Indonesian Journal of Electrical Engineering and Computer Science
Vol. 1, No. 3, March 2016, pp. 597~ 606
DOI: 10.11591/ijeecs.v1.i3.pp597-606

Lightweight Communication Overhead Authentication Scheme Using Smart Card

Ahmed Y. F. Al_Sahlani[1], Songfeng Lu*[1, 2]
[1, 2] School of Computer Science and Technology,
Huazhong University of Science and Technology, Wuhan 430074, China
e-mail: cisco_ah81@yahoo.com[1], lusongfeng@hust.edu.cn[2]

Abstract

Authentication takes its place to grant authorized user a remote access to certain online resources. As well, prevent unauthorized user from accessing that resources. Unforyunatly most of authentication schemes consider only security factors without taking in consideration the communication resources required. Recently, Li et. al. proposed an enhanced smart card based remote user password authentication scheme. We analyzed their scheme and we pointed out that, their scheme required high communication overhead. Furthermore, their scheme suffers from forgery, user impersonation and server impersonation attacks. Through this paper to address aforesaid weaknesses, we propose a Lightweight communication overhead authentication scheme using smart card. The security and performance analysis shows that, our proposed scheme is lightweight communication and computation cost as well secure and can withstand wide spectrum of malicious attacks, like forgery, insider, replay and stolen smart card attack. Besides, our scheme encompasses desired security attributes. Therefore, it is suitable for practical use compared to other related scheme.

Keywords*: Authentication, Security, Key agreement, Smart Card, Lightweight communication*

1. Introduction

Nowadays, internet and online services become very essential as a part of various organization and human daily activities. Especially with the rapid development of internet and communication technologies. E-banking; e-shopping; online gaming; e-learning; …etc, are an examples of online services offered and accessed remotely through internet. On the other hand, accessing such services over insecure channel is a subject of wide spectrum of security risks. Furthermore, various authentication schemes proposed to provid authentication in various invironments such as authentication on client-server invironment and authentication on wireless sensor network WSN invironment [1], etc. Generally, authentication takes its place as an important procedure to verify the legitimacy of the communication participants over insecure environments.

In 1981, Lamport proposed first remote user authentication protocol based password for insecure communication [2]. His scheme is insecure since it requires maintaining a verification table at server side which can be reached and modified by an attacker. In 1991, Chang and Wu [3] proposed the first password based authentication scheme using smart card technology without using verification table. Since Then, many researchers proposed their authentication schemes using smart card to improve and address the security problems of existing authentication schemes [4-10].

Smart card have been widely adopted in modern authentication schemes to add security factor. Low cost, portability, and sufficient capacity are the most important reasons behind using smart card. Only legitimate user who possesses a smart card and knows valid password can gain access to certain online resources. Generally, Two factors authentication protocol using smart card can resist a wide spectrum of attacks such as password guessing attacks, forgery attacks, replay attacks insider attacks, and smart card stolen attacks [11].

Xu et al in 2009 proposed their smart card authentication protocol based password [12]. They claimed that, their scheme can withstand various attacks even when security parameters stored on the smart card is disclosed. However, in 2010, Song analyzed Xu et al's scheme and shows that, authorized user can extract security information stored in his/her own smart card and impersonate another user login. Then, he proposed an enhanced scheme [13]. In Same year, Sood et al show that, Xu et al's scheme is suffering from forgery and offline dictionary

Received November 11, 2015; Revised January 25, 2016; Accepted February 12, 2016

attacks, and then also proposed their enhanced scheme [14]. Chen et al analyzed proposed schemes [12-14] and found that, in Song's scheme [13], user's identity and server's secret key are permanent and both compose the secret key of symmetric encryption. So, an attacker can execute an offline dictionary attacks on stolen smart card to guess user's password and by pass Song's scheme. Sood et al's scheme [14] does not achieve mutual authentication between the remote user and the authentication server. This implies that, the user can not verify the validity of the server connected to. Then, Chen et al proposed their robust smart card based remote user password authentication scheme [15] over Xu et al, Sood et al and Song's schemes. In 2013, Li et al [16] analyzed Chen et al's scheme and found that, their scheme cannot ensure forward secrecy, and login password verified by server which cost unnecessary communication and waste time. Besides, the password change activity of Chen et al [15] requires server assistant. Li et al proposed their scheme to overcome the weaknesses in Chen et al's scheme. Unfortunately, most of aforementioned authentication schemes are still vulnerable to a wide spectrum of malicious attacks.

