ATLANTIS PRESS
Advances in Computer Science Research, volume 44
3rd International Conference on Wireless Communication and Sensor Network (WCSN 2016)

Cryptanalysis of an Untraceable Temporal-Credential-Based Two-Factor Authentication Scheme Using ECC for Wireless Sensor Networks

Shu-Ying Yang
Department of basic, Shandong Women's University, Jinan, China
E-mail: ysystudy2005@163.com

Cheng-Bo Xu
School of Mathematical Sciences, University of Jinan, Jinan, China
E-mail: cbqysy@163.com

***Abstract*-Authentication and key agreement scheme is an important mechanism for legal users to access the services of wireless sensor network. However, the design of authentication and key agreement schemes in WSNs is still quite a challenging problem. In this paper, we analyze an untraceable temporal-credential-based two-factor authentication scheme using ECC for WSNs proposed by Jiang et al. in 2016, and point out the scheme can not resist malicious user impersonation attack, sensor node capture attack and suffer from forward security problem, low efficiency problem, no password change phase problem and time synchronization problem.**

Keywords-authentication; password; smart card; session key agreement; wireless sensor netwoks

I. INTRODUCTION

Nowadays, wireless sensor networks (WSNs) are the first choices for a wide range of real-time monitoring applications, such as health care, environmental monitoring, traffic monitoring, etc. In WSNs, data collected by sensor nodes sometimes contain valuable and confidential information that only authorized users are allowed to access. As yet, the design of user authentication and key agreement scheme for resource deficient wirless sensor networks has been substantially addressed by various researchers.

In 2009, Das [1] first proposed a two-factor authentication scheme for wieless sensor networks using smart card, which leads user authentication for WSNs to a new direction. In this direction, a dozen of authentication schemes have been presented to eliminate the security weaknesses of the earlier ones [2-7]. Das claimed his scheme to be free from the security problems such as stolen-verifier, many logged-in-users with the same identity, guessing, impersonation and replay attacks. In 2010, He et al. [2] pointed out that Das's scheme does not resist impersonation attack, privileged insider attack and lack of password update mechanism. During the same time, Khan and Alghathbar [3] showed that Das's scheme susceptible to gateway node bypassing attack and privileged insider attack and proposed an improved scheme. In 2013, Xue et al. [8] proposed an authentication scheme based on the concept of temporal credential for wireless sensor networks. They claimed that their scheme provides identity and password protection, and is immune to stolen smart card attack. Unfortunately, this scheme was pointed out that it is susceptible to many kinds of attacks such as offline password guessing attack, sensor node impersonation attack et al. by He et al. [9]. Based on these, He et al. improved Xue et al.'s scheme. However, Jiang et al. [10] revealed that He et al.'s scheme is susceptible to stolen smart card attack and prone to tracking attack, and proposed an improved scheme in 2016.

In this paper, we will show that Jiang et al.'s scheme [10] is also not secure and vulnerable to malicious user impersonation attack and node capture attack and suffer from forward security problem, low efficiency problem, no password change phase problem and time synchronization problem.

The rest of this paper is organized as follows: in section 2, we briefly review Jiang et al.'s scheme. Section 3 points out the weaknesses of Jiang et al.'s scheme. Finally, we draw our conclusion in section 4.

The notations used throughout this paper are summarized in Table 1.

TABLE I. NOTATIONS

ID_i, PW_i	The identity and password of user U_i
SID_j	Sensor node identity
DID_i, DID_{GWN}	A dynamic identity of U_i and GWN
K_{GWN-U}, K_{GWN-S}	Master keys only known to GWN
SK_{ij}	The session key agreed between U_i and S_j
PTC_i	The protected temporal credential of U_i
TC_i, TC_j	The temporal credential of U_i and S_j
TE_i	The expiration time of a user's temporal credential
TS	The current timestamp
K_i, K_j	Keys generated by U_i and S_j
$h(\cdot)$	A secure one-way hash function
$\oplus$	The bitwise exclusive-or operation
$\|\|$	Message concatenation operation

II. REVIEW OF JIANG ET AL.'S SCHEME

In this section, we briefly review the Jiang et al.'s scheme [10]. Their scheme includes three phases: registration phase, login phase and authentication phase; and involves three entities: users, gate-way node (GW) and sensor nodes.

