International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

AN IMPROVED AUTHENTICATION SCHEME WITH USER PRIVACY FOR WSNS

Chengbo Xu, School of Mathematical Sciences, University of Jinan, Jinan 250022, Shandong Province, China

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 for WSNs is still quite a challenging problem. In 2013, Kumar et al. proposed an authentication scheme for WSNs. Unfortunately, the scheme was pointed out not to resist known session key attack, impersonation attack and sensor node capture attack by Xu in 2016. In order to conquer these problems, an improved scheme has been proposed in this paper. Through security analysis, we further show that the new scheme does resist those attacks and also has some other properties of security.

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, a two-factor authentication scheme using smart card was proposed by Das [1] 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. Unfortunately, Kumar et al.'s scheme has been pointed out not to resist known session key attack, impersonation attack and sensor node capture attack by Xu in 2016 [10].

In this paper, we will propose an improved authentication scheme with user privacy for WSNs based on Kumar et al.'s shceme [8] in order to conquer those problems pointed out by Xu [10]. Further, through security analysis, we have shown that the proposed scheme does resist those attacks and also has some other properties of security..

The rest of this paper is organized as follows: in section 2, we will propose our improved scheme. Section 3 analyzes the security performance of the proposed scheme. Finally, we draw our conclusion in section 4.

Our Proposed Scheme

In this section, we will propose an improved identity authentication and key agreement scheme, which implements the property of user untracebility. The new scheme is based on Kumar et al.'s scheme. However, it conquers the security flaws of Kumar et al.'s scheme and remains its merits. Our scheme involves three typies of entities: users (U_k), gateway node (GW), sensor nodes (Sn); and consists of four phases: registration phase, Login phase, authentication phase, and password update phase. To begin with, the gateway node GW and sensor nodes Sn 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 notations used throughout this paper are summarized in Table 1.

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
X	GW secret number
b	User random number
$E_x[], D_x[]$	Symmetric encryption and decryption
$h(\cdot)$	A secure one-way hash function
$\oplus$	The bitwise exclusive-or operation
$\|\|$	Message concatenation operation

A. Registration Phase

When user U_k wants to become a legitimate user of wireless sensor networks and obtain the service provided by the network, U_k and GW conducts the following steps.

Step 1: User U_k selects its identity ID_k and password PW_k freely, generates a random number b, and then computes $R_k = h(PW_k \oplus b)$. Eventrually, U_k sends $< ID_k, R_k >$ to GW through a secure channel.

Step 2: When receiving the message $< ID_k, R_k >$, the gateway node GW computes $A_k = E_X[ID_k \| GW_{id} \| h(X)]$ and $B_k = h(ID_k \| A_k \| R_k)$, stores the information A_k, B_k, $h(X)$ and $h(\cdot)$ into a smart card, and then sends the card to user U_k through a secure channel.

Step 3: Upon receiving the smart card from GW, user U_k stores the random number b into the card. As such, the smart card contains $< A_k, B_k, h(X), h(\cdot), b >$.

B. Login Phase

When user U_k wants to obtain data from some sensor node, he/she has to finish the following steps.

Step 1: User U_k inserts his/her smart card into a card reader, and then inputs his/her identity ID_k and password PW_k.

Step 2: The smart card checks the format of ID_k and PW_k inputted. If the format is invalid, it will output reminder information and require the user to enter again; otherwise, it will conduct the following steps.

Step 3: The smart card computes $R_k = h(PW_k \oplus b)$ and $B_k^* = h(ID_k \| A_k \| R_k)$, and checks whether B_k^* and B_k are equal. If they are unequal, it means ID_k or PW_k inputted are not valid. The card will reject the login request; otherwise, it will continue the following steps.

Step 4: The smart card generates two random numbers C_k and W_k, and computes $M = h(h(X) \| ID_k \| T')$, $F_k = h(X) \oplus W_k$, $G_k = E_{h(X)}[A_k \| T']$ and $P_k = E_M[h(ID_k \oplus W_k) \| F_k \| C_k \quad \| T']$, where T' is the current timestamp.

