Management (NETLMM) Working-Group of the IETF as a network-based mobility management protocol.

The PMPIPv6 involves three (3) type of entities including: (i) a mobile-access gateway (MAG), (ii) a local mobility-anchor (LMA), and (iii) an authentication, authorization and accounting (AAA) server.

Although, the PMIPv6 is having better performance than MIPv6 during handover, still its latency is high than desired. Furthermore, PMIPv6 struggles against inefficient authentication, packet loss throughout the handover process [14, 18, 25] and the vulnerability to numerous threats [11].

To improve and extend PMIPv6, several research results have been proposed in recent years. Lee et al. [19] proposed an improvement for PMIPv6 to: (i) enhance the scalability and (ii) reduce signaling cost during mobility. The competent global mobility amid at PMIPv6 was introduced by Lee et al. [20]. The triangle-routing problem of PMIPv6 is astounded by Liebsch et al. [21] and Dutta et al. [4]. In IETF [26, 27, 7] also designed some handover schemes to reduce packet loss and seamless finishing. Until now, secure handover for PMIPv6 has got a very minute attention. Lee and Chung [16] proposed two secure handover schemes: (i) handover re-authentication (HORA) and (ii) handover early-authentication (HOEA). Recently, Chuang et al. [3] also proposed a secure handover for PMIPv6 using a secure password authentication mechanism (SPAM). However, these secure handover for PMIPv6 have not been analyzed for security attributes in the literature. Accordingly, the main contribution of this paper is to analyze the existing security mechanisms for handover in PMIPv6. For this reason, we briefly review Chuang et al.'s security handover for PMIPv6 and demonstrate that it does not satisfy the expected security attributes for a secure handover in PMIPv6. We then show that it is vulnerable to the critical attacks such as: (i) stolen smartcard, (ii) off-line dictionary, (iii) replay and (iv) impersonation attacks. In addition, we point out that the identity of MNs and the session key between MN and MAG can be disclosed by an insider attacker in Chuang et al.'s mechanism; resultantly, anonymity and confidentiality between MNs and MAG will be completely broken. Therefore, in spite of the claims of Chuang et al., we show that their mechanism is not suitable for achieving secure handover in PMIPv6.

The remaining parts of the paper are as follows: Section II describes the network architecture of PMIPv6. Section III reviews of Chuang et al.'s security handover for PMIPv6 in detail. In Section IV, we analyze Chuang et al.'s mechanism and demonstrate the security weaknesses of it. Section V describes the proposed improved scheme. The security analysis and comparisons are discussed in Section VI and Section VII, respectively. Finally, we present our conclusions in Section VIII.

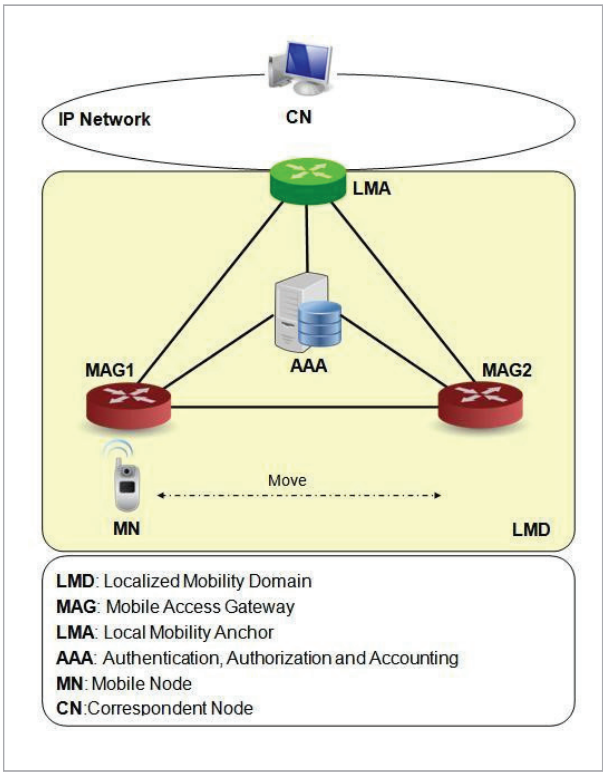
Proxy Mobile IPv6 Protocol Overview

PMIPv6 protocol provides a framework for IP mobility provision to a MN, while hiding the related signaling from MN. The involved entities within the framework track MN's mobility and builds the route state.

The LMA, MAG and AAA server are the main entities in PMIPV6 framework. The LMA is the anchor-point for MN's home network prefix(es) and maintains MN's reachability state. The MAG incorporates the link where MN is anchored and executes MN's mobility management. The MAG is liable for MN's registration with corresponding LMA. A PMIPv6 domain is having various LMAs to serve several grouping of MNs. The MN's authentication is the responsibility of AAA server, which is performed when an MN comes in some PMIPv6 domain, the MAG identifies the MN, extracts its identity and conveys it to AAA server in the domain. A scenario of PMIPv6 domain is solicited in Figure 1.

