南　華　大　學

資 訊 管 理 學 系

碩士論文

一個物聯網環境中異質無線感應網路身份認證協定的改善方案

Improved on an efficient user authentication scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment

研 究 生 ： 吳鴻生

指導教授 ： 周志賢 博士

中 華 民 國　106 年 1 月

南　華　大　學

資訊管理學系

碩 士 學 位 論 文

一個物聯網環境中異質無線感應網路身份認證協定的改善方案

Improved on an efficient user authentication scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment

研究生：吳鴻生

經考試合格特此證明

口試委員：劉建人

邱宏林

周志賢

指導教授：周志賢

系主任(所長)：

口 試 日 期 ： 中 華 民 國 105 年 1 月 5 日

南華大學碩士班研究生

論文指導教授推薦函

資訊管理學系碩士班 吳鴻生 君所提之論文

Improved on an efficient user authentication scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment

係由本人指導撰述，同意提付審查。

指導教授 周志賢

106 年 1 月 7 日

南華大學資訊管理學系碩士論文著作財產權同意書

立書人：吳鴻生　之碩士畢業論文

中文題目：一個物聯網環境中異質無線感應網路身份認證協定的改善方案

英文題目：Improved on an efficient user authentication scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment

指導教授：周志賢 博士

學生與指導老師就本篇論文內容及資料其著作財產權歸屬如下：

☑ 共同享有著作權

☐ 共同享有著作權，學生願「拋棄」著作財產權

☐ 學生獨自享有著作財產權

學　　生：吳鴻生　（請親自簽名）

指導老師：周志賢　（請親自簽名）

中　華　民　國　106　年　1　月　7　日

誌　　謝

此論文的完成歸功於指導教授-周志賢博士認真又親切的指導，引導我進入深澳的資訊安全加解密的領域。從無到有，如果有一點點成果的話，真的很感激周教授無私的傳授，親切的解惑，正確的導引，無時無刻為我的學習操心，讓我在知天命之年還能投入濃厚的興趣。

論文的編撰還要感謝口考委員-邱宏彬教授、劉建人教授的指正與建議，才得以刊登，非常謝謝!

接著要感謝南華的教學團隊，對學生關懷照顧無微不至，備感窩心。

最後要感謝的是相伴兩年多的同學們，時時給我勉勵、提攜，才能堅持到最後，真的很謝謝你們!

鴻生 2017/01/06 南華大學

一個物聯網環境中異質無線感應網路身份認證協定的改善方案

學生 : 吳鴻生　　指導教授 : 周志賢 博士

南 華 大 學 資訊管理學系碩士班

摘　　要

最近 Farash 等人提出一個有效率的使用者認證和金鑰協議方案,該方案係使用 BAN-logic 和 AVISPA 為工具來針對異質的無線感測網路所量身訂做的物聯網環境所做的使用者身分認證。然而，經過分析之後我們確定這個方案不能抵抗 smart card 遺失密碼猜測攻擊和無法達到真正匿名，這是在使用 smart card 安全身分認證的十個基本需求之一，由 Liao 等人所提出的主張。因此，我們提出一個修正方案，我們的修改方法期望包括一般智慧卡所應具有的安全功能，此對一個 smart card 使用者認證系統來說是非常重要的。

關鍵字: 使用者認證、金鑰協定、 智慧卡 、無線感應網路、物聯網、匿名性、雜湊函數

Improved on an efficient user authentication scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment

Student：WU, HUNG-SHENG Advisors：Dr. CHOU, JUE-SAM

Department of Information Management
The Garduated Program
Nan-Hua University

ABSTRACT

Recently, Farash *et al.* proposed an efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. By using BAN-logic and AVISPA tools, they confirmed the security properties of the proposed scheme. However, after analyzing, we determined that the scheme could not resist the smart card loss password guessing attack and suffers anonymity breach, which are two of the ten basic requirements in a secure identity authentication using smart card, insisted by Liao *et al.* Therefore, we modified their method to include the desired security functionality, which are significantly important in a user authentication protocol using smart card.

Keywords: user authentication, key agreement, smart card, wireless sensor network, Internet of Things, anonymity, hash function

目錄

List of Figures

1. Introduction

There have been many cryptographic scientists working in the field of identity authentication system design using smart card [1-13]. A heterogeneous wireless sensor network identity authentication system typically contains three roles: user, sensor node, and the gateway node (GWN); and three protocols: registration, login and authentication, and password change. In the design principle, the user's identity should not be revealed in order to ensure his login privacy. In 2016, Farash *et al.* [11] pointed out that they have found Turkanovic *et al.'*s scheme [6] has some security shortcomings which make it susceptible to some cryptographic attacks. They hence overcome the security weaknesses by proposing a new improved user authentication and key agreement scheme (UAKAS). The proposed scheme improves the security level and enables the heterogeneous wireless sensor networks (WSN) to dynamically grow without influencing any party involved. They claimed that the security analysis results instructed by BAN-logic and AVISPA tools confirm the security properties of the proposed scheme. However, upon a closer examination, we discovered that it does not support the needed security resistance when an attacker launches a smart card loss password guessing attack. To enhance its security, we modified their scheme to include this feature. We will demonstrate the enhancement in this article.

