International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 8 (2017) pp. 1446-1451

Security Analysis of a Biometric-based Authenticated Key Agreement Scheme using ECC for Wireless Sensor Networks

Youngsook Lee*,
**Department of Cyber Security, Howon University, 64 Howon University 3Gil, Impi-Myeon, Gunsan-Si, Jeonrabuk-Do 573-718, Republic of Korea*

Abstract
A biometric-based user authentication scheme for wireless sensor networks is designed to restrict access to the sensor data only to users who are in possession of both a smart card and the corresponding biometrics. While a significant number of biometric-based user authentication schemes have been suggested in recent years, their intended security properties lack formal definitions and proofs in a widely-accepted model. The new technology of biometrics is becoming a popular method for engineers to design a more secure user authentication scheme. In 2014, Yoon and Yoo proposed an biometric-based authenticated key agreement scheme using ECC. Unfortunately, their scheme is still insecure and vulnerable to several security flaws. We show this by mounting the impersonation attack, biometrics error, no revocation phase.

Keywords: Wireless sensor network, Authenticated key agreement, Smart card, Impersonation attack, Biometrics error, Revocation phase.

INTRODUCTION

As various sensors emerge and related technologies advance, there has been a dramatic increase in the interest in wireless sensor networks (WSNs). Today, billions of physical, chemical and biological sensors are being deployed into various types of WSNs for numerous applications, including military surveillance, wildlife monitoring, vehicular tracking and healthcare diagnostics [1]. A major benefit of WSN systems is that they provide unprecedented abilities to explore and understand large-scale, real-world data and phenomena at a fine-grained level of temporal and spatial resolution. However, providing an application service in a WSN environment introduces significant security challenges to be addressed among the involved parties: users, sensors and gateways. One important challenge is to achieve authenticated key exchange between users and sensors (via the assistance of a gateway), thereby preventing illegal access to the sensor data and their transmissions. Authenticated key exchange in WSNs is more challenging to achieve than in traditional networks due to the sensor network characteristics, such as resource constraints, unreliable communication channel and unattended operation. User authentication schemes for WSNs are designed to address these security challenges [2,3,4], and are a subject of active research in network security and cryptography.

Generally speaking, the design of cryptographic schemes (including user authentication schemes for WSNs) is error-prone, and their security analysis is time-consuming. The difficulty of getting a high level of assurance in the security of cryptographic schemes is well illustrated with examples of flaws discovered in many such schemes years after they were published; see, e.g., [5–22]. One of the important issues in security of wireless sensor network is main security goal of authenticating between a remote individual and the sensor nodes, between the sensor node and the gateway node, and between the remote individual and the gateway node.

The new technology of biometrics is becoming a popular method for engineers to design a more secure user authentication scheme. In 2014, Yoon and Yoo proposed an biometric-based authenticated key agreement scheme using ECC [23]. In terms of physiological and behavioral human characteristics, biometrics is used as a form of identity access management and access control, and it services to identity individuals in groups that are under surveillance. In their article, they claim that the user can be authenticated using a biometric information and establishers the session key to be shared with between the server and the user. In addition to making this claim, Yoon and Yoo claim to exhibit various merits with its scheme: (1) their biometric-based authentication is more reliable than conventional authentication based on a password. (2) their scheme provides mutual authentication between not only gateway and sensor node but also between gateway and user. (3) their scheme is adapted to be efficient and lightweight in terms of computational cost and communication cost to decrease the energy consumption of sensor nodes which have limited energy and resources: in order to exploit the key block size, speed, security jointly, their scheme is based on one way hash function and elliptic curve cryptography. (4) their scheme can reduce the total execution time and memory requirement in comparison with previous related scheme. (5) their scheme is not only secure against well-known crypto graphical attacks but also provides perfect forward secrecy. (6) their scheme does not require the user's password and uses only the user' ID_i and biometrics B_i with hash function. However, Yoon and Yoo's scheme has some security problems such as mutual authentication, biometric recognition, and revocation phase. We show this by monitoring impersonation attacks, biometric recognition error, and no revocation phase.

