JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 2 : 322~332 Feb. 2017

WBAN 환경에서의 개선된 ID 기반 익명 인증 기법

정민수 · 석재혁 · 이동훈*

An Improved ID-based Anonymous Authentication Scheme for Wireless Body Area Networks

Min-Soo Jeong · Jae Hyuk Suk · Dong Hoon Lee*

Graduate School of Information Security, Korea University, Seoul 02841, Korea

요 약

WBAN(Wireless Body Area Networks)은 센서를 통해 사용자의 생체 정보를 수집하고 사용자가 요구하는 서비스를 제공해주는 환경을 말한다. 센서의 중요성이 점차 높아짐에 따라 WBAN 또한 주목받고 있다. WBAN은 대표적으로 의료 분야에서 사용되고 환자의 생명과 직결될 수 있다는 문제를 가지고 있기 때문에 안전성은 매우 중요하다. 또한 WBAN에서 사용되는 기기는 연산량에 제한이 있기 때문에 효율성도 매우 중요하게 고려되어야 한다. 이에 따라 WBAN 환경에서의 ID 기반 익명 인증에 관한 연구가 최근 활발하게 진행되고 있다. 본 논문에서는 최근 Wu et al.이 제안한 WBAN 환경에서의 ID 기반 익명 인증 기법이 위장 공격에 취약하다는 것을 보인다. 그리고 Wu et al. 기법 등 이전에 제안되었던 기법들에 대해서 밝혀진 공격에 안전한 새로운 ID 기반 익명 인증 기법을 제안한다. 본 논문에서 제안한 기법은 이전에 제안된 기법들과 비교해서 30.6%, 7.3%만큼 연산량이 개선되었다.

ABSTRACT

Wireless Body Area Networks is an environment that provides an appropriate service remotely by collecting user's biometric information. With the growing importance of sensor, WBAN also attracts extensive attention. Since WBAN is representatively used in the medical field, it can be directly related to the patient's life. Hence security is very important in WBAN. Mutual authentication between the client and the application provider is essential. And efficiency is also important because a used device is limited to computation cost. In this reason, ID-based anonymous authentication scheme in WBAN has been intensively studied. We show that the recent research result of Wu et al. which is about the ID-based anonymous authentication scheme is vulnerable to impersonation attack. And we propose a new ID-based anonymous authentication scheme that is secure against the attacks discovered in the existing schemes. Compared to the existing schemes, the computation cost of our scheme is improved by 30.6% and 7.3%.

키워드 : 무선 신체 영역 네트워크, 익명성, 상호 인증, 위장 공격

Key word : Wireless Body Area Networks, Anonymity, Mutual Authentication, Impersonation Attack

Received 10 November 2016, **Revised** 10 November 2016, **Accepted** 26 November 2016

* **Corresponding Author** Dong Hoon Lee(E-mail:donghlee@korea.ac.kr, Tel:+82-2-3290-4997)
Graduate School of Information Security, Korea University, Seoul 02841, Korea

Open Access http://doi.org/10.6109/jkiice.2017.21.2.322 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

WBAN(Wireless Body Area Networks)은 사용자의 신체에 장착된 센서를 통해 수집된 생체 정보를 서비스 제공자에게 전달하고, 서비스 제공자는 사용자에게 실시간으로 적합한 서비스를 제공하는 환경을 말한다. 1996년 Zimmerman이 처음으로 WBAN 환경을 제안한 이후[1], 센서의 중요성이 점차 부각되면서 WBAN에 대한 연구가 현재까지 활발하게 진행되고 있다[2]. 그림 1은 WBAN을 도식화한 것이다.

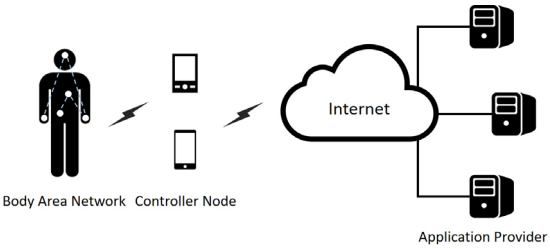

Fig. 1 Wireless Body Area Networks

WBAN은 대표적으로 의료 분야에서 사용된다[3]. 환자의 몸에 장착된 센서를 통해 생체 정보를 수집하고 이를 병원에 제공하면, 병원은 환자의 상태에 적합한 서비스를 실시간으로 제공한다. 환자가 제시간에 적절한 의료서비스를 제공받지 못하면 경우에 따라 환자의 생명에 치명적인 결과를 초래할 수 있기 때문에 WBAN 상의 통신은 여러 가지 공격에 안전해야 한다. 또한 사용자와 서비스 제공자가 주고받는 데이터는 제3자가 접근해서는 안 될 개인정보이기 때문에 정보가 노출되어서도 안 된다. 제3자가 실제 데이터에 접근할 수 없다고 하더라도 단순히 통신량이 증가하는 것만으로 환자의 상황이 위급하다는 것을 유추할 수 있기 때문에 사용자의 익명성도 꼭 지켜져야 한다.

사용자의 생체정보는 PDA(Personal Digital Assistants), 스마트폰, 웨어러블 디바이스(Wearable Device) 등과 같은 무선 단말기를 통해 서비스 제공자로 전송된다. 그런데 사용하는 기기에 따라 배터리 전력과 연산량 등에 제한이 큰 경우가 존재하기 때문에 안전성뿐만 아니라 효율성도 고려되어야 한다[4,5].

안전한 통신을 위해 사용자와 서비스 제공자간의 인증 기법은 처음에 전통적인 공개키 암호 시스템(Traditional Public Key Cryptosystem)으로 설계되었다. 전통적인 공개키 암호 시스템에서 메시지의 암호화를 위한 공개키 또는 서명 검증을 위한 검증키는 난수성을 가지고 있기 때문에 키만 가지고 정당한 사용자의 키인지 확인할 수 없다. 정당한 사용자의 키인지 확인하기 위해서는 제3의 신뢰기관(Trusted Third Authority)에서 발급한 인증서가 필요하다. 그런데 인증서를 사용하는 시스템에서는 인증서의 보관, 분배와 인증서의 유효성을 확인하기 위한 인증서 폐기 목록(Certificate Revocation List) 유지 등의 관리차원의 문제점이 존재한다. 따라서 이러한 문제점을 보완하기 위해 ID 기반 공개키 암호 시스템(ID-based Public Key Cryptosystem)이 등장하였다[6].