The rest of this paper is organized as follows. Section 2 review Farasha *et al.'*s scheme. Section 3 presents the weaknesses of theirs. Section 4 describes the modifications of their scheme in the registration phase and the login and authentication phase. Section 5 analyzes its security. Finally, a conclusion that our modification of Farash *et al.'*s scheme is secure is given in Section 6.

2. Review of Farash *et al.*'s scheme

Farash *et al.*'s heterogeneous wirReeless sensor network identity authentication sheme is based on Turkanovic *et al.*'s scheme [6]. It consists of three roles: user, sensor node, and the gateway node (GWN); and some phases: pre-deployment, registration, login and authentication, password change, and dynamic node addition phase. They claimed that their scheme not only eliminates all security vulnerabilities of Turkanovic *et al.*'s scheme, but also introduces some enhancement, which enables the WSN' dynamically limitless growth, and makes the functionality and efficiency at the same level as theirs. In this article, we only review the registration phase, and login and authentication phase to illustrate its weaknesses. As for the used notations' definitions, please refer to the original article.

2.1 Registration Phase

This phase is divided into two parts: (a). the user registration phase, and (b). the sensor node registration phase. We describe both of them below and depict them in Fig 1 and 2 respectively.

(a) The user registration phase

As shown in Fig 1, the user U_i chooses his username ID_i, password PW_i, and selects a random nonce r_i. He then computes $MP_i = h(r_i \| PW_i)$ and sends $\{MP_i, ID_i\}$ to GWN over a secure channel. After receiving the registration message from U_i, GWN first computes the value $e_i = h(MP_i \| ID_i)$, then by using U_i's secret data combined with its secret master key X_{GWN}, GWN computes $d_i = h(ID_i \| X_{GWN})$, $g_i = h(X_{GWN}) \oplus h(MP_i \| d_i)$, and $f_i = d_i \oplus h(MP_i \| e_i)$. It stores $\{e_i, f_i, g_i\}$ into the smart card (SC) and sends it to U_i. After receiving the SC, U_i inserts the previously selected r_i into it, and terminates the registration phase.

(b) The sensor node registration phase

A specific sensor node S_j has to register to the GWN with a message $\{SID_j, MP_j, MN_j, T_1\}$ over an insecure channel. This is done by S_j which first randomly selects a nonce r_j , then computs the values $MP_j = h(X_{GWN\text{-}Sj} \| r_j \| SID_j \| T_1)$ and $MN_j = r_j \oplus X_{GWN\text{-}Sj}$.