The remainder for this paper is organized as follows. Section 2 reviews Yoon and Yoo's authentication phase. Section 3 presents weakness on Yoon and Yoo's scheme offers. Finally, we conclude this work in Section 4.

REVIEW OF YOON AND YOO'S AUTHENTICATION SCHEME

This section presents Yoon and Yoo's biometric authentication scheme using ECC for wireless sensor

networks [23]. The protocol participants include a gateway node, a remote user, and a server. For simplicity, we denote the gateway node by GW the remote user by U_i, and the sensor node by SR. Their protocol consists of four phases: system initiated phase, registration phase, login phase, and authentication phase. The system initiated phase is carried out whenever the gateway node generates parameters of the system. The registration phase is performed only once per user when a new user registers itself with the gateway node. The authentication phase is carried out whenever a user wants to gain access to sensor nodes. The system parameters listed in Table 1. are assumed to have been established in advance before the scheme is used in practice.

<Table 1.> Notation

U_i	User
ID_i	identity of an entity U_i
ID_{SR}	Identity of a sensor node that will respond to the query of U_i
B_i	the biometric template of U_i
GW	the gateway node of WSN
SR	the sensor node of WSN
S	the secret parameter maintained by GW node only
X	the secret key of GW node and stored in some designated sensor nodes before the nodes in the field are deployed
$h(\cdot)$	a secure one-way hash function whose output length is 160 bits based on SHA-1
$\|\|$	concatenation operation
d(•)	a symmetric parameter function
τ	a predetermined threshold for biometric verification
E	an elliptic curve over a finite field F_p
E(F_p)	the set of all the point on E
P	a base point P ∈ E(F_p), such that the subgroup generated by P has a large order n
⊕	the bitwise exclusive-or XOR operation
RM	respond to the query of U_i

System Initiation Phase :
In this phase, the gateway node GW generates parameter of the system.
S1. The gateway node GW chooses an elliptic curve E over a finite field F_P.
S2. GW chooses a base point $P \in E(F_p)$, such that the subgroup generated by P has a large order n
S3. The gateway node GW chooses a secure one-way hash function h(·), where h: $\{0,1\}^* \rightarrow Z^*_P$.
S4. The gateway node selects its secret key S.
S5. GW keeps S in private and publishes the parameter $(F_P, E, n, P, h(\cdot))$.

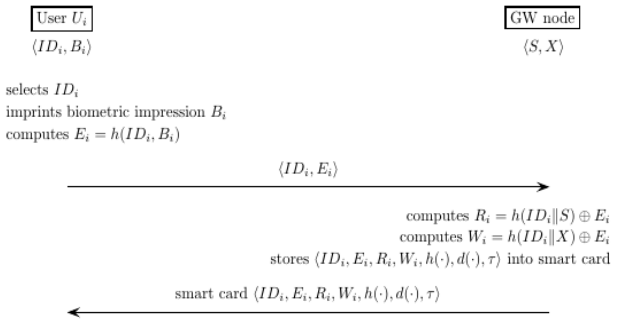


Figure 1. Yoon and Yoo's registration phase

Registration Phase :
A user U_i registers itself with the gateway GW. Yoon and Yoo's registration phase is depicted in Fig. 1 and its description is as follows:
R1. U_i inputs its biometrics B_i on the specific device, computes $E_i = h(ID_i, B_i)$, and submits it with the identity ID_i to GW via a secure channel.
R2. Upon receiving $<ID_i, E_i>$ from U_i, the gateway GW computes

$$R_i = h(ID_i||S) \oplus E_i,$$
$$W_i = h(ID_i||X) \oplus E_i, \text{ and}$$
$$E_i = h(ID_i, B_i).$$

R3. The gateway GW issues U_i a smart card loaded with $\{ID_i, E_i, R_i, W_i, h(\cdot), d(\cdot), \tau\}$. (We assume that τ is a predetermined threshold [23].) Then, GW sends the user's smart card to the user U_i through a secure channel.