Step 5: The smart card transmits the login request message $< P_k, G_k, T' >$ to the gateway node GW.

C. Auhentication Phase

When receiving the login request message $< P_k, G_k, T' >$, the gateway node GW will verify the validity of user U_k through the following steps.

Step 1: The gateway node GW verifies $T'' - T' > \Delta T$, where T'' is the current timestamp and ΔT is the expected transmision delay. If the inequality is correct, GW rejects the login request; otherwise, GW conducts the following steps.

Step 2: GW computes $h(X)$ and uses it to decrypt the values G_k in $< P_k, G_k, T' >$. As such, GW will obtain A_k and $T'*$. Further, the gateway node GW compares $T'*$ and T'. If they are equal, GW conducts the following steps; otherwise, terminates the scheme.

Step 3: GW decrypts A_k using it's master key and obtains $ID_k^{'}$, $GW_{id}^{'}$, $h(X)'$. Then, GW checks $GW_{id}^{'} = GW_{id}$ and $h(X)' = h(X)$. If these two qualities are all correct, GW conducts the following steps; otherwise, terminates the scheme.

Step 4: GW computes $M' = h(h(X) \| ID_k^{'} \| T')$ and uses it to decrypt P_k. As such, the values $h(ID_k \oplus W_k)^*$, F_k^* and $C_k^{'}$ are obtained. Further, GW computes $W_k^* = F_k^* \oplus h(X)$, and compares $h(ID_k^{'} \oplus W_k^*)$ and $h(ID_k \oplus W_k)*$. If they are unequal, terminates the scheme; otherwise, continues the following steps. So far, GW completes the process of verifying user U_k and confirms that the user U_k is a legal one.

Step 5: GW computes $SID_k = E_{LTkey}[h(ID_k \oplus W_k)* \| GW_{id} \| C_k^{'} \| F_k^* \| Sn \| T'']$, where T'' is the current timestamp. Then, GW sends the message $< SID_k, T'' >$ to the nearest sensor node Sn.

Step 6: When receiving $< SID_k, T'' >$, sensor node Sn checks $T''' - T'' > \Delta T$, where T''' is the current timestamp and ΔT is the expected transmision delay. If the inequality is correct, terminates the scheme; otherwise, continues.

Step 7: The sensor node Sn decrypts SID_k using it's long-term key LT_{key}, and obtains $h(ID_k \oplus W_k)*$, $GW_{id}*$, C_k*, F_k**, $Sn*$ and $T''*$.

Step 8: The sensor node Sn checks $T''* = T''$, $GW_{id}* = GW_{id}$ and $Sn* = Sn$. If these three qualities are all correct, the sensor node confirms that the gateway GW and

ISSN:2319-7900

the user U_k are both legal, and continues; otherwise, terminates the scheme.

Step 9: The sensor node computes the session key $S_{key} = h(h(ID_k \oplus W_k)^* \| C_k^* \| F_k^{**} \| Sn \| T''')$, where T''' is the current timestamp.

Step 10: The sensor node computes $N_k = E_{(S_{key} \oplus C_k^*)}[Sn \| C_k \| F_k^{**} \| T''']$, and then sends the message $< N_k, Sn, T''' >$ to user U_k.

Step 11: Upon receiving $< N_k, Sn, T''' >$, the user U_k verifies $T^* - T''' > \Delta T$, where T^* is the current timestamp and ΔT is the expected transmision delay. If it is correct, terminates the scheme; otherwise, continues the following steps.

Step 12: The user U_k computes the session key $S_{key} = h(h(ID_k \oplus W_k) \| C_k \| F_k \| Sn \| T''')$. Then, U_k uses $S_{key} \oplus C_k$ to decrypt N_k and obtains Sn^*, C_k^*, F_k^{***} and T'''^*. Further, U_k checks $T'''^* = T'''$, $Sn^* = Sn$ and $C_k^* = C_k$. If these three equalities are all correct, it means that the sensor node is legal; otherwise, terminates the scheme.

