Robust biometric-based user authentication scheme for wireless sensor networks

Debiao He*

School of Mathematics and Statistics, Wuhan University, Wuhan, China

Email: hedebiao@163.com

Abstract*:* Wireless sensor networks (WSNs) are applied widely a variety of areas such as real-time traffic monitoring, measurement of seismic activity, wildlife monitoring and so on. User authentication in WSNs is a critical security issue due to their unattended and hostile deployment in the field. In 2010, Yuan et al. proposed the first biometric-based user authentication scheme for WSNs. 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.'s proposed an improved scheme and claimed their scheme could withstand various attacks. Unfortunately, we will show Yoon et al.'s scheme is vulnerable to the denial-of-service attack (DoS) and the sensor node impersonation attack. To overcome the weaknesses in Yoon et al.'s scheme, we propose a new biometric-based user authentication scheme for WSNs. The analysis shows our scheme is more suitable for practical applications.

Key words*: Security; Authentication; Biometrics; Wireless sensor networks; Cryptography*

1. Introduction

Wireless sensor networks (WSNs) are innovative ad-hoc wireless networks consisting of a large number of sensor nodes with limited power, computation, storage and communication capabilities [1]. With the development of sensor technology, microelectronic technology, network technology and wireless communication technology, WSNs are widely used in military, environmental monitoring, medical, building condition monitoring and so on. In order to guarantee secure communication, authentication schemes for WSNs have successfully drawn researchers' attention and been studied widely.

In 2004, Benenson et al. [2] first described several security issues in WSNs, especially the access control problem. Then, Benenson et al. [3] proposed a user authentication scheme using elliptic curve cryptography (ECC). Wong et al. [4] pointed out that Benenson et al.'s [3] is vulnerable to impersonation attacks and denial-of-service (DoS) attacks. To improved security, Wong et al. [4] proposed a dynamic user authentication scheme for WSNs. Wong et al.'s scheme is very

efficient since only one-way hash functions and simple XOR operations are required in it. Unfortunately, Wong et al.'s scheme is vulnerable to many attacks such as replay attacks, forgery attacks, stolen-verifier attacks and password guessing attacks [5, 6, 7, 8]. Vaidya et al. [8] also pointed out that Tseng et al.'s scheme [5], Lee et al.'s and Ko et al.'s scheme [7] are vulnerable to replay of account-login attacks, man-in-the-middle attacks, forgery attacks and stolen-verifier attack, and node capture attacks. Vaidya et al. also proposed two improved schemes to improve the security.

In traditional authentication schemes for WSNs [4-8], the security of the authentication schemes is based on passwords. However, simple passwords are easy to break by simple dictionary attacks since they have low entropy. To solve the problem, cryptographic keys (e.g. 128bits for the advanced encryption standard, AES; [9]) are used. However, cryptographic keys are difficult to memorize since they are very long and random. Furthermore, both passwords and cryptographic keys are unable to provide non-repudiation because they can be forgotten, lost or when they are shared with other people, there is no-way to know who actual user is [10]. Therefore, biometric keys are proposed which are based on physiological and behavioral characteristics of persons such as fingerprints, faces, irises, hand geometry, and palm prints, etc. Some advantages of biometric keys are described as follows [11]:

- Biometric keys cannot be lost or forgotten.
- Biometric keys are very difficult to copy or share.
- Biometric keys are extremely hard to forge or distribute
- Biometric keys cannot be guessed easily.
- Someone's biometrics is not easy to break than others.

As a result, biometric-based user authentications are inherently more reliable and secure than usual traditional user authentication schemes.

In 2010, Yuan et al. [12] proposes the first biometric-based user authentication scheme for WSNs. Their scheme is very efficient since only the hash function is used in it. However, Yoon et al. [13] 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.'s proposed an improved scheme and claimed their scheme could withstand various attacks. In this paper, we will demonstrate that Yoon et

al.'s scheme is vulnerable to the denial-of-service attack (DoS) and the sensor node impersonation attack. We also propose an improved scheme to overcome the weaknesses in Yoon et al.'s scheme.

The rest of this paper is organized as follows. Section 2 reviews the concept of Yoon et al.'s scheme, and section 3 discusses its weakness analysis. Section 4 shows the details of our proposed scheme, while section 5 demonstrates the security analysis of our proposed scheme. Section 6 compares the performances of the related schemes. Finally, section 7 concludes this paper.