In this paper, we, focus on both of communication resources required as well as security functionality of the proposed schem to address aforesaid weaknesses. We aim to propose a secure and lightweight communication overhead authentication scheme to save network communication resources and low computation cost. Our proposed scheme detects and prevents duplicated registration requst without using password verification table and allows valid user to use a new fresh password at first login attempt to ensure that, user's login password only known by himself. To achieve this goal we only use hash function and Bit wise XOR operation. Then we show that, our scheme encompasses various security attributes and withstand various attacks.

The rest of this paper is organized as follows: review and security analysis of Li et al's scheme in sections 2 and 3 respectively. Then, review of our proposed scheme and its security analysis in sections 4 and 5 respectively. Finally, performance and conclusion produced in sections 6 and 7, respectively. Table 1 Shows the notation used through this paper.

Table 1. The notations used in this paper.

U	The user
S	The authentication server
ID_u	The identity of U
TPW_u	Temporary password of U
PW_u	The login password of U
Bio	The biometric of U
x	The master secret key of S
T	The timestamp
ΔT	The maximum transmission delay
p, q	Two large prime numbers
Z_q	The ring of integers modulo q
Z_q^*	The multiplicative group of Z_q
$h(.)$	Cryptographic one way hash function
$\oplus$	Bitwise XOR operation
$\|\|$	The message concatenation operator
- - - - →	Secure channel
——→	Public channel

2. Review of Li et al's Scheme

In 2013, Li et al proposed their authentication scheme [16] as an improvement over Chen et al's scheme [15]. Li et al's scheme consists of four phases as follows:

- Registration
- Login
- Authentication
- Password change

At the beginning, two large prime numbers p and q selected by the sever such that, p=2q+1. Then, the server chooses a proper one-way cryptographic hash function.

2.1. Registration Phase

Step 1. User U selects his/her identity IDu and login password PWu. Then, submits them to the server S via secure channel.
Step 2. S computes security parameters to be stored in smart card, such that, Au = $h(IDu||PWu)^{PWu}$ mod p, Bu = $h(IDu)^{(x+PWu)}$ mod p.
Step 3. S stores {Au, Bu, h(.), p, q} on a smart card and issues it to U via secure channel.

2.2. Login Phase

Step 1. U inserts his/her smart card into a proper card reader, and inputs his / her IDu, PWu.
Step 2. The smart card computes Au' = $h(IDu||PWu)^{PWu}$ mod p. Then compare it with already stored Au. If they are not matched, session terminated, since the entered IDu or PWu were incorrect. On the contrary, if Au' equals to Au, the smart card performs next step.
Step 3. Random number $\alpha \in_R Z_q^*$ choose by a smart card. Then computes:
Cu=Bu/ $h(IDu)^{PWu}$ mod p,
Du= $h(IDu)^{\alpha}$ mod p,
Mu= h(IDu||Cu|| Du||Tu), where Tu is the current time stamp of U.
Step 4. The smart card sends {IDu, Du, Mu, Tu} to S as login request message.

2.3. Authentication Phase

Step 1. Upon receiving U's login request message, S validates IDu and check Tu' – Tu $\leq \Delta T$, where Tu' is the current S's timestamp. S rejects login request if either or both are invalid.
Step 2. S computes:
Cu' = $h(IDu)^{x}$ mod p,
Mu'= h(IDu||Cu'||Du||Tu)
Step 3. S compares computed Mu' with received Mu, if they are equal, U is authenticated and login request is accepted by S. Otherwise, S rejects login request.
Step 4. Random number $\beta \in_R Z_q^*$ chooses by S. Then, computes Vu = $h(IDu)^{\beta}$ mod p, SK=Du^{β} mod p , where SK is the shared session key.
Step 5. S computes Ms= h(IDu||Cu'||Vu||SK||Ts) where Ts is the current S's timestamp . Then, {IDu, Vu, Ms, Ts} sent to U by S as a mutual authentication message.
Step 6. Upon receiving the mutual authentication message, U validates IDu and checks Ts' – Ts $\leq \Delta T$ where Ts' is the current timestamp of U. if either or both are invalid, U terminates session. Otherwise, U continue to next step.
Step 7. U computes:
SK' = Vu^{α} mod p ,
Ms' = h(IDu||Cu||Vu||SK'||Ts), U compares Ms' with the received Ms . if they are equal , S is authenticated and mutual authentication achieved. On the contrary, the session is terminated by U. At the end, both of U and S shared a session key SK= $h(IDu)^{\alpha\beta}$ mod p.

