Cryptanalysis of Kim Jiye et al.'s Two-Factor Mutual Authentication with Key Agreement in WSNs

Jiping Li[1], Yaoming Ding[1], Zenggang Xiong[1], Shouyin Liu[2], and Honglai Li[1]
[1] School of Computer and Information Science, Hubei Engineering University, Xiaogan 432000, China
[2] College of Physical Science and Technology, Central China Normal University, Wuhan 430079, China
Email: oucljp2012@yahoo.com; {xgdym2015, xglhl2015}@aliyun.com; jkxxzg2003@163.com; syliu@phy.ccnu.edu.cn

Abstract —User authentication and key management play an important role in the security of WSNs (Wireless Sensor Networks). In WSNs, for some applications, the user needs to obtain real-time data directly from dedicated sensors. For this case, several user authentication schemes have been proposed in recent years. Among these schemes, Kim Jiye et. al's scheme is very novel. However, in the current work, we find that Kim Jiye et. al's scheme is still vulnerable to some attacks such as offline password guessing attack, user impersonation attack using his/her own smart card, sensor node impersonation attack and gateway node bypassing attack. In this paper, we give detailed cryptanalysis of Kim Jiye et. al's two-factor mutual authentication with key agreement in WSNs.

Index Terms—WSN, mutual authentication, key-agreement, smart card, password

I. Introduction

Wireless Sensor Networks (WSNs) are composed of a number of sensors (tens or thousands) that are deployed to collect data in a target area [1], [2]. WSN has been recently applied in various fields, including environment-tal monitoring, healthcare, agriculture, manufacturing, military sensing and tracking, and disaster alert [1]-[5]. The design of specific WSNs is dependent on the given application and the environment under which it operates [1]. In addition, different from traditional wireless net works, sensors in WSNs operate with resource cons-traints such as limited power, low computing and communication ability and small storage capability [1]-[3], [6]-[8]. In WSNs, user queries are generally transmitted to and received from the GW (gateway node). However, in some special applications, user needs to obtain real-time data directly from sensors [1], [3], [8], [9].

In recent years, several two-factor user authentication schemes in WSNs have been proposed. In 2006, Wong *et al*. [10] proposed a dynamic user authentication scheme using only one-way hash functions for computation efficiency on sensor nodes. However, Das [3] in 2009 pointed out that Wong et al.'s scheme cannot prevent some attacks such as many logged-in users with the same login-id threats and stolen-verifier attacks. Das [3] proposed a two-factor user authentication in WSNs using a smart card and a password instead of maintaining a password/verifier table. In the subsequent years, several researchers, however, pointed out that Das's scheme still has certain security flaws. In 2010, Chen and Shih [11] pointed out that Das's scheme does not provide mutual authentication, and proposed a mutual authentication scheme between the user, the gateway, and the sensor nodes. In the same year, He *et al*. [9] insisted that Das's scheme has security weaknesses against insider attacks and impersonation attacks. Khan and Alghathbar [4] pointed out that Das's scheme is vulnerable to gateway node bypassing attacks and privileged-insider attacks. In 2012, Vaidya *et al*. [12] pointed out that the schemes proposed by Das [3], Kan and Alghathbar [4] and Chen and Shih [11] are all insecure against stolen smart card attacks and sensor node impersonation attacks with node capture attacks, and do not provide key agreement. In [12], Vaidya *et al*. proposed a novel two-factor mutual authentication with key agreement scheme to prevent these attacks. In 2014, Kim Jiye *et al*. [13] pointed out that Vaidya et al.'s scheme [12] is vulnerable to gateway node bypassing attacks and user impersonation attacks using secret data stored in sensor nodes or an attacker's own smart card. To remedy the security flaws in Vaidya et al.'s scheme [12], Kim Jiye *et al*. proposed an improved two-factor mutual authentication with key agreement in wireless sensor networks by storing secret data in unique cipher text form in each node. However, we found that Kim Jiye et al.'s scheme still has some security flaws such as offline password guessing attack, user impersona-tion attacks using an attacker's own smart card, sensor node impersonation attacks and gateway node bypassing attacks. In this paper, we give detailed cryptanalysis of Kim Jiye et al's two-factor mutual authentication with key agreement in WSNs.

The remainder of the paper is organized as follows. Section 2 presents review of Kim Jiye et al.'s scheme. Section 3 gives detailed cryptanalysis of Kim Jiye et al.'s scheme. Section 4 finally concludes this paper.

