논문 18-43-06-10 The Journal of Korean Institute of Communications and Information Sciences '18-06 Vol.43 No.06
https://doi.org/10.7840/kics.2018.43.6.968

WBAN 환경에서 효율적인 사용자 인증 방식

유 성 진•, 박 기 성*, 박 영 호°

Efficient User Authentication Scheme in WBAN Environment

SungJin Yu•, KiSung Park*, YoungHo Park°

요 약

최근 ICT(Information and Communication Technology) 및 초소형 전자기기 기술의 발전으로 환자는 웨어러블 기기와 초소형 센서를 통하여 언제 어디서나 의료 서비스를 제공 받을 수 있다. 그러나 이러한 서비스는 공개된 채널을 통하여 제공되므로 환자의 민감한 정보는 공격자의 재전송 공격, 가장 공격 등 다양한 공격에 쉽게 노출될 수 있다. 따라서 WBAN(Wireless Body Area Networks) 환경에서 올바른 사용자 및 의료 종사자를 인증하는 것은 매우 중요한 보안 문제이며 최근 Zhao 등과 Gao 등은 이러한 보안 문제를 해결하기 위하여 타원 곡선 암호 및 Chebyshev Chaotic Map 공개키 암호 기반 인증 방식을 제안하였다. 본 논문에서는 기존의 Zhao와 Gao 등이 제안한 공개키 기반 인증 방식이 저사양 기기를 고려하지 않아 실제 WBAN 환경에 효율적이지 않음을 밝히고 이를 개선한 대칭키 기반의 효율적인 인증 방식을 제안한다. 또한 제안된 인증 방식의 안전성을 분석하여 중간자, 내부자, 위장, 스마트카드 도난 공격 등 다양한 공격에 안전함을 보이고 BAN logic을 통하여 상호 인증이 가능함을 증명하였다. 따라서 제안하는 방식은 안전하며 저사양 기기를 고려한 실제 WBAN 환경에 효율적으로 적용 가능한 인증 방식이다.

Key Words : WBAN, User authentication, Symmetric key, BAN logic, Lightweight

ABSTRACT

With the development of microelectronics and ICT(Information and Communication Technology), a patient can access medical services using micro sensors and wearable devices at anytime and anywhere. However, because the medical services are provided via a public network, the sensitive information of patients are vulnerable to various attacks such as replay and impersonation attack. Therefore, a user authentication scheme becomes an important security issue in WBAN(Wireless Body Area Networks). Recently, to solve the security issue, Zhao et al. and Gao et al. proposed an authentication scheme using elliptic curve cryptosystem and chebyshev chaotic maps based cryptosystem respectively. However, because of limitation of battery and computation ability, traditional cryptosystems such as RSA and ECC are not suitable for WBAN.

In this paper, we propose a lightweight authentication scheme using symmetric key techniques to improve the efficiency of Zhao et al. and Gao et al.'s scheme. Our proposed scheme also prevents various attacks such as insider, replay, impersonation and smart card stolen attacks. In addition, we prove that our scheme provides secure mutual authentication using BAN (Burrows-Abadi-Neddham) logic. We also analyze the performance of our scheme compared with related schemes. Therefore, our proposed scheme is practically applicable for WBAN environments.

※ 본 연구는 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2017R1A2B1002147)
• First Author : (ORCID:0000-0002-3245-781X)Kyungpook National University, darkskiln@naver.com, 학생회원
° Corresponding Author : Kyungpook National University, parkyh@knu.ac.kr, 종신회원
* (ORCID:0000-0002-6172-9175)Kyungpook National University, kisung2@ee.knu.ac.kr, 학생회원
논문번호 : KICS2018-03-073, Received March 31, 2018; Revised May 31, 2018; Accepted June 5, 2018

Ⅰ. 서 론

최근 정보통신기술 및 임베디드 기술의 발전으로 WBAN에 대한 관련 연구가 활발히 이루어지고 있으며 환자는 언제 어디서나 초소형 센서와 웨어러블 기기를 통하여 자신의 혈압, 뇌파, 혈당 등 다양한 생체 정보를 의료 기관에 전송하고 의료 종사자는 전송받은 생체 정보를 토대로 사전에 환자의 질병을 예방하고 안전한 진단을 내릴 수 있다. 그러나 이러한 의료 서비스는 공개된 채널을 통해 제공되므로 공격자가 전송되는 환자의 민감한 생체 정보를 도청하여 환자의 프라이버시를 침해하거나 수정된 생체 정보를 의료 기관에 전송하여 오진을 통해 환자의 생명까지 위협할 수 있다. 따라서 안전한 서비스를 환자에게 제공하기 위하여 시스템은 환자 및 의료종사자가 합법적인 사용자인지 반드시 인증하여야 한다. 또한 체내에서 사용되는 초소형 센서 및 웨어러블 디바이스들은 제한된 배터리 및 연산능력을 가지고 있으므로 기존의 이산대수문제 및 소인수분해 문제를 기반으로하는 ECC 및 RSA 암호화 방식은 효율적이지 않다. 따라서 WBAN 환경에서 올바른 사용자를 인증하는 경량화된 인증 방식에 대한 연구가 활발히 이루어지고 있으며[1-4] 이는 환자의 안전을 위하여 반드시 이루어져야하는 보안 필수요소이다.

2013년 Ramli[5] 등은 WBAN 환경에서 안전한 데이터 인증을 위하여 타원 곡선 암호 기반의 인증 방식을 제안하였으며 2014년 Zhao 등은[6] WBAN 환경에서 타원 곡선 암호를 사용하여 익명성을 보장하는 인증 방식을 제안하였다. 그러나 제안된 방식은 타원 곡선 암호의 이산대수 문제를 기반으로 안전성을 제공하므로 높은 연산량을 요구하는 문제점이 있다. 2016년 Gao 등은[7] WBAN 환경에서 Chebyshev Chaotic Maps[8]를 사용한 사용자 인증 방식을 제안하였으나 Chebyshev Chaotic Maps 또한 타원 곡선 암호와 비슷한 연산량을 요구하므로 WBAN 환경에서 효율적이지 않다.

본 논문에서는 WBAN 환경에서 환자에게 안전한 서비스를 제공하기 위하여 연산량 및 배터리를 고려한 효율적인 인증 방식을 제안한다. 제안된 인증 방식은 중간자 공격, 재전송 공격, 위장 공격 및 내부자 공격과 같은 다양한 공격에 안전하며 익명성, 완전 순방향 비밀성과 상호 인증을 제공한다. 또한 BAN logic 분석을 통하여 상호 인증이 가능함을 증명하였으며 대칭키 연산을 기반으로 낮은 연산량을 제공하므로 실제 WBAN 환경에서 효율적으로 적용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구의 배경지식과 Zhao와 Gao 등이 제안한 인증 방식에 대해 설명한다. 그리고 3장에서 본 논문에서 제안한 대칭키 기반 인증 방식을 설명하고 4장에서는 제안한 방식의 안전성과 효율성을 분석한다. 마지막으로 5장에서는 본 논문에 대한 결론에 대해 제시한다.

