An Improved Two-Factor Mutual Authentication Scheme with Key Agreement in Wireless Sensor Networks

Jiping Li[1], Yaoming Ding[1], Zenggang Xiong[1]and Shouyin Liu[2]
[1] School of Computer and Information Science, Hubei Engineering University
Xiaogan 432000, China
[e-mail: oucljp2012@yahoo.com]
[2] College of Physical Science and Technology, Central China Normal University
Wuhan 430079, China
[e-mail: syliu@phy.ccnu.edu.cn]
*Corresponding author: Yaoming Ding

Received April 30, 2017; revised June 24, 2017; accepted July 18, 2017; published November 30, 2017

Abstract

As a main component of Internet of Things (IoTs), the wireless sensor networks (WSNs) have been widely applied to various areas, including environment monitoring, health monitoring of human body, farming, commercial manufacture, reconnaissance mission in military, and calamity alert etc. Meanwhile, the privacy concerns also arise when the users are required to get the real-time data from the sensor nodes directly. To solve this problem, several user authentication and key agreement schemes with a smart card and a password have been proposed in the past years. However, these schemes are vulnerable to some attacks such as offline password guessing attack, user impersonation attack by using attacker's own smart card, sensor node impersonation attack and gateway node bypassing attack. In this paper, we propose an improved scheme which can resist a wide variety of attacks in WSNs. Cryptanalysis and performance analysis show that our scheme can solve the weaknesses of previously proposed schemes and enhance security requirements while maintaining low computational cost.

Keywords: Mutual authentication, key-agreement, smart card, password, wireless sensor networks

The authors gratefully thank for the helpful suggestions of reviewers. This work is funded by Natural Science Foundation of Hubei Province of China under Grant No.2014CFB577 and partly supported by the National Natural Science Foundation of China under Grant No.61370223.

https://doi.org/10.3837/tiis.2017.11.021 **ISSN : 1976-7277**

1. Introduction

Internet of Things (IoTs) is a novel paradigm and rapidly gains ground in the scenario of modern wireless telecommunications. A variety of pervasive things around us such as radio frequency identification tags, wireless sensor nodes, actuators, and mobile phones, etc., interact with each other and cooperate with their neighbors to reach common goals. US National Intelligence Council foresees that by 2025 internet nodes may reside in everyday things-food packages, furniture, paper documents, and more [1]. Though widespread diffusion of IoTs could contribute invaluably like the present internet to economic development, possible security threats should not be neglected. Towards the IoTs security, current researches mainly focus on three aspects: system security, network security and application security [2]. Wireless sensor networks (WSNs), which are the main component of IoTs, are used to collect data by deploying tens to thousands sensors in the target area [3, 4]. WSNs have been recently applied in all sorts of fields such as environmental monitoring, health monitoring of human body, farming, commercial manufacture, reconnaissance mission in military, and calamity alert [3, 4, 7, 9, 10]. Different from traditional wireless networks, sensor nodes in WSNs work in a limited power, limited storage capacity, limited computing ability, and limited communication ability environment [3, 4, 6, 7, 15, 16]. In general, we send user queries to and receive user queries from gateway node (GW). However, in some specific applications, users are required to get real-time data from sensor nodes directly instead of from the GW [3, 6, 7, 12]. Hence, how to permit only legitimate users to access the WSNs becomes very important.

To ensure the security of WSNs, several user authentication schemes have been proposed in the past decades. In 2006, a dynamic user authentication scheme was proposed by Wong et al. [5] by using only hash functions to improve sensor node's computing efficiency. In 2007, Tseng H. R. et al. [6] pointed out that Wong et al.'s scheme has the vulnerability to replay and forgery attacks, and proposed a dynamic user authentication scheme with low computation cost for WSNs. In 2009, Das [7], however, demonstrated possible attacks such as many logged-in users with the same login-id threats as well as stolen-verifier attacks in Wong et al.'s scheme. To eliminate these weaknesses, an improved user authentication scheme in WSNs was proposed by Das with the help of a smart card and a password. In the subsequent years, several researchers, however, demonstrated that Das's scheme is still susceptive to some attacks. In 2010, Chen and Shih [11] pointed out that Das's scheme cannot provide mutual authentication between users and GW, and then put forward a mutual authentication scheme between two of the communicating parties which are composed of the user, the GW, and the sensor node. In 2010, He et al. [12] insisted that Das's scheme is susceptive to insider attacks as well as impersonation attacks. In the same year, Khan, M. K. and Alghathbar, K. [10] pointed out that Das's scheme has security weaknesses against GW bypassing attacks as well as privileged-insider attacks. In 2012, Vaidya et al. [13] pointed out that some attacks such as stolen smart card attacks, sensor node impersonation with node capture attacks are possible in Das's scheme, Khan and Alghathbar's scheme, and Chen and Shih's scheme. In addition, he insisted that there is no key agreement in Das's scheme. To overcome the pitfalls in the above mentioned schemes, Vaidya et al. put forward a novel two-factor user authentication scheme with key agreement for WSNs. In 2014, Kim et al. [17], however, pointed out that Vaidya et at.'s scheme [13] is vulnerable to GW bypassing attacks and user impersonation attacks either using secret data stored in sensor nodes or using an attacker's own smart card. To remedy the security flaws in Vaidya et al.'s scheme [13], Kim et al. proposed an improved two-factor mutual authentication with key agreement in WSNs by storing secret data in unique cipher text

form in each node. However, I-Pin Chang et al. [18] in 2015 analyzed the weaknesses of Kim et al.'s scheme, which are vulnerable to impersonation attacks, lost smart card attacks, man-in-the-middle attacks, violation of session key security, and invasion of user's privacy. To eliminate these weaknesses, I-Pin Chang et al. proposed an efficient and secure authentication and key agreement scheme for WSNs based on Kim et at.'s scheme. However, in the current research, we found that Kim et al.'s scheme is still vulnerable to some attacks such as offline password guessing attacks, user impersonation attacks, sensor node impersonation attacks as well as gateway node bypassing attacks, besides the weaknesses pointed out by I-Pin Chang et al.

In this study, we first review Kim et al.'s scheme, and then analyze the weaknesses of Kim et al.'s scheme in terms of offline password guessing attack, user impersonation attack, sensor node impersonation attack, and gateway node by passing attack. To eliminate the weaknesses in Kim et al.'s scheme, we propose an improved user authentication and key agreement scheme for WSNs based on Kim et al.'s scheme. Finally, cryptanalysis and performance analysis are presented to show that our scheme not only solves the weaknesses of previously proposed scheme, but also enhances security requirements while maintaining low computational cost.

The remainder of the paper is organized as follows. Section 2 presents a review of Kim et al.'s scheme. Section 3 is devoted to analyzing the security of Kim et al.'s scheme. An improved scheme is put forward in section 4. Security analysis of the proposed scheme is given in section 5, and performance analysis is followed in section 6. Finally, section 7 gives conclusions of this paper.

2. Review of Kim et al.'s Scheme

In this section, we first list notations adopted in this paper, and then briefly review Kim et al.'s two-factor authentication and the key agreement scheme for WSNs. Kim et al.'s scheme [17] comprises registration, login, authentication and key agreement, and password change phases, which are described from subsection 2.1 to 2.4. The notations adopted in the remainder of this paper are shown in **Table 1**.

