International Journal of Engineering & Technology, 7 (2.12) (2018) 58-61

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A study on user authentication and key agreement protocol in wireless sensor network

Jae-young Lee *

School of Information & Communication Systems, Semyung University, Jecheon, 27136, Republic of Korea
**Corresponding author E-mail: klitie@semyung.ac.kr*

Abstract

Background/Objectives: The user authentication and key agreement protocol proposed by Jung et al., which is suitable for a wireless sensor network environment is vulnerable to an attack in which a user who is issued a smart card from the gateway, completing the registration step disguises as a random user.
Methods/Statistical analysis: This study proposed a method of improving the problem of the security technique proposed by Jung et al., which is vulnerable to a user impersonation attack. This method uses the variable that recorded the times of a user's request for registration to the gateway in the registration step in which the user is registered to the gateway and a smart card is issued and the login step in which the user issued the smart card is authenticated as a legitimate user.
Findings: The security technique proposed in this study consists of four steps, same as the security technique of user authentication and key agreement proposed by Jung et al. In the first step, the registration step, if a user requests for registration to the gateway, the variables that recorded the times of the user's request for registration (User: Un and Gateway: Gn) are renewed and stored respectively by the user and the gateway. Once the registration step is completed, the user who got a smart card issued from the gateway is authenticated as a legitimate user in the login step, using the issued smart card, ID, password and Un. When the login step is completed, in the third step, the authentication step, the authentication procedures are carried out for the gateway and the sensor node.
An attacker obtains a user's information through various attacks, such as smart-card loss attack, ID-guessing attack or password-guessing attack and attempts the login step, using the obtained information. However, the technique proposed in this study needs the variable that recorded the times of the user's request for registration to the gateway in addition to a smart card, ID and password to proceed with user authentication in the login step. This variable is a value that only the user and the gateway know, not transmitted in any steps. The attacker who does not know the times of requests for registration cannot proceed with the login step, and the attacker cannot be authenticated as a legitimate user without proceeding to the login step. Thus, the user authentication and key agreement protocol proposed in this study is safe from an attacker's attack of impersonation as a user.
Improvements/Applications: This study proposed a technique of using the variable that recorded the times of the user's request for registration to the gateway, managed and stored only by the user and the gateway, not transmitted in any steps in user authentication. The proposed technique is safe from an attacker's attack of impersonation as a user.

Keywords: *Wireless Sensor Network; User Authentication; Key Agreement; Impersonation Attack; Smart Card; Protocol.*

1. Introduction

A wireless sensor network is a network that distributes micromini sensor nodes in certain areas, observes physical and environmental conditions such as temperature, sound and pressure, processes the data collected in the form that the user wants and transmits them by wireless communications [1]. The wireless sensor network consists of hundreds or thousands of sensor nodes, and the sensor nodes produced at low costs, which generally minimize the costs for the sensor nodes have limited resources as compared to other mobile devices of wireless network [2].
In the wireless sensor network consisting of sensor nodes with limited resources, it is difficult to apply the security techniques used in the existing networks as they are. Accordingly, in spite of its high availability in various fields, it is restricted in application to real life [3]. Thus, an appropriate security technique that satisfies the constraints and security requirements for the wireless sensor network. Since Lamport proposed a remote password authentication technique in 1981, various security techniques suitable for the characteristics of the wireless sensor network are researched, but still security vulnerabilities are found [4-10].
Thus, this study would propose a security technique that improved the vulnerabilities to an attacker's attack of impersonation as a user in the security technique proposed by Jung et al. of the user authentication and key agreement protocols based on the symmetric key cryptography.
This study is composed as follows: Chapter 2 discusses the user authentication and key agreement protocol proposed by Jung et al. Chapter 3 discusses the vulnerabilities of the technique proposed by Jung et al. and proposes a method of improving the vulnerabilities. Chapter 4 analyzes the safety of the proposed method, and Chapter 5 draws a conclusion.

