The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 4, pp.73-79, Aug. 31, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.4.73
JIIBC 2020-4-10

전천 후 생활보조 시스템을 위한 카멜레온 해시 함수 기반의 안전한 인증 프로토콜

Secure Authentication Protocol based on a Chameleon Hash Function for Ambient Living Assisted-Systems

이명규[*], 최현철[**], 황보택근[***]

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

요 약 인구 고령화와 저출산으로 인해 대부분의 국가는 고령화 문제에 직면해있다. 그 결과, 고령화에 대한 연구와 고령화 지원 수단은 전 세계 많은 정부의 우선순위가 되었다. 전천후 생활보조 접근법은 혁신적인 기술과 서비스의 개발을 통해 건강 상태를 모니터링하고 노인들의 더 나은 삶의 상태를 보장하는 방법이다. 전천후 생활보조 기술은 노인을 위한 더 많은 안전을 지원하고, 응급 대응 수단과 낙상 감지 해결책을 제공할 수 있다. 하지만, 전천후 생활보조 시스템에서 전송되는 정보는 매우 사적인 정보이므로, 이러한 데이터의 보안 및 개인 정보 보호는 해결해야 할 중요한 문제가 되고 있다. 본 논문에서는 전천후 생활보조 시스템을 위한 카멜레온 해시 기반의 안전한 인증 프로토콜을 제안한다. 제안된 인증 프로토콜은 전천후 생활보조 시스템에 필요한 여러 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 Due to the rapidly ageing population and low birth rates, most countries have faced with the problems of an ageing population. As a result, research into aging and the means to support an aging population has therefore become a priority for many governments around the world. 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 provide more safety for the elderly, offering emergency response mechanisms and fall detection solutions. Since the information transmitted in AAL systems is very personal, however, the security and privacy of such data are becoming important issues that must be dealt with. In this paper, we propose a Chameleon hash-based secure authentication protocol for 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 IT융합대학 컴퓨터공학과
[**]정회원, 가천대학교 공과대학 건축학과
[***]정회원, 가천대학교 IT융합대학 컴퓨터공학과 (교신저자)
접수일자 2020년 7월 13일, 수정완료 2020년 8월 2일
게재확정일자 2020년 8월 7일

Received: 13 July, 2020 / Revised: 2 August, 2020 / Accepted: 7 August, 2020
[***]Corresponding Author: tkwhangbo@gachon.ac.kr
Dept. of Computer Engineering, Gachon University, Korea