ID 기반 공개키 암호 시스템은 난수성을 가진 공개키를 사용하는 대신에 사용자의 ID를 공개키로 사용하기 때문에 인증서를 관리할 필요가 없다. 따라서 전통적인 공개키 암호 시스템에서 인증서를 관리해야 했던 문제점이 ID 기반 공개키 암호 시스템을 사용하면서 해결되었다. 하지만 ID 기반 공개키 암호 시스템은 전통적인 공개키 암호 시스템보다 연산량이 많다는 단점이 존재한다.

최근 WBAN에서 안전성과 효율성 문제를 해결하기 위해 ID 기반 공개키 암호 시스템을 이용한 사용자와 서비스 제공자 간의 익명 인증 기법이 활발하게 연구되고 있다[7-12]. 본 논문에서는 이전에 제안되었던 기법들의 안전성을 살펴보고, 개선된 새로운 ID 기반 익명 인증 기법을 제안한다.

본 논문의 기여도는 다음과 같다. 우선 최근 Wu et al.[10]이 제안한 ID 기반 익명 인증 기법이 위장 공격에 취약하다는 것을 보인다. 그리고 이전에 제안된 기법들[7-12]에 대해서 밝혀진 여러 가지 공격에 안전한 새로운 ID 기반 익명 인증 기법을 제안한다. 또한 제안하는 기법이 이전에 제안된 기법들과 비교했을 때 효율적이라는 것을 연산량 비교와 실제 구현을 통해 보인다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 이전에 제안된 ID 기반 익명 인증 기법들에 대해서 살펴보고, Ⅲ장에서 ID 기반 익명 인증 기법에 필요한 배경 지식을 다룬다. Ⅳ장에서는 Wu et al. 기법을 살펴보고 위장 공격에 취약하다는 것을 보인다. 또한 Ⅴ장에서 새로운 ID 기반 익명 인증 기법을 제안하고, Ⅵ장에서 제안하

는 기법의 안전성을 분석하며, Ⅶ장에서 제안하는 기법의 성능을 분석한다. 마지막으로 Ⅷ장에서 결론을 맺는다.

Ⅱ. 관련 연구

WBAN의 중요도가 높아짐에 따라 안전성과 효율성을 고려한 ID 기반 익명 인증 기법에 관한 연구가 최근 지속적으로 진행되고 있다[7-12].

2014년 Liu et al.[7]은 처음으로 WBAN 환경에서의 ID 기반 익명 인증 기법을 제안하였다. Liu et al. 기법에서 네트워크 관리자는 사용자에게 서명 인덱스를 발급하고, 서비스 제공자에게 검증 인덱스를 발급한다. 서명 인덱스와 검증 인덱스는 사용자와 서비스 제공자간에 상호 인증을 수행할 때 사용된다. 따라서 서비스 제공자는 모든 사용자에 대한 검증 인덱스 테이블을 유지해야만 한다. Liu et al. 기법이 제안된 이후 Zhao[8]는 Liu et al. 기법이 검증자 테이블 탈취 공격(Stolen Verifier-table Attack)에 취약하다는 것을 밝히고 해당 공격에 안전한 새로운 기법을 제안하였다. 검증자 테이블 탈취 공격은 공격자가 병원과 같은 서비스 제공자의 시스템에 침투해 데이터베이스를 획득하거나 변조하는 공격을 말한다.

2015년 Wang과 Zhang[9]은 Liu et al. 기법과 Zhao 기법보다 효율적인 익명 인증 기법을 제안하였다. Liu et al. 기법과 Zhao 기법의 경우 사용자는 네트워크 관리자로부터 자신의 ID에 해당하는 개인키를 발급받아 ID 기반 암호 시스템을 사용하지만 서비스 제공자는 전통적인 공개키 암호 시스템을 사용한다. 따라서 여전히 인증서 관리에 대한 문제가 남아 있다. 그리고 사용자가 서비스 제공자의 공개키를 검증하기 위해서 인증서를 받아올 때, 제3의 신뢰기관과 통신을 수행해야 하는데 통신에 소요되는 전력과 시간은 기기 내부에서 수행하는 연산보다 훨씬 크다. Wang과 Zhang 기법에서는 서비스 제공자 역시 ID 기반 암호 시스템을 사용하여 이러한 문제점을 해결하였다. 이후 Wu et al.[10]은 Wang과 Zhang 기법이 위장 공격에 취약하다는 것을 보이고 새로운 익명 인증 기법을 제안하였다.

Ⅲ. 배경 지식

3.1. WBAN

WBAN의 개체는 네트워크 관리자(Network Manager), 사용자(Client), 서비스 제공자(Application Provider)로 구성되어 있다. 네트워크 관리자는 시스템 파라미터를 생성하고 사용자와 서비스 제공자에게 ID에 해당하는 개인키를 발급해주는 신뢰기간이다. 사용자는 자신의 생체정보를 서비스 제공자에게 제공해 줌으로써 서비스를 제공받고자 하는 개체이고, 서비스 제공자는 사용자의 생체정보를 토대로 사용자에게 서비스를 제공해 준다.

WBAN 상에서 익명 인증 수행 과정은 다음과 같다[7].

1) 설정 단계: 네트워크 관리자는 시스템 파라미터, 마스터키, 공개키를 생성한다.

2) 등록 단계: 사용자와 서비스 제공자는 네트워크 관리자에게 등록을 요청하고 자신의 ID에 대한 개인키를 발급받는다.

3) 인증 단계: 사용자와 서비스 제공자는 필요시 익명 인증을 수행한다.

4) 서비스 단계: 사용자가 서비스 제공자에게 생체정보를 전달하면 서비스 제공자는 적절한 서비스를 제공한다.

그림 2는 익명 인증 수행 과정을 도식화 한 것이다.