2.4. Password Change Phase

U can change his/her login password PWu as follows:
Step 1. U inserts a smart card into a proper card reader. Then, inputs his/ her IDu, PWu.
Step 2. The smart card computes Au'=$h(IDu||PWu)^{PWu}$ mod p and compares it with stored Au. If they are not equal, the request is rejected. Otherwise. U inputs a new password PWnew and continue to next step.
Step 3. A smart card computes
Au_new = $h(IDu||\ PWnew)^{PWnew}$ mod p,
Bu_new = Bu . $h(IDu)^{PWnew}$ / $h(IDu)^{PWu}$ mod p.
Step 4. A smart card replaces both Au, Bu with Au_new, Bu_new respectively.

3. Cryptanalysis of Li et al's Scheme

In this section, we analysis Li et al's scheme. We show that, their scheme suffer from forgery and user & server impersonation attacks.

3.1. Forgery Attacks

Suppose an attacker intercept U's valid login message <IDu, Du, Mu, Tu>, an attacker can easily achieves U's identity IDu which sent in a plain form. Since, S does not check U's

identity before processing registration request, an attacker can send both intercepted IDu and attacker's password PW* < IDu, PW*> to S as a registration request. S computes Au*= $h(IDu||PWu^*)^{PWu^*}$ mod p, and Bu*= $h(IDu)^{(x+PWu^*)}$ mod p, S stores the security parameters {Au*,Bu*, h(.), p, q} on the smart card and issues it to attacker. Then, an attacker achieves U's secret key Cu, where Cu= Bu*/ $h(IDu)^{PWu^*}$ mod p = $h(IDu)^x$ mod p. intuitively, an attacker using intercepted IDu ,and computed U's secret key Cu can easily forge a valid login message.

3.2. User Impersonation Attacks

An attacker can masquerades as a legitimate U. since, he/she can easily achieves U's identity IDu and secret key Cu as mentioned in forgery attacks section (3.1.). An attacker selects random number $r \in_R Z_q^*$ and calculates Du*= $h(IDu)^r$ mod p, and Mu*= h(IDu||Cu|| Du*||Tu*), where Tu* is attacker's current timestamp. Then, sends <IDu, Du*, Mu*,Tu*> to S.

S verifies attacker's login message, the verification holds, since both Tu* and Mu* are valid. Then, S selects $\beta \in_R Z_q^*$ and calculates Vu = $h(IDu)^\beta$ mod p. S sends the mutual authentication message to U. Again, an attacker intercepts the message <IDu, Vu, Ms, Ts> and computes SK= $(Vu)^r$ mod p = $(IDu)^{r\,\beta}$ mod p. From the analysis above, we show that, an attacker can perform user impersonation attacks. Furthermore, the session key SK also achieved by an attacker.

3.3. Server Impersonation Attacks

An attacker can perform server impersonation attacks using U's identity IDu and secret parameter Cu= $h(IDu)^x$ mod p as mentioned in forgery attacks section (3.1). An attacker intercept U's login message <IDu, Du, Mu, Tu> and generates random $r \in_R Z_q^*$ and computes SK*= $(Du)^r$ mod p; Vu*= $h(IDu)^r$ mod p; Ts* is attacker current timestamp; and Ms*= h(IDu||Cu||Vu*||SK*||Ts*). Then, an attacker sends mutual authentication message {IDu, Vu*, Ms*, Ts*} to U. Upon receiving attacker's message, U validates IDu and Ts*, since both are valid, the verification holds. Then, U computes SK'=$(Vu^*)^\alpha$ mod p which equals to SK*; Ms'= h(IDu||Cu||Vu*||SK'||Ts*). Thus, Ms' is equal to Ms*.

This brief discussion shows that, Li et al's scheme suffers from server impersonation attacks and session key can be easily calculated by an attacker.

4. The Proposed Scheme

In this section, we propose our secure lightweight communication overhead authentication scheme based user's password and biometric with session key agreement using smart card. Our proposed scheme consist of four phases as follows:

- Registration phase
- Login phase
- Authentication phase
- Password change phase

In the beginning of our proposed scheme, server S selects key x as its secret key with proper length like 1024 bits, and one way cryptographic hash function $h(.):\{0,1\}^* \longrightarrow \{0,1\}^n$. The registration, and login & authentication phases of our scheme shown in Figures 1 and 2 respectively.