Ⅰ. 서 론

최근, 의료 분야의 발전으로 인해 기대수명이 증가하고 있으며, 출산율과 사망률이 동시에 낮아지면서 고령자가 인구에서 차지하는 비중이 상대적으로 높아지는 인구의 고령화가 빠른 속도로 진행되고 있다. 한국의 경우, 2017년 고령화 사회에 진입하였으며, 전 세계에서 가장 빠른 속도로 고령화가 이뤄져 약 50년 후인 2067년에는 65세 이상 인구 비중이 유례를 찾아볼 수 없는 47%까지 치솟을 것으로 예상되고 있다. 실제, 지난 10년 동안 기대수명은 12년 증가하였으며, 기대 수명의 증가와 출생의 동시적인 감소는 사람들의 가족 구성, 주거방식 뿐 아니라 건강관리 서비스 유형과 같은 일상생활 방식을 변화시키고 있다. 선진국들은 건강한 고령화를 표방하며 노인 만성질환관리에서 다양한 사회활동 영역에 이르기까지 정보통신기술 활용을 지원하고 있으며, 대표적인 사례로 유럽연합에서 수행중인 전천후 생활보조(Ambient Assisted Living, 이하 AAL)프로젝트를 들 수 있다. AAL은 개인의 일상생활 및 업무 환경에서 정보 통신 기술을 사용하여 노인들이 적극적이고 능동적인 삶을 영위할 수 있도록 지원하는 기술 시스템을 말한다. AAL 기술은 안전하고 건강한 삶을 유지할 수 있도록 도와주며 삶의 질을 향상시키는데 목표를 두고 있다. AAL의 대표적인 사례로는 HELP와 SOFTCARE 시스템이 있다. HELP(Home based Empowered Living for Parkinson's diseases patients)시스템은 파킨슨병 환자들을 위한 웨어러블 건강 모니터링 시스템이며, 주변의 도움을 받을 수 없는 파킨슨병의 환자를 위해 임상전문의가 원격으로 환자의 상태를 모니터링하고 통제할 수 있도록 지원한다. 파킨슨병 환자가 착용한 장비는 혈압, 생체신호, 활동정도를 HELP시스템으로 전송되며, 의료진은 HELP시스템을 통해 환자의 상태를 확인한 후에 약물투여량을 조절 할 수 있다. SOFTCARE는 고령자를 위한 모니터링 시스템이다. 사용자에 손목에 착용된 웨어러블 디바이스와 거주지에 설치된 센서를 통해 활동을 실시간으로 분석하고, 분석한 결과를 바탕으로 잠재적인 위험상황에 대한 알람과 위험추세에 대한 예측 정보를 제공한다. 전천후 생활보조 시스템에서 전송되는 정보는 매우 사적인 정보이므로, 이러한 데이터의 보안 및 개인 정보 보호는 해결해야 할 중요한 문제가 되고 있다[1,2]. 하지만, AAL 시스템 보안에 대한 연구는 아직 미미한 상태이다. 따라서, 본 논문에서는 AAL 시스템에서 요구하는 다양한 보안 요구사항을 만족하기 위하여 카멜레온 함수 기반의 안전한 인증 프로토콜을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장은 AAL 시스템에서의 관련 연구 및 보안 요구조건을 설명하고, 3장은 제안된 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[3-12]. He[8]는 AAL 시스템을 위한 인증 프로토콜을 제안했다. 사용자의 입력을 필요로 하므로 고령자를 고려해야 하는 AAL 시스템에서 적합하지 않다. Yi[9]는 AAL 시스템을 위한 경량 인증 프로토콜을 제안했다. 제안된 인증 프로토콜은 공개키 기반으로 연산이 복잡하고 느리며, 공개키를 관리해야 하는 단점을 가진다. Yi[10]는 AAL 데이터의 특성을 고려한 적응적 인증 프로토콜을 제안하였다. 제안된 기법은 민감 데이터와 비민감 데이터를 구분하기가 쉽지 않은 단점이 있다. AAL 시스템은 모든 정보가 공개된 채널을 통해 전송되기 때문에 보안이 취약할 수밖에 없는 단점을 가지고 있다. 따라서 다양한 유형의 공격을 차단할 수 있도록 안전할 뿐 아니라, AAL 센서의 특성을 감안하여 경량화 된 인증 기법을 설계해야 한다. AAL 시스템에서 필수적으로 만족되어야 할 보안 요구 조건은 다음과 같다.

- 상호 인증 : 인증된 사용자만이 수집한 데이터에 접근 할 수 있도록, AAL 센서와 AAL 서버 간의 상호 인증이 필요하다.
- 완벽한 전달 비밀성(Perfect Forward Secrecy) : 암호화 시스템이 정보를 암호화하고 해독하는 데 사용하는 키를 자동으로 자주 변경하여 최신 키가 손상되더라도 사용자의 중요한 데이터 중 일부만 노출하여 피해를 최소화할 수 있어야 한다.
- 공격 저항(Attack Resistance) : AAL 시스템에서 제공되는 인증 프로토콜은 중간자 공격, 재생 공격, 위장 공격, 위조/변조 공격 측면과 같은 다양한 공격을 견딜 수 있어야 한다.

