International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:6, No:8, 2012

Comments on He et al.'s robust biometric-based user authentication scheme for WSNs

Eun-Jun Yoon, *Member, IEEE,* and Kee-Young Yoo, *Member, IEEE*

Abstract—In order to guarantee secure communication for wireless sensor networks (WSNs), many user authentication schemes have successfully drawn researchers' attention and been studied widely. In 2012, He et al. proposed a robust biometric-based user authentication scheme for WSNs. However, this paper demonstrates that He et al.'s scheme has some drawbacks: poor reparability problem, user impersonation attack, and sensor node impersonate attack.

Keywords—Security, authentication, biometrics, poor reparability, impersonation attack, wireless sensor networks.

I. INTRODUCTION

RECENTLY, wireless sensor networks (WSNs) have received a huge attention due to their promising applications in a variety of areas such as real-time traffic monitoring, measurement of seismic activity, wildlife monitoring and so on. In WSN, a large number of highly resource-constrained sensor nodes deployed to collect data or events in a specified geographic area [1]. In order to protect the important data and to prevent non-authorized users from gaining profit from the data, user authentication scheme should be offered [2], [3].

In 2010, Yuan et al. [4] proposed a biometric-based user authentication scheme for WSNs. Biometric keys can be a solution to solve the above security problems, which are based on physiological or behavioral characteristics of persons, such as fingerprints, faces, irises, and so on [5], [6], [7], [8], [9]. However, Yoon et al. [**?**] pointed out that Yuan et al.'s scheme is vulnerable to the insider attack, user impersonation attack, GW-node impersonation attack and sensor node impersonate attack. To improve security, Yoon et al.' proposed an improved scheme that can withstand various attacks. In 2012, He et al. [10], however, pointed out that Yoon et al.'s scheme is still vulnerable to the denial-of-service attack (DoS) and the sensor node impersonation attack and then proposed another improved scheme to overcome the weaknesses in Yoon et al.'s scheme. Nevertheless, this paper pointed out that He et al.'s scheme also has some drawbacks: poor reparability problem [11], [12], [13], [14], user impersonation attack, and sensor node impersonate attack [15].

This paper is organized as follows. Section 2 reviews He et al.'s scheme and then shows the security problems of the He et al.'s scheme in Section 3. Our conclusions are presented in Section 4.

E.-J. Yoon is with the Department of Cyber Security, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea e-mail: ejyoon@kiu.ac.kr.

K.-Y. Yoo is with the School of Computer Science and Engineering, College of IT Engineering, Kyungpook National University, Daegu 702-701, Republic of Korea e-mail: yook@knu.ac.kr. (Corresponding author.)

Manuscript received July 1, 2012; revised July 1, 2012.

II. REVIEW OF HE ET AL.'S SCHEME

This section briefly reviews He et al.'s scheme [10]. The scheme includes three phases: registration, login, and authentication. The following notations are used throughout this paper.

- U_i: the i-th user;
- ID_i, PW_i, B_i: Identity, password, and biometric template of U_i, respectively;
- $GW-node$: Gateway node of WSN;
- x, y; two master keys of GW-node;
- S_j: the j-th sensor node;
- SID_j: S_j identity;
- $d(\cdot)$: symmetric parametric function;
- τ: predetermined threshold for biometric verification;
- $E_k(\cdot)$: a symmetric encryption function with key k;
- $D_k(\cdot)$: the decryption function corresponding to $E_k(\cdot)$;
- $h(\cdot)$: Secure one-way hash function [16];
- $\oplus$: bit-wise exclusive-or(XOR) operation;
- $||$: concatenation of messages;

In order to execute He et al.'s framework, He et al. considered that the gateway is a trusted node and it hold two master keys (x and y), which are sufficiently large for the sensor network. Before starting the system, it is assumed that a long-term secret key $h(SID_j||y)$ generated by gateway is stored in sensor node S_j before the node is deployed, where SID_j is the identity of S_j.

