The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 5, pp.9-16, Oct. 31, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.5.9
JIIBC 2017-5-2

전천 후 생활 지원 시스템을 위한 경량 인증 프로토콜

A Lightweight Authentication Protocol for Ambient Assisted Living Systems

이명규*, 황보택근**

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

요 약 향상된 의료 기술과 건강관리 기술의 최근 발전으로 인해 지난 수십 년 동안 기대 수명이 꾸준히 늘게 되었다. 그 결과 세계 인구는 빠르게 고령화되고 있다. 고령자의 복지를 향상시키고 일상생활에서 독립성을 제공하는 해결책을 기반으로 하는 정보통신기술 지원에 대한 다양한 연구가 진행되고 있다. 전천후 보조 생활은 개인의 일상생활 및 근무 환경에서 정보 통신 기술을 사용하여 더 오래 활동성을 유지하고 사회활동을 할 수 있도록 하여 노년기에 독립적으로 살아갈 수 있도록 하는 것으로 정의된다. 전천후 생활 보조 시스템에서 전송되는 정보는 매우 민감한 정보이므로, 이러한 데이터의 보안 및 개인 정보는 중요한 문제로 대두되고 있다. 본 논문에서는 전천후 보조 생활 시스템을 위한 새로운 경량 인증 프로토콜을 제안한다. 제안된 인증 프로토콜은 전천후 생활 지원 시스템에 필요한 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 Recent advances in healthcare technologies along with improved medical care have led to a steady increase in life expectancy over the past few decades. As a result, the world population is aging rapidly. Various researches have been carried out to provide information and communication technologies based solutions that enhance the well-being of elderly people and provide them with a well margin of independency in their daily life. Ambient assisted living can be defined as the use of information and communication technologies in a person's daily living and working environment to enable them to stay active longer, remain socially connected and live independently into old age. Since the information transmitted in ambient assisted living systems is very sensitive, the security and privacy of such data are becoming important issues that must be dealt with. In this paper, we propose a novel lightweight authentication protocol for the ambient assisted living systems. The proposed authentication protocol not only supports several important security requirements needed by the ambient assisted living 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

Ⅰ. 서 론

최근 의료기술의 발달로 인해 인간의 기대 수명이 점차 증가하고 있으며, 출산율의 저하와 노인인구 증가로 인해 전 세계적으로 고령화가 빠르게 진행되고 있다. 특히, 한국의 경우 고령화 율은 상대적으로 낮은 편이지만

*정회원, 가천대학교 IT대학 컴퓨터공학과
**정회원, 가천대학교 IT대학 컴퓨터공학과 (교신저자)
접수일자: 2017년 9월 11일, 수정완료: 2017년 10월 5일
게재확정일자: 2017년 10월 13일

Received: 11 September, 2017 / Revised: 5 October, 2017 / Accepted: 13 October, 2017
**Corresponding Author: tkwhangbo@gachon.ac.kr
Dept. of Computer Engineering, Gachon University, KOREA

고령화 속도가 가장 빠른 것으로 나타나고 있다. 한국은 2000년에 총인구 대비 65세 이상 노인인구 비율이 7.2%를 기록하며 고령화 사회에 진입하였으며, 2019년에 노인인구가 14%인 고령화 사회가 될 전망이다. 더욱이 고령사회 진입 후 불과 8년 만인 2026년에 초 고령사회로 진입할 것으로 예상되어 향후 인구사회 구조 변화에 대비할 시간이 절대적으로 부족한 상황이며, 노인인구의 증가와 의료기술 발달로 의료비 지출도 급증하고 있는 상황이다. 따라서, 질병에 조기에 예측하고 건강을 관리하여 국민과 국가의 의료비 부담을 줄일 수 있도록 정보기술과 의료 서비스 기술이 융합된 형태인 u-헬스케어 기술 개발이 필요하며, 선진국에서는 이미 고령화 사회를 대비하기 위해 이러한 u-헬스케어 기술을 활용하는 다양한 정책과 프로젝트를 추진 중이다.

