Security Enhancement to an Biometric Authentication Protocol for WSN Environment★

이영숙*

요 약

Over recent years there has been considerable growth in interest in the use of biometric systems for personal authentication. Biometrics is a field of technology which has been and is being used in the identification of individuals based on some physical attribute. By using biometrics, authentication is directly linked to the person, rather than their token or password. Biometric authentication is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems. In 2013, Althobati et al. proposed an efficient remote user authentication protocol using biometric information. However, we uncovered Althobati et al.'s protocol does not guarantee its main security goal of mutual authentication. We showed this by mounting threat of data integrity and bypassing the gateway node attack on Althobati et al.'s protocol. In this paper, we propose an improved scheme to overcome these security weaknesses by storing secret data in device. In addition, our proposed scheme should provide not only security, but also efficiency since sensors in WSN(Wireless Sensor Networks) operate with resource constraints such as limited power, computation, and storage space.

WSN 환경에서 Biometric 정보를 이용한 안전한 사용자 인증 스킴의 설계

Youngsook Lee*

ABSTRACT

바이오메트릭 정보를 이용한 인증방식은 사용자의 신체정보를 이용하여 신원을 확인 하고 시스템의 접근을 허가한다. 요즘 들어, 패스워드나 보안토큰을 단독으로 이용하는 방식보다는 하나이상의 고유한 신체적, 행동적 형질에 기반하여 개인의 생체 정보인 지문, 홍채 얼굴, 정맥 등을 활용하는 방식이 점차 증가하고 있는 추세이다. 2013년 Althobati 등이 WSN(Wireless Sensor Networks) 환경에 적합한 바이오메트릭 정보를 이용한 사용한 사용자 인증 스킴을 제안하였다. 그러나 그들이 제안 프로토콜은 데이터 무결성에 대한 위협과 바이패싱 게이트웨이 공격에 취약하여 상호인증을 달성할 수 없었다. 본 논문은 이전에 제안된 논문의 취약점을 개선하여 WSN 환경에 적합한 안전한 프로토콜을 제안하였다

Key words : Biometric-based Authentication Scheme, Wireless Sensor Network, Smart Card, Data Intigrity, Mutual Authentication

접수일(2016년 10월 5일), 수정일(2016년 10월 19일), 게재확정일(2016년 10월 20일)

★ 본 논문은 2016년 호원대학교 연구비 지원에 의하여 연구 되었음.

* 호원대학교 사이버수사보안학부

1. 서 론

In 2013, Althobati et al.[1] proposed an efficient remote user authentication protocol using biometric information[2-8]. The new technology of biometrics is becoming a popular method for engineers to design a more secure user authentication scheme. 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. However, in [8], we uncover Althobati et al.'s protocol does not guarantee its main security goal of mutual authentication. We show this by mounting threat of data integrity and bypassing the gateway node attack on Althobati et al.'s protocol.

Now, we proposed improved Althobatie et al.'s pr otocol for wireless sensor networks. This improvem ent shows the effectiveness of the proposed improve d Althobatie et al.'s protocol in terms of computatio n. Our protocol is extremely efficient in terms of the computation cost since protocol participants perform only a few hash function operations. Our improveme nt is both in efficiency and in security; the former b y reducing the use of encryption and decryption and the latter by providing an important security goal.

2. The proposed an Biometric Authentication Protocol for WSN

This section presents our biometric authentication protocol for wireless sensor networks. 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 server by S. Our protocol consists of three phases: registration phase, login phase, and authentication phase. 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 server. The system parameters listed in Table 1 are assumed to have been established in advance before the protocol is used in practice.

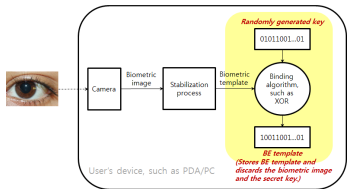
During some initialization phase, the biometric encryption will take place by using a fuzzy commitment scheme as in [16]. Fuzzy commitment scheme overcomes the drawback of traditional biometric systems where there is no need to store neither images nor the template of them in the memory.

<Table 1> Notation

U_i	device of entity U_i
ID_i	identity of an entity U_i
SID_j	identity of a server S_j
$iris_i$	the feature of the user U_i's iris
K	the secret key of the gateway GW
$X_{S_j}^*$	the secret parameter generated by GW and sec urely stored in designated S_j
x_S	the secret key of the gateway GW
$h(\bullet)$	One-way hash function
$\|\|$	Concatenation operation
$\oplus$	XOR operation

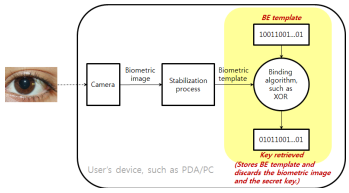
2.1 Registration Phase

This is the phase where a new registration of a u ser takes place. Our protocol is performed by extract ing the features of iris using an Fig 2. Registration phase of our iris recognition system. Additionally, th e hash value of the encryption key will be saved wit h the BE template to be able to reject incorrect keys in an early step, before beginning the process of rem ote authentication as shown in Fig 1. When the BE



(Figure 1) Saving user's secret key

template is saved in the user's device, the user can retrieve his key by capturing an image of his iris vi a the user's device camera. After that, the features o f iris will be extracted by the iris recognition model, then OXRed with the BE template to regenerate the user's key as shown in Fig. 2.