Table 1. Notations used in this paper

Symbol	Description
U_i	$i-th$ user
S_j	$j-th$ sensor node
GW	Gateway node
ID_i, pw_i	Identity and password of U_i
SID_j	Identity of S_j
ID_S	Identify of smart card
K	Secret key known to only GW
x_s	Secret value generated by GW and shared between only GW and S_j
$h(\bullet)$	One-way hash function
RN_j, RN_i	Random nonce of S_j and S_i respectively
$\oplus$, $\|\|$	XOR and concatenation operation
K_S	Session key

$f(x,k)$	Pseudo-random function of variable x with key k
T_i, $T_i^{'}$	Current timestamp of U_i
T_G, $T_G^{'}$	Current timestamp of GW
T_j	Current timestamp of S_j
ΔT	The maximum of transmission delay time permitted

2.1 Registration Phase

In the registration phase, U_i selects ID_i and pw_i, and generates a random nonce RN_r, then computes $H\_PW_i=h(pw_i||RN_r)$ and sends the registration request $\{ID_i, h(pw_i)\}$ to GW. Once receiving the registration request from U_i, the GW computes $H\_ID_i=h(ID_i||K)$, $A_i=h(H\_PW_i||Xs_i)\oplus h(H\_ID_i||K)$, $B_i=h(H\_PW_i\oplus Xs_i)$ and $C_i=Xs_i\oplus h(ID_s||H\_PW_i)$, and then personalizes a smart card with ID_s, H_ID_i, $h(\cdot)$, A_i, B_i and C_i. After personalizing the smart card, then the GW sends the smart card to U_i through a secure channel. When receiving the smart card from the GW, U_i computes $X\_PW_i = h(pw_i)\oplus RN_r$ and writes X_PW_i to the smart card. The detailed registration phase of Kim et al.'s scheme is illustrated in **Fig. 1**.

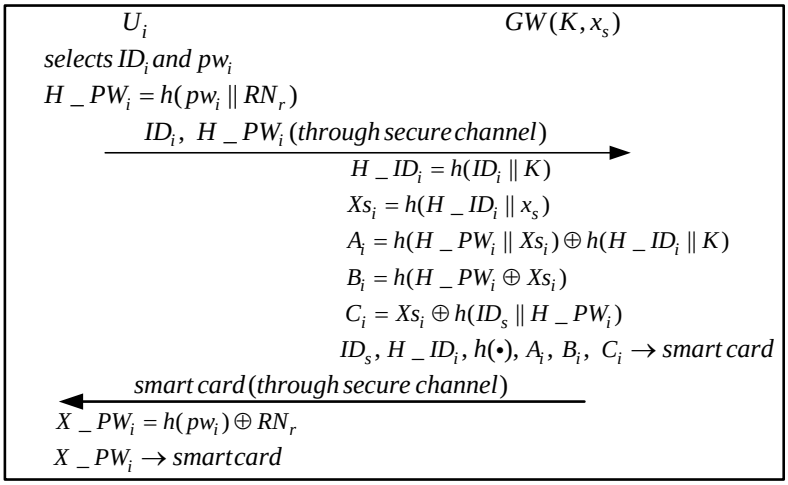

Fig. 1. Registration phase of Kim et al.'s scheme

2.2 Login Phase

In the login phase, U_i inserts his/her smart card into a terminal and inputs ID_i^* and pw_i^*. The smart card computes $B_i^*=h(H\_PW_i^*\oplus Xs_i^*)$ and then verifies $B_i^*=B_i$? If it does not hold, the smart card aborts this request; Otherwise, U_i computes $DID_i=h(H\_PW_i^*||Xs_i^*)\oplus h(Xs_i^*||RN_i||T_i)$, $M_{U_i-G}=h(A_i||Xs_i^*||RN_i||T_i)$ and $v_i=RN_i\oplus Xs_i^*$, where RN_i is a nonce and T_i the current timestamp. Then U_i sends the login request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ to the GW. The detailed login phases of Kim et al.'s scheme are illustrated in **Fig. 2**.

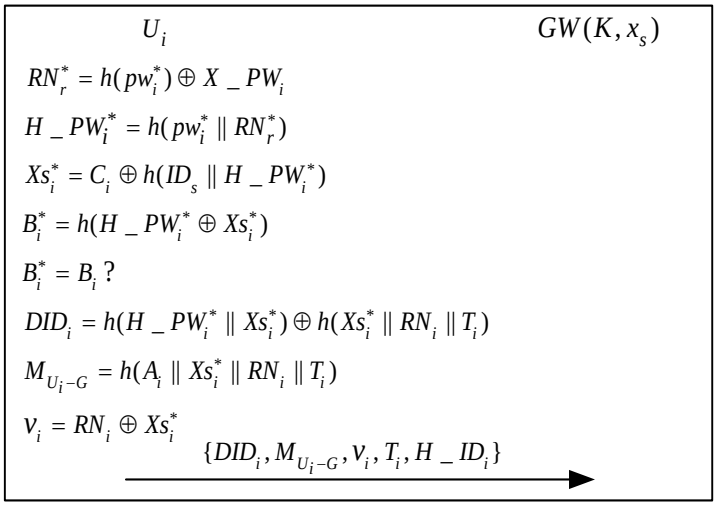

Fig. 2. Login phase of Kim et al.'s scheme

2.3 Authentication and Key Agreement Phase

In this phase, the U_i, GW and S_j send and receive authentication requests from one another to enable U_i and S_j to authenticate each other, and to negotiate a secret key. The detailed phases are illustrated in **Fig. 3**.

When receiving the authentication request from U_i, the GW checks the validity of T_i by verifying if $(T_G - T_i) \leq \Delta T$, where T_G is the current timestamp of the GW system. If it does not hold, the authentication phase is aborted; Otherwise, the GW first computes $M_{U_i-G}^* = h((X^* \oplus h(H\_ID_i \| K)) \| Xs_i^* \| RN_i \| T_i)$ and then verifies $M_{U_i-G}^* = M_{U_i-G}$? , where M_{U_i-G} comes from $U_i's$ login request $\{DID_i, M_{U_i-G}, V_i, T_i, H\_ID_i\}$. If $M_{U_i-G}^* = M_{U_i-G}$ does not hold, the authentication phase is aborted; otherwise, the GW computes $M_{G-S_j} = h(DID_i \| SID_j \| Xs_j \| T_G)$, and then sends authentication request $\{DID_i, M_{G-S_j}, T_G\}$ to S_j, where S_j is the nearest sensor node for U_i.

When receiving the authentication request $\{DID_i, M_{G-S_j}, T_G\}$ from the GW, S_j checks the validity of T_G by verifying if $(T_j - T_G) \leq \Delta T$, where T_j is the current timestamp of S_j. If it does not hold, the authentication phase is aborted; otherwise, S_j computes $M_{G-S_j}^* = h(DID_i \| SID_j \| Xs_j^* \| T_G)$ and verifies $M_{G-S_j}^* = M_{G-S_j}$? , where M_{G-S_j} comes from the GW's authentication request $\{DID_i, M_{G-S_j}, T_G\}$. If $M_{G-S_j}^* = M_{G-S_j}$ does not hold, the authentication phase is aborted; otherwise, S_j computes $y_j = RN_j \oplus Xs_j^*$ and $M_{S_j-G} = h(z_i \| Xs_j^* \| T_j)$, and then sends authentication request $\{y_j, M_{S_j-G}, T_j\}$ to the GW.

