Cryptanalysis of a strong authentication scheme with user privacy for wireless sensor networks

Chengbo Xu

School of Mathematical Sciences, University of Jinan, Jinan 250022,
Shandong Province, P. R. China
E-mail: cbqysy@163.com

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

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 a strong authentication scheme with user privacy for WSNs proposed by Kumar et al. in 2013, and point out the scheme can not resist known session key attack, impersonation attack, sensor node capture attack and suffer from forward security problem, anonymity and untraceability problem.

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 2007, Das [1] proposed a two-factor authentication scheme using smart card in which users are authenticated by gateway nodes. The scheme became a center of attraction for many researchers [2-6] working in this field. 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. Later on, the improved scheme was pointed out that it does not realize mutual authentication and user's anonimity, and lacks a mechanism of establishing a session key. [7] Based on this, Yoo et al. proposed a new scheme in 2012. However, Kumar at al. [8] pointed out that Yoo et al.'s scheme does not resist impersonation attack and man-in-the-middle attack, and further proposed an improved scheme.

In this paper, we will point out that Kumar et al.'s scheme [8] does not resist known session key attack, impersonation attack, sensor node capture attack and suffer from forward security problem, anonymity and untraceability problem.

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

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

Review of Kumar et al.'s scheme

In this section, we briefly review the Kumar et al.'s scheme [8]. Their scheme includes three phases: registration phase, authentication phase and password-change phase; and involves three entities: users, gate-way node (GW) and sensor nodes.

Table 1. Notations

ID_k, PW_k	The identity and password of user U_k
GW_{id}, Sn_{id}	The identities of the gate-way node and sensor node
J and X	GW secret numbers (that is, 256 bits)
b	User random number
$E_x[], D_x[]$	Symmetric encryption and decryption using key x
$h(\cdot)$	A secure one-way hash function
$\oplus$	The bitwise exclusive-or operation
II	Message concatenation operation

Registration phase To begin with, User U_k select his/her identity ID_k and password PW_k freely, and then generates a random number b. In addition, GW and sensor nodes are supposed to share a long-term secret key $LT_{key} = h(GW_{id} \| Sn_{id} \| h(Y))$, where Y is a high entropy secret number generated and maintained by GW. The following steps are:

Step 1: User U_k passes his/her identity ID_k and $h(b \oplus PW_k)$ to the gate-way node(GW).

Step 2: Upon receiving the message, GW computes $A_k = E_J[ID_k \| GW_{id} \| h(X)]$ and $B_k = h(ID_k \| h(b \oplus PW_k) \oplus A_k)$, where the secret number J and X are respectively with a lifetime (such as one year).

Step 3: GW stores A_k, B_k, $h(\cdot)$ and $h(X)$ into a smart card and issues this card to U_k through an security channel.

Step 4: Upon receiving the card, U_k stores the random number b into it such that the number need not be remembered.

Eventually, smart card has the following: A_k, B_k, $h(\cdot)$, $h(X)$ and b.

Authentication Phase In Kumar et al.'s scheme, authentication phase is further divided into two subphases: Login phase and verification phase.

Login Phase: When the user U_k wants to acquire relative data from some sensor node, he/she inserts his/her smart card into a card reader and then keys in his/her identity ID_k and password PW_k.

Step 1: The smart card computes $\mathrm{B}_k^* = h(ID_k \| h(b \oplus PW_k) \oplus A_k)$, and then checks whether B_k^* and B_k are equal. If they are not equal, terminate the scheme; otherwise, conduct the following steps.

Step 2: Generates a random number C_k, computes a temporary key $\mathrm{M{=}h(h(X) \| ID_k \| T')}$, and then use the temporary key to encrypt information $h(ID_k) \| h(X) \| C_k \| T'$, that is $\mathrm{P}_k = E_M(h(ID_k) \| h(X) \| C_k \| T')$, where $\mathrm{T'}$ is user's current timestamp.

Step 3: The smart card sends the login message $<P_k, A_k, T'>$ to gate-way node GW.

Verification Phase: Upon receiving the login request message $<P_k, A_k, T'>$, GW will conduct the following steps to verify the validity of user U_k.

Step 1: Checks the inequality $(T'' - T') > \Delta T$. If yes, terminates; otherwise, proceeds to the next step, where $\mathrm{T''}$ is the current timestamp, $\Delta\mathrm{T}$ is an expected time interval for the message transmission delay.

Step 2: Decrypts $\mathrm{A_k}$ with the GW's secret number J, and obtains ID_k', $\mathrm{GW_{id}}'$ and $h(X)'$.

Step 3: Computes $\mathrm{M}{=}h(h(X) \| ID_k' \| T')$, and then decrypts P_k and obtains $h(ID_k)^*$, $h(X)^*$, C_k.

Step 4: Checks $\mathrm{T'}^* = T'$. If they are not equal, terminates; otherwise, conducts the following steps.