고령화 인구의 삶의 질을 보장하는 문제는 미래에 국가의 보건 및 사회 시스템의 재정적 안정에 치명적인 위험이 될 수도 있다. 노인들이 노년에도 활동적이고 적극적으로 생활하고 최대한 오래 자신의 가정에서 살 수 있도록 하는 방안이 시급한 상황이며, 노인이 활동적이고 독립적으로 생활하기 위해서는 의료 및 헬스케어 기기에서 의료기기 및 센서, 활동 모니터링 시스템에 이르는 기술들이 모두 서로 연결되어야 한다. 전천 후 생활지원(Ambient Assisted Living, 이하 AAL)는 개인의 일상생활 및 근무 환경에서 정보 통신 기술을 사용하여 더 오래 활동성을 유지하고 사회활동을 할 수 있도록 하여 노년기에 독립적으로 살아갈 수 있도록 하는 것으로 정의된다. AAL 시스템은 노약자가 개인 건강관리를 위해 정보통신 기술을 사용하여 선호하는 환경에서 독립적으로 생활하도록 제공하는데 목적이 있다. 또한, 혁신적인 기술과 다양한 의료 서비스의 개발을 통해 고령자 뿐 아니라 만성 질환을 앓고 있는 사람들이나 질병 회복 상태에 있는 일반인에게 더 나은 삶의 조건을 보장 할 수 있다. AAL 시스템은 건강 모니터링을 위한 의료센서, 컴퓨터, 무선 네트워크 및 소프트웨어 응용 프로그램으로 구성된다. 비접촉 특성을 가진 AAL 센서는 옷, 신발, 시계, 안경 등에 내장되어 사용자는 센서착용을 의식하지 못하며 이동할 경우 무선통신 인터페이스를 제공한다. 이러한 비접촉 특성은 사용자의 요구가 없더라도 거주 환경을 탐색하여 거주자의 거동과 생활방식 등에 따른 행동 변화나 건강 이상 등을 실시간으로 감지한다. 또한, AAL 시스템은 비상 대응 메커니즘, 낙상 탐지 솔루션, 비디오 감시 시스템 등의 기술을 통하여 노약자에게 더 많은 안전을 제공 할 수 있으며, 일상생활 지원, 일상생활 활동 모니터링, 주요 행위 인지 알림과 같은 서비스를 통하여 노약자 가족과 의료진을 빠르게 연결하여 응급 상황에 대응할 수 있도록 도와준다. 최근 개인건강 모니터링과 원격의료 서비스를 위해 AAL 시스템과 AAL 어플리케이션, AAL 센서들의 수요가 급증하고 있다.

AAL 센서는 심전도, 심박 수, 호흡 수, 혈압과 같은 사용자의 생체정보와 온도, 습도, 조명과 같은 환경 정보를 수집한다. AAL 센서로부터 수집된 혈액형, 키, 체중, 나이, 보호자 연락처와 같은 개인 식별정보와 혈당, 혈압, 혈압, 간 수치와 같은 생체정보는 민감한 의료정보가 될 수 있으므로 AAL 시스템 내에서 교환되는 정보는 기밀성, 무결성 및 가용성과 같은 보안 요구 사항을 충족해야 한다[1-4]. 이러한 요구사항을 충족시키기 위해서는 AAL 시스템을 통해 교환되는 데이터의 안전성을 보장하고 허가된 사용자만이 AAL 서비스에 접근할 수 있도록 해야 한다. 또한, AAL 센서는 연산능력과 전원소모와 같은 컴퓨팅 자원의 제한 문제를 가지고 있기 때문에 보안 메커니즘을 설계할 때 이러한 AAL 시스템의 특성을 고려해야 한다. 이와 같이 AAL 시스템을 통하여 교환되는 정보는 매우 민감한 개인정보를 포함하여 있으며, 보안 및 프라이버시가 중요한 문제로 대두되고 있다. 하지만, AAL 시스템 보안에 대한 연구는 아직 미미한 상태이다. 따라서, 본 논문에서는 AAL 시스템에서 요구하는 다양한 보안 요구사항을 만족하기 위하여 AAL 시스템의 특성을 반영한 경량 인증 프로토콜을 제안하고자 한다. 제안된 경량 인증 프로토콜은 AAL 센서가 가지고 있는 컴퓨팅 자원의 제약을 고려하여 설계되었다. 제안된 경량 인증 프로토콜은 필요한 보안요구 사항을 지원할 뿐만 아니라 다양한 유형의 공격에 대비할 수 있다.

