The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 4, pp.19-26, Aug. 31, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.4.19
JIIBC 2018-4-3

전천 후 생활보조 시스템을 위한 적응형 인증 프로토콜

An Adaptive Authentication Protocol for Ambient Assisted Living Systems

이명규*, 최현철**, 황보택근***

Myung-Kyu Yi*, Hyunchul Choi, Taeg-Keun Whangbo*****

요 약 최근 몇 년 동안, 인구 평균 연령의 급격히 증가하면서 다른 연령대의 사람들과 비교할 때 고령자가 더 많아지고 있다. 그 결과 산업계와 학계 모두 노인에게 건강하고 안전한 생활 방식을 제공하기 위한 여러 가지 해결 방법 개발에 집중하고 있다. 전천후 생활보조 접근법은 혁신적인 기술과 서비스를 개발함으로써 노인들의 삶의 질을 향상시키고 건강 상태를 모니터링 하는 방법이다. 전천후 생활보조 기술은 또한 노인을 위한 더 많은 안전을 제공하고 응급 대응 메커니즘, 추락 탐지 솔루션 및 비디오 감시 시스템을 제공할 수 있다. 불행히도 전천후 생활보조 데이터의 민감한 특성으로 인해, 전천후 생활보조 시스템은 무결성, 기밀성, 가용성, 익명 성 등과 같은 보안 요구 사항을 충족해야한다. 본 논문에서는 전천후 생활보조 시스템을 위한 적응형 인증 프로토콜을 제안한다. 제안된 인증 프로토콜은 전천후 생활보조 시스템에 필수적인 몇 가지 중요한 보안 요구 사항을 지원할 뿐만 아니라 다양한 유형의 공격으로부터 안전하다. 또한 보안 분석 결과를 통해 제안된 인증 프로토콜이 기존 프로토콜보다 더 효율적이고 안전하다는 것을 보여준다.

Abstract In recent years, the substantial increase in the population's average age leads to an exceeded number of older persons comparing with the number of any other age group. As a result, both industry and academia are focused on the development of several solutions aimed to guarantee a healthy and safe lifestyle to the elderly. Ambient Assisted Living (AAL) approach is the way to guarantee better life conditions for the aged and for monitoring their health conditions by the development of innovative technologies and services. AAL technologies can also provide more safety for the elderly, offering emergency response mechanisms, fall detection solutions, and video surveillance systems. Unfortunately, due to the sensitive nature of AAL data, AAL systems should satisfy security requirements such as integrity, confidentiality, availability, anonymity, and others. In this paper, we propose an adaptive authentication protocol for the AAL systems. The proposed authentication protocol not only supports several important security requirements needed by the AAL systems, but can also withstand various types of attacks. In addition, the security analysis results show that the proposed authentication protocol is more efficient and secure than the existing authentication protocols.

Key Words : AAL, healthcare, wearable computer, security, authentication

*정회원, 가천대학교 IT대학 컴퓨터공학과
**정회원, 가천대학교 공과대학 건축학과
***정회원, 가천대학교 IT대학 컴퓨터공학과 (교신저자)
접수일자 2018년 7월 20일, 수정완료 2018년 8월 9일
게재확정일자 2018년 8월 10일

Received: 20 July, 2018 / Revised: 9 August, 2018 /
Accepted: 10 August, 2018
***Corresponding Author: tkwhangbo@gachon.ac.kr
Dept. of Computer Engineering, Gachon University, KOREA