D. Password Update Phase

When a legal user wants to update his/her current passowrd, he/she needs to conduct the following steps.

Step 1: User U_k inserts his/her smart card into a card reader, and then inputs his/her identity ID_k and password PW_k.

Step 2: The smart card computes $R_k = h(PW_k \oplus b)$ and $B_k^* = h(ID_k \| A_k \| R_k)$, and checks whether B_k^* and B_k are equal. If they are unequal, it means ID_k or PW_k inputted are not valid. The card will reject the password update request; otherwise, it will continue the following steps.

Step 3: User U_k selects a new password PW_{knew}, generates a random number b_{new}, and then computes $R_{knew} = h(PW_{knew} \oplus b_{new})$ and $B_{new} = h(ID_k \| A_k \| R_{knew})$.

Step 4: The smart card substitutes B_k and b with B_{knew} and b_{new} seperately.

Security Analysis

In this section, we will analyse security performance of our proposed scheme. And we also compare our scheme with Kumar et al.'s schemes.

A. Resist Known Session Key Attack

In Kumar et al.'s scheme [8], once one session key S_{key} has been leaked to an attacker, the attacker can use this session key to decrypt information N_k in the messge $< N_k, Sn, T''' >$ which was eavesdropped. And consequently, the attacker obtains Sn, C_k, $h(X)$ and T''' which can be used to attack the scheme. As such, Kumar et al.'s scheme could not resist to known session key attack. In our scheme, we avoid using just negotiated session key to encrypt important message in the identification authentication phase. That is to say, the session key itself agreed in the identification authentication and key agreement phase is only used to encrypt/decrypt the messages exchanged in the following session. Concretely, we use $S_{key} \oplus C_k$ to encrypt the important information Sn, C_k, F_k^{**} and T''' which are used to authenticate sensor node Sn for user U_k, and then obtain N_k. In this way, even if the attacker get the session key S_{key}, he/she still cannot decrypt the value N_k which encapsulates a lot of important information since the random number C_k are unknown. Therefore, the proposed scheme can resist known session key attack and also meet the forward security.

B. User Anonimity and Untraceability

In the proposed scheme, the identification ID_k of user U_k is transmitted secretly, and only the gateway node GW can decrypt the message A_k using master key X. Even if the attacker extracts the information $h(X)$ stored in smart card, he/she only can decrypt G_k and obtain value A_k, but cannot furtherly decrypt A_k to get the identification ID_k of user U_k, since the master key X is unknown. As such, the proposed scheme meets user anonimity.

In Kumar et al.'s scheme [8], the value A_k in the login request message $< P_k, A_k, T' >$ does not vary with the sessions. As long as it is the same user, the value A_k will be the same. According to this, the attacker can trace a user. In our proposed scheme, we substitute A_k with $G_k = E_{h(x)}[A_k \| T']$ which varies with the sessions. In this way, the proposed scheme meets the property of untraceability.

C. Resist Sensor Node Capture Attack

Once a sensor node is captured, the long term key $LTkey$ stored in it is supposed to be extracted generally since the

ISSN:2319-7900

computing power and storage capacity of a sensor node is very limited. If the message $<SID_k, T''>$ was also intercepted, the attacker can use the long term key $LTkey$ to decrypt the information SID_k which is used to verify user and gateway node for sensor node, and obtain $h(ID_k \oplus W_k)*$, $GW_{id}*$, C_k*, F_k*, $Sn*$ and $T''*$. For Kumar et al.'s scheme, the attacker will get $h(ID_k^{'})*$, $GW_{id}*$, C_k*, $h(X)'*$, $Sn*$ and $T''*$. By these information, the attacker can guess the user's identification ID_k, compute M and further construct a legal login request message P_k. In the proposed scheme, we substitute $h(ID_k^{'})*$ with $h(ID_k \oplus W_k)*$, and $h(X)'*$ with $F_k* = h(X) \oplus W_k$, where W_k is a random number generated in the login phase by user U_k. Since the random number W_k is not transmitted online, the attacker has no ways to guess ID_k and construct login request message. Therefore, the proposed scheme can resist sensor node capture attack.