본 논문의 구성은 다음과 같다. 2장은 AAL 시스템에서의 보안위협과 관련 연구를 설명하고, 3장은 AAL 시스템 구조 및 제안된 경량 인증 프로토콜을 설명한다. 4장은 제안된 기법에 대한 효율성과 안전성을 분석한다. 5장에서는 결론을 도출한다.

II. 관련 연구

최근, AAL 시스템을 위한 인증 관련 연구들은 다음과

같다. Yeh et al.[5]은 u-헬스케어 모니터링 시스템을 위한 인증기법을 제안했다. 제안된 시스템은 무선 신체 영역 네트워크(Wireless Body Area Networks. 이하 WBANs), 센서, 개인용 모바일 장치 및 의료용 서버로 구성되며, 각 장치는 배타적 인증과 안전한 통신을 보장하기 때문에 전송된 환자 관련 데이터가 수정 및 차단 공격뿐만 아니라 데이터 작성 공격으로부터 보호 될 수 있다. 하지만, 제안된 인증 프로토콜은 제한된 자원을 가진 모바일 장치에 적합하지 않으며 사용된 암호화 알고리즘은 모바일 장치가 가진 컴퓨터 성능과 저장 공간을 초과할 수 있다. Liu et al.[6]은 타원곡선암호(Elliptic Curve Cryptography, 이하 ECC로 표기)을 사용하여 WBANs 환경에서 익명 인증 프로토콜을 제안했다. ECC는 사용되는 키 크기가 작기 때문에 컴퓨팅 자원이 제한적인 환경에 적합하다. 제안된 인증기법은 WBANs 환경에서 의료서버를 접근할 때 잠재적인 WBANs 사용자의 프라이버시를 보호하기 위해서 서명이 필요 없는 원격인증 프로토콜을 제안했다. 하지만, 제안된 기법은 계산의 복잡도가 높아 만족스러운 성능을 얻기가 쉽지 않다. Debiao He et. al.[7]은 AAL 시스템 환경에서 ECC를 사용한 인증기법을 제안하였다. 제안된 기법에서는 서명이 필요 없는 공개키 암호화와 검증자 테이블과 같이 복잡한 공개키 문제를 피하기 위하여 식별자 기반 공개키 암호화 인증 기법을 사용한다. 하지만, 제안된 기법은 제한적인 자원을 가지고 있는 AAL 센서의 특성을 반영하지 못하고 있다.

정보 보안을 위해서는 기밀성, 무결성, 가용성과 같은 보안 요구조건을 달성해야 한다. AAL 시스템에서 보안 요구조건을 저해할 수 있는 보안 위협은 다음과 같다.

- 도청 (Eavesdropping) : 도청은 AAL 사용자의 생체 신호와 같은 민감한 의료 데이터의 손실이나 개인 정보의 유출과 같은 잘못된 결과를 초래할 수 있다. 도청 위협을 해결하기 위해 데이터를 암호화하여 기밀성을 유지해야한다. 또한, AAL 센서의 제한된 자원 때문에 경량화 된 암호 메커니즘을 채택해야 한다.

- 흐름차단(Interruption) : 시스템의 일부가 파괴되거나 사용할 수 없게 된 상태를 말하며, 보안 요구 요건 중에서 가용성에 대한 위협이다. AAL 센서에서 AAL 플랫폼으로 전달되는 데이터를 가로 챌 경우 민감한 개인의 의료데이터가 유실될 수 있다. 이 공격은 AAL 게이트웨이에서 인증된 AAL 센서만 데이터를 전송하게 함으로써 공격을 완화할 수 있다.