4.1. Registration

Step 1. U chooses his/her identity IDu, temporary password TPWu and random number b. U computes EID=h(IDu||b). Then, sends registration request <EID, TPWu> to S via secure channel.

Step 2. Upon receiving registration message, S computes SID=h(EID || x). S checks SID and rejects this request if it is already registered to prevent duplicated registration for same identity. Otherwise, S updates registered user list with SID. Then, computes Au=SID ⊕ TPWu, Bu=h(SID ⊕ EID). S stored secret parameters {Au, Bu, h(.)} into smart card and issues it to U via secure channel.

Step 3. U insert a smart card into a proper card reader and inputs IDu, TPWu. a smart card computes EID=h(IDu||b), SID = Au ⊕ TPWu , and compares Bu'= h(SID ⊕ EID) with Bu which stored in smart card. If Bu' not equal to Bu, U terminates the session.

Step 4. U chooses and submits his/her fresh login password PWu and imprints biometric Bio like finger print. A smart card computes Au'= Au ⊕ TPWu ⊕ h(PWu||Bio), Bu'= h(SID || h(PWu||Bio)). Then, replaces Au, Bu with Au', Bu' respectively and stores b into smart card. At the end of successful registration process, secret parameters {Au, Bu, h(.) b} stored in a smart card.

4.2. Login Phase

Step 1. U inserts his/her smart card into a proper card reader, and inputs U's identity IDu, password PWu, and imprint biometric Bio. Then, a smart card computes SID=Au ⊕ h(PWu||Bio), Bu'= h(SID || h(PWu||Bio)) and checks whether Bu' is equal to stored Bu, if they are equal, session holds. Otherwise, session terminated because at least one of entered parameters {IDu, PWu, Bio} is incorrect.
Step 2. Smart card generates random α, and computes EID=h(IDu||b) , M_1=h(SID||Tu) ⊕ α, M_2= h(M_1||α). Then, smart card sends login message <EID, M_1, M_2, Tu > to S. Where Tu is U's current timestamp.

4.3. Authentication Phase

Step 1. Upon receiving login message, S checks the validity of SID=h(EID || x) compared to both registered user database and active user list. Then, validates Tu'- Tu ≤ Δ T, where Tu' is S's current timestamp at receiving login message. If either or both are invalid, the login attempt is rejected.
Step 2. S computes, α= M_1 ⊕ h(SID||Tu) , M_2'= h(M_1||α). If M_2' is equal to M_2, session holds and U is authenticated. Otherwise, session terminated.
Step 3. S generates random β, and computes M_3=h(SID||Ts) ⊕ β, where Ts is S's current timestamp, M_4=h(M_3|| β), SK=h(α|| β). Then, S sends mutual authentication message < M_3, M_4, Ts > to U.
Step 4. Upon receiving mutual authentication message at time Ts', Smart card check the validity of Ts Ts' – Ts ≤ ΔT, if it is invalid, smart card terminates session. Otherwise, smart card computes β= M_3 ⊕ h(SID||Ts), M_4'= h(M_3|| β). If M_4' not equal to M_4, session terminated. On the contrary, if M_4' is equal to M_4, S is authenticated and mutual authentication achieved. Then, smart card computes SK=h(α|| β). At the end of successful mutual authentication, both user U and server S share the same session key SK=h(α||β), where α and β have random value for each session.

4.4. Password Change Phase

Whenever authorized user wants to change his/her password PWu to a new password PWu^{new}, this phase is invoked.
Step 1. U inserts his/her smart card into a proper card reader, and inputs identity IDu, current password PWu, imprints biometric Bio. Then, Smart card computes SID=Au ⊕ h(PWu||Bio), Bu'=h(SID||h(PWu||Bio)). If Bu' is not equal to Bu which stored in smart card, password change is rejected due to invalid information. Otherwise smart card continue to next step.
Step 2. U inputs his/her new password PWu^{new}, Smart card computes Au'=Au ⊕ h(PWu||Bio) ⊕ h(PWu^{new}||Bio), Bu'=h(SID||h(PWu^{new}||Bio)).
Step 3. Smart card replaces Au, Bu with Au', Bu' respectively. Which successfully completes password change at U's side without need to S's assistance.