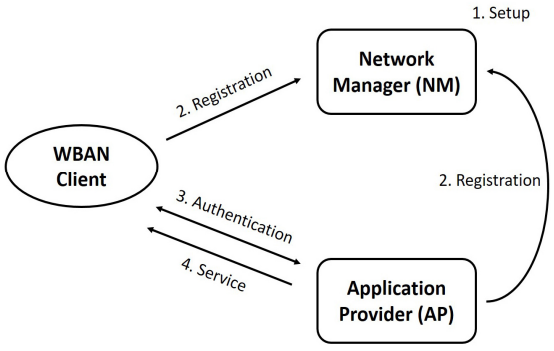

Fig. 2 Anonymous authentication protocol for WBAN

3.2. 겹선형 함수

G_1은 순환 덧셈군, G_2는 순환 곱셈군이고 모두 위수를 소수 q로 갖는다고 가정한다. P를 G_1의 생성자라고

할 때, 다음의 조건을 만족하면 $e : G_1 \times G_1 \rightarrow G_2$ 함수를 겹선형 함수라고 한다.

1) 겹선형성(Bilinearity): 임의의 원소 $Q, R \in G_1$와 $a, b \in \mathbb{Z}_q^*$에 대해서 $e(aQ, bR) = e(Q, R)^{ab}$를 만족한다.

2) 비소실성(Non-degeneracy): $e(P, P) \neq 1$를 만족한다.

3) 계산 가능성(Computability): 임의의 원소 $Q, R \in G_1$에 대해서 $e(Q, R)$를 효율적으로 계산할 수 있다.

Ⅳ. 이전 연구의 안전성 분석

우선 Wu et al.[10]이 제안한 익명 인증 기법을 살펴보고 Wu et al. 기법이 위장 공격에 취약함을 보인다.

4.1. Wu et al. 기법 리뷰

4.1.1. 설정 단계

네트워크 관리자 NM은 주어진 보안 상수 k를 이용하여 시스템 파라미터, 마스터키와 공개키를 생성한다.

큰 소수 q를 위수로 갖는 덧셈군 G_1, 곱셈군 G_2, 겹선형 함수 $e : G_1 \times G_1 \rightarrow G_2$와 G_1의 생성자 P를 선택하고, $g = e(P, P)$를 계산한다. 그리고 암호학적 해시 함수 $h : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_1 : \{0,1\}^* \times G_1 \times \{0,1\}^* \times V_C \rightarrow \mathbb{Z}_q^*$, $h_2 : \{0,1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$, $h_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $h_4 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$를 선택한다. 또한 임의의 $s_{NM} \in \mathbb{Z}_q^*$을 선택하고 $Q_{NM} = s_{NM} \cdot P$를 계산한다. (s_{NM}, Q_{NM})은 각각 NM의 마스터키와 공개키가 된다. $\{k, q, P, G_1, G_2, e, g, h, h_1, h_2, h_3, h_4, Q_{NM}\}$은 시스템 파라미터로 공개한다.

4.1.2. 등록 단계

사용자 C와 서비스 제공자 AP는 사전에 NM에게 각각 자신의 ID에 해당하는 개인키를 발급받는 절차인 등록 단계를 수행한다.

1) C와 AP는 각각 자신의 ID인 ID_C와 ID_{AP}를 NM에게 보낸다.

2) C로부터 ID_C를 받은 NM은 임의의 난수 $w_C \in \mathbb{Z}_q^*$를 선택하고 $W_C = w_C \cdot P$, $h_b = h_2(ID_C, W_C)$, $\alpha_C = w_C + h_b \cdot s_{NM}$을 계산한다. 그리고 NM은 C에게 (W_C, α_C)를 안전한 경로를 통해 전달한다. 유사한 방법으로 NM은 AP의 개인키 $S_{AP} = \frac{1}{s_{NM} + h(ID_{AP})} \cdot P$를 계산하고 안전한 경로를 통해 S_{AP}를 AP에게 전달한다.

3) C와 AP는 개인키를 안전하게 저장한다.

4.1.3. 인증 단계

등록 단계를 통해 개인키를 발급받은 C와 AP는 필요시 상호 인증을 수행하여 세션키를 확립한다. 인증 과정은 그림 3과 같다.

1) C는 임의의 난수 $r_C \in \mathbb{Z}_q^*$를 선택하고 $g = e(P, P)$, $R_C = g^{r_C}$, $K_C = r_C \cdot P$, $V_C = r_C \cdot (Q_{NM} + h(ID_{AP}) \cdot P)$, $h_a = h_1(ID_C, W_C, R_C, V_C)$, $\sigma_C = r_C + \alpha_C \cdot h_a \bmod q$, $Auth_C = E_{R_C}(ID_C, T_C, \sigma_C, K_C, W_C)$를 계산한다.($T_C$: 현재 시간) 그리고 C는 AP에게 메시지 $M_1 = \{V_C, Auth_C, T_C\}$을 전송한다.

2) AP는 $M_1 = \{V_C, Auth_C, T_C\}$을 수신하면 우선 T_C가 유효한지 확인한다. T_C가 유효하지 않다면 요청을 거부하고, 유효하다면 $R_C' = e(S_{AP}, V_C)$을 계산하여 $Auth_C$을 복호화한 후 $(ID_C, T_C, \sigma_C, K_C, W_C)$을 얻는다. 그리고 $h_a' = h_1(ID_C, W_C, R_C', V_C)$, $h_b = h_2(ID_C, W_C)$을 계산한다. $\sigma_C \cdot P = K_C + h_a' \cdot (W_C + Q_{NM} \cdot h_b)$를 만족하는지 확인하고 만족하지 않는다면 세션을 종료하고, 만족한다면 임의의 난수 $r_{AP} \in \mathbb{Z}_q^*$를 선택해서 $R_{AP} = g^{r_{AP}}$, $L_{AP} = (R_C')^{r_{AP}}$, $Auth_{AP} = h_3(T_C \| R_C' \| R_{AP} \| L_{AP} \| T_{AP} \| \sigma_C)$와 세션키 $sk_{AP} = h_4(T_C \| R_C' \| R_{AP} \| L_{AP} \| T_{AP})$를 계산한다.($T_{AP}$: 현재 시간) 마지막으로 AP는 메시지 $M_2 = \{T_{AP}, Auth_{AP}, R_{AP}\}$를 C에게 전송한다.