Ⅱ. 관련 연구

2.1 WBAN

WBAN은 체내에 부착된 센서 및 웨어러블 디바이스 등 다양한 통신 기기를 통하여 환자의 생체 정보를 수집하고 의료 종사자가 수집된 생체 정보를 기반으로 환자의 건강 상태를 분석해 올바른 원격 의료 진단 및 치료 등을 수행할 수 있는 무선 통신 네트워크 기술이며[4] IEEE 802.15 TG(Task Group)을 통하여 2012년 공식적으로 표준화 되었다[9]. 또한 WBAN에 사용되는 센서 및 웨어러블 디바이스 등은 실시간으로 환자의 혈압, 뇌파, 혈당 등 다양한 생체 정보를 의료 기관으로 전송하므로 의료 종사자는 질병을 사전에 예방하거나 환자가 위급한 상황에 빠르게 대처 가능한 장점이 있다.

WBAN 시스템은 환자, 서버, 의사로 구성되며 인증 프로토콜 수행 과정은 그림 1과[4] 같고 각 수행 단계는 다음과 같다.

1) 초기화 단계 : 신뢰할 수 있는 서버는 시스템 매개변수, 서버의 비밀 키를 생성한다.
2) 등록 단계 : 환자와 의사는 서버에게 등록 요청을 하고 요청한 신원 ID에 대한 비밀 키를 발급받는다.
3) 상호인증 단계 : 서비스를 이용하기 위하여 환자와 의사는 서로 합법적인 사용자인지 확인한다.

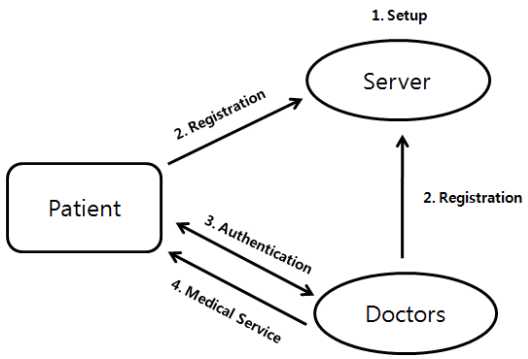

그림 1. WBAN 환경의 인증 프로토콜 수행 과정
Fig. 1. WBAN environment authentication protocol process

4) 서비스 단계 : 상호인증이 완료된 후 환자는 자신의 생체 정보를 의사에게 제공하고 의사는 제공된 생체 정보를 분석하여 올바른 진단 서비스를 제공한다.

2.2 Zhao 등의 ECC 기반 익명 인증 방식

2014년 Zhao 등은 WBAN 환경에서 타원 곡선 암호 기반의 익명성을 보장하는 인증 방식을 제안하였다. 그러나 제안한 방식은 타원 곡선 암호를 사용하여 높은 연산량을 요구하므로 실제 WBAN 환경에서 효율적이지 않다. Zhao 등이 제안한 방식은 사용자 등록 및 인증 단계로 구성되며 각 단계는 그림 2, 그림 3와 같고 수행절차는 다음과 같다.

2.2.1 사용자 등록 단계

■ 1단계 : Client(C)는 신원 ID_C와 임의의 랜덤 값 $\{x_C^1, x_C^2, \cdots x_C^n\} \in Z_q^*$ 을 선택하고 C는 $X_C^i = X_C^i P$을 계산한 후 메시지 $(ID_C, X_C^1, X_C^2, \cdots, X_C^n)$을 $Network\ Manager(NM)$에게 전송한다.

■ 2단계 : 메시지를 수신 받은 NM은 클라이언트의 신원이 유효한지 ID_C를 체크하고 신원 $PID_C = \{pid_C^1, pid_C^2, \cdots, pid_C^n\}$와 임의의 랜덤 값 $\{y_C^1, y_C^2, \cdots y_C^n\} \in Z_q^*$ 을 선택한다. 또한 NM은 $Y_C^i = y_C^i P$, $Q_C^i = X_C^i + Y_C^i$, $Y_C^i = H_1(pid_C^i \| Q_C^i \| right)$ $h_C^i = H_1(pid_C^i \| Q_C^i \|)$, $z_C^i = y_C^i + h_C^i \cdot s_{NM}$를 계산하여 $right, (pid_C^2, z_C^2, Y_C^2), \cdots, (pid_C^n, z_C^n, Y_C^n)$ 을 C에게 전송한다.

■ 3단계 : 메시지를 수신 받은 C는 $Q_C^i = X_C^i + Y_C^i$, $h_C^i = H_1(pid_C^i \| Q_C^i \| right)$와 $z_C^i P = Y_C^i + h_C^i \cdot Q_{NM}$을 체크한 후 $s_C^i = x_C^i + z_C^i$을 계산하고 NM로부터 수신 받은 메시지 (pid_C^n, z_C^n, Y_C^n)와 s_C^i을 디바이스에 저장한다.

2.2.2 인증 단계

■ 1단계 : C는 임의의 랜덤 값 $a_C^i \in Z_q^*$을 생성하고 디바이스에 저장된 (pid_C^n, z_C^n, Y_C^n) 및 타임스탬프 t_C^i를 이용하여 $A_C^i = a_C^i \cdot P$, $\overline{A_C^i} = a_C^i \cdot Q_{AP}$, $l_C^i = H_2(pid_C^i \| Q_C^i \| A_C^i \| \overline{A_C^i} \| t_C^i)$, $v_C^i = (s_C^i + l_C^i)(a_C^i)^{-1} \bmod q$, $K_C^i = H_3(A_C^i \| \overline{A_C^i} \| t_C^i$), $CT = E_{K_C^i}(pid_C^i \| Q_C^i \| right \| v_C^i)$을 계산한 후 인증 메시지 $m_1 = \{R_C^i, CT, t_C^i\}$을 $Application\ Provider(AP)$에게 전송한다.

