RESEARCH ARTICLE

# Security analysis and enhanced user authentication in proxy mobile IPv6 networks

**Dongwoo Kang, Jaewook Jung, Donghoon Lee, Hyoungshick Kim, Dongho Won***

Department of Computer Engineering, Sungkyunkwan University, 2066 Seoburo, Suwon, Gyeonggido 16419, Korea

* dhwon@security.re.kr

## Abstract

The Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol that allows a Mobile Node(MN) connected to the PMIPv6 domain to move from one network to another without changing the assigned IPv6 address. The user authentication procedure in this protocol is not standardized, but many smartcard based authentication schemes have been proposed. Recently, Alizadeh et al. proposed an authentication scheme for the PMIPv6. However, it could allow an attacker to derive an encryption key that must be securely shared between MN and the Mobile Access Gate(MAG). As a result, outsider adversary can derive MN's identity, password and session key. In this paper, we analyze Alizadeh et al.'s scheme regarding security and propose an enhanced authentication scheme that uses a dynamic identity to satisfy anonymity. Furthermore, we use BAN logic to show that our scheme can successfully generate and communicate with the inter-entity session key.

**Citation:** Kang D, Jung J, Lee D, Kim H, Won D (2017) Security analysis and enhanced user authentication in proxy mobile IPv6 networks. PLoS ONE 12(7): e0181031. https://doi.org/10.1371/journal.pone.0181031

**Editor:** Muhammad Khurram Khan, King Saud University, SAUDI ARABIA

**Received:** March 21, 2017

**Accepted:** June 25, 2017

**Published:** July 18, 2017

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

**Funding:** This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2010-0020210) http://www.nrf.re.kr/index.

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

## Introduction

In recent years, the mobile-device market has grown rapidly, and with the increasing availability of wireless Internet access, various services including browsing, file-sharing, and shopping are becoming increasingly available regardless of the time and place. The Internet Engineering Task Force (IETF) has been developing the Internet standards, and after more than 20 releases, the standardization of IPv6-based mobility has been discussed as "Mobility Support in IPv6 (MIPv6)" since the late 1990s; the standardization to the proposed standard "RFC 3775" was completed in June 2004 [1].

However, the MIPv6 imposes a burden on the mobile terminal by increasing the resource usage, and this is due to the signaling between the mobile terminal and the access router and the implementation of a complicated standard specification in a mobile terminal with limited resources. Thus, telecommunication operator were not satisfied. To solve this problem, the IETF proposed the Proxy Mobile IPv6 (PMIPv6) technology, and various research institutes are actively conducting the corresponding research. With the adoption of the PMIPv6, the complicated specification and signaling problems that are highlighted in the existing MIPv6 have been solved. However, it is still necessary to continue research because the technology cannot significantly reduce the handover-delay time that can occur with the movement of the Mobile Node (MN) [2, 3]. Additionally, in the "RFC 5213" document wherein the PMIPv6 standard is defined, the authentication process of the MN is not properly specified. Therefore, a lot of research have been proposed on the authentication process between MN and Mobile Access Gate (MAG) [4].

In this circumstance, a smartcard can be used as an authentication method between MN and MAG. Because of high potability and low cost, authentication schemes using smartcard have been proposed over the past few years. Since Lamport proposed the first password-based authentication scheme in 1981. Smartcard-based authentication has been applied to numerous protocols, such as the session initiation protocol [5], mobile client-client network [6], wireless sensor network [7], Electronic Patient Records(EPR) information systems [8].

In 2013, Chuang et al. proposed a new authentication mechanism using smartcard called "SPAM". SPAM offers a low packet loss and low latency rates compared with the other PMIPv6 mechanisms [9]. However, SPAM is susceptible to the replay and malicious-insider attacks, and it does not provide protection against the compromise of a single node [10]. Also SPAM has several vulnerabilities which is susceptible to impersonation attack and password guessing attack, ignore the MAG and LMA anonymity [11]. To complement with these security drawbacks, Alizadeh et al. proposed a new authentication scheme with revocation process in 2015 [12]. However, Alizadeh et al.'s scheme has a fatal vulnerability when deriving the encryption key using the symmetric key algorithm. It is possible to carry out various attacks, including impersonation attack, password guessing attack, session key derive attack. For that, we proposed a new scheme to defend against the attacks that are present in "RFC 4832" [13] and Alizadeh et al.'s research [14].

1. Man in the middle attack: an adversary can interrupt between two entities during authentication. Thus, the adversary can intercept, modify, or drop the packets sourced by or destined to the MN
2. Impersonation attack: an adversary can impersonate a user to the MN or MAG through inspection and discovery of the authentication information.
3. Replay attack: an adversary can resend the legal message sent earlier in order to disorder the traffic flow or impersonate.
4. Verifier impersonation: impersonation attack that the adversary creates independent connection with the victims and sends messages between them, causing them to think that they can directly communicate to each other.
5. Modification attack: an adversary may try to change the authentication message of the MAG or the MN.
6. Stolen-verifier: an adversary may thieve verification table if the scheme of authentication saves this table with LMA or MAG.

The following paper is organized as follows. Section 2 concisely introduces the requisite preliminary knowledge for an improved comprehension of this paper, including the PMIPv6, hash function, and bio-hash function. Section 3 is a review of Alizadeh et al.'s scheme. Section 4 is an analysis of Alizadeh et al.'s scheme and shows its security vulnerabilities. Section 5 describes the proposed scheme that protects against the attacks shown in Section 4. In Section 6, the proposed scheme is analyzed using a formal security analysis with Burrows-Abadi-Needham (BAN) logic and an informal security analysis. Section 7 presents a comparison of the performances of the prior schemes with that of the proposed scheme, and Section 8 concludes this paper.

## Preliminary knowledge

In this section, we introduce some preliminaries, including the structure of PMIPv6, the hash function based on both Alizadeh et al.'s and our proposed scheme.

### Structure of proxy mobile IPv6(PMIPv6)

The basic method for the provision of Internet protocol (IP) mobility to a mobile terminal involves the use of the mobile IP. But, the mobile IP manages the binding information on the MN's location information by exchanging the signaling message between the MN and the Home Agent (HA). The PMIPv6 does not need a separate protocol stack for mobility management because the network elements handle the exchange of the binding-related messages instead of the MN. The components of the PMIPv6 are shown in Fig 1:

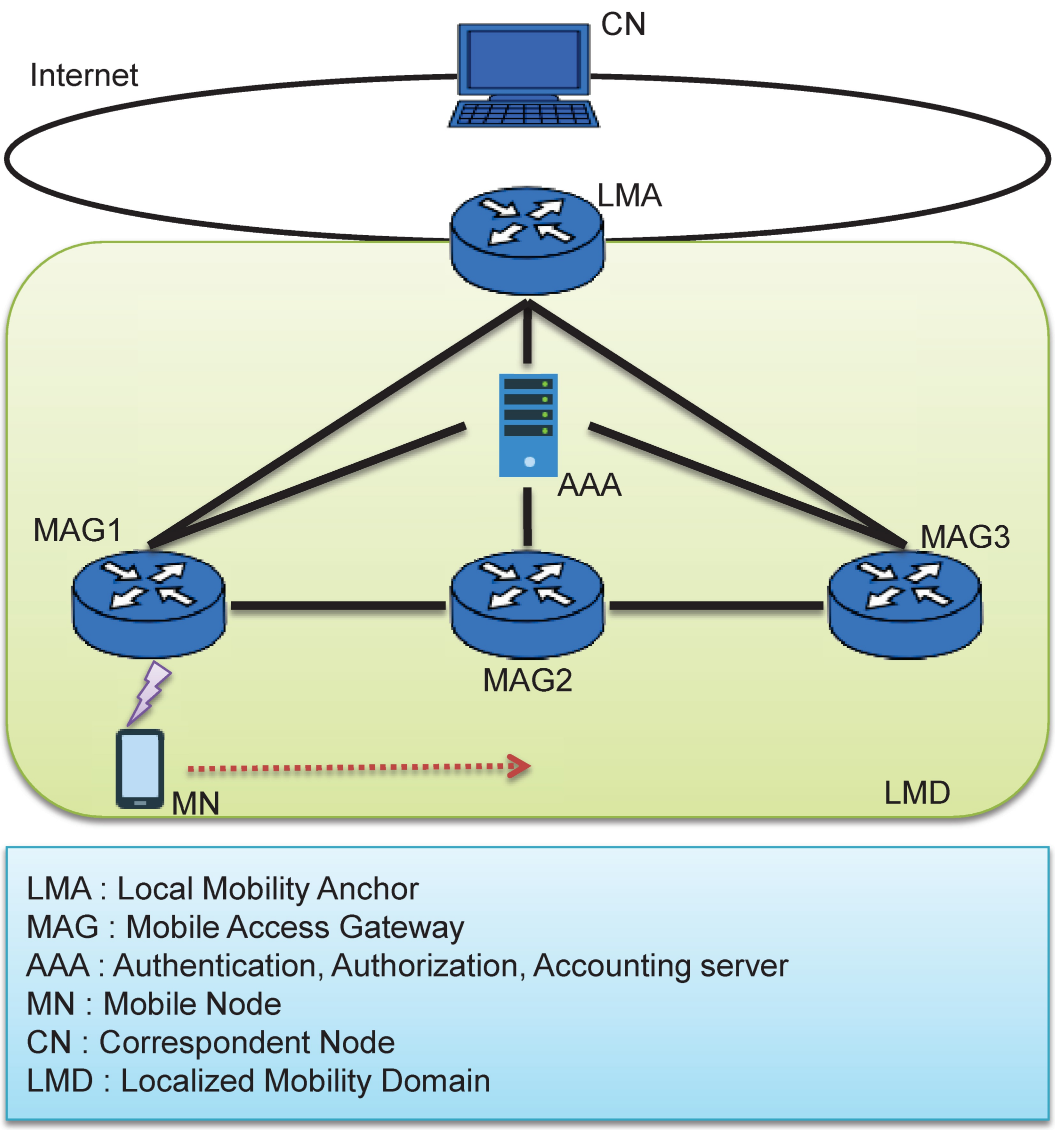

CN
Internet
LMA
AAA
MAG1
MAG3
MAG2
MN
LMD
LMA : Local Mobility Anchor
MAG : Mobile Access Gateway
AAA : Authentication, Authorization, Accounting server
MN : Mobile Node
CN : Correspondent Node
LMD : Localized Mobility Domain

