Cryptanalysis of the Anonymous Authentication with Key Agreement Scheme in Wireless Sensor Networks

Sooyeon Shin and Taekyoung Kwon*
Graduate School of Information, Yonsei University, Seoul, 03722, South Korea
shinsy80@gmail.com, taekyoung@yonsei.ac.kr

Abstract

User authentication and key agreement are important secure services required for wireless sensor networks (WSNs). For this purpose, there have been a large number of proposed authentication and key agreement scheme for WSNs. Recently in 2017, Jung et al. proposed an efficient and security enhanced anonymous authentication with key agreement scheme by employing biometrics information as the third authentication factor. They claimed that their scheme resists on various security attacks and satisfies basic security requirements. However, in this paper, we reveal security weaknesses of Jung et al.'s scheme (i.e., insecurity of the secret key of gateway node, session key compromise, user tracking attack, information leakage attack, and user impersonation attack). We present simple countermeasures against the security weaknesses we have found.

Keywords: Wireless Sensor Networks, User Authentication, Key Agreement

1 Introduction

Wireless sensor networks (WSNs), composed of many low-cost and low-power sensor nodes, have become a popular technology for potential applications in environmental monitoring, wildlife monitoring, health-care, etc. In particular, due to the advent of the Internet of Things (IoT) environment, applications that directly access the WSN and acquire data have also increased. Due to the inherent characteristics of wireless sensor networks, such as the use of wireless communications, unattended deployment of sensor nodes, and resource constraints, there is a high possibility of exposure to various security attacks. In such situations, cryptographic techniques such as encryption and message authentication should be applied to protect user privacy and WSN against various attacks. In order to apply cryptographic techniques, user authentication and key agreement are basically required, and various two-factor and three-factor authentication and key agreement schemes for WSNs have been proposed [6, 5, 9, 12, 13, 11, 2, 4, 1, 10]. In 2015, Chang et al. proposed a two-factor user authenticated key agreement scheme for WSNs [3]. They claimed that their scheme provide session key security and it could resist an off-line password guessing and impersonation attacks. However, their scheme was later proved insecure [8].

Most recently, Jung et al. [8] showed that Chang et al.'s scheme [3] possesses several security weaknesses: their scheme is vulnerable to a password guessing attack and user impersonation attack and it cannot guarantee the secrecy of session key and does not provide session key verification process in the authentication phase. Jung et al. then proposed an improved version of Chang et al.'s scheme by resolving the security weaknesses of Chang et al.'s scheme and by employing biometrics information as an additional authentication factor. They claimed that their improved scheme provides user anonymity and session key security and withstands user impersonation attacks. However, we found that there are fatal security weaknesses in Jung et al.'s scheme. Their scheme basically does not provide strong anonymity,

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 4, Article No. 5 (August 15, 2018)
*Corresponding author: Graduate School of Information, Yonsei University, 50 Yonsei-ro Seodaemun-gu, Seoul, 03722, South Korea, Tel: +82-2-2123-4523

anonymity with untraceability. In addition, although the security of Jung et al.'s scheme depends on the secrecy of the secret key of gateway node, any authorized user can easily obtain it. Therefore, their scheme has resulted in various attack vulnerabilities.

In this paper, therefore, we aim to concretely explain the security weaknesses of Jung et al.'s scheme. We show that their scheme fails to provide the security of the gateway node's secret key and untraceability. We also show that the scheme suffers from information leakage attack, session key compromise, and user impersonation attack. The remainder of the paper is organized as follows. A brief review of Jung et al.'s scheme is presented in Section 2. We reveal the security weaknesses of Jung et al.'s scheme in Section 3. Finally, we conclude the paper in Section 4.

2 Review of Jung et al.'s Scheme

In this section, we review Jung et al.'s scheme [8], a three-factor authentication and key agreement scheme for WSNs. It is composed of four phases: registration, login, authentication, and password change. We briefly present essential phases of Jung et al. scheme to show its security weaknesses. Notations of Jung et al.'s scheme are listed in Table 1.