2. Related research

2.1. The user authentication and key agreement protocol proposed by Jung et al.

Copyright © 2018 Jae-young Lee. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Chapter 2 discusses the operation principle of the security technique proposed by Jung et al.

The security technique proposed by Jung et al. provides user authentication and key agreement in a wireless sensor network environment consisting of a user, gateway and sensor nodes, which consists of four steps, including registration, login, verification and password change[4]. Table 1 summarizes the notation of the symbols used in the security technique proposed by Jung et al.

Table 1: Notations

Symbol	Description
U_i	Remote User i
S_n	Sensor node n
GW_N	Gateway node
ID_i, PW_i	Identity and password of U_i
SID_n	Identity of S_n
DID_i	Dynamic identity of U_i
k	The symmetric key
E_k, D_k	Encryption/Decryption with k
x_a	The secret parameter generated by GW_N
x_s	The secret key between GWN and S_n
h(xs||SIDn)	The secret key instead of xs, stored in S_n
b	A random number chosen by U_i
R_i	Random numbers
h()	One way hash function
||	Concatenation operation
⊕	XOR operation
T_1, T_2, T_3, T_4	Current timestamp
SK	Session key
ΔT	The maximum of transmission delay time

Registration step

The process of the registration step that begins when a user wants to register in the gateway is as follows:

a) The user generates IDi, password PWi, random number b and calculates the masked password RPWi=h(PWi||b). And the user transmits the IDi, the masked password RPWito the gateway through a safe channel.
b) The gateway calculates v=h(xa) and Ni=h(IDi||RPWi)⊕v, Mi=h(RPWi||v), using the user IDi and the masked password it received and stores v in its DB.
c) The gateway stores {Ni, Mi, h()} for the user on a smart card and transmits the smart card to the user through a safe channel.
d) The user who received the smart card stores random number b in the smart card. SCi={Ni, Mi, h (), b}
e) Login step
f) The login step is carried out when a registered user requests for login to the gateway.
g) The user inserts the smart card in the card reader and enters an IDi and PWi. The smart card calculates RPWi'=h(PWi||b) and v'=Ni⊕h(IDi||RPWi'), using the entered values and calculates Mi'=h(RPWi'||v').
h) The smart card compares the stored Mi and Mi' calculated in 1). If the two values are the same, the user is authenticated, and the next step is carried out. If not, the login step is completed.
i) The smart card chooses the random number R1∈{0,1}, calculates DIDi=h (IDi||R1) and calculates k=h(DIDi||v'||T1) and Ai=Ek (DIDi||R1||T1), using DIDi.
j) The smart card transmits <DIDi, Ai, T1> to the gateway through an open channel.
k) Authentication step

The authentication step is a step to check the legitimacy of a user, gateway and sensor nodes, and they are mutually authenticated by checking all messages transmitted after the user requests for login. The authentication step includes agreement with the session key among all participants in the network. The process of the authentication step is as follows:

1) The gateway checks the current |Ts-T1|<ΔT to judge the legitimacy of Ts. If the condition is met, it carries out the next step, and if not, it refuses all requests and terminates the step.
2) The gateway calculates k'=h(DIDi||h(xa)||T1), using the received value <DIDi, Ai, T1> and xa, carries out Dk(Ai)={DIDi||R1||T1}and compares the received value and the value obtained as a result of the calculation. If the values compared are the same, the gateway authenticates the user and proceeds with the next step, and if not, it terminates the step.
3) The gateway chooses the random number R2∈{0, 1}l, calculates Mi=R2⊕h(xs||SIDn), calculates SK=h(DIDi||h(xs||SIDn)||R2||T2) and Bi=h(DIDi||SK||h(xs||SIDn)||SIDn||T2) and transmits <Mi, DIDi, Bi, T2> to sensor nodes through an open channel.
4) The sensor node first obtains Ts and checks |Ts-T2|<ΔT. If the condition is not met, the step is terminated, and if met, it calculates R2'=Mi⊕h(xs||SIDn) and SK'=h(DIDi||h(xs||SIDn)||R2'||T2). It calculates Bi'=h(DIDi||SK'||h(xs||SIDn)||T2), using the calculated values. It compares the calculated Bi' and the received Bi. If the two values are the same, the sensor node authenticates the gateway, and if not, it terminates the step.
5) The sensor node calculates Ci=h(h(xs||SIDn)||SK||DIDi||SIDn||T3) and transmits <Ci, T3> to the gateway, using the open channel.
6) GWN calculates Di=Ek(DIDi||SIDn||SK||R1||T4) and transmits <Di, T4> to the user's smart card through the open channel.
7) The smart card obtains Ts and checks |Ts-T4|<ΔT. If the condition is not met, it terminates the step. If met, it calculates Dk(Di)={DIDi||SIDn||SK||R1||T4} and compares the previous DIDi and R1. If the compared values are the same, the smart card authenticates the gateway and terminates this step.

Password change step

The password change step is executed when a user would change an old password. In the password change step, the smart card decides to accept the password change without the intervention of the gateway.

1) The user inserts the user's smart card in the card reader and enters an IDi, the current password and a new password. The smart card calculates RPWi'=h (PWi||b) and v'=Ni⊕h(IDi||RPWi') and calculates Mi'=h(RPWi'||v'). Comparing with the stored Mi, if the two values are not the same, it terminates the step, and if the same, it carries out the next step.
2) The smart card calculates RPWinew=h(PWinew||b), Ninew=v'⊕h(IDi||RPWinew) and Minew=h(RPWinew||v').
3) The smart card changes Ni and Mi to Ninew and Minew.
4) The proposed user authentication and key agreement protocol

2.2. Vulnerabilities of the security technique proposed by Jung et al.

The user authentication and key agreement protocol proposed by Jung et al. is vulnerable to an attack in which an attacker disguises as a user. Through various attacks, the attacker obtains the user information and can receive legitimate user authentication, using the obtained information, including the user's smart card, ID and password through the following procedures.

1) The attacker inserts a smart card in the card reader and enters an ID_a and password PW_a. Using the values entered in the smart card, RPW_a' and v' are calculated, and using RPW_a' and v', M_a' is calculated.
2) $RPW_a'=h(PW_a||b)$, $v'=Na\oplus h(ID_a||RPW_a')$, $M_a'=h(RPW_a'||v')$
3) The smart card compares the stored M_a and M_a', the result of the calculation. If the two values are the same, the smart card authenticates the attacker as a legitimate user and carries out the next step. In this step, the attacker stores v'.

4) The attacker chooses the random number $R_1 \in \{0,1\}$l, calculates DID_a and calculates k and A_a, using DID_a.
5) $DID_a=h(ID_a||R_1)$,$k=h(DID_a||v'||T_1)$, $A_a=E_k(DID_a||R_1||T_1)$
6) The attacker transmits <DID_a, A_a, T_1> to the gateway through an open channel.

The gateway that received <DID_a, A_a, T_1>authenticates the attacker as a legitimate user, using the verification step.

1) The gateway obtains the current time stamp T_s to judge the legitimacy of the timestamp and check $|T_s-T_1|<\Delta T$, If the condition is met, it carries out the next step.
2) The gateway calculates k', using the received value <DID_a, A_a, T_1> and its own x_a and carries out $D_k(A_a)$. The received value and the value obtained as a result of the calculation are compared.

$k'=h(DID_a||h(x_a)||T_1)$, $D_k(Aa)=\{DID_a||R_1||T_1\}$

If the compared values are the same, the gateway authenticates the attacker and proceeds with the next step.