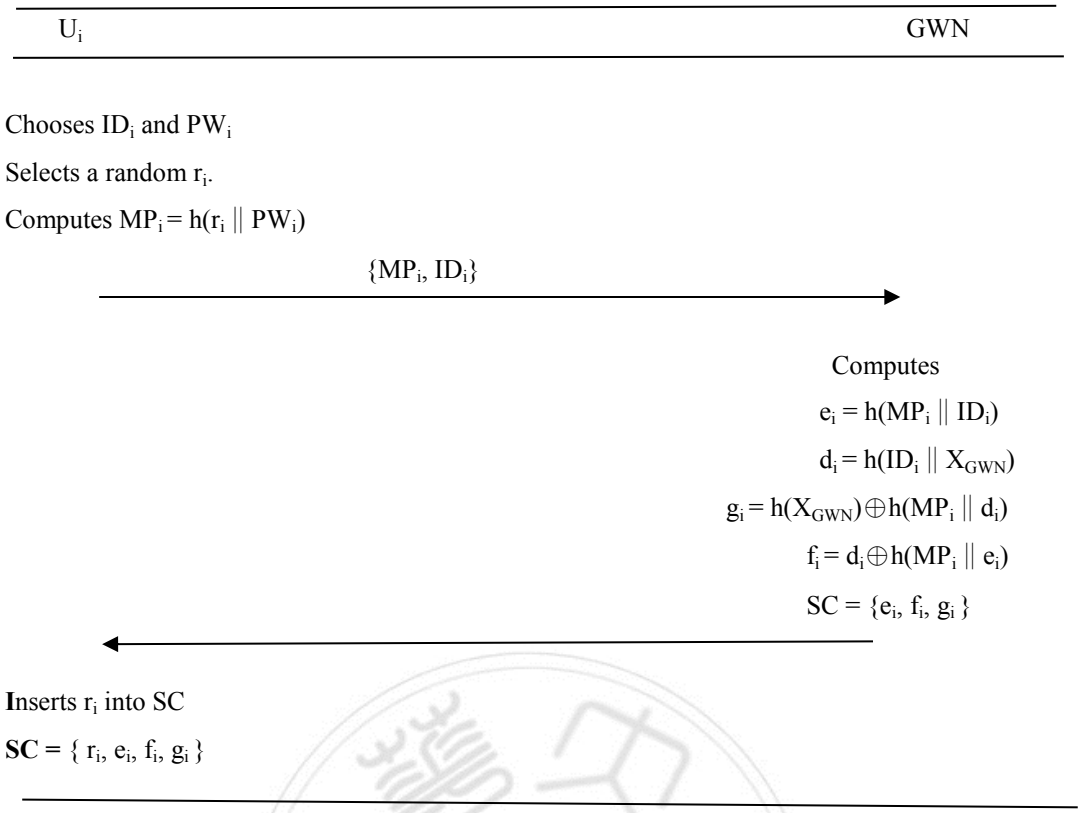

Fig. 1. User registration phase of Farash *et al.*'s scheme

After receiving the registration message from S_j, GWN checks whether $|T_1 - T_c| < \triangle T$ holds, if the verification holds, GWN then computes the random nonce $r_j' = MN_j \oplus X_{GWN-Sj}$ and $MP_j' = h(X_{GWN-Sj} \| r_j' \| SID_j \| T_1)$, and checks to see if it is equal to the received MP_j. If it is, GWN computes the values $x_j = h(SID_j \| X_{GWN})$, $e_j = x_j \oplus X_{GWN-Sj}$, $d_j = h(X_{GWN} \| 1) \oplus h(X_{GWN-Sj} \| T_2)$, and $f_j = h(x_j \| d_j \| X_{GWN-S\,j} \| T_2)$. GWN then sends S_j the following message $\{e_j, f_j, d_j, T_2\}$. S_j then checks whether $|T_2 - T_c| < \triangle T$. If the verification holds, S_j computes $x_j = e_j \oplus X_{GWN-S\,j}$ and compares f_j with $h(x_j \| d_j \| X_{GWN-Sj} \| T_2)$. If they are equal, S_j calculates $h(X_{GWN} \| 1) = d_j \oplus h(X_{GWN-Sj} \| T_2)$ and stores $h(X_{GWN} \| 1)$ and x_j into its memory. Finally, S_j deletes X_{GWN-Sj} and SID_j and sends a confirmation message to GWN.

2.2 Login and authentication phase

This phase is to enable a user to negotiate a session key with a specific sensor node without contacting the GWN. The session key will be used for secure communication between the user and the sensor node.

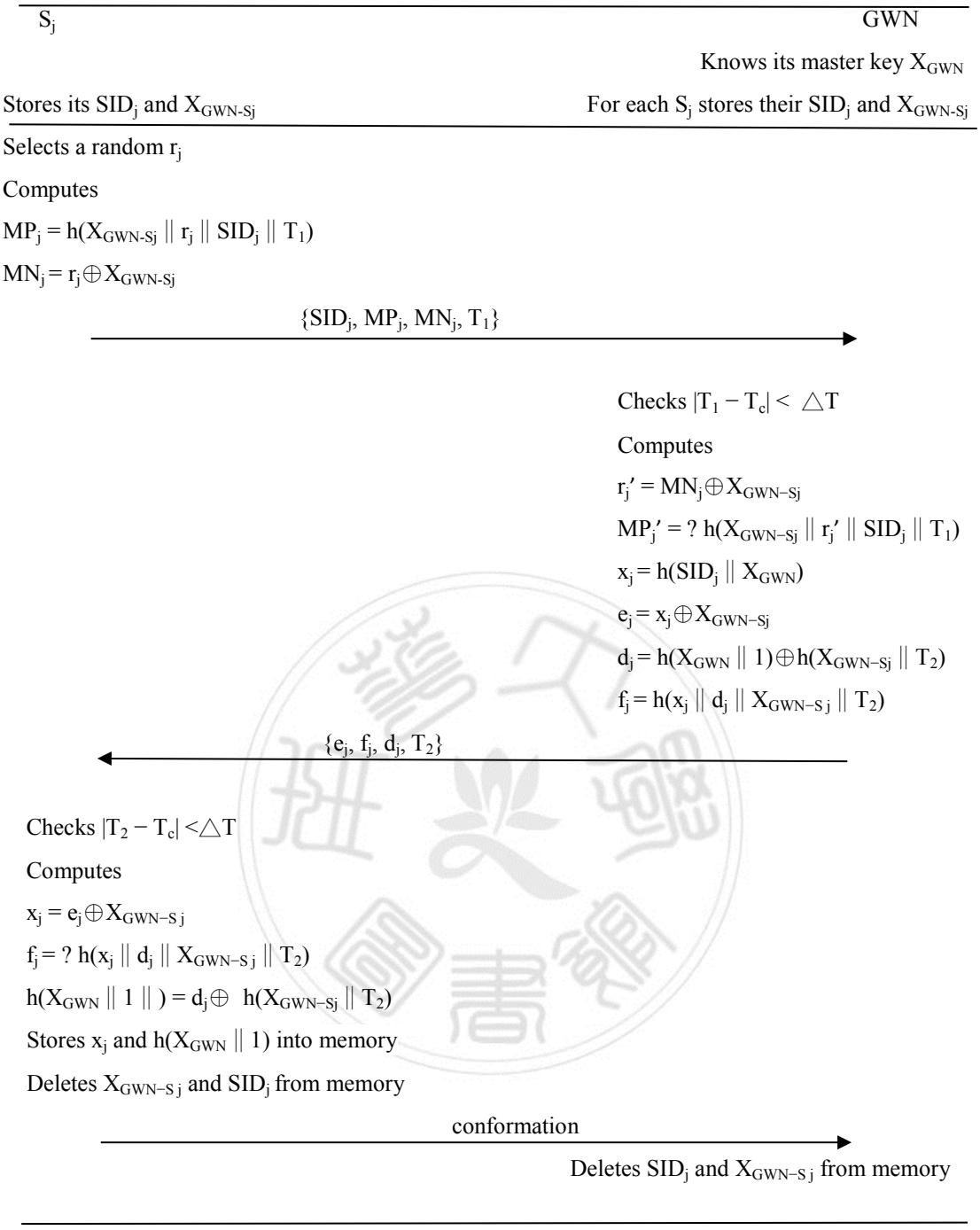

Fig.2. Sensor node registration phase of Farash *et al.*'s scheme

(a) Login phase

U_i inserts his SC into a card reader and inputs its username ID_i and password PW_i. SC then verifies the owner of itself with the secret data stored in its memory. First, it computes $MP_i = h(r_i \| PW_i)$, by using PW_i and the stored r_i. SC then computes the value of $e_i' = h(MP_i \| ID_i)$ and compares it with the stored e_i to see if they are equal. If they are, SC confirms the legitimacy of U_i.