A. Registration Phase

When a user U_i wants to register and become a new legal user, as shown in Fig. 1, the following steps are performed during the user registration phase.

Step 1. $U_i \rightarrow$ GW-node: $\{ID_i, h(PW_i||B_i||b_i), B_i\}$
U_i generates a random number b_i, freely chooses his/her identity ID_i, password PW_i, and also imprints his/her personal biometric impression B_i at the sensor. U_i then interactively submits $ID_i, h(PW_i||B_i||b_i), B_i$ to GW-node via secure channel.

Step 2. GW-node $\rightarrow U_i$: $\mathbf{Smartcard}(R_i, B_i, h(\cdot), d(\cdot), \tau)$
On receiving the registration request, GW-node computes $R_i = h(ID_i||x) \oplus h(PW_i||B_i||b_i)$, where x is a secret key maintained by GW-node. Then, GW-node writes the secure information $\{R_i, B_i, h(\cdot), d(\cdot), \tau\}$ to the memory of U_i's smart card and issues it to U_i through a secure channel.

Step 3. Upon receiving the smart card, U_i inputs the random number b_i into his/her smart card and finish the registration.

User U_i		**GW-node** (x, y)
Generate random number b_i Select ID_i and PW_i Imprint biometric impression B_i		
	$ID_i, h(PW_i\|\|B_i\|\|b_i), B_i$ $\longrightarrow$	
		Compute $R_i = h(ID_i\|\|x) \oplus h(PW_i\|\|B_i\|\|b_i)$ Store $\{R_i, B_i, h(\cdot), d(\cdot), \tau\}$ into Smartcard
	$\longleftarrow$ **Smartcard**$(R_i, B_i, h(\cdot), d(\cdot), \tau)$	
Input random number b_i into Smartcard	(Secure channel)	

Fig. 1. Registration phase of He et al.'s scheme

B. Login Phase

When the user U_i wants to access data from the WSN, the login phase is invoked as shown in Fig. 2. He/she must perform the following steps.

Step 1. U_i inserts his/her smart card into the card reader and inputs the personal biometrics B_i^* on the specific device to verify his/her biometrics. If $d(B_i, B_i^*) \geq \tau$, U_i's smart card rejects the request. Otherwise, U_i enters his/her password PW_i and his/her identity ID_i, and then the smart card generates a random number r_i and computes $D_i = R_i \oplus h(PW_i||B_i||b_i)$, $k_i = h(D_i||T_i)$, $C_i = E_{k_i}(ID_i||r_i)$, where T_i is the current timestamp.

Step 2. $U_i \rightarrow$ GW-node: $M_1 = (ID_i, C_i, T_i)$
U_i sends the login message $M_1 = (ID_i, C_i, T_i)$ to the GW-node.

C. Authentication Phase

When the GW-node receives the login request M_1 at time T', it will perform the following steps to authenticate U_i.

Step 1. GW-node $\rightarrow$ Sensor node S_j: $M_2 = (ID_i, C_g, T_g)$
GW-node checks the freshness of T_i by verifies whether the equation$(T' - T) \geq \Delta T$ holds. If the equation holds, GW-node stops the session, where ΔT is the expected time interval for the transmission delay. GW-node computes $D_i' = h(ID_i||x)$, $k_i' = h(D_i'||T_i)$ and $ID_i'||r_i' = D_{k_i'}(C_i)$. Then GW-node checks whether ID_i and ID_i are equal. If they are not equal, GW-node stops the session. Otherwise, GW-node computes $k_g = h(h(SID_j||y)||T_g)$, $C_g = E_{k_g}(ID_i'||r_i')$ and sends the message $M_2 = (ID_i, C_g, T_g)$ to S_j, here T_g is the current timestamp.