- 가로채기(Interception) : 인가 받지 않은 제 3자가 수집된 AAL 시스템 객체에 접근하는 경우이며, 보안 요구 조건 등 비밀성에 관한 위협이다

- 변조(Modification) : 변조는 인가받지 않은 제3자가 AAL 시스템 객체에 접근 할 뿐 아니라 내용을 임의적으로 수정하는 경우를 의미하며, 보안 요구 조건 중 무결성에 대한 위협이다. 이 공격은 AAL 플랫폼에 수신된 AAL 데이터에 대한 응답을 생성하기 전에 수신된 암호문의 정확성을 검사함으로써 공격을 완화할 수 있다.

- 위조(Fabrication) : 위조는 인가받지 않는 제3자가 위조된 AAL 시스템 객체를 삽입하는 경우를 의미하며, 이는 보안 위협 중 무결성에 대한 위협이다. 공격자는 전송 된 정보를 삽입, 변경 또는 삭제하기 위해 AAL 센서와 AAL 플랫폼 사이의 데이터를 가로 챌 수 있다. 따라서 무결성 검사 메커니즘이 필요하다.

또한, AAL 시스템을 위한 인증 프로토콜은 AAL 시스템 객체간의 배타적 인증, 객체간의 키 동의, 객체 간의 익명성, 무결성과 같은 다양한 공격에 대한 저항을 고려해야 한다. 이와 같이 다양한 보안위협을 고려하여 제안된 인증 프로토콜의 보안 요구 사항은 다음과 같이 정의된다.

- 배타적 인증 : AAL 시스템의 객체는 데이터를 전송하기 위한 상대의 공개키를 인증서버로부터 받아야 한다.

- 키 동의 : AAL 시스템의 객체는 세션이 유지되는 동안 암호화를 위한 세션 키를 만들어야 한다.

- 익명성 : AAL 센서의 식별자는 익명성을 유지해야 하며 AAL 센서의 식별자가 노출되지 말아야 한다.

- 무결성 : 보안되지 않은 채널을 통한 전송 메시지는 상대방에 의해 변경되지 않고 수신 당사자에서 검증 가능해야한다.

- 다양한 공격에 대한 보호 : 제안된 인증 프로토콜은 패스워드 추측공격, 전방향 안정성, 재생 공격(Relay attack), 위장 공격(Impersonation attack), 중간자 공격(Man-in-the-middle attack), 위조/변조 공격과 같은 다양한 공격으로부터 데이터를 안전하게 보호해야 한다.

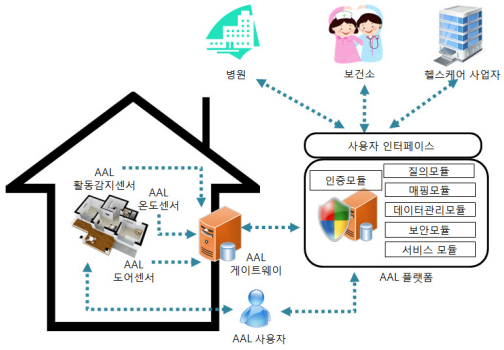

그림 1. AAL 시스템 구성도
Fig. 1. The architecture of the proposed AAL system

III. 제안된 경량 인증 프로토콜

본 장에서는 제안된 AAL 시스템 구조 및 경량 인증 프로토콜에 대해서 설명한다.

1. AAL 시스템 구조

AAL 시스템의 구조는 그림 1과 같다. AAL 서비스를 제공하는 대부분의 AAL 시스템은 공통적으로 AAL 센서, AAL 게이트웨이, AAL 서비스를 위한 AAL 플랫폼으로 구성되어 있다[5-7]. 인증서버의 공개키는 안전한 채널을 통하여 AAL 게이트웨이와 AAL 플랫폼이 공유하고 있다고 가정한다. 또한, AAL 센서의 식별자(ID_S)는 AAL 게이트웨이에 미리 등록되어 있으며 AAL 게이트웨이의 공개키는 AAL 센서가 이미 알고 있다고 가정한다. 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. 기본적으로 AAL 게이트는 사용자의 거주환경 내에 위치하며 인터넷을 통하여 AAL 서비스를 제공하는 AAL 플랫폼과 연결된다. AAL 사용자의 거주환경 내에 위치하는 AAL 센서와 AAL 게이트웨이 간의 데이터 교환은, 위협에 노출되어있는 인터넷을 통하여 데이터 교환이 이루어지는 AAL 게이트웨이와 AAL 플랫폼 구간보다 안전하다고 볼 수 있다.