3) C는 $M_2 = \{T_{AP}, Auth_{AP}, R_{AP}\}$를 수신하면 먼저 T_{AP}가 유효한지 확인한다. T_{AP}가 유효하다면 $L_C = (R_{AP})^{r_C}$를 계산하고 $Auth_{AP} = h_3(T_C \| R_C \| R_{AP} \| L_C \| T_{AP} \| \sigma_C)$를 만족하는지 확인한다. 만족한다면 세션키 $sk_C = h_4(T_C \| R_C \| R_{AP} \| L_C \| T_{AP})$를 계산한다.

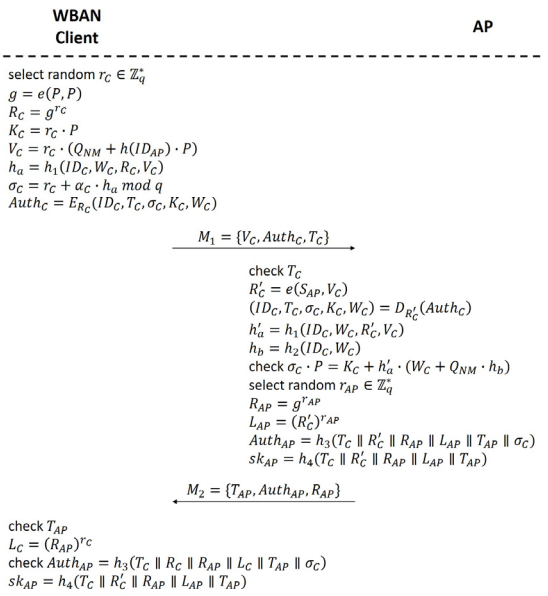

Fig. 3 Wu et al. authentication protocol

4.2. Wu et al. 기법 위장 공격

공격자는 사용자의 개인키를 알지 못하는 상태에서 다음과 같은 방법으로 ID_C를 ID로 사용하는 정당한 사용자로 위장하여 서비스 제공자와 상호 인증을 수행할 수 있다. 위장 공격 과정은 그림 4와 같다.

4.2.1. 위장 공격

공격자는 임의의 $r_C, \sigma_C \in \mathbb{Z}_q^*$를 선택한다. 그리고 $g = e(P,P)$, $R_C = g^{r_C}$, $W_C = r_C \cdot P$, $V_C = r_C \cdot (Q_{NM} + h(ID_{AP}) \cdot P)$, $h_a = h_1(ID_C, W_C, R_C, V_C)$, $h_b = h_2(ID_C, W_C)$, $K_C = -h_a \cdot W_C - h_a \cdot h_b \cdot Q_{NM} + \sigma_C \cdot P$, $Auth_C = E_{R_C}(ID_C, T_C, \sigma_C, K_C, W_C)$를 계산한다. 계산이 완료되면 $M_1 = \{V_C, Auth_C, T_C\}$를 AP에게 전송한다.

4.2.2. 정확성

Wu et al. 기법에서 K_C와 σ_C에는 난수 r_C이 포함되어 있어 난수성을 가지고 있고, 공격자가 값을 변경해도 AP는 이를 알 수 없다.

AP가 $M_1 = \{V_C, Auth_C, T_C\}$를 수신하면 $R'_C = e(S_{AP}, V_C)$을 계산하여 $Auth_C$을 복호화한다. R_C와 V_C의 값은 변경되지 않았기 때문에 AP는 R'_C을 계산하여 $Auth_C$을 복호화 할 수 있다. 그리고 AP가 $\sigma_C \cdot P = K_C + h'_a \cdot (W_C + Q_{NM} \cdot h_b)$를 만족하는지 확인하는 절차는 다음과 같은 과정에 의해 통과한다.

$$\begin{aligned} & K_C + h'_a \cdot (W_C + Q_{NM} \cdot h_b) \\ &= -h_a \cdot W_C - h_a \cdot h_b \cdot Q_{NM} + \sigma_C \cdot P \\ &\quad + h'_a \cdot W_C + h'_a \cdot Q_{NM} \cdot h_b \\ &= \sigma_C \cdot P \end{aligned} \tag{1}$$

따라서 공격자는 사용자의 개인키를 알지 못하는 상태에서 서비스 제공자와 상호 인증을 수행할 수 있다.

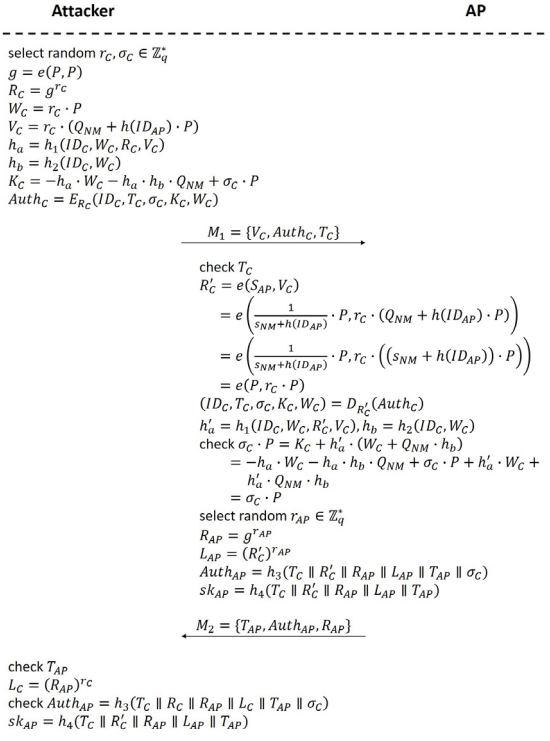

Fig. 4 Wu et al. scheme impersonation attack

Ⅴ. 제안하는 기법

5.1. ID 기반 익명 인증 기법

이전에 제안되었던 기법[7-12]에서 밝혀진 여러 가지 공격에 안전하도록 개선된 새로운 익명 인증 기법을

제안한다.