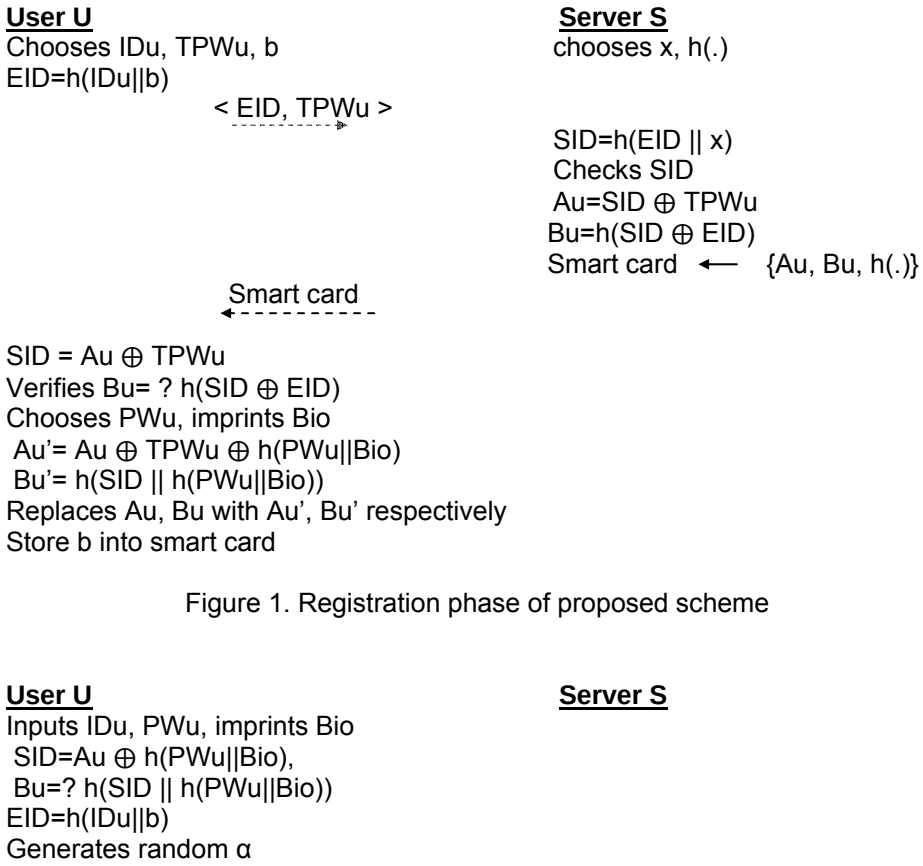

Figure 1. Registration phase of proposed scheme

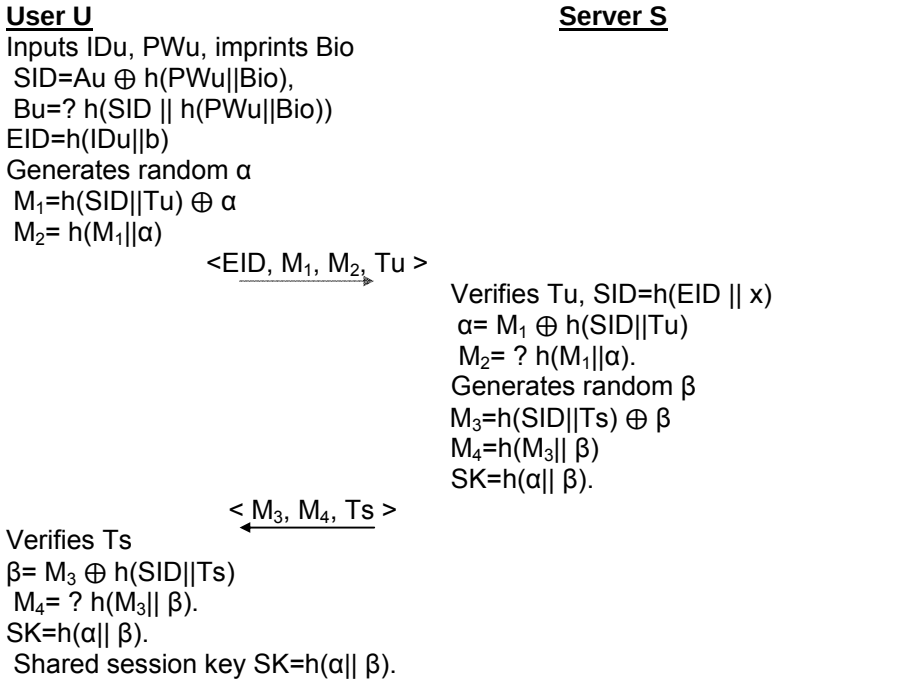

Figure 2. Login and Authentication phases of proposed scheme

5. Security Analysis of Proposed Scheme

In this section, we analysis the security of our proposed lightweight authentication scheme, with a brief discussion.