■ 2단계 : 메시지를 수신 받은 AP은 타임스탬프의 유효성을 확인한 후 $\overline{A_C^i} = s_{AP} \cdot A_C^i$, $K_C^i = H_3(A_C^i \| \overline{A_C^i} \| t_C^i)$, $(pid_C^i \| Q_C^i \| right \| v_C^i) =$ $= D_{K_C^i}(CT)$을 계산한다. 또한 AP은 $h_C^i = H_1(pid_C^i \| Q_C^i \| right), l_C^i = H_2(pid_C^i \| Q_C^i \| A_C^i$ $\overline{A_C^i} \| t_C^i)$을 계산하고 $Q_C^i + h_C^i \cdot Q_{NM} + l_C^i \cdot P =$ $v_C^i A_C^i$을 체크한다. 그 후 AP는 임의의 랜덤 값 $b_C^i \in Z_q^*$을 생성하고 $B_C^i = b_C^i \cdot P$, $Auth$

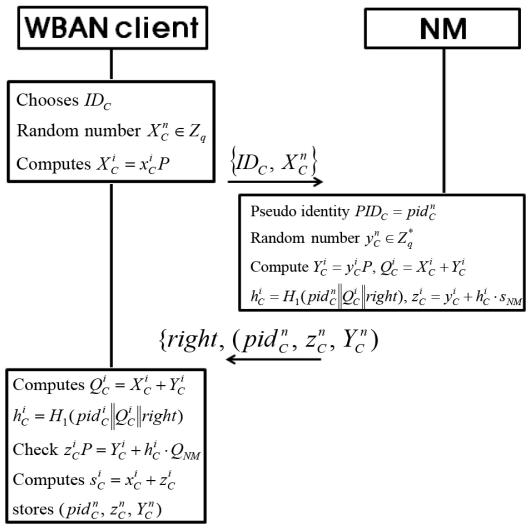

그림 2. Zhao et al. 사용자 등록 단계
Fig. 2. Registration phase of Zhao et al. scheme

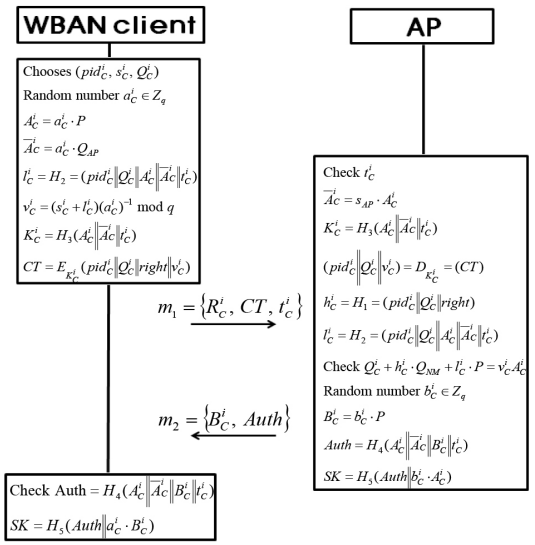

그림 3. Zhao et al. 상호인증 단계
Fig. 3. Authentication phase of Zhao et al. scheme

$= H_4(A_C^i \| \overline{A_C^i} \| B_C^i \| t_C^i)$을 계산한 뒤 세션 키 $SK = H_5(Auth \| b_C^i \cdot A_C^i)$와 인증 메시지 $m_2 = \{B_C^i, Auth\}$를 계산하여 C에게 전송한다.

- 3단계 : 메시지를 수신 받은 C는 $Auth$와 $H_4(A_C^i \| \overline{A_C^i} \| B_C^i \| t_C^i)$ 값이 유효한지 체크하고 세션 키 $SK = H_5(Auth \| a_C^i \cdot B_C^i)$를 계산한다.

2.3 Gao 등의 Chebyshev Chaotic Maps 기반 인증 방식

2016년 Gao 등은 WBAN 환경에서 해시 함수와 Chebyshev Chaotic Maps 공개키 방식을 사용한 인증 방식을 제안하였다. 그러나 Chaotic Maps을 이용한 공개키 암호 방식은 타원 곡선 암호와 비슷한 연산량을 가지므로 실제 WBAN 환경에 효율적이지 않은 문제점이 있다. Gao 등이 제안한 방식은 초기화, 사용자 등록 및 인증 단계로 구성되며 사용자 등록 단계 및 인증 단계는 그림 4, 그림 5과 같다. 또한 Chebyshev Chaotic Maps의 정의 및 각 단계의 수행 절차는 다음과 같다.

2.3.1 Chebyshev Chaotic Maps

Chebyshev 다항식 $T_n(x)$는 n이 정수일 때 범위 $[-1, 1]$에 속하는 x차수를 가지는 다항식이며, 이 때 Chebyshev 다항식은 $T_n(x) : [-1, 1] \rightarrow [-1, 1]$과 같이 정의된다. 또한 Chebyshev 다항식은 삼각함수 $\cos(x)$와 $\arccos(x)$로 식 (1)과 같이 정의된다.

$$T_n(x) = \cos(n \arccos^{-1}(x)) \quad (-1 \le x \le 1) \tag{1}$$

위의 식 (1)을 급수로 표현하면 식 (2)와 같이 정의된다.

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x \\ T_2(x) &= 2x^2 - 1 \\ T_3(x) &= 4x^3 - 3x \\ T_4(x) &= 8x^4 - 8x^2 + 1 \\ T_5(x) &= 16x^2 - 20x^3 + 5x \\ T_6(x) &= 32x^6 - 48x^4 + 18x^2 - 1 \end{aligned} \tag{2}$$

Chebyshev 다항식은 부분군 특성 및 혼돈 성질을 제공하며[10-12] 부분군 특성의 정의는 다음 식 (3)과 같다.

$$\begin{aligned} &T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x)) \\ &r, s \in Z, (s \in [-1, 1]) \end{aligned} \tag{3}$$

2008년 Zhang[13] 등은 부분군 특성이 $[-\infty, +\infty]$ 범위에 정의된 Chebyshev 다항식에 적용될 수 있다는 것을 증명하였으며 Zhang 등의 정의에 따라 Chebyshev 다항식은 $n \ge 2$, $x \in (-\infty, +\infty)$, p와 같은 변수를 사용하여 식 (4)와 같이 정의될 수 있다.

$$T_n(x) = (2x T_{n-1}(x) - T_{n-2}(x)) \tag{4}$$

Chebyshev 다항식은 이산 대수 문제 및 Diffie-Hellan 문제를 기반으로 안전성을 제공하며 기반 문제에 대한 정의는 다음과 같다.

1) Chebyshev Chaotic maps 기반 이산 대수 문제
   x, y 두 요소가 주어지면 $T_n(x) \bmod p = y$ 값이 일치하는 정수 N을 찾기 어렵다.
2) Chebyshev Chaotic maps 기반 Diffie-Hellman 문제
   $x, T_r(x) \bmod p, T_s(x) \bmod p$ 3개의 원소가 주어지면 $T_{rs}(x) \bmod p$를 찾기 어렵다.

