PLOS ONE

RESEARCH ARTICLE

Cryptanalysis and Improvement of "A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks"

Mojtaba Alizadeh[1,3]*, Mazdak Zamani[2], Sabariah Baharun[3], Azizah Abdul Manaf[4], Kouichi Sakurai[1], Hiroki Anada[5], Hassan Keshavarz[3], Shehzad Ashraf Chaudhry[6], Muhammad Khurram Khan[7]

1 Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka, Japan, **2** Department of Computer Science, Kean University, Union, New Jersey, United States of America, **3** Malaysia-Japan International Institute of Technology, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia, **4** Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia, **5** Institute of Systems, Information Technologies and Nanotechnologies (ISIT), Fukuoka, Japan, **6** Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan, **7** Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia

* malizadeh@ieee.org

OPEN ACCESS

Citation: Alizadeh M, Zamani M, Baharun S, Abdul Manaf A, Sakurai K, Anada H, et al. (2015) Cryptanalysis and Improvement of "A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks" PLoS ONE 10(11): e0142716. doi:10.1371/journal.pone.0142716

Editor: Kim-Kwang Raymond Choo, University of South Australia, AUSTRALIA

Received: August 16, 2015

Accepted: October 26, 2015

Published: November 18, 2015

Data Availability Statement: All relevant data are within the paper.

Funding: This work was supported by Malaysia-Japan International Institute of Technology (MJIIT) center at Universiti Teknologi Malaysia, Japan Student Services Organization (JASSO), and Sakurai Lab, Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka Japan. Muhammad Khurram Khan extends his sincere appreciations to the Deanship of Scientific Research at King Saud University for its funding for the Prolific Research

Abstract

Proxy Mobile IPv6 is a network-based localized mobility management protocol that supports mobility without mobile nodes' participation in mobility signaling. The details of user authentication procedure are not specified in this standard, hence, many authentication schemes have been proposed for this standard. In 2013, Chuang et al., proposed an authentication method for PMIPv6, called SPAM. However, Chuang et al.'s Scheme protects the network against some security attacks, but it is still vulnerable to impersonation and password guessing attacks. In addition, we discuss other security drawbacks such as lack of revocation procedure in case of loss or stolen device, and anonymity issues of the Chuang et al.'s scheme. We further propose an enhanced authentication method to mitigate the security issues of SPAM method and evaluate our scheme using BAN logic.

Introduction

Mobile devices have been experiencing rapid growth as people utilize these devices to access different types of services, including the Internet browsing, file sharing, video conferencing, and multimedia applications, anytime and anywhere [1]. This growth does not appear to halt any time soon even though mobile devices are faced with different challenges in using wireless technologies such as computation limitation, wireless communication bandwidth inadequacy, and security problems. The Mobile IPv6 (MIPv6) [2] is a standard of the Internet Engineering Task Force (IETF), that facilitates the roaming of the mobile nodes in the IPv6 network. This

Group (PRG-1436-16). Authors acknowledge support from Malaysia-Japan International Institute of Technology (MJIIT) center at Universiti Teknologi Malaysia, Japan Student Services Organization (JASSO), and Kyushu University, Fukuoka Japan.

Competing Interests: The authors have declared that no competing interests exist.

standardized protocol allows the mobile devices to roam inside the network by providing seamless connection to the network.

The nodes mobility must be transparent to the layers above the IP layer; the continuous connection can be seamless, and it may do not require any manual configurations. If the node has to connect to a different network connection during physical movement that utilizes a variant of the subnet prefix, then a mobile node (MN) is required to get a new IP address. If this does not take place, then the MN cannot be reached. In order for this seamless movement to take place, the Mobile IPv6 nodes utilize two addresses namely the Care-Of-Address (CoA) and the Home Address (HoA). The HoA is a permanent and static address, which can be utilized to connect to the MN despite the present location of the node, but the CoA is a dynamic and robust address, which changes according to the present location of the node. In order for the MN to be reached despite its location, the Mobile IPv6 establishes the HA (Home Agent) which functions as a proxy that is stationary [3].

The mobile IPv6 protocols are facing are several problems such as delay, packet loss, and signaling costs. Therefore, various mobility management protocols are suggested to increase the performance of the MIPv6, including, host-based such as the Hierarchical Mobile IPv6 (HMIPv6) [4], Fast Handover for Mobile IPv6 (FMIPv6) [5], and network-based such as the Proxy Mobile IPv6 (PMIPv6) [6]. Among these protocols, Proxy Mobile IPv6 (PMIPv6) gains fewer handover latency and signaling cost [7]. Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol, which offers mobility services for mobile nodes without the involvement of the mobile nodes in signaling communications. This particular protocol is being utilized as a variant of the wireless networks, including the 3GPP2, WiMAX, and the LAN networks as they need a low mobility signaling over the wireless links [8].

The Local Mobility Anchor (LMA), and the Mobile Access Gateway (MAG) are the main mobility entities in the PMIPv6 domain that provide seamless connectivity for the MN. The MAG typically runs on the access router, and manages mobility signaling instead of the MN. Subsequently, the MN in the PMIPv6 does not require any protocol stack modification in order to support the PMIPv6. The MAG and LMA manage the traffic transmitted to and from the MN using a bi-directional tunnel. Based on the MN view, the entire PMIPv6 domain appears as its home network [7].

Researchers have suggested various schemes of authentication for the PMIPv6 standard ever since it was first established in 2008, because the authentication procedure's details are not specified in the RFC 5213 standard document. Chuang et al., [9] in 2013, suggested the authentication approach known as the SPAM. Nevertheless, the SPAM offers low packet loss and latency rates in comparison to many other schemes; however, it is prone to security threats such as impersonation and password guessing attacks. This study reveals that an attacker can act as a legitimate entity and attack when the mobile device is stolen or lost. In addition, this study demonstrates some present drawbacks in the scheme, including the lack of the revocation process and user anonymity problems. Moreover, the proposed improvement is suggested to make the SPAM secure against the security flaws mentioned above. Finally, the security and privacy of the proposed method is verified and discussed by utilizing the offered security theories and BAN logic, then authentication cost of the proposed method is compared with SPMA scheme.

The rest of this paper is organized in the following manner. The SPAM scheme is reviewed in Section 2. The cryptanalysis of the SPAM approach is established in Section 3. Section 4 provides our proposed solution. In Section 5, we assess the proposed approach by utilizing the security verification theorems. Finally, authentication cost of the proposed method is analyzed and compared to the SPAM scheme.

Table 1. Notations used in SPAM scheme.

Symbol	Description
sv	The AAA and LMA secret key
ID_{MN}	MN identification
ID_{AAA}	AAA identification
ID_{MAG}	MAG identification
PW_{MN}	Password of MN
SK_{i-j}	Session key between entity (i) and entity, (j)
$E_{SK_{i-j}}(M)$	Message M is encrypted using key SKi-j
$E_K(M)$	Message M is encrypted using key K
N_i	Nonce number i
$h()$	One-way hash function
PSK	The symmetric key among the MAGs, the LMAs, and the AAA
$\|\|$	Concatenation
$\oplus$	XOR operation

doi:10.1371/journal.pone.0142716.t001

Review of the SPAM Scheme

The SPAM includes three stages known as the initial registration, mutual authentication process for both the MAG and the MN, and the password changing process. The authentication credentials are stored in smart card under the assumption of using tamper-proof smart card. Table 1 describes the notations utilized in the SPAM scheme.

Initial Registration

The mobile node receives certain credentials for further authentication during the initial registration with the authentication server, AAA. It is assumed that the communication channel between the MN and the AAA server is secure. The initial registration steps are as follows:

1. $MN \rightarrow AAA$: The MN sends its ID and Password to the AAA server using secure channel.
2. The AAA server checks the ID and password on the MN and then computes the required values as follows. $c_1 = h(ID_{MN} \| sv)$, $c_2 = h(PW_{MN}) \oplus c_1$, $c_3 = E_{PSK}(ID_{AAA} \| sv)$, $c_4 = h(ID_{AAA} \| sv)$, $c_5 = h(sv)$
3. $AAA \rightarrow MN$: The AAA stores c_1, c_2, c_3, c_4, c_5, $h()$, ID_{MN} in the smart card and sends it to the MN.

The initial procedure is described in Fig 1.

Mutual Authentication between the MN and the MAG

There are two main sections in this mutual authentication; firstly, the MN's authenticity is checked by the MAG prior to knowing its real ID, and secondly; the MN checks the MAG authentication. The mutual authentication between the MN, and the MAG is described in the following:

1. The user inserts a smart card and enters its ID and password. The smart card verifies whether the equation, $h(PW_{MN}) \oplus c_2 = c_1$, to check mobile user authentication. Then, it generates N and compute $AID_{MN} = ID_{MN} \oplus h(c_5 \| N_1)$ and $AUTH_{MN} = h(c_1 \| N_1)$.