A. Registration Phase

In this phase, GWN selects the additive group G generated by a point P with a large prime order n on an ellipic curve E. Then GWN randomly generates a number x as its private key and compoutes $y = xP$ as the public key. Finally, GWN stores x and publishes the system parameters $\{E, G, P, y\}$.

1) Registration phase for users

Assumpting that user U_i shares a password PW_i with GWN, which maintains the values $\{ID_i, H(PW_i)\}$. The details of this phase are reviewed as follows.

- Step 1: U_i inputs the old password PW_i, and chooses a new one PW_i^{new}. Then he generates two random numbers $a, r_i \in Z_{p-1}^*$, and computes $IV_i = H(TS_1 \| H(PW_i) \| A \| A' \| H(PW_i^{new} \| ID_i \| r_i))$ an $TPW_i = H(PW_i^{new} \| ID_i \| r_i) \oplus H(TS_1 \| H(PW_i) \| A \| A')$, where $A = aP$, $A' = ay = axP$. U_i submits $\{ID_i, TS_1, VI_i, TPW_i, A\}$ to GWN.
- Step 2: Upon receiving the message, GWN verifies the validity of TS_1. Then, GWN retrieves $H(PW_i)$ according to ID_i, computes $H(PW_i^{new} \| ID_i \| r_i) = TPW_i \oplus H(TS_1 \| H(PW_i) \| A \| A'')$, and checks whether VI_i and $H(TS_1 \| H(PW_i) \| A \| A' \| H(PW_i^{new} \| ID_i \| r_i))$ are equal, where $A'' = xA = xaP$. If these two values are equal, GWN computes $TC_i = H(K_{GWN-U} \| ID_i \| TE_i)$, $PTC_i = TC_i \oplus H(PW_i^{new} \| ID_i \| r_i)$, and updates its identity information table with the new entry $\{ID_i, TE_i\}$; otherwise, GWN rejects the request. Finally, GWN stores $\{H(\cdot), TE_i, PTC_i\}$ into a smart card and issues it to U_i.
- Step 3: After receiving the smart card, U_i stores r_i into it. Eventually, smart card has the following: $H(\cdot), TE_i, PTC_i$ and r_i.

2) Registration phase for sensor nodes

Assumpting that each node is preconfigured a password, and GWN maintains the values $\{SID_j, H(PW_j)\}$. The details of this phase are reviewed as follows.

- Step 1: S_j randomly chooses a number $b \in Z_{p-1}^*$, computes $VI_i = H(TS_2 \| H(PW_i) \| B \| B')$, where $B = bP$, $B' = by = bxP$. Then S_j responds $\{SID_j, TS_2, VI_j, B\}$ through a public channel.
- Step 2: When receiving the request message, GWN firstly verifies the validity of TS_2. Then, GWN retrieves $H(PW_j)$ according to SID_j, computes $B'' = xB = xbP$ and verifies whether VI_j and $H(TS_2 \| H(PW_i) \| B \| B'')$ are equal. If these two values are equal, GWN further computes $TC_j = H(K_{GWN-S} \| SID_j)$, $REG_j = TC_j \oplus H(TS_3 \| H(PW_j) \| B \| B'')$ and $VI_{GWN} = H(TC_j \| H(TS_3 \| H(PW_j) \| B \| B''))$. GWN transimits $\{TS_3, REG_j, VI_{GWN}\}$ to S_j.
- Step 3: Upon receiving the message, S_j firstly verifies the validity of TS_3. Then, S_j computes $TC_j = REG_j \oplus H(TS_3 \| H(PW_j) \| B \| B')$ and checks whether VI_{GWN} and $H(TC_j \| H(TS_3 \| H(PW_j) \| B \| B'))$ are equal. If they are unequal, S_j terminates the session; otherwise, it stores TC_j.