U_i	S_j	GWN
Knows its ID_i , PW_i	Stores SID_j , x_j and $h(X_{GWN} \| 1)$	Stores its master key X_{GWN}
Has a SC = { r_i, e_i, f_i, g_i }		

User

Inserts SC into a terminal

Inputs ID_i' and PW_i'

SC computes

$MP_i' = h(r_i \| PW_i')$

$e_i = ?\ h(MP_i' \| ID_i')$

$d_i = f_i \oplus h(MP_i' \| e_i)$

$h(X_{GWN}) = g_i \oplus h(MP_i' \| d_i)$

$M_1 = ID_i' \oplus h(h(X_{GWN}) \| T_1)$

Chooses a random nonce K_i

$M_2 = K_i \oplus h(d_i \| T_1)$

$M_3 = h(M_1 \| M_2 \| K_i \| T_1)$

Chooses S_j

$\{M_1, M_2, M_3, T_1\}$ →

Checks $|T1 - Tc| < \triangle T$

$ESID_j = SID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$

Chooses a random nonce K_j

$M_4 = h(x_j \| T_1 \| T_2) \oplus K_j$

$M_5 = h(SID_j \| M_4 \| T_1 \| T_2 \| K_j)$

$\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}$ →

Checks $| T_2 - Tc| < \triangle T$

$SID_j' = ESID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$

$x_j' = h(SID_j' \| X_{GWN})$

$K_j' = M_4 \oplus h(x_j' \| T_1 \| T_2)$

$M_5 = ?\ h(SID_j' \| M_4 \| T_1 \| T_2 \| K_j')$

$ID_i' = M_1 \oplus h(h(X_{GWN}) \| T_1)$

$d_i' = h(ID_i' \| X_{GWN})$

$K_i' = M_2 \oplus h(d_i' \| T_1)$

$M_3 = ?\ h(M_1 \| M_2 \| K_i' \| T_1)$

$M_6 = K_j' \oplus h(d_i' \| T_3)$

$M_7 = K_i' \oplus h(x_j' \| T_3)$

$M_8 = h(M_6 \| d_i' \| T_3)$

$M_9 = h(M_7 \| x_j' \| T_3)$

← $\{M_6, M_7, M_8, M_9, T_3\}$

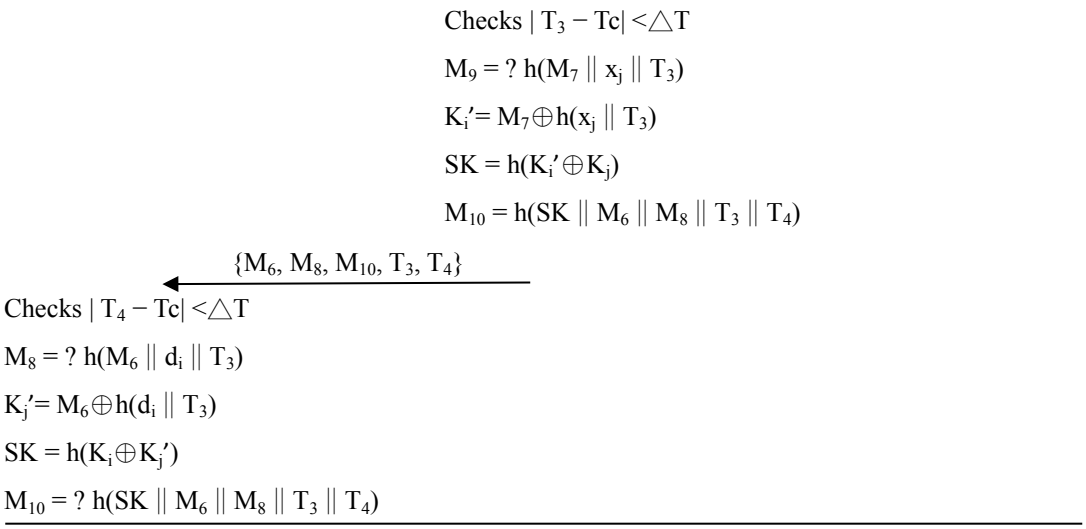

Fig.3. Login and authentication phase of Farash *et al.*'s scheme

(b) Authentication phase

SC first computes $d_i = f_i \oplus h(MP_i || e_i)$, by using the stored values of f_i and e_i, and the computed MP_i, it then computes $h(X_{GWN}) = g_i \oplus h(MP_i || d_i)$, by using the stored g_i , the computed d_i and MP_i. After that, it then computes $M_1 = ID_i \oplus h(h(X_{GWN}) || T_1)$ and randomly chooses a secret nonce K_i to calculate $M_2 = K_i \oplus h(d_i || T_1)$, where T_1 is the current timestamp. Finally, SC computes $M_3 = h(M_1 || M_2 || K_i || T_1)$ and sends the authentication message $\{M_1, M_2, M_3, T_1\}$ to the sensor node S_j via an insecure channel. After receiving the message from U_i, S_j first checks to see whether ($|T1 - Tc| < \triangle T$) holds. If it holds, S_j computes $ESID_j = SID_j \oplus h(h(X_{GWN} || 1) || T_2)$ and randomly chooses a nonce K_j to compute the value $M_4 = h(x_j || T_1 || T_2) \oplus K_j$, where x_j is the stored value, T_1 is U_i's initial timestamp, and T_2 S_j's current timestamp. S_j then uses value M_4, its identity SID_j, K_j, and the timestamps to compute $M_5 = h(SID_j || M_4 || T_1 || T_2 || K_j)$, and sends message $\{M_1, M_2, M_3, T_1, T_2, ESID_j, M_4, M_5\}$ to GWN.

After receiving the message from S_j, GWN first checks for a replay attack. If it does not happen, GWN first computes S_j's identity $SID_j = ESID_j \oplus h(h(X_{GWN} || 1) || T_2)$, by using $ESID_j$ and T_2 both received in the message, alongside with its own secret master key X_{GWN}. After that, GWN computes the values $x_j = h(SID_j || X_{GWN})$ and $K_j = M_4 \oplus h(x_j || T_1 || T_2)$ by using the received values M_4, T_1 and T_2. It then verifies the legitimacy of S_j by computing $M_5 = h(SID_j || M_4 || T_1 || T_2 || K_j)$ and comparing whether M_5 is equal to the received one. If it is, GWN confirms that S_j is authentic. It then computes $ID_i = M_1 \oplus h(h(X_{GWN}) || T_1)$, $d_i = h(ID_i || X_{GWN})$, and $K_i = M_2 \oplus h(d_i || T_1)$, and checks whether the received M_3 is equal to $h(M_1 || M_2 || K_i || T_1)$. If it is, GWN confirms the legitimacy of U_i and prepares four auxiliary values M_6, M_7, M_8