(Figure 2) Retrieving user's secret key

2.2 Login Phase

This phase is carried out whenever the user visits a gateway node and wants to gain access to the server S_j.

L1. After iris acquisition by camera in the U_i's device, the features of U_i's iris are extracted.

L2. The iris's features are corrected by error correcting code and hashed by SHA 256.

L3. Then, U_i computes

$RP_i^* = BE \oplus h(iris_i)$,

$A_i = A_i' \oplus h(iris_i)$,

$C_i = C_i' \oplus h(iris_i)$,

$H\_RP_i^* = h(RP_i^*)$ and checks that whether $H\_RP_i^*$ equals H_RP_i or not. If the variable is not equal, U_i rejects the login request. Otherwise, the application is proceeded. U_i continually obtains the current timestamp T_i and computes

$X_{S_i}^* = C_i \oplus H\_RP_i$,

$DID_i = h(H\_RP_i^* \| X_{S_i}^*) \oplus h(X_{S_i}^* \| RN_i \| T_i)$,

$M_{U-G} = h(A_i \| X_{S_i}^*) \oplus h(X_{S_i}^* \| RN_i \| T_i)$,

$v_i = RN_i \oplus X_{S_i}^*$.

L 4. After that, U_i sends

$<ID_i, DID_i, M_{U-G}, v_i, T_i>$ to the gateway GW node.

2.3 Authentication and key agreement Phase

With the login request message $\langle ID_i, DID_i, M_{U-G}, v_i, T_i \rangle$, the scheme enters the authentication phase during which GW and S_j node perform the following steps:

A1. When the login request arrives $\langle ID_i, DID_i, M_{U-G}, v_i, T_i \rangle$, the GW node checks the freshness of the timestamp T_i. GW aborts if the check T_i fail. Otherwise, GW retrieves the current timestamp T_G and computes

$X_{S_i} = h(ID_i \| x_S)$,

$RN_i = v_i \oplus X_{S_i}$,

$X^* = DID_i \oplus h(X_{S_i} \| RN_i \| T_i)$,

$M_{U-G}^* = h(X^* \oplus h(H\_RP_i \| K) \| X_{S_i} \| RN_i \| T_i)$.

GW verifies that $M_{U-G} = M_{U-G}^*$. If the verification fails, GW aborts the protocol. Otherwise, GW computes

$X_{S_j} = h(SID_j \| x_S)$,

$M_{G-S} = h(DID_i \| SID_j \| X_{S_j})$,

$w_i = RN_i \oplus X_{S_j}$.

Then, GW sends the message $<DID_i, M_{G-S}, w_i, T_G>$ to the server S_j.

A2. After receiving $<DID_i, M_{G-S}, w_i, T_G>$ from GW, S_j checks the freshness of the timestamp T_G.

S_j aborts if the check T_G fail. Otherwise, S_j retrieves the current timestamp T_j and computes

$M^*_{G-S} = h(DID_i \| SID_j \| X^*_{S_j} \| T_G)$,

$RN_i = w_i \oplus X^*_{S_j}$,

$y_j = RN_i \oplus RN_j$,

$M_{S-U} = h(DID_i \| RN_i \| RN_j \| T_j)$.

S_j checks that whether M^*_{G-S} equals M_{G-S} or not. If the verification is not equal, S_j aborts the session. Then, S_j sends the message $<M_{S-U}, y_j, T_j>$ to the user U_i.

A3. After receiving $\langle M_{S-U}, y_j, T_j \rangle$ from S_j, user U_i checks if the timestamp $T_j^{'}$ is fresh. If not, U_i aborts the session. Otherwise, U_i computes $RN_j = y_j \oplus RN_i$ and $M^*_{S-U} = h(DID_i \| RN_i \| RN_j \| T_j)$. U_i verifies that $M^*_{S-U} = M_{S-U}$. If the verification fails, U_i aborts the protocol. Otherwise, U_i computes the session key $K_S = f((DID_i \| RN_j), RN_i)$.

3. Security Analysis in the Proposed Protocol

Passwords are very important to user accounts, and there may come a time when you need to change your password. Or, maybe you've forgotten it. Whatever the case, we also proposed a password change phase.