이러한 특성을 고려하여, 본 논문에서는 AAL 센서와 AAL 게이트웨이 간 인증은 시스템 부하가 적은 임시비표와 해쉬 값을 사용하고, AAL 게이트웨이와 AAL 플랫폼 간의 인증은 해쉬 값, 임시비표, 그리고 인증서버를 통한 공개키 획득을 통해 AAL 시스템 객체 간의 안전한 연결을 설정하고자 한다.

2. 제안된 경량 인증 프로토콜

본 절에서는 2장에서 언급한 보안 요구사항과 AAL 시스템의 특성을 반영하여 그림 2와 같이 경량 인증 프르토콜을 제안한다. AAL 시스템을 위한 경량 인증 프로토콜의 자세한 절차는 다음과 같다.

1) AAL 센서는 자신의 식별자 해쉬 값 $H(ID_S)$과 AAL 센서가 생성한 임시비표 N_s를 AAL 게이트웨이의 공개키로 암호화하여 AAL 게이트웨이에게 전송한다.
2) AAL 게이트웨이는 미리 등록되어 있는 AAL 센서 식별자의 해쉬 값을 계산하고, AAL 센서로부터 받은 해쉬 값을 비교해본다. 두 개의 해쉬 값이 동일하면 인증단계를 진행하고, 일치하지 않으면 인가되지 않은 센서로 가정하고 인증단계를 종료한다. AAL 센서와 성공적인 인증이 끝나면 AAL 센서가 생성한 임시비표를 AAL 게이트웨이의 비밀키로 암호화해서 AAL 센서에게 전달해서 인증이 성공적으로 이루어졌음을 알린다.
3) AAL 게이트웨이는 AAL 플랫폼과 안전한 연결을 설정하기 위한 의도를 인증서버에 알리기 위하여, AAL 게이트웨이의 식별자 ID_G, AAL 플랫폼의 식