Manuscript received July 17, 2015; revised January 6, 2016.
This work was funded by Natural Science Foundation of Hubei Province of China under Grant No.2014CFB577, and partly supported both by the National Natural Science Foundation of China under Grant No.61370223 and partly supported by Hubei Provincial Department of Education Outstanding Youth Scientific Innovation Team Support Foundation under Grant No.T201410.
Corresponding author email: xgdym2015@aliyun.com.
doi:10.12720/jcm.11.1.58-63

II. Review of Kim Jiye et. al.'s Scheme

Three communication parties are involved in Kim Jiye et al.'s scheme [13]: a user, a gateway node, and a sensor node. The scheme is composed of four phases: registration phase, login phase, authentication-key agreement phase, and password change phase. We describe each phase in detail from section A to section D. The notations used in the remainder of this paper are shown in Table I.

TABLE I: NOTATIONS USED IN THIS PAPER

Symbol	Description
U_i	*i*-th user
S_j	*j*-th sensor node
GW	Gateway node
ID_i	Identity of U_i
pw_i	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	Random nonce of s_j
RN_i	Random nonce of U_i
$\oplus$	XOR operation
$\|\|$	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

A. Registration Phase

In the registration phase, U_i selects ID_i and pw_i, generates a random nonce RN_r and computes $H\_PW_i = h(pw_i \| RN_r)$, then sends the registration request $\{ID_i, h(pw_i)\}$ to GW. Then, GW personalizes a smart card for U_i .The detailed registration phases are shown as follows.

R-1: U_i selects ID_i and pw_i.

R-2: U_i generates random nonce RN_r and computes $H\_PW_i = h(pw_i \| RN_r)$. Then U_i sends the registration request $\{ID_i, H\_PW_i\}$ to GW in secure channels.

R-3: GW computes the following when it receives the registration request from U_i. $H\_ID_i = h(ID_i \| K)$, $Xs_i = h(H\_ID_i \| x_s)$, $A_i = h(H\_PW_i \| Xs_i) \oplus h(H\_ID_i \| K)$, $B_i = h(H\_PW_i \oplus Xs_i)$, $C_i = Xs_i \oplus h(ID_s \| H\_PW_i)$, GW personalizes the smart card with ID_s, H_ID_i, $h(\cdot)$, A_i, B_i and C_i, then GW sends the smart card to U_i in secure channels.

R-4: U_i computes $X\_PW_i = h(pw_i) \oplus RN_r$ and adds X_PW_i to the smart card.

B. Login Phase

The login phase begins when U_i inserts his/her smart card into a terminal and inputs ID_i^* and pw_i^*. In this phase, U_i sends the authentication request to GW. The detailed login phase is shown as follows.

L-1: U_i inserts its smart card into a terminal and inputs ID_i^* and pw_i^*.

L-2: The smart card computes $RN_r^* = h(pw_i^*) \oplus X\_PW_i$, $H\_PW_i^* = h(pw_i^* \| RN_r^*)$, $Xs_i^* = C_i \oplus h(ID_s \| H\_PW_i^*)$, $B_i^* = h(H\_PW_i^* \oplus Xs_i^*)$. Then the smart card compares B_i^* with B_i. If $B_i^* = B_i$ holds, the next step proceeds, otherwise, this phase is aborted.

L-3: The smart card generates a random nonce RN_i and computes $DID_i = h(H\_PW_i^* \| Xs_i^*) \oplus h(Xs_i^* \| RN_i \| T_i)$, $M_{U_i-G} = h(A_i \| Xs_i^* \| RN_i \| T_i)$, $v_i = RN_i \oplus Xs_i^*$, T_i is the current timestamp of U_i system. The smart card sends the authentication request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ to GW.

C. Authentication-Key Agreement Phase

The authentication-key agreement phase begins when GW receives an authentication request from U_i. In this phase, U_i, the GW and S_j send and receive authentication request from one another. The following describes the process in detail.

A-1: GW checks if $(T_G - T_i) \le \Delta T$, where T_G the current time-stamp of GW system. If $(T_G - T_i) \le \Delta T$ holds, the next step proceeds; otherwise, this phase is aborted.

A-2: GW computes $Xs_i = h(H\_ID_i \| Xs_i)$, $RN_i = v_i \oplus Xs_i$, $X^* = DID_i \oplus h(Xs_i \| RN_i \| T_i)$, $M_{U_i-G}^* = h((X^* \oplus h(H\_ID_i \| K)) \| Xs_i^* \| RN_i \| T_i)$ GW compares $M_{U_i-G}^*$ with M_{U_i-G} .If $M_{U_i-G}^* = M_{U_i-G}$ holds true, the next step proceeds; otherwise, this phase is aborted.