5.1.1. 설정 단계

네트워크 관리자 NM은 주어진 보안 상수 k를 이용하여 시스템 파라미터, 마스터키와 공개키를 생성한다. 큰 소수 q를 위수로 갖는 덧셈군 G_1, 곱셈군 G_2, 겹선형 함수 $e: G_1 \times G_1 \rightarrow G_2$와 G_1의 생성자 P를 선택한다. 그리고 암호학적 해시 함수 $h_1: \{0,1\}^* \rightarrow G_1$, $h_2: G_2 \rightarrow \{0,1\}^n$, $h_3: \{0,1\}^* \rightarrow \{0,1\}^m$, $h_4: \{0,1\}^* \rightarrow \{0,1\}^n$를 선택한다. 또한 임의의 $s_{NM} \in \mathbb{Z}_q^*$을 선택하고 $P_{NM} = s_{NM} \cdot P$를 계산한다. (s_{NM}, P_{NM})은 각각 NM의 마스터키와 공개키가 된다. $\{k, q, P, G_1, G_2, e, h_1, h_2, h_3, h_4, P_{NM}\}$은 시스템 파라미터로 공개한다.

5.1.2. 등록 단계

사용자 C와 서비스 제공자 AP는 사전에 NM에게 각각 자신의 ID에 해당하는 개인키를 발급받는 절차인 등록 단계를 수행한다.

1) C와 AP는 각각 자신의 ID인 ID_C와 ID_{AP}를 NM에게 보낸다.

2) C로부터 ID_C를 받은 NM은 $Q_C = h_1(ID_C)$를 계산하고 마스터키를 곱해 $S_C = s_{NM} \cdot Q_C$를 계산한다. 그리고 S_C를 C에게 안전하게 전달하고 C는 S_C를 개인키로 저장한다.

3) AP로부터 ID_{AP}를 받은 NM은 C의 등록 과정과 유사하게 $Q_{AP} = h_1(ID_{AP})$와 $S_{AP} = s_{NM} \cdot Q_{AP}$를 계산한다. S_{AP}를 AP에게 안전하게 전달하고 AP는 S_{AP}를 개인키로 저장한다.

5.1.3. 인증 단계

등록 단계를 통해 개인키를 발급받은 C와 AP는 필요시 상호 인증을 수행하여 세션키를 확립한다. 인증 과정은 그림 5와 같다.

1) C는 임의의 난수 $x \in \mathbb{Z}_q^*$를 선택하고 $Q_{AP} = h_1(ID_{AP})$, $X = x \cdot P$, $Y = x \cdot (Q_{AP} + S_C)$, $k = h_2\left(e(S_C, P_{NM})^x\right)$, $Auth_C = E_k(ID_C \| t_C \| x \cdot P_{NM})$를 계산한다.($t_C$: 현재 시간) 그리고 C는 AP에게 $\{t_C, X, Y, Auth_C\}$를 전송한다.

2) AP는 $\{t_C, X, Y, Auth_C\}$을 수신하면 먼저 t_C가 유효한지 확인한다. t_C가 유효하지 않다면 요청을 거부하고, 유효하다면 $k' = h_2\left(\frac{e(Y, P_{NM})}{e(S_{AP}, X)}\right)$을 계산하여 $Auth_C$을 복호화하고 $(ID_C \| t_C \| x \cdot P_{NM})$을 얻는다. $Q_C = h_1(ID_C)$을 계산하고 $e(P_{NM}, X) = e(x \cdot P_{NM}, P)$와 $e(Y, P) = e(Q_{AP}, X) \cdot e(Q_C, x \cdot P_{NM})$가 만족하는지 확인한다. 만족하지 않는다면 세션을 종료하고, 만족한다면 임의의 난수 $y \in \mathbb{Z}_q^*$를 선택해서 $Auth_{AP} = h_3(ID_C \| ID_{AP} \| t_C \| t_{AP} \| x \cdot P_{NM})$와 세션키 $sk = h_4(ID_C \| ID_{AP} \| t_C \| t_{AP} \| y \cdot X)$를 계산한다.($t_{AP}$: 현재 시간) 마지막으로 AP는 $\{t_{AP}, Auth_{AP}, y \cdot P\}$를 C에게 전송한다.

3) C는 $\{t_{AP}, Auth_{AP}, y \cdot P\}$를 수신하면 먼저 t_{AP}가 유효한지 확인한다. t_{AP}가 유효하다면 $Auth_{AP} = h_3(ID_C \| ID_{AP} \| t_C \| t_{AP} \| x \cdot P_{NM})$를 만족하는지 확인하고, 만족한다면 세션키 $sk = h_4(ID_C \| ID_{AP} \| t_C \| t_{AP} \| y \cdot X)$를 계산한다.

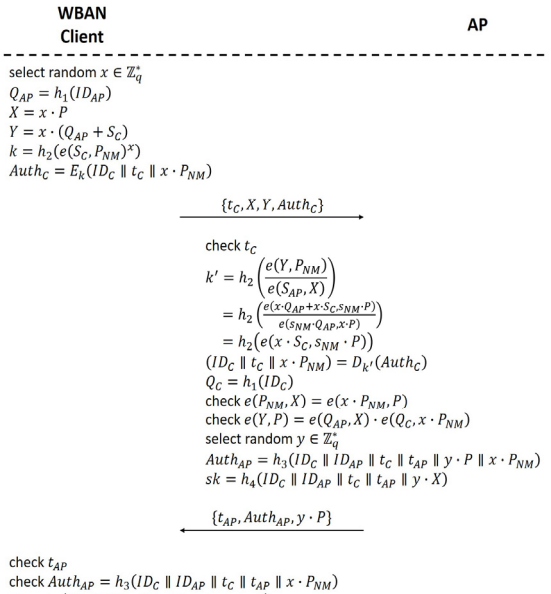

Fig. 5 Proposed authentication protocol

5.2. 정확성

AP가 $\{t_C, X, Y, Auth_C\}$를 수신하면 다음과 같이 k'을 계산한다. 이 때, $X = x \cdot P$, $Y = x \cdot (Q_{AP} + S_C)$, $P_{NM} = s_{NM} \cdot P$, $S_{AP} = s_{NM} \cdot Q_{AP}$이다.

$$\begin{aligned} & h_2\left(\frac{e(Y, P_{NM})}{e(S_{AP}, X)}\right) \\ &= h_2\left(\frac{e(x \cdot Q_{AP} + x \cdot S_C, s_{NM} \cdot P)}{e(s_{NM} \cdot Q_{AP}, x \cdot P)}\right) \\ &= h_2(e(x \cdot S_C, s_{NM} \cdot P)) \\ &= h_2(e(S_C, P_{NM})^x) \\ &= k' \end{aligned} \tag{2}$$