2. Review of Yoon et al.'s Scheme

In this section, we will review Yoon et al.'s scheme. For convenience, the notations used throughout this paper are summarized as follows:

- U_i: the ith user;
- ID_i, PW_i, B_i: U_i's identity, password and biometric template, respectively;
- $GW-node$: the gateway node of WSNs;
- S_j: the jth sensor node;
- SID_j: S_j's 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;
- $\oplus$:bit-wise exclusive-or(XOR) operation;
- $||$: concatenation operation;

Yoon et al.'s scheme includes three phases: registration phase, login phase, and authentication phase. They are described as follows.

2.1. Registration phase

In this phase, U_i submits hash value of his identity ID_i and his biometric template B_i to $GW-node$ in a secure manner. Then, $GW-node$ issues a license to U_i. The detailed steps, as shown in Fig. 1, are depicted as follows:

1). U_i inputs his biometrics B_i on the specific device, computes $E_i = h(ID_i \| B_i)$, and sends ID_i and E_i to the $GW-node$ in a secure manner.

2). On receiving ID_i and E_i, the $GW-node$ computes $R_i = h(ID_i \| x) \oplus E_i$ and $W_i = h(ID_i \| y) \oplus E_i$, where secret information x is known to only $GW-node$ and y is a secret parameter generated by $GW-node$ and stored in some designated sensor nodes before the nodes in the field are deployed.

3). $GW-node$ generates a smart card with parameters ID_i, E_i, R_i, W_i, $h(\cdot)$, $d(\cdot)$ and τ, where $d(\cdot)$ is a symmetric parametric function and τ is a predetermined threshold [14] for biometric verification.

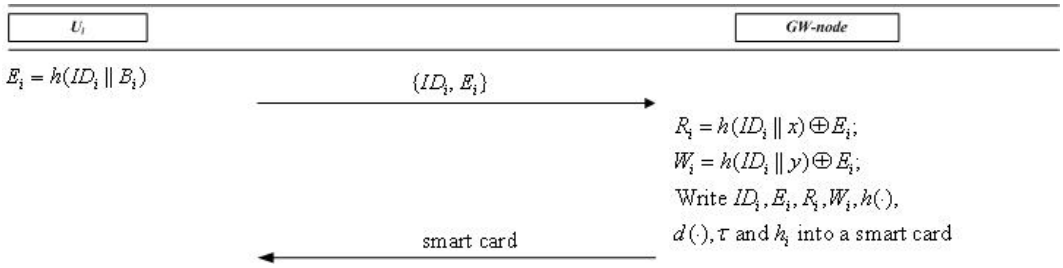

Fig. 1. Registration phase of Yoon et al.'s scheme

2.2. Login phase

When U_i enters B_i in order to deliver some query to or access data from the network, as shown Fig. 2, the smart card must perform the following steps to validate the legitimacy of U_i.

1). U_i inserts his smart card into the card reader and inputs B_i on the specific device.

2). The smart card computes $E_i' = h(ID_i \| B_i)$ and read E_i from the smart card. If $d(E_i', E_i) \geq \tau$, then the smart card stops the session. Otherwise, the smart card computes $D_i = R_i \oplus E_i$, $F_i = W_i \oplus E_i$ and $V_i = h(D_i \| F_i \| T_i)$, where T_i is the current timestamp.

3) U_i sends the login message $M_1 = (ID_i, V_i, T_i)$ to $GW-node$.

2.3. Authentication phase

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

1). $GW-node$ checks the freshness of T_i by verifies whether the equation $T'-T_i \geq \Delta T$ holds. If the equation holds, $GW-node$ stops the session, where ΔT is the expected time interval for the transmission delay.

2). $GW-node$ computes $D_i = h(ID_i \| x)$, $F_i = h(ID_i \| y)$ and $V_i' = h(D_i \| F_i \| T_i)$. Then $GW-node$ checks whether V_i' and V_i are equal. If they are not equal, $GW-node$ stops the session. Otherwise, $GW-node$ computes $V_g = h(ID_i \| SID_j \| F_i \| T_g)$ and sends the message $M_2 = (ID_i, V_g, T_g)$ to S_j, where T_g is the current timestamp.

3). 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.