A-3: GW computes $Xs_j = h(SID_j \| x_s)$, $M_{G-S_j} = h(DID_i \| SID_j \| Xs_j \| T_G)$, where T_G is the current timestamp of GW system. S_j is the nearest sensor node that can respond to $U_i^{'}s$ request. GW sends the authentication request $\{DID_i, M_{G-S_j}, T_G\}$ to S_j.

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

A-5: S_j computes $M^*_{G-S_j} = h(DID_i \| SID_j \| Xs^*_j \| T_G)$. S_j compares $M^*_{G-S_j}$ with M_{G-S_j}. If $M^*_{G-S_j} = M_{G-S_j}$ holds true, then the next step proceeds; otherwise, this phase is aborted.

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

A-7: GW checks if $(T'_G - T_j) \le \Delta T$, where T'_G is the current timestamp of GW. If $(T'_G - T_j) \le \Delta T$ holds true, then the next step proceeds; otherwise, this phase is aborted.

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

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

A-10: U_i checks if $(T'_i - T'_G) \le \Delta T$, where T'_i is the current timestamp of U_i. If $(T'_i - T'_G) \le \Delta T$ holds true, then the next step proceeds; otherwise, this phase is aborted.

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

A-12: The smart card computes the following to get a session key for communication 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 $Xs_j = q_j \oplus RN_j$.

D. Password Change Phase

The password change phase proceeds when U_i changes his/her existing password to a new one. In the password change phase, U_i does not have to commu-nicate with GW. The password change phase is shown as follows in detail.

P-1: U_i inserts its smart card into a terminal and inputs ID^*_i, pw^*_i and pw_{ni}, where pw_{ni} is $U_i's$ new password.

P-2: The smart card computes $RN^*_r = h(pw^*_i) \oplus X\_PW_i$, $H\_PW^*_i = h(pw^*_i \| RN^*_r)$, $Xs^*_i = C_i \oplus h(ID_s \| H\_PW^*_i)$, $B^*_i = h(H\_PW^*_i \oplus Xs^*_i)$. The smart card compares B^*_i with B_i. If $B^*_i = B_i$ holds true, then the next step proceeds, otherwise, this phase is aborted.

P-3: The smart card computes $H\_PW_{ni} = h(pw_{ni} \| RN^*_r)$, $A_{ni} = A_i \oplus h(H\_PW^*_i \| Xs^*_i) \oplus h(H\_PW_{ni} \| Xs^*_i)$, $B_{ni} = h(H\_PW_{ni} \oplus Xs^*_i)$ $h(H\_PW_{ni} \oplus Xs^*_i)$, $C_{ni} = Xs^*_i \oplus h(ID_s \| H\_PW_{ni})$. The smart card replaces the existing values A_i, B_i and C_i with the new values A_{ni}, B_{ni} and C_{ni}.

III. Security Analysis of Kim Jiye et al.'s Scheme

In this section, we analyze the security of Kim Jiye et al.'s scheme. In the following sections, we describe possible attacks in detail. We assume that an attacker can eavesdrop on or intercept all message sent or received between communication parties. We also assume that an attack can read data stored in a smart card in any manner such as found in the related works [2], [3], [14]-[17]. In addition, we have to note that data stored in sensor nodes are not secure since attackers can capture sensor nodes that are deployed in unattended environments and then can extract data from them.

A. Offline Password Guessing Attack

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

Step 1: The attacker U_a read ID_s, $h(\bullet)$, H_ID_i, X_PW_i, A_i, B_i and C_i in $U_i's$ smart card in any manner which is used in the related works[2], [3], [14]-[17].

Step 2: U_a chooses a random nonce H_PW_i, and verifies if $B_i = h(H\_PW_i \oplus C_i \oplus h(ID_s \| H\_PW_i))$ holds true. The operation repeats until $B_i = h(H\_PW_i \oplus C_i \oplus h(ID_s \| H\_PW_i))$ holds.

Step 3: U_a chooses a random nonce PW_i, and verifies if $H\_PW_i = h(pw_i \| (X\_PW_i \oplus h(pw_i)))$ holds true. The operation repeats until $H\_PW_i = h(pw_i \| (X\_PW_i \oplus h(pw_i)))$ holds true.

Step 4: The Xs_i can be computed as $Xs_i = C_i \oplus h(ID_s \| H\_PW_i)$.