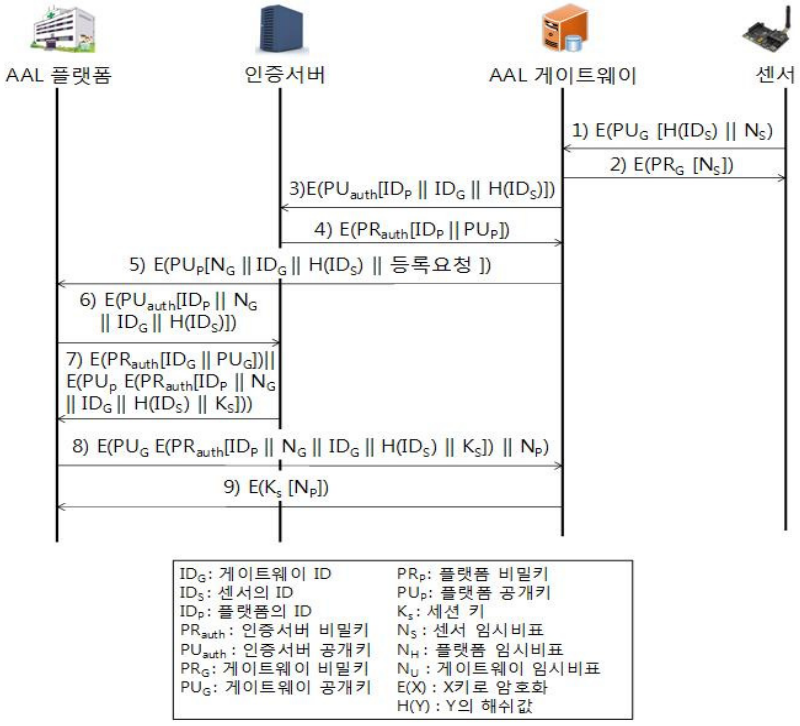

그림 2. 제안된 경량 인증 프로토콜
Fig. 2. The proposed lightweight authentication protocol

별자 ID_P, 센서 식별자의 해쉬 값 $H(ID_S)$을 인증서버의 공개키 PU_{auth} 암호화하여 인증서버로 전송한다.

4) 인증서버는 AAL 게이트웨이의 식별자와 센서 식별자의 해쉬 값을 인증서버에 등록한다. 그리고, 인증서버는 AAL 플랫폼의 식별자 ID_P와 AAL 플랫폼의 공개키 PU_P를 복사한 후 인증서버의 개인키 PR_{auth}로 암호화하여 AAL 게이트웨이에게 반송한다.

5) AAL 게이트웨이는 AAL 플랫폼에게 안전한 연결을 설정하기 위하여 등록요청 메시지를 보낸다. 등록요청 메시지는 AAL 게이트웨이의 식별자와 센서 식별자의 해쉬 값, 그리고 AAL 게이트에서 생성한 임시비표 N_G와 함께 AAL 플랫폼의 공개키로 암호화한다.

6) AAL 플랫폼은 인증서버에게 AAL 게이트웨이 공개키와 세션 키 K_S를 요청하기 위하여 AAL 플랫폼의 식별자, AAL 게이트웨이 식별자, AAL 센서의 해쉬 값, AAL 게이트웨이의 임시비표를 인증서버의 공개키로 암호화하여 전송한다. AAL 플랫폼은 AAL 게이트웨이에서 발행한 임시비표를 포함함으로써 인증 서버가 AAL 게이트웨이의 임시비표에 세션 키를 서명할 수 있도록 한다.

7) 인증서버는 AAL 플랫폼에게 AAL 게이트웨이의 식별자 ID_G와 AAL 게이트웨이의 공개키 PU_G를 복사한 후 인증서버의 비밀키로 암호화한다. 또한, AAL 플랫폼 식별자, AAL 게이트웨이의 임시비표, AAL 게이트웨이 식별자, 센서 식별자의 해쉬 값, 세션 키를 인증서버의 비밀키로 암호화한 후 AAL 플랫폼의 공개키로 암호화하여 AAL 플랫폼에 전송한다. 세션 키 K_s는 AAL 플랫폼을 대신하여 인증서버에 의해 만들어지고 AAL 게이트웨이의 비표에 결부된 세션 키이다. 즉, K_s 와 AAL 게이트웨이 비표 N_G의 결합은 AAL 게이트웨이에게 세션 키 K_s 가 투명하다는 것을 보장한다. 이 세 가지 정보는 인증서버의 비밀 키를 이용하여 암호화됨으

로 AAL 플랫폼에게 인증서버에 의해서 만들어졌음을 검증한다. 이 정보는 또한 AAL 플랫폼의 공개키를 사용하여 암호화됨으로써 사용자와의 부정한 연결을 설립하는 시도에 이용하지 못하게 한다.

8) AAL 플랫폼은 AAL 게이트웨이에게 세션 키를 전송하기 위해서 AAL 플랫폼 식별자, AAL 게이트웨이의 임시비표, AAL 게이트웨이 식별자, 센서 식별자의 해쉬 값, 세션 키를 인증서버의 비밀키로 암호화한 후 AAL 플랫폼에서 생성된 임시비표 N_p와 함께 AAL 게이트웨이의 공개키로 암호화하여 AAL 게이트웨이에 전송한다.
9) AAL 게이트웨이는 세션 키 K_s를 회수하여 AAL 플랫폼의 임시비표를 암호화하여 AAL 플랫폼에 반송한다. 이 마지막 메시지는 세션 키에 대한 정보가 안전하다는 것을 보장한다. AAL 플랫폼과 AAL 게이트웨이는 생성된 세션 키를 사용하여 세션기간동안 센서에서 수집된 정보를 전송할 수 있다.