Ⅰ. 서 론

최근 몇 년 동안 급속도로 고령화되면서 전천후 생활 보조(Ambient Assisted Living, 이하 AAL) 기술이 급속히 도입되고 있다. 실제로 한국 통계청 발표에 따르면 2017년 우리나라 65세 이상 고령자는 전체 인구의 13.8%를 차지하고 있으며, 65세 이상 고령자 가구는 2045년에 47.7%가 될 것으로 전망되고 있다. 한국이 고령화 사회에서 초 고령 사회에 도달하는데 26년밖에 걸리지 않은 것은 프랑스가 154년, 미국이 94년이 걸린 것과 비교했을 때 굉장히 빠른 속도이며, 고령화가 국가적인 문제로 대두 되고 있는 상황이다. 고령화 사회를 대비하기 위해서 IT기술을 적용하여 반드시 가족과 동거하지 않더라도 노인의 독립적인 생활을 유지시키고 사회참여를 지원할 수 있는 서비스정책이 마련되어야 한다. AAL 기술은 고령자 혹은 만성 질환을 앓고 있거나 질병 회복 상태에 있는 사람들이 활동적이고 독립적인 생활이 가능하도록 혁신적인 기술과 서비스의 개발을 통해, 거주자의 거동 및 생활방식 등에 따른 행동 변화나 건강 이상 등을 실시간으로 포착하여 예방적인 조치가 가능하게 함으로써 더 나은 삶의 조건을 보장하는 방법이다. AAL 기술은 응급상황에 따른 응급 호출 및 이동편의를 증진하기 위한 서비스를 제공할 수 있고, 낙상감지, 자연재해 알림, 영상감지 시스템을 제공하여 사용자들에게 더 많은 안전을 제공할 수 있다. 또한 다른 AAL 기술은 일상생활에서의 지원을 제공하고 사용자의 행위를 모니터링하고, 응급 상황에 가족과 의료진에게 연락하여 조치를 취할 수 있도록 설계되었다. AAL 시스템은 그림 1과 같이 AAL 환경에서 데이터를 교환하고 서비스를 제공하기 위해 무선 생체신호 측정 및 의료관련 AAL 센서, 네트워크, 컴퓨터 하드웨어, 응용 프로그램 및 데이터베이스로 구성된다. 무선 생체신호 측정 및 의료관련 AAL 센서는 AAL 응용 프로그램 및 AAL 게이트웨이와 연결되어 의료 및 건강관련 데이터를 실시간 건강관리 모니터링을 위한 AAL 플랫폼에 전송한다. 무선 생체신호 측정 및 의료관련 AAL 센서는 AAL 게이트웨이 및 AAL 플랫폼에 데이터를 전송하기 위하여 무선 및 유선 네트워크와 연결되어 있다. AAL 게이트웨이는 네트워크를 통해 실시간 상태 모니터링을 위해 여러 응용 프로그램을 연결할 수 있는 연결을 제공하는 무선 라우터를 사용한다.

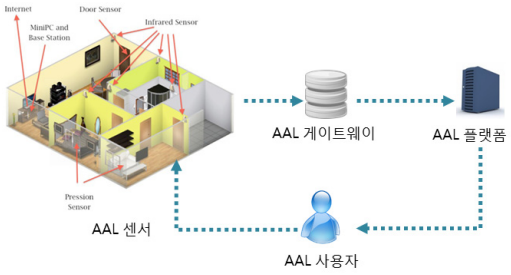

그림 1. AAL 시스템 구성도
Fig. 1. The architecture of the proposed AAL system

혈당, 혈압 및 맥박과 같은 다양한 생체신호를 모니터링하는 센서들은 건강관리 모니터링을 위한 AAL 플랫폼에 데이터를 보낼 수 있어 원격으로 의료인이 환자의 건강을 관리할 수 있다. 또한, 웨어러블 장치 및 휴대용 무선의료기기를 추가하여 의료인이 원격으로 환자의 건강을 관리할 수 있다. 이와 같이 AAL 시스템을 통하여 교환되는 정보는 매우 민감한 의료 및 민감정보를 포함하여 있으며, 보안 및 프라이버시가 중요한 문제로 대두되고 있다[1,2]. 하지만, AAL 시스템 보안에 대한 연구는 아직 미미한 상태이다. 따라서, 본 논문에서는 AAL 시스템에서 요구하는 다양한 보안 요구사항을 만족하기 위하여 AAL 데이터 특성에 기반한 적응형 인증 프로토콜을 제안하고자 한다. 제안된 적응형 인증 프로토콜은 AAL 센서가 가지고 있는 컴퓨팅 자원의 제약을 고려하여 설계되었다. 제안된 적응형 인증 프로토콜은 데이터의 민감도 특성에 따라 적응적인 보안인증을 지원할 뿐만 아니라 다양한 유형의 공격에 대비할 수 있다.

본 논문의 구성은 다음과 같다. 2장은 AAL 시스템에서의 관련연구 및 보안 요구조건을 설명하고, 3장은 제안된 적응적 인증 프로토콜을 설명한다. 4장은 제안된 기법에 대한 효율성과 안전성을 분석한다. 5장에서는 결론을 도출한다.