5.1. User Anonymity

To protect user anonymity in the proposed scheme, plain text U's identity IDu neither saved in smart card nor transmitted over channel through login message. Instead, hashed value of concatenated IDu and parameter b, say EID, sent to S. an attacker has to break one way cryptographic hash function and he must know b to extract IDu. Intuitively, an attacker has no

way to extract U's identity by considering one way property of hash function. So, our proposed scheme can achieve user anonymity.

5.2. Password Guessing Attacks

Our proposed scheme can withstand offline guessing attacks. To prove that, an attacker who attempts to guess U's login password, cannot verify guessed password from Au=SID ⊕ h(PWu||Bio); Bu= h(SID||h(PWu||Bio)); and intercepted login message, because SID and Bio are required.

To compute SID, secret parameter x (1024 bits) is required which is only known by S. Furthermore, U's Biometric value is unknown to the attacker and only authorized user can imprints a valid biometric. Therefore, our proposed scheme can resist offline password guessing attacks.

5.3. Stolen Smart Card Attacks

Our proposed scheme can resist stolen smart card attack. Suppose an attacker extract all parameters stored in the stolen smart card {Au, Bu, b} by power analysis attack [17] Kocher et al in 1999. Then, the attacker tries to initiate a valid login message. An attacker uses his/ her current timestamp Tu*. Although, he/she cannot successfully computes EID = h(IDu||b) without knowing U's identity IDu which neither stored in smart card nor transmitted over channel. In the same way, computes M1=h(SID||Tu*) ⊕ α is infeasible without knowing SID. To compute SID an attacker either computes SID= Au ⊕ h(PWu||Bio) or SID = h(EID || x). Obviously, he/she cannot generates U's password and biometric information.

From the discussion above, we prove that, our propose scheme can resist stolen smart card attacks.

5.4. Replay Attacks

Our proposed scheme forbids replay attacks using timestamp T. suppose an attacker tries to resend previously intercepted login message, this attempt will be rejected by the server S after checking message freshness based on Tu. if the attacker replaces the U's timestamp with attacker's timestamp Tu*, this attempt also rejected by S based on condition M2'=? h(M1||α) = h(h(SID||Tu) ⊕ α)|| α). The other possible chance for the attacker is to generate both Tu*and M1*= h (SID||Tu*) ⊕ α. This attempt also rejected because there is no way to compute valid SID without knowing U's parameters {IDu, PWu, b, x}. This brief discussion shows that, our proposed scheme forbids replay session attacks.

5.5. Mutual Authentication

Our proposed scheme achieves mutual authentication. Both user and server prove their legitimacy to each other where M2, U's timestamp and M4, S's timestamp are used to authenticate user to server, server to user respectively as mentioned in authentication phase in section (4.3). Furthermore, only authorized user and server can prove their authenticity to each other.

5.6. Forgery Attacks

An attacker has to forge a valid login message {EID,M1,M2,Tu} which can be verified and accepted by the authentication server, an attacker has no way to extract or generate parameters {IDu, x, b} to compute M1=h(SID||Tu) ⊕ α = h(h(EID|| x)||Tu) ⊕ α = h(h(h(IDu||b) || x)||Tu) ⊕ α . Intuitively, our scheme resist forgery attacks.

5.7. Known Key Secrecy

Our proposed scheme meets known key secrecy property. If session key SK= h(α||β) is compromised by an attacker, previously captured communication cannot be revealed due to random α and β. Since both have new random value in each new session and there is no way to derive previous session key from the current key. Hence, there is no way to reveal previous communications. This brief discussion shows that, our proposed scheme resists known key secrecy attacks.

