Cryptanalysis on Symmetric Key Techniques Based Authentication Scheme for Wireless Sensor Networks

Younsung Choi, Youngsook Lee and Dongho Won

Abstract In wireless sensor networks, user authentication scheme is a critical and important security issue to prevent adversary's illegal approach to wireless sensors. After Das introduce a user authentication scheme for wireless sensor networks, various studies had proceeded to proposed more secure and efficient authentication scheme but many schemes had security problem on smart card attack. So Chem et al. suggested a secure user authentication scheme against smart card loss attack using symmetric key techniques but this scheme does not still resolve some security vulnerability. So by the cryptanalysis, this paper shows that Chem et al's scheme has problems on perfect forward secrecy, session key exposure by gateway node, anonymity, and the password check.

Keywords User authentication scheme · Cryptanalysis · Wireless Sensor Networks

1 Introduction

Recently, wireless sensor networks (WSNs) have been substantially investigated by researches. It can observe various hazardous conditions, such as volcanic

Y. Choi · D. Won(✉)
Department of Computer Engineering, Sungkyunkwan University, 2066 Seoburo, Suwon, Gyeonggido 440-746, Korea
e-mail: {yschoi,dhwon}@security.re.kr

Y. Lee
Department of Cyber Investigation Police, Howon University,
64 Howon University 3 Gil, Impi-Myeon, Gunsan-Si, Jeonrabuk-Do 573-718, Korea
e-mail: ysooklee@howon.ac.kr

This research was supported by Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Science, ICT & Future Planning (NRF-2014R1A1A2002775)

D.-S. Park et al. (eds.), *Advances in Computer Science and Ubiquitous Computing*,
Lecture Notes in Electrical Engineering 373,
DOI: 10.1007/978-981-10-0281-6_2

temperature, battlefield surveillance[1]. To use more secure and efficient communication on WSNs, various studies on user authentication had progressed from previous times. Das introduced a two-factor user authentication scheme firstly using password and smart card[2]. Since then, various researchers analyzed Das's authentication scheme and showed the problems of the scheme, and proposes more secure and efficient user authentication scheme for WSNs. Nyang and Lee[3] pointed out that Das's scheme has vulnerability on an offline password guessing attack and node compromise attack. Khan-Alghathbar showed Das's scheme is insecure to gateway nodes bypass attack[4]. After analyzing Das's scheme and Khan-Alghathbar's scheme, Vaidya et al. point out that they have security problem attacks such as smart card loss attacks[5].

To resolve the smart card attack such as offline password guessing attack, Yuan proposed biometric-based authentication scheme[6], and Yeh et al. improve Yuan's scheme[7] and Choi et al. proposed security enhanced scheme using elliptic curve cryptography for WSNs to solve Yuan and Yeh et al.'s security problem[8].

Chen et al. proposed a secure user authentication scheme against smart card loss attack for WSNs using symmetric key techniques. This scheme improves the security using only password and symmetric key algorithm without biometrics and public key crypto-system[9]. But we review and analyze Chen et al.'s scheme and found out various security problems on this scheme.

The remainder of this paper is organized as follows. Section 2 briefly reviews Chen et al.'s authentication scheme while Section 3 provides a detailed security analysis on perfect forward secrecy, session key exposure by gateway node, anonymity, and password check problem of Chen et al.'s scheme. Section 4 concludes this paper.

2 Review of Chen et al.'s Authentication Scheme

In this section, we describe the phase of Chen et al.'s scheme. This scheme is divided into three phase: the registration phase, password updating phase, and authentication phase. Figure 1 shows the authentication phase of Chen et al.'s scheme. Gateway node GW has secret values x_a and x_s, and share $h(x_s||SID_n)$ with sensors node S_n[9].