**Fig 1. Network structure for PMIPv6.**

https://doi.org/10.1371/journal.pone.0181031.g001

The PMIPv6 domain refers to a network that manages the movement of the MN using the PMIPv6. Domains require the new functional elements the MAG and the LMA. The MAG monitors the movement of the MN on the access link and transmits the MN's mobile signaling message to the LMA instead of the MN, while the LMA acts as the HA for the MN in the PMIPv6 domain. The LMA is an anchor point on the topology of the home-network prefix that is allocated to the MN and serves to manage the reachability state of the MN in the domain. In general, the function of the MAG can be implemented in the access router, and the LMA can be located in the gateway of the domain.

Between the LMA and the MAG, there is an IP tunnel for the transmission of signaling messages and the data packets for sending and receiving the MN. The MAG can support different IP prefixes for terminals receiving mobility-support services and general terminals using the PMIPv6. The previous MAG (PMAG) detected by the MN is a detached event wherein the MN is not present on its access link, and it notifies the LMA of the detachment of the MN using a Proxy Binding Update (PBU) message. The LMA performs an operation to delete the binding entry associated with the MN and transmits the PBA.

When the MN is connected to a new MAG (NMAG), the NMAG performs the initial access procedure of the MN, and it transmits the home-network-prefix information that the MN has allocated in the initial access through the Router Solicitation/Router Advertisement that is sent to the MN. Therefore, the MN can use the initially assigned address. Fig 2 shows the handover process in the PMIPv6 environment.

### Hash function

A cryptographic hash function can support confidence of data integrity. Hash function is used to construct a short *"dactylogram"* of data. Also hash function can be any function that is used to map data of an arbitrary size to data of a fixed size. Furthermore, There are three main conditions of hash function that are defined as $y = h(x)$ [15, 16] as follows.

1. Preimage Resistance: When $h(x)$ is given, find $x'$ such that $h(x) = h(x')$ is infeasible.
2. Second Preimage Resistance: When $x$ and $h(x)$ are given, find $x' \neq x$ such that $h(x) = h(x')$ is infeasible.
3. Collision Resistance: Find $x' \neq x$ such that $h(x) = h(x')$ is infeasible.

### Bio-hash function

Recently, a three-factor authentication scheme that adds user's biometric information to a two-factor authentication scheme using identity, password for growth security was widely proposed [17–19]. To apply biometric information in user authentication scheme, and since Jin et al. [20] proposed a fingerprint-based function to distinguish person in 2004. The bio-hash function is used in this study. Bio-hash method handles particular tokenized pseudo-random numbers for each user by summarily measuring the biometric information on two fold strands. Bio-hash function $H(\cdot)$ also has features of one-way hash function as mentioned previously.

## Review in Alizadeh et al.'s scheme

In This section, we review the Alizadeh et al.'s secure password authentication mechanism in 2015. Alizadeh et al.'s scheme consists of following phases: registration, mutual authentication, password change phase. The notation utilized in Alizadeh et al.'s and our proposed scheme is

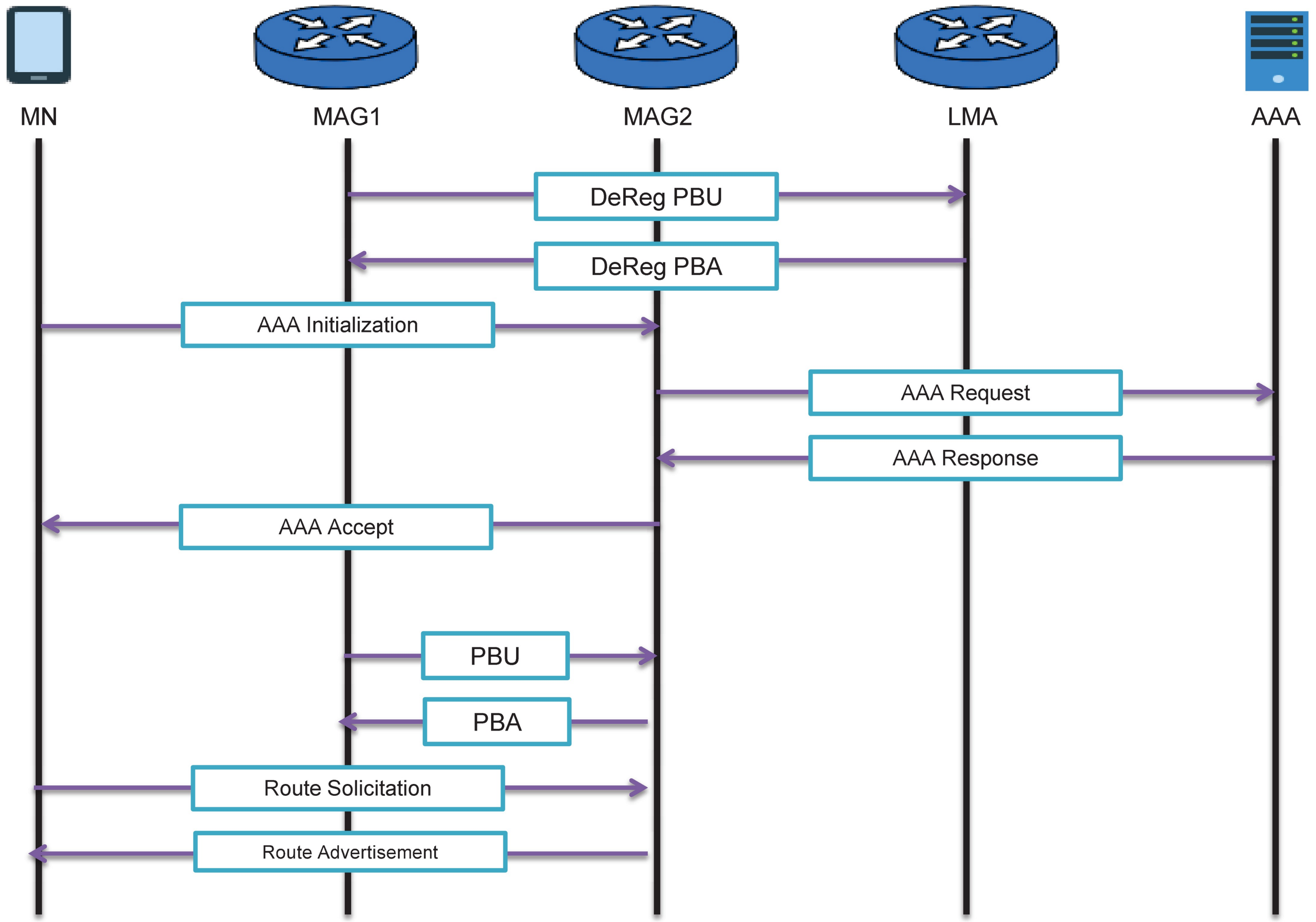


**Fig 2. Handover of PMIPv6 with an authentication.**

https://doi.org/10.1371/journal.pone.0181031.g002

summarized as Table 1. We describe each phase in detail, and Fig 3 describes Alizadeh et al.'s scheme.

## Registration phase

The MN proceeds the registration phase using the Authentication, Authorization, and Accounting (AAA), which is the authentication server, before it commences the mutual authentication phase. In a typical authentication scheme, the registration phase communicates via a secure channel between the user and the server. It is assumed that the communication on this channel is not vulnerable to eavesdropping.

1. Mobile user selects his/her identity and password $ID_{MN}$, $PW_{MN}$ and extra value $R_{MN}$.
2. MN → AAA: Mobile Node(MN) computes $RPW_{MN} = h(PW_{MN}||R_{MN})$. Then, sends $< ID_{MN}, RPW_{MN} >$ via a secure channel.
3. AAA → MN: AAA computes $S_1 = h(ID_{MN}||sv)$, $S_2 = h(RPW_{MN}) \oplus S_1$, $S_3 = E_{PSK}(ID_{MN}||sv|| a_{MN})$ where $a_{MN}$ is random nonce generated by AAA. Then, sends $< S_1, S_2, S_3, h(\cdot) >$ via a secure channel.

**Table 1. Notations used in this paper.**

| Notations | Description |
|---|---|
| $MN$ | Mobile Node |
| $MAG$ | Mobile Access Gateway |
| $AAA$ | Authentication, Authorization and Accounting |
| $ID_{MN}$ | Identity of MN |
| $PW_{MN}$ | Password of MN |
| $ID_{MAG}$ | Identity of MAG |
| $sv$ | Long term Secret key of AAA |
| $PSK$ | The symmetric pre-shared key among the MAGs and the AAA |
| $E_k(M)$ | Message M is encrypted using symmetric key *k* |
| $h(\cdot)$ | One-way hash function |
| $H(\cdot)$ | Bio-hash function |
| $\|\|$ | Concatenate operation |
| $\oplus$ | XOR operation |
| $SK_{i-j}$ | Shared session key between entity *i* and *j* |

https://doi.org/10.1371/journal.pone.0181031.t001

4. MN computes $S_4 = h(ID_{MN}||PW_{MN}) \oplus S_1$, $S_5 = R_{MN} \oplus S_1$, $S_6 = S_3 \oplus S_1$. Then, issues a new smartcard and writes $S_2$, $S_4$, $S_5$, $S_6$ into smartcard's memory.