D. Resist Replay Attack

In the proposed scheme, suppose that an attacker has intercepted or eavesdropped a login request message $<P_k, G_k, T'>$ of user U_k in some session, the attacker tries to replay this message in order to cheat the gateway node GW. When receiving the message $<P_k, G_k, T'>$, GW extracts its current timestamp T'' and checks $|T''-T'| > \Delta T$ firstly. Obviously, the inequality is correct since the message $<P_k, G_k, T'>$ was replayed. Then, GW will terminate the scheme. Therefore, the attacker fails to cheat GW. Maybe the attacker is more clever. He/She does not replay the message $<P_k, G_k, T'>$ directly. Instead, the attacker replaces T' with the current timestamp $T*$, and then sends the modified message $<P_k, G_k, T*>$ to GW. Even so, the attacker is not successful. The reason is that GW will compute $M' = h(h(X) \| ID_k^{'} \| T*)$, and use it to decrypt P_k which was encrypted by $M = h(h(X) \| ID_k^{'} \| T')$, then checks the outputs. The attacker will fail in the process of checking since M' and M are unequal.

Suppose that the attacker has intercepted or eavesdropped the message $<SID_k, T''>$ transmitted from the gateway node GW to sensor node Sn, and will replay this message to deceive the sensor node Sn. This type of replay attack will still not succeed since the sensor node firstly checks the inequality $T''' - T'' > \Delta T$ when receiving the message $<SID_k, T''>$. Obviously, it is correct, so the sensor node will stop the scheme immediately. Even though the attacker replaces the timestamp T'' with the current timestamp $T*$ and then sends the modified message $<SID_k, T*>$ to Sn, he/she still can not succeed. The reason is that the timestamp T'' is still placed in the information $SID_k = E_{LTkey}[h(ID_k \oplus W_k)* \| GW_{id} \| C_k^{'} \| F_k^{*} \| Sn \| T'']$ which will be decrypted by sensor node Sn to get T'', and Sn will further check whether T'' and $T*$ are equal. Obviously, they are different. Therefore, this type of replay attack will fail.

Suppose that the attacker has intercepted or eavesdropped the message $<N_k, Sn, T'''>$ transmitted from the sensor node Sn to the user U_k, and will replay this message directly or send the modified message in which the timestamp T''' was replaced by the current timestamp $T*$. Based on an analysis similar to the above, the attack will still not succeed.

So far, we have analyzed all of the possible replay attacks. The fact is that all of them will fail. Therefore, the proposed scheme can resist replay attacks.

E. Resist Impersonating User Attack

The simplist way to conduct a impersonating user attack is that the attacker intercepts or eavesdrops a login request message $<P_k, G_k, T'>$ of user U_k in some session, and then tries to replay this message in order to cheat the gateway node GW. According to above analysis, this way doesn't work.

Another way to impersonate user is that the attacker intercepts or eavesdrops a login request message $<P_k, G_k, T'>$, the validation message $<SID_k, T''>$ transmitted from the gateway node GW to sensor node Sn, and the validation message $<N_k, Sn, T'''>$ transmitted from the sensor node Sn to the user U_k, and then tries to forge a login request message $<P_k*, G_k*, T*>$ which can be authenticated. Since both $P_k = E_M[h(ID_k \oplus W_k) \| F_k \| C_k \| T']$ and $G_k = E_{h(X)}[A_k \| T']$ are messages encrypted, and the keys $M = h(h(X) \| ID_k \| T')$ and $h(X)$ are both unknown to the attacker, this way still doesn't work.

