PLOS ONE

RESEARCH ARTICLE

A lightweight and secure two factor anonymous authentication protocol for Global Mobility Networks

Ahmed Fraz Baig[1☯]*, Khwaja Mansoor ul Hassan[1☯], Anwar Ghani[1☯], Shehzad Ashraf Chaudhry[1☯], Imran Khan[1☯], Muhammad Usman Ashraf[1,2☯]

1 Department of Computer Science & Software Engineering, International Islamic University, Islamabad, Pakistan, **2** IBMS, Agriculture University Faisalabad, Pakistan

☯ These authors contributed equally to this work.
* ahmed.mscs812@iiu.edu.pk

OPEN ACCESS

Citation: Baig AF, Hassan KMu, Ghani A, Chaudhry SA, Khan I, Ashraf MU (2018) A lightweight and secure two factor anonymous authentication protocol for Global Mobility Networks. PLoS ONE 13(4): e0196061. https://doi.org/10.1371/journal.pone.0196061

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

Received: January 3, 2018

Accepted: April 5, 2018

Published: April 27, 2018

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

Funding: The author(s) received no specific funding for this work.

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

Abstract

Global Mobility Networks(GLOMONETs) in wireless communication permits the global roaming services that enable a user to leverage the mobile services in any foreign country. Technological growth in wireless communication is also accompanied by new security threats and challenges. A threat-proof authentication protocol in wireless communication may overcome the security flaws by allowing only legitimate users to access a particular service. Recently, Lee et al. found Mun et al. scheme vulnerable to different attacks and proposed an advanced secure scheme to overcome the security flaws. However, this article points out that Lee et al. scheme lacks user anonymity, inefficient user authentication, vulnerable to replay and DoS attacks and Lack of local password verification. Furthermore, this article presents a more robust anonymous authentication scheme to handle the threats and challenges found in Lee et al.'s protocol. The proposed protocol is formally verified with an automated tool(ProVerif). The proposed protocol has superior efficiency in comparison to the existing protocols.

1 Introduction

The wireless communications are extensively used in current decade, the internet based applications are accessed by mobile networks at anytime and from anywhere. Nowadays, roaming in mobile communication become extremely famous. Due to the technological improvements many security issues have been raised up because anyone can intercept the communication anytime. While traveling, the mobility services assure that wireless devices are connected with a network without any breakage of connection. When a person visits some other country he/she has to use the mobile services. Global Mobility Networks(GLOMONETs) facilitates a roaming user to leverage their home mobile services in a foreign country [1]. A roaming Mobile Node(MN) uses the mobile services at foreign country with the help of their home country network. Mobile Node(MN) connects to a foreign network in foreign country and

Foreign Node(FN) verifies the legitimacy of the Mobile Node(MN) through his/her home network by Home Node(HN)as shown in Fig 1.

Authentication in wireless environment essential and decisive task. Authentication is the only source that ensures the Mobile Node(MN) is a legitimate node [2]. A valid and threat-proof authentication is required for prevention of illegal usage. numerous symmetric, asymmetric and lightweight hash, XOR based authentication schemes are proposed to to provide mutual authentication, node anonymity and to handle different security flaws in GLOMONETs [3–15]. A threat-proof authentication fulfills following requirements: Node anonymity (R1); Node Traceability(R2); Man-in-Middle attack(R3); Backward/Forward secrecy(R4); Replay and Dos attacks(R5); Known-key attacks(R6); Friendliness(R7); Local node and Password verification(R8); Insider attacks(R9); Mutual authentication(R10); Impersonation attacks(R11).

Suzuki et al. [16] in 1997 presented a distributed security based authentication scheme to enable a user to access mobile services in foreign country. Zhu et al. [17] in 2004 presented an authentication protocol that facilitates the features of mutual authentication and implicit mutual secret-key management. Lee et at. [18] disclosed that Zhu et al. [17] scheme is incapable to attain the feature of mutual authentication, moreover, scheme does not resist backward secrecy and impersonation attacks. Lee et al. [18] presented an enhanced authentication protocol to efficiently resolve the imperfections of scheme [17]. Later, the Wei et al. [19]also notified that Zhu et al. [17] scheme inefficient to achieve the user anonymity and also discloses secret

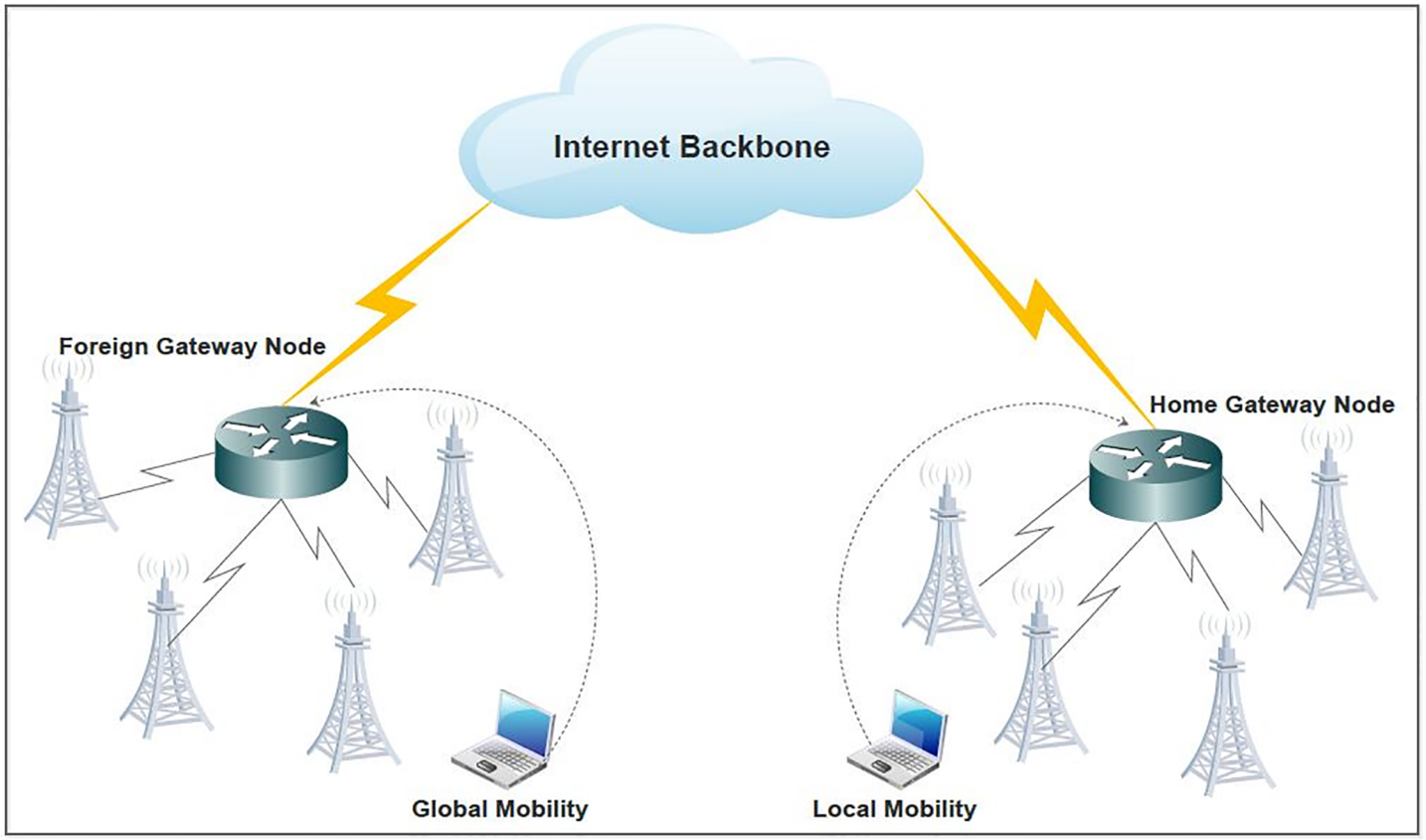

Fig 1. Global mobility networks authentication.