Figure 1

Network architecture for PMIPv6

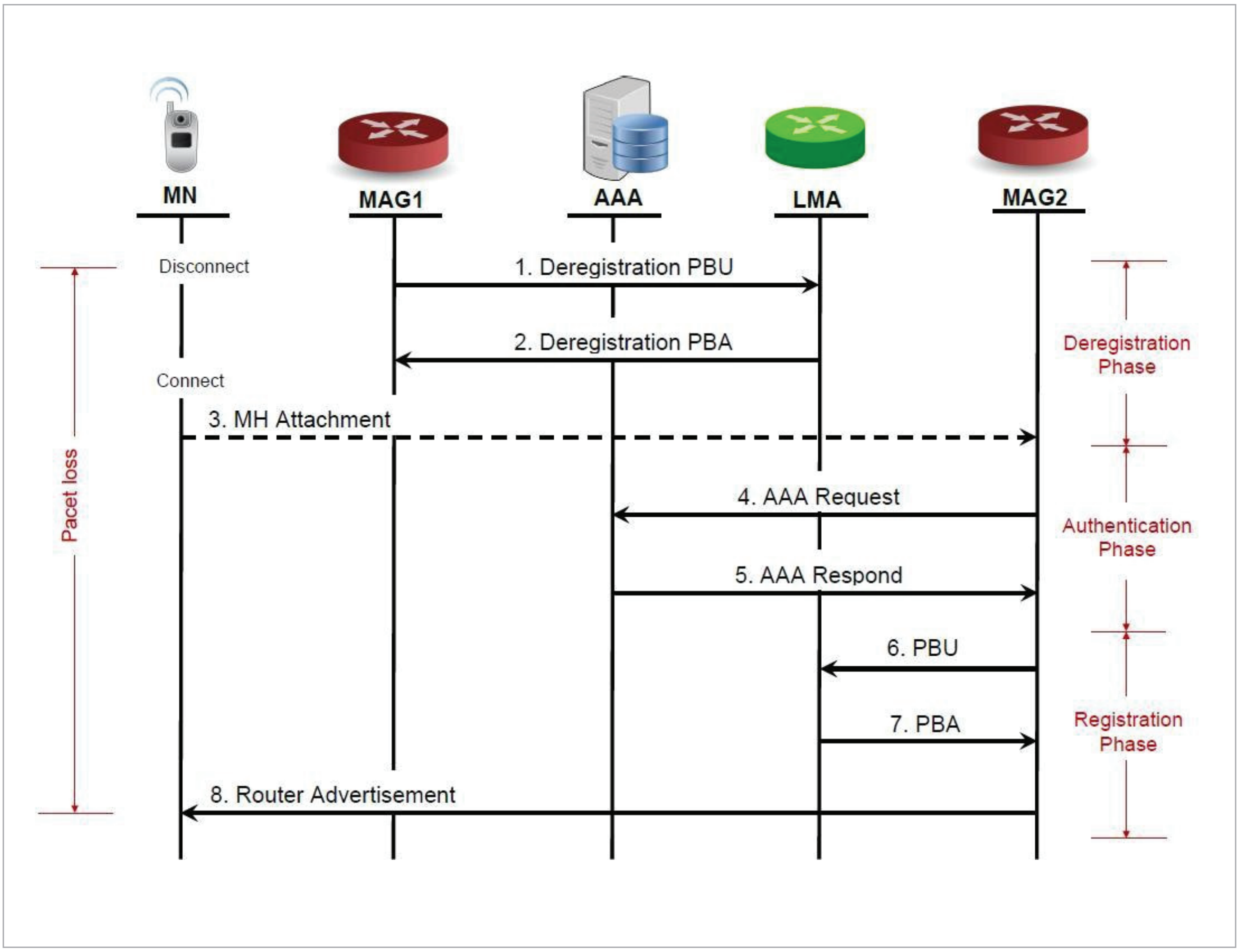

IP Network
CN
LMA
AAA
MAG1
MAG2
Move
MN
LMD
LMD: Localized Mobility Domain
MAG: Mobile Access Gateway
LMA: Local Mobility Anchor
AAA: Authentication, Authorization and Accounting
MN: Mobile Node
CN:Correspondent Node

The mobility signaling flow of PMIPv6 encompasses two situations: (i) initial attachment and (ii) handover situations. The initial attachment commences when a MN attaches to the PMIPv6 domain until it becomes able to process the data transmission [6]. The latter situation is occurred when the MN travels from the current MAG (MAG1) to a new MAG (MAG2) in the localized mobility domain (LMD), as shown in Fig. 2. The handover entails three phases: reregistration phase, authentication phase and registration phase.

- *Reregistration phase*: MAG1 sends the reregistration Proxy Binding Update (PBU) to the LMA to delete the overdue Binding Cache Entry (BCE) for the MN. Then, the LMA responds a proxy binding acknowledgment (PBA) to the previous MAG.
- *Authentication phase*: This phase activates upon attaching of a MN to a new MAG, which involves MN's identity. The new MAG requests to AAA server for MN's access authentication. The

Figure 2

Network architecture for PMIPv6



AAA sends the MN's profile to new MAG upon successful authentication.

- *Registration phase*: after the successful authentication, the new MAG requests to update MN's location by sending PBU to the LMA. When the LMA receives this PBU, it updates its MN's BCE record and sends a PBA to the new MAG. Consequently, the new MAG construct the MN's Binding Update List (BUL) entry. Then a bidirectional tunnel between the LMA and the new MAG is shaped. The MAG then sends Router Advertisement (RA) message to the MN. Upon receiving the message (RA), the MN considers himself on the home link and resumes its data session.

Review of Chuang et al.'s security handover for PMIPv6

Chuang et al. proposed an authentication scheme to provide a secure password authentication mechanism (SPAM) for protecting a valid user from attacks in PMIPv6 networks.

This paper is focused on the analysis of SPAM, whose details are given in the following subsections. Please refer to [3] for the description of the other parts of Chuang et al.'s scheme. SPAM consists of three phases: (i) initial registration phase, (ii) authentication phase, and (iii) password change phase. The notations used to analyze Chuang et al.'s scheme are declared in Table 1.

Table 1

Notations

Notation	Description
sv	AAA's secret key.
ID_{MAG}	MAG's public identity.
PW_{MN}	MN's password.
ID_{MN}	MN's public identity.
ID_{AAA}	AAA's public identity.
ID_{LMA}	LMA's public identity.
SK_{i-j}	The session key between the entities i and j, where $SK_{i-j} = SK_{j-i}$.
E_K / D_K	Symmetric encryption/decryption.
$h()$	A hash function.
N_i	A random number.
PSK	Preshared key among legal $MAGs$, LMA, and AAA.
$\oplus$	XOR.
$\|\|$	Concatenation.

A. Initial registration phase

For registration, following steps are performed among an MN and AAA server using a secure channel:

Step 1. MN sends its public identity ID_{MN} and its password PW_{MN} to AAA.

Step 2. After receiving ID_{MN} and PW_{MN}, AAA computes $c_1 = h(ID_{MN} \| sv)$, $c_2 = h(PW_{MN}) \oplus c_1$, $c_3 = E_{PSK}(ID_{AAA} \| sv)$, $c_4 = h(ID_{AAA} \| sv)$, and $c_5 = h(sv)$.

Step 3. AAA saves the parameters $\{ID_{MN}, c_1, c_2, c_3, c_4, c_5, h()\}$ in a smartcard and sends it to MN.

B. Authentication phase

This phase entails two parts, the authentication among: MN and MAG (MN-MAG), and (ii) MAG and LMA (MAG-LMA), which are depicted as follows:

1 *MN-MAG Authentication:* MN-MAG authentication is performed when a MN enters a LMD or attach to a different MAG, it performs the following steps:

Step 1. The user inserts his/her smartcard into a card reader and inputs ID_{MN} and PW_{MN}. The smartcard retrieves c_1, c_2, c_3, c_4 and c_5, checks ID_{MN}, and then verifies whether $h(PW_{MN}) \oplus c_2 = c_1$. If it holds, the MN generates the nonce N_1, computes the alias $AID_{MN} = ID_{MN} \oplus h(c_5 \| N_1)$, the authentication vector $AUTH_{MN} = h(c_1 \| N_1)$, and $E_{c_4}(AUTH_{MN} \| N_1)$.

Step 2. MN sends the authentication request $\{AID_{MN}, c_3, E_{c_4}(AUTH_{MN} \| N_1)\}$ to the MAG.

Step 3. On reception of the authentication request $\{AID_{MN}, c_3, E_{c_4}(AUTH_{MN} \| N_1)\}$, the MAG using a preshared key (PSK) decrypts c_3, and obtains ID_{AAA} and sv. The MAG further computes c_4 by hashing ID_{AAA} and sv, and decrypts $E_{c_4}(AUTH_{MN} \| N_1)$ to obtain $AUTH_{MN}$ and N_1. It computes c_5 $(h(sv))$, the identity of MN as $AID_{MN} \oplus h(c_5 \| N_1)$ and c_1 as $h(ID_{MN} \| sv)$. Finally, verifies the authentication vector $AUTH_{MN}$. If the value of $AUTH_{MN}$, calculated as $h(c_1 \| N_1)$, is equal to that of decrypting $E_{c_4}(AUTH_{MN} \| N_1)$, the MAG generates N_2, and computes $h(ID_{MAG} \| N_2)$ and a session key SK_{MN-MAG} as $h(N_1 \| N_2)$. Otherwise, the MAG rejects the authentication request.

Step 4. The MAG sends the replay message $\{ID_{MAG}, E_{c_4}(N_1 + 1 \| N_2 \| h(ID_{MAG} \| N_2))\}$ to the MN.

Step 5. Upon receiving the reply $\{ID_{MAG}, E_{c_4}(N_1 + 1 \| N_2 \| h(ID_{MAG} \| N_2))\}$, the MN uses c_4 for decryption and obtains $N_1 + 1$ and N_2. The MN then checks the validity of $N_1 + 1$ and $h(ID_{MAG} \| N_2)$. If the check is passed, the MN generates key $SK_{MN-MAG} = h(N_1 \| N_2)$ with the MAG.

Step 6. The MN sends $E_{SK_{MN-MAG}}(N_2 + 1)$ to MAG.

Step 7. The MAG using SK_{MN-MAG} decrypts the received message and checks the $N_2 + 1$ to elude the replay attack.