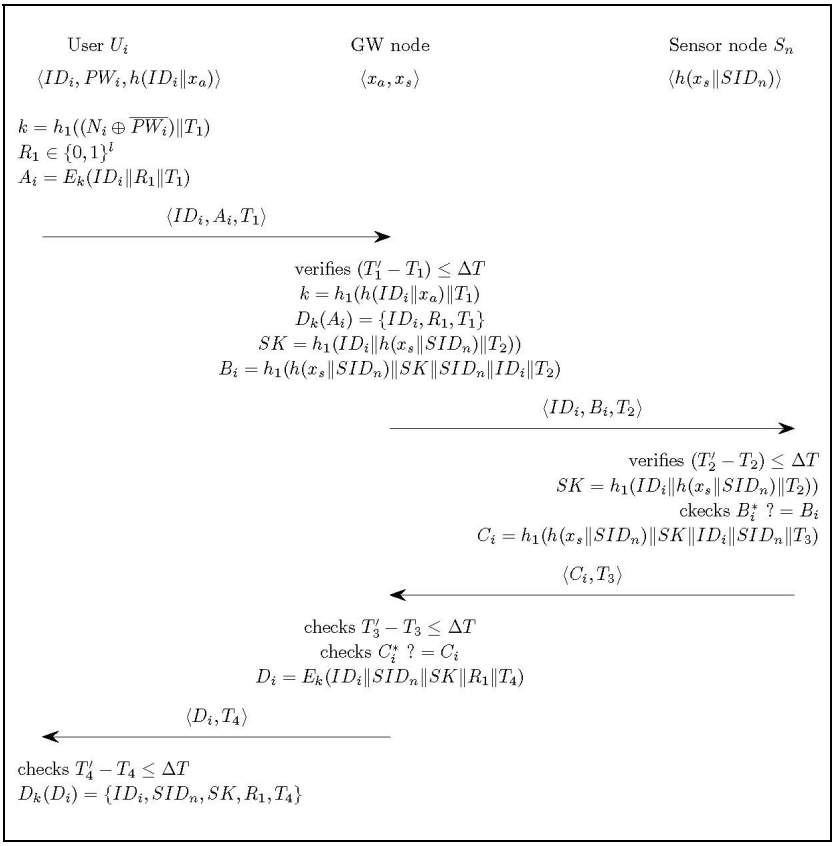

Fig. 1 Authentication phase of Chen et al.'s scheme

[Registration phase] (1) User U_i selects identifier ID_i and password PW_i, generates a random number b, and computes $\overline{PW_i} = h(PW_i \| b)$. Then U_i sends ID_i and $\overline{PW_i}$ to the gateway node GW over a secure channel. **(2)** GW computes $N_i = h(ID_i \| x_a) \oplus \overline{PW_i}$. GW stores $\{ID_i, N_i, h(\cdot)\}$ into a smart card and sends it to U_i. **(3)** After U_i receives the smart card, U_i inputs b into smart card and finishes the registration phase.

[Password updating phase] (1) U_i inserts smart card into the terminal and enters ID_i, old password PW_i, new password PW_i^*. **(2)** U_i's smart card verifies the entered ID_i using stored value ID_i. If ID_i is accurate, then U_i is approved to change the password. **(3)** U_i's smart-card calculates $\overline{PW_i} = h(PW_i \| b)$, $\overline{PW^*_i} = h(PW_i^* \| b)$, and $N_i^* = N_i \oplus \overline{PW_i} \oplus \overline{PW^*_i}$ and then replaces old value N_i with new value N_i^*, and finishes this phase.

[Authentication phase] (1) U_i inserts smart card to terminal and ID_i and PW_i. Smart card computes $\overline{PW_i} = h(PW_i \| b)$, $k = h_1((N_i \oplus PW_i) \| T_1)$, T_1 is current timestamp of U_i. The smart card generates random number $R_1 \in \{0, 1\}^l$, computes $A_i = E_k(ID_i \| R_1 \| T_1)$,

$E(\cdot)$ is asymmetric key cryptography function; $E_k(*)$ means that "$*$" is encrypted by $E(\cdot)$ with symmetric key k. Then it sends $\{ID_i, A_i, T_1\}$ to GW. **(2)** GW receives $\{ID_i, A_i, T_1\}$. GW verifies T_1. If $(T'_1 - T_1) \leq \Delta T$, then GW continues to the next step, ΔT denotes expected time interval for the delay. GW computes $k=h_1(h(ID_i||x_a)||T_1)$ and $D_k(A_i) = \{ID_i, R_1, T_1\}$, where $D_k(*)$ means that "$*$" is decrypted by the key k. Then GW checks whether decrypted messages ID_i and T_1 are equal to received ones. GW computes $SK=h_1(ID_i||\ h(x_s||SID_n)||T_2)$, $B_i = h_1(h(x_s||\ SID_n)||SK||SID_n||ID_i||T_2)$, SK is the session key between U_i and S_n. Then the GW sends the message $\{ID_i, B_i, T_2\}$ to the sensor node S_n. **(3)** S_n validates T_2, computes the $SK = h_1(ID_i||h(x_s||SID_n)||T_2)$. S_n computes $B_i^* = h_1(h(x_s||\ SID_n)||SK||SID_n||ID_i||T_2)$ and then checks whether $B_i^* = B_i$. S_n computes $C_i = h_1(h(x_s||\ SID_n)\ ||SK\ ||\ ID_i||SID_n||\ T_3)$. S_n sends the message $\{C_i, T_3\}$ to GW. **(4)** GW first verifies T_3, computes $C_i^* = h_1(h(x_s||\ SID_n)||SK||ID_i||SID_n||T_3)$ and then checks whether $C_i^* = C_i$. GW computes $D_i = (ID_i||\ SID_n||\ SK\ ||R_1||\ T_4)$, then sends the message $\{D_i, T_4\}$ to U_i. **(5)** U_i computes $(D_i) = \{ID_i, SID_n, SK, R_1, T_4\}$; then U_i checks whether the decrypted messages ID_i, R_1, and T_4 are equal to the previous ones. If it is same, user U_i establishes trust on GW and establishes SK with sensor node S_n.