https://doi.org/10.1371/journal.pone.0196061.g001

information. To overcome these issues the Wei et al. [19] presented a more enhanced protocol that provides secure features like user anonymity and mutual authentication. Wu et al. [20] also found Lee et al. [18] protocol does not achieve the backward secrecy, user anonymity and vulnerable to off-line key guessing attacks. Thus, Wu et al. [20] proposed an efficient protocol that provides resistance of aforementioned attacks. He et al. [21] notified that Wu et al. [20] protocol unable to achieve user anonymity and also vulnerable to replay and forgery attacks. Therefore, He et al. [21] presented a lightweight authentication scheme with the features of strong resistance of stolen verification attacks. Li et al. [22] pointed out He et al. [21] protocol unable to provide the features of user anonymity and also provides unfair key-exchange system. Li et al. [22] presented a protocol that provides the feature of user anonymity and fair key-agreement system. Li et al. [23] pointed out Li et al's [22] protocol is inefficient due to extra computational cost. Das. [24] also pointed out Li et al. [22] protocol cannot withstand the replay attacks. Yoon et al. [25] presented a new lightweight authentication protocol to handle the loopholes of different protocol with the features of mutual authentication, user friendliness, User anonymity. Niu et al. [26] pointed out the Yoon et al. [25] protocol and proved that protocol does not provide user anonymity and also has an insecure key management system. Therefore, Niu. [26] presented a novel based authentication protocol that provides the feature of user anonymity. Jiang et al. [27] also pointed out that He et al. protocol [21] does not provide strong of two-factor authentication furthermore, the protocol is vulnerable to insider attack, replay attack and failure of user friendliness. The present protocol of Jiang et al. [27] improves the privacy and authentication. Wen et al. [28] proved Jiang et al. [27] protocol does not resist the replay attack and password based verification-attack. Wen et al. [28] presented new protocol that does not enable the users to share the secret-key. Mun et al. [29] presented a new hash and concatenation operation based lightweight scheme. Lee et al. [30] found Mun et al. [29] scheme cannot withstand man-in-the middle attack, masquerade attack and perfect forward secrecy They proposed a more efficient protocol for GLOMNET.

This article notifies that the Lee et al. [30] scheme lacks unfair user registration, inefficient user authentication, unable to provide local user/password verification and vulnerable to replay and DoS attacks.

2 Contributions

In this article a detailed analysis of Lee et al. protocol has been presented to check its strengths against various attacks. As a result the following improvements are contributed:

1. Various security weaknesses of the Lee et al. protocol have been identified and elaborated in this paper.
2. A new and lightweight protocol has been proposed in this article which resists different possible attacks and provides the requirement of user friendliness.
3. The proposed protocol has been formally verified using an automated tool "ProVerif" to ensure its security strength.
4. Finally, the proposed protocol has been analyzed for computation and communication efficiency showing better performance than its counterpart protocols.

3 Brief review of Lee et al. scheme

Lee et al. presented a lightweight authentication using simple hash operation, XOR and concatenation operations. This section presents precise review of four phases of Lee et al. scheme

Table 1. Notations guide.

Notation	Description	Notation	Description
MN	Mobile Node	HN	Home Node
FN	Foreign Node	T_A	Timestamps of entity A
FH_k	Pre-shared key between FN and HN	SK	Session key
$h(.)$	one way hash function	$\oplus$	The XOR operation
ΔTS	Expected time interval for transmission delay	$\|\|$	The concatenation operation

https://doi.org/10.1371/journal.pone.0196061.t001

[30] in following sequence: registration phase, AESK phase, the session key update phase, and the password alter phase. The notation guide is given in Table 1.

3.1 Registration phase

The registration phase of Lee et al. scheme is between Mobile Node(MN) and Home Node (HN). The Mobile Node(MN) and Home Node(HN) perform the registration in following steps:

Step 1: The Mobile Node(MN) chooses {password PW_{MN}, nonce s} and computes EID = $h(ID_{MN} \oplus PW_{MN}) \oplus s$. Afterward MN forwards a message $M = \{EID\}$ to the Home Node (HN) over a secure channel.

Step 2: The Home Node(HN) obtains the message M calculates $S = h(EID||h(SK_{HN}))$ and sends S to MN

Step 3: Upon receiving S the MN computes $SPW = S \oplus h(PW_{MN})$. Finally the MN stores SPW and s in smartcard(SC).

3.2 Authentication and establishment of session-key(AESK Phase)

AESK phase of Lee et al. [30] is performed in following steps:

Step 1: $MN \rightarrow FN$: $M_1 = \{EID', V_{MN}, Q_{MN}, N_{MN}\}$
The Mobile Node(MN) calculates $EID' = h(ID_{MN} \oplus PW_{MN}) \oplus s$ and $S' = h(EID||h(SK_{HN}))$. MU chooses two nonce s_{new}, N_{MN}. Afterward MN calculates following values $EID_{new} = h(ID_{MN} \oplus PW'_{MN}) \oplus s_{new}$, $V_{MN} = EID_{new} \oplus h(S'||N_{MN})$ and $Q_{MN} = h(EID_{new}||S'||N_{MN})$. Ultimately, a login request message $M_1 = \{EID', V_{MN}, Q_{MN}, N_{MN}\}$ is forwarded to Foreign Node(FN).

Step 2: $FN \rightarrow HN$: $M_2 = \{EID', V_{MN}, Q_{FN}, N_{MN}, V_{FN}, ID_{FN}\}$
After receiving the message M_1 Foreign Node FN generates a nonce N_{FN} and calculates $Q_{FN} = h(Q_{MN}||N_{FN}||SK_{FN})$, $V_{FN} = N_{FN} \oplus h(SK_{FN})$. The Foreign Node FN sends the message $M_2 = \{EID', V_{MN}, Q_{FN}, N_{MN}, V_{FN}, ID_{FN}\}$ to Home Node(HN)

Step 3: $HN \rightarrow FN$: $M_3 = \{V_{HN}\}$
Upon receiving the message M_2 the HN computes $S' = h(EID'||h(SK_{HN}))$ and afterward computes $EID'_{new} = V_{MN} \oplus h(S' \parallel N_{MN})$ and retrieves EID'_{new}, after that HN computes $SK_{FN} = h(ID_{FN} \oplus SK_{HN})$, $N_F = V_F \oplus h(SK_{HN})$. Afterward HN verifies $Q_{FN} \stackrel{?}{=} h(h(EID'_{new} \parallel S' \parallel N_{MN}) \parallel N_{FN} \parallel SK_{FN})$ for authentication of Mobile Node(MN) and Foreign Node(FN). Furthermore Home Node(HN) computes $S_{new} = h(EID_{New}||h(SK_{HN})$, $V_{HN} = (EID_{new}||S||S_{new}) \oplus h(SK_{FN}||N_{FN})$ and forwards M_3 to FN.

Step 4: $FN \rightarrow MN$: $M_4 = \{V_{FN2}, Q_{FN2}, N_{FN2}\}$
Upon receiving M_3, FN derives $(EID_{new}||S||S_{new})$ and verifies $Q_{MN} \stackrel{?}{=} h(EID_{new} \parallel S' \parallel N_{MN})$ if the verification holds then Foreign Node(FN) authenticates the Mobile Node(MN) and Home Node(HN). Afterward FN generates a nonce and computes $V_{FN2} = S_{new} \oplus h(S||N_{FN2})$, $Q_{FN2} = h(EID||S_{new}||N_{FN2})$ and transmits M_4 to Mobile Node(MN).

Step 5: Upon receiving the M_4 the Mobile Node(MN) calculates S_{new} and checks $Q_{FN2} \stackrel{?}{=} h(EID||S_{new} \parallel N_{FN2})$ to authenticate the Foreign Node(FN). Afterward the FN updates $SPW_{new} = S_{new} \oplus h(PW_{MN})$ for further use. For a session communication Mobile Node(MN) computes $K_{FM} = h(N_{MN}||N_{FN2}||S)$, $Q_{MF} = h(N_{MN}||S||N_{FN2}||S_{new})$ and sends Q_{MF} to Foreign Node(FN) for reconfirmation.

Step 5: FN verifies $Q_{MF} \stackrel{?}{=} h(N_{MN} \parallel S \parallel N_{FN2} \parallel S_{new})$ and computes $K_{FM} = h(N_{MN}||N_{FN2}||S)$ for the communication of current session.

3.3 Session-Key update phase

Step 1: The Mobile Node(MN) selects a nonce N'_{MN} and calculates $U_{MN} = N_{MN} \oplus h(S||N_{MN}||N_{FN2})$, $Q'_{MN} = h(N'_{MN} \oplus S)$ and transmits Q'_{MN}, U_{MN} to FN

Step 2: The Foreign Node(FN) computes $N'_{MN} = U_{MN} \oplus h(S \parallel N_{MN} \parallel N_{FN2})$ and checks Q'_{MN}. Afterward, FN selects a nonce and calculates $U_{FN} = N'_{FN} \oplus h(S \parallel N_{FN2} \parallel N'_{MN})$, $Q'_{FN}h(N_{FN} \oplus S)$. Afterward, FN transmits U_{FN} and Q'_{FN} to MN.