## Mutual authentication phase

In the mutual-authentication phase, the MN checks the authenticity of the user data, such as the user identity or password, and sends an authentication request message to the MAG. The MAG also authenticates the MN, generates a session key when the authentication is passed, and transmits the authentication confirmation message to the MN again. Lastly, the MN generates a session key using the received message, and the session key is finally shared between the MN and the MAG.

1. Mobile user inserts his/her smartcard and inputs $ID'_{MN}$, $PW'_{MN}$. Smartcard computes $S'_1 = h(ID'_{MN}||PW'_{MN}) \oplus S_4$, $R'_{MN} = S'_1 \oplus S_5$, $RPW'_{MN} = h(R'_{MN}||PW'_{MN})$, $S'_2 = h(RPW'_{MN}) \oplus S_1$. Verify $S'_2$ is equal to smartcard contained value $S_2$. If this satisfies, proceeds with the next step.
2. MN → MAG: Smartcard generates random nonce $N_1$, calculates $AID_{MN} = S_1 \oplus S_6$, $AUTH_{MN} = h(S_1||N_1)$. Then, sends $< AID_{MN}, E_{S_1}(AUTH_{MN}, N_1) >$ to the MAG via public channel.
3. MAG decrypts $AID_{MN}$ using pre-shared Key(PSK) and obtains $(ID_{MN}, sv, a_{MN})$. Then, calculates $S_1 = h(ID_{MN}||sv)$ and decrypts $E_{S_1}(AUTH_{MN}, N_1)$.
4. MAG verifies $h(S_1||N_1)$ is equal to $AUTH_{MN}$. If this holds, proceeds with the next step
5. MAG → MN: MAG generates random nonce $N_2$, computes $h(N_2||ID_{MAG})$, $SK_{MN-MAG} = h(N_1||N_2)$. Then sends $E_{S_1}(N_1 + 1, N_2, ID_{MAG}, h(N_2||ID_{MAG})$ to MN.
6. MN → MAG: MN decrypts message using $S_1$. Checks $N_1 + 1$ and $h(N_2||ID_{MAG})$. MN calculates $SK_{MN-MAG} = h(N_1||N_2)$. Then, sends $(E_{SK_{MN-MAG}}(N_2 + 1))$ to MAG.
7. MAG decrypts message using $SK_{MN-MAG}$. Then, checks $N_2 + 1$.

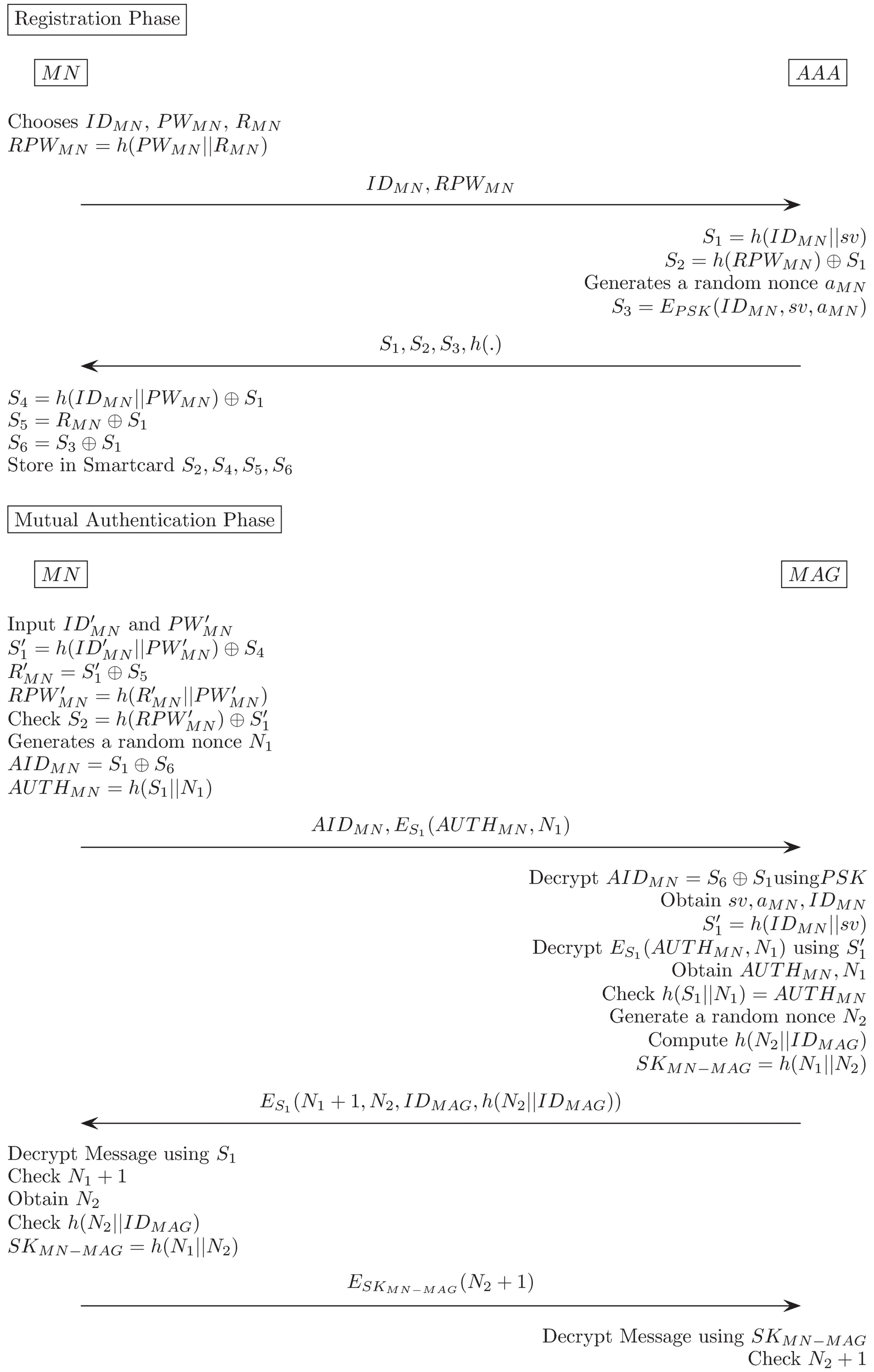

Registration Phase
$MN$
$AAA$
Chooses $ID_{MN}$, $PW_{MN}$, $R_{MN}$
$RPW_{MN} = h(PW_{MN}||R_{MN})$
$ID_{MN}, RPW_{MN}$
$S_1 = h(ID_{MN}||sv)$
$S_2 = h(RPW_{MN}) \oplus S_1$
Generates a random nonce $a_{MN}$
$S_3 = E_{PSK}(ID_{MN}, sv, a_{MN})$
$S_1, S_2, S_3, h(.)$
$S_4 = h(ID_{MN}||PW_{MN}) \oplus S_1$
$S_5 = R_{MN} \oplus S_1$
$S_6 = S_3 \oplus S_1$
Store in Smartcard $S_2, S_4, S_5, S_6$
Mutual Authentication Phase
$MN$
$MAG$
Input $ID'_{MN}$ and $PW'_{MN}$
$S'_1 = h(ID'_{MN}||PW'_{MN}) \oplus S_4$
$R'_{MN} = S'_1 \oplus S_5$
$RPW'_{MN} = h(R'_{MN}||PW'_{MN})$
Check $S_2 = h(RPW'_{MN}) \oplus S'_1$
Generates a random nonce $N_1$
$AID_{MN} = S_1 \oplus S_6$
$AUTH_{MN} = h(S_1||N_1)$
$AID_{MN}, E_{S_1}(AUTH_{MN}, N_1)$
Decrypt $AID_{MN} = S_6 \oplus S_1$using$PSK$
Obtain $sv, a_{MN}, ID_{MN}$
$S'_1 = h(ID_{MN}||sv)$
Decrypt $E_{S_1}(AUTH_{MN}, N_1)$ using $S'_1$
Obtain $AUTH_{MN}, N_1$
Check $h(S_1||N_1) = AUTH_{MN}$
Generate a random nonce $N_2$
Compute $h(N_2||ID_{MAG})$
$SK_{MN-MAG} = h(N_1||N_2)$
$E_{S_1}(N_1 + 1, N_2, ID_{MAG}, h(N_2||ID_{MAG}))$
Decrypt Message using $S_1$
Check $N_1 + 1$
Obtain $N_2$
Check $h(N_2||ID_{MAG})$
$SK_{MN-MAG} = h(N_1||N_2)$
$E_{SK_{MN-MAG}}(N_2 + 1)$
Decrypt Message using $SK_{MN-MAG}$
Check $N_2 + 1$

**Fig 3. Alizadeh et al.'s authentication scheme.**

https://doi.org/10.1371/journal.pone.0181031.g003

## Password change phase

The password change phase is performed when the user wants to change his/her password. Primarily, the smartcard first verifies the authenticity and the user then inputs his/her new password. Based on the new password, the smartcard replaces the existing values with the new password based values.