When receiving authentication request $\{y_j, M_{S_j-G}, T_j\}$ from S_j, the GW checks the validity of T_j by verifying if $(T_G' - T_j) \leq \Delta T$, where T_G' is the current timestamp of the GW. If it does not

hold, the authentication phase is aborted; otherwise, the GW computes $M^{*}_{S_j-G}=h(z^{*}_i||Xs_j||T_j)$ and verifies $M^{*}_{S_j-G}=M_{S_j-G}$? If it does not hold, the authentication phase is aborted; otherwise, the GW computes $M_{G-U_i}=h(DID_i||M_{G-S_j}||M_{U_i-G}||Xs_i||T^{'}_G)$, $w_i=z^{*}_i\oplus Xs_i$, $y_i=RN_j\oplus Xs_i$ and $q_j=Xs_j\oplus RN_j$, and then sends the authentication request $\{y_i, w_i, M_{G-U_i}, q_j, T^{'}_G\}$ to U_i .

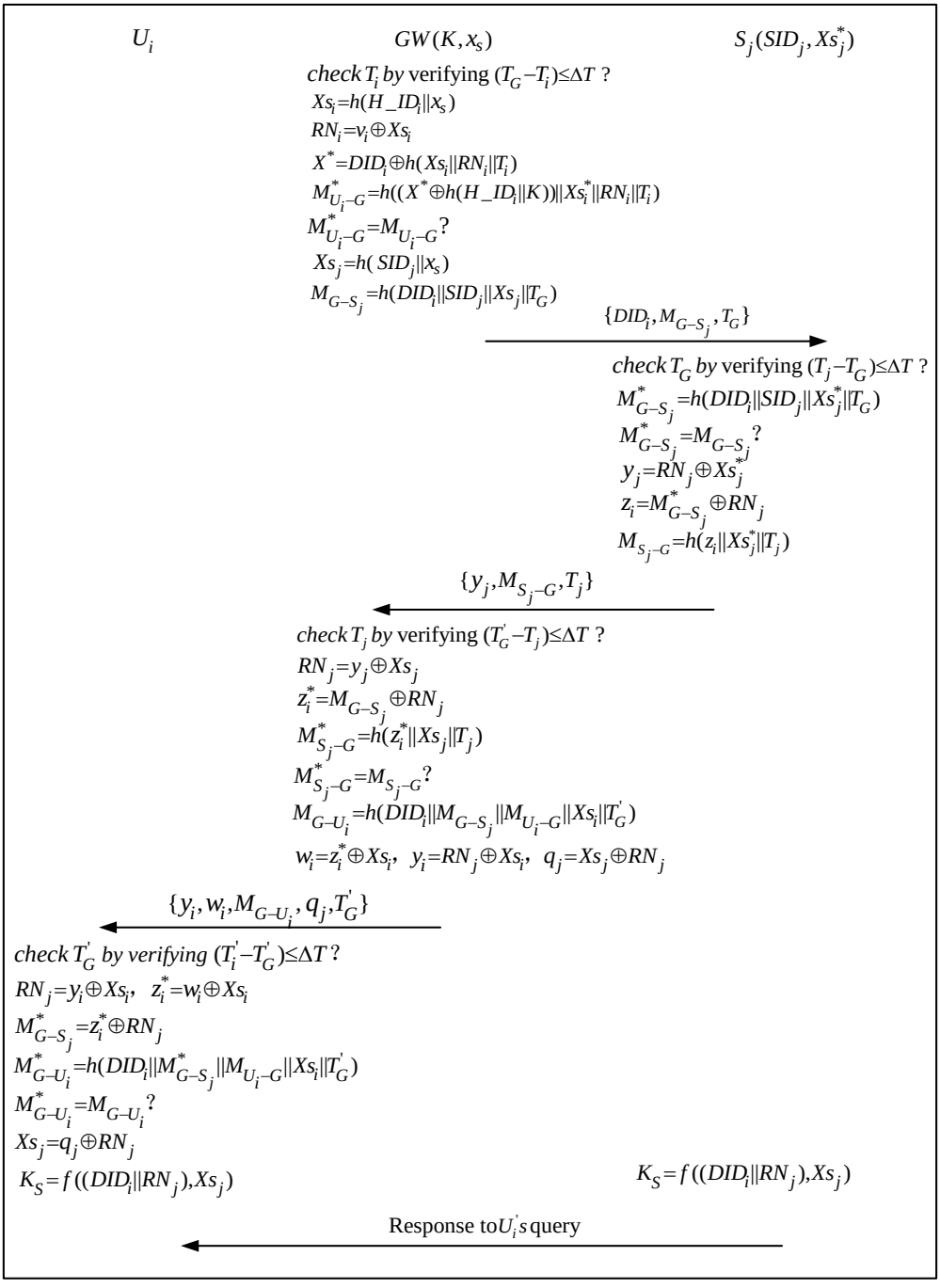

Fig. 3. Authentication-key agreement phase of Kim et al.'s scheme

When receiving authentication request $\{y_i, w_i, M_{G-U_i}, q_j, T_G^{'}\}$ from the GW, U_i checks the validity of $T_G^{'}$ by verifying if $(T_i^{'}-T_G^{'})\leq\Delta T$, where $T_i^{'}$ is the current timestamp of U_i. When it does not hold, the authentication phase is aborted; otherwise, U_i computes $M_{G-U_i}^{*}=h(DID_i||M_{G-S_j}^{*}||M_{U_i-G}||Xs_i||T_G^{'})$ and verifies $M_{G-U_i}^{*}=M_{G-U_i}$?, where M_{G-U_i} comes from the GW's authentication request $\{y_i, w_i, M_{G-U_i}, q_j, T_G^{'}\}$. If it does not hold, the authentication phase is aborted; otherwise, U_i computes $Xs_j=q_j\oplus RN_j$ and $K_S=f((DID_i||RN_j),Xs_j)$. With the computed session key $K_S=f((DID_i||RN_j),Xs_j)$, S_j responses to $U_i^{'}s$ query in a secure way.

2.4 Password Change Phase

In the password change phase, U_i can change the existing password to a new one without communicating with the GW.

When changing password, U_i inserts his/her smart card into a terminal and inputs ID_i^{*}, pw_i^{*} and pw_{ni}, where pw_{ni} is $U_i^{'}s$ new password. Then the smart card computes $RN_r^{*}=h(pw_i^{*})\oplus X\_PW_i$, $H\_PW_i^{*}=h(pw_i^{*}||RN_r^{*})$, $Xs_i^{*}=C_i\oplus h(ID_s||H\_PW_i^{*})$ and $B_i^{*}=h(H\_PW_i^{*}\oplus Xs_i^{*})$, and verifies $B_i^{*}=B_i$?, where B_i is the value stored in the memory of the smart card in the registration phase. If $B_i^{*}=B_i$ does not hold, the password change phase is aborted; otherwise, the smart card computes $H\_PW_{ni}=h(pw_{ni}||RN_r^{*})$, $A_{ni}=A_i\oplus h(H\_PW_i^{*}||Xs_i^{*})\oplus h(H\_PW_{ni}||Xs_i^{*})$, $B_{ni}=h(H\_PW_{ni}\oplus Xs_i^{*})$ and $C_{ni}=Xs_i^{*}\oplus h(ID_s||H\_PW_{ni})$, and then replaces the existing values A_i, B_i and C_i with the new values A_{ni}, B_{ni} and C_{ni}.