Step 3: Mobile Node(MN) receives message and calculates $N'_{FN} = U_{FN} \oplus h(S \parallel N_{FN2} \parallel N_{MN})$. Afterward, MN update $K'_{FM} = h(N'_{MN} \parallel N'_{FN} \parallel S)$, $Q'_{MF} = h(N'_{MN} \oplus N_{FN} \oplus S)$ and transmits Q'_{MF} to FN

Step 3: Foreign Node(MN) verifies $Q'_{MF} \stackrel{?}{=} h(N'_{MN} \oplus N_{FN} \oplus S)$ and updates $K'_{FM} = h(N'_{MN} \parallel N'_{FN} \parallel S)$ and completes update phase.

3.4 Password alter phase

Step 1: Lee et al. scheme enables a Mobile Node(MN) to update his/her password. When a Mobile Node(*MN*) desires to update the password, the Mobile Node(MN) has to login with ID_{MN} and password PW_{MN}.

Step 2: MN uses new password and calculates $EID_{new} = h(ID_{MN}) \oplus PW_{New}) \oplus S_{New}$. Furthermore, for authentication and establishment phase SPW_{New} is computed and S_{New} is encrypted with old password PW_{MN}, $SPW_{New} = S_{New} \oplus PW_{MN}$ and for this phase the new password PW_{New} is used to encrypt S_{New}, $SPW_{New} = S_{New} \oplus PW_{New}$. At the end password is altered successfully.

4 Security weaknesses of Lee et al. scheme

This section demonstrates the security weakness of Lee et al. scheme [30]. The Lee et al. scheme suffers unfair user registration, inefficient user authentication, vulnerable to replay and DoS attacks furthermore, the Lee et al. scheme does not provide local user and old password verification. The detailed discussion is given in following subsections:

4.1 Unfair user registration and inefficient user authentication

The Lee et al. Scheme suffers with a serious flaw in registration phase. The Mobile Node(MN) computes $EID = h(ID_{MN} \oplus PW_{MN}) \oplus s$ and sends EID to Home Node(HN) for registration in step1. Whereas, the Mobile Node(MN) takes one way hash(OWH) of ID_{MN} and password PW_{MN}. When the Home Node(HN) receives registration request message EID, the HN would not be able to extract the identity ID_{MN} form EID because there is no such mechanism of de-hashing. Hence, the Home Node(HN) would be unable to recognize user at the registration time and the registration request would be rejected.

In AESK phase of Lee et al. Scheme the Home Node(HN) receives login request through Foreign Node(FN) sent by Mobile Node(MN). The identity of MN is saved in EID'. To authenticate the Mobile Node(HN) the Home Node(HN) searches for Identity of Mobile Node(MN) in database. Hence, the ID_{MN} does not exist in Home Node(HN) database and Home Node (HN) cannot recognize the user has sent the login request as a result the Home Node(HN) will reject the authentication request.

4.2 Replay and DoS attacks

In Lee et al. Scheme an adversary A will intercept the channel and will obtain login-request message $M_1 = \{EID', V_{MN}, Q_{MN}, N_{MN}\}$. As no timestamp or sequence number is associated with login message M_1 the Adv A can replay M_1 in login phase latter on. Likewise the adversary A will perform the replay attacks in step2 with $M_2 = \{EID', V_{MN}, Q_{FN}, N_{MN}, V_{FN}, ID_{FN}\}$, step3 with $M_3 = V_{HN}$ and in step4 with $M_4 = \{V_{FN2}, Q_{FN2}, N_{FN2}\}$ of authentication phase because any no timestamps or sequence numbers are used with any message. Although, the adversary A is unable to compute the session key but adversary A will send too many login requests intentionally to overwhelm the MN, FN and HN. Simultaneous repetition of replay attacks in large numbers can exhaust the communication and computation cost and also leads to Denial of service(DoS)attacks that may cause the prevention of access the resource to legal user.

4.3 Lack of local user and password verification

Lee et al. scheme does not verify old password in phase 5 password alter phase. Any malicious user with a stolen Smartcard(SC) can submit request to change the password. Although the malicious user would not be succeed in this process but He/she can send multiple requests which also lead to DoS as discussed previously. Furthermore, suppose in login phase a Mobile Node(MN) unintentionally, inputs ID_{MN} and old PW_{MN}. Before transmitting the login request to Home Node(HN) the scheme does not verify the identity ID or password PW are correct or incorrect in login phase. Even if the user enters old password PW_{MN} for login, the authentication steps(1-4)can still be executed with old ID/PW. Although, at step 4 the Home Node(HN) would reject authentication but this process takes unnecessary computation and communication overhead. Hence, the smartcard(SC) cannot verify the the identity and password of Mobile Node(MN) at login phase which proves inefficiencies in Lee et al. scheme.

5 Proposed scheme

Proposed scheme includes of following phases: registration phase, login and authentication phase and password change phase. The detailed description of these phases is as following:

5.1 Registration phase

The registration phase of proposed scheme is between Mobile Node(MN) and Home Node (HN). In registration phase the Mobile Node(MN) freely chooses an Identity ID_{MN}, password

PW_{MN} and a random number $r \in Z_n^*$(natural number). Afterward the *MN* computes $U = h(PW_{MN}||r)$ and transmits a registration request message to *HN* $M = \{ID_{MN}, U\}$ on secure channel.

When the Home Node(*HN*) receives the registration request message he/she selects a random number $m \in Z_n^*$ and computes the following:

$$B = U \oplus h(ID_{MN} \parallel m) \quad (1)$$

$$N_{MN} = h(U \parallel R_T) \oplus ID_{MN} \quad (2)$$

Where R_T is the registration time, after that the Home Node(*HN*) stores $\{B, N_{MN}, m, h(.)\}$ in SC and afterward the smart card(SC) is issued to *MN* through a reliable network channel.

The Mobile Node *MN* regenerates *r* and stores it in smartcard(SC). Now $\{B, U, r, h(.)\}$ are stored in SC database.

5.2 Login and authentication phase

For the authentication phases we presume, the Mobile Node(*MN*) is in foreign country under the administration of foreign network. The Mobile Node(MN) intends to use the mobile services in foreign area. To avail the mobile services in foreign region the Mobile Node(*MN*) has to login with Identity ID_{MN}, password PW_{MN} and afterward for the security and legitimacy he/she will authenticate himself/herself with the help of their Foreign Node(*FN*) and Home Node (*HN*) in a proper manner as shown in Fig 2. After the successful authentication Mobile Node (*MN*) will use the services with collaboration hosted country's network.

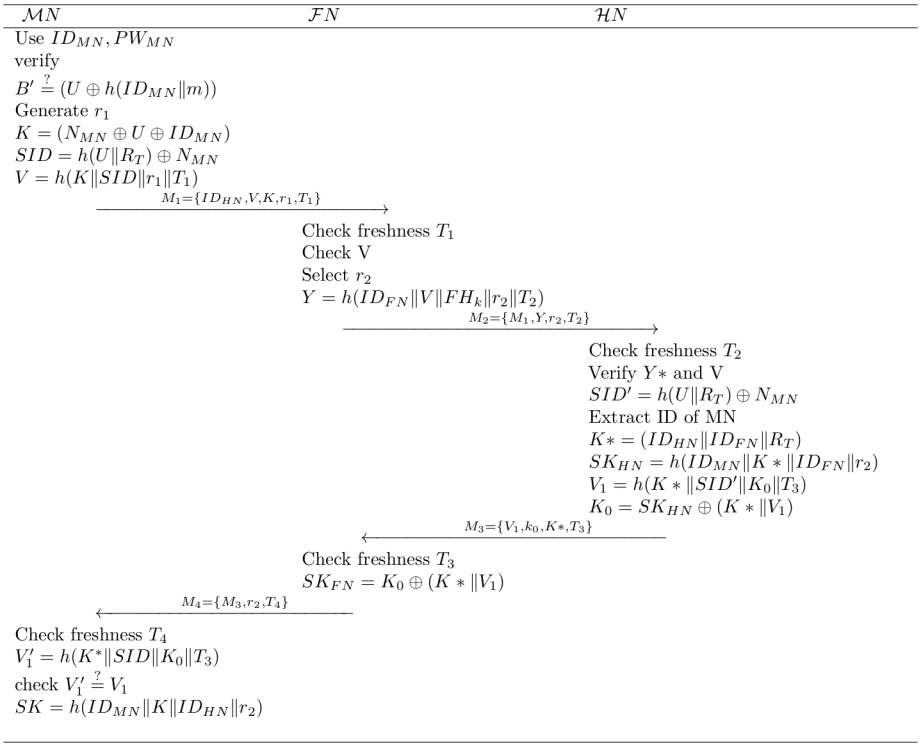

Fig 2. Login and mutual authentication phase of proposed scheme.