5.8. Session Key Agreement

In our proposed scheme during authentication phase, user and server compute their session key SK= h(α ||β). Furthermore, M2'=? h(M1||α), M4'=? h(M3|| β) these two conditions are used to verify the established session key. This clearly shows that, our scheme achieves session key agreement.

5.9. Insider Attacks

Our proposed scheme prevents insider attack, since security parameters {IDu, PWu, Bio, b, x} cannot be obtained by an attacker. For instance, U's biometric imprints only by authorized user as well as login password. Besides, server secret key x is only known to the server. Furthermore, all secret values protected using cryptographic hash function. Without knowing these parameters, an attacker cannot perform insider attacks. This shows our scheme resists insider attacks.

5.10. Friendly User Password Change

The user is free to change his/her login password without need to communicate the server. Efficient and secure steps are used to handle password change as mentioned in section (4.4). Furthermore, wrong entered password can be detected quickly. On the other hand, an attacker has no way to change user's password, since he/she has no sufficient information to perform this change. Thus, our proposed scheme achieves friendly and securely user's password change.

6. Performance Analysis

In this section. We evaluate our proposed scheme and compare it with related schemes, Xu et al [12]; Song [13]; Sood et al [14]; Chen et al [15]; Li et al [16]. We focus on Login and authentication phases since both are more frequent and required in each login attempt. The comparison based on communication overhead and computation complexity. We assume that, the output of hash function is 160 bits; timestamp 32 bits; user's identity, password, biometric, and random nonce are 160 bits; server secret key x is 1024 bits to avoid guessing attacks. According to this assumption, we found that, single login attempt in Li et al's scheme required 2752 bits as communication overhead in two messages, first messeage for login request and scond one for mutual verification. Whereas, our proposed scheme required only 864 bits communication overhead under same conditions. Figure 3 shows the communication overhead comparison of related schemes. Furthermore, the comparison of computation complexity of various operations used in mentioned schemes such as hash function; exponential; multiplication/ division; and exclusive XOR operations are shown in table 2. To achieve lowest computation time complexity, our proposed scheme uses only hash function and exclusive XOR operations.

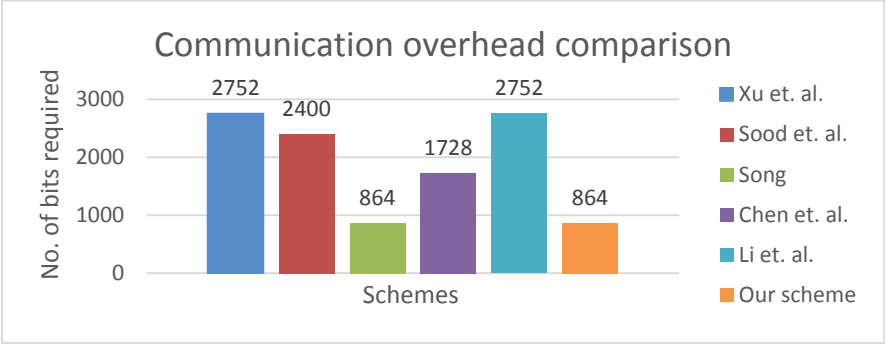

Figure 3. Communication overhead comparison between proposed and related schemes

Table 2. Computation cost comparisons between proposed and related schemes

Scheme	Login phase	Authentication phase	Total
Xu et al	$3T_h + 2T_e$	$4T_h + 2T_e$	$7T_h + 4T_e$
Sood et al	$3T_h + 3T_e + 2T_m$	$3T_h + 2T_e + 1T_m$	$6T_h + 5T_e + 3T_m$
Song	$2T_h + 1T_S$	$6T_h + 1T_e + 1T_S$	$8T_h + 1T_e + 2T_S$
Chen et al	$2T_h + 2T_e + 2T_m$	$6T_h + 1T_e + 1T_m$	$8T_h + 3T_e + 3T_m$
Li et al	$4T_h + 3T_e + 1T_m$	$5T_h + 4T_e$	$9T_h + 7T_e + 1T_m$
Our scheme	$5T_h + 2T_{XOR}$	$9T_h + 3T_{XOR}$	$14T_h + 5T_{XOR}$

T_h : complexity of hash function
T_e : complexity of exponential operation
T_m : complexity of multiplication/division operation
T_S : complexity of symmetric encryption-decryption operation
T_{XOR} : complexity of exclusive XOR operation

Additionaly, Table 3. Briefly shows the comparison results for security attributes of our proposed and related schemes.
This performance analysis shows that, our proposed scheme encompasses the desired security attributes and resist wide spectrum of malicious attacks. Besides, our proposed scheme is efficient and lightweight communication overhead. Thus, it is secure and more suitable to practical use compared to other related schemes.