Step 5: Computes $h(ID_k')$ and checks $h(ID_k)^* = h(ID_k')$, $GW_{id} = GW_{id}'$, $h(X)^* = h(X)'$. If the three equations are all correct, the validity of user U_k is verified by GW; otherwise, terminate the scheme.

Step 6: Computes $SID_k = E_{LT_{key}}[h(ID_k') \| GW_{id} \| C_k \| h(X)' \| Sn \| T'']$, where T" is the current timestamp. Then, GW sends message $< SID_k, T'' >$ to the wireless sensor node Sn.

Step 7: Upon receiving the message $< SID_k, T'' >$, the sensor node checks the inequality $(T''' - T'') > \Delta T$. If yes, terminate the scheme; otherwise, conduct the following steps, where T''' is the current timestamp, ΔT is an expected time interval for the message transmission delay.

Step 8: The sensor node Sn uses its long-term key LT_{key} to decrypt message SID_k and obtains $h(ID_k')^*$, $GW_{id}{}^*$, $C_k{}^*$, $h(X)'^*$, Sn^* and T''^*.

Step 9: Checks $T''^* = T''$, $GW_{id}{}^* = GW_{id}$ and $Sn^* = Sn$. If the three equations are all correct, the validity of user U_k and GW is verified by Sn; otherwise, terminate the scheme.

Step 10: The sensor node Sn computes session key $S_{key} = h(h(ID_k')^* \| C_k{}^* \| h(X)'^* \| Sn \| T'''')$, where T'''' is the current timestamp of the sensor node Sn.

Step 11: Computes $N_k = E_{S_{key}}[Sn \| C_k \| h(X)'^* \| T'''']$, and then sends message $< N_k, Sn, T'''' >$ to U_k.

Step 12: Upon receiving the message $< N_k, Sn, T'''' >$, the sensor node checks the inequality $(T^* - T'''') > \Delta T$. If yes, terminate the scheme; otherwise, conduct the following steps, where T* is the current timestamp, ΔT is an expected time interval for the message transmission delay.

Step 13: User U_k computes session key $S_{key} = h(h(ID_k) \| C_k \| h(X) \| Sn \| T'''')$, and then uses the session key S_{key} to decrypt message N_k and obtains Sn^*, $C_k{}^*$, $h(X)'^{**}$ and T''''^*. Finally, U_k checks the following equations $T''''^* = T''''$, $Sn^* = Sn$, $C_k{}^* = C_k$ and $h(X)'^{**} = h(X)$. If the four equations are all correct, the validity of the sensor node Sn is verified by U_k; otherwise, terminate the scheme.

Weaknesses of Kumar et al.'s scheme

In this section, we will show that Kumar et al.'s scheme [8] does not implement forward security and user's untraceability, and is also vulnerable to known session key attack and node capture attack.

Known session key attack According to the process of Kumar et al.'s scheme, attacker A can easily eavesdrop the login request message $< P_k, A_k, T' >$ which user U_k sends to the gate-way node GW and the verification message $< N_k, Sn, T'''' >$ which the sensor node Sn sends to user U_k. Suppose a session key S_{key} is acquired by attacker A in some way. Then, the attacker can uses the session key S_{key} to decrypt the data N_k in the message $< N_k, Sn, T'''' >$ and obtains Sn, C_k, h(X) and T''''. Based on these information, the attacker A can off-line guess user U_k's identity ID_k. The concrete steps are as follows:

a) Attacker A guesses a possible identity ID_k';

b) Computes $M' = h(h(X) \| ID_k' \| T')$, where $h(X)$ and T' have been obtained.

c) Computes $P_k' = E_{M'}[h(ID_k') \| h(X) \| C_k \| T']$;

d) Attacker A checks whether P_k' and P_k are equal. If they are equal, it means the guessed ID_k' is equal to the actual identity ID_k and the attacker succeeds; otherwise, repeat the steps a)-d) until guess succeeds.

Once attacker obtains the identity ID_k, he/she can further implement the following two types of attackers.

Impersonation attack

a) Attacker A extracts the current timestamp T_a, and generates a random number C_k' simultaneously.

b) Computes $\mathrm{M} = h(h(X) \| ID_k \| T_a)$, where $\mathrm{h}(X)$ has been already obtained.

c) Computes $\mathrm{P}_k = E_k[h(ID_k) \| h(X) \| C_k' \| T_a]$, where ID_k has been obtained from offline guess.

d) Attacker A sends the constructed login request message $< P_k, A_k, T_a >$ to GW. Then, the login request message will pass the verification from GW and Sn, and a session key $S_{key} = h(h(ID_k) \| C_k' \| h(X) \| Sn \| T_a'''')$ will be agreed in the end, where T_a''' is the corresponded timestamp generated by the sensor node Sn.