1. Mobile user inputs his/her original $ID_{MN}$, $PW_{MN}$, $R_{MN}$.
2. Smartcard computes $S_1 = h(ID_{MN}||PW_{MN}) \oplus S_4$, $R_{MN} = S_1 \oplus S_5$, $RPW_{MN} = h(R_{MN}||PW_{MN})$. Then, checks $S_2$ is same as $h(RPW_{MN}) \oplus S_1$. If holds, password change phase proceeds with the next step.
3. User inputs his/her new password and extra value $PW'_{MN}$, $R'_{MN}$.
4. Smartcard computes $RPW'_{MN} = h(PW'_{MN}||R'_{MN})$, $S'_2 = h(RPW'_{MN}) \oplus S_1$, $S'_4 = h(RPW'_{MN}||ID_{MN}) \oplus S_1$, $S'_5 = R'_{MN} \oplus S_1$, $S'_6 = S_3 \oplus S_1$.
5. Smartcard replaces $S_2$, $S_4$, $S_5$, $S_6$ new values $S'_2$, $S'_4$, $S'_5$, $S'_6$.

# Security drawbacks of Alizadeh et al.'s scheme

In this section, we point out security drawbacks of Alizadeh et al.'s scheme. Before showing the security weakness, we discuss some widely accepted threat model concerning user authentication and key agreement scheme [21–23].

1. The smartcard contains the MN and AAA's information in plaintext form. Therefore, an adversary can extract the smartcard information by monitoring the diffrential power analysis [24].
2. An adversary can eavesdrop all the message between the entities via to public channel. Additionally, He/She can modify, delete, resend the eavesdropped message.
3. An adversary can guess low entropy password and identity individually easily but guessing two secret parameters are computationally infeasible in polynomial time [25, 26].
4. An adversary may be a valid user or with the order reversed.
5. An adversary already knows all authentication scheme between MN, AAA and MAG.

Under these threat models, this study shows that Alizadeh et al.'s scheme is unable to resist against various attacks, including the offline password guessing and session-key-derived attacks.

## Leak of symmetric encryption/decryption key

Most significant weakness of Alizadeh et al.'s scheme is leak of symmetric encryption key by following steps:

1. Adversary can extract $S_6$ which in the smartcard and $AID_{MN}$ which in the login message via to public channel.
2. Adversary computes $S_1 = S_6 \oplus AID_{MN}$.

Computing value $S_1$ is the symmetric encryption key from all of the messages communicated between the MN and the MAG. Therefore, an adversary can easily encrypt or decrypt every message and attack using various security threats.

## Offline password guessing attack

If an outsider adversary $U_a$ successfully derives symmetric key $S_1$. $U_a$ can perform offline password guessing attack by following steps:

1. $U_a$ derives $R_{MN} = S_5 \oplus S_1$, which $S_5$ is in the smartcard.
2. $U_a$ selects random password candidate $PW'_{MN}$ and calculates $S'_2 = h(h(PW'_{MN}||R_{MN})) \oplus S_1$.
3. If $S'_2$ is equal to $S_2$ which is in the smartcard, adversary infers that it has guessed the MN's password accurately.
4. Otherwise, $U_a$ chooses another password nominee and performs same steps just before discover password.

## Offline identity guessing attack

If an outsider adversary $U_a$ successfully derives $MN$'s password by offline password guessing attack, $U_a$ also can do offline identity guessing attack by following steps:

1. $U_a$ selects random identity candidate $ID'_{MN}$ and calculates $S'_4 = h(ID'_{MN}||PW_{MN}) \oplus S_1$.
2. If $S'_4$ is equal to $S_4$ which is in the smartcard, adversary infers that it has guessed the MN's identity accurately.
3. Otherwise, adversary chooses another identity nominee and repeats the same steps that precede the discovery of the identity.

## MN impersonation attack

The MN impersonation attack means a outsider adversary $U_a$ has made a fake login request message that it sends to the MAG. However, MAG cannot identify it, and accepts it as a legal login request message. In Alizadeh et al.'s scheme, an adversary can make a fake login request message using the following steps:

1. Adversary $U_a$ eavesdrops $AID_{MN}$ beforehand because $AID_{MN}$ is always same as $E_{PSK}(ID_{MN}$, $sv$, $a_{MN})$. So, adversary can reuse it.
2. $U_a$ selects random nonce $N'_1$ and computes $AUTH'_{MN} = h(S_1||N'_1)$.
3. $U_a$ makes login request message $< AID_{MN}, E_{S_1}(AUTH'_{MN}, N'_1) >$ then, sends it MAG.
4. MAG decrypts message then obtains $AUTH'_{MN}, N'_1$.
5. MAG checks $AUTH'_{MN} = h(S_1||N'_1)$. Then, successfully accepts login request message which made by outsider adversary $U_a$.

## MAG impersonation attack

Similar with MN impersonation attack, MAG impersonation attack means outsider adversary $U_a$ makes fake authentication message and sends it to the MN. Also, MN can not attention it, then MN accept it is legal authentication message. MAG impersonation attack is performed by following steps:

1. Adversary $U_a$ eavesdrops $E_{S_1}(N_1 + 1, N_2, ID_{MAG}, h(N_2||ID_{MAG})$ then, acquire $ID_{MAG}$. In the same way, acquire $N_1$ from $E_{S_1}(AUTH_{MN}, N_1)$

2. $U_a$ selects random nonce $N_2'$ and computes $h(N_2'||ID_{MAG})$.
3. $U_a$ makes authentication request message $E_{S_1}(N_1+1, N_2', ID_{MAG}, h(N_2'||ID_{MAG}))$ then, sends it MN.
4. MN decrypts message then obtains $N_2'$.
5. MN successfully accepts authentication request message which made by $U_a$.

## Session key derive attack

Session key derive attack means adversary can compute session key and then use it after communication between MN and MAG. According to Alizadeh et al.'s scheme, adversary can derive session key between legal entities by following steps:

1. Adversary $U_a$ eavesdrops $E_{S_1}(N_1 + 1, N_2, ID_{MAG}, h(N_2||ID_{MAG}))$ and $E_{S_1}(AUTH_{MN}, N_1)$.
2. $U_a$ can derive $N_1$, $N_2$ by using symmetric key $S_1$.
3. $U_a$ computes session key $SK_{MN-MAG} = h(N_1||N_2)$.

Since then, adversary can communicate using derived session key either MN or MAG without registration or login.

# The proposed scheme

In this section, the scheme that is an improvement compared with Alizadeh et al.'s scheme is proposed. The proposed enhancements are described, as follows:

1. Use of a dynamic identity to satisfy the MN anonymity. The main idea is the changing of the dynamic identity to another value upon the completion of the authentication phase. Therefore, the $U_a$ cannot identify the initiation of two different sessions by the same user.
2. Use of an encryption key that the $U_a$ cannot derive without the legal user's information.
3. Use of biometric information with Bio-hashing to protect the MN's information more securely.

Our proposed scheme consists of following phases: registration, mutual authentication and password change phase.

## Registration phase

We designed a 3-factor authentication scheme by registering the user's bio information in order to enhance safety. Also, at this phase, the dynamic identity $DID_{MN}$ is created based on the random number generated by the AAA. The dynamic identity provides the MN anonymity because it is continuously changed in a mutual authentication phase that is performed later. Details procedure of registration phase is in Fig 4.

1. Mobile user selects his/her identity and password $ID_{MN}$, $PW_{MN}$ and imprints his/her biometrics $B_{MN}$.
2. MN → AAA: Mobile Node(MN) computes $RPW_{MN} = h(PW_{MN}||H(B_{MN}))$. Then, sends $< ID_{MN}, RPW_{MN} >$ via a secure channel.
3. AAA → MN: AAA computes $S_1 = h(ID_{MN}||RPW_{MN})$, $S_2 = h(a_{MN}||sv)$, $DID_{MN} = E_{PSK}(ID_{MN}, a_{MN})$, $S_3 = E_{PSK}(sv, DID_{MN}) \oplus S_2$ where $a_{MN}$ is random nonce generated by AAA. Then, AAA sends $< S_1, S_2, S_3, DID_{MN}, h(.) >$ via a secure channel.