제안된 경량 인증 프로토콜을 통하여 AAL 시스템 간의 객체, 즉 AAL 센서, AAL 게이트웨이, AAL 플랫폼의 인증이 성공적으로 이루어지면 AAL 센서는 AAL 게이트웨이의 공개키로 암호화하여 데이터를 전송하고, AAL 게이트웨이는 세션 키를 이용하여 AAL 플랫폼에게 데이터를 전송할 수 있다.

IV. 제안방식 분석

본 장에서는 제안한 경량 인증 프로토콜의 효율성과 안정성을 분석하고자 한다. 경량 인증 프로토콜의 효율석 분석을 위하여 표 1과 같이 계산 비용을 위한 표기를 정의한다[7-10]. X. Cao et. al[8] 과 J. Huang et al.[9]의 연구를 통하여 각각 (1)~(5)식과 같이 정리할 수 있다[7]

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

표 1. 계산 비용을 위한 표기
Table 1. 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

제안된 경량 인증 프로토콜에서 AAL 센서는 1번의의 해쉬 값 계산, 1번의 임시비표 생성, 1번의 임시비표 검사, 그리고 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}으로 계산될 수 있으며, 제안된 경량 인증 프로토콜은 59.2 T_{mm} 으로 계산될 수 있다. 따라서, 제안된 프로토콜은 AAL 센서 측에서 보다 효율성이 좋다고 말할 수 있다.

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

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

제안된 경량 인증 프로토콜의 안전성을 패스워드 추측공격, 전방향 안정성, 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 게이트웨이, AAL 플랫폼, 인증서버로부터 모두 공개키 정보만 획득할 수 있고, 공개키로부터 비밀키를 획득하는 것은 이산대수의 어려움에 근거한다. 따라서, 제안된 경량 인증 프로토콜은 패스워드 추측공격에 안전하다. 전방향 보안성은 공격자가 오랜 기간동안 사용하는 비밀키를 알고 있을 때 이전 세션키를 회득할 수 있는지 여부를 통해 결정

한다. 본 논문에서 제안한 기법에서 세션 키는 세션이 유지되는 기간만 유효하고 세션이 종료된 이후에는 새로운 보안연결을 통해 세션 키가 생성되므로 전방향 안정성을 제공한다. 재생공격의 경우, 제안된 경량 인증 프로토콜에서 임시비표는 AAL 센서, AAL 게이트웨이, AAL 플랫폼 간의 교환되는 모든 메시지에 사용된다. 수신된 임시비표는 기존에 수신된 임시비표와 비교함으로써 재생공격으로부터 보호할 수 있다.

위장 공격의 경우, 악의적인 AAL 센서들이 AAL 게이트웨이에 등록하려면 자신의 식별자의 해쉬 값을 전송해야 한다. AAL 게이트웨이에 미리 등록된 AAL 센서의 해쉬 값을 비교하여 식별자의 해쉬 값을 계산하여 무결성을 검증하므로 위장공격에 대비할 수 있다. 또한, 인증서버, AAL 게이트웨이, AAL 플랫폼으로 전송되는 모든 데이터는 각자가 소유한 비밀키 외에는 복호화 할 수 없으므로 기밀성을 보장하며, AAL 게이트웨이와 AAL 플랫폼은 인증 서버를 통해 전송하고자 하는 수신자의 공개키를 받을 수 있고 인증서버에 의해 복사된 AAL 게이트웨이와 AAL 플랫폼의 공개키는 인증서버의 개인키로 암호화되어 인증서버에 의해 생성되었음을 보장하므로 기밀성을 보장한다. 마지막으로, AAL 플랫폼의 경우 AAL 게이트웨이에서 전달한 AAL 센서 식별자의 해쉬 값으로부터 AAL 센서의 식별자를 유출할 수 없으므로 배타적인 인증을 가능하게 한다. 따라서 제안된 경량 인증 프로토콜은 위장공격에 안전하다고 말할 수 있다.