2.3.2 초기화 단계

초기화 단계에서 서버 S는 256 bit 이상의 길이를 갖는 비밀 키 mk, 임의의 랜덤 값 $x \in (-\infty, +\infty)$, 단방향 해시 함수 $h()$를 포함한 시스템 매개 변수를 생성하고 초기화 단계를 마친다.

2.3.3 사용자 등록 단계

- 1단계 : $User(U)$은 ID, PW 그리고 임의의 랜덤 값 b를 선택한 후 ID와 $h(PW) \oplus b$ 값을 안전한 통신 채널을 통해 $Server(S)$에게 전송한다.
- 2단계 : 서버는 사용자로 부터 ID와 $h(PW) \oplus b$을 수신하고 임의의 랜덤 값 p을 선택한 후 $X_u = h(ID \| mk)$, $Y = X_u \oplus h(PW) \oplus b$을 계산한다. 또한 $\{X_u, Y, h(), x, T_{mk}(x), p\}$값을 스마트카드에 저장한 후 사용자에게 전송한다.
- 3단계 : 사용자는 $Y_u = Y \oplus b$을 계산한 후 Y를 Y_u로 대체한 다음 임의의 랜덤 값 b를 스마트카드에 저장하고 등록 단계를 완료한다.

2.3.4 인증 단계

- 1단계 : 사용자는 카드 리더기에 스마트카드 SC을 삽입하고 아이디 ID와 패스워드 PW를 입력한다.

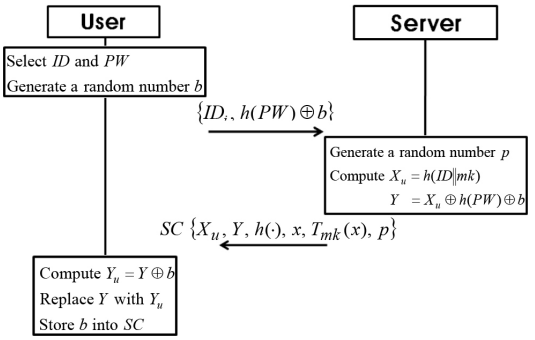

그림 4. Gao et al. 사용자 단계
Fig. 4. Registration phase of Gao et al. scheme

스마트카드는 임의의 랜덤 값 u을 선택하고 $C_1 \equiv T_u(x) \bmod p$, $KA \equiv T_u(T_{mk}(x)) \bmod p$, $X_u = Y \oplus h(PW)$, $DID = ID \oplus h(KA)$을 계산한 후 인증 메시지 $M_{us} = h(ID \| DID \| X_u \| C_1 \| KA)$을 생성하고 인증 요청 메시지 $M_1 = (C_1, DID, M_{us}, \| T_1)$을 생성하여 공개된 채널을 통해 서버에게 전송한다.

- 2단계 : 서버는 인증 요청 메시지를 수신한 후 타임스탬프 $T_2 - T_1 \le \Delta T$가 성립하는지 여부를 확인한다. 만약 성립하지 않는다면 세션을 종료하고 그렇지 않다면 서버는 $KA' \equiv T_{mk}(\ T_u(X)) \bmod p$, $ID' = DID \oplus h(KA'), X'_u = h(ID \| mk)$을 계산한다. 또한 서버는 $h(ID' \| DID \| X'_u \|\ C_1 \| KA') = M_{us}$ 메시지를 검증하여 유효한 값이 아닌 경우 세션을 종료하고 그렇지 않다면 $C_2 \equiv T_r(x) \bmod p$와 세션키 $sk \equiv T_r(T_u(x)) \bmod p$을 계산한다. 마지막으로 서버는 $M_{su} = h(ID' \ \| C_2 \| KA' \| sk)$을 계산하고 응답 메시지를 사용자에게 보낸다.

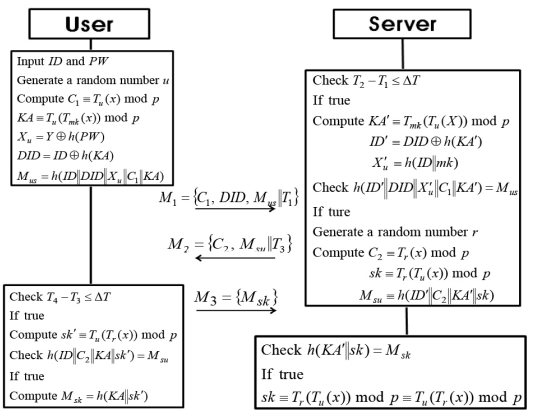

그림 5. Gao et al. 인증 단계
Fig. 5. Authentication phase of Gao et al. scheme

- 3단계 : 사용자는 응답 메시지 M_2을 수신한 후 $T_4 - T_3 \le \Delta T$가 유효한지 여부를 확인한다. 만약 성립하지 않는다면 세션을 종료하고 그렇지 않다면 사용자는 $sk' = T_u(T_r(x)) \bmod p$을 계산하고 $h(ID \| C_2 \| KA \| sk') = M_{su}$이 유효한 값인지 체크한다. 만약 유효한 값이라면 사용자는 인증 메시지 $M_{sk} = h(KA \| sk')$을 계산하고 $M_3 = \{M_{sk}\}$을 서버에게 전송한다.
- 4단계 : 서버는 메시지 M_3을 수신한 후 $h(KA' \| sk) = M_{sk}$가 유효한 값인지 여부를 확인하고 만약 유효한 값이라면 사용자와 인증을 마친다.

Ⅲ. 제안한 프로토콜

본 논문에서는 WBAN 환경에서 안전한 서비스 제공을 위하여 대칭키 기반의 효율적인 기반 인증 방식을 제안한다. 제안한 방식은 Zhao 등이 제안한 타원곡선 암호 방식과 Gao 등이 제안한 Chebyshev Chaotic Maps 기반 방식의 안전성을 그대로 보존하여 중간자 공격, 내부자 공격, 스마트카드 도난 공격 및 위장 공격 등 다양한 공격에 안전하며 익명성과 완전 순방향 비밀성을 보장한다. 또한 대칭키를 사용하여 저사양 기기 및 초소형 센서에서 효율적으로 동작할 수 있으므로 실제 WBAN 환경에 효율적으로 활용될 수 있다. 제안한 방식의 시스템 매개 변수 및 제안한 프로토콜은 다음과 같다.

3.1 시스템 매개 변수

제안하는 방식의 시스템 매개 변수는 표 1과 같다.

표 1. 매개 변수 표기법
Table 1. Parameter Notations

표기법	의미
U_i	User
ID_i	$U's$ identity
PW_i	$U's$ password
S_i	WBAN server
mk	$S's$ master key
K_i	Pre-distributed secret key between U_i and S_i
SC	Smart card
$h()$	Hash function
T	Timestamp
$\|$	concatenation operation
$\oplus$	XOR operation

3.2 사용자 등록 단계

제안하는 방식의 사용자 등록 단계는 그림 6과 같으며 각 단계는 다음과 같다.