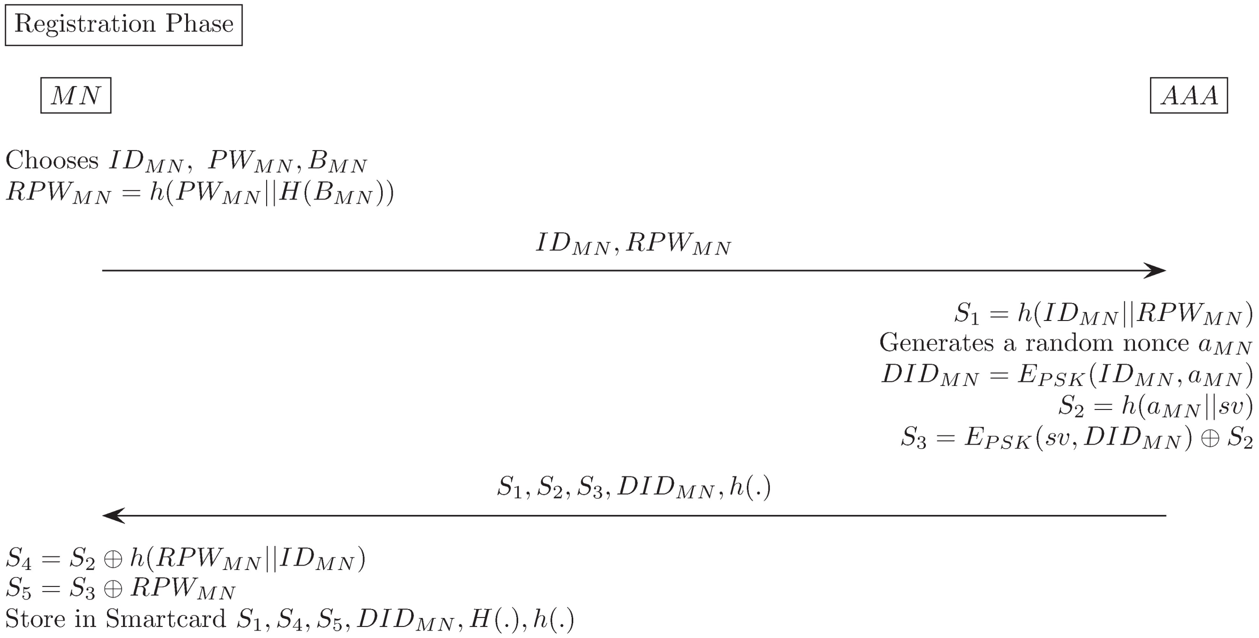

Registration Phase
$MN$
$AAA$
Chooses $ID_{MN},\ PW_{MN}, B_{MN}$
$RPW_{MN} = h(PW_{MN}||H(B_{MN}))$
$ID_{MN}, RPW_{MN}$
$S_1 = h(ID_{MN}||RPW_{MN})$
Generates a random nonce $a_{MN}$
$DID_{MN} = E_{PSK}(ID_{MN}, a_{MN})$
$S_2 = h(a_{MN}||sv)$
$S_3 = E_{PSK}(sv, DID_{MN}) \oplus S_2$
$S_1, S_2, S_3, DID_{MN}, h(.)$
$S_4 = S_2 \oplus h(RPW_{MN}||ID_{MN})$
$S_5 = S_3 \oplus RPW_{MN}$
Store in Smartcard $S_1, S_4, S_5, DID_{MN}, H(.), h(.)$

**Fig 4. Our proposed scheme(Registration phase).**

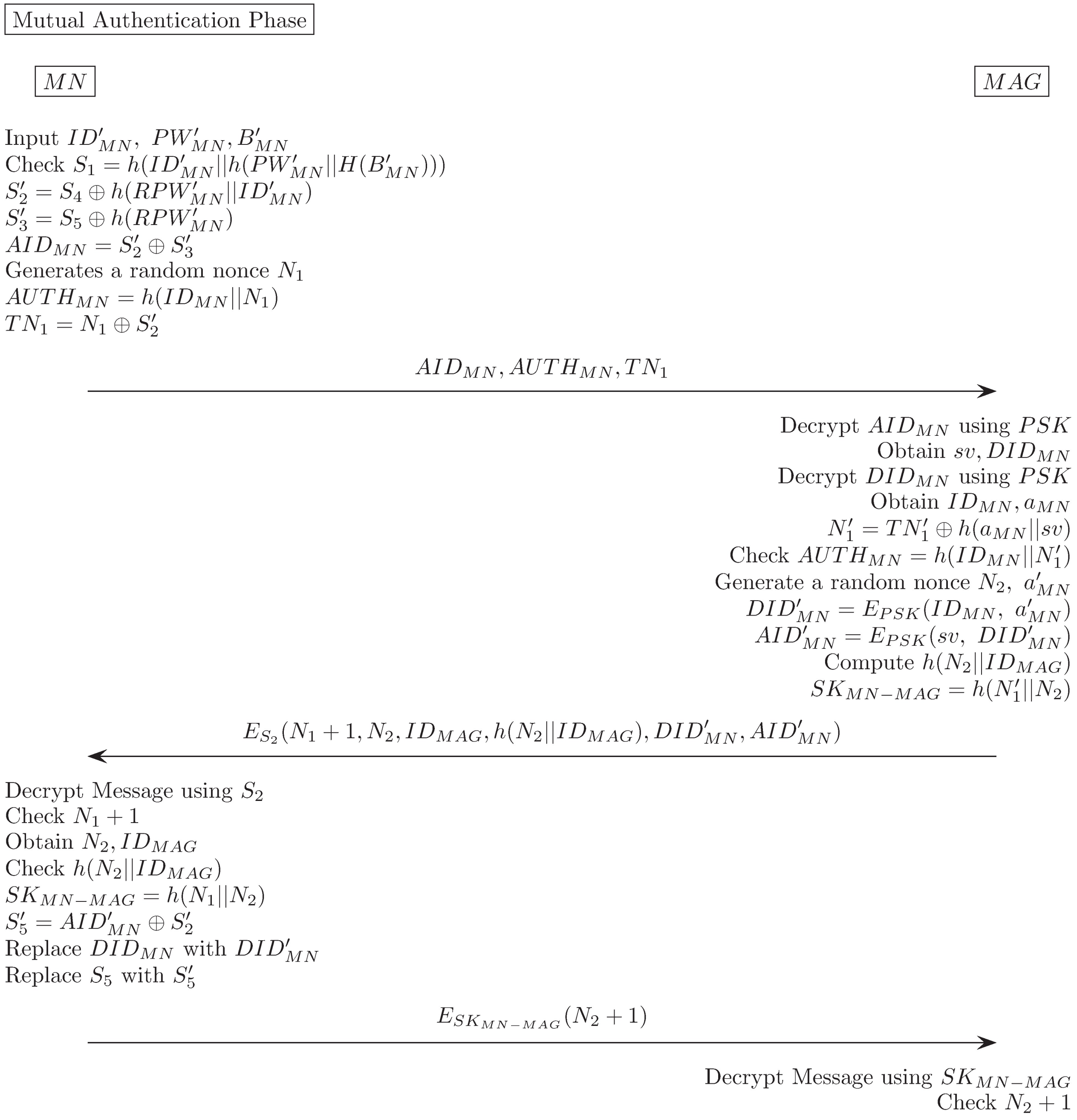
https://doi.org/10.1371/journal.pone.0181031.g004

4. MN computes $S_4 = S_2 \oplus h(RPW_{MN}||ID_{MN})$, $S_5 = S_3 \oplus RPW_{MN}$. Then, issues a new smartcard and writes $< S_1, S_4, S_5, DID_{MN}, H(.), h(.) >$ into smartcard.

## Mutual authentication phase

When an MN joins a localized mobility domain, it must pass a mutual authentication step with the MAG. To enhance the safety of the proposed method, this process prevents an attacker from deriving an encryption key even if he/she eavesdrops a public channel or extracts a smartcard's contents. In addition, once the authentication is completed, the MAG issues new dynamic identity value, $DID'_{MN}$, and the MN changes the $DID_{MN}$ value in the smartcard. Thereby, an outsider adversary can not infer that same user performs mutual authentication several times. Details procedure of mutual authentication phase is in Fig 5.

1. Mobile user inserts his/her smartcard and inputs $ID'_{MN}$, $PW'_{MN}$ and imprints his/her biometric information $B'_{MN}$. Smartcard computes $RPW'_{MN} = h(PW'_{MN}||H(B'_{MN}))$, $S'_1 = h(ID'_{MN}||RPW'_{MN})$. Then, smartcard verifies $S'_1$ is equal to smartcard contained value $S_1$. If this satisfies, proceeds with the next step.
2. MN → MAG: Smartcard generates random nonce $N_1$, calculates $S'_2 = S_4 \oplus h(RPW'_{MN}||ID'_{MN})$, $S'_3 = S_5 \oplus h(RPW'_{MN})$, $AID_{MN} = S'_2 \oplus S'_3$, $AUTH_{MN} = h(ID_{MN}||N_1)$, $TN_1 = N_1 \oplus S'_2$. Then, sends $< AID_{MN}, AUTH_{MN}, TN_1 >$ to the MAG via public channel.
3. MAG decrypts $AID_{MN}(= E_{PSK}(sv, DID_{MN}))$ using Pre-Shared Key(PSK) and obtains $(sv, DID_{MN})$. Then MAG decrypts $DID_{MN}$ using PSK once again and obtains $ID_{MN}$, $a_{MN}$. Then, MAG calculates $N'_1 = TN_1 \oplus h(a_{MN}||sv)$.
4. MAG verifies $h(ID_{MN}||N'_1)$ is equal to $AUTH_{MN}$. If this holds, proceeds with the next step.