https://doi.org/10.1371/journal.pone.0196061.g002

Step 1: $MN \rightarrow FN$: $M_1 = \{ID_{HN}, K, V, r_1, T_1\}$

In first step the user *MN* puts his/her smart card(SC) into the machine and uses his/her identity ID_{MN} and password PW_{MN} for login, on login request the machine calculates $B' = U \oplus h(ID_{MN} \| m)$ that was saved at the registration phase and afterward *MN* compares whether $B' \stackrel{?}{=} B$ if no then session is terminated and login request is rejected. If both B' and B are same then the legality holds. The smartcard(SC) chooses random number r_1 and calculates the following:

$$K = (N_{MN} \oplus U \oplus ID_{MN}) \tag{3}$$

$$SID = h(U \parallel R_T) \oplus N_{MN} \tag{4}$$

$$V = h(K \parallel SID \parallel r_1 \parallel T_1) \tag{5}$$

Where, T_1 is timestamp of Mobile Node(MN). Ultimately, *MN* sends login request message M_1 to Foreign Node(*FN*) over a public channel.

Step 2: $FN \rightarrow HN$: $M_2 = \{M_1, Y, r_2, T_2\}$

After receiving the message *M*1 Foreign Node(FN) checks the freshness of T_1 if the comparison fails, *FN* does not accept the login request. Afterward Foreign Node(FN) generate a nonce r_2, and calculates the following equations:

$$Y = h(ID_{FN} \parallel V \parallel FH_k \parallel r_2 \parallel T_2) \tag{6}$$

Where, FH_k is a pre-shared key between FN and HN. Afterward Foreign Node(*FN*) transmits the M_2 to Home Node(*HN*).

Step 3: $HN \rightarrow FN$: $M_3 = \{V_1, k_0, K^*, T_3\}$.

When *HN* obtains M_2, the Home Node *HN* confirms the freshness of timestamp T_2 and afterward, verifies both values $V' \stackrel{?}{=} V$ and $Y* \stackrel{?}{=} Y$ if comparison do not match, the Home Node(HN) rejects M_2 and terminates the session. Afterward Home Node(HN) generates a nonce r_3 and compute following values:

$$SID' = h(U \parallel R_T) \oplus N_{MN} \tag{7}$$

$$\begin{aligned} SID' &= \cancel{h(U \parallel R_T)} \oplus \cancel{h(U \parallel R_T)} \oplus ID_{MN} \\ SID' &= ID_{MN} \\ K* &= h(ID_{HN} \parallel ID_{FN} \parallel R_T) \end{aligned} \tag{8}$$

$$SK_{HN} = h((ID_{MN}) \parallel K* \parallel ID_{FN} \parallel r_3) \tag{9}$$

$$V_1 = h(K* \parallel SID' \parallel K_0 \parallel T_3) \tag{10}$$

$$K_0 = SK_{HN} \oplus (K* \parallel V_1) \tag{11}$$

When the Home Node verifies all step then $M_3 = \{V_1, k_0, K^*, T_3\}$ is sent to Foreign Node (*FN*).

Step 4: $FN \rightarrow MN$: $M_4 = \{M_3, r_2, T_4\}$

When *FN* obtains message M_3, he/she confirms the freshness T_3 if freshness fails the *FN*

rejects the message, otherwise the Foreign Node(*FN*) computes the following equations:

$$\begin{aligned} SK &= (K_0 \oplus (K* \parallel SID \parallel V') \\ &= SK \oplus (\cancel{K^* \parallel SID \parallel V'}) \oplus (\cancel{K^* \parallel SID \parallel V'}) \\ &= SK \end{aligned} \tag{12}$$

After that for further processing the message $M_4 = \{M_3, r_2, T_4\}$ is transmitted to Mobile Node(*MN*).

Upon receiving the message M_4 The Mobile Node *MN* confirms the freshness of T_3 if time-stamp is fresh then checks $V_1' \stackrel{?}{=} h(K^* \parallel SID' \parallel T_3)$ if the resultant values do not match, then the Mobile Node(MN) terminates the session. Otherwise authentication procedure is completed by Foreign Node(*FN*) and Home Node(*HN*). Afterward, for further communication the Mobile Node(*MN*) computes the session key as following in equation:

$$SK = h(ID_{MN} \parallel K \parallel ID_{HN} \parallel r_2) \tag{13}$$

5.3 Password change phase

The password change phase makes the scheme user friendly and enhances the security of the proposed scheme. Our proposed scheme allows the user to update or change their password. Whenever the Mobile Node(*MN*) requests to change the password he/she has to perform the following steps:

Step 1: Proposed scheme allows the user to Alter or update the password. When a user with a smartcard(SC) wants to change the password. The user has to login with his/her identity ID'_{MN} and enters the password PW'_{MN} and performs following steps:

Step 2: On the request the smartcard(SC) executes and verifies the following steps:

$$U^* = h(PW'_{MN} \parallel r') \tag{14}$$

After the calculation of U^* smart card checks whether $U* \stackrel{?}{=} U$. If the values of U^* and U are not same then SC reject the request otherwise, it requests the Mobile Node(MN) to choose another new password PW_{new}.

Step 3: The Smartcard(SC) calculates the following equations:

$$B* = (U* \oplus h(PW_{new} \parallel m)) \tag{15}$$

$N^*_{MN} = h(ID_{MN} \| ID_{HN} \| R_T \oplus U^*)$ where, $\{B, U, N_{MN}\}$ are replaced with $\{B^*, U^*, N^*_{MN}\}$ and smartcard(SC) carries $\{B^*, U^*, r', h(.)\}$.

Security analysis

This section shows the formal and informal security analysis of proposed scheme. We have analyzed formal verification of proposed scheme with automated tool ProVerif and informally analyzed the scheme against different attacks.

5.4 Security analysis with ProVerif

ProVerif [31] may be defined as an automated reasoning software tool or verifier, which verifies cryptographic protocols. The ProVerif handles different cryptographic primitives like:

```
(* --------- Channels ----------*)
free ChSec:channel [private].  (*secure channel between MN and HN*)
free ChPub:channel.            (*public channel between MN,FN and HN*)

   (*———— Constants and Variables ————*)

free IDMN :bitstring.
free IDFN :bitstring.
free IDHN :bitstring.
free PWMN : bitstring [private].
free FHk :bitstring [private].

   (*————————-Constructors and Equation——-*)

fun h(bitstring):bitstring.
fun Inverse(bitstring):bitstring.
fun Concat(bitstring,bitstring):bitstring.
fun XOR(bitstring,bitstring):bitstring.
fun Mult(bitstring,bitstring):bitstring.
equation forall a:bitstring; Inverse(Inverse(a))=a.
equation forall a:bitstring, b:bitstring; XOR(XOR(a,b),b)=a.
(*-------Events---------*)
event start_MN(bitstring).
event end_MN(bitstring).
event start_FN(bitstring).
event end_FN(bitstring).
event start_HN(bitstring).
event end_HN(bitstring).
```

Fig 3. 1(a).

https://doi.org/10.1371/journal.pone.0196061.g003

Encryption/decryption, MAC, signatures, hash, Symmetric and asymmetric key cryptography and many others [33]. The formal verification of proposed protocol is tested with this tool, the detailed description of code and results are given below.