F. Achieve the Mutual Authentication

When receiving the login request message $<P_k, G_k, T'>$ generated by user U_k, the gateway node will authenticate the user comprehensively through the first four steps in the

ISSN:2319-7900

authentication phase. After the gateway node confirmed the legitimacy of the user, it will generate message $< SID_k, T" >$ and send it to a sensor node. Apon receiving the message $< SID_k, T" >$, the sensor node will verify it through conducting step 6 to step 8 in the authentication phase. If there is no problem, it means that the sensor node has confirmed the legitimacy of the gateway node and the user. Then, the sensor node will generate message $< N_k, Sn, T''' >$ and send it to the user. When receiving the message, the user will authenticate the sensor node through the last two steps in the authentication phase. As such, it is easy to know that the mutual authentication is achieved between the user and the sensor node.

Table 2. The Comparison of Security Performance

Security	[2]	[7]	[11]	[12]	[8]	new
Anonymity	No	No	No	No	Yes	Yes
Mutual	No	No	No	No	Yes	Yes
Session Key	No	No	No	No	Yes	Yes
PW Update	Yes	Yes	No	Yes	Yes	Yes
Impersonate	No	No	No	No	Yes	Yes
Untraceable	No	No	No	No	No	Yes
No Replay	Yes	Yes	Yes	Yes	Yes	Yes
Known SK Attack	No	Yes	Yes	No	No	Yes
Forward Security	No	Yes	Yes	No	No	Yes
Parrelel SK Attack	No	Yes	No	No	Yes	Yes

In Table 2, the performance of security is compared among six related schemes including the proposed scheme. According to the table, it is not difficult to find that the proposed scheme has better security performance.

Conclusions

In this paper, we propose an improved authentication scheme with user privacy for WSNs based on Kumar et al.'s shceme which has been pointed out not to resist known session key attack, impersonation attack, sensor node capture attack by Xu. Furtherly, through security analysis, we have shown that the proposed scheme does resist those attacks and also has some other properties of security.

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, Vol. 8, No. 3, pp. 1086-1090, 2009.

[2] M. K. Khan, and K. Alghathbar, "Cryptanalysis and security improvement of two-factor user authentication in wireless sensor networks," Sensors, Vol. 10, No. 3, pp. 2450 - 2459, 2010.

[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., Vol. 10, No. 4, pp. 1-11, 2010.

[4] T. H. Chen, and W. K. Shih, "A robust mutual authentication protocol for wireless sensor networks," ETRI J., Vol. 32, No. 5, pp. 704-712, 2010.

[5] C. C. Chang, and H. D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," IEEE Trans. Wireless Communication, Vol. 15, No. 1, pp. 357-365, 2016.

[6] R. Amin, and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," Ad Hoc Networks, Vol. 36, No. 1, pp. 58-80, 2016.

[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, Article ID 382810, 2012.

[8] P. Kumar, A. Gurtov, M. Ylianttila, et al., "A strong authentication scheme with user privacy for wireless sensor networks," ETRI Journal, Vol. 35, No. 5, pp. 889-899, 2013.

[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, Vol. 35, No. 5, pp. 1646-1656, 2012.

[10] C. B. Xu, "Cryptanalysis of a strong authentication scheme with user privacy for wireless sensor networks," 4th International Conference on Sensors, Mechatronics, Automation, pp. 425- 430, 2016.

ISSN:2319-7900

[11] Nyang D, and Lee M, “Improvement of Das’s two-factor authentication protocol in wireless sensor networks,” Cryptology ePrint Archive 2009/631,. http://eprint.iacr.org/ 2009 / 631.pdf.

[12] Huang H F, Chang Y F, Liu C H, “Enhancement of two-factor user authentication in wireless sensor networks,” Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Processes, Darmstadt, Germany, pp. 27-30, 2010.

Biographies

CHENGBO XU received the B.S. degree in Mathematics from the Liaocheng University, China, in 2002, the M.S. degree in Cryptology from the Hubei University, China, in 2005, and the Ph.D. degree in Computer Science from the Beijing University of Post and Telecommunication, China, in 2014, respectively. Currently, He is a Lecture in the School of Mathimatical Sciences at University of Jinan. His research interests include information security and cry ptology. Dr. Xu may be reached at ss_xucb@ujn.edu.cn.