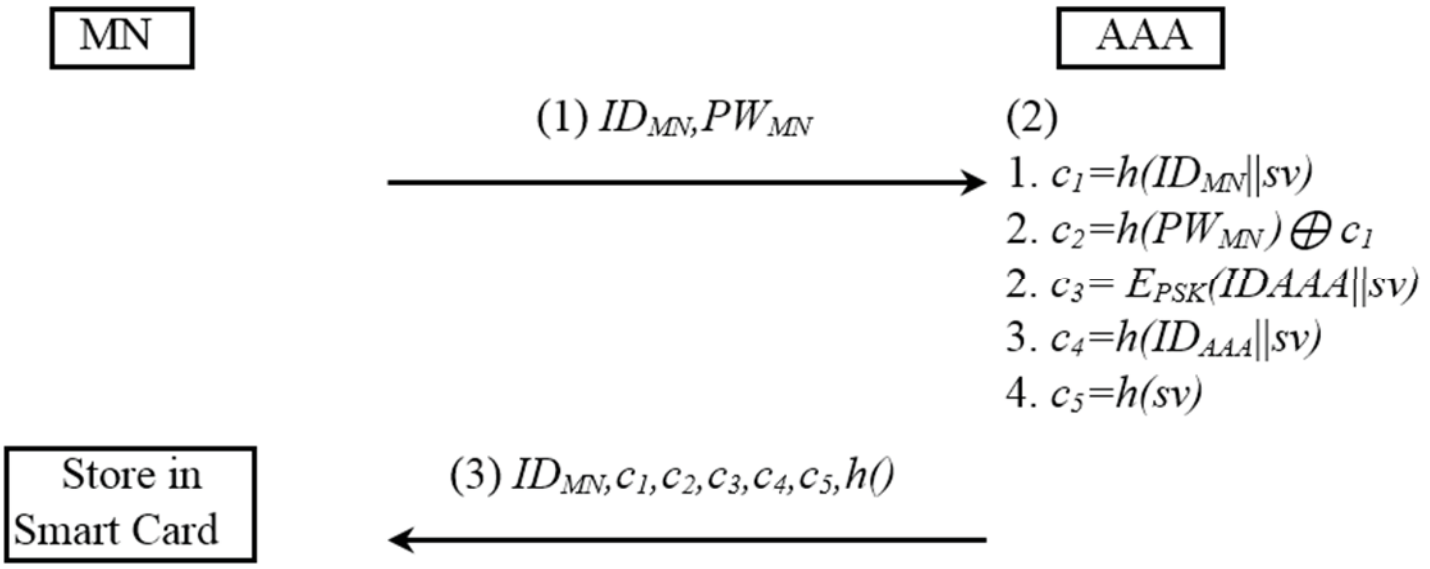

Fig 1. Initial registration procedure of SPAM method.

doi:10.1371/journal.pone.0142716.g001

2. $MN \rightarrow MAG$: The authentication request, AID_{MN}, c_3, $E_{c_4}(AUTH_{MN} \| N_1)$, is generated by the MN and sent to the MAG.
3. The MN verification by the MAG: After receiving authentication request, the MAG decrypts c_3 to obtain ID_{AAA} and sv using PSK, which is a pre-shared symmetric key. Then, the $AUTH_{MN}$ and N_1 are retrieved by decrypting $E_{c_4}(AUTH_{MN} \| N_1)$ using c_3. To obtain the ID_{MN}, the MAG computes c5 and gets $ID_{MN} = AID_{MN} \oplus h(c_5 \| N_1)$. After computing $c_1 = h(ID_{MN} \| sv)$, the MAG can verify the MAG authentication by checking the value of $AUTH_{MN} = h(c_1 \| N_1)$ to the value of $AUTH_{MN}$ obtained from $E_{c_4}(AUTH_{MN} \| N_1)$. If both $AUTH_{MN}$ value are the same, the MN is authenticated and the MAG generates N_2, $SK_{MN-MAG} = h(c_1 \| N_1)$ that is a session key between the MAG and the MN, and $h(ID_{MAG} \| N_2)$.
4. $MAG \rightarrow MN$: The MAG reply ID_{MAG}, $E_{c_4}((N_1 + 1)\|N_2 \| h(N_2 \| ID_{MAG}))$ back to the MN.
5. The MAG verification: The MN decrypts the $E_{c_4}((N_1 + 1)\|N_2 \| h(N_2 \| ID_{MAG}))$ and obtains $(N_1 + 1)$ and N_2. Then, it checks the value of $h(N_2 \| ID_{MAG})$ and $(N_1 + 1)$ for the MAG authentication. After verifying the MAG authenticity, the MN generates a session key, $SK_{MN-MAG} = h(N_1 \| N_2)$.
6. $MN \rightarrow MAG$: The MAG computes $E_{SK_{MN-MAG}}(N_2 + 1)$, and sends it to the MAG.
7. The MAG decrypts the encrypted message using the session key and checks $(N_2 + 1)$ to prevent replay attack.

Fig 2 shows the communication between the MN and the MAG.

After mutual authentication between the MN and the MAG, the mutual authentication between the MAG and the LMA is processed in the SPAM method. The details of this authentication procedure are as follows.

1. The MAG generates N_3 to compute $h(N_3 \| ID_{MAG})$.
2. $MAG \rightarrow LMA$: The authentication message, ID_{MAG}, $E_{PSK}(N_3 \| h(N_3 \| IDMAG)$ to the LMA.

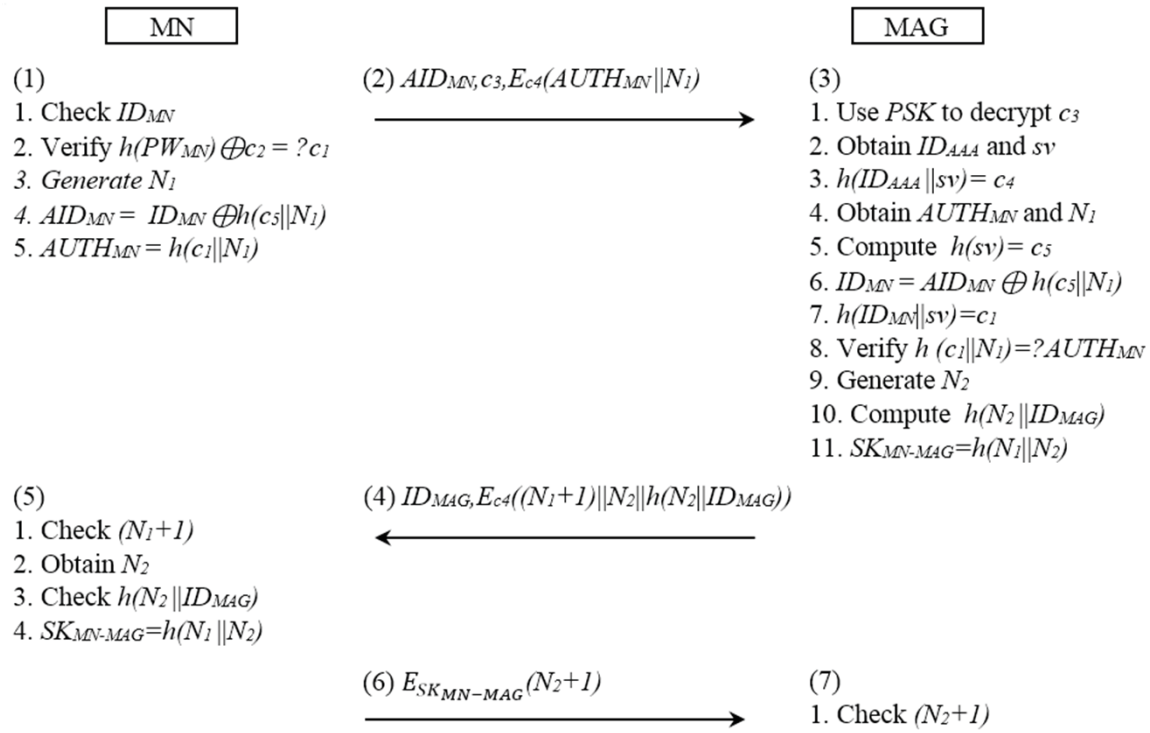

Fig 2. The SPAM authentication procedure between the MN and the MAG.

doi:10.1371/journal.pone.0142716.g002

3. The LMA decrypts the received message from the MAG using PSK and retrieves $h(N_3 \| ID_{MAG})$ and N_3. The LMA computes $h(N_3 \| ID_{MAG})$ and compares to the received $h(N\,3 \| IDMAG)$ and N_3. Then, it computes $h(N_3 \| ID_{MAG})$ and compares to the received $h(N_3 \| ID_{MAG})$ to check the MAG authenticity. Finally, it generates N_4 and computes the session key, $SK_{LMA-MAG} = h(N_3 \| N_4)$, if the MAG is authentic, otherwise, it drops the message.
4. *LMA* → *MAG*: The MAG replies ID_{MAG}, $E_{PSK}((N_3 + 1)\|N_4 \| h(ID_{LMA} \| N_4))$ back to the MAG.
5. *The LMA verification:* The MAG decrypts $E_{PSK}((N_3 + 1)\|N_4 \| h(ID_{LMA} \| N_4))$ and obtains $(N_3 + 1)$ and N_4. Then, it checks the value of $h(N_4 \| ID_{LMA})$ and $(N_1 + 1)$ for the MAG authentication. After verifying the MAG authenticity, the MAG generates a session key, $SK_{LMA-MAG} = h(N_3 \| N_4)$.
6. *MAG* → *LMA*: The MAG computes $E_{SK_{LMA-MAG}}(N_4 + 1)$, and sends it to the LMA.
7. The LMA decrypts the encrypted message using the session key and checks $(N_4 + 1)$ to prevent the replay attack.

The message exchange flow chart of mutual authentication between the LMA and the MAG is illustrated in Fig 3.