중간자 공격의 경우, 제안된 경량 인증 프로토콜은 AAL 센서, AAL 게이트웨이, AAL 플랫폼 간의 배타적인 인증을 제공한다. 또한, AAL 게이트웨이에서 생성한 임시비표와 세션키, AAL 플랫폼에서 생성한 임시비표와 세션 키의 결합은 세션 키가 투명하다는 것을 보장한다. 또한, 세션 키와 임시비표는 공개키로 암호화되어 이산대수의 어려움에 근거하므로 제안된 경량 인증 프로토콜은 중간자 공격에 안전하다고 말할 수 있다. 위조/변조 공격의 경우, AAL 센서, AAL 게이트웨이, AAL 플랫폼은 수신된 메시지에 대한 응답을 생성하기 전에 임시비표를 통해 수신된 암호문의 정확성을 검사한다. 제안된 프로토콜에 의해 사용된 암호화 알고리즘이 안전하기 때문에, 전송된 데이터의 변조나 위조는 쉽게 검출될 것이다. 따라서, 제안된 경량 인증 프로토콜은 변조/위조 공격에 안전하다고 말할 수 있다. 위에서 살펴본 바와 같이 제안된 경량 인증 프로토콜은 보안적으로 안전하며 다양한 유형의 공격으로부터 데이터를 보호할 수 있다.

V. 결 론

노약자의 삶의 질은 기능적인 어려움 없이 독립적이고 건강한 생활을 영위할 수 있는 신체활동의 수준에 따라 좌우된다. AAL은 노약자들에게 정보통신기술을 활용한 공공서비스 제공을 통해 의료 모니터링, 안전 및 보안, 응급시스템 사회참여와 같은 독립적인 생활을 지원하는 것을 목표로 한다. AAL 서비스 제공을 위한 AAL 시스템은 개인 신체정보와 환경정보와 같은 민감한 데이터를 수집하기 때문에 보안이 필수적이다. 본 논문에서는 AAL 시스템에서 요구하는 다양한 보안 요구사항을 만족하기 위하여 AAL 시스템의 특성을 반영한 경량 인증 프로토콜을 제안하였다. 제안된 경량 인증 프로토콜은 AAL시스템에 필요한 보안요구 사항을 지원할 뿐만 아니라 효율적이며, 패스워드 추측, 전방향 안전성, 위장공격, 중간자공격과 같은 다양한 공격에 안전하다. 제안된 기법은 향후 AAL 서비스 분야에서 유용하게 활용될 것으로 기대한다.

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(JIIBC), Vol.15, No. 6, pp.163-171, Dec. 31, 2015.
DOI: https://doi.org/10.7236/JIIBC.2015.15.6.163

[3] Myung-Kyu Yi, Hee-Joung Hwang, "Design of Secure Personal Health Record Management Systems", Journal of Korean Institute Of Information Technology, Vol. 13(8), pp. 71-80, 2015.8

[4] Myung-Kyu Yi, Done-sik Yoo, Taeg-Keun Whangbo, "A Security Labeling Scheme for

Privacy Protection in Personal Health Record System", The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol.15, No. 6, pp.173-180, Dec. 31, 2015.
DOI: https://doi.org/10.7236/JIIBC.2015.15.6.173

[5] 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

[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: https://doi.org/10.1109/MCOM.2015.7010518

[7] 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.

[8] 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. DOI: https://doi.org/10.1016/j.ins.2010.04.002

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

[10] Hyung-Uk Kim, Bumryong Kim, Moon-Seog Jun, "A Design of User Authentication Protocol using Biometric in Mobile-cloud Environments," Journal of the Korea Academia-Industrial cooperation Society(JKAIS), Vol. 18, No. 1, pp. 32-39, 2017.
DOI: http://dx.doi.org/10.5762/KAIS.2017.18.1.32

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>

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 2017년도 국토교통과학기술진흥원 연구비 지원에 의한 결과의 일부임.
과제번호: 17RERP-B090228-04