Mutual Authentication Phase

$MN$

$MAG$

Input $ID'_{MN},\ PW'_{MN}, B'_{MN}$
Check $S_1 = h(ID'_{MN}||h(PW'_{MN}||H(B'_{MN})))$
$S'_2 = S_4 \oplus h(RPW'_{MN}||ID'_{MN})$
$S'_3 = S_5 \oplus h(RPW'_{MN})$
$AID_{MN} = S'_2 \oplus S'_3$
Generates a random nonce $N_1$
$AUTH_{MN} = h(ID_{MN}||N_1)$
$TN_1 = N_1 \oplus S'_2$

$AID_{MN}, AUTH_{MN}, TN_1$

Decrypt $AID_{MN}$ using $PSK$
Obtain $sv, DID_{MN}$
Decrypt $DID_{MN}$ using $PSK$
Obtain $ID_{MN}, a_{MN}$
$N'_1 = TN'_1 \oplus h(a_{MN}||sv)$
Check $AUTH_{MN} = h(ID_{MN}||N'_1)$
Generate a random nonce $N_2,\ a'_{MN}$
$DID'_{MN} = E_{PSK}(ID_{MN},\ a'_{MN})$
$AID'_{MN} = E_{PSK}(sv,\ DID'_{MN})$
Compute $h(N_2||ID_{MAG})$
$SK_{MN-MAG} = h(N'_1||N_2)$

$E_{S_2}(N_1+1, N_2, ID_{MAG}, h(N_2||ID_{MAG}), DID'_{MN}, AID'_{MN})$

Decrypt Message using $S_2$
Check $N_1 + 1$
Obtain $N_2, ID_{MAG}$
Check $h(N_2||ID_{MAG})$
$SK_{MN-MAG} = h(N_1||N_2)$
$S'_5 = AID'_{MN} \oplus S'_2$
Replace $DID_{MN}$ with $DID'_{MN}$
Replace $S_5$ with $S'_5$

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

Decrypt Message using $SK_{MN-MAG}$
Check $N_2 + 1$

**Fig 5. Our proposed scheme(Mutual authentication phase).**

https://doi.org/10.1371/journal.pone.0181031.g005

5. MAG → MN: MAG generates random nonces $N_2$, $a'_{MN}$, computes $DID'_{MN} = E_{PSK}(ID_{MN}, a'_{MN})$, $AID'_{MN} = E_{PSK}(sv, DID'_{MN})$, $SK_{MN-MAG} = h(N'_1||N_2)$. Then MAG sends $E_{S_2}(N_1+1, N_2, ID_{MAG}, h(N_2||ID_{MAG}), DID'_{MN}, AID'_{MN})$ to MN via public channel.

6. MN decrypts message using $S'_2$. Checks $N_1 + 1$ and $h(N_2||ID_{MAG})$. Then, MN calculates $SK_{MN-MAG} = h(N_1||N_2)$, $S'_5 = AID'_{MN} \oplus S'_2$. Further, MN replaces $DID_{MN}$ with $DID'_{MN}$ and $S_5$ with $S'_5$.

7. MN → MAG: MN sends $(E_{SK_{MN-MAG}}(N_2 + 1))$ to MAG.
8. MAG decrypts message using $SK_{MN-MAG}$. Checks $N_2 + 1$.

### Password change phase

1. Mobile user inputs his/her original identity, password and biometric information $ID_{MN}$, $PW_{MN}$, $B_{MN}$.
2. Smartcard computes $RPW_{MN} = h(PW_{MN}||H(B_{MN}))$ checks $S_1$ is same as $h(ID_{MN}||RPW_{MN})$. If holds, password change phase proceeds with the next step.
3. User inputs his/her new password $PW'_{MN}$.
4. Smartcard computes $RPW'_{MN} = h(PW'_{MN}||H(B_{MN}))$, $S'_1 = h(ID_{MN}||RPW'_{MN})$, $S'_4 = S_4 \oplus h(RPW_{MN}||ID_{MN}) \oplus h(RPW'_{MN}||ID_{MN})$, $S'_5 = S_5 \oplus RPW_{MN} \oplus RPW'_{MN}$.
5. Smartcard replaces $S_1$, $S_4$, $S_5$ new values $S'_1$, $S'_4$, $S'_5$.

## Security analysis of the proposed scheme

In this section, the proposed scheme is analyzed using the following two methods: informal analysis and formal analysis. The informal analysis proves that the proposed scheme is secure against many security threats compared with the other existing schemes. On the other side, using BAN logic, the formal analysis shows the proposed scheme's generation of the session key's legality to the entities who take part in the proposed scheme.

### Informal security analysis

In this subsection, we check our proposed scheme is safe with various secure threat, and satisfies some basic requirements to design authentication scheme.

**Insider attack.** The insider attack is performed by someone who is in the server's side and then guesses the user's password from the registration message. However in our proposed scheme, MN sends user's password to server in a form of $RPW_{MN} = h(PW_{MN}||H(B_{MN}))$. In this case, server's insider is not able to guess password because password is protected with bio-hash value based on user's biometric.

**MN anonymity.** An authentication scheme is said to satisfy anonymity if it can satisfy two main conditions: (1) User's identity is not disclose to adversary and (2) the adversary cannot find out two different sessions are initiated by same user [27, 28]. In Our proposed scheme, we use dynamic identity $DID_{MN} = E_{PSK}(ID_{MN}, a_{MN})$. Additionally, after a authentication phase, *MAG* computes new dynamic identity $DID'_{MN} = E_{PSK}(ID_{MN}, a'_{MN})$ and sends it. New dynamic identity is protected by encryption key $S_2$ known only MAG and MN. Then, *MN* replaces the previous $DID_{MN}$ with received $DID'_{MN}$, and calculate new $S'_5$ which contains new dynamic identity. In conclusion, outsider adversary can not figure out two different sessions are initiated by the same user.

**Provide mutual authentication.** Our proposed scheme provides mutual authentication between *MN* and *MAG*. Mutual authentication means there are processes that each entity completes to authenticate the other party during the progression of the protocol. In our proposed scheme *MAG* checks *MN*'s legality by checking derived $AUTH_{MN}$ is equal to receiving value. The other way, *MN* checks *MAG*'s legality by checking derived $h(N_2||ID_{MAG})$ is equal to receiving value. Additionally, *MN* can check *MAG*'s legality by $N_1 + 1$ whether *MAG* can derive *MN* generated nonce $N_1$.

**Resistant to stolen-verifier attack.** Several authentication schemes comprise a verification table that stores some of the user information. However, the use of a verification table can cause overhead problems in the server's side and a vulnerability to the stolen-verifier attack. However, the proposed scheme does not need to store any information during the entire phase, and this means it prevents not only the AAA overhead but also the stolen-verifier attack.

**Resistant to MN impersonation attack.** To do *MN* impersonation attack, adversary need to make $AID_{MN}$, $AUTH_{MN}$, $TN_1$. However $AID_{MN}$ is encrypted text with pre-shared-key, $AUTH_{MN}$ is mixed $ID_{MN}$, $TN_1$ is mixed with *AAA*'s secret key *sv* and *AAA* generated random nonce $a_{MN}$. So, even though adversary $U_a$ generates his/her own random nonce $N_1'$, $U_a$ can not make any require value which sends to *MAG*. Therefore, our proposed scheme prevents *MN* impersonation attack.

**Resistant to MAG impersonation attack.** To do *MAG* impersonation attack, adversary needs to make $S_2$ to encrypt message. However $S_2$ is mixed with *AAA*'s secret key *sv* and *AAA* generated random nonce $a_{MN}$. Like the preceding attack, even though adversary $U_a$ can not derive $E_{S_2}(N_1 + 1, N_2, ID_{MAG}, h(N_2||ID_{MAG}), DID'_{MN}, AID'_{MN})$ normally. Therefore, our proposed scheme prevents *MAG* impersonation attack.

**Resistant to replay attack.** *MN* and *MAG* generate random nonce $N_1$, $N_2$ during our proposed scheme process to resist replay attack. When adversary $U_a$ eavesdrops login message $< AID_{MN}, AUTH_{MN}, TN_1 >$ then resends it. In this case $U_a$'s login request is rejected by *MAG*, because our proposed scheme can expose an wrong number by contrasting $AUTH_{MN}$. Supplementary, our proposed scheme uses various numbers when each session begins. Therefore, our proposed scheme can resist replay attack.

**Resistant to Denial-of-service attack.** Denial-of-service(DOS) attack is occurred by adversary's continuous wrong login requests. If *MN*'s identity, password verification process is in the *MAG*'s side, adversary inputs wrong identity and password in succession. In this circumstance, *MAG* is received a lot of login request message. As a result, *MAG* is overloaded by adversary. To prevent this attack, our proposed scheme checks *MN*'s identity and password in *MN*'s smartcard side. So, when adversary inputs wrong information, smartcard rejects login request in *MN*'s side quickly. As a result, our proposed scheme resists Denial-of-service attack.

**Resistant to MN guessing attack.** According to our proposed scheme, adversary who guess *MN*'s password/identity must using $S_1$'s value. Nevertheless, $S_1$ has 3 *MN*'s information, identity, password and biometric. Even if adversary can guess user's identity and password at same time in polynomial time, there is a precondition that adversary already knows *MN*'s biometric information. But, it is not possible to know *MN*'s biometric information in our scheme. Therefore, our scheme resist *MN* guessing attack.

**Does not need time synchronization.** Several authentication scheme using timestamp to resist replay attack. However, using timestamp in authentication scheme, *MN* and *MAG* have to synchronize there clock beforehand. In the synchronization process, there is possibility that time synchronization error. To prevent this problem, our proposed scheme only use random nonce based authentication instead timestamp.

**Efficient and freely password choose and change.** In our proposed scheme, *MN* user always chooses his/her password without any restriction in registration phase. Additionally, when *MN* changes his/her password in password change phase, smartcard checks the original password's legality at first. Then, *MN* can change password. In this process, the MN only needs to communicate with the smartcard and not with the MAG.

**Comparison with previous work.** Also, the proposed scheme is compared with two existing schemes regarding the PMIPv6 user authentication, as shown in Table 2. The results are described as follows.

**Table 2. Comparison between proposed scheme and other similar environment scheme.**

| Security Features | Chuang | Alizadeh | Our Proposed |
|---|---|---|---|
| Insider attack | No Resistance | Resistance | Resistance |
| MN anonymity | Not Satisfied | Not Satisfied | Satisfied |
| Mutual authentication | Satisfied | Satisfied | Satisfied |
| Stolen-verifier attack | Resistance | Resistance | Resistance |
| MN impersonation attack | Not Satisfied | Not Satisfied | Satisfy |
| MAG impersonation attack | Not Satisfied | Not Satisfied | Satisfy |
| Replay attack | Resistance | Resistance | Resistance |
| Denial-of-service attack | Resistance | Resistance | Resistance |
| MN password guessing attack | No Resistance | No Resistance | Resistance |
| Need Time synchronization | Not Needed | Not Needed | Not Needed |
| Free/Efficient password change | Satisfied | Satisfied | Satisfied |

https://doi.org/10.1371/journal.pone.0181031.t002

## Formal security analysis

Formal security analysis is usually used to analyse and judge various authentication schemes' performance [29–32]. There are many formal security analysis methods can be applied to authentication scheme such as BAN logic [33], GNY [34], AVISPA [35] and ProVerif [36]. In this paper, we used BAN logic to prove our scheme's legality.