Ⅱ. 관련 연구

최근, 건강관리 시스템 및 AAL 시스템을 위한 인증 관련 연구들은 다음과 같다[3-7]. Lo[3]은 PKC(Public Key Cryptography)를 기반의 유비쿼터스 건강 모니터링 시스템을 위한 인증 프로토콜을 제안했다. PKC 기반 프로토콜은 고사양의 컴퓨팅 성능과 저장 공간을 필요로 하

는 모듈러 지수 연산을 요구하는 단점을 가지고 있다. Liu[4] 는 프로토콜에서의 성능을 향상시키기 위해 익명 인증서 기반의 인증 프로토콜을 제안했다. 하지만, 검증자 테이블 유지를 필수로 요구하며 복잡한 연산이 필요하는 단점을 가지고 있다. Zao[5]는 Liu[4]의 단점을 피하기 위하여 의사 신원 정보를 사용한다. 하지만, 인증의 추적이 가능한 단점이 있다. He[6]는 AAL 시스템을 위한 인증 프로토콜을 제안했다. 하지만, 사용자의 입력을 필요로 하므로 고령자를 고려해야 하는 AAL 시스템에서 적합하지 않다. 인증 프로토콜은 고령자인 사용자의 특성을 고려하여 설계되어야 한다. 인증 프로토콜은 정보 보안을 위해서는 기밀성, 무결성, 가용성과 같은 보안 요구 조건을 달성해야 한다. AAL 시스템에서 필수적으로 만족되어야 할 보안 요구 조건은 다음과 같다.

- 상호 인증 : 인증된 사용자만이 AAL 시스템에서 수집한 데이터에 접근할 수 있도록 하려면, AAL 센서, AAL 게이트웨이, 그리고 AAL 플랫폼 간의 상호 인증이 필요하다.
- 익명성 : AAL 데이터의 민감한 특성 때문에 사용자는 자신의 신원을 비밀로 유지하기를 원한다. 악의적인 상대방으로부터 사용자의 신원을 확인할 수 있는 경우 사용자의 개인 정보가 침해되어 사용자에게 불편을 초래할 수 있다. 따라서, 익명성은 AAL 인증 프로토콜의 핵심 요구사항으로 간주된다.
- 비 추적 가능성 : AAL 데이터가 암호화 되더라도 악의적인 상대방이 통신 및 정보 흐름을 추적 할 수 있으며, 이를 통하여 사용자에 대한 정보를 추측할 수 있다. 따라서, 비 추적 성은 AAL 시스템에서 중요한 보안 요구 사항으로 받아들여진다.
- 세션 키 동의 : AAL 객체 간의 상호 인증이 완료된 후에, AAL 객체간의 전송되는 데이터는 세션 키를 사용하여 암호화 되어야 한다. 따라서, 세션 키는 상호 인증 프로세스 중에 생성되어야 하며, AAL 시스템에 대한 세션 키 동의에 대한 인증 프로토콜을 제공해야 한다.
- 완벽한 전달 비밀성(Perfect Forward Secrecy) : 완벽한 전달 보안은 악의적인 사용자가 AAL 객체에 접근할 수 있더라도 이전 세션에서 생성된 세션 키에 접근할 수 없음을 의미한다. 안전한 정보 전송을 보장하기 위해 AAL 시스템에 대한 인증 프로토콜은 완벽한 전달 비밀성을 제공해야 한다.
- 공격 저항(Attack Resistance) : 인증 프로토콜은 다양한 공격에 취약하다. 보안 통신을 보장하기 위해 인증 프로토콜은 패스워드 추측공격, 재생 공격, 위장 공격, 중간자 공격, 위조/변조 공격 측면과 같은 다양한 공격을 견딜 수 있어야 한다.

III. 제안된 적응형 인증 프로토콜

본 장에서는 제안된 적응형 인증 프로토콜에 대해서 설명한다. AAL 센서는 사용자의 거주환경으로부터 심전도, 심박수, 호흡 수, 혈압과 같은 사용자의 생체정보와 온도, 습도, 조명과 같은 환경 정보를 수집한다. 다양한 AAL 센서로부터 수집된 정보는 AAL 게이트를 통하여 AAL 플랫폼으로 전송된다. 하지만, 다양한 AAL 센서로부터 수집되는 데이터의 양은 기하급수적으로 커지게 되며, 이러한 데이터를 모두 암호화/복호화를 통해 전송하기는 시스템 부하가 너무 크다. 따라서, 사용자 개인정보에 민감한 데이터와 민감하지 않은 데이터를 구분하여, 데이터의 특성에 맞는 인증을 적응적으로 수행하는 인증 프로토콜이 필요하다. 따라서, 본 논문에는 데이터의 민감도를 고려하여 적응적으로 인증을 수행하는 인증 프로토콜을 제안하고자 한다. 2장에서 언급한 보안 요구사항과 AAL 시스템의 특성을 반영하여 적응형 인증 프로토콜을 제안한다. 등록절차의 수행 전에 AAL센서와 AAL 게이트는 공개키 좌표 G, AAL 게이트와 AAL 플랫폼은 공개키 좌표 G'을 미리 공유하고 있다고 가정한다. 그림 2와 같이 자세한 등록절차는 다음과 같다.