Login Phase :
U_i needs to perform this phase with the gateway GW whenever it wishes to access data from the WSN. It should perform the following steps.
L1. The user U_i inserts its smart card into a card reader and inputs its biometrics B_i on the specific device to verify its biometrics.
L2. Given ID_i, and B_i, the smart card computes $E^*_i = h(ID_i, B_i)$. After having received E_i and E^*_i, the smart card verifies that $d(E_i, E^*_i) < \tau$. If the verifications fail, it generates reject message. Otherwise U_i passes the biometric verification.
L3. The smart card retrieves the current timestamp T_1, selects a random $\alpha \in F^*_P$ and computes:

$$D_i = R_i \oplus E_i,$$
$$F_i = W_i \oplus E_i,$$
$$A = \alpha P,$$
$$M_i = h(ID_i||F_i||A||T_1,).$$

After the computations, the smart card sends $<ID_i, A, M_i, T_1>$ to the gateway GW.

Key Agreement Phase :
The user U_i needs to perform this phase with the gateway GW and the sensor node SR whenever it wishes to gain access to the sensor network and data. The steps of the phase are depicted in Fig. 2 and are described as follows:
A1. Upon receiving $<ID_i, A, M_i, T_1>$, the gateway GW first

checks the freshness of T_1. If T_1 is not fresh, GW aborts the scheme. Otherwise, the gateway GW retrieves the current time T_2, computes D^*_i, F^*_i, and M^*_i as follows.

$$D^*_i = h(ID_i, ||S),$$
$$F^*_i, = h(ID_i, ||X),$$
$$M^*_i = h(ID_i||F^*_i||A||T_1).$$

Then, GW checks if $M_i = M^*_i$. the gateway GW aborts the scheme if the check fail. Otherwise, GW computes $Y_i = h(ID_i||ID_{SR}||A'||F^*_i||T_2)$ and sends $<ID_i, A, Y_i, T_2>$ to the sensor node SR .

A2. After having received $<ID_i, A, Y_i, T_2>$, SR computes F'^*_i and Y'^*_i as follows.

$$F'^*_i, = h(ID_i||X),$$
$$Y'^*_i = h(ID_i||ID_{SR}||A'||F'^*_i||T_2) .$$

SR verifies that : (1) T_2 is fresh;, (2) $Y'^*_i = Y_i$. If any of the verification fails, SR aborts the scheme. Otherwise, SR selects a random $\beta \in F^*_P$, the time stamp T_3 and computes $B = \beta P$ and the session key $SK = \beta A = \alpha\beta P$. Then the sensor node SR sets the respond to the query of U_i RM and computes $V_i = h(ID_i||F_i||RM||SK||T_3)$. Finally, SR sends the message < RM, B, V_i, T_3> to the user U_i.

A3. Upon receiving the message < RM, B, V_i, T_3>, the user U_i first checks the freshness of T_3. If $T_3$is not fresh, U_i aborts the scheme. Otherwise, the user U_i computes the session key $SK = \alpha B = \alpha\beta P$ and $V^*_i = h(ID_i||F_i||RM||SK||T_3)$. Then, U_i verifies that $V^*_i = V_i$. U_i aborts the scheme if the check fails. Otherwise, the user U_i accepts the sensor node's responding message RM.