Step 2. Sensor node $S_j \rightarrow U_i$: $M_3 = (RM, V_s, T_s)$
Upon receiving the message M_2 , S_j checks the freshness of T_g by verifies whether the equation $(T'' - T_g) \geq \Delta T$ holds, where T'' is the time S_j receives M_2. If the equation holds, S_j stops the session, where ΔT is the expected time interval for the transmission delay. S_j computes $k_g' = h(h(SID_j||y)||T_g)$ and $ID_i''||r_i'' = D_{k_g'}(C_g)$. Then S_j checks whether ID_i'' and ID_i are equal. If they are not equal, S_j stops the session. Otherwise, S_j computes $V_s = h(ID_i''||r_i''||RM||T_s)$ and sends (RM, V_s, T_s) to U_i, where T_s is the current timestamp and RM is S_j's respond.

Step 3. Upon receiving the message $M_3 = (RM, V_s, T_s)$, U_i checks the freshness of T_s by verifies whether the equation $(T''' - T_s) \geq \Delta T$ holds, where T''' is the time U_i receives M_3. If the equation holds, U_i stops the session, where ΔT is the expected time interval for the transmission delay. U_i checks whether V_s and $h(ID_i||r_i||RM||T_s)$ are equal. If they are not equal, U_i stops the session key. Otherwise, U_i accepts the response message RM.

III. Security Weaknesses of He et al.'s Scheme

This section demonstrates that He et al.'s scheme [10] has some drawbacks: poor reparability problem, user U_i impersonation attack attacks, and sensor node S_j impersonation attack.

A. Assumptions for Security Analysis [13], [14]

Suppose that an adversary Eve has total control ability over the communication channel between the user U_i and the GW-node (including sensor node S_j, which means that he/she can insert, delete, or alter any messages in the channel. According to the researches in [13], [14], all existing smart cards are vulnerable to differential power analysis since the secret values stored into a smart card could be extracted by monitoring its power consumption. Based on these facts[13], [14], this paper assumes that the adversary Eve can steal the user's smart card and extract the secret values stored in the smart card. Based on these two assumptions, this paper shows some drawbacks of He et al.'s scheme [10].

B. Poor Reparability Problem [11], [12]

He et al.'s scheme is not reparable [11], [12]. In He et al.'s scheme, an adversary Eve can extract the secret value $R_i =$

User U_i $(ID_i, PW_i, \mathbf{Smartcard})$	**GW-node** (x, y)	**Sensor node** S_j $(h(SID_j\|\|y))$
Insert **Smartcard** Input biometric B_i^* Verify $d(B_i, B_i^*) \geq \tau$ Input ID_i and PW_i Generate random number r_i $D_i = R_i \oplus h(PW_i\|\|B_i\|\|b_i)$ Pick up timestamp T_i $k_i = h(D_i\|\|T_i)$ $C_i = E_{k_i}(ID_i\|\|r_i)$		
$M_1 = (ID_i, C_i, T_i)$ $\longrightarrow$		
	Verify $(T' - T) \geq \Delta T$ $D_i' = h(ID_i\|\|x)$ $k_i' = h(D_i'\|\|T_i)$ $ID_i'\|\|r_i' = D_{k_i'}(C_i)$ Verify $ID_i' \stackrel{?}{=} ID_i$ Pick up timestamp T_g $k_g = h(h(SID_j\|\|y)\|\|T_g)$ $C_g = E_{k_g}(ID_i'\|\|r_i')$	
	$M_2 = (ID_i, C_g, T_g)$ $\longrightarrow$	
		Verify $(T'' - T_g) \geq \Delta T$ $k_g' = h(h(SID_j\|\|y)\|\|T_g)$ $ID_i''\|\|r_i'' = D_{k_g'}(C_g)$ Verify $ID_i'' \stackrel{?}{=} ID_i$ Pick up timestamp T_s RM = Respond to the query of U_i $V_s = h(ID_i''\|\|r_i''\|\|RM\|\|T_s)$
$\longleftarrow$ $M_3 = (RM, V_s, T_s)$		
Verify $(T''' - T_s) \geq \Delta T$ Verify $V_s \stackrel{?}{=} h(ID_i\|\|r_i\|\|RM\|\|T_s)$ Accept RM		