1) 스마트 폰을 포함한 AAL 센서는 자신의 비밀키로 난수 p를 선택한다.

2) AAL 센서는 비밀키 p에 공개키 좌표 G를 곱하여 좌표 값 pG를 계산한다.

3) AAL 센서는 계산된 pG 값을 AAL 게이트웨이에 전송한다.

4) AAL 게이트웨이는 자신의 비밀키로 난수 q를 선택한다. 또한, 수신된 좌표 값 pG을 비밀키인 q과 곱을 하여 pqG을 생성한다. 생성된 pqG는 AAL 센서와 AAL 게이트웨이 간의 보안연결을 위한 공개키로 사용된다.

5) AAL 게이트웨이는 AAL 센서와 보안연결을 위하

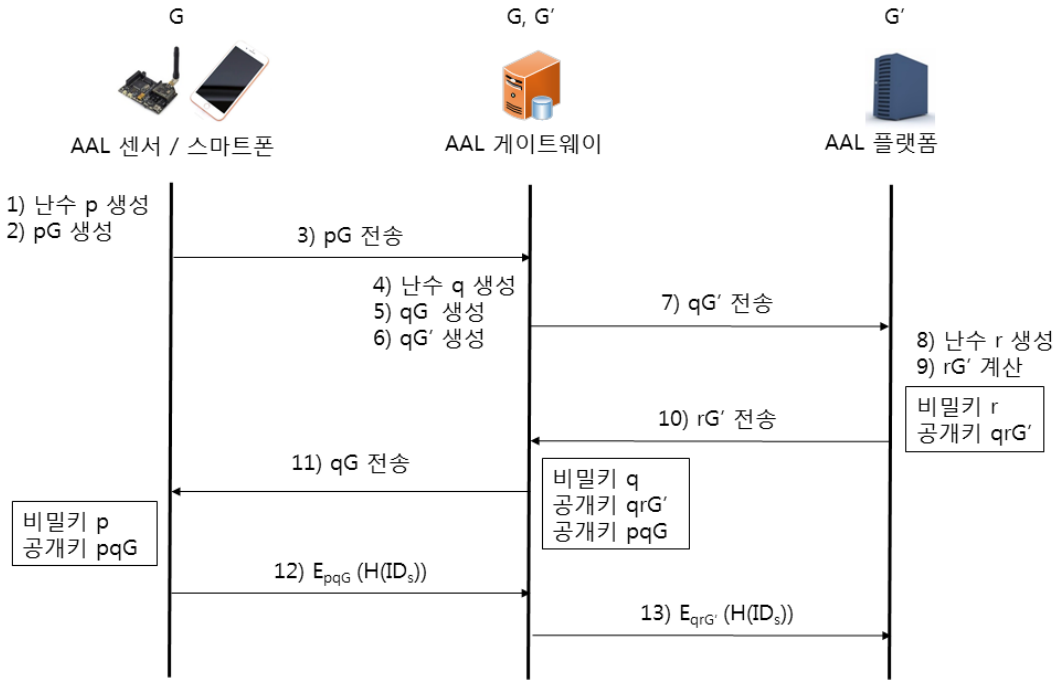

그림 2. 제안된 AAL 시스템 등록 절차
Fig. 2. The proposed registration procedure for AAL system

여 비밀키 q에 공개키 좌표 G를 곱하여 좌표 값 qG를 계산한다.

6) 또한, AAL 게이트웨이는 AAL 플랫폼과 보안연결을 위해 비밀키 q에 공개키 좌표 G'를 곱하여 좌표 값 qG'를 계산한다.

7) AAL 게이트웨이는 계산된 qG'값을 AAL 플랫폼에 전송한다.

8) AAL 플랫폼은 자신의 비밀키로 난수 r를 선택한다.

9) AAL 플랫폼은 비밀키 r에 공개키 좌표 G'를 곱하여 좌표 값 rG'를 계산한다. 또한, AAL 게이트웨이로부터 수신된 좌표 값 qG'을 비밀키인 r과 곱을 하여 qrG'을 생성한다. 생성된 qrG'는 AAL 게이트웨이와 AAL 플랫폼 간의 보안연결을 위한 공개키로 사용된다.

10) AAL 플랫폼은 계산된 rG'를 AAL 게이트웨이에 전송한다. AAL 게이트웨이는 AAL 플랫폼으로부터 수신된 좌표 값 rG'을 비밀키인 q과 곱을 하여 qrG'을 생성한다. 생성된 qrG'는 AAL 게이트웨이와 AAL 플랫폼 간의 보안연결을 위한 공개키로 사용된다.