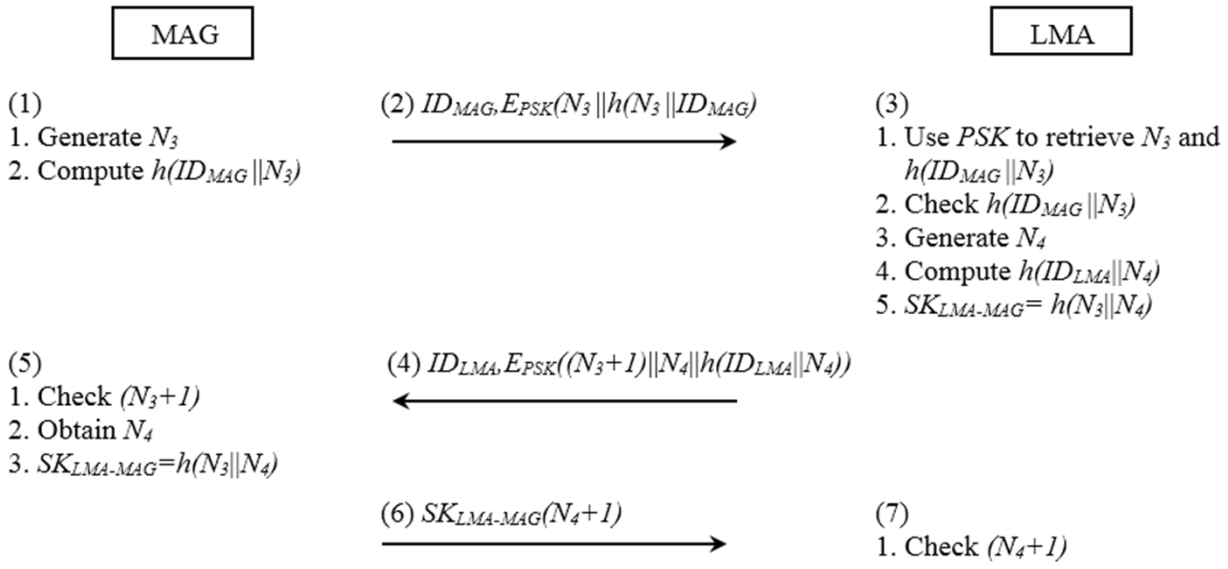

Fig 3. The authentication procedure between the MAG and the LMA.

doi:10.1371/journal.pone.0142716.g003

SPAM Password Change Phase

The SPAM scheme provides the password change process. Mobile users are able to change their passwords without contacting other entities like the AAA server and the MAG. The procedure is described as follows:

1. The user inserts the smart card and enters his ID and password.
2. The smart card verifies user ID by checking $h(PW_{MN}) \oplus c_2 = c_1$. If the equation is correct, then lets user to enter new password, PW^*_{MN}. After receiving the new password, the smart card computes $c^*_2 = c_2 \oplus h(PW_{MN}) \oplus h(PW^*_{MN})$ and replaces c_2 by c^*_2.

   The password change flow chart is described in Fig 4.

Security Issues of the SPAM Method

This section discusses the security strengths of the authentication methods in the PMIPv6 using the assumption that smart cards are not exactly free from tampering. The suitable authentication method should fulfill some security and privacy criteria such as anonymity, mutual authentication, session key secrecy, and user unlinkability [10–15]. Furthermore, authentication schemes should secure enough against some security attacks such as session hijacking, denial of service, impersonation, replay, password guessing, man-in-the-middle, stolen-verifier, and eavesdropping attacks [16–24]. Therefore, we discuss the security and privacy of the SPAM method under the assumption that smart cards are not exactly free from tampering. In addition, the potential for utilizing smart cards in PMIPv6 that are tamper resistant are explained according to these researchers [25–31] by offering several examples. After that, the SPAM method's security issues are discussed using certain evidences.

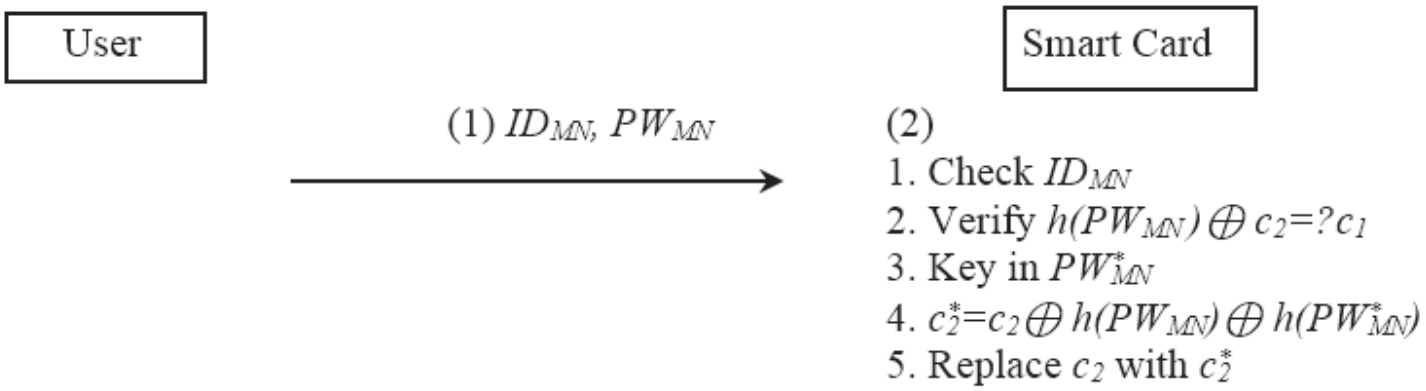

Fig 4. SPAM password change procedure.

doi:10.1371/journal.pone.0142716.g004

The conventional remote authentication using passwords [32, 33] utilizes a password table, which is stored in an authentication server. This kind of approach is susceptible to attacks on password, including password dictionary attacks, offline guessing attack, tampering of the password table, and corruption attacks. This also gives rise to an increase overhead for protecting and maintaining the password table. Therefore, many smart card based password authentication schemes that do not require a password table have been proposed [34–43] to improve security of the authentication protocols. However, these schemes remain vulnerable to sophisticated attacks that use offline password dictionary searches, observation of power consumption, or physically exposition of the chip to extract the data it stores [44].

Khan et al. [26] and Rhee et al. [29] claim that mobile devices, including smart phones, PDAs, and notebooks are not free from tampering and users' data inside the mobile devices are susceptible to different forms of security attacks [31]. Various methods have been suggested to crack the security of smart cards in the past few years. For instance, Kocher et al. [45] proposed the potential of retrieving the smart card's secret key by observing the smart card's power consumption. The vulnerability of the smart card is observed through its power analysis attack [46]. Another form of the threat against the smart cards is the fault-based cryptanalysis, as demonstrated by Bellcore's press release [47]. This attack occurs when an attacker initiates a particular form of fault into the mobile device and later retrieves the secrets embedded within according to the incorrect responses received from the mobile devices. Therefore, given the assumption of utilizing a non-tamper-proof smart card, many of the authentication methods in the PMIPv6 are susceptible to different forms of attacks like the impersonation attack; thus, making it is crucial to offer an appropriate method of authentication according to the assumption of the non-tamper-proof smart card.

This paper assumes that the attacker could have complete control of the channel of communication between the MAG and the MN, and he/she would be able to change, insert, and tap into any messages of communication. In the following sections, the security and privacy issues of the SPAM method are discussed.

The MN Impersonation Attack

Mobile devices such as smartphones, PDAs, and Tablets are vulnerable to threats such as stolen or loss. In addition, most of the authentication mechanisms use smart card to store critical

information such as secret keys, passwords, and encryption functions. Therefore, if an attacker access to smart card inside mobile devices and steal the keys, even if he leaves the mobile device intact, he can impersonate legitimate user or access point [26, 48](Khan and Kumari, 2014; Wei-Chi and Chang, 2005). In SPAM method, the information are stored in smart card, hence impersonation attack can be launched. The smart card in the SPAM method contains (ID_{MN}, C_1, C_2, C_3, C_4, C_5, $h()$), if an attacker accesses to this smart card secrets, and sniffs the first message, (AID_{MN}, c_3, $E_{C_4}(AUTH_{MN} \parallel N_1)$) between the MN and the MAG in login phase, he can impersonate the MN as follows:

1. First, an attacker generates his own nonce, N_1^*, then computes $AID_{MN} = ID_{MN} \oplus h(C_5 \parallel N_1^*)$, and $AUTH_{MN} = h(C_1 \parallel N_1^*$ using retrieved secrets from smart card an login request message, ID_{MN}, C_1, and C_5.
2. An attacker generates authentication request, $AID_{MN}, C_3, E_{C_4}(AUTH_{MN} \parallel N_1^*)$, and sends it to the MAG.
3. The MAG decrypts C_3 using *PSK* and obtains ID_{AAA} and *sv*. Then, calculates $C_4 = h(ID_{AAA} \parallel sv)$ to decrypts $Ec4(AUTH_A||N*1)$ to obtain the value of $AUTH_A$ and N_1*. The MAG computes $ID_{MN} = AID_A \oplus h(C_5 \parallel N_1^*)$ and $h(ID_{MN} \parallel sv) = C_1$. Finally, for checking MN authentication, the MAG compares the value of the $AUTH_{MN} = h(C_1 \parallel N_1^*)$ to the value of $AUTH_{MN}$ obtained from $Ec4(AUTH_{MN} \parallel N_1^*)$. It is clear that the value, $AUTH_{MN}$, which is retrieved from $(AUTH_{MN} \parallel N_1^*)$, is equal to the value, $AUTH_{MN}$, retrieved from $AUTH_{MN} = h(C_1 \parallel N_1^*)$, because $AUTH_{MN}$, is generated using the values, C_1, C_2, and N_1^*, which can be captured or generated by an attacker. This means an attacker is authenticated to the MAG successfully.

The MAG Impersonation Attack

Similar to the MN impersonation attack, we assume that an attacker retrieved the smart cart secrets, (ID_{MN}, C_1, C_2, C_3, C_4, C_5, $h()$), and sniffed the login request, (AID_{MN}, c_3, $E_{C_4}(AUTH_{MN} \parallel N_1)$). An attacker can impersonate the MAG as follows:

1. An attacker decrypts $E_{C_4}(AUTH_{MN} \parallel N_1)$ to get N_1, then generate N_2^*, and selects a fake ID_{MAG}^*. Finally, computes $(E_{C_4}((N_1 + 1) \parallel N_2^* \parallel h(N_2^* \parallel ID_{MAG}^*), ID_{MAG}^*)$ and sends it back to the MN.
2. The MN decrypts $E_{C_4}((N_1 + 1) \parallel N_2^* \parallel h(N_2^* \parallel ID_{MAG}^*)$ to obtain $(N_1 + 1)$ and (N_2^*). Then, it checks the value, $h(ID_{MAG}^* \parallel (N_2^*))$, and $(N_1 + 1)$ for the MAG authentication. As the value, N_1 is the original nonce issued by the MN, then, the MN verifies $(N_1 + 1)$, which means an attacker is authenticated to the MN. When an attacker is verified, the MN completes the rest of authentication.