The proposed scheme uses two channels one channel "ChSec" is a secure channel which is used between MN and HN in registration phase. Whereas, "ChPub" is called a public or insecure channel. The ChPub is used is login and authentication phase. The Fig 3 1(a) elaborates channels, Constructs and events used in proposed scheme. In Fig 4 1(b) following authentication properties are verified: The query 1 is used to verify whether the session key is secure or not. The query 2 is used for the verification process 1, It determines whether event of Mobile Node(MN) started and terminated successfully or not. The query 3 is used for the verification process 2, It determines whether event of Foreign Node(FN) started and terminated successfully or not. The query 4 is used for the verification process 3, It determines whether event of Home Node(HN) started and terminated successfully or not. Furthermore, we introduced six events, every event represents start and end of each process. Furthermore, Figs 5 1(c), 6 1(d) and 7 1(e) contain full code of three processes(MN, FN and HN)

```
(*-------queries------*)
free SK:bitstring [private].
query attacker(SK).
query id:bitstring; inj-event(end_MN(IDMN)) ==> inj-event(start_MN(IDMN)).
query id:bitstring; inj-event(end_FN(IDFN)) ==> inj-event(start_FN(IDFN)).
query id:bitstring; inj-event(end_HN(IDHN)) ==> inj-event(start_HN(IDHN)).
```

Fig 4. 1(b).

https://doi.org/10.1371/journal.pone.0196061.g004

```
(*---------------Mobile Node--------*)
(*-----------*registration*-----------*)
let  pMN=
(* Registration *)
new r :bitstring;
let U = h(Concat(PWMN,r)) in
out(ChSec,(IDMN,U));
in (ChSec,(B:bitstring,NMN:bitstring));
(*-------------MN login--------------*)
event start_MN(IDMN);
new m :bitstring;
if (B=XOR(U,(h(Concat(IDMN,m))))) then
new r1: bitstring;
new T1: bitstring;
new T3: bitstring;
new TR :bitstring;
let K = XOR(NMN,U) in
let SID = XOR(XOR(h(Concat(U,TR)),K) ,NMN) in
let V = h(Concat(K,(SID,r1,T1))) in
out(ChPub,(IDHN,V,K,r1,T1));
in (ChPub,(V1:bitstring,xr2:bitstring,xT3:bitstring));
let xSK= h(h(Concat(IDMN,(K,IDFN,T3)))) in
event end_MN(IDMN)
else
 0.
```

Fig 5. 1(c).

https://doi.org/10.1371/journal.pone.0196061.g005

```
(*--------------------Foreign Node---------------------*)

let pFN=
event start_FN(IDFN);
in(ChPub,(xIDHN:bitstring,SID:bitstring,
V:bitstring,K:bitstring,T1:bitstring));
new r2 :bitstring;
new T2 :bitstring;
new T3: bitstring;
new T4: bitstring;
let Y= h(Concat(IDFN,(FHk,r2,T2))) in
out(ChPub,(V,IDHN,r2,T1,Y,r2,T2));
in (ChPub,(V1:bitstring,K0:bitstring,Kstar:bitstring,
xT3:bitstring));
let V1' =  h(Concat(Kstar,(SID,T3))) in
if  V1' =  h(Concat(Kstar,(SID,T3))) then
let SKFN= XOR(K0,Concat(Kstar,(SID,V1)))in
out(ChPub,(V1,K0,T3,r2,T4));
event end_FN(IDFN)
else
0.
```

Fig 6. 1(d).

https://doi.org/10.1371/journal.pone.0196061.g006

The automatic tool ProVerif returns true or false result, When a protocol do not prove the any of the required property then this tool return false result otherwise it returns true result. The results of proposed scheme are shown in Fig 8 1(f) and further elaboration is stated below:

The result 1 demonstrates that process of Home Node(HN) with identity ID_{HN} has successfully started and terminated The result 2 demonstrates that process of Foreign Node(FN) with identity ID_{FN} has successfully started and terminated The result 3 demonstrates that process of Mobile Node(MN) with identity ID_{MN} has successfully started and terminated The result 4 presents the attacker does not access the session-key(*SK*). However, all results demonstrates that the proposed scheme preserves the secrecy and authentication.

All processes (!pHN) | (!pFN) | (!pMN) are executed parallel.

5.5 Informal security analysis

This section presents the informal security analysis of proposed scheme, The detailed discussions about different attacks and counter measurements to withstand these attacks are stated in subsections:

5.5.1 Node anonymity. Anonymity is considered a valuable factor in secure authentication protocol, identity of Mobile Node(MN) should not reveal to anyone except the authorized participants. A secure protocol protects personal data and sensitive information of a node so, an attacker/adversary could not analyze any information that can help to breach the security requirements. Our proposed scheme achieves the anonymity requirements because we used

```
(*------------Home Node----------*)
let pHN=
(*---- Registration ----*)
in (ChSec,(xIDMN:bitstring,U:bitstring));
new m:bitstring;
let B = XOR(U,Concat(IDMN,m))in
let NMN =XOR(h(Concat(U,RT)),IDMN) in
out(ChSec, (B,NMN));
(*-------Authentication-process------*)
in (ChPub,(V:bitstring,Y:bitstring,r2:bitstring,
K:bitstring,T2:bitstring));
event start_HN(IDHN);
new T3: bitstring;
new T1: bitstring;
new TR: bitstring;
let SID' = XOR(XOR(h(Concat(IDMN,TR)),K) ,IDMN) in
let Kstar= Concat(IDHN,(IDFN,TR)) in
let SKHN = h(Concat(IDMN,(Kstar,IDFN,r2,SID'))) in
let V1 =  h(Concat(Kstar,(SID',T3))) in
let K0 = XOR(SKHN,Concat(Kstar,(SID',V1))) in
out (ChPub,(V1,K0,T3));
event end_HN(IDHN)
else
0.
```

Fig 7. 1(e).

https://doi.org/10.1371/journal.pone.0196061.g007

strong encryption techniques in our proposed scheme we used hash function in registration phase, $M = \{ID_{MN}, U\}$ is sent through secure and reliable channel and we used random numbers that protects our messages. In login-authentication phase lets suppose adversary A captures the message M_1 and tires to attain the ID_{MN} but, identity of Mobile Node is saved in SID and $SID = h(U||R_T) \oplus N_{MN}$, Adversary A cannot extract SID, we can say that our proposed scheme achieves all requirements of Mobile Node(MN) anonymity.

5.5.2 Node traceability. For a secure protocol traceability is vulnerable issue because, the node traceability may leads to many attacks. Our scheme does not disclose login information or previous history because we used random numbers(r_1, r_2, m). Hence in our scheme Mobile Node(MN) is untraceable.

5.5.3 Man in the middle attack. In this type of attack the malicious adversary $\mathcal{A}$ illegitimately intercepts two parties Communication. The Adversary can capture the sensitive data/information, can send or receive data anytime and may impersonate both parties by pretending Himself/Herself a legal user. In our proposed scheme adversary or attacker cannot perform the Man-In-Middle attack because our proposed scheme provides mutual authentication and endpoint authentication at each side. In our proposed scheme we used the timestamps of each

```
Completing equations...
Completing equations...
1-- Query inj-event(end_HN(IDHN[])) ==> inj-event(start_HN(IDHN[]))
Completing...
Starting query inj-event(end_HN(IDHN[])) ==> inj-event(start_HN(IDHN[]))
RESULT inj-event(end_HN(IDHN[])) ==> inj-event(start_HN(IDHN[])) is true.
2-- Query inj-event(end_FN(IDFN[])) ==> inj-event(start_FN(IDFN[]))
Completing...
Starting query inj-event(end_FN(IDFN[])) ==> inj-event(start_FN(IDFN[]))
RESULT inj-event(end_FN(IDFN[])) ==> inj-event(start_FN(IDFN[])) is true.
3-- Query inj-event(end_MN(IDMN[])) ==> inj-event(start_MN(IDMN[]))
Completing...
Starting query inj-event(end_MN(IDMN[])) ==> inj-event(start_MN(IDMN[]))
RESULT inj-event(end_MN(IDMN[])) ==> inj-event(start_MN(IDMN[])) is true.
4-- Query not attacker(SK[])
Completing...
Starting query not attacker(SK[])
RESULT not attacker(SK[]) is true.
```

Fig 8. 1(f).

https://doi.org/10.1371/journal.pone.0196061.g008

participant with every message $\{M_1, M_2, M_3, M_4\}$ first time difference is checked at each end if time difference is valid then session begins else more we used random numbers so adversary $\mathcal{A}$ cannot guess any secret nor the adversary can compute the session key in addition, proposed scheme provides fair *SK* establishment. Thus, Our proposed scheme can withstand the Man-In-Middle attack.

5.5.4 Backward and forward secrecy. Proposed scheme fulfills backward and forward secrecy requirements due to random numbers and freshly generated timestamps(T), with every new session random numbers and timestamps are freshly generated. So, if current communication keys are revealed to some malicious user, it is not possible to predict previous or future communication key with current keys. the Adversary $\mathcal{A}$ can neither generate same random number nor $\mathcal{A}$ can generate fresh timestamps. Hence, Adversary $\mathcal{A}$ may not compute the *SK*. Therefore we can say that our proposed-scheme accomplishes backward/forward secrecy.