4). S_j checks whether V_g and $h(ID_i \| SID_j \| h(ID_i \| y) \| T_g)$ are equal. If they are not equal, S_j stops the session key. Otherwise, S_j computes $V_s = h(ID_i \| h(ID_i \| y) \| RM \| T_s)$ and sends $M_3 = (RM, V_s, T_s)$ to U_i, where T_s is the current timestamp and RM is S_j's respond.

5). Upon receiving the message M_3, 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.

6). U_i checks whether V_s and $h(ID_i \| F_i \| RM \| T_s)$ are equal. If they are not equal, U_i stops the session key. Otherwise, U_i accepts the response message RM.

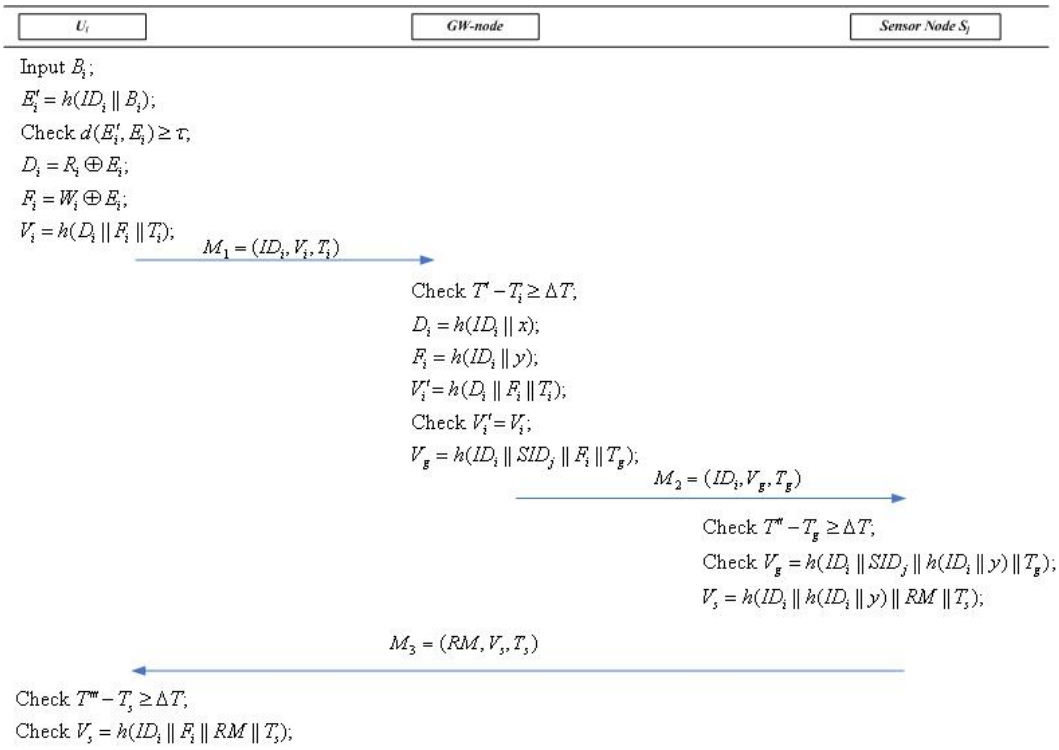

Fig. 2. Login and authentication phase of Yoon et al.'s scheme

3. Cryptanalysis of Yoon et al's scheme

3.1. Denial-of-service attack

One of the fundamental properties of a secure one-way hash function is that the outputs are very sensitive to small perturbations in their inputs. The cryptographic hash function cannot be applied straightforwardly when the input data are with noisy such as biometrics [15]. Then the predetermined threshold for biometric verification cannot be used to measure outputs of hash functions.

In registration phase of Yoon et al.'s scheme, the user U_i computes $E_i = h(ID_i \| B_i)$ based on his identity ID_i and personal biometric template B_i. The hash value E_i is stored in the smart card for purpose of authentication. However, the authentication procedure may result in serious flaws because $d(E_i', E_i) < \tau$ may never succeed, since the inputted biometrics belonging to the same person may differ slightly from time to time. Thus, the condition $d(E_i', E_i) < \tau$ may never succeed due to basic property of the one-way hash function $h(\cdot)$. As a result, this may cause the legal user unable to pass biometric verification at the login phase of Yoon et al.'s scheme. Therefore, Yoon et al.'s scheme is vulnerable to the denial-of-service attack.