Anonymity

The SPAM method does not preserve the MN anonymity. An attacker can easily find the ID_{MN} using the intercepted login request and smart card secrets. Firstly, an attacker extracts $E_{C_4}(AUTH_{MN} \parallel N_1)$ in the login request message, (AID_{MN}, C_3, $E_{C_4}(AUTH_{MN} \parallel N_1)$), and decrypts it using C_4 to get N_1. After obtaining N_1, the ID_{MN} can be retrieved by computing, $ID_{MN} = AID_{MN} \oplus h(C_5 \parallel N_1)$, because an attacker received (AID_{MN}) from login request, and (C_5) from smart card. Secondly, ID_{MAG} can be retrieved from the message, (ID_{MAG}, $E_{C_4}((N_1 + 1)||N_2 \parallel h(ID_{MAG} \parallel N_2))$), as this message is sent by the MAG to the MN in a plain

text, during the mutual authentication phase. Clearly, the anonymity of user is not protected because an attacker can find the ID of network entity.

Lack of Revocation of Smart Card

The revocation procedure is used in case of the MN misbehavior or lost mobile device. The user can report the loss of the mobile device to the AAA server to prevent the further security problems like impersonation attack [30] in case of the lost or stolen mobile device. The revocation procedure is not provided for the SPAM method.

Password Guessing Attack

In this section, we show that how an attacker can retrieve the MN password using intercepted login message based on the reference [49, 50]. An attacker can get the value, (AID_{MN}, C_3, $E_{C_4}(AUTH_{MN} \| N_1)$) and the stored information inside the smart card, (ID_{MN}, C_1, C_2, C_3, C_4, C_5, $h()$). From the equation, $C_2 = h(PW_{MN}) \oplus C_1$, as an attacker knows C_1 and C_2, he can compute $h(PW_{MN}) = C_1 \oplus C_2$. Now, he can guess a password PW^*_{MN} and compute $h(PW^*_{MN})$, then check if $h(PW^*_{MN}) = h(PW_{MN})$, if so, then an attacker possesses PW_{MN}.

Proposed Method

In the section, our proposed enhancement is described. First, we change registration phase in the way that if even an attacker finds the secrets inside the smart card, he cannot launch impersonation attack. Subsequently, mutual authentication procedure between the MN and the MAG is proposed. The main is idea is that smart card needs user name and password of the MN to calculate other secrets and initiate authentication.

Initial Registration Procedure

In this phase, the AAA server generates the secrets for the MN. The main objective of the improvement is to prevent revealing smart card information in the case of a stolen or loss device. All the stored information in smart card should be useless for an attacker. We introduce an extra value, R_{MN}, in this step. Fig 5 depicts the initial registration procedure.

Authentication Procedure

The MN should perform mutual authentication with the MAG when it joins to the localized mobility domain. We assume that an attacker can retrieve the secrets inside the smart card if the case of the stolen or lost mobile device. The main idea of our approach is not to store critical secrets inside the smart card. The mobile user enters his ID and password to the smart card to start the authentication procedure. The proposed authentication procedure is as follows:

1. The user inserts a smart card and enters its ID and password. First, it computes $S_1 = h(ID_{MN} \| PW_{MN}) \oplus S_4$. The smart card checks if, $h(PW_{MN}) \oplus S_2 = S_1$, then generates N_1 and computes $S_3 = S_6 \oplus S_1$, $AID_{MN} = S_1 \oplus S_6$, and $AUTH_{MN} = h(S_1 \| N_1)$.
2. $MN \rightarrow MAG$: The authentication request is formatted as AID_{MN}, $E_{S_1}(AUTH_{MN} \| N_1)$ and sent to the MAG by the MN.
3. The MN verification by the MAG: After receiving the authentication request, the MAG decrypts $AID = S_1 \oplus S_6 = E_{PSK}(ID_{MN} \| sv \| aMN)$ to obtain ID_{MN}, aMN and sv using PSK, which is a pre-shared symmetric key between the MAG and AAA. Then, it computes $S_1 = h(ID_{MN} \| sv)$ to decrypt $E_{S_1}(AUTHM_{NM} \| N_1)$ and retrieve $AUTH_{MN}$ and N_1. To obtain the ID_{MN}, the MAG computes C_5 and gets $ID_{MN} = AID_{MN} \oplus h(C_5 \| N_1)$. After computing $S_1 =$

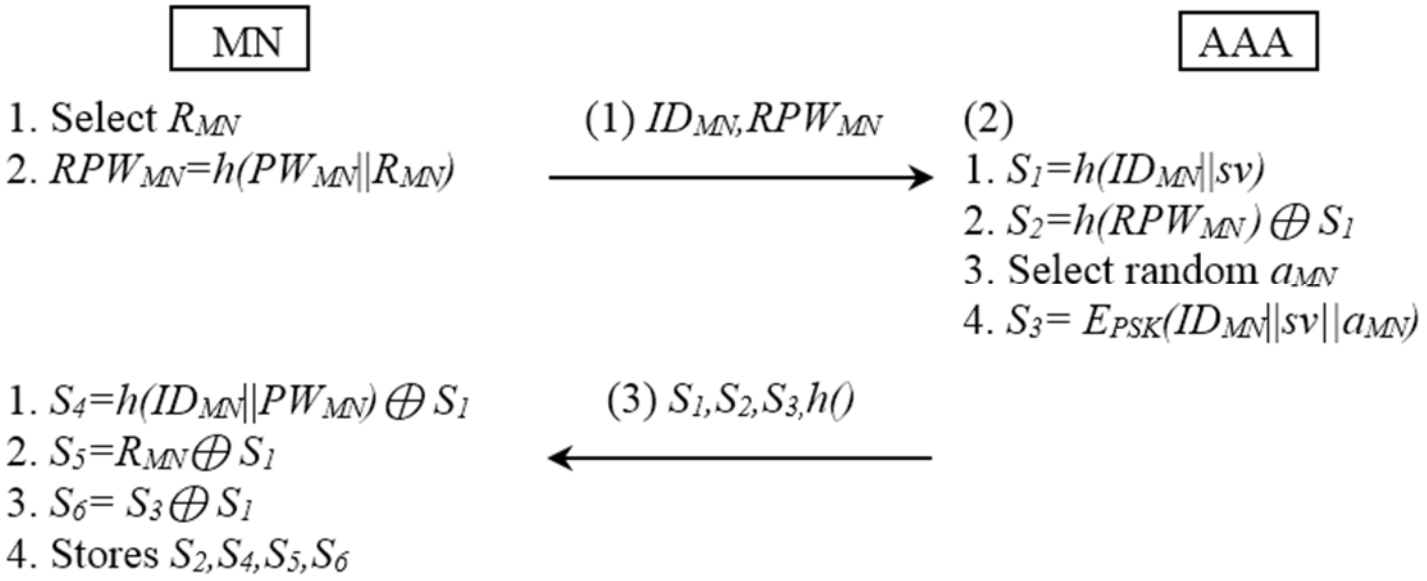

Fig 5. Registration procedure of the proposed method.

doi:10.1371/journal.pone.0142716.g005

$h(ID_{MN} \| sv)$, the MAG can verify the MAG authentication by checking the value of $AUTH_{MN} = h(S_1 \| N_1)$ to the value of $AUTH_{MN}$ obtained from $E_{S_1}(AUTH_{MN} \| N_1)$. If both $AUTH_{MN}$ values are the same, the MN is authenticated and the MAG generates N_2, $SK_{MN-MAG} = h(N_1 \| N_2)$ that is a session key between the MAG and the MN, and $h(ID_{MAG} \| N_2)$.

4. $MAG \rightarrow MN$: The MAG replies $E_{S_1}((N_1 + 1)\|N_2 \| ID_{MAG} \| h(N_2 \| ID_{MAG})$ back to the MN.
5. The MAG verification: The MN decrypts $E_{S_1}(N1 + 1)\|N_2 \| h(N_2 \| ID_M AG))$ to obtain $(N_1 + 1)$ and N_2. Then, it checks the value of $h(N_2 \| ID_{MAG})$ and $(N_1 + 1)$ for the MAG authentication. After verifying the MAG authenticity, the MN generates a session key, $SK_{MN-MAG} = h(N_1 \| N_2)$.
6. $MN \rightarrow MAG$: The MAG computes $E_{SK_{MN-MAG}}(N_2 + 1)$, and sends it to the MAG.
7. The MAG decrypts the received message using the session key and checks $(N_2 + 1)$ to prevent replay attack.

This mutual authentication between the MN and the MAG is described in Fig 6.

Password Change Phase

We improved the password change phase as described in Fig 7. It is worth noticing that the random number, R_{MN}, should be changed as well the user password, PW_{MN}. The symbol,♯, means the new value in Fig 7.

It worth noticing the mutual authentication procedure between the MAG and the LMA in our proposed method is the same as the SPAM method.