그리고 $e(Y, P) = e(Q_{AP}, X) \cdot e(Q_C, x \cdot P_{NM})$를 만족하는지 확인하는 과정은 다음과 같다.

$$\begin{aligned} & e(Q_{AP}, X) \cdot e(Q_C, x \cdot P_{NM}) \\ &= e(Q_{AP}, x \cdot P) \cdot e(Q_C, x \cdot s_{NM} \cdot P) \\ &= e(x \cdot Q_{AP}, P) \cdot e(x \cdot s_{NM} \cdot Q_C, P) \\ &= e(x \cdot (Q_{AP} + S_C), P) \\ &= e(Y, P) \end{aligned} \tag{3}$$

Ⅵ. 안전성 분석

6.1. 상호 인증

다음의 6.1.1 C-to-AP 인증과 6.1.2 AP-to-C 인증에 의해 제안하는 기법은 사용자와 서비스 제공자간의 상호 인증을 만족한다.

6.1.1. C-to-AP 인증

사용자는 네트워크 관리자로부터 받은 개인키 S_C를 소유하고 있다고 증명해서 자신이 정당한 사용자라는 것을 인증한다. 사용자가 서비스 제공자에게 전송하는 $Y = x \cdot (Q_{AP} + S_C)$에 개인키 S_C가 포함되어 있다. 그리고 서비스 제공자는 사용자가 Y를 S_C로 생성했는지 확인하기 위해 $e(Y, P) = e(Q_{AP}, X) \cdot e(Q_C, x \cdot P_{NM})$를 검증한다. $e(Q_C, x \cdot P_{NM}) = e(Q_C, x \cdot s_{NM} \cdot P) = e(s_{NM} \cdot Q_C, x \cdot P) = e(S_C, X)$와 같이 검증식에 포함된 $e(Q_C, x \cdot P_{NM})$에 S_C가 포함되어 있기 때문에 서비스 제공자는 사용자가 개인키를 소유하고 있는지 확인할 수 있다. 따라서 개인키를 모르는 공격자는 인증을 받을 수 없고, 제안하는 기법은 사용자의 인증을 제공한다.

6.1.2. AP-to-C 인증

서비스 제공자는 네트워크 관리자로부터 받은 개인키 S_{AP}를 소유하고 있다고 증명해서 자신이 정당한 서비스 제공자라는 것을 인증한다. 사용자가 $\{t_C, X, Y, Auth_C\}$를 서비스 제공자에게 전달하고, 서비스 제공자는 k'을 계산해 $Auth_C$를 복호화한다. 서비스 제공자는 암호화된 메시지 중 $x \cdot P_{NM}$를 포함한 해시값 $Auth_{AP} = h_3(ID_C \| ID_{AP} \| t_C \| t_{AP} \| x \cdot P_{NM})$을 사용자에게 전송해 k'을 계산했다고 증명한다. $k = h_2(e(S_C, P_{NM})^x)$에서 서비스 제공자는 S_C와 x를 알 수 없기 때문에 S_C와 x가 포함된 $Y = x \cdot (Q_{AP} + S_C)$를 이용해 k를 계산해야 한다. $e(S_C, P_{NM})^x$를 계산하기 위해 Y와 P_{NM}의 겹선형 함수 연산을 하면 $e(x \cdot Q_{AP} + x \cdot S_C, s_{NM} \cdot P)$가 되고, $e(S_C, P_{NM})^x$를 얻기 위해 $e(x \cdot Q_{AP}, s_{NM} \cdot P)$를 나눠줘야 한다. 그런데 서비스 제공자는 x를 모르기 때문에 $e(s_{NM} \cdot Q_{AP}, X)$를 계산해야 하고, 이 값은 S_{AP}를 가지고 있는 정당한 서비스 제공자만 계산할 수 있다. 따라서 개인키를 모르는 공격자는 인증을 받을 수 없고, 제안하는 기법은 서비스 제공자의 인증을 제공한다.

6.2. 익명성

사용자가 전송하는 메시지 $\{t_C, X, Y, Auth_C\}$의 X, Y 값에는 난수 x가 포함되어 있기 때문에 제3자는 이 값을 통해 사용자를 유추할 수 없다. 그리고 $Auth_C$에 사용자의 ID가 암호화 되어 있지만 암호화키는 6.1에 의해 정당한 사용자와 정당한 서비스 제공자만 계산할 수 있다. 그리고 서비스 제공자가 전송하는 메시지 $\{t_{AP}, Auth_{AP}, y \cdot P\}$에서 해시 함수의 역상 저항성에 의해 $Auth_{AP}$의 내용을 알 수 없고, $y \cdot P$는 난수이기 때문에 사용자를 유추할 수 없다. 따라서 제3자가 사용자와 서비스 제공자가 주고받는 메시지를 통해 사용자를 유추할 수 없어 제안하는 기법은 익명성을 만족한다.

6.3. 세션키 확립

사용자는 임의의 난수 x를 선택해서 서비스 제공자에게 $x \cdot P$를 전달하며, 서비스 제공자는 임의의 난수 y를 선택해서 사용자에게 $y \cdot P$를 전달한다. 그리고 $x \cdot y \cdot P$를 이용해서 세션키 $sk = h_4(ID_C \| ID_{AP} \| t_C \| t_{AP} \| y \cdot X)$를 생성한다. 공격자는 $x \cdot P$와 $y \cdot P$를 이용해서 세션키를 생성할 수 없으며, $x \cdot P$와 $y \cdot P$가 암호화 되지 않은 채 전송되지만 $Auth_C$와 $Auth_{AP}$에 $x \cdot P$, $y \cdot P$가 포함되어 있기 때문에 공격자는 값을 변경하여 공격할 수 없다. 따라서 제안하는 기법은 안전한 세션키 확립을 제공한다.