본 논문에서는 이러한 보안 요구조건을 만족하기 위해 카멜레온 해시 함수 기반의 안전한 인증 프로토콜을 제안한다. 카멜레온 해시 함수는 해시 함수의 확장된 개념이며, 수신자가 충돌 값을 찾을 수 있는 특징이 있기 때

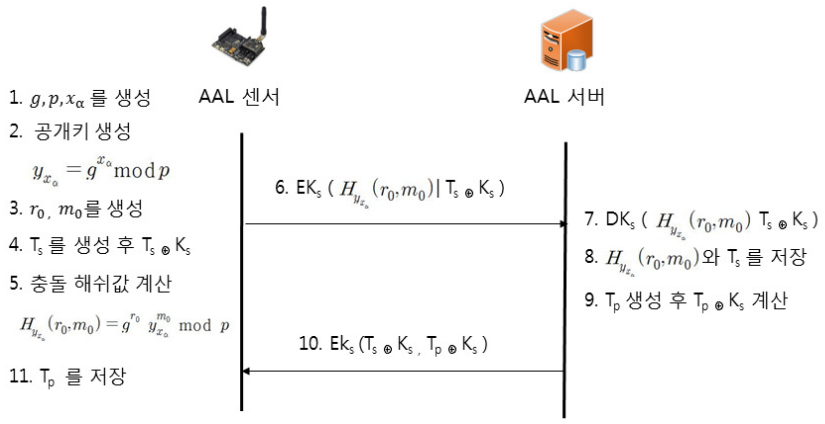

그림 1. AAL 인증절차를 위한 초기등록
Fig. 1. The Initial registration for AAL authentication procedure

문에 서명 검증 절차를 거친 메시지와 상이한 메시지를 찾을 수 있는 트랩도어 함수이다. 카멜레온 해시 값을 생성하기 위해서는 먼저 큰 솟수 g, p를 생성하고, 비밀값 x_α를 선택한다. ($x_\alpha \in Z_p^*$). 그리고, 카멜레온 해시에 해당하는 공개키 y를 식 (1)과 같이 계산한다.

$$y = g^x \bmod p \quad (1)$$

또한, 랜덤 값 r_0와 메시지 m_0를 생성한 후, 공개키 y_x를 이용하여 카멜레온 해시 값 $H_y(r_0,m_0)$ 을 식 (2)와 같이 구한다.

$$H_y(r_0,m_0) = g^{r_0}\, y^{m_0} \bmod p \quad (2)$$

이후, 새로운 메시지 m_1를 생성한 후 동일한 카멜레온 해시 값을 가지는 충돌 값 r_1는 식 (3)과 같이 계산한다.

$$r_1 = r_0 + x(m_0 - m_1) \quad (3)$$

새롭게 생성한 r_1와 m_1에 대한 카멜레온 해시 값은 r_0와 m_0에 대한 해시 값과 동일하다. 이에 대한 증명은 식 (4)를 통해 알 수 있다.

$$\begin{aligned} H_y(r_1,m_1) &= g^{r_1}\, y^{m_1} \bmod p \\ &= g^{r_0 + x(m_0 - m_1)}\, g^{x m_1} \bmod p \\ &= g^{r_0} g^{x m_0} \bmod p \\ &= H_y(r_0,m_0) \end{aligned} \quad (4)$$

III. 제안된 인증 프로토콜

본 장에서는 제안된 인증 프로토콜에 대해서 설명한다. 제안된 인증 프로토콜을 위해 다음과 같은 기호를 정의한다.

- x_y : 카멜레온 해시 값 생성을 위한 비밀 값
- y_{x_z} : 비밀 키 x_z를 활용하여 카멜레온 해시 값을 생성하기 위한 공개키
- T_s : AAL 센서에서 생성한 타임스탬프
- T_p : AAL 서버에서 생성한 타임스템프
- K_s : AAL 서버와 센서를 위한 세션키
- $H_{y_{x_\alpha}}(r_0,m_0)$: 랜덤 값 r_0, 메시지 m_0, 비밀값 x_α을 이용하여 생성한 카멜레온 해시 값

AAL 센서와 AAL 서버는 안전한 채널을 통해 세션키 K_s를 공유하고 있다고 가정한다. 그림 1와 같이 자세한 초기등록 절차는 다음과 같다.