Step 5: The x_s can be guessed as follows. U_a chooses a random nonce x_s and verifies if $Xs_i = h(H\_ID_i \| x_s)$ holds . The operation repeats until $Xs_i = h(H\_ID_i \| x_s)$ holds true.

Step 6: The secret K can be guessed as follows. U_a chooses a random nonce K, and verifies if $A_i = h(H\_PW_i \| Xs_i) \oplus h(H\_ID_i \| K)$ holds true. The operation repeats until the equation holds true.

Step 7: U_i identity can be guessed as follows. U_a chooses a random nonce ID_i, and verifies if $H\_ID_i = h(ID \| K)$ holds. The operation repeats until the equation holds true.

B. User Impersonation Attacks Using an Attacker's Own Smart Card

If attacker U_a has registered with GW, he/she can receive the smart card personalized with his/her own identity ID_a and password pw_a. The detailed registration and login processes can be shown as follows.

Step 1: U_a selects ID_a and pw_a.

Step 2: U_a generates a random nonce RN_a and computes $H\_PW_a = h(pw_a \| RN_a)$, then sends the registration request $\{ID_a, H\_PW_a\}$ to GW in a secure channel.

Step 3: When GW receives a registration request from U_a, it computes $H\_ID_a = h(ID_a \| K)$, $Xs_a = h(ID_a \| x_s)$, $A_a = h(H\_PW_a \| Xs_a) \oplus h(H\_ID_a \| K)$, $B_a = h(H\_PW_a \oplus Xs_a)$, $C_a = Xs_a \oplus h(ID_s \| H\_PW_a)$, GW personalizes the smart card with ID_s, H_ID_a, $h(\bullet)$, A_a, B_a and C_a, and 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 sends the authentication request to GW and inputs ID_a^* and pw_a^*.

Step 6: The smart card computes $RN_a^* = h(pw_a^*) \oplus X\_PW_a$, $H\_PW_a^* = h(pw_a^* \| RN_a^*)$, $Xs_a^* = C_a \oplus h(ID_s \| H\_PW_a^*)$, $B_a^* = h(H\_PW_a^* \oplus Xs_a^*)$. The smart card compares B_a^* with B_a. Obviously $B_a^* = B_a$ holds true, then next step proceeds.

Step 7: The smart card generates random nonce RN_a and computes the following. $DID_a = h(H\_PW_a^* \| Xs_a^*) \oplus h(Xs_a^* \| RN_a \| T_a)$, where T_a is the current timestamp of U_a system. $M_{U_a-G} = h(A_a \| Xs_a^* \| RN_a \| T_a)$, $v_a = RN_a \oplus Xs_a^*$. The smart card sends the authentication request $\{DID_a, M_{U_a-G}, v_a, T_a, H\_ID_a\}$ to GW.

Step 8: When GW receives the authentication request $\{DID_a, M_{U_a-G}, v_a, T_a, H\_ID_a\}$ from U_a, it checks if $(T_G - T_a) \le \Delta T$, where T_G is the current timestamp of GW system. If it holds true, the next step proceeds; otherwise, this phase is aborted.

Step 9: GW computes $Xs_a = h(H\_ID_a \| x_s)$, $RN_a = v_a \oplus Xs_a$, $X^* = DID_a \oplus h(Xs_a \| RN_a \| T_a)$, $M_{U_a-G}^* = H((X^* \oplus h(H\_ID_a \| K)) \| Xs_a \| RN_a \| T_a)$, and then compares $M_{U_a-G}^*$ with M_{U_a-G}. Obviously, if $M_{U_a-G}^* = M_{U_a-G}$ holds true, the attacker U_a is authenticated by the GW. Once U_a is authenticated by GW, with the help of GW, a mutual authentication between U_a and S_j is completed successfully. 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 communication.

C. Sensor Node Impersonation Attacks

In Kim Jiye et al.'s scheme, if an attacker U_a captures S_j deployed in unattended environments, he/she can extract $Xs_j = h(SID_j \| x_s)$ from it. Once U_a eavesdrops on or intercepts $U_i^{'}s$ login request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$, he/she can forge a valid sensor node S_j and complete 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 process can be shown as follows.

Step 1: U_a strives to capture S_j, and then extracts SID_j and $Xs_j = h(SID_j \| x_s)$ stored in S_j.

Step 2: 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 GW, and then gets $U_i^{'}s$ dynamic identity DID_i.