3.2 The proposed user authentication and key agreement protocol

This chapter proposes a security technique that improved the problems of the user authentication and key agreement protocol proposed by Jung et al. The proposed method is a method of adding and allowing to use a variable that records the times of the user's request for registration to the gateway in the registration step. The variable that records the times of requests for registration is a value that increases by 1 whenever the user requests registration to the gateway, which is stored and managed separately by the user and the gateway, not transmitted in any steps of the user authentication and key agreement protocol.

The registration step and the login step of the proposed technique are as follows:

Registration step

A user generates an ID_i, password $PW_i$and random number b, generates and stores U_{ni}, a variable that records the times of requests for registration. If it is the first request for registration in the gateway, the value of the variable is initialized as 0, and whenever the user requests registration in the gateway, the value of the variable increases by 1. The gateway, too, generates G_{ni}, a variable that records the times of the user's request for registration, manages and stores it in the same way.

1) The user generates the masked password RPW_i, using password and random number b, changes and stores the value of Uni. ID_i and RPW_i are transmitted to the gateway through a safe channel.

$RPW_i=h(PW_i||b)$.

2) The gateway changes the value of G_{ni} and calculates v, N_i and M_i, using x_a and G_{ni}. It stores v and G_{ni} in the database.

$v=h(x_a)$, $N_i=h\ (ID_i||RPW_i||G_{ni})\oplus v$, $M_i=h(RPW_i||v)$

The gateway stores $\{N_i, M_i, h\ ()\}$ in the user's smart card and transmits the smart card to the user through the safe channel.

3) The user that received the smart card additionally stores the random number b on the smart card.

$SC_i=\{N_i, M_i, h(), b\}$

Login step

A user begins the login step, inserting a smart card in the card reader.

1) The user enters ID_i, password $PW_i$and U_{ni}. The smart card calculates RPW_i' and v' and calculates M_i', using RPW_i' and v'.

$RPW_i'=h(PW_i||b)$, $v'=Ni\oplus h(ID_i||RPW_i'||U_{ni})$, $M_i'=h(RPW_i'||v')$

The smart card compares the stored M_i and M_i' as a result of the calculation. If the two values are the same, the smart card authenticates the user and proceeds with the next procedure. And if not, it terminates the login step.

2) The smart card chooses the random number $R_1 \in \{0,1\}$l, calculates DID_i and calculates k and A_i, using DID_i.

$DID_i=h(ID_i||R_1)$, $k=h(DID_i||v'||T_1)$, $A_i=E_k(DID_i||R_1||T_1)$

3) The smart card transmits <DID_i, A_i, T_1> to the gateway through the open channel.

The technique proposed in this study consists of four steps, including registration step, the login step, the authentication step and password change step like the security technique proposed by Jung et al., but the authentication step and password step are omitted since they are the same as the existing method proposed by Jung et al.

3. Safety analysis

In Chapter 4, safety is analyzed by presenting how the technique proposed in this study copes with an attack in which an attacker disguises as a user.

In the proposed security technique, the user should have a smart card, transmitted from the gateway, the user ID, password and U_n, the user's variable that recorded the times of the user's request for registration in the gateway in order to start the login step.

The attacker obtains the user information such as the user's smart card, ID and password through various attacks such as smartcard loss attack, ID-guessing attack and password-guessing attack. However, U_n, the variable that recorded the times of the user's request for registration to the gateway is a value, not transmitted in any steps, stored and managed separately by the user and the gateway, which is not disclosed to a third party.

The process in which an attacker proceeds with the login step is as follows:

1) The attacker inserts a random user's smart card in the card reader, where $\{N_b, M_b, h(), b\}$ are stored and enters the user ID_b, password PW_b and the guessed U_{nb}.
2) The smart card calculates $RPW_b'=h\ (PW_b||b)$, using the entered password and b stored in the smart card and calculates $v'=N_b\oplus h(ID_b||RPW_b'||U_{nb})$, using N_b, stored in the smart card, RPW_b' the result of the calculation and the entered U_{nb}. And it calculates $M_b'= h(RPW_b'||v')$, using RPW_b' and v'.
3) The smart card compares the calculated M_b' and the stored M_b and check if the two values are the same.