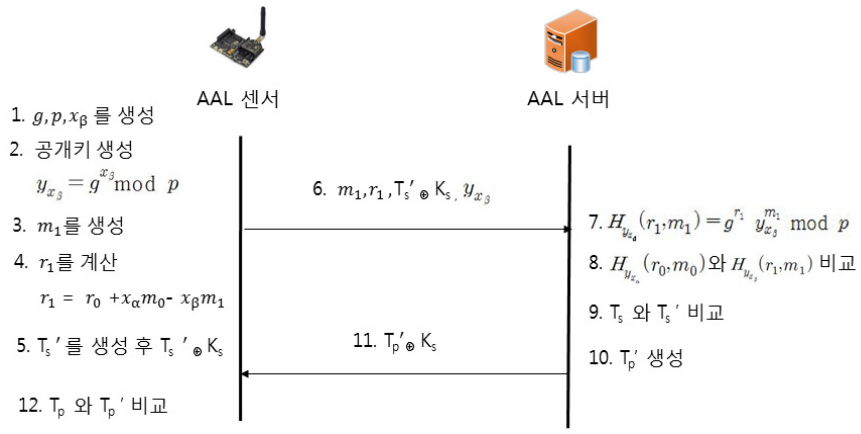

그림 2. 초기등록 후 AAL 인증절차
Fig. 2. The AAL authentication procedure after initial registration

1) AAL 센서는 큰 솟수 g, p를 생성하고, 비밀값 x_α를 선택한다. ($x_\alpha \in Z_p^*$)
2) 공개키 y_{x_α}를 식 (5)과 같이 계산한다.

$$y_{x_\alpha} = g^{x_\alpha} \bmod p \quad (5)$$

3) 랜덤 값 r_0와 메시지 m_0를 생성한다.
4) AAL 센서의 타임스탬프 T_s를 생성하고, $T_s \oplus K_s$를 계산한다.
5) 해시값 $H_{y_{x_\alpha}}(r_0,m_0)$ 를 식 (6)와 같이 계산한다.

$$H_{y_{x_\alpha}}(r_0,m_0) = g^{r_0}\ y_{x_\alpha}^{m_0} \bmod p \quad (6)$$

6) $H_{y_{x_\alpha}}(r_0,m_0)$와 $T_s \oplus K_s$ 를 세션키 K_s 로 암호화하여 AAL 서버에 전송한다.
7) AAL 서버는 수신한 값을 복호화하고, 수신한 $T_s \oplus K_s$을 세션키 K_s로 XOR 연산하여 T_s 값을 구한다.
8) $H_{y_{x_\alpha}}(r_0,m_0)$와 T_s 값을 AAL 서버에 저장한다.
9) AAL 서버의 타임스탬프 T_p를 생성하고, $T_p \oplus K_s$ 값을 계산한다.
10) $T_s \oplus K_s$ 과 $T_p \oplus K_s$ 값을 세션 키 K_s 로 암호화하여 AAL 센서에 전송한다.
11) AAL 센서는 수신한 값을 복호화하고, 수신한 $T_p \oplus K_s$을 세션키 K_s로 XOR 연산하여 T_p 값을 구하고 AAL 센서에 저장한다. 또한, $T_s \oplus K_s$을 세션키 K_s로 XOR 연산하여 T_s 값을 구한다. AAL 서버로부터 수신한 T_s 값이 AAL서버에게 전송한 T_s 값과 일치하면 초기등록 절차가 성공적으로 이루어진 것으로 간주하고 등록절차를 완료한다.

초기등록 후, AAL 센서와 AAL 서버를 위한 인증절차는 그림 2와 같다.