3.2. Sensor node impersonation attack

Generally speaking, sensor nodes are often deployed in a hostile environment [16]. Then some sensor nodes may be captured by the adversary $\mathcal{A}$. Once $\mathcal{A}$ capture a sensor node S_{j+1}, he could extract the secret key y through the differential power attack [17, 18]. Then he could impersonate any other legal sensor node S_j as follows.

1) $\mathcal{A}$ intercepts the message $M_2 = (ID_i, V_g, T_g)$ sent to S_j by $GW-node$.

2) $\mathcal{A}$ forges a respond RM, computes $V_s = h(ID_i \| h(ID_i \| y) \| RM \| T_s)$ and sends $M_3 = (RM, V_s, T_s)$ to U_i, where T_s is the current timestamp.

It is to say V_s could pass the verification of U_i. Then U_i believes that the received message is sent by S_j. Therefore, Yoon et al.'s scheme is vulnerable to the node impersonation attack.

4. Proposed scheme

To solve the weakness of Yoon et al.'s scheme, we propose a new biometric-based user authentication scheme for WSNs. In order to execute the proposed framework, we 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.

4.1. Registration phase

When a user U_i wants to register and become a new legal user, as shown in Fig. 3, the following steps are performed during the user registration phase.

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

2) $GW-node$ 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.

3) Upon receiving the smart card, U_i inputs the random number b_i and finish the registration.

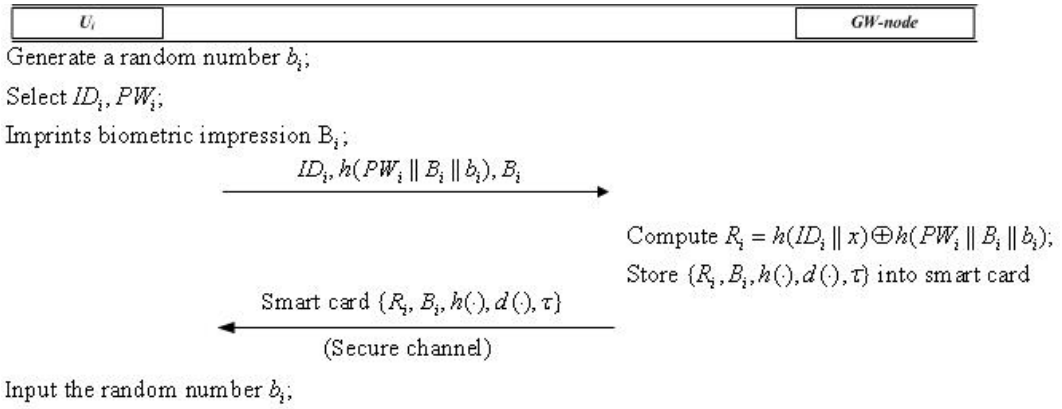

Fig. 3. Registration phase of our scheme

4.2. Login phase

When U_i enters B_i in order to deliver some query to or access data from the network, as shown Fig. 4, the smart card must perform the following steps to validate the legitimacy of U_i.

1). U_i inserts his smart card into the card reader and inputs B_i^* on the specific device.

2) If $d(B_i, B_i^*) \geq \tau$, U_i's smart card rejects the request. Otherwise, U_i enters his password PW_i and his identity ID_i, and then the smart card generates a random number r_i and computes $D_i = Z_i \oplus h(PW_i \| B_i \| b_i)$, $k_i = h(D_i \| T_i)$, $C_i = E_{k_i}(ID_i \| r_i)$, where T_i is the current timestamp.

3) U_i sends the login message $M_1 = (ID_i, C_i, T_i)$ to $GW-node$.

2.3. Authentication phase

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

1). $GW-node$ checks the freshness of T_i by verifies whether the equation $T'-T_i \geq \Delta T$ holds. If the equation holds, $GW-node$ stops the session, where ΔT is the expected time interval for the transmission delay.

2). $GW-node$ 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, where T_g is the current timestamp.

3). 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.

4). S_j computes $k_g' = h(D_j \| T_g)$ 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 $M_3 = (RM, V_s, T_s)$ to U_i, where T_s is the current timestamp and RM is S_j's respond.

5). Upon receiving the message M_3, 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.

6). 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.