Mb stored on the smart card is a value calculated, using the variable that recorded the times of the user's request for registration to the gateway managed by the gateway. M_b' calculated with the guessed U_{nb} cannot be the same as M_b stored on the smart card, and if M_b stored in the smart card is not the same as the calculated M_b', the user that requested the login step cannot be authenticated.

The technique proposed in this study, which uses the variable that records the times of requests for registration stored and managed only by the user and the gateway in the step in the user's registration in the gateway in the formula and allows the user to use this again in the login step is safe from an attacker's attack of impersonation as a user.

4. Conclusion

In the user authentication and key agreement protocol, consisting of four steps, proposed by Jung et al., a user who completed the registration step is issued a smart card from the gateway and get certified as a legitimate user in the phase of login with the issued smart card. However, the user authentication made using the information stored in the smart card, ID and password may be exposed to the attacker's an attack of impersonation as a user if the information is disclosed by smart-card loss attack, ID-guessing attack or password-guessing attack.

Thus, this study proposed the use of the variable that recorded the times of the user's request for registration to the gateway in the registration step to supplement the user authentication and key agreement protocol proposed by Jung et al. and the use of the variable in the user authentication in the login step. The variable that recorded the times of the user's request for registration to the gateway is a value that only the user and the gateway store and manage, which is a variable that a third party cannot know, not transmitted in any steps. The attacker who does not know the variable that recorded the times of the user's request for registration cannot receive user authentication in the login step using the information even if the attacker obtained the random user information through smart-card loss attack, ID-guessing attack or password-guessing attack. Thus, the technique proposed in this study can cope with the attacker's an attack of impersonation as a user.

References

[1] Sungkon P.An Efficient Key management for Wireless Sensor Network.Journal of Digital Contents Society. 2012, 13(1), pp.129-139.

[2] Sensor Network Security Technology. http://terms.naver.com/entry.nhn?docId=3435129&cid=58462&categoryId=58462

[3] Deukhun K, Jin K.Design of Improved Authentication Protocol for Sensor Networks in IoT Environment.Journal of the Korea Institute of Information Security and Cryptology. 2015, 25(2), pp.467-478.

[4] Haewon C, Hyunsung K.Impersonation Attacks on Anonymous User Authentication and Key Agreement Scheme in Wireless Sensor Networks.Journal of Digital Convergence. 2016, 14(10), pp.287-293.

[5] Yiroo B, Kwangeun G, Jaecheol H.A Remote Authentication Protocol Using Smartcard to Guarantee User Anonymity.Journal of Korean Society for Internet Information. 2009, 10(6), pp. 229-239.

[6] Hyunsung K. Remote User Authentication Scheme with Key Agreement Providing Forward Secrecy. Journal of Security Engineering. 2015, 12(1), pp.1-12.

[7] Eunjun Y, Haejung K. Secure Anonymous Remote User Mutual Authentication and Key Agreement Protocol. The Institute of Electronics Engineers of Korea. 2012. pp.1918-1921.

[8] Miog P. Weaknesses Cryptanalysis of Khan's Scheme and Improved Authentication Scheme preserving User Anonymity. The Korean Society of Computer and Information. 2013, 18(2), pp.87-94.

[9] Sungyup L, Kisung P, Yohan P, Youngho P. Symmetric Key-Based Remote User Authentication Scheme With Forward Secrecy. Journal of Korea Multimedia Society. 2016, 19(3), pp.585-594.

[10] Jongho M, Dongho W. An Enhanced Symmetric Key-Based Remote User Authentication Scheme with Forward Secrecy.Journal of Korea Multimedia Society. 2017, 20(3), pp.500-510.