11) AAL 게이트웨이는 5)에서 계산된 좌표 값 qG값을 AAL 센서에 전송한다. AAL 센서는 AAL 게이트웨이로부터 수신된 좌표값 qG을 비밀키인 p과 곱을 하여 pqG을 생성한다. 생성된 pqG는 AAL 센서와 AAL 게이트웨이 간의 보안연결을 위한 공개키로 사용된다.

12) AAL 센서는 자신의 ID의 해쉬 값을 공개키인 pqG로 암호화하여 AAL 게이트웨이에 등록한다.

13) AAL 게이트웨이는 저장된 pqG의 공개키를 이용하여 수신된 센서 ID의 해쉬 값을 복호화한다. AAL 게이트웨이에 수신된 센서 ID의 해쉬 값을 저장한 후, 다시 공개키인 qrG'로 암호화하여 AAL 플랫폼에 전송한다. AAL 플랫폼은 저장된 qrG'의 공개키를 이용하여 수신된 센서 ID의 해쉬 값을 복호화하고 AAL 플랫폼에 저장한다.

제안된 적응형 인증 프로토콜의 등록절차를 마치게 되면 그림 3과 그림 4와 같이 데이터의 중요도에 따라서 적응형 인증과정을 통해서 데이터를 전송할 수 있다. 그림 3은 비민감 데이터 전송을 위한 인증절차 보여준다. AAL 센서 및 스마트 폰은 각각 인증을 위한 타임스탬프 T_S, T_G를 가지고 있으며, 시간이 지나면 자동적으로 값을 증가한다. 증가한 값은 $T_s^{'}$, $T_G^{'}$ 로 표기하였다. 자세한 절차는 다음과 같다.

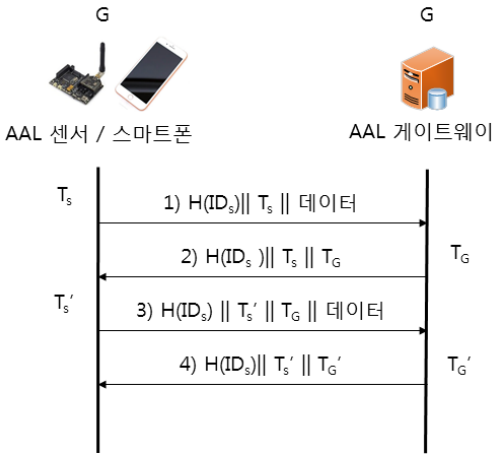

그림 3. 비민감 데이터를 위한 AAL 인증절차
Fig. 3. The authentication procedure for non-sensitive data

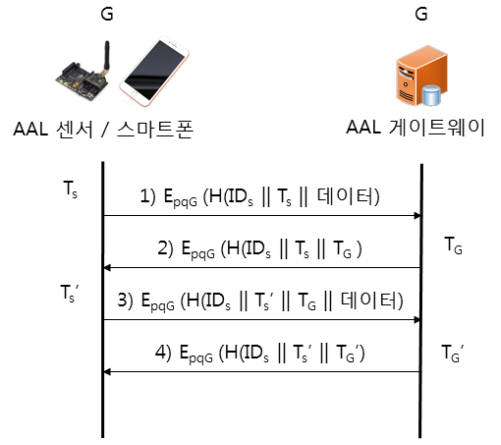

그림 4. 민감 데이터를 위한 AAL 인증절차
Fig. 4. The authentication procedure for sensitive data

1) 스마트 폰을 포함한 AAL 센서는 임시 비표로 사용되는 타임스탬프 T_s를 생성하고 자신의 ID의 해쉬 값과 측정된 데이터와 함께 AAL 게이트웨이에 전송한다.

2) AAL 게이트웨이는 수신된 센서 ID의 해쉬 값을 등록절차를 통해 저장된 센서 ID의 해쉬 값과 비교한다. 두 값이 일치하는 경우 인증을 승인하고, 일치하지 않으면 인증을 거부하고 연결을 종료한다. 인증이 성공적으로 수행되면 AAL 게이트웨이는 임시 비표로 사용되는 타임스탬프 T_G를 생성하고, 수신된 T_s 값, 그리고 등록된 센서 ID의 해쉬 값과 함께 센서로 전송한다.

3) 센서는 수신된 T_G 값을 저장하고, 수신된 T_s 값과 증가한 $T_s^{'}$ 값을 비교하고. 증가한 $T_s^{'}$ 값이 수신된 T_s 보다 크고 수신된 센서 ID의 해쉬 값이 센서 ID의 해쉬 값과 비교하여 일치하면 성공적으로 데이터 전송이 이루어졌음을 알 수 있다. 센서는 센서 ID의 해쉬 값과 $T_s^{'}$ 값, T_G 값, 그리고 추가로 측정된 데이터를 AAL 게이트웨이에 전송한다.