1) AAL 센서는 비밀 값 x_β를 선택한다. ($x_\beta \in Z_p^*$)
2) 공개키 y_{x_β}를 식 (7)과 같이 계산한다.

$$y_{x_\beta} = g^{x_\beta} \bmod p \quad (7)$$

3) 새로운 메시지 m_1를 생성한다.
4) 해시 충돌값 $r_1 = r_0 + x_\alpha m_0 - x_\beta m_1$ 를 계산한다.
5) AAL 센서는 타임스탬프 T_s의 값을 증가시킨 T_s'를 생성하고, $T_s' \oplus K_s$ 를 계산한다.
6) 공개키 y_{x_β} , r_1 , m_1, $T_s' \oplus K_s$ 를 AAL 서버로 전송한다.
7) AAL 서버는 수신한 y_{x_β} , r_1 , m_1 를 이용하여 해시 값 $H_{y_{x_\beta}}(r_1,m_1)$ 를 식 (8)와 같이 계산한다.

$$H_{y_{x_\beta}}(r_1,m_1) = g^{r_1}\ y_{x_\beta}^{m_1} \bmod p \quad (8)$$

8) 초기등록 과정을 통해 저장된 $H_{y_{x_\alpha}}(r_0,m_0)$값과 계산된 $H_{y_{x_\beta}}(r_1,m_1)$가 일치하는지를 체크한다. 또한, 수신한 $T_s' \oplus K_s$을 세션키 K_s로 XOR 연산하여

$T_s^{'}$ 값을 구한다.

9) AAL 서버는 초기등록에 저장된 T_s과 수신된 $T_s^{'}$를 비교한다. 만약, 수신된 $T_s^{'}$이 서버에 저장된 T_s의 값보다 크고, 해시 값 $H_{y_{x_\alpha}}(r_0, m_0)$값과 $H_{y_{x_\beta}}(r_1, m_1)$이 일치한다면 인증을 허가한다. 두 해시 값이 일치하지 않거나, 수신된 $T_s^{'}$이 서버에 저장된 T_s의 값보다 같거나 작은 경우 인증을 거부한다.

10) 인증절차가 성공적으로 이루어지면, AAL 서버는 T_s 값을 수신된 $T_s^{'}$으로 치환하고, T_p 값을 증가시켜 $T_p^{'}$ 값을 생성한다.

11) AAL 서버는 $T_p^{'} \oplus K_s$ 를 AAL 센서로 전송한다.

12) AAL 센서는 초기등록에 저장된 T_p과 수신된 $T_{p'}$를 비교한다. 만약, 수신된 $T_p^{'}$이 AAL 센서에 저장된 서버에 저장된 T_p보다 크면 인증이 성공적으로 이루어진 것으로 간주하고 T_p 값을 수신된 $T_p^{'}$ 값으로 치환한다. 그렇지 않다면, 인증을 취소한다.

IV. 제안방식 분석

본 장에서는 제안한 카멜레온 인증 프로토콜의 효율성과 안정성을 분석하고자 한다.

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

표기법	설명
T_h	해시, 타임스팸프, 임시비표, XOR 연산 수행시간
T_{sym}	대칭키 암호화 혹은 복호화연산 수행시간
T_{asym}	비대칭키 암호화 혹은 복호화연산 수행시간
T_{mm}	모듈러 곱 연산 수행시간

제안된 인증 프로토콜의 효율성 분석을 위하여 표 1과 같이 계산 비용을 위한 표기를 정의한다[7-9]. X. Cao et. al[4] 과 J. Huang et al.[7]의 연구를 통하여 각각 (9)~(11)식과 같이 정리할 수 있다.

$$T_h \cong 0.4\ T_{mm} \quad (9)$$

$$T_{sym} \cong 0.4\ T_{mm} \quad (10)$$

$$T_{asym} \cong 29\ T_{mm} \quad (11)$$

(1)~(3)식을 사용하면 연산비용을 표 2와 같이 각각 계산할 수 있다. 제안된 인증 기법에서 AAL 센서와 AAL 서버에서 총 3번의 XOR 연산, 그리고 2번의 모듈러 연산을 수행하므로, 인증 프로토콜에 소요되는 시간은 총 2.0 T_{mm}로 계산될 수 있다. 따라서 제안된 인증기법은 기존 기법들보다 효율성이 더 좋다고 말할 수 있다.