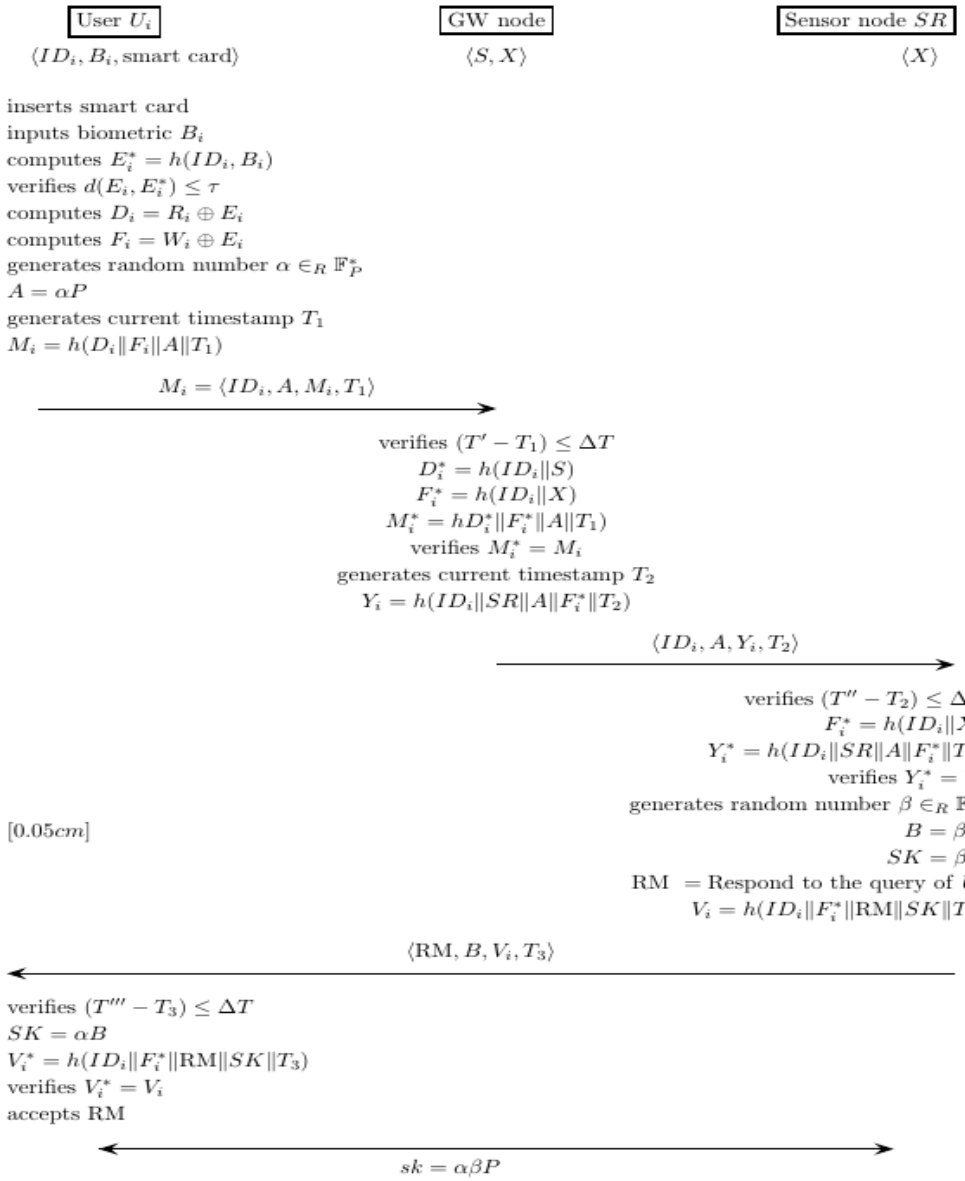


Figure 2. Yoon and Yoo's login and key agreement phase

WEAKNESSES IN YOON AND YOO'S BIOMETRIC-BASED AUTHENTICATED KEY AGREEMENT SCHEME

In this section, we point out weaknesses in Yoon and Yoo's scheme, starting with the most obvious one.

Vulnerability to mutual authentication :

Yoon and Yoo's scheme does not provide mutual authentication. First, we subscribe user impersonation attack where an attacker $U_a$can easily compute forged login request message. Before describing the attack we assume that the secret values stored in a smart card could be extracted by monitoring its power consumption [25, 26].

Impersonating U_i to GW and SR . We now proceed to present the user impersonation attack.