Fig. 2. Login and authentication phases of He et al.'s scheme

$h(ID_i||x) \oplus h(PW_i||B_i||b_i)$, biometric impression B_i, and random number b_i, which is stored in the smart card of the user U_i by using above described differential power analysis attack [13], [14]. After obtaining these secret values (R_i, B_i, b_i), Eve can obtain the corresponding password PW_i by performing the following off-line password guessing attack.

Step 1. The adversary Eve intercepts the login request $M_1 = (ID_i, C_i, T_i)$.

Step 2. Eve guesses a password PW_i^* and then obtains D_i^* by computing $R_i \oplus h(PW_i^*||B_i||b_i)$.

Step 3. Eve computes $k_i^* = h(D_i^*||T_i)$ and obtains $ID_i^*||r_i^*$ by decrypting $C_i = E_{k_i}(ID_i||r_i)$ with k_i^*.

Step 4. Eve verifies ID_i^* is equal to ID_i. If $ID_i^* = ID_i$, then Eve has correctly guessed the password $PW_i^* = PW_i$ and $D_i^* = D_i$.

Step 5. Once the adversary Eve has correctly obtain $D_i = h(ID_i||x)$, then Eve can impersonate the legal user U_i.

The above attack can be failed if user U_i has detected that his/her identity D_i has been compromised and then changed his/her current password PW_i via some means that is not specified in He et al.'s scheme [12]. Because the password PW_i is the function of the identity ID_i of the user U_i and the secret key x of GW-node, GW-node has to change ID_i or x when changing the password PW_i for U_i. However, we can see that x is commonly used for all users rather than specifically used for only U_i in He et al's scheme. That is, it is not reasonable and efficient to change the secret key x for the security of a single user U_i. Moreover, it is also impractical to change identity of the user U_i. As a result, He et al.'s scheme is not reparable.

C. User U_i Impersonation Attack

He et al.'s scheme is vulnerable to the user U_i impersonation attack [15]. Once the adversary Eve obtained PW_i through above described differential power analysis attack [13], [14], he/she can obtain the secret value $D_i = h(ID_i||x)$ by computing $D_i = R_i \oplus h(PW_i||B_i||b_i)$. Then Eve can forge U_i's login message M_1 by computing $k_i = h(D_i||T_a)$ and $C_a = E_{k_i}(ID_i||r_a)$, where T_a is the current timestamp and r_a is the random number which generated by the adversary Eve. Finally, Eve sends a forged message $M_1 = (ID_i, C_a, T_a)$ to the GW-node. It is easy to see the forged message can pass GW-node's verification because GW-node will also compute same secret value $D_i = h(ID_i||x)$ with ID_i and its secret key x. Hence, He et al.'s scheme is vulnerable to user U_i impersonation attack.

D. Sensor Node S_j Impersonation Attack

He et al.'s scheme is vulnerable to sensor node S_j impersonation attack [15]. Once the adversary Eve obtained the secret value $D_i = h(ID_i||x)$ by the above described differential power analysis attack [13], [14], he/she can impersonate the sensor node S_j as follows:

Step 1. Upon intercepting the login request message $M_1 = (ID_i, C_i, T_i)$, Eve computes $k_i^* = h(D_i||T_i)$ and obtains $ID_i||r_i$ by decrypting C_i as $ID_i||r_i = D_{k_i^*}(C_i)$.

Step 2. Eve masquerades the sensor node S_j by computing $V_a = h(ID_i||r_i||RM^*||T_a)$ and sending a forged message $M_a = (RM^*, V_a, T_a)$ to U_i, where T_a is the current timestamp and RM^* is faked S_j's respond message.