3 Cryptanalysis of Chen et al.'s Authentication Scheme

3.1 No Perfect Forward Secrecy

Chen et al.'s authentication scheme does not provide the perfect forward secrecy. Perfect forward secrecy means that a session key derived from a set of long-term keys will not be compromised if one of the long-term keys is compromised in the future [8,10]. So an adversary can compute the session key sk between the U_i and S_j if the adversary knows the one of long-term key $h(x_s||SID_n)$ in future. Figure 2 describes the lack of perfect forward secrecy on Chen's authentication scheme. Adversary can get ID_i and T_2 in public communication. If adversary know one of user's long-term secret $h(x_s||SID_n)$, the adversary can compute the session key $SK = h_1(ID_i||\ h(x_s||SID_n)||T_2)$. Moreover, the adversary can get the previous information ID_{pi} and T_{p2}. Then, the adversary can compute all of previous session key SK_p between user and sensor node.

- Adversary get ID_i and T_2 in public channel.
- Adversary know one of long-term secret : $h(x_s\ ||\ SID_n)$.
  - Adversary has ID_i and T_2 , computes SK as follows,
  - $SK = h_1(ID_i\ ||\ h(x_s\ ||\ SID_n)\ ||\ T_2)$.
- Adversary can get previous ID_{pi} and T_{p2}, then computes SK_p.
  - $SK_p = h_1(ID_{pi}\ ||\ h(x_s\ ||\ SID_n)\ ||\ T_{p2})$.
- Adversary can compute all of previous session key SK_p.

Fig. 2 Lack of perfect forward secrecy on Chen et al.'s scheme

3.2 Session Key Exposure by GW node

In Chen et al.'s scheme, session key is used for secure communication between U_i and S_n after authentication phase. It is important matter that anyone cannot compute SK with the exception of U_i and S_n even if GW node is trust node. However, Chen et al.'s scheme is vulnerable to this problem. Figure 3 describes the session key exposure by GW on Chen et al.'s scheme. GW can have ID_i, x_s, SID_n and T_2, so GW can compute session key SK=$h_1(ID_i \| h(x_s \| SID_n) \| T_2)$. Therefore, GW can compute all of session key between U_i and S_n. It means that GW decrypts the secret message between U_i and S_n so GW can gain all of the important information between every U_i and S_n.

- Session key SK is used to communicate securely between U_i and S_n.
- It is important that anyone cannot compute the SK except for U_i and S_n.
- But GW can compute the SK between all of registrated U_i and S_n.
  - GW has ID_i, x_s, SID_n, T_2.
  - $SK = h_1(ID_i \| h(x_s \| SID_n) \| T_2)$.

$\Rightarrow$ GW can compute all session key sk between U_i and S_n.

$\Rightarrow$ GW can decrypt the secret messages between U_i and S_n.

$\Rightarrow$ GW can acquire the important information between U_i and S_n.

Fig. 3 Session key exposure by GW node of Chen et al.'s scheme

3.3 Lack of Anonymity

Figure 4 describes the problem due to the lack of anonymity on Chen et al.'s scheme. User U_i sends own ID_i to GW using public communication, and GW sends ID_i to the sensor S_n without any protection. So an adversary can easily acquire ID_i from public communications. Therefore the adversary can get various information using user's ID_i. For observing GW's receiving communication, the adversary can obtain how many users are registered to GW. Moreover, the

- Adversary can get ID_i in public communication between U_i and GW, GW and S_n.

User U_i $\xrightarrow{< ID_i, A_i, T_1 >}$ Gateway GW $\xrightarrow{< ID_i, B_i, T_2 >}$ Sensor S_n

$\Rightarrow$ Adversary can get to know how many users are registered in GW.

$\Rightarrow$ Adversary can get to know which users provide the data by accessing to S_n.

- Due to the lack of anonymity,
  Adversary can acquire important information using ID_i in Chen et al.' scheme.

Fig. 4 Lack of Anonymity on Chen et al.'s scheme

adversary can get to know which users communicate with S_n, in other words, which users obtain the data by accessing to S_n. the lack of anonymity in Chen et al.'s scheme cause various problem so it need to be addressed by providing user anonymity through various *ID* protection technique.

3.4 Lack of Password Check

Chen et al.'s scheme cannot provide the password check in user's smart card therefore various problems occur in authentication phase and password updating phase. Figure 5 describes the problems due to the lack of password check on Chen et al.'s scheme.