Table 1: List of notations used in Jung et al.'s scheme.

Notation	Description	Notation	Description
U_i	User	K	Secret key generated by the GWN
S_j	Sensor node	K_S	Session key
GWN	Gateway node	T_x	Current timestamp values
ID_i	Identity of the user U_i	ΔT	The maximum of the transmission delay time
PW_i	Password of the user U_i	$h(\cdot)$	One-way hash function
Bio_i	Biometric information of U_i	$H(\cdot)$	Biohash function
TID_i	Temporary identity for U_i's next login	$f(s,k)$	Pseudo-random function of variable s with the key k
SID_j	Identity of the sensor node S_j	$\|\|$	Concatenate operation
u	Random number of U_i	$\oplus$	Bit wise XOR operation

2.1 Registration Phase

For each sensor node, GWN loads pre-defined values SID_j and $X^*_{S_j} = h(SID_j||K)$ into S_j's memory. For user registration, the following steps need to be executed via a secure channel.

(1) U_i selects ID_i and PW_i, and imprints his/her biometric information Bio_i. U_i selects u and comptutes $HPW_i = h(PW_i||H(Bio_i))$ and $TID_i = h(ID_i||u)$. U_i then sends a registration request $\langle TID_i, HPW_i \rangle$ to GWN.

(2) GWN computes $HID_i = h(TID_i||K) \oplus HPW_i$, $A_i = h(HPW_i||TID_i) \oplus HID_i$, $B_i = h(HPW_i||HID_i)$, and $C_i = HID_i \oplus K$. GWN issues a smart card with $\{A_i, B_i, C_i, h(\cdot), H(\cdot)\}$ to U_i.

(3) U_i computes $D_i = u \oplus H(Bio_i)$ and stores it in the smart card.

2.2 Login and Authentication Phases

The login and authentication phases are executed when a user wants to access to the WSN and to achieve mutual authentication and session key agreement between U_i, GWN, and S_j.

(1) U_i inserts the smart card into a terminal, inputs ID_i and PW_i, and imprints Bio_i. The smart card computes $HPW_i^* = h(PW_i||H(Bio_i))$, $u = D_i \oplus H(Bio_i)$, $TID_i = h(ID_i||u)$, $HID_i^* = A_i \oplus h(HPW_i^*||TID_i)$, and $B_i^* = h(HPW_i^*||HID_i^*)$. The smart card verifies $B_i^* \stackrel{?}{=} B_i$, if no so, it terminates this phase. Otherwise, the smart card acknowledge the legitimacy of the U_i.

(2) The smart card computes $DID_i = TID_i \oplus HID_i^*$ and $M_{U_i,G} = h(TID_i||HPW_i^*||HID_i^*||T_1)$ and sends a login request $\langle DID_i, M_{U_i,G}, C_i, T_1 \rangle$ to GWN via a public channel.

(3) GWN first checks the validity of the time stamp $|T_1' - T_1| < \Delta T$ and computes $TID_i^* = DID_i \oplus C_i \oplus K$, $HID_i = C_i \oplus K$, $HPW_i^* = HID_i \oplus h(TID_i^*||K)$, and $M_{U_i,G}^* = h(TID_i^*||HPW_i^*||HID_i^*||T_1)$. GWN verifies $M_{U_i,G}^* \stackrel{?}{=} M_{U_i,G}$, if not so, it terminates this phase. Otherwise, GWN acknowledges the legitimacy of U_i.

(4) GWN selects a random number R and computes $X_{S_j} = h(SID_j||K), M_j = R \oplus X_{S_j}$, $K_S = f(DID_i, R)$, and $M_{G,S_j} = h(DID_i||SID_j||X_{S_j}||K_S||T_2)$. GWN sends the message $\langle DID_i, M_{G,S_j}, M_j, T_2 \rangle$ to S_j via a public channel.