5.5.5 Replay attacks. In replay attacks the malicious user repeats or delays the transmission. There are three participants in Global-Mobility-Networks *MU*, *FNandHN* who authenticate each other and four messages are transmitted among them $\{M_1, M_2, M_3, M_4\}$ over a public channel. Lets assume an adversary A captures the M_1 and try to perform the replay attacks to FN. On M_1 FN compares the timestamps if it is valid then message is accepted otherwise message would be rejected by FN if adversary generates a timestamps T_1 and timestamp comparison becomes true then adversary tries to compute V' which is impossible for adversary because adversary has no knowledge of values saved in V' so adversary cannot forge FN. Similarly we used timestamps with all messages M_2, M_3, M_4 and timestamps(TS) comparison at each session also some other comparisons of different values at different sessions so, an adversary cannot replay any message. Furthermore, without knowing ID_{MN} an adversary is unable to compute the *SK*. Due to following reasons, our proposed-scheme can resist the replay attacks.

5.5.6 Known key attacks. An Adversary $\mathcal{A}$ performs known key attacks when he/she finds palintext associated with ciphertext and the malicious attacker simply perform back-tracking operations to trace the plaintext. As stated in previous subsections our proposed scheme uses fresh random numbers and timestamps for each sessions the random numbers are freshly generated. Furthermore, all participants create the session key independently. If an attacker gets the previous session key He/She cannot compute recent session key. Hence, the proposed scheme resists the known-key-attacks.

5.5.7 User friendliness. A secure and useful protocol fulfills requirements of a user friendliness, this means to enable a user to freely pick out his/her identity, password. User friendly schemes provide freedom to change or update his/her password to enhance the security and privacy.

Proposed scheme permits the users to select an identity *ID* and password *PW* freely. Whereas, the SC verifies the inputs and correctness. A User may freely generate the nonce and also can change or updates his/her password so password may keep save from attackers and adversaries.

5.5.8 Local user and password verification. To avoid the illegal access proposed scheme provides the password verification in login-authentication phase and also in password change phase. In registration phase the Mobile Node(*MU*) computed $U = (PW_{MN} \| r)$ and then computes $B = U \oplus h(ID_{MN} \| m)$ where, in login-authentication phase is re-verified locally if $B' \stackrel{?}{=} B$ then the login phase proceeds to next step otherwise session in aborted. So, by using local password-verification we enhanced our proposed scheme more secure.

5.5.9 Insider attacks. Insider attack may defined as malicious network attack that is committed by an authorized person with legal access. In our proposed scheme let's suppose some insider of Home Node(*HN*) tries to attain the password of Mobile User(*MU*) by registration message $M = \{ID_{MN}, U\}$. The insider of Home Node(HN) can see the message *M* but could not compute the *U* whereas, $U = h(PW_{MU} \| r)$. The user password is concatenated with a nonce and have been hashed with one-way-hash function. Hence, the insider cannot achieve nonce *r* and it is infeasible for any one to compute password from hash value. So, by following assumptions we say that proposed scheme may prevent the insider attacks.

5.5.10 Stolen-verifier attacks. Proposed scheme resist the stolen-verifier-attacks as, the Mobile Node(*MN*) stored the user's password in encrypted format even the HN and FN cannot get any information about the user password. If SC is stolen then no one can extract the password because password is save in *U* and this value is in encrypted form, adversary cannot alter the password. Hence, proposed scheme can resist the stolen-verifier attacks.

5.5.11 Mutual authentication. Mutual authentication is robust feature of an authentication protocol, which enables the participants of a protocol to mutually authenticates each other at the same time. Proposed scheme furnished all conditions of mutual authentication between participants *MN*, FN and HN.

- *MN* and *HN* Mutual authentication:

In our proposed scheme *MN* authenticates the *HN* by verifying the $V_1^{'} \stackrel{?}{=} V_1$ in step 4 and Home Node(HN) confirms the *MU* by checking $V_1^{'} \stackrel{?}{=} h(K^* \| SID' \| K_0 \| T_3)$ in step 2 only a legitimate user can compute $V_1^{'}$ where both participants transfer the secret parameter ID_{MN} with each other also both participants compute the SK mutually so *MN* and FN authenticates each other mutually in proposed scheme.

- *HN* and *FN* Mutual authentication:

Likewise FN and HN authenticates each other in step 3 HN verifies $Y^* \stackrel{?}{=} Y$ where Y is computed by real Foreign Node FN. a Pre-shared key FH_k is used to secure the Y. In step 3 FN is

authenticated by HN, afterward session key(SK) is computed mutually so, our proposed scheme provides the mutual authenticity of FN and HN.

- *FN* and *MN* Mutual authentication:

FN authenticates *MN* in step 1 by checking $V \stackrel{?}{=} h(K \parallel SID \parallel r_1 \parallel T_1)$ there is $MN's$ time-stamp and only a legal *MN* can compute V. So, after the verification of $V \stackrel{?}{=} V$ the Foreign Node(FN) authenticates *MN*.

5.5.12 Impersonation attacks. Impersonation attack means an adversary may forge a legitimate user by pretending himself/herself a legal user. Adversary/attacker can delete or modify any message in different manners or can forge the other participants by pretending their self a legitimate user. In proposed scheme we withstand the forgery attacks in following ways as stated in subsections:

- *MN* Impersonation attacks:

Suppose the adversary $\mathcal{A}$ intercepts the login message $M_1 = \{ID_{HN}, V, K, r_1, T_1\}$ in step 1. When session terminates the Adversary A can try to send login message M_1 to FN. When Adversary A transmits login request message M1 the Foreign Node(FN) confirms freshness of T_1 as, timestamps is not fresh the login request will not be accepted by FN. The adversary can generate a new timestamp $\overline{T_1}$ and resend $M_1 = \{ID_{HN}, V, r_2, K, \overline{T_1}$ with fresh $\overline{T_1}$ to FN. FN confirms the freshness of T_1 the freshness comparison may successful this time. For further confirmation FN scrutinizes whether $V \stackrel{?}{=} h(K \parallel SID \parallel r_1 \parallel T_1)$. Here the values of V is not equal to V' so request will be rejected. Adversary may also try to impersonate in step 4 but due to comparison of V1' with V1 the adversary will fail to play the impersonation game in each phase.

- FN Impersonation attacks:

In step 2 adversary will try to impersonate the Home Node(HN) by sending message $M_2 = \{M_1, Y, r_2, T_2\}$. Without knowing the pre-shared key FH_k the adversary cannot impersonate the FN. Moreover proposed protocol also scrutinizes the differentiation of $Y^* \stackrel{?}{=} Y$ in second phase. Furthermore the HN and FN share the SK secretly. The adversary will not be able to impersonate HN or FN by any mean or by any message.

- HN Impersonation attacks:

Proposed protocol can efficiently withstand HN forgery attacks. If the adversary attempts to forge the MN or FN with the message $M_3 = \{V_1, k_0, K^*, T_3\}$ in third phase. In M_3 we used V_1 for local verification hence, the adversary cannot compute the values of V_1. Thus, proposed protocol can easily withstand the HN impersonation in different steps.

6 Security requirements and performance analysis

This section presents the requirements analysis and computation cost analysis of our proposed scheme. The first subsection provides the comparison of different security requirements and the second subsection demonstrates computation cost analysis, cost comparison and execution time comparison with other schemes.

6.1 Security requirements

To evaluate the different security requirements, this article compares following security requirements with with Yoon et al. [25], Mun et al. [29] and Lee et al. [30] scheme. R1:Node anonymity; R2:Node Traceability; R3:Man-in-the Middle attack; R4:Backward/Forward

Table 2. Security Requirements.

Schemes	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13
Yoon et al.	0	0	1	1	1	0	0	0	0	1	1	1	0
Mun et al.	0	1	0	0	1	0	1	0	1	1	1	0	0
Lee et al.	0	1	1	1	0	1	1	0	1	1	1	0	0
Proposed Scheme	1	1	1	1	1	1	1	1	1	1	1	1	1
1: Provides, 0: Does not Provide													

https://doi.org/10.1371/journal.pone.0196061.t002

secrecy; R5:Replay and Dos attacks; R6:Known-key attacks; R7:User friendliness; R8:Local User and Password verification; R9:Insider attacks; R10:Mutual authentication; R11:Impersonation attacks; R12: Efficiency in user authentication; R13:Formal Verification. As shown in Table 2 only our proposed protocol fulfills all security requirements. Furthermore, this article provides user friendliness, mutual authentication and also formally tested with a well-known verification tool ProVerif. The detailed comparison shown in Table 2.