B. Login and Authentication Phase

- Step 1: U_i inserts his smart card to a card reader, and inputs ID_i and PW_i. The smart card calculates $TC_i = PTC_i \oplus H(PW_i \| ID_i \| r_i)$. U_i randomly chooses $c \in Z_{p-1}^*$ and a key K_i. Then U_i calculates $C_i = cP$, $D_i = cy = cxP$, $DID_i = ID_i \oplus H(C_i \| D_i)$, $PKS_i = K_i \oplus H(TC_i \| TS_4 \| D_i)$, $E_i = H(H(ID_i \| TS_4) \oplus D_i \oplus PKS_i \oplus TC_i)$, where TS_4 is the current timestamp. U_i sends $\{DID_i, C_i, PKS_i, TS_4, E_i\}$ to GWN.
- Step 2: When receiving this message, GWN firstly verifies the validity of TS_4. Then, GWN computes $D_i = xC = xcP$, $ID_i = DID_i \oplus H(C_i \| D_i)$, $TC_i = H(K_{GWN-U} \| ID_i \| TE_i)$ and checks whether E_i and $H(H(ID_i \| TS_4) \oplus D_i \oplus PKS_i \oplus TC_i)$ are equal. If they are unequal, GWN rejects the request; otherwise, GWN computes $K_i = PKS_i \oplus H(TC_i \| TS_4 \| D_i)$. Then GWN selects

a sensor node S_j, and computes $TC_j = H(K_{GWN-s} \| SID_j)$, $DID_{GWN} = ID_i \oplus H(DID_i \| TC_j \| TS_5)$, $C_{GWN} = H(ID_i \| TC_j \| TS_5)$, $PKS_{GWM} = K_i \oplus H(TC_j \| TS_5)$. Then, GWN sends $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ to S_j.

- Step 3: Upon receiving the message, S_j firstly verifies the validity of TS_5. Then, S_j computes $ID_i = DID_{GWN} \oplus H(DID_i \| TC_j \| TS_5)$, and checks whether $H(ID_i \| TC_j \| TS_5)$ and C_{GWN} are equal. If they are equal, S_j generates a random key K_j, computes $K_i = PKS_{GWN} \oplus H(TC_j \| TS_5)$, $SK_{ij} = H(K_i \oplus K_j)$, $C_j = H(K_j \| ID_i \| SID_j \| TS_6)$, $PKS_j = K_j \oplus H(K_i \| TS_6)$, and responds $\{SID_j, TS_6, C_j, PKS_j\}$ to U_i; otherwise, S_j rejects the request.
- Step 4: When receiving the validity of TS_6, U_i computes $K_j = PKS_j \oplus H(K_i \| TS_6)$, and checks whether C_j and $H(K_j \| ID_i \| SID_j \| TS_6)$ are equal. If they are equal, U_i confirms that S_j and GWN are authenticated, and further computes the shared session key $SK_{ij} = h(K_i \oplus K_j)$; otherwise, U_i aborts this session.

III. WEAKNESSES OF JIANG ET AL.'S SCHEME

In this section, we will show that Jiang et al.'s scheme [10] is vulnerable to malicious user impersonation attack and node capture attack and suffer from forward security problem, low efficiency problem, no password change phase problem and time synchronization problem.

A. Forward security problem

Forward security problem means that once attacker obtains the master key stored by GWN in some way, he/she will restore some previous session keys using the known master key and the information intercepted or eavesdropped from the public communicational channel. In this way, the attacker can easily decrypt the data transmitted in previous sessions.