1. The attacker U_a who has obtained ID_i E_i, R_i and $W_i$stored in its smart card, and computes
$$D_a = R_i \oplus E_i = h(ID_i||S),$$
$$F_a = W_i \oplus E_i = h(ID_i||X).$$
2. When U_i initiates the login phase with login request message <ID_i, A, M_i, T_1> , the attacker U_a posing as U_i intercepts this login request and sends to GW a forged login request message as follows :
   (1) U_a retrieves the current timestamp T'_1 , selects a random $\alpha' \in F^{\star}_P$ and computes $A' = \alpha' P$ and $M_a = h(ID_i||F_a||A'||T'_1)$.
   (2) Then U_a posing as some registered user U_i sends the forged login request message <ID_i, A', M_a, T'_1> as a login request message to the gateway GW.
3. Since, from GW's point view, ID_i , A', M_a , T'_1 of an honest execution, GW believes that the message ID_i , A', M_a , T'_1 is from the legitimate user U_i. Hence, GW operates as specified in scheme using the received message from U_a.
   (1) GW chooses a current timestamp T_2 and proceeds to verify the authenticity of the login request. That is, GW computes D^*_i, F^*_i, and M^*_i and checks that $T'_1$is fresh and M_a equals M^*_i. Since it hold, GW will welcome U_a 's visit to the system. Then, GW computes $Y_i = h(ID_i||ID_{SR}||A'||F^*_i||T_2)$ and sends $<ID_i, A', Y_i, T_2>$ to the sensor node SR .
   (2) Since ID_i, A', Y_i , and T_2 are all valid, everything proceeds as usual. In respond to $U_a's$ login request, SR computes F'^*_i and Y'^*_i and verifies that T_2 is fresh and Y'^*_i equals Y_i . Since it hold, SR seselects a random $\beta \in F^{\star}_P$, the time stamp T_3 and computes $B = \beta P$ and the session key $SK = \beta A = \alpha\beta P$. Then, SR computes V_i and sends < RM, B, V_i, T_3>.
   (3) Now, an attacker U_a upon receiving < RM, B, V_i, T_3> from SR compute the session key $SK = \alpha B = \alpha\beta P$. Finally, the gateway GW and the sensor node SRwill be unaware of attack and believes U_a as the legitimate user U_i. The attacker U_a succeed to gain access to the sensor network and data.

Impersonating GW and SR to U_i . An attacker $U_a$can easily impersonate the gateway node GW or the sensor node SR. Before the describing the attack, we note that the secret values the stored in a smart card could be extracted by monitoring its power consumption [25, 26]. As a preliminary step, the attacker U_a extracts the secret values ID_i E_i, R_i and W_i stored in its smart card, and computes
$$D_a = R_i \oplus E_i = h(ID_i||S),$$
$$F_a = W_i \oplus E_i = h(ID_i||X).$$

1. **Impersonating GW to SR.** When U_i initiate the login phase with login request message <ID_i, A, M_i, T_1>, the attacker U_a posing as GW intercepts this message and sends a forges the gateway GW's response message as follows : U_a who has acquired the login message ID_i, A, M_i, T_1, and a secret value $h(ID_i||X)$, first
   (1) retrieves the current time T_2.
   (2) computes Y'_i=h$(ID_i||ID_{SR}||A||h(ID_i||X)||T_2)$.
   (3) And then, sends <ID_i, A, Y_i, T_2> to the sensor node SR .

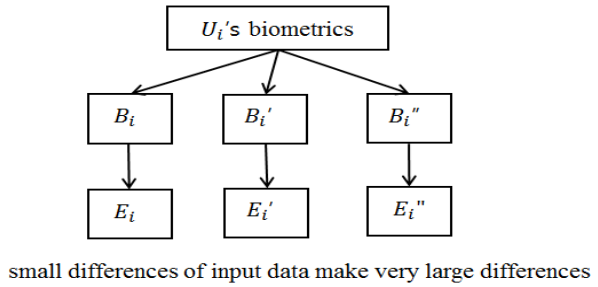
   The forged response message <ID_i, A, Y_i', T_2> will pass the verification test by SR since Y'_i is equal to h$(ID_i||ID_{SR}||A||h(ID_i||X)||T_2)$. Hence, SR believes U_a as the authentic GW.
2. **Impersonating SR to U_i .** When the gateway GW proceed the authentication phase with authentication request message <ID_i, A, Y_i, T_2>, the attacker U_a posing as SR intercepts ID_i, A, Y_i , T_2 and a secret value $h(ID_i||X)$ and sends a forges the sensor node SR 's response message as follows :
   (1) selects a random $\beta' \in F^{\star}_P$, the time stamp T_3.
   (2) sets the respond to the query of U_i RM
   (3) computes $B' = \beta' P$, V_i'=h$(ID_i||h(ID_i||X)||RM||SK||T_3)$, and the session key $SK = \beta' A = \alpha\beta' P$.
   (4) sends < RM, B', V_i', T_3> in response to U_i's login request message.