Table 3. Security attributes comparison between proposed and related schemes

Security attributes	*Xu et al*	*Song*	*Sood et al*	*Chen et al*	*Li et al*	*Our scheme*
Resist smart card stolen attacks	Yes	No	Yes	Yes	Yes	Yes
Resist forgery attacks	No	Yes	Yes	Yes	No	Yes
Resist impersonation attacks	No	No	No	No	No	Yes
Resist insider attacks	No	No	No	No	No	Yes
Resist offline password guessing attacks	No	No	No	No	No	Yes
Achieve mutual authentication	No	Yes	No	Yes	Yes	Yes
Support session-key agreement	Yes	Yes	No	Yes	Yes	Yes
Quickly detect wrong password	No	No	No	No	Yes	Yes
Friendly password change	No	No	No	No	Yes	Yes
Using temporary registration password	No	No	No	No	No	Yes
Prevent duplicated registration	No	No	No	No	No	Yes

7. Conclusion

Communication resources is a crucial issue to be considered in modern authentication protocols. In this paper, we show more interesting in communication resources as well as security functionality of the proposed authentication scheme. We reduce communication and computation cost required to achieve secure and mutual authentication between remote user and server. We propose our secure Lightweight communication overhead authentication scheme using smart card. Through cryptanalysis and performance evaluation comparison, we show that, our proposed scheme achieves desired security attributes and withstand various malicious attacks which other schemes suffer from. Our proposed scheme required only 864 bits totally communication overhead also requires low computation cost compared to other related schemes and supporting mutual authentication and session key agreement using smart card technology. Thus, our scheme is more suitable for practical use to secure remote access over public environment.

References

[1] Yu X, Fang JJ, Zhang ZL. A Security Mechanism based on Authenticated Diffie Hellman for WSN. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(6): 3349 - 3354.
[2] Lamport L. Password authentication with insecure communication. *Communications of the ACM*. 1981; 24(11): 770-772.
[3] Chang CC, Wu TC. *Remote password authentication with smart card*. Computers and Digital Techniques. IEEE Proceedings. 1991; 138(3): 165-168.
[4] Sun HM. An efficient remote use authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*. 2000; 46(4): 958-961.

[5] Ku WC, Chen SM. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*. 2004; 50(1): 204-207.
[6] Chan CK, Cheng LM. Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*. 2000; 46(4): 992-993.
[7] Chien HY, Jan JY, Tseng YM. An efficient and practical solution to remote authentication: smart card. *Computers & Security*. 2002; 21(4): 372-375.
[8] Hsu CL. Security of Chien et al.'s remote user authentication scheme using smart cards. *Computer Standards & Interfaces*. 2004; 26(3): 167-169.
[9] Hwang MS, Li LH. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*. 2000; 46(1): 28-30.
[10] Wei Chi KU, Chang ST. Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards. *IEICE Transactions on Communications*. 2005; 88(5): 2165-2167.
[11] Devi T, Ganesan R. Platform-as-a-Service (PaaS): Model and Security Issues. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2015; 15(1): 151 – 161.
[12] Xu J, Zhu WT, Feng DG. An improved smart card based password authentication scheme with provable security. *Computer Standards & Interfaces*. 2009; 31(4): 723-728.
[13] Song R. Advanced smart card based password authentication protocol. *Computer Standards & Interfaces.* 2010; 32(5): 321-325.
[14] Sood SK, Sarje AK, Singh K. *An improvement of Xu et al.'s authentication scheme using smart cards*. Proceedings of the Third Annual ACM Bangalore Conference. Bangalore. 2010.
[15] Chen BL, Kuo WC, Wuu LC. Robust smart-card-based remote user password authentication scheme. *International Journal of Communication Systems*. 2014; 27(2): 377-389.
[16] Li X, Niu J, Khurram Khan M, Liao J. An enhanced smart card based remote user password authentication scheme. *Journal of Network and Computer Applications*. 2013; 36(5): 1365-1371.
[17] Kocher P, Jaffe J, Jun B. Differential power analysis. In: Advances in cryptology CRYPTO99. Springer. 1999: 388-397.