Forward security problem Forward security problem means that once attacker obtains a session key in some way, he/she will restore some previous session keys using the known session 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 Kumar et al.'s scheme, suppose attacker eavesdrops the mutual information $< P_{k-0ld}, A_{k-old}, T_{old}' >$ and $< N_{k-old}, Sn_{old}, T_{old}''' >$ in the authentication phase of some previous session, the attacker can restore the session key as follows:

a) Computes $M_{old} = h(h(X) \| ID_k \| T_{old}')$, where $h(X)$ and ID_k have been obtained previously.

b) Uses M_{old} to decrypt P_{k-old} and obtains C_{k-old}.

c) Computes $S_{key-old} = h(h(ID_k) \| C_{k-old} \| h(X) \| Sn_{old} \| T_{old}''')$, where Sn_{old} and T_{old}''' are from the eavesdropped message $< N_{k-old}, Sn_{old}, T_{old}''' >$. Obviously, the obtained $S_{key-old}$ is the actual key applied into that session.

Sensor node capture attack Generally, any identity authentication and session key agreement scheme for wireless sensor network would encounter sensor node capture attack. In this case, how to measure the degree of an authentication scheme's resistance to sensor node capture attack? That is, how to campare the security performance of different schemes in the sense of sensor node which may be captured.

In 2012, Ashok Kumar Das et al. [9] proposed a method of measuring. In the assumption that there are c nodes have been captured successfully, they define the ratio between the number of captured sessions and that of the total sessions as the toughness of an authentication scheme's resistance to sensor node capture attack. For a specific scheme, the value of toughness is between 0 and 1, and as small as possible. A scheme would be uncounditional security to resist sensor node capture attack if you could prove the value of toughness is 0. The basic idea of this method is quantitative analysis that the c caputured nodes effects on all other nodes in this wireless sensor network. Though the value of toughness in this definition would be very difficult to calculate in practice, it took the first step after all in the problem that how to measure the degree of an authentication scheme's resistance to sensor node capture attack.

In terms of Kumar et al.'s scheme, suppose that some sensor node S_n has been captured, the attacker is able to extract data $LTkey$ stored in node S_n. Once $LTkey$ is known, attacker can obtain $h(ID_k)$, C_k, $h(X)$ and S_n from SID_k stored in $< SID_k, T'' >$ which was sended from gateway node to sensor node. Further, attacker can restore the session key $S_{key} = h(h(ID_k) \| C_k \| h(X) \| S_n \| T''')$ from the eavesdropped message $< N_k, S_n, T''' >$. For sessions between user U_k and other nodes (such as S_m), as long as eavesdrop the login request message $< P_k, A_k, T' >$ and the verification message $< N_k, S_m, T''' >$ sended from S_m to user U_k, an attacker is able to obtain the session key as follows:

1) Guess ID_k offline using $h(ID_k)$;

2) Compute $M = h(h(X) \| ID_k \| T')$;

3) Obtain C_k through decrypting P_k using M;

4) So far, all the information needed to compute the session key has been known, compute $S_{key} = h(h(ID_k) \| C_k \| h(X) \| S_m \| T''')$.

Through above analysis, it is easy to find that for Kumar et al.'s scheme, once one sensor node is captured, the data transferred between user and any other sensor node will be obtained since attacker would compute the session key. According to the definition of toughness in [9], it is not difficult to know the value of toughness to resist to sensor node captured attack is 1. In other words, whole the sensor network would have no secure data communication as long as some sensor node has been captured.

Anonymity and untraceability problem In [8], Kumar et al. indicated that their scheme has realized user anonymity. The reason is that an attacker could not obtain the real identity ID_k of user U_k from the login request message $<P_k, A_k, T'>$ intercepted or eavesdropped, since A_k is encrypted by the advanced secret key J of gateway GW, P_k is encrypted by M which is difficult to compute. If we don't consider that attacker could be beyond the ability to control the communication channel, the analysis of Kumar et al. is correct. However, it is a common case in reality to capture sensor nodes or steal user's smart card and extract the information stored. According to the former analysis, it is not difficult to know that several methods can be used to obtain user's identity in this case.

When it comes to user's untraceability, for Kumar et al.'s scheme [8], even if the ability beyond that to control the communication channel is not took into consideration, an attacker can also easily judge whether two users are the same from the login request message eavesdropped. The reason is that the data A_k in the login request message $<P_k, A_k, T'>$ is not changed along with the different of the session, which is decided by the identity of the user itself. Thus, when attacker intercepted or eavesdropped two or more login request messages $<P_k, A_k, T'>$, he/she can recognize whether the two or more users is the same by comparing the data of A_k in $<P_k, A_k, T'>$. The same A_k implies the same user, different A_k means different users.

Conclusions

In this paper, we analyze a strong authentication scheme with user privacy for WSNs proposed by Kumar et al. in 2013, and point out the scheme can not resist known session key attack, impersonation attack, sensor node capture attack and suffer from forward security problem, anonymity and untraceability problem.

Acknowledgements

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

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] S. G. Yoo, K. Y. Park, J. Kim. A security-performance-balanced user authentication scheme for wireless sensor networks. Journal of Distributed Sensor Networks, 2012, Article ID 382810.

[8] 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.

[9] A. K. Das, P. Sharma, S. Chatterjee, et al.. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. Journal of Network and Computer Applications, 2012, 35(5): 1646-1656.