   The forged response < RM, B', V_i', T_3> will pass the verification test by U_i since V_i' is equal to h$(ID_i||h(ID_i||X)||RM||SK||T_3)$. Hence, U_i believes U_a as the authentic sensor node.

Vulnerability to biometric recognition:

Yoon and Yoo's authentication scheme uses a one-way hash function to provide biometric verification. A hash is a function that can be used to map data of arbitrary size to data of fixed size. The slight differences in input data produce very big differences in output data. This output is called hash value. Biometrics have general limitations such as false acceptance and false rejection. This means that the output of the imprinted biometrics is not always constant. Although the user U_i inputs its own biometrics to the scanning device, it is possible to output a different $B^*_i{}'$. Therefore, the same biometrics can produce different output.

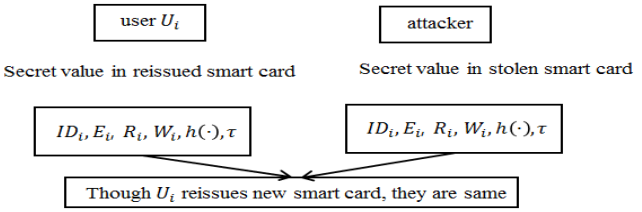
A different $B^*_i{}'$ causes very large difference in E^*_i and $E^*_i{}'$ due to the property of hash function. The large difference between E^*_i and $E^*_i{}'$ causes a biometric recognition error, so a legitimate user cannot pass the authentic test of login phase. As a result, advanced techniques are needed to improve the success rate of a legitimate user's verification [22].



small differences of input data make very large differences

Vulnerability to revocation phase :

A user U_i who wants to registration with the system submits only its identity ID_i and biometrics B_i to the gateway GW via secure channel. Yoon and Yoo's authentication scheme does not use password. So, password change phase is not necessary. If an attacker steals or pick up the user's smart card, revocation problem occurs. If the U_i sends the same ID_i and B_i to the gateway node GW, GW issues the smart card without verifying the used ID_i. It always makes same secret values $\{ID_i, E_i, R_i, W_i, h(\cdot), d(\cdot), \tau\}$ stored in smart card. Although U_i reissues new smart card , it is no longer new. The user U_i cannot discard the lost smart card because the reissued smart card and lost smart card are same. For this reason, U_i has to change its ID_i to reissue different smart card.



CONCLUDING REMARKS

This work demonstrated that Yoon and Yoo's authentication scheme for wireless sensor networks fails to achieve major security properties - mutual authentication, biometrics recognition error, recognition phase - in the presence of a malicious adversary. We have shown that failure to achieving mutual authentication is due to the vulnerability to an impersonation attack while failure to achieving biometrics recognition is due to the vulnerability to a biometrics recognition error. Note that the latter vulnerability implies that Yoon and Yoo's scheme does not achieve revocation phase. We hope that similar security flaws as identified in this work can be prevented in the future design of anonymous authentication schemes.

Acknowledgments:

This work was supported by Howon University in 2017.

REFERENCES

[1] Rawat, P., Singh, K., Chaouchi, H., Bonnin, J., Wireless sensor networks: A survey on recent developments and potential synergies. J. Supercomput., 68 (2014), 1–48.

[2] Kumar, P., Choudhury, A., Sain, M., Lee, S., Lee, H. RUASN, A robust user authentication framework for wireless sensor networks. Sensors, 11 (2011), 5020–5046.