2 *MAG-LMA Authentication:* This type of authentication is required to evade the threats affecting MAG and LMA. The details are as below:

Step 1. The MAG generates N_3 and computes $h(N_3 \| ID_{MAG})$.

Step 2. The MAG sends the authentication message $\{ID_{MAG}, E_{PSK}(N_3 \| h(N_3 \| ID_{MAG}))\}$ to the LMA.

Step 3. Upon reception of $\{ID_{MAG}, E_{PSK}(N_3 \| h(N_3 \| ID_{MAG}))\}$, the LMA using PSK extracts N_3 and $h(N_3 \| ID_{MAG})$. The LMA computes $h(N_3 \| ID_{MAG})$ and compares it with the retrieved one. LMA rejects the request if output is not same. Contrarily, LMA generates N_4 and computes $SK_{LMA-MAG} = h(N_3 \| N_4)$.

Step 4. The LMA replies the message $\{ID_{LMA}, E_{PSK}(N_3+1\|N_4\|h(N_4 \| ID_{LMA}))\}$ to the MAG.

Step 5. After receiving the message $\{ID_{LMA}, E_{PSK}(N_3+1\|N_4\|h(N_4 \| ID_{LMA}))\}$, the MAG using PSK extracts N_3+1, and verifies $h(N_4 \| ID_{LMA})$. The MAG rejects the message if output is not same. Contrarily, the MAG computes $SK_{LMA-MAG}$ as $h(N_3 \| N_4)$.

Step 6. The MAG uses $SK_{LMA-MAG}$ to compute $E_{SK_{LMA-MAG}}(N_4+1)$ and sends it to the LMA.

Step 7. After receiving the encrypted message $E_{SK_{LMA-MAG}}(N_4+1)$, the LMA using $SK_{LMA-MAG}$ decrypts it and checks the N_4+1 to elude the replay attack.

C. Password Change phase

The password change phase is committed by MN without any intervention of AAA or MAG. The detailed steps of this phase are as follows:

Step 1. The user inserts his smartcard into a reader and feeds his ID_{MN} and PW_{MN}.

Step 2. The smartcard computes and verifies whether $h(PW_{MN}) \oplus c_2$ is same as c_1. For successful verification, the user is allowed to feed the desired password PW^*_{MN}. The smartcard then calculates $c^*_2 = c_2 \oplus h(PW_{MN}) \oplus h(PW^*_{MN})$. The smartcard replaces c_2 by c^*_2.

Security weaknesses of Chuang et al.'s scheme

Chuang et al. claimed that their scheme can resist many types of attacks and satisfy all the essential requirements for password-based authentications. However, we show that Chuang et al.'s scheme is vulnerable to the stolen smartcard and off-line dictionary attack, the user's identity and the session key disclosure, replay attack and the MAG impersonation attack. Now, we will elaborate the assumptions regarding the security of the smartcard and power of the adversary as follows [2, 24]:

1 The adversary $\mathcal{A}$ controls the communication media through which all the entities are communicating with each other i.e., $\mathcal{A}$ can listen, stop, insert, or modify any communicated messages.

2 $\mathcal{A}$ can either (i) snips user's smartcard and excerpt secret values stored by techniques described in [13, 22] or (ii) obtains a his password. However, (i) and (ii) cannot be done simultaneously.

A. Stolen smartcard and off-line dictionary attack

In the literature, many papers assumed that the smartcards are equipped with tamper resistant hardware. However, this is not the case. Since all the sensitive information stored in the memory of a smartcard can be extracted by monitoring the power consumption of the smartcard as explained in the papers [13, 22]. Therefore, we assume that all the sensitive information stored in the memory of a smartcard are known for its owner or an attacker who found or stolen it. Therefore, if the smartcard of a user MN is stolen, $\mathcal{A}$ can extract the information $\{ID_{MN}, c_1, c_2, c_3, c_4, c_5, h()\}$. Then $\mathcal{A}$ can launch off-line dictionary attack on $c_2 = h(PW_{MN}) \oplus c_1$ to know the password PW_{MN} of the user MN because $\mathcal{A}$ knows c_1. Now $\mathcal{A}$ possesses the valid smartcard of user MN, knows the identity ID_{MN}, password PW_{MN} and hence can login on to the MAG.

It can be clearly seen, the parameters $c_3 = E_{PSK}(ID_{AAA} \| sv)$, $c_4 = h(ID_{AAA} \| sv)$, and $c_5 = h(sv)$ (see 5.1) are equal for all MNs because no information about the MN is considered in these parameters. Therefore, the adversary $\mathcal{A}$ who possesses c_3, c_4, and c_5 is able to perform the following scenarios:

_ Disclosure of MNs' identities

_ Disclosure of the session key between the MN and the MAG

_ Replay attack

_ Impersonation attack

The details are as follows.

B. Disclosure of MNs' identities

In this subsection, we show that the adversary $\mathcal{A}$ who knows $c_3 = E_{PSK}(ID_{AAA} \| sv)$, $c_4 = h(ID_{AAA} \| sv)$, and $c_5 = h(sv)$ can disclose all MNs' identities.

Assume $\mathcal{A}$ eavesdropped and recorded the message $\{AID_{MN}, c_3, E_{c_4}(AUTH_{MN} \| N_1)\}$ sent from the user MN to the MAG in the authentication phase. The adversary $\mathcal{A}$ can use $c_4 = h(ID_{AAA} \| sv)$ to decrypt $E_{c_4}(AUTH_{MN} \| N_1)$, and obtains $AUTH_{MN}$ and

N_1. $\mathcal{A}$ then can retrieve the original identity ID_{MN} as $AID_{MN} \oplus h(c_5 \| N_1)$ by $c_5 = h(sv)$. Therefore, a malicious user or an adversary who corrupted a user can break the anonymity of all users and trace their transactions.

C. Disclosure of the session key between the MN and the MAG

In this subsection, we show that the adversary $\mathcal{A}$ who knows $c_3 = E_{PSK}(ID_{AAA} \| sv)$, $c_4 = h(ID_{AAA} \| sv)$, and $c_5 = h(sv)$ can disclose the session key between any user MN and the MAG.

Assume the adversary $\mathcal{A}$ eavesdropped and recorded the message $\{AID_{MN'}, c'_3, E_{c'_4}(AUTH_{MN'} \| N'_1)\}$ sent from the user MN to the MAG and the message $\{ID_{MAG}, E_{c'_4}(N'_1 + 1 || N_2 || h(ID_{MAG} \| N_2))\}$ sent from the MAG to the user MN in the authentication procedure. $\mathcal{A}$ can use $c_4 = h(ID_{AAA} \| sv)$ to decrypt $E_{c_4}(AUTH_{MN} \| N_1)$ and $E_{c_4}(N_1 + 1 || N_2 || h(ID_{MAG} \| N_2))$, and obtains N_1 and N_2. $\mathcal{A}$ then can easily compute the session key SK_{MN-MAG} as $h(N_1 \| N_2)$. Therefore, the adversary $\mathcal{A}$ can break the confidential MN-MAG communication.

D. Replay attack

In this subsection, we show that the adversary $\mathcal{A}$ who knows $c_3 = E_{PSK}(ID_{AAA} \| sv)$, $c_4 = h(ID_{AAA} \| sv)$, and $c_5 = h(sv)$ can replay the same message of the user MN to the MAG by masquerading as the user MN.