(5) After receiving the message, S_j checks the validity of the time stamp T_2 and computes $R^* = M_j \oplus X_{S_j}^*$, $K_S^* = f(DID_i||R^*)$, and $M_{G,S_j}^* = h(DID_i||SID_j||X_{S_j}^*||K_S^*||T_1)$. S_j then verifies $M_{G,S_j}^* \stackrel{?}{=} M_{G,S_j}^*$, if not so, it terminates this phase. Otherwise, S_j believes that the GWN is authentic.

(6) S_j computes $k_j = (X_{S_j}^*||T_3)$ and $M_{S_j,G} = h(k_j||X_{S_j}^*||K_S^*||T_3)$ and sends the message $\langle M_{S_j,G}, T_3 \rangle$ to GWN via a public channel.

(7) GWN checks the validity of the time stamp T_3 and computes $k_j^* = h(X_{S_j}||T_3)$ and $M_{S_j,G}^* = h(k_j^*||X_{S_j}||K_S||T_3)$. GWN then verifies $M_{S_j,G}^* \stackrel{?}{=} M_{S_j,G}$, if not so, it terminates this phase. Otherwise, GWN believes that the S_j is authentic.

(8) GWN computes $k_i = R \oplus h(TID_i^*||K)$ and $M_{G,U_i} = h(K_S||k_i||T_4)$ and sends the message $\langle k_i, M_{G,U_i}, T_4 \rangle$ to U_i via a public channel.

(9) U_i checks the validity of the time stamp T_4 and computes $R^* = k_i \oplus HPW_i \oplus HID_i^*$, $K_S^* = f(DID_i, R^*)$, and $M_{G,U_i}^* = h(K_S^*||k_i||T_4)$. U_i verifies $M_{G,U_i}^* \stackrel{?}{=} M_{G,U_i}$, if not so, he/she terminates this phase. Otherwise, U_i believes that the GWN is authentic and successfully ends the authentication phase.

3 Cryptoanalysis of Jung et al.'s Scheme

In this section, we discuss the security weaknesses of Jung et al.'s scheme [8] and show that an attacker can mount different types of attacks on Jung et al.'s scheme.

3.1 User Tracking Attack

As the concern for privacy increases in our lives, user anonymity has become a vital security requirement in various applications including WSN applications. In general, the preservation of identity privacy in the context of an authentication protocol requires not only anonymity but also untraceability [7]. Although untraceability is not a necessary condition of anonymity, strong anonymity with untraceability is required for fully protecting user privacy. In Jung et al.'s scheme, every time U_i uses the fixed values DID_i and C_i to login the WSN thus anyone can track U_i according to these strings constantly. Therefore, Jung et al.'s scheme is prone to user tracking attack and fails to provide untraceability.

3.2 Insecurity of the Secret key of the Gateway Node

Security of Jung et al.'s scheme depends on the secrecy of the secret key K generated by GWN. Unfortunately, any authorized user U_i can extract the secret key K used to compute critical parameters of users' smart cards and the secret keys of all sensor nodes. Assume that U_i retrieves the information $\langle A_i, B_i, C_i, D_i \rangle$ from his or her smart card, where $A_i = h(HPW_i||TID_i) \oplus HID_i$, $B_i = h(HPW_i||HID_i)$, $C_i = HID_i \oplus K$, and $D_i = u \oplus H(Bio_i)$. As the smart card calculates at the login phase, U_i then computes $u = D_i \oplus H(Bio_i)$, $TID_i' = h(ID_i||u)$, and $HID_i' = A_i \oplus h(HPW_i||TID_i')$. Based on HID_i' and C_i, U_i computes K', where $K' = C_i \oplus HID_i'$. Since he or she now knows the secret key K', U_i can impersonate GWN and further launch the following attacks.