- 1단계 : 사용자는 ID_i, PW_i와 임의의 랜덤 값 a_i을 선택한 후 $MP_i = h(ID_i \| PW_i \| a_i)$ 값을 계산하고 안전한 통신 채널을 통해 서버에게 전송한다.
- 2단계 : 서버는 ID_i, MP_i 값을 수신하고 임의의 랜덤 값 x_i, y_i을 선택한 후 $d_i = h(ID_i \| mk)$, $f_i = h(d_i \| MP_i)$, $K = h(ID_i \oplus x_i)$을 계산한다. 또한 서버는 $\{ID_i, K_i, y_i\}$을 데이터베이스 내에 저장하고 $\{f_i, h()\}$ 값을 스마트카드 내에 저장한 후 $\{Smart\ card, K_i, y_i\}$ 사용자에게 전송한다.
- 3단계 : $Smart\ card, K_i$ 값을 수신한 사용자는 $Q_i = h(ID_i \| PW_i) \oplus y_i$을 계산하여 $\{MP_i, a_i, Q_i\}$을 스마트카드 내에 저장하고 K_i을 사용자 장치에 저장한 후 등록 단계를 마친다.

3.3 인증 단계

제안하는 방식의 인증 단계는 그림 7과 같으며 각 단계는 다음과 같다.

- 임의의 랜덤 값 r_1, v_1을 선택한 후 $G_i = h(ID_i \| K_i) \oplus v_1$, $UK_i = h(v_1 \| y_i \| K_i)$을 계산하여 K_i 키를 업데이트한다. 키 업데이트가 완료된 후 사용자는 $B_i = E_{UK_i}(r_1), DID_i = ID_i \oplus h(r_1)$, $M_1 = = h(ID_i \| d_i \| T_1 \| r_1)$을 계산하여 유저는 $\{B_i, G_i, DID_i, M_1, T_1\}$을 공개된 채널을 통해 서버에게 전송한다.
- 2단계 : 서버는 유저가 보낸 메시지 $\{B_i, G_i, DID_i, M_1, T_1\}$를 수신한 후 타임스탬프 T_1의 유효성을 확인한다. 만약 타임스탬프가 유효한 시간 안에 전송된 값이라면 서버는 $v_1 = h(ID_i \| K_i) \oplus G_i$, $UK_i = h(v_1 \| y_i \| K_i)$, $B_i = D_{UK_i}(r_1)$, $ID_i = DID_i \oplus h(r_1)$을 계산한 후 $d_i = h(ID_i \| mk)$와 $M_1 = h(ID_i \| d_i \| T_1 \| r_1)$를 통하여 사용자가 유효한 신원이 맞는지 검증한다. 만약 사용자의 신원이 유효한 신원이 아닌 경우 서버는 세션을 종료하고 그렇지 않다면 임의의 랜덤 값 r_2을 선택하고 $C = E_{UK_i}(r_2), M_2 = h(r_2 \| ID_i \| M_1 \| r_1 \| T_1)$와 세션 키 $SK = h(r_1 \| r_2)$을 계산하여 $\{C_i, M_2\}$을 사용자에게 전송한다.
- 3단계 : 사용자는 응답 메시지 $\{C_i, M_2\}$를 수신한 후 $M_2 = h(r_2 \| ID_i \| M_1 \| r_1 \| T_1)$가 유효한 값인지 검증한다. 만약 M_2가 유효한 값이라면 $C_i = D_{UK_i}(r_2)$를 복호화하여 r_2값을 얻고 세션 키 $SK = h(r_1 \| r_2)$을 계산하여 상호 인증을 마친다.

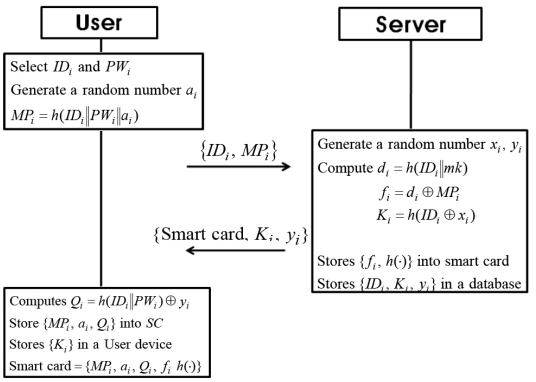

그림 6. 제안한 사용자 등록 단계
Fig. 6. Registration phase of propose scheme

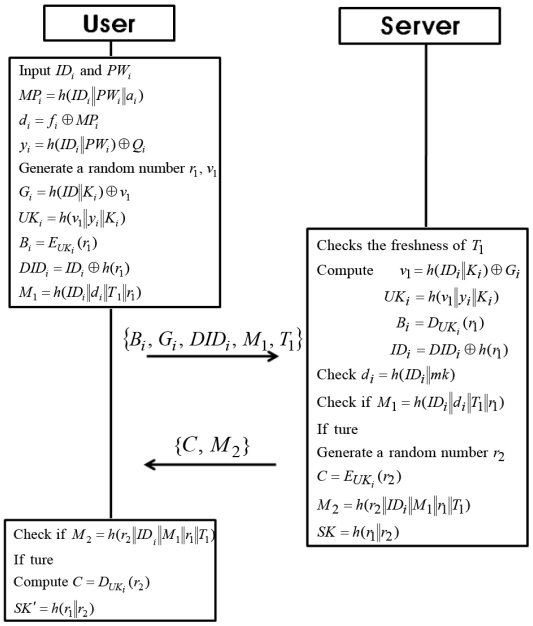

그림 7. 제안한 인증 단계
Fig. 7. Authentication phase of propose scheme

Ⅳ. 성능 분석

본 논문에서는 제안한 인증 방식과 기존의 Gao 등과 Zhao 등이 제안한 인증 방식의 연산량을 비교 분석하였으며 제안한 인증 방식의 안전성을 informal 분

석으로 분석하였다. 또한 제안한 방식이 상호 인증을 제공함을 BAN logic[14] 분석을 통하여 증명하였다.

4.1 연산량 분석

제안한 인증 방식과 Gao 등 및 Zhao 등의 인증 방식의 연산량을 비교 분석하기 위하여 각 방식들을 등록 단계, 인증 단계로 구분하였으며 비교 분석한 결과는 표 2와 같다.