and M_9 by computing $M_6 = K_j \oplus h(d_i \| T_3)$, $M_7 = K_i \oplus h(x_j \| T_3)$, $M_8 = h(M_6 \| d_i \| T_3)$, and $M_9 = h(M_7 \| x_j \| T_3)$, respectively. GWN finally sends them to S_j.

If S_j receives the confirmation message from GWN, it knows that U_i is legitimate and then checks for any replay attack. If it does not happen, S_j checks the legitimacy of the received message by calculating $M_9 = h(M_7 \| x_j \| T_3)$ and comparing it with the received one. If the verification holds, S_j computes $K_i = M_7 \oplus h(x_j \| T_3)$ and constructs the session key $SK = h(K_i \oplus K_j)$. Finally, it computes $M_{10} = h(SK \| M_6 \| M_8 \| T_3 \| T_4)$ and sends $\{M_6, M_8, M_{10}, T_3, T_4\}$ to U_i.

U_i also checks for any replay attacks and verifies the legitimacy of the received message to avoid any GWN or S_j impersonation attacks. If a replay attack is ruled out, U_i computes the value $M_8 = h(M_6 \| d_i \| T_3)$ and compares it to the received one. If they are equal, it stands for that U_i successfully verifies GWN. After successfully authenticating GWN, U_i calculates $K_j = M_6 \oplus h(d_i \| T_3)$ and $SK = h(K_i \oplus K_j)$. And verifies the legitimacy of SK by comparing whether the received M_{10} is equal to $h(SK \| M_6 \| M_8 \| T_3 \| T_4)$. If they are equal, U_i ensures the authenticity of S_j.

3. Weakness of the scheme

Due to that the smart card stores the parameters f_i, e_i, g_i ,r_i and the user himself can compute the value MP_i, if the user plays the role of an insider attacker, he can compute his own $d_i = f_i \oplus h(MP_i \| e_i)$ and $h(X_{GWN}) = g_i \oplus h(MP_i \| d_i)$. That is, each insider can know the value $h(X_{GWN})$. Under this situation, we can see that their scheme suffers both (1) The smart card loss password guessing attack, and (2) Anonymity breach. We describe them both in the following.

3.1 The smart card loss password guessing attack

If a user loses his smart card which is then obtained by an insider attacker, the insider can launch a smart card loss password guessing attack as follows.The insider first calculates $A = g_i' \oplus h(X_{GWN})$ and guesses the lost card owner's password as pw_i'. He then computes $MP_i' = h(r_i' \| pw_i')$, $d_i' = f_i' \oplus h(MP_i' \| e_i')$, and $h(MP_i' \| d_i')$, where r_i', g_i', f_i', e_i' are the parameters stored in the lost smart card. That is, if the attacker guesses the right password pw_i', he will obtain the user's d_i', then the computed value $h(MP_i' \| d_i')$ will definitely equals to A. Therefore, the attacker can confirm that he succeeds.

3.2 Anonymity breach

Due to the two equations, $M_1 = ID_i \oplus h(h(X_{GWN}) \| T_1)$ and $ESID_j = SID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$, and both of the messages transferred in the login and authentication phase, $\{M_1, M_2, M_3, T_1\}$ from U_i to S_j and $\{M_1, M_2, M_3, T_1, T_2, ESID_j,$

M_4, M_5} from S_j to GWN, where T_1, T_2 are the current timestamps, an insider user can compute $ID_i = M_1 \oplus h(h(X_{GWN}) \| T_1)$ from the calculated $h(X_{GWN})$ and an insider sensor node can compute $SID_j = ESID_j \oplus h(h(X_{GWN} \| 1) \| T_2)$ from the stored $h(X_{GWN} \| 1)$, respectively. Thus, their scheme does not possess the anonymous property for both user and sensor node.