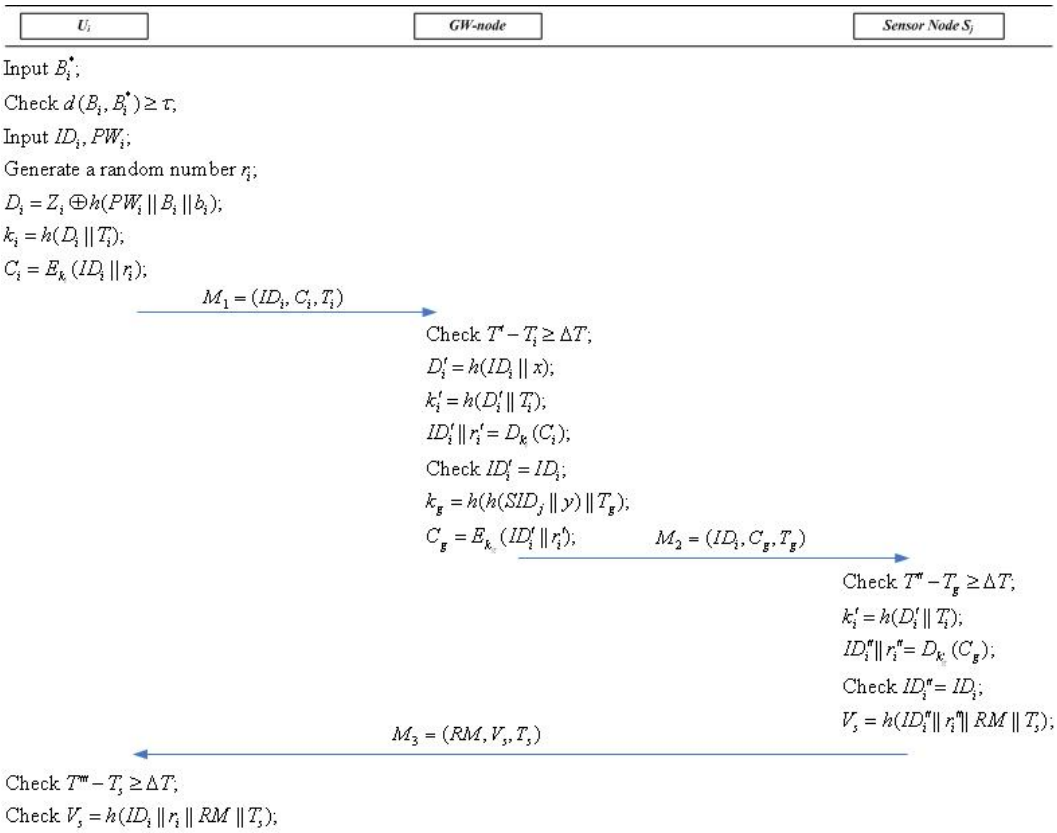

Fig. 4. Login and authentication phase of our scheme

4. Security analysis

In this section, we will discuss the security of our scheme as follows.

Denial-of-service attack. In our scheme, when the user inputs biometrics B_i^*, the smart will check the validity of B_i^* bye checking whether $d(B_i, B_i^*) \geq \tau$ holds. Through the work in [15], we know that B_i^* could pass the verification of the smart card although there is some slight difference between B_i^* and B_i. Therefore, our scheme could withstand denial-of service attacks.

Sensor impersonation attacks. The adversary $\mathcal{A}$ may capture some sensor node S_{j+1} and extract the secret key $h(SID_{j+1} \| y)$ through the differential power attack [17, 18]. He may intercept the message $M_2 = (ID_i, C_g, T_g)$ transmitted to the sensor node S_j. However, he cannot decrypt the message C_g since he does not have S_j's secret key $h(SID_j \| y)$. Then he cannot generate a legal message $M_3 = (RM, V_s, T_s)$. Therefore, our scheme could withstand the sensor impersonation attacks.

User impersonation attacks. Suppose an attacker want to forge a login message $M_1 = (ID_i, C_i, T_i)$. However, the attacker can not forge C_i without knowing $D_i = h(ID_i \| x)$ or the master key x. Therefore, our scheme could withstand user impersonation attacks.