Revocation Procedure

The revocation phase can be applied for the SPAM authentication scheme to protect the network entities in case of lost or stolen of smart card. Firstly, the mobile user requests the AAA

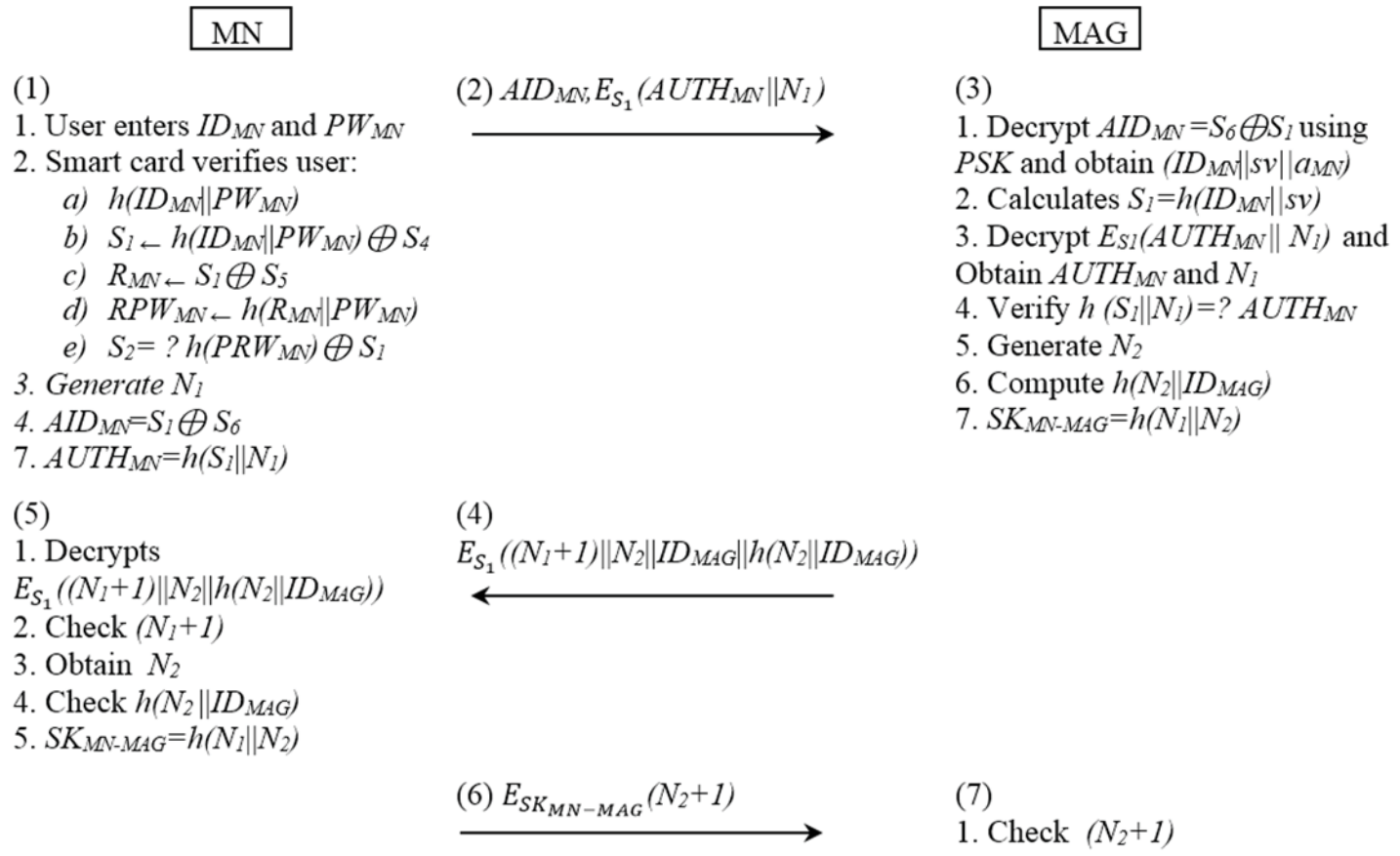

Fig 6. The Proposed authentication procedure between the MN and the MAG.

doi:10.1371/journal.pone.0142716.g006

server for its revocation. Then, the AAA server checks the user credentials, which can be the values known by the user. In case of revocation, the AAA server revokes all the secrets of the mobile user and creates a new set of secrets for the mobile user. Later on, the mobile user can re-register to the AAA server.

Security Analysis of the Proposed Scheme

In this section, we analyze the security and privacy of the proposed enhanced method. Furthermore, the security comparison of the SPAM authentication scheme is provided to prove the security improvement of our proposed method. The proposed authentication method satisfies following requirements:

Anonymity

We applied two methods to protect the MN and the MAG anonymity. For the MN anonymity, we generate an alias ID for the MN, $AID_{MN} = E_{PSK}(ID_{MN} \parallel sv \parallel aMN)$. The ID of the mobile node is mixed with *aMN*, and secret key *sv*. An adversary cannot find ID_{MN} the without knowing the secret key *PSK*. Furthermore, the use of *aMN* and *sv* restricts the adversary to launch identity guessing attack. Furthermore, in the SPAM scheme, the ID_{MAG} is transferred in the plain text during mutual authentication between the MN and the MAG. In our proposed

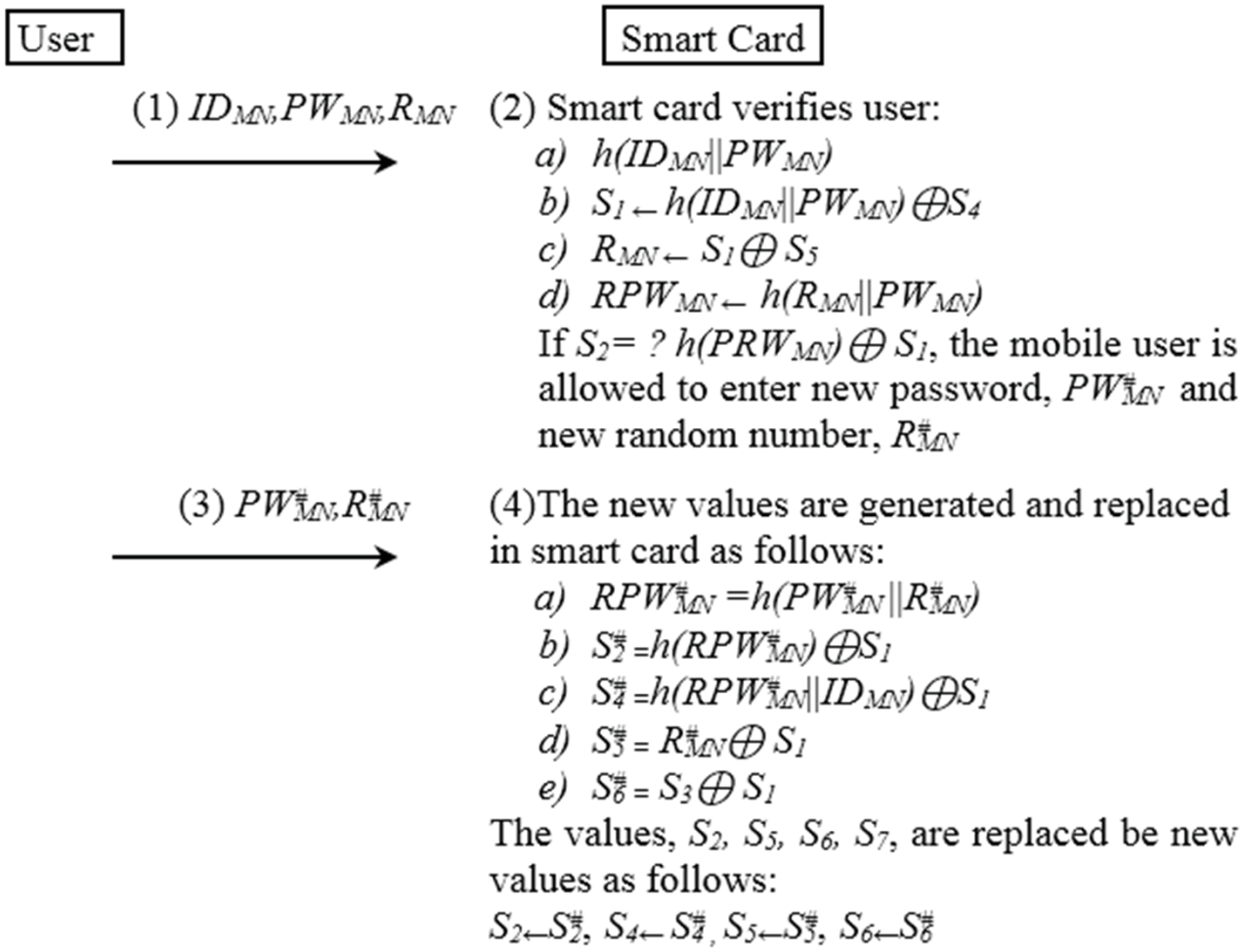

Fig 7. The password change procedure of the proposed method.

doi:10.1371/journal.pone.0142716.g007

methods; we mix the ID_{MAG} with the MAG nonce, N_2, then we encrypt using one-way hash function and N_2 in the message, $E_{S_1}((N_1 + 1)||N_2 \parallel h(N_2 \parallel ID_{MAG}))$. An attacker must know N_2 and N_1 to find the ID_{MAG}, which is impossible for him because he does not know N_2 and N_1 even if he accesses to the smart card.

Mutual Authentication

The mutual authentication between the MN and the MAG is provided in proposed method. As it is shown in Fig 6, the MAG checks the MN authentication in Step 3, by comparing the value, *AUTHMN* received from the MN and the value, $h(S_1 \parallel N_1)$, where it calculates $S_1 = h(ID_{MN} \parallel sv)$. Furthermore, the MN checks the MAG authenticity is Step 5 by checking the value of $h(N_2 \parallel ID_{MAG})$ and $(N_1 + 1)$. Actually, the mobile node checks the value of its nonce, N_1 to be sure that the MAG is legitimate, as the authentic MAG has the pre-shared secrets to decrypt the received messages from the MN.

Revocation Procedure

The revocation of the lost mobile device is provided in proposed method to prevent further security threats against the PMIPv6. In case of loss or stealing the mobile device, the mobile user can inform the AAA server and request to revoke his secret credentials. Therefore, the mobile user can re-register to the AAA server.

Resistance to the MN Impersonation Attack

An attacker must know some values such as S_1, S_6, ID_{MN}, and N_1 to generate the required values, $AID_{MN} = E_{PSK}(ID_{MN} \| sv \| aMN)$ and $AUTH_{MN} = h(S_1 \| N_1)$ and impersonate the MN. Under the assumption of not using tamper-proof smart card; we assume that an attacker can accesses to the smart card, S_2, S_4, S_5, S_6, and even sniffs the communication messages, he cannot find out the values, AID_{MN}, and $AUTH_{MN}$ because he does not know the values, S_1, S_3, ID_{MN}, and R_{MN}.

Resistance to the MAG Impersonation Attack

To impersonate the MAG, an attacker must know the value, S_5, which is the symmetric key between the network entities, to decrypt the sniffed message, $E_{S_1}((N_1 + 1)\|N_2 \| h(N_2 \| ID_{MAG}))$. Furthermore, both the MN and the MAG nonce are required to decrypt this message.