3.1 Password Change Phase

During the password change phase, U_i updates the password without any assistance from server and gateway.

This phase consists of the following steps.

Step 1. Extracts $iris_i$

$RP^*_i = BE \oplus h(iris_i)$

$H\_RP^*_i = h(RP^*_i)$

$X_{S_i^*} = C_i \oplus h(ID_i \| H\_RP^*_i)$

$B^*_i = h(H\_RP^*_i \oplus X_{S_i^*})$

$B^*_i = ?\, B_i$

Step 2. Generates $RP_{ni} = h(RP_{ni})$

$H\_RP_{ni} = h(RP_{ni})$

$A_{ni} = A_i \oplus h(H\_RP^*_i \| X^*_{S_i}) \oplus h(H\_RP_{ni} \| X_{S_i^*})$

$B_{ni} = h(H\_RP_{ni} \oplus X_{S_i^*})$

$C_{ni} = X_{S_i^*} \oplus h(ID_i \| H\_RP_{ni})$

Step 3. Replace A_i, B_i and C_i with A_{ni}, B_{ni} and C_{ni}

3.2 Security Analysis on the Proposed Protocol

We now analyze the security of the proposed protocol, considering impersonation attacks and gateway node bypassing attack.

- To forge a valid response message $< L^{'}, T_5>$ of U_a posing as S, it is not suffices to obtain the information stored in U_i's device ; H_RP_i. $A_i^{'}$, $C_i^{'}$, and BE
- To forge a valid response message $<M_{S-U}$, y_j, $T_j^{'}>$ of U_a bypassing the gateway node, it is not suffices to obtain the information stored in U_i's device ; H_RP_i. $A_i^{'}$, $C_i^{'}$, and BE

Security analysis : Our protocol is extremely efficient in terms of the computation cost since protocol participants perform only a few hash function operations. Our improvement is both in efficiency and in security; the former by reducing the use of encryption and decryption and the latter by providing an important security goal. In Table. 2, we compare the considerations on security of our protocol with Althobaiti et al.'s protocol.

<Table 2> Comparison of considerations on security

considerations on security	[1]	※
password change phase	×	○
impersonation attacks	×	○
gateway node bypassing attacks	×	○
session key establishment	×	○
mutual authentication	×	○
data integrity	×	○
message confidentiality	×	○

※ : our proposed work

4. Conclusion

This work has considered the security of Althobaiti et al.'s authentication protocol[1] using biometric information. We demonstrated this by a server impersonation attack that completely compromises mutual authentication of the protocol[8]. Now, we proposed improved Althobatie et al.'s protocol for WSN. This improvement shows the effectiveness of the proposed improved Althobatie et al.'s protocol in terms of computation.

Reference

[1] O. Althobaiti ,M. Al-Rodhaan, and A. Al-Dhelaan, An Efficient Biometric Authentication Protocol for Wireless Sensor Networks, International Journal of Distributed Sensor Networks Volume 2013, Article ID 407971, 13 pages

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

[3] Z. Cheng, Y. Lee, C. Chang, C. L, A novel biometric-based remote user authentication scheme using Quadratic Residues, International Journal of Information and Electronics Engineering, 3{4} (2013) 419-422.

[4] Yuan, C. Jiang, and Z. Jiang, A biometric-based User Authentication for wireless Sensor Networks, Wuhan university journal of national sciences 5(3) (2010) 272-276.

[5] E.-J. Yoon, K. Y. Yoo, A new biometric-based user authentication scheme without using password for wireless sensor networks, Proceedings of 2011 IEEE International workshops of enabling technologies: Infrastructure for collaborative enterprises, (2011) 279-284

[6] Y. Lee, Security Analysis of a Biometric-Based User Authentication Scheme, The Korea-Society of Digital Industry& Information Management, 10(1), (2014), 81---87

[7] Y. Choi, Y. Lee, D. Won, Security Improvement on Biometric Based Authentication Scheme for Wireless Sensor Networks Using Fuzzy Extraction, International Journal of Distributed Sensor Networks Volume 2016, Article ID 8572410, 16 pages http://dx.doi.org/10.1155/2016/8572410

[8] Y. Lee, Security Analysis to an Biometric Authentication Protocol for wireless Sensor Networks, The Korea-Society of Digital Industry& Information Management, 1 (1) (2015) 59-67

[저 자 소 개]

이 영 숙 (Youngsook Lee)

2009년 ~ 현재 호원대학교 사이버수사보안학부 부교수
2008년 8월 성균관대학교 컴퓨터공학과 공학박사
2005년 2월 성균관대학교 정보보호학과 공학석사
1987년 2월 성균관대학교 정보공학과 공학사

email : ysooklee@howon.ac.kr