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

인증 프로토콜		인증시간	
Debiao He et. al.[8] 인증 기법		$2T_h + 2T_{sym} + 3T_{asym}$	88.6 T_{mm}
Yi et al[9] 인증 기법		$3T_h + 2T_{asym}$	59.2 T_{mm}
Yi et al[10]	민감 데이터	$2T_h + 2T_{asym}$	58.8 T_{mm}
	비민감 데이터	$2T_h$	0.8 T_{mm}
Yi et al[11]		$7T_h$	2.8 T_{mm}
제안된 인증기법		$5T_h$	2.0 T_{mm}

제안된 인증 프토토콜의 보안요구 사항을 고려한 안정성을 분석하면 다음과 같다.

- 상호인증(Mutual Authentication) : 상호인증은 AAL 센서와 AAL 서버 모두 정당한 통신자인지 명시적인 인증을 통해 확인하는 과정이다. AAL 센서는 AAL 센서 만이 생성할 수 있는 충돌 값과 타임스탬프/세션 키의 조합을 통해 AAL 서버에게 인증한다. 충돌 값은 비밀 값을 아는 AAL 센서 만이 계산할 수 있으므로 인증조건을 만족한다고 볼 수 있다. 또한, AAL 서버도 자신만이 생성할 수 있는 타임스탬프/세션 키 조합을 통하여 AAL 센서에게 인증한다. 타임스탬프 값은 지속적으로 변경되므로 상호인증 조건을 만족한다고 볼 수 있다.
- 재전송 공격(Replay Attack) : 재전송 공격이란 프로토콜 상 메시지를 복사한 후 재전송함으로써 승인된 사용자로 오인하게 만들어 공격하는 방법이다. 하지만, 제안된 인증 프로토콜에서는 AAL 센서에서 AAL 서버로 전송될 때마다 새로운 랜덤 값과 메시지를 생성하고 이를 통해 충돌 값을 계산함으로써

재전송 공격에 안전하다고 말할 수 있다. 또한, AAL 센서와 AAL 서버에서 생성한 타임스탬프 값을 세션 키와 XOR한 값을 전송하며, 타임스탬프 값은 지속적으로 변경되므로 재전송 공격으로부터 안전하다고 볼 수 있다.

- 완전한 순방향 비밀성(Perfect Forward Secrecy) : 완전한 순방향 비밀성은 AAL 시스템에서 정보를 암호화하고 해독하는데 사용되는 키를 자동으로 자주 변경하여 최신 키가 손상되더라도 사용자의 중요한 데이터 중 일부만 노출함을 의미한다. 제안된 프로토콜에서는 충돌 값만 전달하기 때문에 악의적인 사용자가 충돌 값을 얻더라도 비밀 값을 알지 못하면 해시 값을 계산할 수 없다. 따라서, 제안된 인증 프로토콜은 완전한 순방향 비밀성을 만족한다고 볼 수 있다.
- 위장공격(Impersonation Attack) : 위장공격이란 상대방이 공격자를 해당 AAL 시스템의 정당한 AAL 센서 혹은 서버로 여기도록 속이는 것을 의미한다. 제안된 인증 프로토콜은 사전에 공유한 큰 솟수를 알아내는 것이 어렵고, 랜덤 값과 메시지만 가지고 카멜레온 해시 값을 계산하기가 어렵다. 또한, 공개키는 이산 멱승으로 생성하기 때문에 비밀 값을 알 수 없으므로 정상적인 사용자로 가정한 위장 공격은 불가능하다.
- 중간자 공격(Man-In-The-Middle Attack) : 중간자 공격이란 공격자가 통신하고 있는 AAL 센서와 AAL 서버 사이에 정당한 통신 주체처럼 위장하고 끼어들어 메시지를 조작하거나 공격에 필요한 정보를 얻어내는 공격 유형이다. AAL 센서와 AAL 서버 사이에 중간자 공격을 시도할 수는 있지만, 동일한 카멜레온 해시 값을 생성하는 것이 불가능하고 AAL 센서는 AAL 서버로 전송 할 때마다 센서는 지속적으로 다른 비밀 값을 선택함으로써 카멜레온 키 쌍을 추측하여 공격하는 것은 어렵다. 또한, 전송 할 때마다 매번 생성되는 타임스탬프 값이 포함되어 있으므로 비밀 값 공격은 불가능하다. 비밀 키에 대한 공격은 이원 일차 연립방정식의 문제로 귀결되고, 서로가 전송하는 공개키는 이산 멱승의 연산으로 생성하기 때문에 중간자 공격에 안전하다고 말할 수 있다.