Assume the adversary $\mathcal{A}$ has intercepted a valid authentication request message $\{AID_{MN}, c_3, E_{c_4}(AUTH_{MN} \| N_1)\}$ sent from the user MN to the MAG in the public communication channel. $\mathcal{A}$ uses $c_4 = h(ID_{AAA} \| sv)$ to decrypt $E_{c_4}(AUTH_{MN} \| N_1)$ and obtains $AUTH_{MN}$ and N_1. Then $\mathcal{A}$ replays the authentication request message $\{AID_{MN}, c_3, E_{c_4}(AUTH_{MN} \| N_1)\}$ to the MAG by masquerading as the user MN at some time latter. After verification of the authentication request, the MAG sends back the replay message $\{ID_{MAG}, E_{c'_4}(N'_1 + 1 \| N_2 \| h(ID_{MAG} \| N_2))\}$ to $\mathcal{A}$ who is masquerading as the user MN. $\mathcal{A}$ uses $c_4 = h(ID_{AAA} \| sv)$ to decrypt $E_{c_4}(N_1 + 1 \| N_2 \| h(ID_{MAG} \| N_2))$ and obtains N_2. $\mathcal{A}$ then computes the session key $SK_{MN-MAG} = h(N_1 \| N_2)$ since he knows the values of N_1 and N_2. Next, $\mathcal{A}$ sends $E_{SK_{MN-MAG}}(N_2 + 1)$ to the MAG. The MAG using SK_{MN-MAG} to decrypts and verifies the $N_2 + 1$. Finally after mutual authentication, the adversary $\mathcal{A}$ masquerading as the user MN and the MAG agree on the common session key $SK_{MN-MAG} = h(N_1 \| N_2)$.

E. Impersonation attack

By this attack, the adversary $\mathcal{A}$ who knows $c_3 = E_{PSK}(ID_{AAA} \| sv)$, $c_4 = h(ID_{AAA} \| sv)$, and $c_5 = h(sv)$ can masquerade as the MAG.

Assume $\mathcal{A}$ has intercepted a valid authentication request message $\{AID_{MN}, c_3, E_{c_4}(AUTH_{MN} \| N_1)\}$ sent from the user MN to the MAG in the public communication channel. $\mathcal{A}$ can use $c_4 = h(ID_{AAA} \| sv)$ to decrypt $E_{c_4}(AUTH_{MN} \| N_1)$ and obtains $AUTH_{MN}$ and N_1. Then $\mathcal{A}$ can generate a nonce N'_2, and compute $h(ID_{MAG} \| N'_2)$ and a session key $SK_{MN-MAG} = h(N_1 \| N'_2)$. $\mathcal{A}$ then sends back the authentication replay message $\{ID_{MAG}, E_{c_4}(N_1 + 1 || N'_2 || h(ID_{MAG} \| N'_2))\}$ by masquerading as MAG to the user MN. After receiving the message $\{ID_{MAG}, E_{c_4}(N_1 + 1 || N'_2 || h(ID_{MAG} \| N_2))\}$, MN decrypts the encrypted message to obtain $N_1 + 1$ and N'_2, and verifies $N_1 + 1$ and $h(ID_{MAG} \| N'_2)$. Then MN computes the session key $SK_{MN-MAG} = h(N_1 \| N'_2)$ and sends the encrypted message $E_{SK_{MN-MAG}}(N'_2 + 1)$ to the MAG who is masquerading as $\mathcal{A}$. Then $\mathcal{A}$ decrypts the received message and checks the validity of the nonce $N'_2 + 1$. Finally after mutual authentication, the adversary $\mathcal{A}$ masquerading as the MAG and the user MN agree on the common session key $SK_{MN-MAG} = h(N_1 \| N'_2)$.

The proposed scheme

The vulnerabilities of Chaung et al.'s scheme were due to the design of the initial registration phase and the authentication between the MN and the MAG. Hence, in this section, we redesign these two phases to evade the flaws. The outline of the proposed improved scheme is also shown in Figure 3.

A. Initial registration phase

The detail of registration is as follows:

1. MN selects his identity ID_{MN}, password PW_{MN} and a large random number $c_0 \geq 2^{160}$ and then sends ID_{MN}, $h(ID_{MN} \| PW_{MN} \| c_0)$ to AAA via a secure channel.
2. For the received registration request, AAA selects a large random number c_g, then computes $c_1 = h(ID_{MN} \| PW_{MN} \| c_0) \oplus c_g$, $c_2 = h(ID_{MN} \| PW_{MN} \| c_0) \oplus h(sv \| ID_{MN}) \oplus c_g$, $c_3 = E_{PSK}(ID_{AAA} \| h(sv \| ID_{MN}))$ and $c_4 = h(h(ID_{MN} \| PW_{MN} \| c_0) \| h(sv \| ID_{MN}) \oplus c_g)$.

3 AAA saves the parameters $\{c_1, c_2, c_3, c_4, h()\}$ in a smartcard and sends it to MN using some secure channel.

4 Upon reception of the smartcard, MN inserts c_0 in it.

B. MN-MAG Authentication

Step 1. The user inserts his/her smartcard into a card reader and inputs ID_{MN} and PW_{MN}. The MN using c_0 computes $c_g = c_1 \oplus h(ID_{MN} \| PW_{MN} \| c_0)$ and $h(sv \| ID_{MN}) = c_2 \oplus c_g \oplus h(ID_{MN} \| PW_{MN} \| c_0)$. The smartcard then verifies whether $h(h(ID_{MN} \| PW_{MN} \| c_0) \| h(sv \| ID_{MN}) \| c_g) =? c_4$. If it holds, the MN generates the nonce N_1, computes $AID_{MN} = ID_{MN} \oplus h(h(sv \| ID_{MN}) \| N_1$, the authentication vector $AUTH_{MN} = h(ID_{MN} \| h(sv \| ID_{MN}) \| N_1)$, and $E_{h(sv\|ID_{MN})}(AUTH_{MN} \| N_1)$.

Step 2. MN sends the authentication request $\{AID_{MN}, c_3, E_{h(sv\|ID_{MN})}(AUTH_{MN} \| N_1)\}$ to the MAG.

Step 3. On reception of the authentication request $\{AID_{MN}, c_3, E_{h(sv\|ID_{MN})}(AUTH_{MN} \| N_1)\}$, the MAG using PKS decrypts c_3, and obtains ID_{AAA} and $h(sv \| ID_{MN})$. Next, the MAG decrypts $E_{h(sv\|ID_{MN})}(AUTH_{MN} \| N_1)$ to obtain $AUTH_{MN}$ and N_1. It computes the original identity ID_{MN} of MN as $AID_{MN} \oplus h(h(sv \| ID_{MN}) \| N_1)$. Finally, it verifies authentication vector $AUTH_{MN}$. If the value of $AUTH_{MN}$, calculated as $h(ID_{MN} \| h(sv \| ID_{MN}) \| N_1)$, is equal to that of decrypting $E_{h(sv\|ID_{MN})}(AUTH_{MN} \| N_1)$, the MAG generates a nonce N_2, and computes $h(ID_{MAG} \| N_2)$ and a session key SK_{MN-MAG} as $h(h(sv \| ID_{MN}) || N_1 || N_2)$. Otherwise, the MAG rejects the request.

Step 4. The MAG sends reply $\{ID_{MAG}, E_{h(sv\|ID_{MN})}(N_1 + 1 || N_2 || h(ID_{MAG} \| N_2))\}$ to the MN.

Step 5. After receiving the reply $\{ID_{MAG}, E_{h(sv\|ID_{MN})}(N_1 + 1 || N_2 || h(ID_{MAG} \| N_2))\}$, the MN using $h(sv \| ID_{MN})$ decrypts and obtains N_1+1 and N_2. The MN then checks the validity of N_1+1 and $h(ID_{MAG} \| N_2)$. If the check is passed, the MN using N_2 generates the key $SK_{MN-MAG} = h(h(sv \| ID_{MN}) || N_1 || N_2)$ with the MAG.