Resistance to Replay Attack

A nonce is used for both the MN and the Mag during authentication procedure to prevent replay attack in the proposed method. Therefore, if an attacker intercepts the authentication communication messages and accesses to the secrets inside the smart card, he cannot replay the sniffed messages, as the MAG or the MN rejects the request because of using invalid nonce by an attacker.

Forgery Attack Resistance

In this section, we discuss that a valid MN cannot launch forgery attack. If an attacker uses the it secrets, S_2, S_4, S_5, S_6, to forge another valid MN, it is impossible to find $AUTH_{MN}$ because he does not know the AAA secret key, sv, to calculate $S_1 = h(ID_{MN} \| sv)$, an then use it to get $AUTH_{MN} = h(S_1 \| N_1)$. As explained in Fig 6, the valid MN must calculate $AUTH_{MN}$ to initiate authentication procedure.

Denial-of-service Attack Resistance

The denial-of-service (DoS) can be discussed in two different situations in our proposed method. First, when the mobile user inserts wrong username and password during the login phase, if there is no suitable mechanism, the smart card processes some procedure and sends the login request to the MAG. In our proposed method, the smart card checks the username and password of the mobile user before computing login request. As described in Fig 6, Step 1, the smart card checks the validity of the mobile user before generating N_1 and the rest of procedure. Second, an attacker can launch DoS attack by requesting password change; however, the smart card first checks PW_{MN} and R_{MN} before updating with new values, $PW^{\sharp}_{MN}$ and $R^{\sharp}_{MN}$. Therefore, DoS cannot happen by requesting password change message.

Table 2. Comparison between proposed scheme and Chuang *et al*.s scheme.

Security Feature	SPAM	Proposed scheme
Anonymity	No	Yes
Mutual authentication	Yes	Yes
Revocation procedure	No	Yes
Resistance to the MN impersonation attack	No	Yes
Resistance to the MAG impersonation attack	No	Yes
Resistance to replay attack	Yes	Yes
Forgery attack resistance	Yes	Yes
Denial-of service attack resistance	Yes	Yes
Resistance to password guessing attack	No	Yes
Stolen-verified attack resistance	No	Yes

doi:10.1371/journal.pone.0142716.t002

Resistance to Password Guessing Attack

In the proposed method, an attacker should know at least ID_{MN}, to find RPW_{MN} for guessing the password, which is impossible as we protect the mobile user privacy by using alias ID of the MN, AID_{MN} instead of real mobile node ID, ID_{MN}. Furthermore, even an attacker can get to find ID_{MN}; he cannot guess the password because he does not know the R_{MN} to calculate $RPW_{MN} = h(PW_{MN} \| R_{MN})$.

Stolen-verified Attack Resistance

The verification table is not required for the AAA server in our method. Therefore, an attacker cannot obtain the authentication secrets of the MN, even if he can access to the AAA server data base. In addition, the MAG does not need the verification table to verify the mobile node authenticity. In other words, even if the MAG reveals the MN secrets, an attacker cannot find another required information for authentication procedure. The security and privacy comparison between SPAM scheme and the proposed enhancement is summarized in Table 2.

Formal Security Analysis

Formal security analysis techniques are commonly used to analyze and evaluate various authentication schemes. According to literature [51–59], many security analysis methods can be employed to evaluate authentication methods. These methods can be categorized into three groups [60]; modal logic such as BAN logic [61], and GNY [62]; theorem proving; model checking such as AVISPA [63] and ProVerif [64]. In this paper, we used both security theorems and BAN logic.

BAN Logic

BAN logic is widely used to analyze security vulnerabilities of security schemes. It consists of three main steps, including translating a target scheme into an idealized version, defining assumption, and applying BAN logic rules to achieve the intended beliefs. The notations of this logic are described in Table 3.

In order to evaluate the security scheme, BAN logic rules should be applied. We just use some of these rules as follows:

Table 3. BAN logic notations.

$P \triangleleft X$	P see X
$P \mid\equiv X$	P believes X
$P \mid\Rightarrow X$	P has jurisdiction over X
$P \mid\sim X$	P once said X
#(X)	X is fresh
$P \overset{K}{\leftrightarrow} Q$	P and Q may use a shared key, K
$(X)_K$	X is encrypted using, key, K

doi:10.1371/journal.pone.0142716.t003

R1: Message-meaning rule: $\frac{P \mid\equiv P \overset{K}{\leftrightarrow} Q, P \triangleleft (X)_K}{P \mid\equiv Q \mid\sim X}$

R2: Jurisdiction rule: $\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \equiv X}{P \mid\equiv X}$

R3: Freshness-conjuncatenation rule: $\frac{P \mid\equiv \#(X), P \mid\equiv Q \sim X}{P \mid\equiv Q \mid\equiv X}$

R4: Break conjuncatenation rule: $\frac{P \mid\equiv (X, Y)}{P \mid\equiv X, P \mid\equiv Y}$

The main goals of our proposed method are mutual authentication between the MN and the MAG. Furthermore, both the MN and the MAG should believe in the shared key. Based on BAN logic and our objectives, the goals of our proposed method are as follows:

- $\mathbf{Goal\ 1}: MAG \mid\equiv MN \mid\equiv (MN \overset{h(ID_{MN} \| sv)}{\longleftrightarrow} MAG)$
- $\mathbf{Goal\ 2}: MAG \mid\equiv (MN \overset{h(ID_{MN} \| sv)}{\longleftrightarrow} MAG)$
- $\mathbf{Goal\ 3}: MN \mid\equiv MAG \mid\equiv (MN \overset{h(ID_{MN} \| sv)}{\longleftrightarrow} MAG)$
- $\mathbf{Goal\ 4}: MN \mid\equiv (MN \overset{h(ID_{MN} \| sv)}{\longleftrightarrow} MAG)$

After identifying the main objectives of our proposed method, the communication messages are transformed to the idealized version.

$\mathbf{M1.1}: MN \rightarrow MAG: (MAG \overset{PSK}{\leftrightarrow} AAA, MN \overset{h(ID_{MN} \| sv)}{\longleftrightarrow} AAA, ID_{MN}, sv, aMN, PSK) K_{PSK}$

$\mathbf{M1.2}: MN \rightarrow MAG: (MN \overset{h(ID_{MN} \| sv}{\longleftrightarrow} AAA, MN \overset{h(ID_{MN} \| sv)}{\longleftrightarrow} MAG, N_1, ID_{MN}, h(ID_{MN} \| sv)) h(ID_{MN} \| sv)$

$\mathbf{M2}: MAG \rightarrow MN: (MN \overset{h(ID_{MN} \| sv}{\longleftrightarrow} AAA, MN \overset{h(ID_{MN} \| sv)}{\longleftrightarrow} MAG, N_1, N_2, ID_{MAG}, h(ID_{MN} \| sv)) h(ID_{MN} \| sv)$

$\mathbf{M3}: MN \rightarrow MAG: (MN \overset{h(ID_{MN} \| sv}{\longleftrightarrow} MAG, N_2, h(ID_{MN} \| sv)) h(ID_{MN} \| sv)$

The initial assumptions of our proposed method are as follows:

1. $\mathbf{A1}: MAG \mid\equiv \sharp aMN$
2. $\mathbf{A2}: MAG \mid\equiv \sharp N^x_{MAG}$
3. $\mathbf{A3}: MN \mid\equiv \sharp N^x_{MN}$
4. $\mathbf{A4}: MN \mid\equiv (MN \overset{h(ID_{MN} \| sv}{\longleftrightarrow} AAA)$
5. $\mathbf{A5}: MAG \mid\equiv (MAG \overset{PSK}{\leftrightarrow} AAA)$
6. $\mathbf{A6}: MN \mid\equiv MAG \Rightarrow (MN \overset{h(ID_{MN} \| sv}{\longleftrightarrow} MAG)$

7. $\mathbf{A7}: MAG \mid\equiv MN \Rightarrow (MN \overset{h(ID_{MN}\|sv}{\leftrightarrow} MAG)$

In this section, we analyzed our proposed method based on idealized messages and the assumptions using BAN logic rules. The proofs are as follows:

1. According to message M1.1 and assumptions A5 (message-meaning rule):

S1: $MAG|\equiv MN|\sim$
$(MAG \overset{PSK}{\leftrightarrow} AAA, MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} AAA, ID_{MN}, sv, aMN, PSK)$

2. According to S1 and assumptions A1 (freshness-conjuncatenation):

S2: $MAG|\equiv MN|\equiv$
$(MAG \overset{PSK}{\leftrightarrow} AAA, MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} AAA, ID_{MN}, sv, aMN, PSK)$

3. According to message S2 and BAN logic break conjuncatenation rule:

$\mathbf{S3}: MAG \mid\equiv MN \mid\equiv (MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} AAA)$

4. According to message M1.2 and S3 (message-meaning rule):

S4: $MAG|\equiv MN|\sim$
$(MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} AAA, MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} MAG, N_1, ID_{MN}, h(ID_{MN} \parallel sv))$

5. According to S4 and assumptions A1 (freshness-conjuncatenation):

S5: $MAG|\equiv MN|\equiv$
$(MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} AAA, MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} MAG, N_1, ID_{MN}, h(ID_{MN} \parallel sv))$

6. According to message S5 and BAN logic break conjuncatenation rule:

$\mathbf{S6}: MAG \mid\equiv MN \mid\equiv (MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} MAG)$ **(Goal 1)**

7. According to message S6 and A7 and BAN logic jurisdiction rule:

$\mathbf{S7}: MAG \mid\equiv (MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} MAG)$ **(Goal 2)**

8. According to message M2 and assumptions A4 (message-meaning rule):

S8: $MN|\equiv MAG|\sim$
$(MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} AAA, MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} MAG, N_1, N_2, ID_{MN}, h(ID_{MN} \parallel sv))$

9. According to S8 and assumptions A3 (freshness-conjuncatenation):

S9: $MN|\equiv MAG|\equiv$
$(MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} AAA, MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} MAG, N_1, N_2, ID_{MN}, h(ID_{MN} \parallel sv))$

10. According to message S9 and BAN logic break conjuncatenation rule:

$\mathbf{S10}: MN \mid\equiv MAG \mid\equiv (MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} MAG)$ **(Goal 3)**

11. According to message S10 and A6 and BAN logic jurisdiction rule:

$\mathbf{S11}: MN \mid\equiv (MN \overset{h(ID_{MN}\|sv)}{\leftrightarrow} MAG)$ **(Goal 4)**

Performance Analysis

The performance of our proposed method is analyzed in this section. We evaluate authentication procedure for our proposed method and compare to SPAM (Ming-Chin *et al.*, 2013). The notations used in this evaluation are provided as follows:

Table 4. Performance comparison between proposed scheme and SPAM.