Gateway impersonation attacks. As long as an attacker does not possess the secret key $h(SID_j \| y)$, he cannot impersonate the gateway and cannot cheat the sensor node since he cannot generate legal C_g. Hence, it frustrates attackers to generate the valid message $M_2 = (ID_i, C_g, T_g)$ to the sensor node. Therefore, our scheme could withstand gateway impersonation attacks.

Mutual authentication. Our scheme provides mutual authentication, where all entities (i.e., user, gateway and sensor node) are mutually authenticating each other. More specifically, when $GW-node$ receives the message $M_1 = (ID_i, C_i, T_i)$, it can make sure that whether the message is generated by U_i through checking whether the equation $ID_i' = ID_i$ holds. When the sensor node receives message $M_2 = (ID_i, C_g, T_g)$, it ensures that this message is generated by $GW-node$ through checking whether the equation $ID_i'' = ID_i$. Furthermore, when the user receives message $M_3 = (RM, V_s, T_s)$, he can also confirm that this message is generated by the sensor node by checking whether the equation $V_s = h(ID_i \| r_i \| RM \| T_s)$ holds. Therefore, our scheme could provide mutual authentication.

Replay attacks. Our scheme is resistant to replay attacks, because the authenticity of messages M_1, M_2 and M_3 are validated by checking the freshness of four timestamps. Let's assume an intruder intercepts a login request message $M_1 = (ID_i, C_i, T_i)$ and attempt to access the sensor node by replaying the same message M_1. The verification of this login attempt fails, since the time difference expires (i.e., $T' - T_i \geq \Delta T$). Similarly, if an intruder intercepts a valid message $M_2 = (ID_i, C_g, T_g)$ and attempts to replay it to the sensor node, the verification request will fail at the sensor node because of the time difference expires again (i.e., $T'' - T_g \geq \Delta T$). Therefore, our scheme could withstand replay attacks.

Man-in-the-middle attack: Man-in-the-middle attack means that an active attacker intercepts the communication line between a legal user and the server and uses some means to successfully masquerade as both the server to the user and the user to the server. Then, the user will believe that he is talking to the intended server and vice versa. From the above discussion we know that our scheme can provide mutual authentication, then our scheme could withstand man-in-the-middle' attacks.

Stolen-verifier attacks. An attacker who steals the password-verifier (e.g., hashed passwords) from the gateway can use the stolen-verifier to impersonate a legal user to login to the system. The proposed scheme is free from the stolen verifier attack. There is no such information stored at the server, by which an adversary can make a fabricated login request to impersonate a legal user to login the server, or can impersonate the gateway to cheat the legal user and the sensor node.

Insider attacks. It is possible in a real-time environment, when the gateway manager or system administrator can use the user password PW_i (e.g., weak password) to impersonate the user U_i through any other network gateways. In this case, our scheme does not give any room for privileged insiders, since, in the registration phase, the user U_i is passing $h(PW_i \| B_i \| b_i)$ instead of the plain password. Thus, the insider of $GW-node$ cannot get pw_U easily. Here, b_i is a sufficiently high entropy number, which is not revealed to $GW-node$. Furthermore, the proposed scheme does not store any verifier table and can resist the insider attacks.

5. Performance comparison

For the convenience of evaluating the computational cost, we define some notations as follows

T_h: The time of executing a one-way hash function.

T_{sym}: The time of executing a symmetric encryption/decryption function.

In Table 1, we summarize the performance results of the proposed scheme. According to Table 1, we know that the user, the sensor node and the gate way require $3T_h+1T_{sym}$, $2T_h+1T_{sym}$, $3T_h+2T_{sym}$ separately. It is well known that a one-

way hash function and a symmetric encryption/decryption function has almost same computational cost. Then, the computational costs of the user, the sensor node and the gate way in our scheme are slightly higher than that of Yuan et al.'s scheme and Yoon et al.'s scheme. However, Yuan et al.'s scheme cannot withstand denial-of-service attacks, insider attacks, user impersonation attacks, gateway node impersonation attacks and sensor node impersonation attacks. Besides, Yoon et al.'s scheme is vulnerable denial-of-service attacks and sensor node impersonation attacks. It is acceptable to enhance the security at the cost of increasing user's computation cost slightly. Then our scheme is more suitable for WSNs.