위에서 살펴본 바와 같이 제안된 인증 프로토콜은 AAL 시스템에서 필수적으로 만족되어야 할 보안 요구조건을 만족하며, 다양한 유형의 공격으로부터 안전하게 데이터를 보호할 수 있다.

V. 결 론

전 세계적으로 출산율의 감소와 평균수명의 연장으로 노인인구의 수 및 인구비중이 높아지고 있는 추세를 보이고 있으며, 급속한 고령사회 및 초 고령사회에 진입할 것으로 예상됨에 따라 노인 만성질환관리에서 다양한 사회활동 영역에 이르기까지 정보통신 기술 활용을 지원에 대한 관심이 높아지고 있다. AAL 시스템은 개인의 일상생활 및 작업 환경에서 정보 통신 기술을 사용하여 더 오랫동안 사회생활을 유지하면서 독립적으로 생활할 수 있도록 지원하는 시스템이다. 하지만, AAL 시스템은 민감한 데이터를 수집하기 때문에 보안이 필수적이다. 본 논문에서는 AAL 시스템에서 요구하는 다양한 보안 요구사항을 만족하기 위하여 카멜레온 함수 기반의 안전한 인증 프로토콜을 제안하였다. 제안된 인증 프로토콜은 AAL 시스템에서 요구되는 필수적인 보안요구 사항을 지원할 뿐만 아니라 효율적이며, 다양한 공격에 안전하다. 제안된 인증 프로토콜은 사용자들이 안전하고 편리하게 AAL 서비스를 제공받는데 활용될 수 있다.

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://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: https://doi.org/10.5405/jmbe.1478

[4] 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

[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] 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: https://doi.org/10.1007/s10916-014-0013-5

[7] 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

[8] 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

[9] 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://doi.org//10.7236/JIIBC.2017.17.5.9

[10] Myung-Kyu Yi, Hyunchul Choi, and Taeg-Keun Whangbo, "An Adaptive Authentication Protocol for Ambient Assisted Living Systems", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.18, No. 4, pp.19-26, Aug. 31, 2018.
DOI: https://doi.org/10.7236/JIIBC.2018.18.4.19

[11] Myung-Kyu Yi, Hyunchul Choi, and Taeg-Keun Whangbo, "A Secure and Lightweight Authentication Scheme for Ambient Assisted Living Systems", The Journal of The Institute of Internet, Broadcasting and Communication (IIBC) Vol. 19, No. 4, pp.77-83, Aug. 31, 2019.
DOI: https://doi.org/10.7236/JIIBC.2019.19.4.77

저 자 소 개

이 명 규(정회원)

- 2005년 2월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 10월~현재 : 가천대학교 IT 융합대학 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 IT대학융합 컴퓨터공학과 교수

- 주관심분야 : 영상처리, 패턴인식, 컴퓨터그래픽스, 3D 게임엔진, 의료정보

※ 이 연구는 2020년도 국토교통과학기술진흥원 연구비 지원에 의한 결과의 일부임
(과제번호 : 20RERP-B090230-07)