Criterion	Chuang *et al*.'s scheme	Proposed scheme
SC's memory (in bit)	6 × 128 = 768 bit	5 × 128 = 640 bit
Communication cost	9 × 128 = 1152 bit	7 × 128 = 896 bit
Computational cost		
Authentication (MN)	5Thash+2Txor+3Tsym+1Tran	4Thash+3Txor+3Tsym+1Tran
Authentication (MAG)	5Thash+1Txor+4Tsym+1Tran	3Thash+0Txor+4Tsym+1Tran
Total	10Thash+3Txor+7Tsym+2Tran 0.20015 S	7Thash+3Txor+7Tsym+2Tran

doi:10.1371/journal.pone.0142716.t004

- T_{hash}: Hash function execution time
- T_{xor}: XOR operation execution time
- T_{sym}: Symmetric cryptography execution time
- T_{ran}: Time for generating a random number

The performance of our proposed method is evaluated according to the methodology used in [65–69] and described in Table 4. The computation time for one-way hash function, symmetric cryptography, and random number generation time [70], are 0.0005 s, 0.0087 s, and 0.063075 s respectively. The computation time for XOR operation can be ignored because it trivial compare to other operations. It worth noticing that the computation time for each cryptographic operation is calculated relatively and is not the exact amount, because computation time varies based on the computation resource of network entities. In memory efficiency section, we assume that the length of ID, PW, random number, and output of hash function, is 128 bits. Table 3 summarizes performance evaluation of our proposed method and SPAM method based on criteria such as communication cost, memory requirement, and computational cost. The proposed method requires 640 bits memory space in smart card, but SPAM requires memory storage, 768 bits. Likewise, the communication cost of the proposed scheme is 896 bits, and SPAM requires 1152 bits. Similarly, the proposed scheme also having less computation cost as compared with Chuang et al.'s scheme.

Conclusion

In this paper, we show that how an attacker can launch different attacks such as impersonation attack and password guessing attack using smart card secrets and sniffed login request message on Chuang et al.'s scheme. Furthermore, other security flaws such as lack of revocation procedure in case of loss or stolen device, and anonymity issues of this scheme, are discussed. In addition, we proposed an enhanced scheme to cover the discussed security drawbacks. The security of the proposed scheme is analyzed using BAN logic. The results show that proposed scheme while mitigating all the discussed security flaws, is also more efficient in terms of memory communication and computation costs.

Acknowledgments

Authors acknowledge the support from Malaysia-Japan International Institute of Technology (MJIIT) center at Universiti Teknologi Malaysia, Japan Student Services Organization (JASSO), and Kyushu University, Fukuoka, Japan. The authors extend their sincere

appreciations to the Deanship of Scientific Research at King Saud University for its funding this Prolific Research Group (PRG-1436-16).

Author Contributions

Conceived and designed the experiments: MA. Performed the experiments: MA. Analyzed the data: MZ SB AAM HK. Contributed reagents/materials/analysis tools: KS MKK HA. Wrote the paper: SAC. Analyzed and evaluated manuscript: MKK.

References

1. Soto I, Bernardos CJ, Calderón M, Melia T. PMIPv6: A Network-Based Localized Mobility Management Solution. The Internet Protocol Journal. 2010; 13(3):2–15. Available from: http://goo.gl/mF8KBl
2. Johnson D, Perkins C, Arkko J. Mobility Support in IPv6. RFC 3775. 2004;Available from: http://tools.ietf.org/html/rfc3775
3. Kim S, Koo J, Oh H. Ticket-Based Binding Update Protocol for Mobile IPv6. In: Madria S, Claypool K, Kannan R, Uppuluri P, Gore M, editors. Distributed Computing and Internet Technology SE—6. vol. 4317 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2006. p. 63–72. Available from: http://dx.doi.org/10.1007/11951957_6
4. Soliman H, Bellier L, Elmalki K, Castelluccia C. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management-RFC 5380. IETF; 2008. Available from: https://tools.ietf.org/html/rfc5380
5. Koodli ER. Mobile IPv6 Fast Handovers. RFC5568. IETF; 2009. Available from: https://tools.ietf.org/html/rfc5568
6. Gundavelli S, Leung L, Devarapalli V, Chowdhury K, Patil B. Proxy Mobile IPv6-RFC 5213. IETF; 2008. Available from: https://tools.ietf.org/html/rfc5213
7. Chiussi FM, Khotimsky DA, Krishnan S. Mobility management in third-generation all-IP networks; 2002. Available from: http://dx.doi.org/10.1109/MCOM.2002.1031839
8. Jiang Q, Ma J, Li G, Ye A. Security Enhancement on an Authentication Method for Proxy Mobile IPv6. In: Jiang L, editor. International Conference on Informatics, Cybernetics, and Computer Engineering. Melbourne, Australia; 2012. p. 345–352. Available from: http://dx.doi.org/10.1007/978-3-642-25185-6_45
9. Chuang MC, Lee JF, Chen MC. SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks. IEEE Systems Journal. 2013; 7(1):102–113. Available from: http://dx.doi.org/10.1109/JSYST.2012.2209276
10. Alizadeh M, Baharun S, Zamani M, Khodadadi T, Darvishi M, Gholizadeh S, et al. Anonymity and Untraceability Assessment of Authentication Protocols in PMIPv6. Jurnal Teknologi. 2015; 72(5):31–34. Available from: http://dx.doi.org/10.11113/jt.v72.3936
11. Choo KKR. Secure Key Establishment. vol. 41. Springer Science & Business Media; 2009. Available from: http://dx.doi.org/10.1007/978-0-387-87969-7
12. Li X, Niu J, Khurram Khan M, Liao J. An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications. 2013 Sep; 36(5):1365–1371. Available from: http://dx.doi.org/10.1016/j.jnca.2013.02.034
13. Nam J, Choo KKR, Han S, Kim M, Paik J, Won D. Efficient and Anonymous Two-Factor User Authentication in Wireless Sensor Networks: Achieving User Anonymity with Lightweight Sensor Computation. PLoS ONE. 2015 Apr; 10(4):e0116709. Available from: http://dx.doi.org/10.1371%2Fjournal.pone.0116709 PMID: 25849359
14. Farash MS, Chaudhry SA, Heydari M, Sajad Sadough SM, Kumari S, Khan MK. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. International Journal of Communication Systems. 2015;Available from: http://dx.doi.org/10.1002/dac.3019
15. Wang S, Cao Z, Cheng Z, Choo KK. Perfect forward secure identity-based authenticated key agreement protocol in the escrow mode. Science in China Series F: Information Sciences. 2009; 52(8):1358–1370. Available from: http://dx.doi.org/10.1007/s11432-009-0135-4
16. Alizadeh M, Zamani M, Baharun S, Hassan WH, Khodadadi T. Security and Privacy Criteria to Evaluate Authentication Mechanisms in Proxy Mobile IPv6. Jurnal Teknologi. 2015; 72(5):27–30. Available from: http://dx.doi.org/10.11113/jt.v72.3935
17. Raymond Choo KK, Boyd C, Hitchcock Y. The importance of proofs of security for key establishment protocols: Formal analysis of Jan-Chen, Yang-Shen-Shieh, Kim-Huh-Hwang-Lee, Lin-Sun-Hwang, and Yeh-Sun protocols. Computer Communications. 2006 Sep; 29(15):2788–2797. Available from: http://dx.doi.org/10.1016/j.comcom.2005.10.030