6.4. 완전 전방향 안전성(Perfect Forward Secrecy)

공격자가 사용자와 서비스 제공자의 개인키를 획득했다고 가정한다. 세션키 $sk = h_4(ID_C \| ID_{AP} \| t_C \| t_{AP} \| x \cdot y \cdot P)$는 사용자와 서비스 제공자의 ID, 현재 시간과 임의로 선택한 난수 x, y로 생성한 $x \cdot y \cdot P$ 값으로 계산된다. 공격자가 사용자와 서비스 제공자의 개인키를 알고 있다고 하더라도 $x \cdot P$와 $y \cdot P$로부터 x, y를 구할 수 없고 $x \cdot y \cdot P$를 계산할 수 없기 때문에 이전 세션의 세션키를 알 수 없다. 따라서 제안하는 기법은 완전 전방향 안전성을 제공한다.

6.5. 위장 공격

인증 단계에서 서비스 제공자는 $e(Y, P) = e(Q_{AP}, X) \cdot e(Q_C, x \cdot P_{NM})$를 만족하는지 검증한다. $e(Q_C, x \cdot P_{NM}) = e(Q_C, x \cdot s_{NM} \cdot P) = e(s_{NM} \cdot Q_C, x \cdot P) = e(S_C, X)$와 같이 검증식에 포함된 $e(Q_C, x \cdot P_{NM})$에 사용자의 개인키 S_C가 포함되어 있기 때문에 사용자가 개인키를 소유하고 있는지 확인할 수 있다. 따라서 개인키를 소유하고 있지 않은 공격자는 정당한 사용자로 위장하여 인증을 받을 수 없고, 제안하는 기법은 위장 공격에 안전하다.

6.6. 재전송 공격

사용자가 전송하는 메시지 $Auth_C$와 서비스 제공자가 전송하는 메시지 $Auth_{AP}$에는 현재 시간인 t_C와 t_{AP}가 포함되어 있다. 따라서 공격자가 이전에 전송되었던 메시지를 추후에 재전송 한다고 해도 메시지에 포함된 시간은 유효한 시간이 아니기 때문에 인증 과정에서 검증을 통과할 수 없다. 따라서 공격자는 재전송 공격을 수행할 수 없다.

6.7. 중간자 공격

6.1에 의해 개인키를 소지하고 있는 정당한 사용자와 정당한 서비스 제공자만이 상호 인증을 수행할 수 있다. 따라서 개인키를 모르는 공격자가 사용자와 서비스 제공자 사이에서 메시지를 조작하여 중간자 공격을 수행할 수 없다.

6.8. 검증자 테이블 탈취 공격

서비스 제공자는 사용자의 개인키를 검증하기 위해서 따로 검증자 테이블을 유지하고 있지 않고, 네트워크 관리자가 공개한 시스템 파라미터만을 이용해 사용자의 인증을 검증한다. 서비스 제공자는 자신의 개인키만 소지하고 있고, 이는 안전하게 보관되어 있기 때문에 제안하는 기법은 검증자 테이블 탈취 공격에 안전하다.

Ⅶ. 성능 분석

WBAN 환경에서 사용자가 사용하는 무선 단말기는 배터리 전력과 연산량에 제한이 크기 때문에 익명 인증 기법은 안전성뿐만 아니라 효율성도 매우 중요하게 고려되어야 한다. 따라서 본 논문에서 제안한 기법은 이전에 제안되었던 기법들[7-12]과 비교했을 때 연산량 측면에서 더 효율적으로 설계되었다. 서비스 제공자는 성능에 제약이 없는 개체이기 때문에 사용자 측면에서의 연산량만 분석하였다.

서비스 제공자가 전통적인 공개키 암호 시스템을 이용하는 경우에는 사용자가 인증서를 통해 검증을 해야 하기 때문에 추가적인 통신이 필요하다. 그런데 통신에 소요되는 배터리 전력과 시간은 기기 내부에서 수행되는 연산과 비교했을 때 훨씬 크다. 따라서 이전에 제안되었던 기법 중 서비스 제공자 역시 ID 기반 공개키 암호 시스템을 사용하는 기법과 본 논문에서 제안하는 기법을 비교하였다. Wang과 Zhang[9] 기법과 Wu et al.[10] 기법의 사용자 측 연산량을 본 논문에서 제안하는 기법의 사용자 측 연산량과 비교하고, 실제 환경에 구현해 소

요되는 시간을 분석하였다.

7.1. 연산량

먼저 사용자가 수행하는 연산의 횟수를 비교해 본다. 해시 함수와 같이 무시할 만한 수준의 연산은 제외하고, 상대적으로 연산량이 큰 연산들끼리 비교하였다. 연산량이 큰 연산들은 다음과 같다.

1) T_{bp}: 겹선형 함수 연산
2) T_{mul}: 스칼라 곱 연산
3) $T_{\exp}$: 모듈라(modular) 지수 연산
4) T_H: map-to-point 해시 함수 연산

표 1은 각 기법의 사용자 측 연산량을 나타내는 표이다. Wang과 Zhang 기법은 1개의 겹선형 함수 연산, 3개의 스칼라 곱 연산, 2개의 map-to-point 해시 함수 연산을 사용한다. 3개의 기법 중 유일하게 겹선형 함수 연산을 사용하기 때문에 가장 비효율적이다. Wu et al. 기법은 3개의 스칼라 곱 연산, 2개의 모듈라 지수 연산을 사용한다. 마지막으로 본 논문에서 제안하는 기법은 4개의 스칼라 곱 연산, 1개의 모듈라 지수 연산, 1개의 map-to-point 해시 함수 연산을 사용한다. Wu et al. 기법과 비교했을 때, 1개의 스칼라 곱 연산과 1개의 map-to-point 해시 함수 연산을 추가적으로 사용하지만 상대적으로 연산량이 큰 모듈라 지수 연산의 사용량이 적기 때문에 본 논문에서 제안하는 기법이 더 효율적이다.