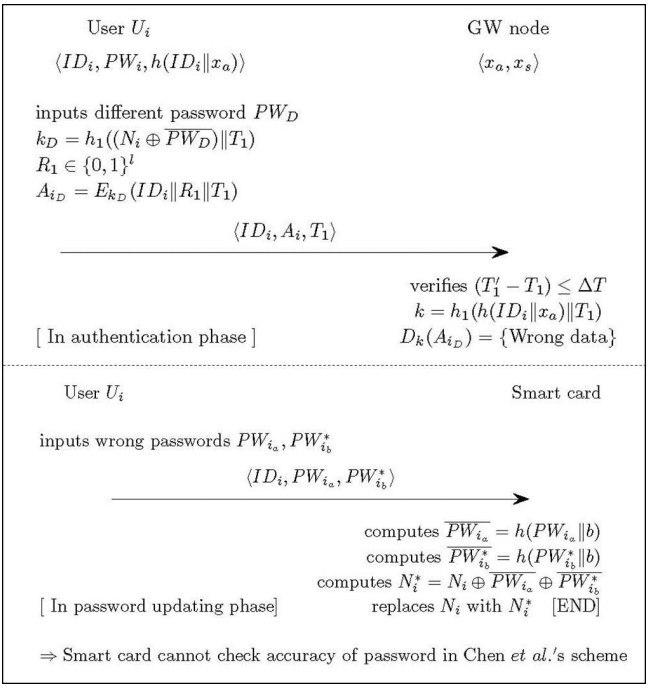

Fig. 5 Lack of Password Check on Chen et al.'s scheme

In authentication phase, user's smart card cannot recognize user's wrong password so encrypts the data using $k_{D,}$ which is made by wrong password. Moreover, U_i sends the faulty authentication messages <ID_i, A_{iD}, T_1> to GW. In password updating phase, smart card cannot discontinue the phase even if U_i inputs wrong old password. Therefore, smart card computes wrong values such as $\overline{PW_{ia}}$, $\overline{PW^*_{ib}}$, and $N_i^* = N_i \oplus \overline{PW_{ia}} \oplus PW^*_{ib}$, then replace N_i with wrong N_i^*. This problem causes that user cannot execute authentication phase due to wrong N_i^* even if U_i inputs normal new password.

4 Conclusion

To solve various problems such as smart card loss attack, Chen et al. proposed a secure user authentication scheme using symmetric key techniques for WSNs but it still has some problems. In this paper, we first review Chen et al.'s scheme and analyze this scheme using the cryptanalysis. So we have identified that Chen et al.'s scheme designed for WSNs is vulnerable to: lack of perfect forward secrecy, session key exposure by GW node, lack of anonymity, lack of password check. This study on cryptanalysis analysis can be used to make more secure authentication scheme.

References

1. Nam, J., Choo, K.K.R., Han, S., Kim, M., Paik, J., Won, D.: Efficient and Anonymous Two-Factor User Authentication in Wireless Sensor Networks: Achieving User Anonymity with Lightweight Sensor Computation. PLOS ONE **10**(4) (2015)
2. Das, M.L.: Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communications **8**(3), 1086–1090 (2009)
3. Nyang, D., Lee, M.K.: Improvement of Das's two-factor authentication protocol in wireless sensor networks. IACR Cryptology ePrint Archive (2009)
4. Khan, M.K., Alghathbar, K.: Security analysis of 'two-factor user authentication in wireless sensor networks'. In: Advances in Computer Science and Information Technology. Lecture Notes in Computer Science, vol. 6059, pp. 55–60. Springer, Germany (2010)
5. Vaidya, B., Makrakis, D., Mouftah, H.T.: Improved two factor user authentication in wireless sensor networks. In: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2010), pp. 600–606, October 2010
6. Yuan, J.J.: An enhanced two-factor user authentication in wireless sensor networks. Telecommunication Systems **55**(1), 105–113 (2014)
7. Yeh, H.L., et al.: A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography. Sensors **11**(5), 4767–4779 (2011)
8. Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J., Won, D.: Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors **14**(6), 10081–10106 (2014)
9. Chen, L., Fushan, W., Chuangui, M.: A Secure User Authentication Scheme against Smart-Card Loss Attack for Wireless Sensor Networks Using Symmetric Key Techniques. International Journal of Distributed Sensor Networks (2015)
10. Kim, J., Lee, D., Jeon, W., Lee, Y., Won, D.: Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks. Sensors **14**(4), 6443–6462 (2014)

http://www.springer.com/978-981-10-0280-9

Advances in Computer Science and Ubiquitous Computing
CSA & CUTE
Park, D.-S.; Chao, H.-C.; Jeong, Y.-S.; Park, J.J. (Eds.)
2015, XXXI, 918 p. 415 illus. in color., Hardcover
ISBN: 978-981-10-0280-9