상호 인증을 위하여 Zhao 등의 방식은 타원 곡선 스칼라 곱셈과 해시 함수 등을 사용하여 총 130.3ms의 연산 시간이 소요되었으며 Gao 등의 방식은 Chebyshev Chaotic Map 공개키 방식과 해시 함수, XOR 연산 등을 사용하여 총 104.76ms 연산 시간이 소요되었다[6,7]. 따라서 Gao 등의 방식이 Zhao 등의 방식보다 약 20% 정도 더 효율적이나 Gao 등의 방식은 Chebyshev Chaotic Map 공개키 암호화 방식을 사용하고 제안된 방식은 대칭키 암호화 방식을 사용하므로 제안된 방식이 더 빠른 암호화 및 복호화 연산을 제공한다. 따라서 제안된 인증 방식은 WBAN 환경에서 기존의 타원 곡선 암호 기반 및 Chebyshev Chaotic Map 기반 공개키 암호보다 효율적인 인증 방식이다.

표 2. 연산량 비교 분석
Table 2. Comparison of computation overhead

	Zhao et al. scheme[6]	Gao et al. scheme[7]	Proposed scheme
사용자 등록단계	2H+3E	2H+4X+1C	4H+3X
상호인증 단계	9H+3E+2S	8H+3X+6C	12H+6X+4S

E : ECC scalar multiplication, H : Hash,
S : Symmetric encrypt/decrypt, X : XOR,
C : Chebyshev chaotic map

4.2 안전성 분석

본 논문에서는 제안한 인증 방식의 안전성을 informal 분석으로 분석하였으며 제안한 방식은 중간자 공격 및 재전송 공격, 위장 공격, 스마트카드 도난 공격 그리고 내부자 공격 등 다양한 공격에 안전할 뿐만 아니라 익명성 및 완전 순방향 비밀성을 보장한다.

4.2.1 중간자 공격

중간자 공격은 공격자가 네트워크 통신을 조작하여 사용자와 서버 중간에서 데이터를 도청하거나 위조하는 공격 방식이다. 제안한 인증 방식에서 공격자는 변수 r_1, d_i를 알 수 없으므로 인증 메시지 $M_1 = h(ID_i \| d_i \| T_1 \| r_1)$, $DID_i = ID_i \oplus h(r_1)$를 생성할 수 없다. 따라서 제안하는 인증 방식은 중간자 공격에 안전하다.

4.2.2 재전송 공격

재전송 공격은 공격자가 이전의 세션에서 전송된 사용자의 메세지를 도청하여 해당 세션에서 다시 전송하여 정보를 얻거나 인증을 수행하는 공격이다. 제안한 방식은 타임스탬프 T_1을 사용하여 상호인증에 전송되는 인증 메시지 M_1, M_2을 계산하며 인증 단계에서 서버는 메시지를 수신하고 타임스탬프의 유효성을 확인한다. 따라서 공격자가 이전에 전송되었던 메시지를 도청하여 재전송 공격을 수행하여도 메시지에 포함된 타임스탬프를 통하여 메시지의 무결성을 보장할 수 있으므로 제안한 방식은 재전송 공격에 안전하다.

4.2.3 완전 순방향 비밀성

완전 순방향 안전성은 공격자에게 long-term key가 노출되어도 이전의 세션에 영향을 줄 수 없어야 하는 특성을 의미한다. 제안한 방식에서는 long-term key K_i가 공격자에게 노출되더라도 사용자는 매 인증 단계마다 랜덤 넘버 v_1, y_i를 사용하여 $UK_i = h(v_1 \| y_i \| K_i)$로 계산하므로 공격자는 UK_i를 계산할 수 없다. 따라서 제안한 방식에서 완전 순방향 비밀성은 보장된다.

4.2.4 내부자 공격

내부자 공격은 시스템안의 또 다른 합법적인 사용자가 공격자가 되어 다른 사용자의 아이디나 패스워드와 같은 민감한 정보를 얻으려 시도하는 공격이다. 제안한 방식에서 사용자는 랜덤 넘버 v_1 및 y_i를 사용하여 $G_i = h(ID_i \| K_i) \oplus v_1$, $UK_i = h(v_1 \| y_i \| K_i)$를 계산하므로 공격자는 자신이 가진 서버의 정보로 다른 사용자의 정보를 얻을 수 없다. 따라서 제안하는 방식은 내부자 공격에 안전하다.

4.2.5 스마트카드 도난 공격

스마트카드 도난 공격은 공격자가 사용자의 스마트카드를 획득하고 스마트카드 안에 저장된 데이터를 이용하여 사용자의 정보를 얻으려고 시도하는 공격이다. 제안한 방식에서 공격자가 사용자의 스마트카드를 획득하여 카드 내의 정보 $\{MP_i, a_i, Q_i, f_i, h()\}$를 획득하더라도 실제 사용자의 ID_i 및 PW_i는 알 수 없으므로 DID_i, UK_i와 같은 중요한 값들을 계산할 수 없다.

따라서 스마트카드를 공격자가 획득하더라도 공격자는 사용자의 어떠한 중요 정보도 얻을 수 없다.

4.2.6 위장 공격

위장 공격은 공격자가 합법적인 사용자 또는 서버로 위장하여 인증을 수행하는 공격으로 위장 공격을 수행하기 위하여 공격자는 로그인 요청 메시지, 인증 메시지 또는 응답 메시지를 성공적으로 생성할 수 있어야 한다. 제안된 방식에서 공격자가 위장 공격을 시도하는 경우 $(UK_i, ID_i, r_1, r_2, v_1, y_i)$ 값을 정확히 알아야 인증 단계에 사용되는 요청 메시지 $\{B_i, G_i, DID_i, M_1, T_1\}$ 또는 응답 메시지는 $\{C_1, M_2\}$를 계산할 수 있다. 그러나 공격자는 사용자의 중요 파라미터 값을 알 수 없으므로 제안하는 방식은 위장 공격에 안전하다.

4.3 BAN logic 분석

BAN(Burrows – Abadi – Needham) logic은[14] 1990년 인증 프로토콜의 상호 인증을 증명하기 위해 제안된 증명 방식으로 현재 상호 인증의 안전성 분석을 위하여 널리 사용되고 있다. 본 논문에서는 BAN logic을 이용하여 제안하는 인증 방식의 안전성을 분석하였으며 BAN logic의 표기법은 다음 표 3와 같다. 또한 BAN logic 분석을 위하여 BAN logic 분석에 사용되는 규칙, 가정, 보안 목표 및 이상화 형태를 정의하고 BAN logic 분석을 수행한다.

4.3.1 BAN logic 표기법

표 3. BAN logic 표기법
Table 3. BAN logic notation

Notation	Description
$P\mid\equiv X$	P believes a statement X
$\#X$	X is fresh
$P\lhd X$	P sees X
$P\mid\sim X$	P once said X
$P\mid\Rightarrow X$	P control X
$\langle X\rangle_Y$	X is combined with the formula Y
$\{X\}_K$	X is encrypted by the K
$\overset{K}{\leftrightarrow}$	P and Q use the shared key K to communicate

4.3.2 규칙

BAN logic 분석을 위한 규칙들의 표기법 및 의미는 다음과 같다.