4. Modification

From the weaknesses found in Section 3, we note that the key point is the insider can obtain GWN's secret $h(X_{GWN})$. To further disguise it, we modify the messages in the registration phase and the login and authentication phase as follows. We also show the results in Fig4 and 5 respectively.

4.1 For user i

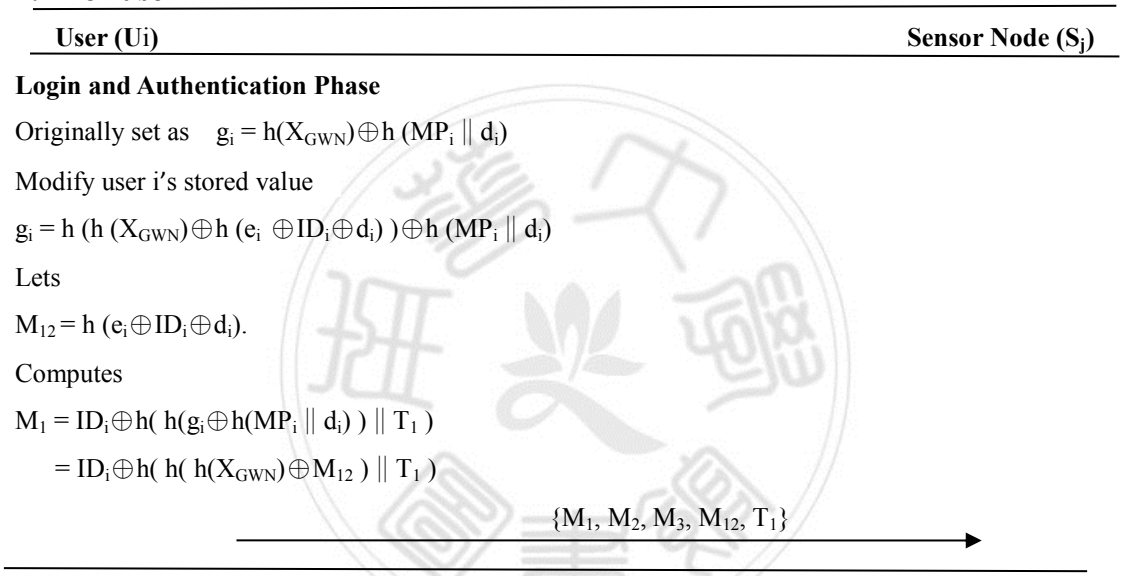

Fig. 4. Modified User (Ui) Login and Authentication Phase

First, we modify user i's stored value $g_i = h(h(X_{GWN}) \oplus h(e_i \oplus ID_i \oplus d_i)) \oplus h(MP_i \| d_i)$, which is originally set as $h(X_{GWN}) \oplus h(MP_i \| d_i)$. Hence, $h(h(X_{GWN}) \oplus h(e_i \oplus ID_i \oplus d_i)) = g_i \oplus h(MP_i \| d_i)$ in the login and authentication phase of the user side. Let $M_{12} = h(e_i \oplus ID_i \oplus d_i)$. Then, the user computes $M_1 = ID_i \oplus h((g_i \oplus h(MP_i \| d_i)) \| T_1) = ID_i \oplus h(h(h(X_{GWN}) \oplus M_{12}) \| T_1)$ and transfers the authentication message $\{M_1, M_2, M_3, M_{12}, T_1\}$ to the sensor node S_j.

In the modified registration phase of GWN, GWN computes $o = h (X_{GWN} \oplus r_g)$, $p = h(X_{GWN} \| r_s)$ and sends message $\{ r_s, o, p\}$ to S_j . S_j stores r_s , o, p. In the login phase, S_j selects a random number r_j and computes $y_j = h(o) \oplus r_j$, $ps = h(p \| r_s)$. In the authentication phase, S_j computes $ESID_j = SID_j \oplus h(h(ps) \| T_2) \oplus y_j$, $z_j = y_j \oplus h(h(ps) \| T_2)$ and sends message $\{M_1, M_2, M_3, M_{12}, T_1, T_2, ESID_j, M_4, M_5, r_s, z_j\}$ to GWN. Then GWN computes $ps = h(h(X_{GWN} \| r_s) \| r_s)$, $r_j = z_j \oplus h(o) \oplus h(h(ps) \|$

T_2), $y_j = h(o) \oplus r_j$ and $SID_j = ESID_j \oplus h(h(ps) \| T_2) \oplus y_j$. GWN then selects nonce r_s'