Step 6. The MN sends $E_{SK_{MN-MAG}}(N_2 + 1)$ to the MAG.

Step 7. The MAG using SK_{MN-MAG} decrypts and checks N_2+1 to elude the replay attack.

C. Password Change phase

The password change phase is committed by MN without any intervention of AAA or MAG. The detailed steps of this phase are as follows:

Step 1. The user inserts his smartcard into a reader and feeds his ID_{MN} and PW_{MN}.

Step 2. The smartcard using c_0 computes $c_g = c_1 \oplus h(ID_{MN} \| PW_{MN} \| c_0)$ and $h(sv \| ID_{MN}) = c_2 \oplus c_g \oplus h(ID_{MN} \| PW_{MN} \| c_0)$. The smartcard then verifies whether $h(h(ID_{MN} \| PW_{MN} \| c_0) \| h(sv \| ID_{MN}) \| c_g) =? c_4$. If it holds, the smartcard asks for new password. Then, the user keys the new password PW^*_{MN}, the smartcard computes $c_1^* = c_1 \oplus h(ID_{MN} \| PW_{MN}) \oplus h(ID_{MN} \| PW^*_{MN})$, $c_2 = h(ID_{MN} \| PW^*_{MN} \| c_0) \oplus h(sv \| ID_{MN}) \oplus c_g$ and $c_4 = h(h(ID_{MN} \| PW^*_{MN} \| c_0) \| h(sv \| ID_{MN}) \| c_g)$. The smartcard replaces $\{c_1, c_2, c_4, h()\}$ by $\{c_1^*, c_2^*, c_4^*, h()\}$.

Security analysis of the improved protocol

This section proves that the proposed protocol is provably secure. Starting from the formal model and assumption, the proof will proceed as follows:

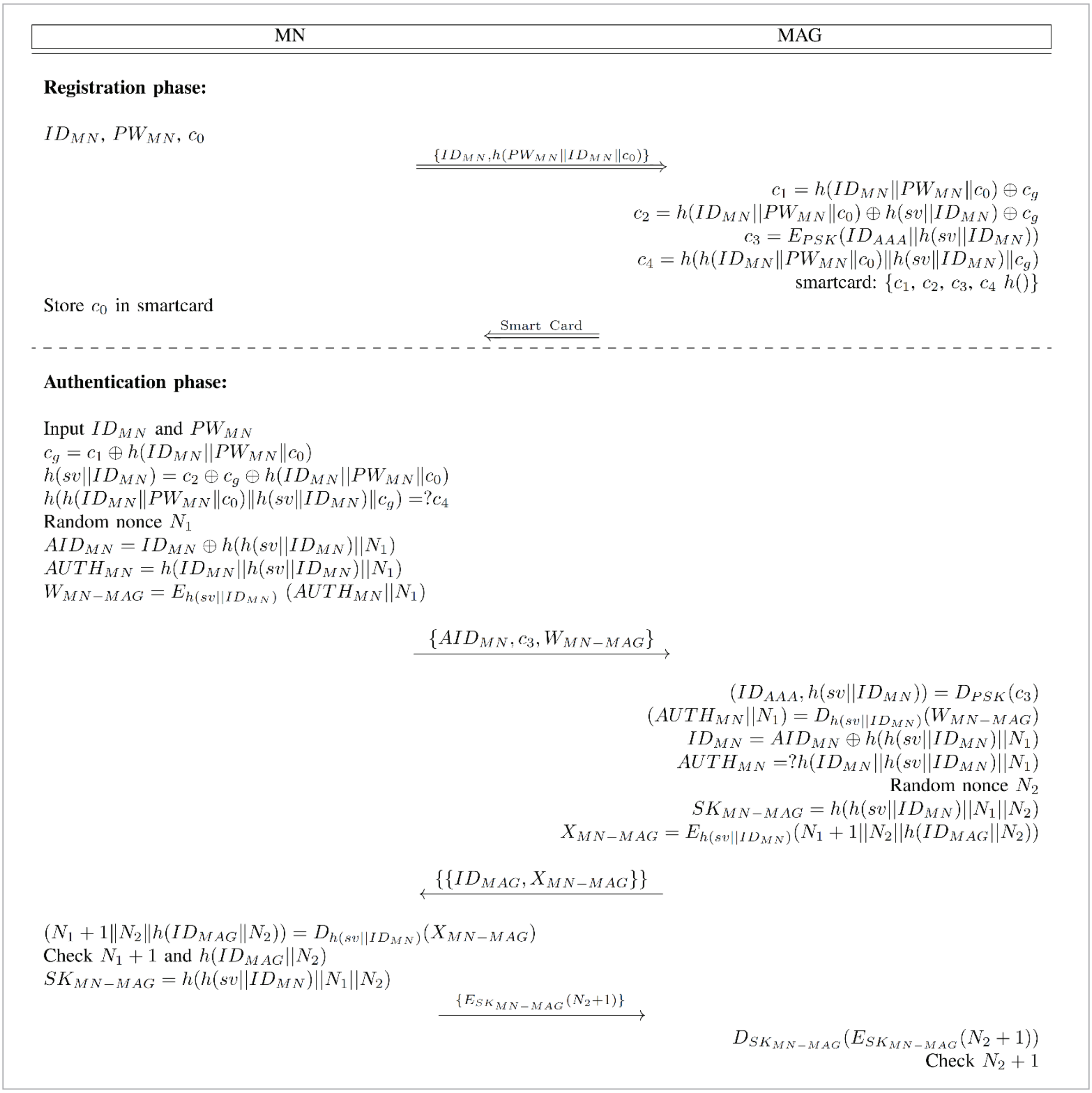
A. Security model

The provable security model is used to prove the robustness of proposed scheme.

1 Participants: The proposed protocol involves two entities: $MAG \in \mathcal{G}$ and $MN \in \mathcal{M}$. For simplicity we consider a single instance of $MAG \in \mathcal{G}$. The i-th instance of MN and MAG in a session are refereed as Π^i_{MN} and Π^i_{MAG}, respectively.
Every instance Π^i_{MN} (resp. Π^i_{MAG}) has a partner identifier pid^i_{MN} (resp:pid^j_{MAG}), a session identifier sid^i_{MN} (resp:sid^j_{MAG}), and a key sk^i_{MN} (resp:sk^j_{MAG}). pid^i_{MN} (resp:pid^j_{MAG}) contains a several identities involved in the instance. sid^i_U (resp:sid^j_S) denotes the flows that are exchanged by the instance Π^i_{MN} (resp. Π^j_{MAG}). An instance Π^i_{MN} (resp. Π^i_{MAG}) is said to be *accepted* if it holds a session key sk^i_{MN} (resp:sk^j_{MAG}), a session identifier sid^i_{MN} (resp:sid^j_{MAG}), and a partner identifier pid^i_{MN} (resp:pid^j_{MAG}).