It is easy to see that the forged message $M_a = (RM^*, V_a, T_a)$ can pass U_i's verification because V_a is always equal to $h(ID_i||r_i||RM^*||T_a)$. Hence, He et al.'s scheme is vulnerable to Sensor node S_j impersonation attack.

IV. Conclusions

This paper demonstrated that He et al.'s robust biometric-based user authentication scheme for WSNs has some drawbacks: poor reparability problem, user U_i impersonation attack attacks, and sensor node S_j impersonation attack. Thus, He et al.'s scheme cannot be applicable to real WSN communication environments. The schemes based on timestamps must overcome the problems of clock synchronization and delay-time limitation so that we better implement them in fast local area networks. Because He et al.'s scheme also used timestamps to resist replay attacks, the scheme can lead to serious clock synchronization problems, namely that the user's time and the GW-node's time (including sensor nodes) must differ only in a small range. For example, in a large-scale WSN network, it is almost impossible to maintain the synchronization of clocks among all entities in the WSN network and to guarantee the delay time of transmission. Further works will be focused on improving the He et al.'s scheme which can be able to provide greater security and provides computation efficiency.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript.

References

[1] C. Y. Chong and S. Kumar, Sensor networks: Evolution, opportunities and challenges, *Proceedings of IEEE*, vol. 91, no. 8, pp. 1247-1256, 2003.

[2] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, TinyPK: Securing sensor networks with public key technology, *ACM Workshop Security of Ad Hoc Sensor Networks*, Washington D C: ACM Press, pp. 59-64, 2004.

[3] K. Wong, Y. Zheng, J. Cao, and S. Wang, A dynamic user authentication scheme for wireless sensor networks, *IEEE International Conference Sensor Networks, Ubiquitous, Trustworthy Computing*, Taibei: IEEE Computer Society, pp. 244-251, 2006.

[4] J. J. Yuan, C. J. Jiang, and Z. W. Jiang A biometric-based user authentication for wireless sensor networks, *Wuhan University Journal of Natural Sciences*, vol. 15, no. 3, pp. 272-276, 2010.

[5] M. K. Khan and J. Zhang, Improving the security of a flexible biometrics remote user authentication scheme, *Computer Standards and Interfaces*, vol. 29, no. 1, pp. 82-85, 2007.

[6] M. K. Khan, J. Zhang, and X. Wang, Chaotic Hash-based fingerprint biometric remote user authentication scheme on mobile devices, *Chaos, Solitons and Fractals*, vol. 35, no. 3, pp. 519-524, 2008.

[7] J. K. Lee, S. R. Ryu, and K. Y. Yoo, Fingerprint-based remote user authentication scheme using smart cards, *Electronic Letters*, vol. 38, no. 12, pp. 554-555, 2002.

[8] C. H. Lin and Y. Y. Lai, A flexible biometrics remote user authentication scheme, *Computer Standards and Interfaces*, vol. 27, no. 1, pp. 19-23, 2004.

[9] C. T. Li and M. S. Hwang, An efficient biometrics-based remote user authentication scheme using smart cards, *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

[10] D. He, Robust biometric-based user authentication scheme for wireless sensor networks, *IACR Cryptology ePrint Archive 2012*, vol. 203, pp. 1-15, 2012.

[11] W. C. Ku, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, 2004, 50(1): 204-207.

[12] M. Kumar, On the weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, *CiteSeerX*, pp. 1-12, 2004.

[13] P. Kocher, J. Jaffe, and B. Jun, Differential power analysis, *Proceedings of Advances in Cryptology (Crypto'99)*, pp. 388-397, Santa Barbara, USA, 1999.

[14] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, Examining smart card security under the threat of power analysis attacks, *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541-552, 2002.

[15] D. He, J. Chen, and J. Hu, Weaknesses of a remote user password authentication scheme using smart card, *International Journal of Network Security*, Vol. 13, No. 1, pp. 58-60, July 2011.

[16] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, Handbook of applied cryptography, *CRC Press New York*, 1997.