4.2 For the sensor node S_j

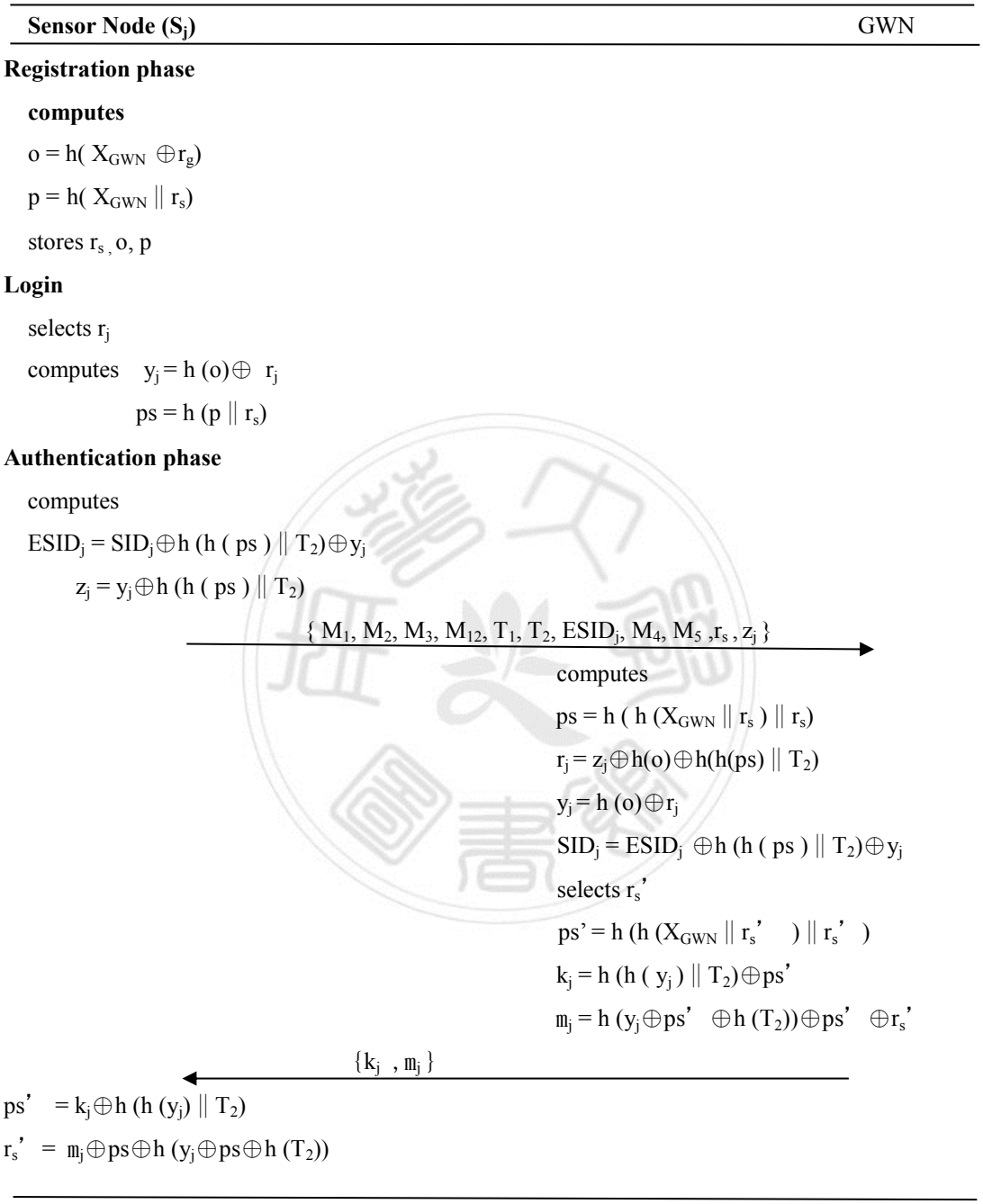

Fig. 5. Modified GWN Registration phase and Sensor Node Authentication Phase

and computes $ps' = h(h(X_{GWN} \| r_s') \| r_s')$, $k_j = h(h(y_j) \| T_2) \oplus ps'$, $m_j = h(y_j \oplus ps' \oplus h(T_2)) \oplus ps' \oplus r_s'$. Then GWN sends message $\{k_j, m_j\}$ to S_j. S_j computes $ps' = k_j \oplus h(h(y_j) \| T_2)$ and $r_s' = m_j \oplus ps \oplus h(y_j \oplus ps \oplus h(T_2))$. After the above modification, we can see that even if an insider obtains a lost card and knows the parameter e_i,

however, from $g_i = h(h(X_{GWN}) \oplus h(e_i \oplus ID_i \oplus d_i)) \oplus h(MP_i \| d_i)$, he cannot compute the value $h(X_{GWN})$. Because it is now further xored by $h(e_i \oplus ID_i \oplus d_i)$ and protected in the outer hash function. Due to the one-way hash function and the unknown values of both ID_i and d_i, each user cannot obtain $h(X_{GWN})$ to launch an insider attack, because $h(X_{GWN})$ does not equal to $g_i \oplus h(MP_i \| d_i)$.

Hence, the smart card loss password guessing attack does not exist. And also, he may corrupt S_j, to obtain r_s, o, and p, however, without the knowledge of gateway node's secret X_{GWN} and r_j, he cannot calculate $SID_j = ESID_j \oplus h(h(ps) \| T_2) \oplus y_j$, where $y_j = h(o) \oplus r_j$, $o = h(X_{GWN} \oplus r_g)$. Thus, the anonymity breach is patched.