3.3 Information Leakage Attack

We described how an authorized user U_j can know K' in Section 3.2. After getting K', U_j who acts as an adversary $\mathcal{A}$ can achieve secret information required for authentication and key agreement as follows:

(1) $\mathcal{A}$ intercepts the user U_i's login message $\langle DID_i, M_{U_i,G}, C_i, T_1 \rangle$, where $DID_i = TID_i \oplus HID_i$, $M_{U_i,G} = h(TID_i||HPW_i||HID_i||T_1)$, and $C_i = HID_i \oplus K$.

(2) $\mathcal{A}$ computes $HID_i' = C_i \oplus K'$ and $TID_i' = DID_i \oplus HID_i'$.

(3) $\mathcal{A}$ then computes $HPW_i' = HID_i' \oplus h(TID_i'||K')$.

Thus, $\mathcal{A}$ can obtain all secret values TID_i', HID_i', and HPW_i' need to login the WSN and launch session key recovery attack and user impersonation attack.

3.4 Session Key Compromise

We assume that $\mathcal{A}$ can obtain the secret information by intercepting the U_i's login message and also can intercept the last message of the authentication phase. After getting the secret information in Section 3.3 and k_i, $\mathcal{A}$ can successfully launch a session key recovery attack as follows:

(1) $\mathcal{A}$ intercepts the last message $\langle k_i, M_{G,U_i}, T_4 \rangle$ sent from GWN, where $k_i = R \oplus h(TID_i||K')$ and $M_{G,U_i} = h(K_S||k_i||T_4)$.

(2) $\mathcal{A}$ computes $R' = k_i \oplus h(TID_i'||K)$.

(3) $\mathcal{A}$ discovers the session key K_S' between the user U_i, GWN, and the sensor node S_j by computing $K_S' = f(DID_i||R')$.

Thus, according to the above procedure an adversary can successfully construct the session key K_S' between U_i, GWN, and S_j.

3.5 User Impersonation Attack

Once an adversary $\mathcal{A}$ achieves the GWN's secret key K and secret information TID_i', HID_i', and HPW_i' as described in Section 3.2 and Section 3.3, respectively, $\mathcal{A}$ can also impersonate a user U_i in Jung et al.'s scheme without the target user's identity ID_i, password PW_i, and biometric information Bio_i as follows:

(1) $\mathcal{A}$ computes $DID_i' = TID_i' \oplus HID_i', C_i' = HID_i' \oplus K'$ and $M_{U_i,G}' = h(TID_i'||HPW_i'||HID_i'||T_1')$, where T_1' is the current time stamp used by $\mathcal{A}$. Of course, since DID_i and C_i are the fixed values, it is possible to use the previously intercepted one.

(2) $\mathcal{A}$ sends the login message $\langle DID_i', M_{U_i,G}', C_i', T_1' \rangle$.

(3) At GWN, user authentication is successfully performed and $\mathcal{A}$ calculates the session key K_S' after receiving the last message as described in Section 3.4.

It is clear from the above discussion that $\mathcal{A}$ can masquerade as a valid user U_i to login to the WSN without ID_i, PW_i and Bio_i. Thus, Jung et al.'s scheme is vulnerable to the user impersonation attack.

4 Countermeasure

In this section, we present a simple countermeasure against the attacks mentioned in the previous section. The problem of the Jung et al.'s scheme is that C_i includes K through a simple XOR operation. This K is GWN's secret value commonly used for all users and sensor nodes thus any user who has completed the legitimate registration phase can easily find out this value. It is also a problem to use C_i as the login message with the fixed DID_i value. If these two problems are solved, it is possible to defend five attacks mentioned in the previous section at once.

4.1 Modified Registration Phase

To support untraceability and to counter the attacks, there is an alternative in which the GWN issues a one-time pseudonym PID_i^1 for U_i and changes C_i to its masked value. GWN then stores the one-time pseudonym PID_i^1 with TID_i and HID_i into its memory. Since PID_i^1 is one-time value, GWN will send a new pseudonym for the next login and authentication before the end of the login and authentication phase and U_i will update the related value in own smart card. The details of the modified registration phase are as follows.