**Authentication proof with BAN logic.** In this subsection, BAN logic is used to analyze the proposed scheme. BAN logic helps to prove whether or not a protocol does or does not meet its security goals. Also, BAN logic contributes to the improvement of the efficiency of a protocol by eliminating messages, message content, or message encryptions. The BAN-logic notation is defined in Table 3.

In order to achieve the reasonable result of BAN logic, we define some rules about introduction and elimination as follows:

- Message-meaning rule: $\frac{P|\equiv P\overset{K}{\leftrightarrow}Q, P\triangleleft<X>_K}{P|\equiv Q|\sim X}$: When $P$ sees a message which is encrypted with the shared key of $P$ and $Q$, than $P$ believes that $Q$ has sent the message. As the secret key only is known to $P$ and $Q$, only $P$ or $Q$ are able to produce the message and $P$ knows what it has said.

- Nonce-verification rule: $\frac{P|\equiv\#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$: When $P$ believes that $X$ is a fresh message, and $P$ believes that it was said by $Q$ than $P$ believes that $Q$ still believes the message $X$.

- Believe rule(1): $\frac{P|\equiv X, P|\equiv Y}{P|\equiv(X, Y)}$: A composite message can be when a principal believes in both parts, this can be generalised to more than two parts.

**Table 3. Notations.**

| Notations | Description |
|---|---|
| $P\mid\equiv X$ | $P$ believes that $X$ holds |
| $P\triangleleft X$ | $P$ sees/holds the $X$ |
| $P\mid\sim X$ | $P$ has once said $X$ |
| $P\Rightarrow X$ | $P$ has complete control over $X$ |
| $\sharp(X)$ | $X$ is fresh and recent |
| $P\overset{K}{\leftrightarrow}Q$ | $P$ and $Q$ share a secret key $K$ |
| $<X>_K$ | $X$ is encrypted with key $K$ |

https://doi.org/10.1371/journal.pone.0181031.t003

- Believe rule(2): $\frac{P|\equiv(X,Y)}{P|\equiv X,P|\equiv Y}$: A more then two message can be when a principal believes in, this can be generalised to composite message.
- Freshness-conjuncatenation rule: $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$: When a value is found to be fresh by an entity, than the entity also believes that the message, in which the value is used, is also fresh.
- Jurisdiction rule: $\frac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$: $P$ believes that the principal $Q$ jurisdiction has over the formula $X$. This means that $Q$ is trusted to make statements over $X$.

The major objective of our proposed scheme is mutual authentication between the MN and MAG with shared key. Our objectives symbolized by BAN logic are as follows:

- Objective 1. $MN\ |\equiv\ (MN\overset{sk}{\longleftrightarrow}MAG)$
- Objective 2. $MAG\ |\equiv\ (MN\overset{sk}{\longleftrightarrow}MAG)$

After establishing the main objectives, convert the message between MN and MAG to the idealized form.

- Message 1. $MN \rightarrow MAG$: $< ID_{MN} >_{S_2}, < N_1 >_{ID_{MN}}, < N_1 >_{S_2}$
- Message 2. $MAG \rightarrow MN$: $< N_2 >_{S_2}, < N_2 >_{ID_{MN}}$

Also there are some assumptions of our proposed scheme to derive proper objective.

- A1: $MAG\ |\equiv \sharp(N_1)$
- A2: $MN\ |\equiv \sharp(N_2)$
- A3: $MAG\ |\equiv MN \Rightarrow N_1$
- A4: $MN\ |\equiv MAG \Rightarrow N_2$
- A5: $MN\ |\equiv\ (MN\overset{S_2}{\longleftrightarrow}MAG)$
- A6: $MAG\ |\equiv\ (MN\overset{S_2}{\longleftrightarrow}MAG)$

Now, we describe our main proof as follows. According to Message 1, we could get:

- V1: $MAG \lhd < ID_{MN} >_{S_2}, < ID_{MN} >_{N_1}, < N_1 >_{S_2}$
  According to assumption $A_6$, we apply the message meaning rule to obtain V2 and V3.
- V2: $MAG\ |\equiv MN\ |\sim\ ID_{MN}$
- V3: $MAG\ |\equiv MN\ |\sim\ N_1$
  According to assumption $A_1$, we apply the freshness conjuncatenation rule to obtain V4.
- V4: $MAG\ |\equiv MN\ |\equiv N_1$
  According to assumption $A_3$ and V4, we apply the jurisdiction rule to obtain V5.
- V5: $MAG\ |\equiv N_1$
  According to $sk = h(N_1||N_2)$, V5 and assumption $A_3$, we derive:
- V6: $MAG\ |\equiv\ (MN\overset{sk}{\longleftrightarrow}MAG)$ **(Goal 2.)**
  According to Message 2, we could get:
- V7: $MN \lhd < N_2 >_{S_2}, < N_2 >_{ID_{MN}}$
  According to assumption $A_5$, we apply the message meaning rule to obtain V8.

**Table 4. Comparison of the computational costs between the proposed scheme and other related schemes.**

| Schemes | Registration | Mutual Authentication | Total |
|---|---|---|---|
| Chuang | $4T_h + 1T_x + 1T_s$ | $12T_h + 3T_x + 7T_s$ | $16T_h + 4T_x + 8T_s$ |
| Alizadeh | $4T_h + 4T_x + 1T_s$ | $10T_h + 5T_x + 7T_s$ | $14T_h + 9T_x + 8T_s$ |
| Proposed | $5T_h + 3T_x + 2T_s$ | $12T_h + 4T_x + 8T_s$ | $17T_h + 7T_x + 10T_s$ |

https://doi.org/10.1371/journal.pone.0181031.t004

- V8: $MN \mid\equiv MAG \mid\sim N_2$
  According to assumption $A_2$, we apply the freshness conjuncatenation rule to obtain V9.
- V9: $MN \mid\equiv N_2$
  According to $sk = h(N_1 || N_2)$, V9 and assumption $A_4$, we derive:
- V10: $MN \mid\equiv (MN \overset{sk}{\leftrightarrow} MAG)$ **(Goal 1.)**

The preceding discussion clearly shows that *MN* and *MAG* achieve mutual authentication, and based on (Goal.1) and (Goal.2), *MN* and *MAG* trust that the session key *sk* is securely shared between them.

## Performance analysis of the proposed scheme

In this section, we measure our proposed scheme's performance and compare with those of existing schemes. The notations used in this measurement are described as follows:

- $T_h$: the time of executing a one-way hash function/bio-hash function.
- $T_x$: the time of executing a XOR operation.
- $T_s$: the time of executing a symmetric encryption or decryption.

Table 4 shows a analysis of the comparison of the computational cost for our proposed scheme and existing schemes. Time comparison results show that the scheme of Chuang et al.'s scheme is $16T_h + 4T_x + 8T_s$, Alizadeh et al.'s scheme is $14T_h + 9T_x + 8T_s$, and our proposed scheme is $17T_h + 7T_x + 10T_s$. The totals of the hash-function and XOR-operation executions that were recorded for the proposed scheme are similar to those of the two existing schemes. The proposed scheme implements the dynamic identity to satisfy the user anonymity, and it needs two further symmetric-encryption and symmetric-decryption operations

Based on the results in Table 4, Crypto++ Library is used to measure the computation process time of each operation [37]. A simulation was performed to obtain the execution time of each cryptographic operation, and Table 5 shows our simulation environment.

Under this simulation environment, the value of each cryptographic operation time was measured. Table 6 shows execution time for each operation and the comparison of the total execution time between our proposed scheme and other scheme. In addition, $T_x$ is not counted

**Table 5. Simulation environment.**

| Feature | Description |
|---|---|
| Operating System | 64-bits Windows 7 |
| Compiler | Visual C++ 2013 Software |
| Cryptographic Library | Crypto++ Library, 5.6.1 |
| Processor | Intel(R) Core(TM) i5-4160 CPU, 3.60GHz |
| Memory | 8.0GB |

https://doi.org/10.1371/journal.pone.0181031.t005

**Table 6. Execution time for each operation and our scheme and other schemes.**

| Operation | Execution time | Operation | Execution time |
|---|---|---|---|
| $T_h$ | 0.48ms | $T_s$ | 0.73ms |
| Schemes | Registration | Mutual Authentication | Total amount time |
| Chuang | 2.65ms | 10.87ms | 13.52ms |
| Alizadeh | 2.65ms | 9.91ms | 12.56ms |
| Our Proposed | 3.86ms | 11.6ms | 15.46ms |

https://doi.org/10.1371/journal.pone.0181031.t006

because it is too petty compared with other operations such as symmetric encryption or hash function.