Figure 3

The proposed improved scheme



MN | MAG

Registration phase:

ID_{MN}, PW_{MN}, c_0

$$\xrightarrow{\{ID_{MN}, h(PW_{MN}\|ID_{MN}\|c_0)\}}$$

$$c_1 = h(ID_{MN}||PW_{MN}\|c_0) \oplus c_g$$
$$c_2 = h(ID_{MN}||PW_{MN}\|c_0) \oplus h(sv||ID_{MN}) \oplus c_g$$
$$c_3 = E_{PSK}(ID_{AAA}||h(sv||ID_{MN}))$$
$$c_4 = h(h(ID_{MN}\|PW_{MN}\|c_0)\|h(sv\|ID_{MN})\|c_g)$$

smartcard: $\{c_1, c_2, c_3, c_4\ h()\}$

Store c_0 in smartcard

$$\xleftarrow{\text{Smart Card}}$$

Authentication phase:

Input ID_{MN} and PW_{MN}

$c_g = c_1 \oplus h(ID_{MN}||PW_{MN}\|c_0)$

$h(sv||ID_{MN}) = c_2 \oplus c_g \oplus h(ID_{MN}||PW_{MN}||c_0)$

$h(h(ID_{MN}\|PW_{MN}\|c_0)\|h(sv\|ID_{MN})\|c_g) =?c_4$

Random nonce N_1

$AID_{MN} = ID_{MN} \oplus h(h(sv||ID_{MN})||N_1)$

$AUTH_{MN} = h(ID_{MN}||h(sv||ID_{MN})||N_1)$

$W_{MN-MAG} = E_{h(sv||ID_{MN})}\ (AUTH_{MN}||N_1)$

$$\xrightarrow{\{AID_{MN}, c_3, W_{MN-MAG}\}}$$

$$(ID_{AAA}, h(sv||ID_{MN})) = D_{PSK}(c_3)$$
$$(AUTH_{MN}||N_1) = D_{h(sv||ID_{MN})}(W_{MN-MAG})$$
$$ID_{MN} = AID_{MN} \oplus h(h(sv||ID_{MN})||N_1)$$
$$AUTH_{MN} =?h(ID_{MN}||h(sv||ID_{MN})||N_1)$$

Random nonce N_2

$$SK_{MN-MAG} = h(h(sv||ID_{MN})||N_1||N_2)$$
$$X_{MN-MAG} = E_{h(sv||ID_{MN})}(N_1 + 1||N_2||h(ID_{MAG}||N_2))$$

$$\xleftarrow{\{\{ID_{MAG}, X_{MN-MAG}\}\}}$$

$(N_1 + 1\|N_2\|h(ID_{MAG}||N_2)) = D_{h(sv||ID_{MN})}(X_{MN-MAG})$

Check $N_1 + 1$ and $h(ID_{MAG}||N_2)$

$SK_{MN-MAG} = h(h(sv||ID_{MN})||N_1||N_2)$

$$\xrightarrow{\{E_{SK_{MN-MAG}}(N_2+1)\}}$$

$$D_{SK_{MN-MAG}}(E_{SK_{MN-MAG}}(N_2 + 1))$$

Check $N_2 + 1$

Definition 1 (Partner instances): Two instances Π^i_{MN} and Π^j_{MAG} are considered to be partnered if and only if (1) both of them have accepted, (2) $pid^i_{MN} = pid^j_{MAG}$, (3) $sid^i_{MN} = sid^j_{MAG}$, (4) $sk^i_{MN} = sk^j_{MAG}$.

2 *Adversary model:* The insecure communication link is assumed under adversary $\mathcal{A}$'s control. $\mathcal{A}$ initiates and arbitrates the session between the participants. $\mathcal{A}$ can issue following queries:

- Execute (Π^i_{MN}, Π^j_{MAG}): Execute simulates a passive attack, where $\mathcal{A}$ listens the honest communication between Π^i_{MN} and Π^i_{MAG}. The results entail the messages exchanged between Π^i_{MN} and Π^i_{MAG}.
- Reveal (Π^i_{MN}/ Π^j_{MAG}): This query is a simulation of known key attack. The session key instance Π^i_{MN}

(resp. Π^j_{MAG}) is returned against this query.

- Send (Π^i_{MN}/ Π^j_{MAG}, m). This query returns the messages Π^i_{MN} or Π^j_{MAG} generated against reception of m.
- Corrupt (MN). It outputs MN's password and the stored information in MN's smartcard.
- Test (Π^i_{MN}). When this query is invoked a coined value $c \in \{0,1\}$ is selected. The session key haunted by Π^i_{MN} is returned, if c = 0. Contrarily, this query returns a random value. This query can be called once.

Definition 2 (fresh oracle): An oracle Π^i_{MN} or Π^j_{MAG} is assumed fresh subject to following two conditions: (i) it is accepted, and (ii) its partner has not been asked the Reveal after acceptance.

3 *Protocol Security:* The protocol security is modeled a game ***Game*** **(Π, $\boldsymbol{\mathcal{A}}$)**. $\boldsymbol{\mathcal{A}}$, while interacting this game is allowed to make numerous queries (declared above) to $\boldsymbol{\Pi^i_{MN}}$ and $\boldsymbol{\Pi^j_{MAG}}$. When $\boldsymbol{\mathcal{A}}$ asks Test ($\boldsymbol{\Pi^i_{MN}}$) and it is *accepted* and *fresh*. A random coined value $\boldsymbol{c'}$ is returned. $\boldsymbol{\mathcal{A}}$ intends to guess the original value of $\boldsymbol{c'}$ in *Test* session. Th advantage carried by $\boldsymbol{\mathcal{A}}$ is given below:

$$Adv_{\Pi,Di}\left(\mathrm{A}\right)=\left|2Pr\left[c'=c\right]-1\right|. \tag{1}$$

Π is secure if $Adv_{\Pi,Di}(A)$ is negligible, where Di is the MN's password dictionary.

B. Security proof

Theorem 1: *We consider Di a dictionary of all passwords distributed uniformly. The length of the dictionary is* $|Di|$. *Let h is modeled as a random oracle model. Then,*

$$Adv_{\Pi,Di}(\mathcal{A}) \leq \frac{q_h^2+(q_s+q_e)^2}{2^l}+\frac{q_h}{2^l}+\frac{q_s}{|Di|}, \tag{2}$$

where q_s are total Send queries; q_e are total Execute queries; q_h are total hash queries to h.

Proof 1: *The following proof entails numerous games, initiated at* G_0 *(a real attack) and terminated at* G_3. *During execution of these games,* $\mathcal{A}$ *is having no advantage. Let* $Succ_i$ *be the event such that* $\mathcal{A}$ *guesses coined value c correctly in test respectively against each game* $G_i (0 \leq i \leq 3)$.

Game G$_0$. It is the real protocol, where the instances of *MN* and *MAG* are simulated as real execution. The event $Succ_0$ in *Test*-query, where $\mathcal{A}$ guesses c correctly is as follows:

$$Adv_{\Pi,Di}(A)=2|\Pr[Succ_0]-\frac{1}{2}| \tag{2}$$

Game G$_1$. It is a similar game extending G_0 to simulate h and maintains a list h_{List} having records as (*Ipt*, *Opt*). Against any query h, if a record (*Ipt*, *Opt*) is found in h_{List}, the record *Opt* is returned. Otherwise, an output $Opt \in \{0,1\}^l$ is returned and a record (*Ipt*, *Opt*) is stored in h_{List}. All the instances are simulated as actual players for Send, Test, SendServer, SendClient, Corrupt, Reveal and Execute queries. We can see that this query is perfectly indistinguishable from the real attack. Hence:

$$\Pr\left[\,Succ_1\,\right]=\Pr\left[\,Succ_0\,\right]. \tag{3}$$

Game G$_2$. This game is very similar to G_1, but G_2 is terminated if we receive some collisions of the partial transcripts N_1 and N_2, and the hash h. Conferring the birthday paradox, the maximum probability of partial collision on h is $q_h^2/2^{l+1}$. Likewise, maximum probability of collisions is $(q_s+q_e)^2/2^{l+1}$, where l is the length of h value and random numbers. Therefore:

$$\left|\Pr\left[\,Succ_2\,\right]-\Pr\left[\,Succ_1\,\right]\right|\leq\frac{q_h^2+(q_s+q_e)^2}{2^{l+1}}. \tag{4}$$

Game G$_3$. In this game, we once again change the simulation of queries to the SendClient oracle for the selected session in game G_2. This time, we change the way we compute *SK* so that it becomes independent of password and ephemeral keys. When Send (Π^i_{MN}, ID_{MAG}, $E_{h(sv||ID_{MN})}(N_1+1\,||\,N_2\,||\,h(ID_{MAG}\,||\,N_2)))$ and Send (Π^j_{MAG}, AID_{MN}, c_3, $E_{h(sv||ID_{MN})}(AUTH_{MN}||N_1)$) are asked, we set $SK_{MN-MAG}=h(h(sv\,||\,ID_{MN})\,||\,w\,||\,N_2)$, where w is selected at random. So, there are two possible cases where the adversary distinguishes game $G_2$and game G_3 as follows:

Case 1. The adversary queries $(h(sv\,||\,ID_{MN})\,||\,w\,||\,N_2)$ to h. The probability that this event occurs is $q_h/2^l$.