3. Security Analysis of Kim et al.'s Scheme

In this section, we give detailed analysis towards the weaknesses of Kim et al.'s authentication and key agreement scheme. From subsection 3.1 to 3.4, four possible attacks are analyzed on the assumption that all messages sent or received between communication parties can be eavesdropped on or intercepted by an attacker. It is also assumed that the data stored in a smart card can be read by an attacker by using side channel attacks [3, 7, 8, 14, 19, 20].

3.1 Offline Password Guessing Attack

Since B_i and C_i are stored in $U_i^{'}s$ smart card, an attacker can obtain $U_i^{'}s$ password by using offline password guessing attack. Besides password PW_i and identity ID_i, some important secrets such as x_S and K can also be derived. The detailed analysis is shown as follows.

Step1 Attacker U_a read ID_s, $h(\bullet)$, H_ID_i, X_PW_i, A_i, B_i and C_i from $U_i^{'}s$ smart card in the manner as those used in the works [3, 7, 8, 14, 19, 20].

Step2 U_a arbitrarily chooses a random nonce as H_PW_i (instead of deriving H_PW_i), and verifies if $B_i=h(H\_PW_i\oplus C_i\oplus h(ID_s||H\_PW_i))$ holds or not. If unsuccessful, repeats step 2; otherwise, the next step proceeds.

Step3 In the similar way used in step 2, U_a arbitrarily guesses a password pw_i (instead of deriving pw_i), and then verifies if $H\_PW_i=h(pw_i||(X\_PW_i\oplus h(pw_i)))$ holds or not. If

unsuccessful, repeats Step 3; otherwise, the next step proceeds.

Step4 Deriving secret Xs_i . Xs_i can be derived according to the equation $Xs_i=C_i \oplus h(ID_s||H\_PW_i)$ since H_PW_i is guessed in Step 2.

Step5 Guessing secret x_s . U_a arbitrarily chooses a random nonce as x_s , and then verifies if $Xs_i=h(H\_ID_i||x_s)$ holds or not. If unsuccessful, repeats step 5; otherwise, the next step proceeds.

Step6 Guessing secret K . U_a arbitrarily chooses a random nonce as K , and then verifies if $A_i=h(H\_PW_i||Xs_i)\oplus h(H\_ID_i||K)$ holds or not. If unsuccessful, repeats step 6; otherwise, the next step proceeds.

Step7 Guessing $U_i^{'}s$ identity. U_a arbitrarily chooses a random nonce as ID_i , then verify if $H\_ID_i=h(ID_i||K)$ holds or not. The guessing and verifying operation repeats until the equation $H\_ID_i=h(ID_i||K)$ holds.

3.2 User Impersonation Attack

A legitimate user can act as an attacker and launch a user impersonation attack with his/her own personalized identity ID_a and password pw_a .The detailed registration and login processes are shown as follows.

Step1 U_a arbitrarily selects ID_a and pw_a .

Step2 U_a generates a random nonce as RN_a and computes $H\_PW_a = h(pw_a \,||\, RN_a)$, and then sends the registration request $\{ID_a, H\_PW_a\}$ to the GW in a secure channel.

Step3 When receiving the registration request $\{ID_a, H\_PW_a\}$ from U_a , the GW successively computes $H\_ID_a = h(ID_a \,||\, K)$, $Xs_a = h(ID_a \,||\, x_s)$, $A_a = h(H\_PW_a \,||\, Xs_a) \oplus h(H\_ID_a \,||\, K)$, $B_a = h(H\_PW_a \oplus Xs_a)$, and $C_a = Xs_a \oplus h(ID_s \,||\, H\_PW_a)$, and personalizes the smart card with ID_s , H_ID_a , $h(\bullet)$, A_a , B_a and C_a , and then sends the smart card to U_a in a secure channel.

Step 4 U_a computes $X\_PW_a=h(pw_a)\oplus RN_a$, and adds X_PW_a to the smart card.

Step 5 U_a inputs ID_a^* and pw_a^* .

Step6 The smart card successively computes $RN_a^*=h(pw_a^*)\oplus X\_PW_a$, $H\_PW_a^*=h(pw_a^*||RN_a^*)$, $Xs_a^*=C_a\oplus h(ID_s||H\_PW_a^*)$, and $B_a^*=h(H\_PW_a^*\oplus Xs_a^*)$, and then verifies if $B_a^*=B_a$? Obviously $B_a^*=B_a$ holds, so the next step proceeds.

Step7 The smart card generates a random nonce as RN_a , and then successively computes $DID_a=h(H\_PW_a^*||Xs_a^*)\oplus h(Xs_a^*||RN_a||T_a)$, $M_{U_a-G}=h(A_a||Xs_a^*||RN_a||T_a)$, and $v_a=RN_a\oplus Xs_a^*$, where T_a is the current timestamp of U_a . Then the smart card sends authentication request $\{DID_a, M_{U_a-G}, v_a, T_a, H\_ID_a\}$ to the GW.

Step8 When receiving the authentication request $\{DID_a, M_{U_a-G}, v_a, T_a, H\_ID_a\}$ from U_a , the GW checks the validity of T_a by verifying if $(T_G-T_a)\le\Delta T$? ,where T_G is the current timestamp of GW system. If it does not hold, the authentication phase is aborted; otherwise, the next step proceeds.

Step9 The GW successively computes $Xs_a=h(H\_ID_a||x_s)$, $RN_a=v_a\oplus Xs_a$, $X^*=DID_a\oplus h(Xs_a||RN_a||T_a)$ and $M_{U_a-G}^*=H((X^*\oplus h(H\_ID_a||K))||Xs_a||RN_a||T_a)$, and then verifies if $M_{U_a-G}^*=M_{U_a-G}$

holds or not. Obviously, $M^*_{U_a-G}=M_{U_a-G}$ holds, so U_a is authenticated by the GW. Once U_a is authenticated by the GW, a mutual authentication between U_a and S_j is completed successfully with the help of the GW. In addition, the smart card and S_j both compute a session key $K_S=f((DID_a||RN_j),Xs_j)$ and share it when communicating.

3.3 Sensor Node Impersonation Attack

In Kim et al.'s scheme, if an attacker U_a captures S_j deployed in unattended environments, he/she can extracts $Xs_j = h(SID_j \| x_s)$ from it. Once eavesdropping on or intercepting $U_i's$ login request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$, U_a forges a valid sensor node S_j and completes mutual authentication between U_i and U_a .With the help of session key $K_S = f((DID_a \| RN_j), Xs_j)$, U_a can send fake message to U_i. The detailed steps are shown as follows.

Step1 U_a strives to capture S_j, and then extracts SID_j and Xs_j stored in S_j.

Step2 U_a eavesdrops on or intercepts $U_i's$ login request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ sent to the GW, and then extracts $U_i's$ dynamic identity DID_i.