(2) GWN randomly selects a one-time pseudonym PID_i^1 for the first login and authentication and computes $HID_i = h(TID_i||K) \oplus HPW_i$, $A_i = h(HPW_i||TID_i) \oplus HID_i$, $B_i = h(HPW_i||HID_i)$, and $C_i = h(TID_i||HID_i) \oplus PID_i^1$. GWN issues a smart card with $\{A_i, B_i, C_i, h(\cdot), H(\cdot)\}$ to U_i. GWN then stores PID_i^1 with TID_i and HID_i into own memory for U_i.

4.2 Modified Login and Authentication Phases

In the modified registration phase, a user is issued a one-time pseudonym and C_i no longer contains K. The details of the modified login and authentication phases are as follows.

(2) The smart card computes $PID_i^1 = C_i \oplus h(TID_i||HID_i^*)$ and $M_{U_i,G} = h(TID_i||HPW_i^*||HID_i^*||PID_i^1||T_1)$ and sends a login request $\langle PID_i^1, M_{U_i,G}, T_1 \rangle$ to GWN via a public channel.

(3) GWN first checks the validity of the time stamp $|T_1' - T_1| < \Delta T$ and searches TID_i and HID_i from the memory using PID_i^1. GWN then computes $HPW_i^* = HID_i \oplus h(TID_i||K)$ and $M_{U_i,G}^* = h(TID_i||HPW_i^*||HID_i||PID_i^1||T_1)$. GWN verifies $M_{U_i,G}^* \stackrel{?}{=} M_{U_i,G}$, if not so, it terminates this phase. Otherwise, GWN acknowledges the legitimacy of U_i.

(4) GWN selects a random number R and computes $X_{S_j} = h(SID_j||K), M_j = R \oplus X_{S_j}$, $K_S = f(PID_i^1, R)$, and $M_{G,S_j} = h(PID_i^1||SID_j||X_{S_j}||K_S||T_2)$. GWN sends the message $\langle PID_i^1, M_{G,S_j}, M_j, T_2 \rangle$ to S_j via a public channel.

(5) After receiving the message, S_j checks the validity of the time stamp T_2 and computes $R^* = M_j \oplus X_{S_j}^*$, $K_S^* = f(PID_i^1||R^*)$, and $M_{G,S_j}^* = h(PID_i^1||SID_j||X_{S_j}^*||K_S^*||T_2)$. S_j then verifies $M_{G,S_j}^* \stackrel{?}{=} M_{G,S_j}^*$, if not so, it terminates this phase. Otherwise, S_j believes that the GWN is authentic.

(8) *GWN* randomly selects the next pseudonym PID_i^2 and computes $C_i' = h(TID_i||HID_i) \oplus PID_i^2$, $p_i = C_i' \oplus H(HPW_i^*)$, $k_i = R \oplus h(TID_i^*||K)$ and $M_{G,U_i} = h(C_i'||p_i||K_S||k_i||T_4)$ and sends the message $\langle p_i, k_i, M_{G,U_i}, T_4 \rangle$ to U_i via a public channel.

(9) U_i checks the validity of the time stamp T_4 and computes $R^* = k_i \oplus HPW_i \oplus HID_i^*$, $K_S^* = f(PID_i^1, R^*)$, $C_i'^* = p_i \oplus H(HPW_i)$, and $M_{G,U_i}^* = h(C_i'^*||p_i||K_S^*||k_i||T_4)$. U_i verifies $M_{G,U_i}^* \stackrel{?}{=} M_{G,U_i}$, if not so, he/she terminates this phase. Otherwise, U_i believes that the *GWN* is authentic, updates C_i in the smart card to $C_i'^*$, and successfully ends the authentication phase.

In the modified login and authentication phases, the user can login in with the one-time pseudonym thus the modified version supports untraceability. In addition, no one including a legitimate user can easily retrieve K from any values of the smart card. Thus, it is impossible for an adversary to launch information leakage and user impersonation attacks and to compromise the session key.