Case 2. The adversary asks Send query except Send (Π^i_{MN}, Π^i_{MN}, ID_{MAG}, $E_{h(sv||ID_{MN})}(N_1+1\,||\,N_2\,||\,h(ID_{MAG}\,||\,N_2)))$

and successfully impersonates *MN*. The adversary is not allowed to reveal static key PW_{MN}. Thus, in order to impersonate *MN*, $\mathcal{A}$ should acquire PW_{MN} related information, having probability $1/|Di|$. However there are q_s sessions, the occurrance probability is lower than $q_s/|Di|$.

The difference between the game G_3 and the game G_2 is as follows:

$$\left|\Pr\left[Succ_3\right]-\Pr\left[Succ_2\right]\right| \le \frac{q_h}{2^l}+\frac{q_s}{|Di|}. \tag{5}$$

On the other hand,

$$\Pr\left[Succ_3\right]=\frac{1}{2}. \tag{6}$$

Combining Eqs. (2)-(6), we get following results:

$$\begin{aligned}
&Adv_{\Pi,Di}(\mathrm{A}) = \left|2\ \Pr\left[Succ_0\right]-\frac{1}{2}\right| \\
&= 2\left|\Pr\left[Succ_0\right]-\Pr\left[Succ_3\right]\right| \\
&\le 2(|\ \Pr\left[Succ_1\right]-\Pr\left[Succ_2\right]+\Pr\left[Succ_2\right]-\Pr\left[Succ_3\right]| \\
&\le \frac{q_h^2+(q_s+q_e)^2}{2^l}+\frac{q_h}{2^l}+\frac{q_s}{|Di|}.
\end{aligned}$$

Security attributes and comparisons

A. Stolen-verifier attack

In proposed protocol no tables containing PW_{MN} for verification are stored by AAA server. The server authenticates MN by its own secret parameter *sv*. Therefore, proposed scheme is free from stolen verifier attack.

B. Man-in-middle attack

Consider the attacker $\mathcal{A}$ who intercepted the messages between *MN* and *MNG*, and replaced part or the whole message with some fake information. However, $\mathcal{A}$ cannot generate so called legal fabricated message because $\mathcal{A}$ does not know PW_{MN} and *sv*. Therefore, our scheme withstands impersonation and modification attacks.

C. Mutual authentication

In proposed scheme both MAG and MN authenticates each other without possibility of impersonation. Therefore, mutual authentication property is satisfied in proposed scheme.

D. Freely chosen password

Proposed scheme provides MN the facility to freely select and change his password anytime anywhere without intervention of server.

E. Known-key security

The peripheral keys N_1 and N_2 are freshly chosen values during each session. The session keys are independent to each other. Thus, the compromise of one or more previous session keys does not affect the next session keys.

F. User anonymity and untraceability

Any adversary $\mathcal{A}$ cannot extract the real identity of *MN*, because ID_{MN} is protected by *sv*. Furthermore, AID_{MN} is dynamic and varies session to session based on random N_1. So proposed scheme provides MN's anonymity and untraceability.

G. Resistance of smartcard loss/theft problem

We assume that $\mathcal{A}$ is able to steal a user's smartcard. Once the attacker gets a smartcard, he can derive the confidential data $\{c_1, c_2, c_3, c_3, h()\}$ stored in the smartcard by physical attack. In proposed scheme, PW_{MN} is hidden in $h(sv||ID_{MN})$ and c_g. $\mathcal{A}$ can get hold the information stored in the smartcard but he cannot check the correctness of the guessed password because he is lacking the knowledge of *sv* and ID_{MN}.

H. Performance and security comparisons

To evaluate the performance of the improved scheme, it is compared with Chuang et al. CLC13. In Table 2, the comparison is provided based on the security, while their efficiency is compared in terms of computation in Table 3. Three parameters of time complexity are adopted in this analysis and they are defined as follows:

- T_h: Hash function's running time,
- T_S: Symmetric encryption/ decryption's running time.

Table 2

Security comparison

	Chuang et al.'s scheme **[3]**	**Our** scheme
Prevent password guessing attacks	No	Yes
Prevent replay attack	No	Yes
Prevent stolen-verifier attack	Yes	Yes
Prevent stolen smartcard attack	No	Yes
Prevent impersonation attack	No	Yes
Prevent reflection attack	Yes	Yes
Resistant to modification attack	Yes	Yes
Secure session key agreement	No	Yes
Mutual authentication	No	Yes
Known-key security	Yes	Yes
Anonymity	No	Yes
Provable security	No	Yes

Table 3

Comparison of computation cost

	Chuang et al.'s scheme **[3]**	**Our** scheme
MN	$5T_h + 3t_s \approx 0.0253$ms	$7T_h + 3t_s \approx 0.0299$ms
MAG	$6T_h + 4t_s \approx 0.0322$ms	$3T_h + 4t_s \approx 0.0253$ms
Total	$11T_h + 7t_s \approx 0.0575$ms	$9T_h + 7t_s \approx 0.0552$ms

Experiment results in [12] show that the execution times of a hash function operation and a symmetric encryption/decryption operation, are 0.0023 ms and 0,0046 ms, respectively. From Table 2 and Table 3, it can be concluded that the proposed scheme provides better security and efficiency than the Chuang et al.'s scheme.

Conclusion

In this paper, we briefly reviewed Chuang et al.'s security handover for PMIPv6 and demonstrated that it does not satisfy the expected security attributes for a secure handover in PMIPv6. We then showed that it is vulnerable to the critical attacks, such as stolen smartcard and off-line dictionary attack, replay attack and impersonation attack. In addition, we pointed out that the identity of MNs and the session key between MN and MAG can be disclosed by an insider attacker in Chuang et al.'s mechanism; resultantly, anonymity and confidentiality between MNs and MAG will be completely broken. Therefore, in spite of the claims of Chuang et al., we showed that their scheme is not suitable to achieve a secure handover for PMIPv6. Moreover, an improved authentication scheme was proposed to overcome the security problems of Chuang et al.'s scheme. The security analysis showed that the improved scheme could satisfy required security attributes.

References

1. Al-Surmi, I., Othman, M., Hamid, N.-A., Ali, B.-M. Enhancing inter-PMIPv6-domain for superior handover performance across IP-based wireless domain networks. Wireless Networks, 2013, 19(6), 1317-1336. https://doi.org/10.1007/s11276-012-0535-z
2. Chen, T.-H., Hsiang, H.-C., Shih, W.-K. Security enhancement on an improvement on two remote user authentication schemes using smart cards. Future Generation Computer Systems, 2011, 27, 377-380. https://doi.org/10.1016/j.future.2010.08.007
3. Chuang, M-C., Lee, J.-F., Chen, M.-C. SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks. IEEE Systems Journal, 2013, 7(1), 102-113. https://doi.org/10.1109/JSYST.2012.2209276
4. Dutta, A., Das, S., Yokota, H., Chiba, T., Schulzrinne, H. Proxy MIP Extension for Inter-MAG Route Optimization. https://tools.ietf.org/html/draft-dutta-netlmm-pmipro-01. Accessed on June 16, 2015.
5. Farash, M. S., Attari, M. A., Kumari, S. Cryptanalysis and improvement of a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps. International Journal

of Communication Systems, 2014, 30(1). https://doi.org/10.1002/dac.2912

6. Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B. Proxy Mobile IPv6. RFC, 2008, 5213. https://doi.org/10.17487/rfc5213

7. Han, Y., Park, B. A fast handover scheme in Proxy Mobile IPv6. https://tools.ietf.org/id/draft-han-netlmm-fast-pmipv6-00.txt. Accessed on June 15, 2015.