6.2 Computation cost analysis

The main focus of the proposed protocol is to safeguard against various security attacks and issues present in the Lee et al. proposal for global mobility networks. In addition, the proposed protocol provides a realistic solution which guarantees reasonable computational cost. In this subsection, a comparison of the protocol with the security protocols of Mun et al. and Lee et al. has been presented based on the number of the state of the art XOR operation, concatenation and hash encryption used in these protocols. The detailed notation guide for each terminology is given in Table 3. For analyzing the proposed protocol in terms of computation cost on the security front, Kilinc and Yanik [32] experimental measurements have been adopted for different encryption operation and functions. According Kilinc and Yanik [32] single Hash encryption utilize 0.0023ms of time in computation. As shown in Table 4, Mun et al. protocol contain 11 times hash encryption, 8-times XOR operation, 4-times Elliptic-curve Point Multiplication(ECMP) and generates the random number 5-times, which in total is $11T_h + 8T_{\oplus} + 5T_{RG} + 2T_{SE} + 4T_{PM}$. Similarly, total computation cost of Gope et al. is $21T_h + 16T_{\oplus} + 3T_{RG}$,

Table 3. Notations guide for computation cost.

CC_{MN}:	Computation-cost of *MN*	T_h	One-way-hash operation
CC_{HN}:	Computation-cost of *HN*	$T_{\oplus}$	XOR operation
CC_{FN}	Computation-cost of *FN*	T_{RG}	Random number generation
CC_{total}	Total Computation-cost	T_{PM}	Elliptic curve Point Multiplication
T_{SE}	Symmetric Encryption	T_{SD}	Symmetric Decryption

https://doi.org/10.1371/journal.pone.0196061.t003

Table 4. Computation Cost.

Schemes	CC_{MN}	CC_{HN}	CC_{FN}	CC_{Total}
Mun et al.	$3T_h + 2T_{\oplus} + 2T_{RG} + 1T_{SE} + 2T_{PM}$	$5T_h + 4T_{\oplus} + 1T_{RG}$	$3T_h + 2T_{\oplus} + 2T_{RG} + 1T_{SE} + 2T_{PM}$	$11T_h + 8T_{\oplus} + 5T_{RG} + 2T_{SE} + 4T_{PM}$
Gope et al.	$6T_h + 4T_{\oplus} + 1T_{RG}$	$10T_h + 8T_{\oplus} + 1T_{RG}$	$5T_h + 4T_{\oplus} + 1T_{RG}$	$21T_h + 16T_{\oplus} + 3T_{RG}$
Lee et al.	$12T_h + 11T_{\oplus} + 3T_{RG}$	$10T_h + 3T_{\oplus} + 0T_{RG}$	$10T_h + 4T_{\oplus} + 2T_{RG}$	$32T_h + 18T_{\oplus} + 5T_{RG}$
Chaudhry et al.	$5T_h + 2T_{\oplus} + 2T_{RG}$	$3T_h + 4T_{\oplus} + 0T_{RG} + 2T_{SE} + 1T_{SD}$	$1T_h + 0T_{\oplus} + 0T_{RG} + 1T_{SE} + 1T_{SD}$	$8T_h + 6T_{\oplus} + 3T_{RG} + 3T_{SE} + 2T_{SD}$
Proposed Scheme	$6T_h + 4T_{\oplus} + 2T_{RG}$	$5T_h + 5T_{\oplus} + 1T_{RG}$	$1T_h + 1T_{\oplus} + 1T_{RG}$	$12T_h + 10T_{\oplus} + 4T_{RG}$

https://doi.org/10.1371/journal.pone.0196061.t004

and the computation cost of Lee et al. protocol is $32T_h + 18T_{\oplus} + 5T_{RG}$, The computation cost of Chaudhry et al. is $8T_h + 6T_{\oplus} + 3T_{RG} + 3T_{SE} + 2T_{SD}$. However, total computation cost of the proposed protocol is equal to $12T_h + 10T_{\oplus} + 4T_{RG}$ as shown in Table 4. Moreover, execution time of Mun et al. is 0.0345 and with ECMP it takes total 4.4865ms, the total execution time of Gope et al. scheme is 0.0483ms, the total execution time of Lee et al. scheme is 0.0736ms, Chaudhry et al. scheme takes 0.0414ms and total execution time of our proposed scheme is 0.0276ms the graphical representation of execution time is shown in Fig 9. It is quite clear from the comparison Table 4 and Fig 9 that the proposed scheme has efficient performance. In addition, our proposed scheme satisfies all security requirements using minimum encryption operations and functions. The proposed security protocol successfully attains mutual authentication, node anonymity and have strong resistance against different security attacks.

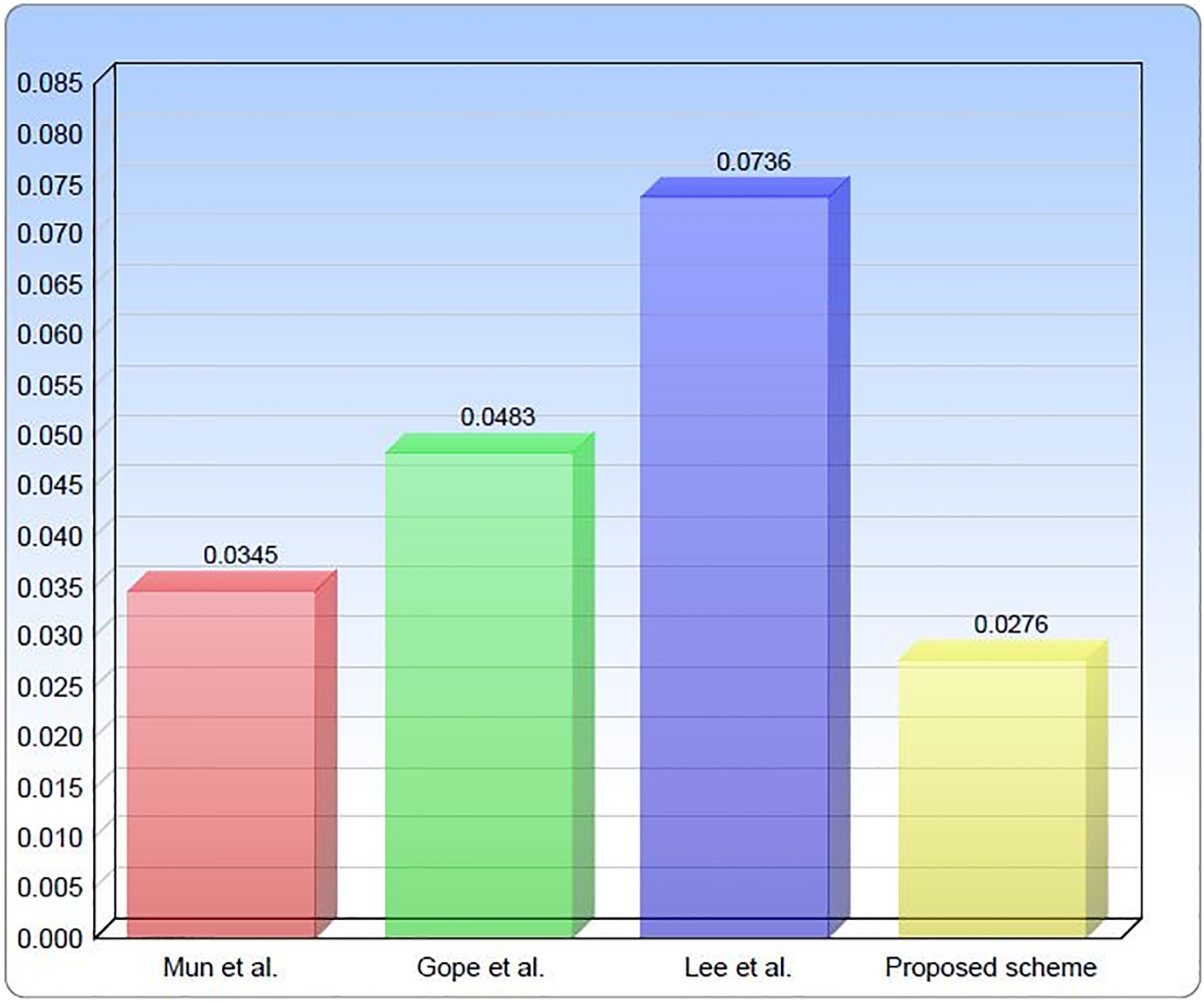

Fig 9. Execution time and performance comparison.

https://doi.org/10.1371/journal.pone.0196061.g009

7 Conclusion

This article scrutinized Lee et al.'s authentication scheme. It has been disclosed that Lee et al. scheme suffers with different security weaknesses. We propose a lightweight and secure two-factor authentication protocol, based on lightweight cryptographic primitives functions such as XOR operations, one-way hash(owh) and concatenation operation. The formal protocol Verification is tested with ProVerif a well known automated tool that confirms the correctness of the proposed scheme and informal security analysis demonstrates that the proposed scheme can withstand different attacks. Security comparison and performance analysis show that the proposed scheme is resistant against all possible attacks and it has very efficient performance making it suitable for practical environment.