Step3 When intercepting the authentication request $\{DID_i, M_{G-S_j}, T_G\}$ from the GW to S_j, U_a checks the validity of T_G by verifying if $(T_a - T_G) \le \Delta T$?, where T_a is the current timestamp of U_a system. If it does not hold, the authentication request is aborted; otherwise, the next step proceeds.

Step4 U_a computes $M^*_{G-U_a}=h(DID_i||SID_j||Xs_j||T_G)$, and then checks if $M^*_{G-U_a}=M_{G-S_j}$? Since it holds, the next step proceeds.

Step5 U_a generates a random nonce RN_a and uses the extracted Xs_j, which is previously stored in S_j, to successively compute $y_a=RN_a \oplus Xs_j$, $z_i=M_{G-U_a} \oplus RN_a$ and $M_{U_a-G}=h(z_i||Xs_j||T_a)$, and then sends the authentication request $\{y_a, M_{U_a-G}, T_a\}$ to the GW.

Step6 When receiving the authentication request $\{y_a, M_{U_a-G}, T_a\}$ from U_a, the GW checks if $(T_G^{'}-T_a) \le \Delta T$?, where $T_G^{'}$ is the current timestamp of the GW. If it does not hold, the authentication request is aborted; otherwise, the next step proceeds.

Step7 The GW computes $RN_a=y_a \oplus Xs_j$, $z_i^*=M_{G-S_j} \oplus RN_a$, $M^*_{U_a-G}=h(z_i^*||Xs_j||T_a)$, and then checks if $M^*_{U_a-G}=M_{U_a-G}$? Since $M^*_{U_a-G}=M_{U_a-G}$ holds, the next step proceeds.

Step8 The GW successively computes $M_{G-U_i} = h(DID_i \| M_{G-Ua} \| M_{Ua-G} \| Xs_i \| T_G^{'})$, $w_i = z_i^* \oplus Xs_i$, $y_i = RN_a \oplus Xs_i$, and $q_a = Xs_a \oplus RN_a$, and then sends the authentication request $\{y_i, w_i, M_{G-U_i}, q_a, T_G^{'}\}$ to U_i.

Step9 When receiving the authentication request $\{y_i, w_i, M_{G-U_i}, q_a, T_G^{'}\}$, U_i checks if $(T_i^{'}-T_G^{'}) \le \Delta T$? If it does not hold, the authentication request is aborted; otherwise, the next step proceeds.

step10 The smart card successively computes $RN_a=y_i \oplus Xs_i$, $z_i^*=w_i \oplus Xs_i$, $M_{G-S_j}=z_i^* \oplus RN_a$, $M^*_{G-U_i}=h(DID_i||M^*_{G-S_j}||M_{U_i-G}||Xs_i||T_G^{'})$, and then checks if $M^*_{G-U_i}=M_{G-U_i}$? Since

$M^{*}_{G-U_i}=M_{G-U_i}$ holds, the mutual authentication between U_i and U_a is completed successfully.

3.4 Gateway Node Bypassing Attack

In Kim et al.'s scheme, U_a can derive Xs_i from the smart card by offline password guessing attack stated in section 3.1, and extract SID_j from a captured sensor node S_j .Once eavesdropping on the authentication request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ from U_i to the GW, U_a can launch gateway node bypassing attack with the obtained Xs_i and SID_j . The detailed phases of gateway node bypassing attack are shown as follows.

Step1 U_a extracts SID_j from a compromised sensor node S_j and derives Xs_i from $U_i's$ smart card in the method stated in section 3.1.

Step2 U_a eavesdrops on the authentication request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ from U_i to the GW.

Step3 With the extracted SID_j , Xs_i , and the intercepted message $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$, U_a successively computes $y_i=RN_a \oplus Xs_i$, $M_{G-S_j}=h(DID_i||SID_j||Xs_i||T_a)$, $z_i^{*}=M_{G-S_j}\oplus RN_a$, $w_i=z_i^{*}\oplus Xs_i$, and $M_{G-U_i}=h(DID_i||M_{G-S_j}||M_{U_i-G}||Xs_i||T_a^{'})$, where T_a and $T_a^{'}$ are the current timestamp of U_a system, RN_a is a random nonce generated by U_a , and then U_a forges the authentication message transmitted from the GW to U_i in authentication-key agreement phase using $\{y_i, w_i, M_{G-U_i}, T_a^{'}\}$.

Step4 When receiving $\{y_i, w_i, M_{G-U_i}, T_a^{'}\}$ from U_a , U_i checks if $(T_U - T_a^{'}) \le \Delta T$, where T_U is the current timestamp of U_i system, and checks if $(T_U - T_a^{'}) \le \Delta T$? If it does not hold, this phase is aborted; otherwise, the next step proceeds.

Step5 The smart card successively computes $RN_a=y_i \oplus Xs_i$, $z_i^{*}=w_i \oplus Xs_i$, $M_{G-S_j}=z_i^{*}\oplus RN_a$, and $M^{*}_{G-U_i}=h(DID_i||M_{G-S_j}||M_{U_i-G}||Xs_i||T_a^{'})$, and then checks if $M^{*}_{G-U_i}=M_{G-U_i}$? Since $M^{*}_{G-U_i}=M_{G-U_i}$, U_i regards $\{y_i, w_i, M_{G-U_i}, T_a^{'}\}$ as being transmitted from the GW. Therefore, U_a can communicate with U_i using session key $K_s=f((DID_i||RN_a), Xs_i)$.

4. The Proposed Scheme

To overcome the weaknesses in Kim et al.'s scheme presented in section 3, we propose an improved scheme in this section. The detailed phases of the proposed authentication and key agreement scheme are presented from subsection 4.1 to 4.4.

4.1 Registration Phase

In Kim et al.'s scheme, any legitimate user can register with the GW using his/her identity ID_i and masked password H_PW_i . This will bring about serious security risks because any attacker may launch user impersonation attack by using his/her smart card. In addition,

$U_i's$ password and some important secrets can be derived through offline password guessing attack. In order to overcome these security weaknesses, the registering process can be improved as follows in detail.

R-1 U_i sends its identity ID_i to GW in a secure channel.

R-2 GW computes $H\_ID_i^*=h(ID_i||K)$ and stores $H\_ID_i^*$ in its memory.

R-3 U_i selects pw_i, generates a random nonce RN_r, and then computes $H\_PW_i=h(pw_i||RN_r)$, and sends registration message $\{ID_i, H\_PW_i\}$ to the GW in a secure channel.

R-4 The GW computes $H\_ID_i=h(ID_i||K)$ and verifies if $H\_ID_i=H\_ID_i^*$. If it does not hold, the registration process is aborted; otherwise, the next step proceeds.

R-5 The GW successively computes $Xs_i=h(H\_ID_i||x_s||K)$, $A_i=h(H\_PW_i||Xs_i)\oplus h(H\_ID_i||K)$, $B_i=h(H\_PW_i\oplus Xs_i\oplus h(K))$, $C_i=Xs_i\oplus h(ID_s||H\_PW_i)$, and personalizes the smart card with ID_s, H_ID_i, $h(\cdot)$, A_i, B_i and C_i, and then delivers the smart card to U_i in secure methods.

R-6 U_i computes $X\_PW_i=h(pw_i)\oplus RN_r$ and adds X_PW_i to the smart card.