18. Chaudhry SA, Farash MS, Naqvi H, Kumari S, Khan MK. An enhanced privacy preserving remote user authentication scheme with provable security. Security and Communication Networks. 2015;Available from: http://dx.doi.org/10.1002/sec.1299
19. Li X, Niu J, Wang Z, Chen C. Applying biometrics to design three factor remote user authentication scheme with key agreement. Security and Communication Networks. 2013; 7(10):1488–1497. Available from: http://dx.doi.org/10.1002/sec.767
20. He D, Kumar N, Chilamkurti N. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Information Sciences. 2015 Nov; 321:263–277. Available from: http://dx.doi.org/10.1016/j.ins.2015.02.010
21. Nam J, Choo KKR, Kim M, Paik J, Won D. Dictionary Attacks against Password-Based Authenticated Three-Party Key Exchange Protocols (2013). KSII Transactions on Internet and Information Systems (TIIS). 2013; 7(12):3244–3260. Available from: http://dx.doi.org/10.3837/tiis.2013.12.016
22. Chaudhry SA. Comment on 'Robust and efficient password authenticated key agreement with user anonymity for session initiation protocol-based communications' (2015). IET Communications. 2015; 9 (7):1034–1034. Available from: http://dx.doi.org/10.1049/iet-com.2014.1082
23. Li X, Niu JW, Ma J, Wang WD, Liu CL. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications. 2011 Jan; 34(1):73–79. Available from: http://dx.doi.org/10.1016/j.jnca.2010.09.003
24. Chaudhry S, Naqvi H, Shon T, Sher M, Farash M. Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems. Journal of Medical Systems. 2015; 39(6):1–11. Available from: http://dx.doi.org/10.1007/s10916-015-0244-0
25. Ma CG, Wang D, Zhao SD. Security flaws in two improved remote user authentication schemes using smart cards. International Journal of Communication Systems. 2012; 27(10):2215–2227. Available from: http://dx.doi.org/10.1002/dac.2468
26. Khan MK, Kumari S. Cryptanalysis and Improvement of "An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems". Security and Communication Networks. 2014; 7(2):399–408. Available from: http://dx.doi.org/10.1002/sec.791
27. Xu J, Zhu WT, Feng DG. An improved smart card based password authentication scheme with provable security. Computer Standards and Interfaces. 2009 Jun; 31(4):723–728. Available from: http://dx.doi.org/10.1016/j.csi.2008.09.006
28. Wang Yy, Liu Jy, Xiao Fx, Dan J. A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme. Computer communications. 2009; 32(4):583–585. Available from: http://dx.doi.org/10.1016/j.comcom.2008.11.008
29. Rhee HS, Kwon JO, Lee DH. A remote user authentication scheme without using smart cards. Computer Standards & Interfaces. 2009 Jan; 31(1):6–13. Available from: http://dx.doi.org/10.1016/j.csi.2007.11.017
30. Fan CI, Chan YC, Zhang ZK. Robust remote authentication scheme with smart cards. Computers & Security. 2005 Nov; 24(8):619–628. Available from: http://dx.doi.org/10.1016/j.cose.2005.03.006
31. Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers. 2002; 51(5):541–552. Available from: http://dx.doi.org/10.1109/TC.2002.1004593
32. Haller N. The S/KEY One-Time Password System. In: Proceedings of 1994 internet society symposium on network and distributed system security. San Diego, USA; 1994. p. 151–157. Available from: https://tools.ietf.org/html/rfc1760
33. Lamport L. Password authentication with insecure communication. Communications of the ACM. 1981; 24(11):770–772. Available from: http://dx.doi.org/10.1145/358790.358797
34. Hwang MSHMS, Li LHLLH. A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics. 2000; 46(1):28–30. Available from: http://dx.doi.org/10.1109/30.826377
35. Lee NY, Chiu YC. Improved remote authentication scheme with smart card. Computer Standards & Interfaces. 2005 Jan; 27(2):177–180. Available from: http://dx.doi.org/10.1016/j.csi.2004.06.001
36. Lee SW, Kim HS, Yoo KY. Improvement of Chien et al.'s remote user authentication scheme using smart cards. Computer Standards & Interfaces. 2005 Jan; 27(2):181–183. Available from: http://dx.doi.org/10.1016/j.csi.2004.02.002
37. Chien HY, Jan JK, Tseng YM. A modified remote login authentication scheme based on geometric approach. Journal of Systems and Software. 2001 Jan; 55(3):287–290. Available from: http://dx.doi.org/10.1016/S0164-1212(00)00077-7

38. Das ML, Saxena A, Gulati VP. A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics. 2004; 50(2):629–631. Available from: http://dx.doi.org/10.1109/TCE.2004.1309441

39. Juang WS. Efficient multi-server password authenticated key agreement using smart cards. IEEE Transactions on Consumer Electronics. 2004; 50(1):251–255. Available from: http://dx.doi.org/10.1109/TCE.2004.1277870

40. He D, Zeadally S. Authentication protocol for an ambient assisted living system; 2015. Available from: http://dx.doi.org/10.1109/MCOM.2015.7010518

41. Li X, Xiong Y, Ma J, Wang W. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. Journal of Network and Computer Applications. 2012 Mar; 35(2):763–769. Available from: http://dx.doi.org/10.1016/j.jnca.2011.11.009

42. Kumari S, Chaudhry S, Wu F, Li X, Farash M, Khan M. An improved smart card based authentication scheme for session initiation protocol. Peer-to-Peer Networking and Applications. 2015;p. 1–14. Available from: http://dx.doi.org/10.1007/s12083-015-0409-0

43. Li X, Ma J, Wang W, Xiong Y, Zhang J. A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments. Mathematical and Computer Modelling. 2013 Jul; 58(1-2):85–95. Available from: http://dx.doi.org/10.1016/j.mcm.2012.06.033

44. Chen HM, Lo JW, Yeh CK. An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. Journal of Medical Systems. 2012; 36(6):3907–3915. Available from: http://dx.doi.org/10.1007/s10916-012-9862-y PMID: 22673892

45. Kocher P, Jaffe J, Jun B. Introduction to differential power analysis and related attacks; 1998. Available from: http://goo.gl/Z9AINa

46. Kocher P, Jaffe J, Jun B. Differential Power Analysis. In: Advances in Cryptology- CRYPTO' 99. Springer Berlin Heidelberg; 1999. p. 388–397. Available from: http://dx.doi.org/10.1007/3-540-48405-1_25

47. Boneh D, DeMillo R, Lipton R. New Threat Model Breaks Crypto Codes. Bellcore Press Release. 1996;Available from: http://goo.gl/gMujHn

48. Ku WC. Impersonation Attack on a Dynamic ID-Based Remote User Authentication Scheme Using Smart Cards. IEICE Transactions on Communications. 2005; E88-B:2165–2167. Available from: http://dx.doi.org/10.1093/ietcom/e88-b.5.2165

49. Khan MK, Kumari S, Gupta MK, Muhaya FTB. Cryptanalysis of Truong et al.'s fingerprint biometric remote authentication scheme using mobile device. In: 6th International Conference on Brain Inspired Cognitive Systems. vol. 7888 LNAI. Beijing, China; 2013. p. 271–277. Available from: http://dx.doi.org/10.1007/978-3-642-38786-9_31

50. Yoon EJ, Yoo KY. Comments on modified user friendly remote authentication scheme with smart cards. IEICE Transactions on Communications. 2007; 90(2):331–333. Available from: http://dx.doi.org/10.1093/ietcom/e90-b.2.331

51. Ch S, Uddin N, Sher M, Ghani A, Naqvi H, Irshad A. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. Multimedia Tools and Applications. 2015; 74(5):1711–1723. Available from: http://dx.doi.org/10.1007/s11042-014-2283-9

52. Chaudhry S, Naqvi H, Sher M, Farash M, Hassan M. An improved and provably secure privacy preserving authentication protocol for SIP. Peer-to-Peer Networking and Applications. 2015;p. 1–15. Available from: http://dx.doi.org/10.1007/s12083-015-0400-9

53. Choo KKR. An integrative framework to protocol analysis and repair: Bellare-Rogaway model plus planning plus model checker. Informatica. 2007; 18(4):547–568. Available from: http://goo.gl/xwjtJp

54. Choo KKR, Nam J, Won D. A mechanical approach to derive identity-based protocols from Diffie-Hellman-based protocols. Information Sciences. 2014 Oct; 281:182–200. Available from: http://dx.doi.org/10.1016/j.ins.2014.05.041

55. Shen J, Tan H, Wang J, Wang J, Lee S. A Novel Routing Protocol Providing Good Transmission Reliability in Underwater Sensor Networks. Journal of Internet Technology. 2015; 16(1):171–178. Available from: http://goo.gl/hkYdf9

56. Choo KKR. A proof of revised Yahalom protocol in the Bellare and Rogaway (1993) model. Computer Journal. 2007; 50(5):591–601. Available from: http://dx.doi.org/10.1093/comjnl/bxm019

57. Chaudhry S, Farash M, Naqvi H, Sher M. A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electronic Commerce Research. 2015;p. 1–27. Available from: http://dx.doi.org/10.1007/s10660-015-9192-5

58. Guo P, Wang J, Geng XH, Kim CS, Kim JU. A Variable Threshold-value Authentication Architecture for Wireless Mesh Networks. JIT Journal of Internet Technology. 2014; 15(6):929–935. Available from: http://goo.gl/7IBFZ6

59. He D, Wang D. Robust Biometrics-Based Authentication Scheme for Multiserver Environment. IEEE Systems Journal. 2015; 9(3):816–823. Available from: http://dx.doi.org/10.1109/JSYST.2014.2301517

60. You I. Design and analysis of mobile internet security protocol by using [Thesis]. Kyushu University; 2012.

61. Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems. 1990; 8:18–36. Available from: http://dx.doi.org/10.1098/rspa.1989.0125 doi: 10.1145/77648.77649

62. Mathuria aM, Safavi-naini R, Nickolas PR. On the automation of GNY logic. Australian Computer Science Communications. 1995; 17:370–379. Available from: http://goo.gl/NDqTNe

63. Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuellar J, et al. The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In: Etessami K, Rajamani S, editors. Computer Aided Verification SE- 27. vol. 3576 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2005. p. 281–285. Available from: http://dx.doi.org/10.1007/11513988_27

64. Blanchet B. ProVerif: Cryptographic protocol verifier in the formal model; 2012. Available from: http://goo.gl/AIznu8

65. Hsieh WB, Leu JS. Anonymous authentication protocol based on elliptic curve Diffie-Hellman for wireless access networks. Wireless Communications and Mobile Computing. 2014; 14(10):995–1006. Available from: http://dx.doi.org/10.1002/wcm.2252

66. He D, Zhang Y, Chen J. Cryptanalysis and Improvement of an Anonymous Authentication Protocol for Wireless Access Networks. Wireless Personal Communications. 2014; 74(2):229–243. Available from: http://dx.doi.org/10.1007/s11277-013-1282-x

67. Li CT, Hwang MS, Chu YP. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Computer Communications. 2008 Jul; 31(12):2803–2814. Available from: http://dx.doi.org/10.1016/j.comcom.2007.12.005

68. Wen F, Li X. An improved dynamic ID-based remote user authentication with key agreement scheme. Computers and Electrical Engineering. 2012; 38(2):381–387. Available from: http://dx.doi.org/10.1016/j.compeleceng.2011.11.010

69. Kumari S, Gupta MK, Khan MK, Li X. An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement. Security and Communication Networks. 2014; 7 (11):1921–1932. Available from: http://dx.doi.org/10.1002/sec.906

70. Koblitz N, Menezes A, Vanstone S. The State of Elliptic Curve Cryptography. In: Koblitz N, editor. Towards a Quarter-Century of Public Key Cryptography SE—5. Springer US; 2000. p. 103–123. Available from: http://dx.doi.org/10.1007/978-1-4757-6856-5_5