8. Heydari, M., Sadough, S. M. S., Chaudhry, S. A., Farash, M. S., Aref, M. R. An Improved Authentication Scheme for Electronic Payment Systems in Global Mobility Networks. Information Technology and Control, 2015, 44(4), 387-403. https://doi.org/10.5755/j01.itc.44.4.9197

9. Heydari, M., Sadough, S. M. S., Chaudhry, S. A., Farash, M. S., Mahmood, K. An improved one-to-many authentication scheme based on bilinear pairings with provable security for mobile pay-TV systems. Multimedia Tools and Applications, 2016, 76(12), 14225-14245. https://doi.org/10.1007/s11042-016-3825-0

10. Johnson, D., Perkins, C., Arkko, J. Mobility Support in IPv6. IETF RFC, 2004, 3775. https://doi.org/10.17487/rfc3775

11. Kempf, J. Problem statement for network-based localized mobility management. RFC, 2007, 4830. https://doi.org/10.17487/rfc4830

12. Kilinc, H., Yanik, T. A survey of SIP authentication and key agreement schemes. IEEE Communications Surveys Tutorials, 2014, 16(2), 1005-1023. https://doi.org/10.1109/SURV.2013.091513.00050

13. Kocher, P., Jaffe, J., Jun, B. Differential power analysis. Advances in Cryptology, 1999, 388-397. https://doi.org/10.1007/3-540-48405-1_

14. Kong, K.-S., Lee, W., Han, Y.-H., Shin, M.-K., You, H. Mobility management for all-IP mobile networks: Mobile IPv6 versus proxy mobile IPv6. IEEE Wireless Communication, 2008, 15(2), 36-45. https://doi.org/10.1109/MWC.2008.4492976

15. Koodli, R (Ed.). Mobile IPv6 Fast Handovers. RFC, 2008, 5268.

16. Lee, J.-H., Chung, T.-M. Secure handover for Proxy Mobile IPv6 in next-generation communications: scenarios and performance. Wireless Communications and Mobile Computing, 2011, 11(2), 176-186. https://doi.org/10.1002/wcm.895

17. Lee, J.-H., Chung, T.-M. How much do we gain by introducing Route optimization in Proxy Mobile IPv6 networks? Annals of Telecommunications, 2010, 65(5-6), 233-246. https://doi.org/10.1007/s12243-009-0127-9

18. Lee, J.-H., Chung, T.-M., Pack S., Gundavelli, S. A fast handoff scheme in proxy mobile IPv6. In: Proceedings IEEE CECNET, 2011, 1297-1300.

19. Lee, J.-H., Chung, T.-M., Pack, S., Gundavelli, S. Shall we apply paging technologies to Proxy Mobile IPv6. In: Proceedings of ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch), 2008, 37-42. https://doi.org/10.1145/1403007.1403016

20. Lee, J.-H., Lim, H.-J., Chung, T.-M. A competent global mobility support scheme in NETLMM. International Journal of Electronics and Communications, 2009, 63(11), 950-967. https://doi.org/10.1016/j.aeue.2008.07.010

21. Liebsch, M., Le, L., Abeille, J. Route Optimization for Proxy Mobile IPv6. https://tools.ietf.org/html/draft-abeille-netlmm-proxymip6ro-01. Accessed on June 15, 2015.

22. Messerges, T. S., Dabbish, E. A., Sloan, R. H. Examining smartcard security under the threat of power analysis attacks. IEEE Transactions on Computers, 2002, 51(5), 541-552. https://doi.org/10.1109/TC.2002.1004593

23. Soliman, H., Castelluccia, C., ElMalki, K., Bellier, L. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. RFC, 2008, 5380.

24. Song, R. Advanced smart card based password authentication protocol. Computer Standards and Interfaces, 2010, 32, 321-325. https://doi.org/10.1016/j.csi.2010.03.008

25. Vogt, C., Kempf, J. Security Threats to Network-Based Localized Mobility Management (NETLMM). RFC, 2007, 4832. https://doi.org/10.17487/rfc4832

26. Xia, F., Sarikaya, B. Mobile node agnostic fast handovers for Proxy Mobile IPv6. https://tools.ietf.org/html/draft-xia-netlmm-fmip-mnagno-02. Accessed on June 16, 2015.

27. Yokota, H., Chowdhury, K., Koodli, R., Patil, B., Xia, F. Fast Handovers for PMIPv6. https://tools.ietf.org/html/rfc5949. Accessed on June 16, 2015.

Summary / Santrauka

The main contribution of this paper is to analyze a secure password authentication mechanism (SPAM), proposed by Chuang et al. in 2013 (IEEE Syst J.). The SPAM was used for designing a secure handover in Proxy Mobile IPv6 (PMIPv6) networks. Chuang et al. in the original paper claimed that SPAM provides high security properties and can resist various attacks. However, in this paper we point out that SPAM is vulnerable to the critical attacks, such as stolen smart card and off-line dictionary attack, replay attack and impersonation attack. In addition, we show that the identity of mobile nodes (MNs) and the session key between MNs and mobile access gateway (MAG) can be disclosed by an insider attacker; resultantly, anonymity and confidentiality between MNs and MAG will be completely broken in SPAM. In-order to counter these problems, an improved scheme is offered which also reduces the computational cost. Moreover, the scheme delivers the anonymity/untraceability and secure session key agreement. Finally, the security of the scheme is proved in the random oracle model.

Straipsnyje analizuotas saugaus slaptažodžių identifikavimo mechanizmas (angl. s*ecure password authentication mechanism, (SPAM)*), 2013 m. pasiūlytas autorių Chuang et al. Šis mechanizmas buvo naudojamas saugaus perdavimo Proxy Mobile IPv6 (PMIPv6) tinkluose kurti. Savo straipsnyje autoriai Chuang et al. teigia, kad mechanizmas turi aukštos apsaugos savybes ir gali priešintis įvairioms atakoms. Šiame straipsnyje parodoma, kad jis visgi neapsaugotas nuo tokių kritinių atakų: pavogtos išmaniosios kortelės ar atjungto režimo žodyno atakos, atkartojimo atakos ir apsimetimo kitu atakos. Šiame straipsnyje taip pat parodoma, kad mobilių mazgų (angl. *mobile nodes (MNs)*) tapatybė ir sesijos raktai tarp MN ir mobilaus prieigos tinklų sietuvo (angl. *mobile access gateway (MAG)*) gali būti atskleisti atakuotojo tinklo viduje. Dėl šios priežasties anonimiškumas ir konfidencialumas tarp MN ir MAG būtų visiškai palaužtas SPAM sistemoje. Kad būtų galima spręsti šias problemas, straipsnyje siūloma patobulinta schema, kuri taip pat sumažina ir skaičiavimo kainą. Be to, schema užtikrina anonimiškumą (neatsekamumą) ir saugų sesijos raktų sutarimą. Schemos saugumas įrodytas atsitiktiniame orakulo modelyje.