4.2 Login Phase

In login phase, U_i inserts his/her smart card into a terminal and inputs ID_i^* and pw_i^*. If the identity of the user is verified, U_i transmits the authentication message to the GW. The following shows the detailed login phase.

L-1 U_i inserts his/her smart card into a terminal and inputs ID_i^* and pw_i^*.

L-2 The smart card successively computes $RN_r^*=h(pw_i^*)\oplus X\_PW_i$, $H\_PW_i^*=h(pw_i^*||RN_r^*)$, $Xs_i^*=C_i\oplus h(ID_s||H\_PW_i^*)$, $h(K)=A_i\oplus h(H\_PW_i^*||Xs_i^*)$, $B_i^*=h(H\_PW_i^*\oplus Xs_i^*\oplus h(K))$, and then compares B_i^* with B_i. If $B_i^*=B_i$, the next step proceeds; otherwise, the login phase is aborted.

L-3 The smart card generates RN_i, and then computes $DID_i=h(H\_PW_i^*||Xs_i^*)\oplus h(Xs_i^*||RN_i||T_i)$, $M_{U_i-G}=h(A_i||Xs_i^*||RN_i||T_i)$, $v_i=RN_i\oplus Xs_i^*$, where T_i represents $U_i's$ the current timestamp. Finally, the smart card transmits the authentication message $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ to the GW.

4.3 Authentication and key Agreement Phase

The authentication and key agreement phase begins when the GW receiving an authentication message from U_i. In this phase, sending and receiving authentication request is performed among U_i, the GW and S_j. The detailed phases are shown as follows.

A-1 The GW checks if $(T_G-T_i)\le\Delta T$?, where T_G represents the GW system's current timestamp. If $(T_G-T_i)\le\Delta T$ holds, the next step proceeds; otherwise, this phase is aborted.

A-2 The GW computes $Xs_i=h(H\_ID_i||x_s||K)$, $RN_i=v_i\oplus Xs_i$, $X^*=DID_i\oplus h(Xs_i||RN_i||T_i)$, $M_{U_i-G}^*=h((X^*\oplus h(H\_ID_i||K))||Xs_i^*||RN_i||T_i)$, and then compares $M_{U_i-G}^*$ with M_{U_i-G}. If

$M^*_{U_i-G}=M_{U_i-G}$, the next step proceeds; otherwise, this phase is aborted.

A-3 GW computes $Xs_j=h(SID_j||x_s)$, $M_{G-S_j}=h(DID_i||SID_j||Xs_j||x_s||T_G)$, where S_j represents the nearest sensor node replying to $U_i's$ request, and then sends the authentication request $\{DID_i, M_{G-S_j}, T_G\}$ to S_j.

A-4 S_j checks if $(T_j-T_G)\leq\Delta T?$, where T_j is the current timestamp of S_j. If it holds, the next step proceeds; otherwise, this phase is aborted.

A-5 S_j computes $M^*_{G-S_j}=h(DID_i||SID_j||Xs^*_j||x_s||T_G)$, where $Xs^*_j=h(SID_j||x_s)$ is stored in S_j before it is deployed in a designated field, and then compares $M^*_{G-S_j}$ with M_{G-S_j}. If $M^*_{G-S_j}=M_{G-S_j}$ holds, the next step proceeds; otherwise, this phase is aborted.

A-6 S_j generates a random nonce RN_j and computes $y_j=RN_j\oplus Xs^*_j$, $z_i=M^*_{G-S_j}\oplus RN_j$, $M_{S_j-G}=h(z_i||Xs^*_j||T_j)$, and then sends the authentication request $\{y_j, M_{S_j-G}, T_j\}$ to the GW.

A-7 The GW checks if $(T^{'}_G-T_j)\leq\Delta T?$, where $T^{'}_G$ is the current timestamp of the GW. If $(T^{'}_G-T_j)\leq\Delta T$ holds, the next step proceeds; otherwise, this phase is aborted.

A-8 The GW successively computes $RN_j=y_j\oplus Xs_j$, $z^*_i=M_{G-S_j}\oplus RN_j$, $M^*_{S_j-G}=h(z^*_i||Xs_j||T_j)$, and then compares $M^*_{S_j-G}$ with M_{S_j-G}. If $M^*_{S_j-G}=M_{S_j-G}$ holds, the next step proceeds; otherwise, this phase is aborted.

A-9 The GW computes $M_{G-U_i}=h(DID_i||M_{G-S_j}||M_{U_i-G}||Xs_i||T^{'}_G)$, $w_i=z^*_i\oplus Xs_i$, $y_i=RN_j\oplus Xs_i$, and $q_j=Xs_j\oplus RN_j$, and then sends authentication request $\{y_i, w_i, M_{G-U_i}, q_j, T^{'}_G\}$ to U_i.

A-10 U_i checks if $(T^{'}_i-T^{'}_G)\leq\Delta T?$, where $T^{'}_i$ is the current timestamp of U_i. If $(T^{'}_i-T^{'}_G)\leq\Delta T$ holds, the next step proceeds; otherwise, this phase is aborted.

A-11 The smart card successively computes $RN_j=y_i\oplus Xs_i$, $z^*_i=w_i\oplus Xs_i$, $M^*_{G-S_j}=z^*_i\oplus RN_j$, and $M^*_{G-U_i}=h(DID_i||M^*_{G-S_j}||M_{U_i-G}||Xs_i||T^{'}_G)$, and then compares $M^*_{G-U_i}$ with M_{G-U_i}. If $M^*_{G-U_i}=M_{G-U_i}$ holds, the next step proceeds; otherwise, this phase is aborted.

A-12 The smart card computes $K_S=f((DID_i||RN_j), Xs_j)$ to obtain a session key, with which U_i can communicate with S_j. Meanwhile, S_j also computes $K_S=f((DID_i||RN_j), Xs_j)$ to share a session key with U_i, where $Xs_j=q_j\oplus RN_j$.

4.4 Password Change Phase

In this phase, U_i can freely change the existing password to a new one without communicating with the GW. The detailed password change phases are shown as follows.

P-1 U_i inserts his/her smart card into a terminal and inputs ID^*_i, pw^*_i and new password pw_{ni}.

P-2 The smart card successively computes $RN^*_r=h(pw^*_i)\oplus X\_PW_i$, $H\_PW^*_i=h(pw^*_i||RN^*_r)$, $Xs^*_i=C_i\oplus h(ID_s||H\_PW^*_i)$, $B^*_i=h(H\_PW^*_i\oplus Xs^*_i)$, and then compares B^*_i with B_i. If

$B_i^*=B_i$ holds, the next step proceeds, otherwise, this phase is aborted.

P-3 The smart card computes $H\_PW_{ni}=h(pw_{ni}\|RN_r^*)$, $A_{ni}=A_i\oplus h(H\_PW_i^*\|Xs_i^*)\oplus h(H\_PW_{ni}\|Xs_i^*)$, $B_{ni}=h(H\_PW_{ni}\oplus Xs_i^*)$, $C_{ni}=Xs_i^*\oplus h(ID_s\|H\_PW_{ni})$, and then replaces the existing values A_i, B_i and C_i with the new values A_{ni}, B_{ni} and C_{ni}.