[3] Khan, M., Kumari, S. An improved user authentication protocol for healthcare services via wireless medical sensor networks. Int. J. Distrib. Sens. Netw. 2014, 2014, No. 347169.

[4] Junghyun N., Moonseong K., Juryon P., Youngsook L., Dongho W., A Provably-Secure ECC-Based Authentication Scheme for Wireless Sensor Networks. Sensors, 14(2014) 21023-21044; doi:10. 3390/s141121023.

[5] Das, M.L., Two-factor user authentication in wireless sensor networks. IEEE Trans Wirel. Comm. 8 (2009), 1086–1090.

[6] [6] Khan, M.K., Alghathbar, K., Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. Sensors 10 (2010), 2450–2459 .

[7] Tan, Z.: Cryptanalyses of a two-factor user authentication scheme in wireless sensor networks. Adv. Inf. Sci. Serv. Sci. 6(4) (2011), 117–128.

[8] He, D.; Gao, Y., Chan, S., Chen, C., Bu, J. An enhanced two-factor user authentication scheme in wireless sensor networks. Adhoc Sens. Wirel. Netw., 10 (2010), 361–371.

[9] Khan, M., Alghathbar, K. Cryptanalysis and security improvements of "two-factor user authentication in wireless sensor networks". Sensors, 10 (2010), 2450–2459.

[10] Chen, T., Shih, W. A robust mutual authentication protocol for wireless sensor networks. ETRI J., 32 (2010), 704–712.

[11] Yeh, H.; Chen, T., Liu, P., Kim, T., Wei, H. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 11 (2011), 4767–4779.

[12] Kumar, P., Lee, S., Lee, H. E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors, 12 (2012), 1625–1647.

[13] Yoo, S., Park, K., Kim, J. A security-performance-balanced user authentication scheme for wireless sensor networks. Int. J. Distrib. Sens. Netw. (2012), 2012, No. 382810.

[14] Vaidya, B., Makrakis, D., Mouftah, H. Two-factor mutual authentication with key agreement in wireless sensor networks. Secur. Commun. Netw. (2012), doi:10.1002/sec.517.

[15] Xue, K., Ma, C., Hong, P., Ding, R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. J. Netw. Comput. Appl., 36 (2013), 316–323.

[16] Shi, W., Gong, P. A new user authentication protocol for wireless sensor networks using elliptic curves

cryptography. Int. J. Distrib. Sens. Netw. (2013), 2013, No. 730831.

[17] Kumar, P., Gurtov, A., Ylianttila, M.; Lee, S., Lee, H. A strong authentication scheme with user privacy for wireless sensor networks. ETRI J., 35(2013), 889–899.

[18] He, D., Kumar, N., Chen, J., Lee, C., Chilamkurti, N., Yeo, S. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimed. Syst. (2013), doi:10.1007/s00530-013-0346-9.

[19] Chi, L.; Hu, L.; Li, H.; Chu, J. Analysis and improvement of a robust user authentication framework for ubiquitous sensor networks. Int. J. Distrib. Sens. Netw. 2014, (2014), No. 637684.

[20] Kim, J.; Lee, D.; Jeon, W.; Lee, Y.; Won, D. Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks. Sensors, 14(2014), 6443–6462.

[21] Jiang, Q.; Ma, J.; Lu, X.; Tian, Y. An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. Peer-to-Peer Netw. Appl. (2014), doi:10.1007/s12083-014-0285-z.

[22] Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J.; Won, D. Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 14(2014), 10081–10106.

[23] Eun, Y., Kee, Y., A biometric-based authenticated key agreement scheme using ECC for wireless sensor netwoks. SAC (2014), 699-705.

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

[25] Kocher, P., Jaffe, J., Jun, B. Differential power analysis. In Proceedings of CRYPTO 1999, SantaBarbara, CA, USA, 15–19 August (1999), 388–397.

[26] Messerges, T., Dabbish, E., Sloan, R. Examining smart-card security under the threat of power analysis attacks. IEEE Trans. Comput., 51(2002), 541–552.