Table. 1 Computation cost comparison

scheme	cost
Wang & Zhang scheme	$1T_{bp}+3T_{mul}+2T_H$
Wu et al. scheme	$3T_{mul}+2T_{\exp}$
our scheme	$4T_{mul}+1T_{\exp}+1T_H$

7.2. 구현

기법을 실제 환경에 구현해서 성능을 분석하였다. 구현 환경은 Nexus 5x 스마트폰이고, JPBC (Java Pairing-Based Cryptography) 라이브러리[13]를 이용하여 구현하였다. 그림 6은 사용자가 수행하는 기기 내부의 연산을 구현하여 실행 시간을 측정한 결과이다. Wang과 Zhang 기법은 411.1 ms가 소요되었고, Wu et al. 기법은 307.7 ms가 소요되었다. 그리고 본 논문에서 제안하는 기법은 가장 적은 시간인 285.3 ms을 소요하였다. Wang과 Zhang 기법과 비교해서 30.6%, Wu et al. 기법과 비교해서 7.3% 향상되었다. 7.1에서 기법들의 연산량을 비교한 분석과 구현을 통한 분석이 동일한 결과를 보였다.

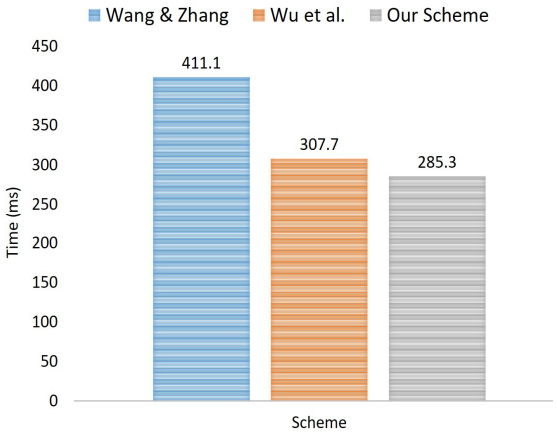

Fig. 6 Computation cost comparison

Ⅷ. 결 론

센서에서 사용자의 생체 정보를 수집하고 이를 통해 서비스를 제공받는 WBAN은 안전성 및 효율성이 매우 중요하다. 최근 Wu et al.[10]은 Wang과 Zhang[9]이 제안한 WBAN 상에서의 ID 기반 익명 인증 기법이 위장 공격에 취약하다는 것을 밝히고 새로운 익명 인증 기법을 제안하였다.

하지만 본 논문에서 Wu et al. 기법이 위장 공격에 취약하다는 것을 보여 여전히 같은 문제가 존재한다는 것을 밝혔다. 그리고 이전에 제안되었던 기법들[7-12]에서 밝혀진 공격들에 대해 안전한 새로운 기법을 제안하였다. 또한 성능 분석을 통해 이전 기법들과 비교했을 때, 더 효율적이라는 것을 보였다. 따라서 본 논문에서 제안한 WBAN 상에서의 ID 기반 익명 인증 기법은 지금까지 제안된 기법 중에서 가장 안전하고 효율적인 기법이다.

ACKNOWLEDGMENTS

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning (No. NRF-2014M3C4A 7030649)

REFERENCES

[1] T.G. Zimmerman, “Personal area networks: near-field intrabody communication,” *IBM systems Journal*, vol. 35, no. 3.4, pp. 609-617, 1996.

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

[3] IEEE Std. 802.15, *IEEE Standard for Local and Metropolitan Area Networks: Part 15.6: Wireless body area networks*, IEEE, 2012.

[4] C. Otto, A. Milenkovic, C. Sanders and E. Jovanov, “System architecture of a wireless body area sensor network for ubiquitous health monitoring,” *Journal of mobile multimedia*, vol. 1, no. 4, pp. 307-326, Jan. 2006.

[5] B. Latré, B. Braem, I. Moerman, C. Blondia and P. Demeester, “A survey on wireless body area networks,” *Wireless Networks*, vol. 17, no. 1, pp. 1-18, Jan. 2011.

[6] A. Shamir, “Identity-based cryptosystems and signature schemes,”*Workshop on the Theory and Application of Cryptographic Techniques*, Springer Berlin Heidelberg, pp. 47-53, 1984.

[7] J. Liu, Z. Zhang, X. Chen and K. S. Kwak, “Certificateless remote anonymous authentication schemes for wirelessbody area networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332-342, Feb. 2014.

[8] Z. Zhao, “An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem,” *Journal of medical systems*, vol. 38, no. 2, pp. 1-7, Feb. 2014.

[9] C. Wang and Y. Zhang, “New authentication scheme for wireless body area networks using the bilinear pairing,” *Journal of medical systems*, vol. 39, no. 11, pp. 1-8, Feb. 2014.

[10] L. Wu, Y. Zhang, L. Li and J. Shen, “Efficient and Anonymous Authentication Scheme for Wireless Body Area Networks,” *Journal of medical systems*, vol. 40, no. 6, pp. 1-12, Jun. 2016.

[11] D. He, S. Zeadally, N. Kumar and J. H. Lee, “Anonymous authentication for wireless body area networks with provable security,” *IEEE Systems Journal*, pp. 1-12, Apr. 2016.

[12] J. Liu, L. Zhang and R. Sun, “1-RAAP: An Efficient 1-Round Anonymous Authentication Protocol for Wireless Body Area Networks,”*Sensors*, vol. 16, no. 5, May 2016.

[13] The Java Pairing-Based Cryptography Library (JPBC) [Internet]. Available: http://gas.dia.unisa.it/projects/jpbc/#.V_XP3uCLR1M.

정민수(Min-Soo Jeong)

2015년 2월: 서울시립대학교 수학과 학사
2015년 3월~현재: 고려대학교 정보보호대학원 석사과정
※관심분야 : 생체인증, 무선 신체 영역 네트워크, 인증 프로토콜

석재혁(Jae Hyuk Suk)

2012년 2월: 서울시립대학교 전자전기컴퓨터공학부 학사
2014년 2월: 고려대학교 정보보호대학원 석사
2014년 3월~현재: 고려대학교 정보보호대학원 박사과정
※관심분야 : 소프트웨어 보안, 소프트웨어 역공학, 코드 난독화

이동훈(Dong Hoon Lee)

1983년: 고려대학교 경제학과 학사
1987년: Oklahoma University 전산학 석사
1992년: Oklahoma University 전산학 박사
1993년~1997년: 고려대학교 전산학과 조교수
1997년~2001년: 고려대학교 전산학과 부교수
2001년~현재: 고려대학교 정보보호대학원 교수
※관심분야 : 정보보호이론, 암호 프로토콜, USN, 키 교환, 프라이버시 향상 기술(PET), 익명성 연구