5. Security Analysis of the Proposed Scheme

In this section, we first analyze the security of the proposed scheme on the assumptions declared in section 3, and discuss the security of our scheme according to the security requirements stipulated in section 4 of Kim et al.'s scheme [17]. Table 2 shows a security comparison of the proposed scheme with related schemes.

Table 2. Security comparison with other related schemes.

Security features	Das's Scheme[7]	Khan and Alghathbar's scheme[10]	Vaidya et al.'s Scheme[13]	Kim et al.'s scheme[17]	I. P. Chang et al.' scheme[18]	The proposed Scheme
Resists offline password guessing attacks	No	No	No	No	No	Yes
Resists replay attacks	Yes	Yes	Yes	Yes	Yes	Yes
Resists user impersonation attacks	No	No	No	No	Yes	Yes
Resists gateway node bypassing attacks	No	No	No	No	Yes	Yes
Resists parallel session attacks	No	No	Yes	Yes	Yes	Yes
Resists sensor node capture attacks	No	No	No	No	No	Yes
Resists lost smart card attacks	No	No	Yes	No	No	Yes
Resists stolen-verifier attacks	Yes	Yes	Yes	Yes	Yes	Yes
Realizes mutual authentication	No	No	Yes	Yes	Yes	Yes
Provides key agreement	No	No	Yes	Yes	Yes	Yes
Provides password change phase	No	Yes	Yes	Yes	Yes	Yes

- *Offline password guessing attacks:* The proposed scheme can resist offline password guessing attacks because another secret $h(K)$ is needed in the guessing equation $B_i=h(H\_PW_i \oplus C_i \oplus h(ID_s||H\_PW_i) \oplus h(K))$. In the guessing equation, B_i, C_i, and ID_s can be extracted from $U_i^{'}s$ smart card, however, it's difficult to guess the hashed password H_PW_i because $h(K)$ cannot be obtained.
- *Replay attacks:* In the proposed scheme, all authentication messages transmitted between communication parties have current timestamps, such as T_i of $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$, so our scheme can resist replay attacks.
- *User impersonation attacks:* In the proposed scheme, an attacker cannot create valid authentication message $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ because he/she cannot compute the secret data x_s. Therefore, user impersonation attacks can be resisted.
- *Gateway node bypassing attacks:* In the proposed scheme, an attacker cannot create valid authentication message $\{y_i, w_i, M_{G-U_i}, q_j, T_G^{'}\}$ because he/she cannot compute the secret data x_s. Therefore, gateway node bypassing attacks can be resisted.
- *Parallel session attacks:* In the proposed scheme, random nonces such as DID_i, M_{U_i-G} and v_i in $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ are contained in all the authentication messages, so our scheme is secure against parallel session attacks.
- *Sensor node capture attacks:* Though secret data such as SID_j and Xs_j^* can be obtained from a sensor node S_j after being captured by an attacker, Xs_i for U_i and x_s for the GW cannot be computed. In addition, secret data of other sensor nodes except S_j cannot be computed yet by the attacker.
- *Stolen smart card attacks and lost smart card attacks:* Though ID_s, H_ID_i, $h(\cdot)$, A_i, B_i, C_i and X_PW_i can be extracted from $U_i^{'}s$ smart card by an attacker U_a, any secret data $h(K)$ or x_s cannot be computed for the attacker. Therefore, stolen smart card attacks and lost smart card attacks can be prevented in the proposed scheme.
- *Attacks by using adversary's own smart card:* In the proposed scheme, valid user's masked identity $H\_ID_i^*=h(ID_i||K)$ is stored in the memory of the GW in advance. In the registration phase, if an attacker U_a hopes to register using his/her own identity ID_a, the registration procedure is aborted because the computed $H\_ID_a=h(ID_a||K)$ by the GW is not equal to $H\_ID_i^*=h(ID_i||K)$. Therefore, attacks by using adversary's own smart card can be resisted in the proposed scheme.
- *Privileged-insider attacks:* Since pw_i is transmitted as a digest of some other secret components, privileged-insider attacks can be prevented in the proposed scheme.
- *Stolen-verifier attacks:* Though all valid users' masked identities are kept in the memory of the GW in the proposed scheme, a valid user's identity ID_i cannot be derived, so the stolen-verifier attacks can be prevented in our scheme.
- *Mutual authentication, key agreement, and password change phase*: In the design of the proposed scheme, mutual authentication between two communicating parties, key agreement between U_i and S_j, and password change phase are also taken into account.

6. Performance Analysis of the Proposed Scheme

Due to the limited resource of sensor nodes, it's very important to conceive an authentication scheme with low computation and low communication cost in WSNs. In this section, we evaluate the computation and communication cost of the proposed scheme in terms of the number of hash and XOR operations. To give a clear illustration, comparison is performed among related schemes: Das'scheme [7], Khan and Alghathbar's scheme [10], Vaidya et al.'s scheme [13], Kim et al.'s scheme [17] and I-Pin Chang et al.'s scheme [18]. Comparing with Kim et al.'s scheme, our scheme can overcome offline password guessing attack, user impersonation attack by using his/her own smart card, sensor node impersonation attack, and gateway node bypassing attack with the increase of 2H operation plus 1X in the registration phase, and 2H plus 2X operations in the login phase, however, and with the decrease of 1X operation in the Authentication and key agreement phase, where H and X represent the number of hash operations and the number of XOR operations, respectively. The detailed comparison results are shown in Table 3 according to the computation and communication cost.

Table 3. Performance comparison with other related schemes.

Phase		**Das's scheme [7]**	**Khan and Alghathbar's scheme [10]**	**Vaidya et al.'s Scheme [13]**	**Kim et al.'s scheme [17]**	**I. P. Chang et al.' scheme [18]**	**Our scheme**
Registration phase	U_i	0	1H	1H	2H+1X	2H+1X	2H+1X
	GW	3H+1X	2H+1X	4H+3X	6H+3X	5H+3X	8H+4X
	S_j	0	0	0	0	0	0
Login phase	U_i	3H+1X	3H+1X	6H+4X	7H+5X	7H+4X	9H+7X
	GW	0	0	0	0	0	0
	S_j	0	0	0	0	0	0
Authentication and key agreement phase	U_i	0	0	1H+3X	1H+4X	2H+1X	1H+3X
	GW	4H+2X	5H+2X	6H+6X	8H+8X	9H+4X	8H+8X
	S_j	1H	2H	2H+2X	2H+2X	3H+1X	2H+2X
Password change phase	U_i	-	3H+2X	8H+6X	9H+7X	9H+7X	9H+7X
	GW	-	0	0	0	0	0
	S_j	-	0	0	0	0	0
Total		11H+4X	16H+6X	28H+24X	35H+30X	37H+21X	39H+32X

7. Conclusions

In this study, we have crypto-analyzed a two-factor mutual authentication with key agreement in WSNs proposed by Kim et al., and demonstrated its vulnerability to offline password guessing attack, user impersonation attack by using his/her own smart card, sensor node impersonation attack and gateway node bypassing attack. To address the security weaknesses in Kim et al.'s scheme, we propose an improved two-factor mutual authentication with key agreement in WSNs. Security analysis and performance comparison show that our scheme can eliminate various weaknesses in the existing user authentication with key agreement schemes in WSNs with negligible increase in computation or communication cost.