- Message meaning rule : 만약 P가 암호 키 K를 Q와 공유하고 있는 사실을 신뢰하고 K로 암호화된 메시지 X를 목격하면 P는 Q가 X를 언급한 사실을 신뢰한다. Message meaning rule은 식 (5)과 같다.

$$\frac{P\mid\equiv P\overset{K}{\leftrightarrow}Q,\ P\ \triangleleft\ \{X\}_K}{P\mid\equiv Q\mid\sim X} \tag{5}$$

- Nonce verification rule : 만약 P가 X를 이번 세션에만 사용된 변수임을 신뢰하고 Q가 X를 언급한 사실을 신뢰하면 P는 Q가 X를 언급한 사실을 신뢰한다. Nonce verification rule은 식 (6)과 같다.

$$\frac{P\mid\equiv\#(X),\ P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X} \tag{6}$$

- Jurisdiction rule : 만약 P는 Q가 X를 제어하는 사실을 신뢰하고 Q가 X를 언급한 사실을 신뢰하면 P는 X를 신뢰한다. Freshness rule은 식 (7)과 같다.

$$\frac{P\mid\equiv P\mid\Rightarrow X,\ P\mid\equiv Q\mid\equiv X}{P\mid\equiv X} \tag{7}$$

- Freshness rule : 만약 P가 X를 이번 세션에만 사용된 변수임을 신뢰하면 P는 (X, Y)의 현재성을 신뢰한다. Freshness rule은 식 (8)과 같다.

$$\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X, Y)} \tag{8}$$

- Belief rule : 만약 P가 (X, Y)를 신뢰하면 P는 X를 신뢰한다. Belief rule은 식 (9)과 같다.

$$\frac{P\mid\equiv(X, Y)}{P\mid\equiv X} \tag{9}$$

4.3.3 보안 목표

제안된 프로토콜에서 인증 과정 후 키 합의를 수행하고 있으므로 BAN logic 분석 결과 안전성을 보장하기 위하여 만족해야하는 보안 목표는 다음과 같다.

Goal 1. $S|\equiv(S\overset{SK}{\longleftrightarrow}U)$

Goal 2. $S|\equiv U|\equiv(S\overset{SK}{\longleftrightarrow}U)$

Goal 3. $U|\equiv(S\overset{SK}{\longleftrightarrow}U)$

Goal 4. $U\equiv S|\equiv(S\overset{SK}{\longleftrightarrow}U)$

4.3.4 가정

BAN Logic 분석을 위한 초기 상태 가정은 다음과 같다.

A1. $S|\equiv\#(r_1)$

A2. $U|\equiv\#(r_2)$

A3. $S|\equiv S\overset{K_i}{\longleftrightarrow}U$

A4. $U|\equiv S\overset{K_i}{\longleftrightarrow}U$

A5. $S|\equiv U|\equiv\#(r_2)$

A6. $U|\equiv S|\equiv\#(r_1)$

A7. $S|\equiv\#(y_i)$

A8. $U|\equiv\#(y_i)$

4.3.5 이상화 형태

제안된 프로토콜에서 전송되는 각 파라미터를 BAN logic 분석을 위하여 주요 파라미터를 포함한 이상화 형태로 변환하여야하며 변환된 이상화 형태는 다음과 같다.

Message 1. $U\rightarrow S:(ID_i, v_1, y_i, d_i, \{r_1\}_{UK_i})_{K_i}$

Message 2. $S\rightarrow U:(ID_i, r_1, \{r_2\}_{UK_i})_{K_i}$

4.3.6 증명

Step 1. 서버가 유저로부터 전송받는 Message 1의 주요 파라미터를 정리한 이상화 형태로부터 다음 식 (10)을 얻는다.

$$(S_1):S\triangleleft(ID_i, v_1, y_i, d_i, r_1)_{K_i} \tag{10}$$

Step 2. S_1과 A_3로부터 message meaning rule을 적용하여 다음 식 (11)을 얻는다.

$$(S_2):S|\equiv U|\sim(ID_i, v_1, y_i, d_i, r_1)_{K_i} \tag{11}$$

Step 3. A_1로부터 freshness rule을 적용하면 서버는 식 (12)이 공격자에 의해 안전하다는 것을 보장한다.

$$(S_3):S|\equiv U|\equiv\#(ID_i, v_1, y_i, d_i, r_1)_{K_i} \tag{12}$$

Step 4. S_2과 S_3에 따르면 nonce verification rule을 적용하면 서버는 변수에 대한 검증을 통해 식 (13)을 얻는다.

$$(S_4):S|\equiv U|\equiv(ID_i, v_1, y_i, d_i, r_1)_{K_i} \tag{13}$$

Step 5. S_3과 S_4로부터 belief rule을 적용하여 식 (14)을 얻는다.

$$(S_5):S|\equiv U|\equiv(r_1)_{K_i} \tag{14}$$

Step 6. S_5와 A_2에 따르면 $SK=h(r_1\|r_2)$ 연산을 통해 서버는 식 (15)과 같이 보안목표 goal 2를 얻는다.

$$(S_6):S|\equiv U|\equiv(S\overset{SK}{\longleftrightarrow}U) \tag{15}$$

Step 7. S_6와 A_5로부터 jurisdiction rule을 적용하여 서버는 식 (16)과 같이 보안목표 goal 1을 얻는다.

(16)

Step 8. 유저는 서버로부터 전송받는 Message 2의 주요 파라미터를 정리한 이상화 형태로부터 다음 식 (17)을 얻는다.

$$(S_8):U\triangleleft(ID_i, r_1, r_2)_{K_i} \tag{17}$$

Step 9. S_8과 A_4로부터 message meaning rule을 적용하여 다음 식 (18)을 얻는다.

$$(S_9):U|\equiv S|\sim(ID_i, r_1, r_2)_{K_i} \tag{18}$$

Step 10. A_2로부터 freshness rule을 적용하면 서버는 식 (19)이 공격자에 의해 안전하다는 것을 보장한다.

$$(S_{10}):U|\equiv S|\equiv\#(ID_i, r_1, r_2)_{K_i} \tag{19}$$

Step 11. S_9과 S_{10}에 따르면 nonce verification rule을 적용하면 서버는 변수에 대한 검증을 통해 식 (20)을 얻는다.

$$(S_{11}):U|\equiv S|\equiv(ID_i, r_1, r_2)_{K_i} \quad (20)$$

Step 12. S_{10}과 S_{11}로부터 belief rule을 적용하여 식 (21)을 얻는다.