4) AAL 게이트웨이는 수신된 T_G 값과 증가한 $T_G^{'}$ 값을 비교하고. 증가한 $T_G^{'}$ 값이 수신된 T_G 보다 크고 수신된 센서 ID의 해쉬 값이 등록된 센서 ID의 해쉬 값이 일치하는 경우 인증을 승인하고, 일치하지 않으면 인증을 거부하고 연결을 종료한다. 인증이 성공적으로 수행되면 AAL 게이트웨이는 증가된 타임스탬프 $T_G^{'}$값, 수신한 $T_s^{'}$ 값, 그리고 등록된 센서 ID의 해쉬 값을 센서에게 전송한다.

이와 같은 과정을 통하여 비민감 데이터들에 대한 인증과 데이터 전송을 수행할 수 있다. 그림 4는 민감 데이터 전송을 위한 인증 절차을 보여주고 있다. AAL 센서와 AAL 게이트웨이 간의 전송되는 데이터가 모두 공개키 E_{pqG}를 사용하여 암호화 및 복호화되는 과정을 제외하면 그림 3과 모든 과정이 동일하다. 이와 같이 데이터의 중요도에 따라서 민감 데이터와 비민감 데이터를 적응적으로 선택하여 인증 및 전송이 가능하다.

IV. 제안방식 분석

본 장에서는 제안한 적응형 인증 프로토콜의 효율성과 안정성을 분석하고자 한다. 적응형 인증 프로토콜의 효율석 분석을 위하여 표 1과 같이 계산 비용을 위한 표기를 정의한다[7-9].

표 1. 계산 비용을 위한 표기
Table 2. Natation for computational costs

표기법	설명
T_h	해쉬 및 임시비표 연산 수행시간
T_{sym}	대칭키 암호화 혹은 복호화연산 수행시간
T_{exp}	지수함수연산 수행시간
T_{asym}	비대칭키 암호화 혹은 복호화연산 수행시간
T_{pair}	이중선형결합연산 수행시간
T_{mm}	모듈러 곱 연산 수행시간

X. Cao et. al[8] 과 J. Huang et al.[9]의 연구를 통하여 각각 (1)~(5)식과 같이 정리할 수 있다[10]

$T_h \cong 0.4T_{mm}$ (1)
$T_{sym} \cong 0.4\ T_{mm}$ (2)
$T_{exp} \cong 240\ T_{mm}$ (3)
$T_{asym} \cong 29\ T_{mm}$(4)
$T_{pair} \cong 620\ T_{mm}$ (5)

표 2. 연산 비용 비교
Table 2. Computational cost comparisons

인증 프로토콜		사용자 측 인증시간
Liu et al.[4] 인증		$3T_h + T_{sym} + 4T_{asym}$
Debiao He et. al.[6]인증		$2T_h + 2T_{sym} + 3T_{asym}$
Yi et al[7]인증		$3T_h + 2T_{asym}$
제안된 적응형 인증	민감데이터	$2T_h + 2T_{asym}$
	비민감데이터	$2T_h$

제안된 적응형 인증 프로토콜에서 AAL 센서는 1번의 임시비표 생성, 1번의 임시비표 검사, 그리고 민감데이터의 경우 각각 1번씩 공개키 기반의 암호화와 복호화를 수행한다. 따라서, 사용자 측에서 발생하는 수행시간은 표 2와 같다. (1)~(5)식을 사용하면, Liu et al.[6] 인증방식은 357.6 T_{mm}, Debiao He et. al.[7]인증방식은 88.6 T_{mm}. Yi et al[7]인증방식은 59.2 T_{mm} 으로 계산될 수 있으며, 제안된 인증방식은 민감데이터의 경우 0.8 T_m, 민감데이터의 경우 58.8 T_m로 계산될 수 있다. 따라서, 제안된 프로토콜은 AAL 센서 측에서 보다 효율성이 좋다고 말할 수 있다. 제안된 적응형 인증 프토토콜의 보안요구 사항을 고려한 안정성을 분석하면 다음과 같다.