Author Contributions

Conceptualization: Ahmed Fraz Baig, Shehzad Ashraf Chaudhry.

Data curation: Ahmed Fraz Baig, Imran Khan, Muhammad Usman Ashraf.

Formal analysis: Ahmed Fraz Baig, Khwaja Mansoor ul Hassan, Anwar Ghani, Muhammad Usman Ashraf.

Investigation: Ahmed Fraz Baig.

Methodology: Ahmed Fraz Baig, Khwaja Mansoor ul Hassan, Anwar Ghani, Shehzad Ashraf Chaudhry, Imran Khan.

Resources: Ahmed Fraz Baig.

Supervision: Anwar Ghani, Shehzad Ashraf Chaudhry.

Validation: Ahmed Fraz Baig, Anwar Ghani, Imran Khan.

Visualization: Ahmed Fraz Baig, Imran Khan, Muhammad Usman Ashraf.

Writing – original draft: Ahmed Fraz Baig, Khwaja Mansoor ul Hassan, Anwar Ghani, Shehzad Ashraf Chaudhry.

Writing – review & editing: Ahmed Fraz Baig, Khwaja Mansoor ul Hassan, Anwar Ghani, Shehzad Ashraf Chaudhry, Muhammad Usman Ashraf.

References

1. Bhagwat P, Perkins C, Tripathi S. Network layer mobility: an architecture and survey. IEEE Personal Communications 3 (3) (1996) 54–64. https://doi.org/10.1109/98.511765
2. Molva R, Samfat D, Tsudik G. Authentication of mobile users. IEEE Network 8 (2) (1994) 26–34. https://doi.org/10.1109/65.272938
3. Alveras D, Grotschel M, Jonas P, Paul U. Survivable mobile phone network architectures: models and solution methods. IEEE Communications Magazine. 1998. 3 p. 88–93. https://doi.org/10.1109/35.663332
4. Krishnamurthy P, Kabara J. Security architecture for wireless residential networks. In:IEEE Vehicular Technology Conference, 2000 p. 1960–1966.
5. Horn G, Preneel B. Authentication and payment in future mobile systems. In: Journal of Computer Security 55 (1); (2002) 183–207.
6. Go J, Kim K. Wireless authentication protocol preserving user anonymity. Citeseer; (2001).
7. Rahman MG, & Imai H Security in wireless communication. Wireless Personal Communications, 22(2), (2002) 213–228. https://doi.org/10.1023/A:1019968506856
8. Tzeng ZJ, & Tzeng WG. Authentication of mobile users in third generation mobile system. Wireless Personal Communications, 16(1), (2001) 35–50. https://doi.org/10.1023/A:1026530706019

9. Gope P, & Hwang T. Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. IEEE Systems Journal, p. 10(4),2016, p.1370–1379. https://doi.org/10.1109/JSYST.2015.2416396
10. Dressler F. Authenticated Reliable and Semi-reliable Communication in Wireless Sensor Networks. IJ Network Security, 7(1), (2008) p. 61–68 (pp. 882–887). Vancouver, Canada.
11. Farash MS, Chaudhry SA, Heydari M, Sajad S, Mohammad S, Kumari S, Khan MK. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. International Journal of Communication Systems, 30(4), (2017), p. e3019–n/a https://doi.org/10.1002/dac.3019
12. Amin R, Islam SKH, Biswas GP, Khan MK, Leng L, Kumar N. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Computer Networks, 101, (2016), p.42–62. https://doi.org/10.1016/j.comnet.2016.01.006
13. Kumari S, & Khan MK. More secure smart card-based remote user password authentication scheme with user anonymity. Security and Communication Networks, 7(11), (2014), p.2039–2053. https://doi.org/10.1002/sec.916
14. Khan MK. Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world. IETE Technical Review, 26(3), (2009), p.191–195. https://doi.org/10.4103/0256-4602.50703
15. Kumari S, Chaudhry SA, Wu F,Li X, Farash MS, Khan MK. An improved smart card based authentication scheme for session initiation protocol. Peer-to-Peer Networking and Applications, 10(1), (2017), p.92–105. https://doi.org/10.1007/s12083-015-0409-0
16. Suzuki S, Nakada K. An authentication technique based on distributed security management for the global mobility network. In:IEEE Journal on Selected Areas in Communications 15 (8) (1997) 1608–1617. https://doi.org/10.1109/49.634798
17. Zhu J, Ma J new authentication scheme with anonymity for wireless environments, Consumer Electronics. IEEE Transactions on Consumer Electronics 50 (1); (2004) 231–235. https://doi.org/10.1109/TCE.2004.1277867
18. Lee CC, Hwang MS, Liao IE. Security enhancement on a new authentication scheme with anonymity for wireless environments, Industrial Electronics. In: IEEE Transactions on Industrial Electronics 53 (5); (2006) 1683–1687. https://doi.org/10.1109/TIE.2006.881998
19. Wei Y, Qiu H, Hu Y. Security analysis of authentication scheme with anonymity for wireless environments. (2006); 1–4.
20. Wu CC, Lee WB, Tsaur WJ. A secure authentication scheme with anonymity for wireless communications. In: IEEE Communications Letters 12 (10); (2008) 722–723. https://doi.org/10.1109/LCOMM.2008.080283
21. He D, Ma M, Zhang Y, Chen C, Bu J. strong user authentication scheme with smart cards for wireless communications. Computer Communications 34 (3); (2011) 367–374. https://doi.org/10.1016/j.comcom.2010.02.031
22. Li CT. A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. Information Technology and Control 41 (1); (2012) 69–76. https://doi.org/10.5755/j01.itc.41.1.1024
23. Li CT, Lee CC. A novel user authentication and privacy preserving scheme with smart cards for wireless communications. In: Mathematical and Computer Modelling 55 (1); (2012) 35–44. https://doi.org/10.1016/j.mcm.2011.01.010
24. Das AK. A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. Networking Science 2 (1-2) (2013) 12–27. https://doi.org/10.1007/s13119-012-0009-8
25. Yoon EJ, Yoo KY, Ha KS. A user friendly authentication scheme with anonymity for wireless communications. Computers & Electrical Engineering 37 (3); (2011) 356–364. https://doi.org/10.1016/j.compeleceng.2011.03.002
26. Niu J, Li X. A novel user authentication scheme with anonymity for wireless communications. Security and Communication Networks 7 (10); (2014) 1467–1476.
27. Jiang Q, Ma J, Li G, Yang L. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. Wireless Personal Communications 68 (4); (2013) 1477–1491. https://doi.org/10.1007/s11277-012-0535-4
28. Wen F, Susilo W, Yang G. secure and effective anonymous user authentication scheme for roaming service in global mobility networks. Wireless personal communications 73 (3); (2013) 993–1004. https://doi.org/10.1007/s11277-013-1243-4

29. Mun H, Han K, Lee YS, Yeun CY, Choi HH. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks Mathematical and Computer Modelling 55 (1); (2012) 214–222. https://doi.org/10.1016/j.mcm.2011.04.036

30. Lee CC, Lai YM, Chen CT, Chen SD. Advanced secure anonymous authentication scheme for roaming service in global mobility networks. Wireless Personal Communications 94 (3); (2017) 1281–1296. https://doi.org/10.1007/s11277-016-3682-1

31. Blanchet B. ProVerif is a software tool for automated reasoning. [Online; accessed 01-June-2002] (2008).

32. Kilinc HH, & Yanik T. A survey of sip authentication and key agreement schemes. IEEE Communications Surveys & Tutorials 16 (2); (2014) 1005–1023. https://doi.org/10.1109/SURV.2013.091513.00050

33. 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, Volume 93, (2017), p. 311–335 https://doi.org/10.1007/s11277-015-3139-y