As shown in Table 6, the execution time of the our proposed scheme requires 15.46ms $(17T_h + 10T_s \approx 17 \times 0.48ms + 10 \times 0.73ms)$. The execution times for Chuang et al.'s and Alizadeh et al.'s schemes are 13.52ms $(16T_h + 8T_s \approx 16 \times 0.48ms + 8 \times 0.73ms)$ and 12.56ms$(14T_h + 8T_s \approx 14 \times 0.48ms + 8 \times 0.73ms)$, respectively. The results show that our proposed scheme's execution time is more than those of the other schemes. However, in terms of security, the other schemes show has several vulnerabilities. Contrarily, our proposed scheme implements the dynamic identity at a relatively low additional cost, to satisfy MN anonymity and provide protection against various secure attacks. Thus, our proposed scheme also takes into account the necessary efficiency.

## Conclusion

This paper shows that Chuang et al.'s scheme, which was proposed as the authentication scheme for the PMIPv6, is vulnerable to an attacker who can derive the symmetric key that is used in overall communication, and the execution of this attack is relatively simple. Then, we demonstrate how an outsider adversary can execute various security threats, such as the offline password guessing, MN impersonation, and MAG impersonation attacks, on Alizadeh et al.'s scheme. Accordingly, we propose an improved and efficient scheme using the MN user's biometric information and a dynamic identity that provide protection against the previous security drawbacks. As a result, this paper shows that the proposed scheme can prevent attacks such as the MN guessing, MAG impersonation, and session key derived attacks, and its effectiveness is also due to the fact that it does not use timestamps or verification tables. Furthermore, BAN logic shows that the proposed scheme exhibited successful and stable session-key sharing between the MN and the MAG, and it is more efficient in terms of the computational-time cost.

## Acknowledgments

I thank all of the authors, especially the corresponding author Dongho Won. I am also grateful to the anonymous reviewers for their time, priceless comments, and advice regarding this paper.

## Author Contributions

**Conceptualization:** Dongho Won.

**Data curation:** Dongwoo Kang, Jaewook Jung, Donghoon Lee, Dongho Won.

**Formal analysis:** Dongwoo Kang, Jaewook Jung, Donghoon Lee, Dongho Won.

**Funding acquisition:** Dongho Won.

**Investigation:** Jaewook Jung, Dongho Won.

**Methodology:** Jaewook Jung, Dongho Won.

**Project administration:** Jaewook Jung, Donghoon Lee, Dongho Won.

**Resources:** Dongwoo Kang, Donghoon Lee, Hyoungshick Kim, Dongho Won.

**Software:** Dongwoo Kang, Jaewook Jung, Donghoon Lee, Hyoungshick Kim.

**Supervision:** Jaewook Jung, Dongho Won.

**Validation:** Jaewook Jung, Donghoon Lee, Dongho Won.

**Visualization:** Dongwoo Kang.

**Writing – original draft:** Dongwoo Kang, Donghoon Lee.

**Writing – review & editing:** Dongwoo Kang, Jaewook Jung, Donghoon Lee, Hyoungshick Kim, Dongho Won.

## References

1. Johnson, David, Charles Perkins, and Jari Arkko. Mobility support in IPv6. No. RFC 3775. 2004;
2. Kong KS, Lee WJ, Han YH, Shin MK, You HR. Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6. IEEE Wireless communications. 2008; 15(2).
3. Giaretta, Gerardo. Interactions between proxy mobile IPv6 (PMIPv6) and mobile IPv6 (MIPv6): Scenarios and related issues. No. RFC 6612. 2012;
4. S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil. Proxy mobile IPv6. No. RFC 5213. 2008;
5. 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; 1–14.
6. Heydari M, Sadough SMS, Farash MS, Chaundhry SA, Mahmood K. An efficient password-based authenticated key exchange protocol with provable security for mobile client–client networks. Wireless Personal Communications. 2016; 88(2):337–356. https://doi.org/10.1007/s11277-015-3123-6
7. Chaudhry SA, Farash MS, Naqvi H, Islam SH, Shon T. A robust and efficient privacy aware handover authentication scheme for wireless networks. Wireless Personal Communications. 2017; 93(2): 311–335. https://doi.org/10.1007/s11277-015-3139-y
8. Jung J, Kang D, Lee D, Won D. An Improved and Secure Anonymous Biometric-Based User Authentication with Key Agreement Scheme for the Integrated EPR Information System. PloS one. 2017; 12(1):1–26 https://doi.org/10.1371/journal.pone.0169414
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. https://doi.org/10.1109/JSYST.2012.2209276
10. You I, Leu FY. Comments on "SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks". IEEE Systems Journal. 2015; 1–4
11. Alizadeh M, Baharuna S, Zamanib M, Khodadadia T, Darvishi M, Gholizadeh S, Ahmadi H. Anonymity and Untraceability Assessment of Authentication Protocols in PMIPv6. Jurnal Teknologi. 2015; 72(5): 31–34. https://doi.org/10.11113/jt.v72.3936
12. Alizadeh M, Zamani M, Baharun S, Manaf AA, Sakurai K, Anada H, Keshavarz H, Chaudhry SA, Khan MK. Cryptanalysis and improvement of "a secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks". PloS one. 2015; 10(11): 1–21.
13. J Kempf, C Vogt. Security threats to network-based localized mobility management (NETLMM). No. RFC 4832. 2007;
14. 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. https://doi.org/10.11113/jt.v72.3935
15. P Rogaway, T Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. International Workshop on Fast Software Encryption. 2004; 371–388.
16. Burrows JH. Secure hash standard. National Institute of Standards and Technology. 1995; 17–45.

17. Moon J, Choi Y, Kim J, Won D. An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. Journal of medical systems. 2016; 40(3): 70. https://doi.org/10.1007/s10916-015-0422-0 PMID: 26743628

18. Choi Y, Lee Y, Won D. Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction. International Journal of Distributed Sensor Networks. 2016; 12(1): 1–16. https://doi.org/10.1155/2016/8572410

19. Jung J, Kang D, Lee D, Won D. An Improved and Secure Anonymous Biometric-Based User Authentication with Key Agreement Scheme for the Integrated EPR Information System. PloS one. 2017; 12(1): 1–26. https://doi.org/10.1371/journal.pone.0169414

20. Jin ATB, Ling DNC, Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition. 2004; 37(11):2245–2255. https://doi.org/10.1016/j.patcog.2004.04.011

21. Tan Z. A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. Journal of medical systems. 2014; 38(3): 16. https://doi.org/10.1007/s10916-014-0016-2 PMID: 24643750

22. Liao IE, Lee CC, Hwang MS. A password authentication scheme over insecure networks. Journal of Computer and System Sciences. 2006; 72(4): 727–740. https://doi.org/10.1016/j.jcss.2005.10.001

23. Yang G, Wong DS, Wang H, Deng X. Two-factor mutual authentication based on smart cards and passwords. Journal of Computer and System Sciences. 2008; 74(7): 1160–1172. https://doi.org/10.1016/j.jcss.2008.04.002

24. Kocher P, Jaffe J, Jun B, Rohatgi P. Introduction to differential power analysis. Journal of Cryptographic Engineering. 2011; 1(1): 5–27. https://doi.org/10.1007/s13389-011-0006-y

25. Amin R, Biswas GP. A secure light weight scheme for user authentication and key agreement in multigateway based wireless sensor networks. Ad Hoc Networks. 2016; 36: 58–80. https://doi.org/10.1016/j.adhoc.2015.05.020

26. Ma CG, Wang D, Zhao SD. Security flaws in two improved remote user authentication schemes using smart cards. International Journal of Communication Systems. 2014; 27(10): 2215–2227. https://doi.org/10.1002/dac.2468

27. Chaudhry SA, Farash MS, Nagvi H, Kumari S, Khan MK. An enhanced privacy preserving remote user authentication scheme with provable security. Security and Communication Networks. 2015; 8(18): 3782–3795. https://doi.org/10.1002/sec.1299

28. Chaudhry SA, Nagvi H, Sher M, Farash MS, Hassan MU. An improved and provably secure privacy preserving authentication protocol for SIP. Peer-to-Peer Networking and Applications. 2017; 10(1): 1–15. https://doi.org/10.1007/s12083-015-0400-9

29. Farash MS, Turkanovic M, Kumari S, Holbi M. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Networks. 2016; 36: 152–176. https://doi.org/10.1016/j.adhoc.2015.05.014

30. Amin R, Kumar N, Biswas GP, Iqbal R, Chang V. A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. Future Generation Computer Systems. 2016; 1–15.

31. Sutrala AK, Das AK, Odelu V, Wazid M, Kumari S. Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems. Computer Methods and Programs in Biomedicine. 2016; 135: 167–185. https://doi.org/10.1016/j.cmpb.2016.07.028 PMID: 27586489

32. Jung J, Kim J, Choi Y, Won D. An Anonymous User Authentication and Key Agreement Scheme Based on a Symmetric Cryptosystem in Wireless Sensor Networks. Sensors. 2016; 16(8): 1299. https://doi.org/10.3390/s16081299

33. Wessels J, CMG FINANCE BV. “Application of BAN-logic.” CMG FINANCE BV 19. 2001; 1–23.

34. Mathuria AM, Safavi-Naini R, Nickolas PR. On the automation of GNY logic. Australian Computer Science Communications. 1995; 17: 370–379.

35. Vigano L. Automated security protocol analysis with the AVISPA tool. Electronic Notes in Theoretical Computer Science. 2006; 155: 61–86. https://doi.org/10.1016/j.entcs.2005.11.052

36. Blanchet, Bruno, Ben Smyth, and Vincent Cheval. “ProVerif 1.90: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial.” URL: http://prosecco.gforge.inria.fr/personal/bblanche/proverif/manual.pdf. 2015.

37. Wei Dai. 2017. Crypto++® Library. [ONLINE] Available at: https://www.cryptopp.com/. [Accessed 2 March 2017].