- 상호 인증 : 초기 등록절차를 수행한 후에, AAL 센서 및 스마트폰은 AAL 게이트와 자신이 알고 있는 동일한 세션키로 사용되는 공개키를 공유한다. 공개키의 도움으로 AAL 센서 및 스마트폰은 AAL 게이트와 인증한다. 또한, AAL 게이트웨이는 AAL 센서/스마트폰만 생성할 수 있는 임시비표를 통하여 AAL 게이트웨이를 인증하고, AAL 게이트웨이는 AAL 게이트웨이만 생성할 수 있는 임시비표를 통하여 서로를 추가적으로 인증한다. 인증이 끝나면 새로운 공개키를 생성하고 이전 공개 키는 제거된다. 따라서, 상호인증 조건을 만족한다고 볼 수 있다.
- 익명성 : 익명성을 제공하기 위해 사용자는 해시된 ID 값만 사용한다 해시 된 ID값은 스마트 폰에서만 계산 할 수 있다. AAL 게이트웨이 및 AAL 플랫폼과 같은 다른 객체는 사용자 ID의 해쉬 값을 알고 있지만 해쉬 함수의 특성을 감안해 볼 때 사용자 ID의 해쉬 값에서 사용자 ID를 추출할 수 없다. 따라서, 제안된 프로토콜은 익명성을 제공한다고 말할 수 있다.
- 비 추적성 : 제안된 인증 프로토콜은 ID 해쉬 값만 존재하며 상대방에 대한 정보는 드러나지 않는다. 따라서, 악의적인 사용자가 정보의 흐름을 관찰하고 싶어도 데이터의 출처나 데이터의 수신처에 대한 정보를 전혀 알 수가 없다. 악의적인 사용자는 오직 한 쪽만을 찾을 수 있고, 반대 방향은 찾을 수 없다. 따라서, 제안된 인증 프로토콜은 추적 할 수 없는 것으로 간주된다.
- 세션 키 동의 : 제안된 인증 프로토콜의 주요 목표는 세션 키 동의이다. 제안된 인증프로토콜은 ECC 알고리즘을 사용하여 세션 키로 사용되는 공개키를 공유하며, 데이터의 암호화에 사용될 수 있다. 추가적인 암호화를 위해 대칭키 알고리즘을 사용할 수 있으며, 세션이 끝나면 사용되던 공개키는 폐기하게 된다. 따라서, 세션키 동의 조건을 만족한다고 볼 수 있다.
- 완벽한 전달 비밀성 : 제안된 인증프로토콜은 완벽한 전달 비밀성의 요구 사항을 만족시킬 수 있다. 매 세션마다 세션 키를 생성하고 상대방이 타원 점만 교환하기 때문에 악의적인 사용자가 타원 점을 얻더라도 ECC의 계산 불가능한 수학적 특성 때문에 공개키를 계산할 수 없다. 따라서, 제안된 프로토콜은 매우 효과적이고 강력한 완벽한 전달 비밀성을 제공한다.
- 공격저항 : 제안된 적응형 인증 프로토콜의 안정성을 패스워드 추측공격, 재생 공격, 위장 공격, 중간자 공격, 위조/변조 공격 측면에서 분석하고자 한다. 패스워드 추측공격은 사용자와 서버간의 통신 내용을 도청한 후, 이를 특정 보안 알고리즘에 대입하여 사용자의 패스워드를 획득함으로써 이루어진다. 하지만, AAL 객체로부터 타원 점만 획득할

수 있고, 타원 점으로부터 공개키를 획득하는 것은 이산대수의 어려움에 근거한다. 따라서, 제안된 인증 프로토콜은 패스워드 추측공격에 안전하다. 재생공격의 경우, 제안된 적응형 인증 프로토콜에서 임시비표를 사용하여 자동적으로 증가되는 값을 이전 값과 비교함으로써 재생 공격으로부터 보호할 수 있다. 위장 공격의 경우, AAL 게이트웨이에 미리 등록된 AAL 센서의 해쉬 값을 비교하여 식별자의 해쉬 값을 계산하여 무결성을 검증하므로 위장공격에 대비할 수 있다. 중간자 공격의 경우, 제안된 적응형 인증 프로토콜은 AAL 객체간의 상호인증을 제공한다. 세션 키로 사용되는 공개키와 임시비표는 이산대수의 어려움에 근거하므로 중간자 공격에 안전하다고 말할 수 있다. 마지막으로, 위조/변조 공격의 경우, AAL 객체에게 데이터를 전송 및 수신하는 경우 임시비표를 통해 전송하므로, 전송된 데이터의 변조나 위조는 쉽게 검출될 것이다. 따라서, 제안된 적응형 인증 프로토콜은 변조/위조 공격에 안전하다고 말할 수 있다. 위에서 살펴본 바와 같이 제안된 적응형 인증 프로토콜은 보안적으로 안전하며 다양한 유형의 공격으로부터 데이터를 보호할 수 있다.