$$(S_{12}):U|\equiv S|\equiv(r_1, r_2)_{K_i} \quad (21)$$

Step 13. S_{12}에 따르면 $SK=h(r_1 \| r_2)$ 연산을 통해 서버는 식 (22)과 같이 보안목표 goal 4를 얻는다.

$$(S_{13}):U|\equiv S|\equiv(S\xleftrightarrow{SK}U) \quad (22)$$

Step 14. S_{13}와 A_6로부터 jurisdiction rule을 적용하여 서버는 식 (23)과 같이 보안목표 goal 3을 얻는다.

$$(S_{14}):U|\equiv(S\xleftrightarrow{SK}U)_{K_i} \quad (23)$$

V. 결 론

WBAN 환경에서 사용자는 언제 어디서나 편리하게 자신의 생체 정보를 의료 기관에 제공하고 의료 기관으로부터 다양한 의료 서비스를 제공 받을 수 있다. 그러나 이러한 생체 정보가 공격자에게 노출될 경우 사용자의 프라이버시 침해 및 오진으로 인한 인명피해까지 발생할 수 있으므로 WBAN 환경에서 올바른 사용자 및 의료 종사자를 인증하는 방식은 반드시 필요하다. 또한 WBAN 환경에 사용되는 저사양 기기들은 배터리 및 연산량이 제한적이므로 기존의 타원 곡선 암호 및 Chebyshev Chaotic Map 기반 공개키 암호는 적합하지 않다.

본 논문에서는 최근 제안된 Zhao 등과 Gao 등의 인증 방식이 공개키 기반 암호를 사용하여 WBAN 환경에 효율적이지 않음을 보이고 이를 개선하기 위하여 대칭키 기반의 효율적인 인증 방식을 제안하였다. 또한 제안한 인증 방식의 안전성을 분석하여 중간자 공격, 내부자 공격, 위장 공격 및 스마트카드 도난 공격 등 다양한 공격에 안전함을 보이고 BAN logic 분석을 통하여 상호 인증을 보장함을 증명하였을 뿐만 아니라 제안된 대칭키 기반 방식과 기존의 인증 방식들을 비교 분석하여 Zhao 등의 방식은 타원 곡선 암호화 연산 3번, Gao 등의 방식은 Chebyshev Chaotic Maps 암호화 연산 6번을 수행함을 보이고 제안된 방식이 더 효율적인 암호화 및 복호화 연산을 제공함을 입증하였다. 따라서 제안하는 인증 방식은 실제 저사양 기기가 많은 WBAN 환경을 고려하여 제안되었으며 생체 정보와 같은 민감한 정보들을 안전하게 의료 기관으로 전송하여 위급한 상황에 빠르게 대처가능하며 원격 진단 및 치료 등의 의료 서비스에 효율적으로 활용 가능한 인증 방식이다.

References

[1] T. G. Zimmerman, “Personal area networks: Near-field intrabody communication,” *J. IBM Syst.*, vol. 35, no. 3, pp. 609-617, Feb. 1996.

[2] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, “Body area networks:A survey,” *Mob. Netw. Appl.*, vol. 16, no. 2, pp. 171-193, Apr. 2011.

[3] H. S. Ahn, E. J. Yoon, and K. D. Bu, “A practical authentication system for wireless body area networks(WBAN),” *Korea Inst. Inf. Commun. Eng.*, vol. 37, no. 4, pp. 290-296, Apr. 2012.

[4] M. S. Jeong, J. H. Suk, and D. H. Lee, “An improved ID-based anonymous authentication scheme for wireless body area networks,” *Korea Inst. Inf. Commun. Eng.*, vol. 21, no. 2, pp. 322-332, Apr. 2017.

[5] S. N. Ramli, R. Ahmad, and M. F. Abdollah, “A biometric based security for data authentication in wireless body area network(WBAN),” *in Proc. ICACT ICC 2013*, pp. 998-1001, PyeongChang, Korea, Jan. 2013.

[6] Z. Zhao, “An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem,” *J. Med. Syst.*, vol. 38, no. 2, pp. 1-7, Jan. 2014.

[7] G. Gao, X. Peng, Y. Tian, and Z. Qin, “A chaotic maps-based authentication scheme for wireless body area networks,” *J. Distrib. Sensor Netw.*, vol. 12, no. 7, pp. 1-12, Jul. 2016.

[8] L. Kocarev, J. Makraduli, and P. Amato, “Public key encryption based on chebyshev polynomials,” *Cir. Syst. and Sign. Process.*, vol. 24, no. 5, pp. 497-517, Oct. 2005.

[9] R. Heile, *IEEE Standard for Local and Metropolitan Area Networks*(2012), Retrieved Mar. 20, 2018, from http://standards.ieee.org/findstds/standard/802.15.6-2012.html.

[10] S. Han and E. Chang, "Chaotic map based key agreement with out clock synchronization," *Chaos Solitons&Fractals*, vol. 39, no. 3, pp. 1283-1289, Feb. 2009.

[11] C. C. Lee, C. L. Chen, C. Y. Wu, and S. Y. Huang, "An extended chaotic maps based key agreement protocol with user anonymity," *Nonlinear Dynamics*, vol. 69, no. 1-2, pp. 79-87, Jul. 2012.

[12] D. He, Y. Chen, and J. Chen, "Cryptanalysis and improvement of an extended chaotic maps based key agreement protocol," *Nonlinear Dynamics*, vol. 69, no. 3, pp. 1149-1157, Aug. 2012.

[13] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos Solitons&Fractals*, vol. 37, no. 3, pp. 669-674, Aug. 2008.

[14] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18-36, Feb. 1990.

유 성 진 (SungJin Yu)

2017년 2월 : 대구대학교 전자공학과 학사

2017년 3월~현재 : 경북대학교 대학원 전자공학부 석사과정

<관심분야> 정보보호, 무선통신보안, 네트워크보안

박 기 성 (KiSung Park)

2015년 2월 : 경북대학교 산업전자 전기공학부 학사

2017년 2월 : 경북대학교 대학원 전자공학부 석사

2017년 3월~현재 : 경북대학교 대학원 전자공학부 박사과정

<관심분야> 정보보호, 네트워크보안, PQ암호

박 영 호 (YoungHo Park)

1989년 2월 : 경북대학교 전자공학과 학사

1991년 2월 : 경북대학교 전자공학과 석사

1995년 2월 : 경북대학교 전자공학과 박사

1996년~2008년 : 상주대학교 전자전기공학부 교수

2003년~2004년 : Oregon State Univ. 방문 교수

2008년~2014년 : 경북대학교 산업전자공학과 교수

2014년~현재 : 경북대학교 전자공학부 교수

<관심분야> 정보보호, 네트워크보안, 모바일 컴퓨팅