In Jiang et al.'s scheme, suppose attacker obtains the master key K_{GWN-S} and eavesdrops the mutual information $\{DID_i, C_i, PKS_i, TS_4, E_i\}$, $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ and $\{SID_j, TS_6, C_j, PKS_j\}$ in the authentication phase of some previous session, the attacker can restore the session key as follows:

- Computes $TC_j = H(K_{GWN-S} \| SID_j)$, where SID_j have been obtained from $\{SID_j, TS_6, C_j, PKS_j\}$.
- Computes $K_i = PKS_{GWN} \oplus H(TC_j \| TS_5)$, where PKS_{GWN} and TS_5 are from $\{DID_i, C_i, PKS_i, TS_4, E_i\}$ and $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ separately.
- Computes $K_j = PKS_j \oplus H(K_i \| TS_6)$, where PKS_j and TS_6 are from $\{SID_j, TS_6, C_j, PKS_j\}$.
- Restore the session key $SK_{ij} = H(K_i \oplus K_j)$.

B. Malicious user impersonation attack

Malicious user impersonation attack means that a malicious registered user can impersonate as other registered users to login the system, and access the sensed data under the name of other legitimate users. Suppose that a malicious user A has captured the message $\{DID_i, C_i, PKS_i, TS_4, E_i\}$ and collected ID_i and TE_i of a registered user U_i. Then A can manipulate his smart card to launch the attack as follows.

- A inserts his card and inputs ID_A and PW_A. Then the card computes $TC_A = PTC_A \oplus H(PW_A \| ID_A \| r_A)$, and randomly chooses $c \in Z_{p-1}^*$ and a key K_A. Then A calculates $C_A = cP$, $D_A = cy = cxP$, $DID_i' = ID_i \oplus H(C_A \| D_A)$, $PKS_i' = K_A \oplus H(TC_A \| TS_4 \| D_A)$, $E_i' = H(H(ID_i \| TS_4) \oplus D_A \oplus PKS_A \oplus TC_A$. U_i sends $\{DID_i', C_A, PKS_i', TS_4, E_i'\}$ to GWN.
- When receiving the message, GWN computes $D_i' = xC_A = xcP$, $ID_i = DID_i' \oplus H(C_A \| D_i')$, $TC_i' = H(K_{GWN-U} \| ID_i \| TE_i)$. It is easy to see that the value $H(H(ID_i \| TS_4) \oplus D_i' \oplus PKS_i' \oplus TC_i')$ and E_i' are equal. GWN accepts A as the legal user to access the data.Then, GWN conducts the rest of operations in Step (2) of authentication and key agreement phase of Jiang et al.'s scheme and sends $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ to S_j.
- Upon receiving the message, S_j follows the operations in Step (3) of authentication and key agreement phase of Jiang et al.'s scheme, and reponds $\{SID_j, TS_6, C_j, PKS_j\}$ to U_i.
- A intercepts the message, and computes $K_j = PKS_j \oplus H(K_i \| TS_6)$ and the shared session

key $SK_{ij} = h(K_i \oplus K_j)$. Then A can access the data of S_j.

C. Sensor node capture attack

Suppose a sensor node S_j was captured by an attacker A. Since the capabilities of computation and storage of the sensor node S_j are both limited, A can easily extract the data stored in the sensor node S_j, especially the value TC_j. Once the attacker A obtained TC_j and eavesdrops the mutual information $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ and $\{SID_j, TS_6, C_j, PKS_j\}$ in the authentication phase of some previous session, the attacker A can restore the session key as follows:

- A computes $ID_i = DID_{GWN} \oplus H(DID_i \| TC_j \| TS_5)$, where DID_{GWN}, DID_i and TS_5 have been obtained from the message $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$.
- A computes $K_i = PKS_{GWN} \oplus H(TC_j \| TS_5)$, where PKS_{GWN} and TS_5 are from $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$.
- A computes $K_j = PKS_j \oplus H(K_i \| TS_6)$, where PKS_j and TS_6 are from $\{SID_j, TS_6, C_j, PKS_j\}$.
- A computes the session key $SK_{ij} = H(K_i \oplus K_j)$.

D. Low efficiency in wrong password detection

If the legal user U_i inputs a wrong password by mistake, this wrong password will not be detected until the remote gateway node GWN verifies whether E_i and $H(H(ID_i \| TS_4) \oplus D_i \oplus PKS_i \oplus TC_i)$ are equal in step 2 of the login and authentication phase. Therefore, Jiang et al.'s scheme is low efficient to detect the user's wrong password.