4.3 Password change phase

In addition our proposed scheme enables a registered user U_i to change its password. This security feature can be done offline by only using only the smart card SC. The U_i can freely change its password at will without affecting the authentication process or without the need of changing any data by the GWN or any sensor node side. An illustration of the phase is depicted in Fig. 6. In order to change the password, U_i first needs to login to the SC using the ID_i and current PW_i. After SC verifies U_i by the equation $e_i = ?\ h(MP_i \| ID_i)$, it then proceeds with changing the current password PW_i with the new PW_i'. For this purpose the SC needs to change all the values stored in the memory, including the old password PW_i. Prior to this, the SC needs to compute the

U_i
Knows its ID_i and PW_i
Has a SC = { r_i, e_i, f_i, g_i }
User: Inserts SC into a terminal
User: Inputs PW_i and ID_i
SC: $MP_i = h(r_i \| PW_i)$
SC: $e_i = ?\ h(MP_i \| ID_i)$
SC: $d_i = f_i \oplus h(MP_i \| e_i)$
SC: $h(X_{GWN}) = g_i \oplus h(MP_i \| d_i)$
User: Chooses and inputs new password PW_i'
SC: $MPi' = h(r_i \| PW_i')$
SC: $e_i' = h(MP_i' \| ID_i)$
SC: $f_i' = d_i \oplus h(MP_i' \| e_i')$
SC: $g_i' = h(X_{GWN}) \oplus h(MP_i' \| d_i)$
SC: Changes e_i with e_i'
SC: Changes f_i with f_i'

SC: Changes g_i with g_i'

Fig.6. U_i password change phase of the proposed scheme

values $d_i = f_i \oplus h(MP_i||e_i)$ and $h(X_{GWN}) = g_i \oplus h(MP_i \,||\, d_i)$ by using the current versions of e_i, MP_i and g_i. After this, the SC can compute the new values of e_i', f_i' and g_i' by using the new password PW_i' (i.e. $MP_i' = h(r_i \,||\, PW_i')$) chosen by the U_i. Having computed the new values of e_i', f_i' and g_i', the SC substitutes these to the corresponding old values and thus successfully completes the password change phase.

5. Conclusions

In this paper, we show that Farash *et al.'*s scheme is flawed, because it suffers from (1) The smart card loss password guessing attack. and (2) Anonymity breach. We have described the reasons in Section 3. To further disguise it, we modify the messages in the registration phase and the login and authentication phase, respectively. From the analysis shown in Section 4, we conclude that we have corrected the security issues. And from Section 5, we determine that our modification is secure.

References

[1] Chun-Ta Li, Min-Shiang Hwang, *"An efficient biometrics-based remote user authentication scheme using smart cards"*, Journal of Network and Computer Applications, Volume 33, Issue 1, January 2010, Pages 1–5

[2] Wen-Chung Kuo, Hong-Ji Wei, Jiin-Chiou Cheng, *"An efficient and secure anonymous mobility network authentication scheme"*, journal of information security and applications 19 (2014) 18-24

[3] Jue-Sam Chou, Yalin Chen, *"An Efficient Two-Pass Anonymous Identity Authentication Protocol Using a Smart Card"*, Vol 63, No. 8;Aug 2013

[4] Ding Wang, Ping Wang, *"Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks"*, Ad Hoc Networks 20 (2014) 1–15

[5] *"Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity"*, Ding Wang, Nan Wang b, Ping Wang, Sihan Qing, Information Sciences 321 (2015) 162–178

[6] Muhamed Turkanovic´, Boštjan Brumen, Marko Hölbl, *"A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion"*, Ad Hoc Networks 20 (2014) 96–112

[7] Kaiping Xue, Peilin Hong, Changsha Ma, *"A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture"*, Journal of Computer and System Sciences 80 (2014) 195–206

[8] Ding Wang, Ping Wang, *"On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions"* Computer Networks 73 (2014) 41–57

[9] Chun-Ta Li, Cheng-Chi Lee , *"A novel user authentication and privacy preserving scheme with smart cards for wireless communications"*, Mathematical and Computer Modelling 55 (2012) 35–44

[10] Ding Wang, Ping Wang,*"Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks"*, Ad Hoc Networks 20 (2014) 1–15

[11] Mohammad Sabzinejad Farasha, Muhamed Turkanovic, Saru Kumaric,Marko Hölblb,*"An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things*

environment" Ad Hoc Networks 36 (2016) 152–176

[12] Celia Li, Uyen Trang Nguyen, Hoang Lan Nguyen, Nurul Huda, "*Efficient authentication for fast handover in wireless mesh networks*", computers & securit y 37(2013) I 24 -I 42

[13] I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang, "*A password authentication scheme over insecure networks*", Journal of Computer and System Sciences, Vol. 72, No. 4, pp. 727-740, 2006.

附錄

符 號 說 明

Table 1. notations definitions

Notation table
ID_i : user $_i$'s identity.
PW_i : user $_i$'s password.
r_i : user $_i$'s random number.
GWN : gate way node.
H(.) : a collison free one-way hash function.
$\|$: concatenation operation.
$\oplus$: bitwise Xor operation.
SC : smart card.
U_i : the $_i$th user.
S_j : the $_j$th sensor node.
SID_j : sensor node's identity.
X_{GWN} : gate way node's secret.
$X_{GWN-S\,j}$: gate way node's and sensor node's secret.
T_1 : fist timestamp.
T_2 : second timestamp.
T_3 : third timestamp.
SK : session key
T_c : standard time
ΔT :Time interval for the allowed transmission delay