6. Conclusions

The paper demonstrates that Yoon et al.'s scheme is vulnerable to the denial-of-service attack and the sensor node impersonation attack. To overcome the security vulnerability, we provides a new biometric-based user authentication scheme for WSNs. The analysis shows the proposed scheme is more suited to WSNs environments.

Reference

[1] Akyildiz I., Su W., San Y., Cayirci, E. A survey on saensor network. IEEE Comm. Mag. 2002, 40, 102-114.

[2] Benenson, Z.; Gartner, F.; Kesdogan, D. User Authentication in sensor network (extended abstract). In Proceedings of the Informatik 2004, 34. Jahrestagung der Gesellschaft fur Informatik, Workshop on Sensor Networks, Ulm, Germany, September 2004.

[3] Benenson, Z.; Gedicke, N.; Raivio, O. Realizing robust user authentication in sensor networks. In Proceedings of the Workshop on Real-World Wireless Sensor Network (REALWSN'05), Stockholm, Sweden, 20–21 June 2005.

[4] Wong, K.H.M.; Zheng, Y.; Cao, J.; Wang, S. A dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), Taichung, Taiwan, 5–7 June 2006.

[5] Tseng, H.R.; Jan, R.H.; Yang, W. An improved dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE Global Communications Conference (GLOBECOM'07), Washington, DC, USA, 26–30 November 2007; pp. 986-990.

[6] Lee, T.H. Simple dynamic user authentication protocols for wireless sensor networks. In Proceedings of the 2nd International Conference on Sensor Technologies and Application (SENSORCOMM'08), Cap Esterel, France, 25–31 August 2008; pp. 657-660.

[7] Ko, L.C. A novel dynamic user authentication scheme for wireless sensor networks. In Proceeding of the IEEE International Symposium on Wireless Communication Systems 2008, ISWCS'08, Reykjavik, Iceland, 21–24 October 2008; pp. 608-612.

[8] Vaidya, B.; Rodrigues, J.J.P.C.; Park, J.H. User authentication schemes with pseudonymity for ubiquitous sensor network in NGN. International Journal Communication Systems, 2010, 23, 1201-1222.

[9] Advanced Encryption Standard /http://csrc.nist.gov/encryption/aes/S.

[10] Li, C., Hwang, M.: An efficient biometric-based remote authentication scheme using smart cards, Journal of Network and Computer Applications 2010, 33, 1-5.

[11] Lin, C., Lai, Y.: A flexible biometric remote user authentication scheme, Comput. Standards Interf., 2004, 27, (1), 19 – 23.

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

[13] Yoon E., Yoo K., A New Biometric-based User Authentication Scheme without using Password for Wireless Sensor Networks, 2011 20th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 279-284, 2011.

[14] Inuma M., Otsuka A., Imai H., Theoretical framework for constructing matching algorithms in biometric authentication systems, In proc. of ICB 2009, LNCS 5558, pp. 806-815, 2009.

[15] Linnartz, J.-P., Tuyls, P.: New shielding functions to enhance privacy and prevent misuse of biometric templates. Proc. Audio and Video-Based Biometric Person Authentication, 2003, (LNCS, 2688), pp. 393 – 402.

[16] Perrig A, Stankovic J, Wagner D, Security in Wireless Sensor Networks. Communications of the ACM, 2004, 47 (6):53-57.

[17] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, Proceedings of Advances in Cryptology (CRYPTO 99), 1999, pp. 388 – 397.

[18] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers 2002; 51 (5): 541 – 552.

Table 1. Performance comparisons among different schemes

	Yuan et al.'s scheme[12]	Yoon et al.'s scheme [13]	Our scheme
Computational cost (User)	$4T_h$	$3T_h$	$3T_h+1T_{sym} \approx 4T_h$
Computational cost (Sensor node)	$1T_h$	$3T_h$	$2T_h+1T_{sym} \approx 3T_h$
Computational cost (Gateway)	$4T_h$	$4T_h$	$3T_h+2T_{sym} \approx 5T_h$
Resist denial-of-service attacks	×	×	✓
Resist user impersonation attacks	×	×	✓
Resist sensor node impersonation attack	×	✓	✓
Resist gateway impersonation attack	×	✓	✓
Resist inside attack	×	✓	✓
Mutual authentication	✓	✓	✓
Resist replay attacks	✓	✓	✓
Resist stolen-verifier attacks	✓	✓	✓
Resist man-in-the-middle attack	✓	✓	✓