References

[1] L. Atzori, A. Iera and G. Morabito, "The internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, June, 2010. Article (CrossRef Link)
[2] H. Ning, H. Liu and L T. Yang, "Aggregated-proof based hierarchical authentication scheme for the Internet of Things," *IEEE trans. on parallel and distribution systems*, vol. 26, no. 3, pp. 657-667, March, 2015. Article (CrossRef Link)
[3] Yoon, E. J., Yoo, K. Y., " Cryptanalysis of robust mutual authentication protocol for wireless sensor networks," in *Proc. of the 10th IEEE International Conference on Cognitive Informatics & Cognitive Computing*, pp. 392-396, August 18-20, 2011. Article (CrossRef Link)
[4] Yick, J., Mukherjee, B., Ghosal, D., "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292-2330, August, 2008. Article (CrossRef Link)
[5] Wong K. H. M., Zheng, Y., Cao, J., Wang S., "A dynamic user authentication scheme for wireless sensor networks, " In *Proc.of the IEEE international conference on sensor networks, ubiquitous, and trustworthy computing*, pp. 244-251, June 5-7, 2006. Article (CrossRef Link)
[6] Tseng H. R., Jan R. H., Yang W, "An improved dynamic user authentication scheme for wireless sensor networks," In *Proc. of the Global Telecommunications Conference*, pp. 986-990, November 26-30, 2007. Article (CrossRef Link)
[7] Das, M. L., "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp.1086-1090, March, 2009. Article (CrossRef Link)
[8] Xu J., Zhu W. T., Feng D. G., "An improved smart card based password authentication scheme with provable security," *Computer Standards Interfaces*, vol. 31, no. 4, pp. 723-728, June, 2009. Article (CrossRef Link)
[9] Nyang D. H., Lee M. K., "Improvement of Das's two-factor authentication protocol in wireless sensor networks," *IACR Cryptology ePrint Archive*, vol. 2009, pp. 1-5, 2009. Article (CrossRef Link)
[10] Khan, M. K., Alghathbar, K., "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp.2450-2459, March, 2010. Article (CrossRef Link)
[11] Chen T. H., Shih W. K., "A robust mutual authentication protocol for wireless sensor networks," *Electronic Telecommunication Research Institute*, vol. 32, no. 5, pp.704-712, October, 2010. Article (CrossRef Link)
[12] He D, Gao Y., Chan S., Chen C., Bu J., "An enhanced two-factor user authentication scheme in wireless sensor networks, "*Ad Hoc Sensor Wireless Networks*, vol. 10, no. 4, pp. 361-371, January, 2010. Article (CrossRef Link)
[13] Vaidya B., Makrakis D., Mouftah H., "Two-factor mutual authentication with key agreement in wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 2, pp. 171-183, April, 2012. Article (CrossRef Link)

[14] Das A. K., Sharma P., Chatterjee S., Sing J. K., "A dynamic password-based user authentication scheme for hierarchical wireless networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp.1646-1656, September, 2012. Article (CrossRef Link)
[15] Li C. T., Weng C. Y., Lee C. C., "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks," *Sensors*, vol. 13, no. 8, pp.9589-9603, July, 2013. Article (CrossRef Link)
[16] Yoo, S. G., Lee H., Kim J., "A performance and usability aware secure two-factor user authentication schemes for wireless sensor networks, "*International Journal of Distributed Sensor Networks*, vol. 2013, no. 2, pp. 543950, January, 2013. Article (CrossRef Link)
[17] Kim J., Lee D., Jeon W., Lee Y. and Won D., "Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks," *Sensors*, vol. 14, no. 4, pp.6443-6462, April, 2014. Article (CrossRef Link)
[18] I-Pin Chang, Tian-Fu Lee, Tsung-Hung Lin and Chuan-Ming Liu, "Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks," *Sensors*, vol. 15, no. 12, pp.29841-29854, November, 2015. Article (CrossRef Link)
[19] Turkanovic M., Holbl M., "An improved dynamic password-based user-authentication scheme for hierarchical wireless sensor networks," *Elektronika Ir Elektrotechnika*, vol. 19, no. 6, pp. 109-116, June, 2013. Article (CrossRef Link)
[20] Xue K., Ma C., Hong P., Ding R., "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, "*Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316-323, January, 2013. Article (CrossRef Link)
[21] Li Jiping, Ding Yaoming, Xiong Zenggang and Liu Shouyin, "An Improved Biometric-based User Authentication Scheme for C/S system," *International Journal of Distributed Sensor Networks*, vol. 2014, no. 2, pp. 275341, January, 2014. Article (CrossRef Link)
[22] Debiao He, Neeraj Kumar, Naveen Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Science*, vol. 321, no. 10, pp. 263-277, November, 2015. Article (CrossRef Link)
[23] Debiao He, Sherali Zeadally, "Authentication protocol for ambient assisted living system," *IEEE Communications Magazine*, vol. 53, no. 1, pp.71-77, January, 2015. Article (CrossRef Link)
[24] Honglong Chen and Wei Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, Part A, pp. 36-50, January, 2015. Article (CrossRef Link)
[25] Honglong Chen, Guoliang Xue and Zhibo Wang, "Efficient and reliable missing tag identificaiton for large-scale RFID systems with unknown tags," *IEEE internet of things Journal*, vol. 4, no. 3, pp. 736-748, February, 2017. Article (CrossRef Link)
[26] Zhibo Wang, Honglong Chen, Qing Cao, Hairong Qi, Zhi Wang and Qian Wang, "Achieving location error tolerant barrier coverage for wireless sensor networks," *Computer Networks*, vol. 112, no. 15, pp. 314-328, January, 2017. Article (CrossRef Link)
[27] Zhibo Wang, Qing Cao, Hairong Qi, Honglong Chen and Qian Wang, "Cost-Effective Barrier Coverage Formation in Heterogeneous Wireless Sensor Networks," *Ad Hoc Networks*, vol. 64, pp. 65-79, September, 2017. Article (CrossRef Link)

Jiping Li was born in Hubei Province, China, in 1972. He received M.S. degree in application of computer from Ocean University of China, Qingdao in 2006, and the Ph.D. degree in radio physics from Central China Normal University, Wuhan in 2012 respectively. He is presently an associate professor in computer science of Hubei Engineering University. His research interests include network security, wireless resource management and application of internet of things.

Yaoming Ding was born in Hubei Province, China, in 1963. He received B.S. and M.S. degree in physic science from Central China Normal University, Wuhan in 1986 and in 2000 respectively. He received Ph.D. degree in Huazhong University of Science and Technology in 2011. He is presently a professor in physic science in Hubei Engineering University. His research interests include optical communication and security of wireless communication.

Zenggang Xiong was born in Hubei Province, China, in 1974. He received M.S degree in computer application from Hubei University in 2005 and Ph.D. degree in computer application from University of Science and Technology Being in 2009 respectively. He is presently a professor in computer science at Hubei Engineering University. His research interest includes cloud computing and big data.

Shouyin Liu was born in Henan Province, China, in 1963. He received BS degree in physics in 1985 and MS degree in radio electronics in 1988 both from Central China Normal University, Wuhan, China, respectively. He received Ph.D. degree from Hanyang University, Korea in 2005 in electronic communication engineering. From 2004, he has been a professor at Central China Normal University. His current research interests include digital communication, WSN and location techniques.