V. 결 론

최근 인간의 평균수준이 증가하고 출생률이 감소하는 인구통계학적 변화로 인해 고령자가 증가하고 있으며, 고령자의 삶의 질, 복지 및 안전을 향상시키는 서비스, 제품 개발에 초점이 맞춰지고 있다. AAL은 노인과 일상적으로 특별한 도움이 필요한 사람들을 지원하는 기술 시스템을 포함하며, 사용자의 자율성을 유지하고 육성하여 생활양식과 가정 환경의 안전을 향상시키는 것에 목적이 있다. 하지만, AAL 서비스 제공을 위한 AAL 시스템은 사용자 생체신호와 같은 민감한 데이터를 수집하기 때문에 보안이 필수적이다. 본 논문에서는 AAL 시스템에서 요구하는 다양한 보안 요구사항을 만족하기 위하여 AAL 데이터의 특성을 고려한 적응적 인증 프로토콜을 제안하였다. 제안된 적응적 인증 프로토콜은 AAL시스템에 필요한 보안요구 사항을 지원할 뿐만 아니라 효율적이며, 다양한 공격에 안전하다. 제안된 기법은 향후 AAL 서비스 분야에서 유용하게 활용될 것이다.

References

[1] Personal Health Records and the HIPAA Privacy Rule.

[2] Myung-Kyu Yi, Hee-Joung Hwang, "A Study on Security Weakness and Threats in Personal Health Record Services", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.15, No. 6, pp.163-171, Dec. 31, 2015.
DOI : https://dx.doi.org/10.7236/JIIBC.2015.15.6.163

[3] C. Yeh, H. Chen, and J. Lo, "An Authentication Protocol for Ubiquitous Health Monitoring Systems," J. Medical and Biological Engineering, vol. 33, no. 4, 2013
DOI : 10.5405/jmbe.1478

[4] J. Liu et al., "Certificateless Remote Anonymous Authentication Schemes for WirelessBody Area Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, pp. 332 - 342, 2014.
DOI: https://doi.org/10.1109/TPDS.2013.145

[5] Z. Zhao, "An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem," J. Medical Systems, vol. 38, no. 2, 2014.
DOI 10.1007/s10916-014-0013-5

[6] Debiao He, Sherali Zeadally, "Authentication protocol for an ambient assisted living system", IEEE Communications Magazine, Vol. 53, No 1, pp. 71-77, Jan. 16, 2015
DOI: 10.1109/MCOM.2015.7010518

[7] Myung-Kyu Yi, Taeg-Keun Whangbo, "A Lightweight Authentication Protocol for Ambient Assisted Living Systems", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.17, No. 5, pp.9-16, Oct. 31, 2017.
DOI : https://dx.doi.org/10.7236/JIIBC.2017.17.5.9

[8] C. Yeh, H. Chen, and J. Lo, "An Authentication Protocol for Ubiquitous Health Monitoring Systems," J. Medical and Biological Engineering, Vol. 33, No. 4, pp. 415 - 419, 2013

[9] X. Cao and W. Kou, "A Pairing-Free Identity-Based Authenticated Key Agreement Scheme with

Minimal Message Exchanges," Information Sciences, Vol. 180, pp. 2895 - 2903, 2010

[10] J. Huang et al., "Robust and Privacy Protection Authentication in Cloud Computing," Int'l. J. InnovativeComputing, Information and Control International, Vol. 9, No. 11, pp. 4247 - 61, 2013

저자 소개

이 명 규(정회원)

- 2005년 2월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 10월 ~ 현재 : 가천대학교 IT대학 컴퓨터공학과 연구교수
- TTA 유헬스 프로젝트그룹 개인건강정보 표준화 전담반 위원

<주관심분야 : u-Health, Big Data, Medical Informatics, Security, Ubiquious Computing>

최 현 철(정회원)

- 2002년 2월 : 서울대학교 건축학과(공학석사)
- 2008년 8월 : 서울대학교 건축학과(공학박사)
- 2017년 2월 ~ 현재 : 가천대학교 공과대학 건축학과

<주관심분야 : IT in Architectural Field, Parametric Design, AAL Healthcare Service>

황 보 택 근(정회원)

- 1988년 : CUNY 컴퓨터공학 졸업 (공학석사)
- 1995년 : Stevens Institute of Technology 컴퓨터공학 졸업 (공학박사)
- 1997년 ~ 현재 : 가천대학교 IT대학 교수

<주관심분야 : 영상처리, 패턴인식, 컴퓨터그래픽스, 3D 게임엔진, 의료정보>

※ 이 연구는 2018년도 국토교통과학기술진흥원 연구비 지원에 의한 결과의 일부임
(과제번호 : 18RERP-B090228-05)