E. No password change phase

In Jiang et al.'s scheme, there is no password change phase. Actually, it is not difficult to add this phase. When the user U_i wants to change his/her password, he/she inserts the smart card into a card reader, inputs the identity ID_i and password PW_i, then calls for changing password. U_i will select and input a new password PW_{new}. And then the smart card computes $PTC_{new} = PTC_i \oplus H(PW_i \| ID_i \| r_i) \oplus H(PW_{new} \| ID_i \| r_i)$, and replaces PTC_i with PTC_{new}. As such, the password is changed.

However, since no wrong password detection mechanism is designed in the smart card, the password change phase would suffer from the following weakness. If an attacker A stole user U_i's smart card for a short time, he/she inserts U_i's smart card into a card reader, enters the ID_i and an arbitrary password PW_a, and calls for changing password. Then A enters an arbitrary new password PW_a^*. The smart card will compute $PTC_a^* = PTC_i \oplus H(PW_a \| ID_i \| r_i) \oplus H(PW_a^* \| ID_i \| r_i)$, which yields $PTC_a^* = PTC_i \oplus H(PW_a \| ID_i \| r_i) \oplus H(PW_a^* \| ID_i \| r_i) = TC_i \oplus H(PW_i \| ID_i \| r_i) \oplus H(PW_a \| ID_i \| r_i) \oplus H(PW_a^* \| ID_i \| r_i)$, and then replaces PTC_i with PTC_a^* without any checking. Later, the legal user U_i's succeeding login requests will be denied.

F. Time synchronization problem

Since time stamp was adopted in the login and authentication phase of Jiang et al.'s scheme, it is inevitable that there is a probability of time synchronization problem between user and gateway node. Also same problem can be occurred between gateway node and sensor nodes during communication.

IV. CONCLUSIONS

In this paper, we analyze an untraceable temporal-credential-based two-factor authentication scheme using ECC for WSNs proposed by Jiang et al. in 2016, and point out the scheme can not resist malicious user impersonation attack, sensor node capture attack and suffer from forward security problem, low efficiency problem, no password change phase problem and time synchronization problem.

ACKNOWLEDGMENT

This work was partially supported by the Doctoral Fund of University of Jinan (Granted No. XBS1455), the project of Shandong Natural Science Foundation (Granted No. ZR2013FM009), and the Youth Fund of Shandong Women's University (Granted No. 2014ZDX15).

REFERENCES

[1] M. L. Das. Two-factor user authentication in wireless sensor networks. IEEE Trans. Wireless Communication, 2009, 8(3): 1086-1090.

[2] M. K. Khan, K. Alghathbar. Cryptanalysis and security improvement of two-factor user authentication in wireless sensor networks. Sensors, 2010: 2450-2459.

[3] D. J. He, Y. Gao, S. Chan, et al.. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc Sensor Wireless Netw., 2010, 10(4): 1-11.

[4] T. H. Chen, W. K. Shih. A robust mutual authentication protocol for wireless sensor networks. ETRI J., 2010, 32(5): 704-712

[5] C. C. Chang, H. D. Le. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Trans. Wireless Communication, 2016, 15(1): 357-365.

[6] R. Amin, G. P. Biswas. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks, 2016, 36(1): 58-80.

[7] P. Kumar, A. Gurtov, M. Ylianttila, et al.. A strong authentication scheme with user privacy for wireless sensor networks. ETRI Journal, 2013, 35(5): 889-899.

[8] K. Xue, C. Ma, P. Hong, R. Ding. A temporal-credential-based mutual authentication and key agreement scheme for wirless sensor networks. Journal of Network and Computer Applications, 2013, 36(1): 316-323.

[9] D. He, N. Kumar, N. Chilamkurti. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wirless sensor networks. Inf. Sci., 2015, 321: 236-277.

[10] Q. Jiang, J. Ma, F. Wei, et al.. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. Journal of Network and Computer Applications, http: // dx.doi.org/10.1016/j.jnca.2016.10.001.