Step 3: When intercepting the authentication request $\{DID_i, M_{G-S_j}, T_G\}$ from GW to S_j, U_a checks if $(T_a - T_G) \le \Delta T$, where T_a is the current timestamp of U_a system. If $(T_a - T_G) \le \Delta T$ holds true, the next step proceeds; otherwise, this phase is aborted.

Step 4: U_a computes $M_{G-U_a}^* = h(DID_i \| SID_j \| Xs_j \| T_G)$, U_a compares $M_{G-U_a}^*$ with M_{G-S_j}, since it holds, the next step proceeds.

Step 5: U_a generates a random nonce RN_a and uses the extracted Xs_j stored in S_j to compute $y_a = RN_a \oplus Xs_j$, $z_i = M_{G-U_a} \oplus RN_a$, $M_{U_a-G} = h(z_i \| Xs_j \| T_a)$. U_a sends the authentication request $\{y_a, M_{U_a-G}, T_a\}$ to GW.

Step 6: GW checks if $(T_G^{'} - T_a) \le \Delta T$, where $T_G^{'}$ is the current timestamp of GW. If $(T_G^{'} - T_a) \le \Delta T$ holds true, the next step proceeds; otherwise, this phase is aborted.

Step 7: GW computes $RN_a = y_a \oplus Xs_j$, $z_i^* = M_{G-S_j} \oplus RN_a$, $M_{U_a-G}^* = h(z_i^* \| Xs_j \| T_a)$. GW compares $M_{U_a-G}^*$ with M_{U_a-G}. Since $M_{U_a-G}^* = M_{U_a-G}$ holds true, the next step proceeds.

Step 8: GW computes $M_{G-U_i} = h(DID_i \| M_{G-U_a} \| M_{U_a-G} \| Xs_i \| T_G^{'})$, $w_i = z_i^* \oplus Xs_i$, $y_i = RN_a \oplus Xs_i$, $q_a = Xs_a \oplus RN_a$. GW sends the authentication request $\{y_i, w_i, M_{G-U_i}, q_a, T_G^{'}\}$ to U_i.

Step 9: U_i checks if $(T_i^{'} - T_G^{'}) \le \Delta T$, where $T_i^{'}$ is the current timestamp of U_i system. If $(T_i^{'} - T_G^{'}) \le \Delta T$ holds, then the next step proceeds; otherwise, this phase is aborted.

Step 10: The smart card computes $RN_a = y_i \oplus Xs_i$, $z_i^* = w_i \oplus Xs_i$, $M_{G-S_j} = z_i^* \oplus RN_a$, $M_{G-U_i}^* = h(DID_i \| M_{G-S_j}^* \| M_{U_i-G} \| Xs_i \| T_G^{'})$. The smart card compares $M_{G-U_i}^*$ with M_{G-U_i}. Since

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

D. Gateway Node Bypassing Attacks

In Kim Jiye et al.'s scheme, if an attacker U_a derives Xs_i from smart card and extracts SID_j from a captured sensor node S_j, and then eavesdrops on the authentication request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ from U_i to GW, he/she can mount gateway node bypassing attacks. The detailed process is as follows.

Step 1: U_a gets Xs_i from U_i's smart card and extracts SID_j from a captured sensor node S_j.

Step 2: When U_i sends the authentication request $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$ to GW, U_a eavesdrops on it.

Step 3: U_a computes the following using Xs_i, SID_j and $\{DID_i, M_{U_i-G}, v_i, T_i, H\_ID_i\}$, T_a and $T_a^{'}$ are the current time-stamp of U_a system, and $T_a \le T_a^{'}$, RN_a is a random nonce generated by U_a. $y_i = RN_a \oplus Xs_i$, $M_{G-S_j} = h(DID_i \| SID_j \| Xs_i \| T_a)$, $z_i^* = M_{G-S_j} \oplus RN_a$, $w_i = z_i^* \oplus Xs_i$, $M_{G-U_i} = h(DID_i \| M_{G-S_j} \| M_{U_i-G} \| Xs_i \| T_a^{'})$. U_a forges the authentication request sent from GW to U_i in the authentication-key agreement phase using $\{y_i, w_i, M_{G-U_i}, T_a^{'}\}$.

Step 4: 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. If $(T_U - T_a^{'}) \le \Delta T$ holds true, the next step proceeds; otherwise, this phase is aborted.