5 Conclusion

In this paper, we have reviewed the recently proposed Jung et al.'s authentication and key agreement scheme for WSNs. We have analyzed the security weaknesses of Jung et al.'s scheme. We have pointed out that Jung et al.'s scheme failed to provide user's anonymity and session key security. We have also pointed out that Jung et al.'s scheme is vulnerable to user tracking attack, information leakage attack, and user impersonation attack. We have briefly presented the countermeasures against those security weaknesses of the Jung et al.'s scheme. In the future work, we will propose an enhanced user authentication and key agreement scheme for WSNs. We will also analysis security and performance of the enhanced scheme.

Acknowledgement

This work was supported in part by the National Research Foundation of Korea (NRF-2016-R1C1B2011095) and also by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2016-0-00304) supervised by the IITP(Institute for Information & communications Technology Promotion).

References

[1] R. Amin and G. Biswas. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks*, 36(P1):58–80, January 2016.

[2] C. C. Chang and H. D. Le. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Transactions on Wireless Communications*, 15(1):357–366, August 2015.

[3] I. Chang, T. Lee, T. Lin, and C. Liu. Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks. *Sensors*, 15(12):29841–29854, November 2015.

[4] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. *Ad Hoc Networks*, 36(1):152–176, January 2016.

[5] 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*, 10(4):361–371, February 2010.

[6] H. F. Huang, Y. F. Chang, and C. H. Liu. Enhancement of two-factor user authentication in wireless sensor networks. In *Proc. of the 6th Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'10), Darmstadt, Germany*, pages 27–30. IEEE, October 2010.

[7] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang. An untraceable temporal-credential-based two-factor authentication scheme using ecc for wireless sensor networks. *Journal of Network and Computer Applications*, 76(C):37–48, December 2016.

[8] J. Jung, J. Moon, D. Lee, and D. Won. Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks. *Sensors*, 17(3):644, Mar 2017.

[9] A. K. Khan MK. Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'. *Sensors*, 10(3):2450–2459, March 2010.

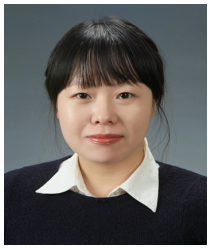
[10] W.-L. Tai, Y.-F. Chang, and W.-H. Li. An IoT notion–based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks. *Journal of Information Security and Applications*, 34(2):133–141, June 2017.

[11] M. Turkanović, B. Brumen, and M. Hölbl. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*, 20:96–112, September 2014.

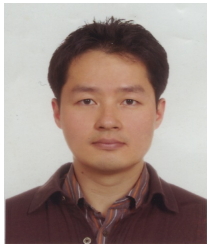
[12] M. Turkanović and M. Hölbl. An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Elektronika ir Elektrotechnika*, 19(6):109–116, June 2013.

[13] 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*, 36(1):316–323, January 2013.

Author Biography



Sooyeon Shin received her B.S., M.S., and Ph.D. degrees in computer science and engineering from Sejong University, Seoul, Korea, in 2004, 2006, and 2012, respectively. From 2012 to 2013, she was a post-doctoral researcher at Sejong University. In 2013, she joined Yonsei University, Seoul, Korea, to continue her post-doctoral research. Her current research interests include cryptographic protocol, privacy preservation, user authentication, computer network security, wireless sensor network security, and usable security.



Taekyoung Kwon received his B.S., M.S., and Ph.D. degrees in computer science from Yonsei University, Seoul, Korea, in 1992, 1995, and 1999, respectively. He is currently an Associate Professor of information at Yonsei University, Seoul, Korea. From 1999 to 2000, he was a Post-Doc Researcher at the University of California, Berkeley, CA, USA. From 2001 to 2013, he was a professor of computer engineering at Sejong University, Seoul, Korea. In 2013, he returned to Yonsei University, Seoul, Korea. His current research interests include applied cryptography, cryptographic protocol, network protocol, usable security, and human-computer interactions.