Step 5: The smart card computes $RN_a = y_i \oplus Xs_i$, $z_i^* = w_i \oplus Xs_i$, $M_{G-S_j} = z_i^* \oplus RN_a$, $M^*_{G-U_i} = h(DID_i \| M_{G-S_j} \| M_{U_i-G} \| Xs_i \| T_a^{'})$. The smart card compares M_{G-U_i} with $M^*_{G-U_i}$. 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 GW. Therefore, U_a can communicate with U_i using session key $K_s = f((DID_i \| RN_a), Xs_i)$

IV. Conclusions

In this study, we have cryptanalyzed a two-factor mutual authentication with key agreement in wireless sensor networks proposed by Kim Jiye *et al.*, and point out the scheme's vulnerability to offline password guessing attack, user impersonation attacks using an attacker's own smart card, sensor node impersonation attacks and gateway node bypassing attacks. In the future work, we will propose an improved authentication scheme to remedy the security weakness of Kim Jiye et al.'s scheme.

Acknowledgment

The authors gratefully thanks for the helpful and suggestions of reviewers. This work is funded by Natural Science Foundation of Hubei Province of China under Grant No.2014CFB577, and partly supported both by the National Natural Science Foundation of China under Grant No.61370223 and by Hubei Provincial Department of Education Outstanding Youth Scientific Innovation Team Support Foundation under Grant No.T201410.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, pp. 2292-2330, August 2008.

[2] E. J. Yoon and K. Y. Yoo, "Cryptanalysis of robust mutual authentication protocol for wireless sensor networks," in *Proc. 10th IEEE International Conference on Cognitive Informatics & Cognitive Computing*, Banff, Canada, 2011, pp. 392–396.

[3] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. on Wireless Communication*, vol. 8, pp. 1086-1090, March 2009.

[4] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," *Sensors*, vol. 10, pp. 2450-2459, March 2010.

[5] D. H. Nyang and M. K. Lee. Improvement of Das's two-factor authentication protocol in wireless sensor networks. [Online]. Available: http://eprint.iacr.org/2009/631.pdf

[6] C. T. Li, C. Y. Weng, and C. C. Lee, "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks," *Sensors*, vol. 13, pp. 9589-9603, November 2013.

[7] S. G. Yoo, H. Lee, and J. Kim, "A performance and usability aware secure two-factor user authentication schemes for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, March 2013.

[8] H. R. Tseng, R. H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proc. Global Telecommunications Conference*, Washington, DC, USA, 2007, pp. 986–990.

[9] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc Sensor Wireless Networks*, vol. 10, pp. 361-371, February 2010.

[10] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, Taiwan, 2006, pp. 244–251.

[11] T. H. Chen and W. K. Shih, "A robust mutual authentication protocol for wireless sensor networks," *Electronic Telecommunication Res. Inst*, vol. 32, pp. 704-712, October 2010.

[12] B. Vaidya, D. Makrakis, and H. Mouftah. (April 2012). Two-factor mutual authentication with key agreement in wireless sensor networks, Security and Communication Networks. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/sec.517/full.

[13] J. Kim, D. Lee, W. Jeon, Y. Lee, and D. Won, "Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks," *Sensors*, vol. 14, pp. 6443-6462, April 2014.

[14] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless networks," *Journal of Network and Computer Applications*, vol. 35, pp. 1646-1656, September 2012.

[15] J. Xu, W. T. Zhu, and D. G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, pp. 723-728, June 2009.

[16] M. Turkanovic and M. Holbl, "An improved dynamic password-based user-authentication scheme for hierarchical wireless sensor networks," *Elektronika Ir Elektrotechnika*, vol. 19, pp. 109-116, June 2013.

[17] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, pp. 316-323, January 2013.

[18] M. Dheerendra, "Understanding security failures of two authentication and key agreement schemes for telecare medicine information systems," *Journal of medical systems*, vol. 39, no. 3, pp. 1-8, March 2015.

[19] M. Dheerendra, "On the security flaws in id-based password authentication schemes for telecare medical information systems," *Journal of Medical Systems*, vol. 39, no. 1, pp. 1-16, January 2015.

[20] M. Dheerendra, A. K. Das, A. Chaturvedi, and S. Mukhopadhyay, "A secure password-based authentication and key agreement scheme using smart cards," *Journal of Information Security and Applications*, vol. 23, pp. 28-43, August 2015.

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. 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 the BS degree in physics and the MS degree in radio electronics from Central China Normal University, Wuhan, China, in 1985 and in 1988, respectively. He received the 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.

Honglai Li was born in Hubei Province, China, in 1964. He received B.S. degree in information manage-ment from Zhongnan University of Economics and Law. He is presently a senior Experimentalist at Hubei Engineering University. His research interest includes zigbee network.