Journal of Digital Convergence
Vol. 17. No. 2, pp. 187-194, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.2.187

웨어러블 장치를 이용한 헬스케어시스템을 위한 안전한 통신 기법에 대한 분석 및 해결책

최해원[1], 김상진[2*],류명춘[2]
[1]DGIST 기술벤처경영 교수, [2]경운대학교 항공컴퓨터학과 교수

Cryptanalysis and Solution on Secure Communication Scheme for Healthcare System using Wearable Devices

Hae-Won Choi[1], Sangjin Kim[2*], Myungchun Ryoo[2]
[1]Department of Innovation Management, DGIST
[2]Department of Aerospace & Industrial Computing Security, Kyungwoon University

요 약 기존에 다양한 헬스케어 시스템에 대한 보안 개념이 제시되었다. 하지만 제시된 다양한 프로토콜에서 좀 더 나은 연산의 효율성과 안정성을 갖추기 위한 개선점이 보인다. 본 논문은 Vijayakumar등이 제안한 웨어러블 장치를 이용한 헬스케어시스템을 위한 효율적인 안전한 통신 기법에 대한 보안 분석 및 이에 대한 해결책을 제시한다. 특히, Vijayakumar등의 기법은 서비스거부공격에 취약하고 무결성을 제공하지 못하는 문제점이 있다. 이러한 문제들을 해결하기 위해서 본 논문에서는 새로운 안전한 통신 기법을 제안한다. 새롭게 제안한 기법은 인증 및 무결성을 제공함으로서 Vijayakumar등의 기법에 대한 효율적인 보안 해결책이 될 수 있다. 특히, 제안한 기법은 연산의 오버헤드 관점에서도 장점을 제시한다.

주제어 : 헬스케어보안, 정보보호, 무선 통신 보안, 안전한통신, 프라이버시

Abstract A security company has been proposed for various healthcare systems. However, there are improvements in order to achieve better efficiency and stability in the various protocols presented. The purpose of this paper is to provide cryptanalysis and solution on Vijayakumar et al.'s secure communication scheme for healthcare system using wearable devices. Especially, it is weak against denial of service attack and it does not provide integrity of the transmitted messages. Thereby, this paper proposes a new secure communication scheme to cope from the problems in Vijayakumar et al.'s scheme. It provides authentication and integrity, which could be the security solution against Vijayakumar et al.'s scheme. Furthermore, it also provides a good computational overhead compared to Vijayakumar et al.'s scheme.

Key Words : Healthcare security, Information security, Wireless communication security, Secure communication, Privacy

1. 서론

유비쿼터스 컴퓨팅 기술의 발전과 정보통신기술, 생명공학기술, 나노기술등을 포함한 기술간 컨버전스(convergence) 경향은 헬스케어(healthcare)의 실현을 가속화 하고 있다[1,2]. 헬스케어는 시간적, 공간적 제약 없이 환자가 생활 공간속에서 다양한 건강관리 및 의료 서비스를 지원하기 위한 기술이다. 특히, 이러한 헬스케어의 비제약성은 해킹으로 인한 정보유출 발생 시 기존 의료서비스에 비해서 더욱더 광범위한 국가와 사회적인 혼

*Corresponding Author : Sangjin Kim(mcryoo@ikw.ac.kr)
Received December 26, 2018
Revised January 21, 2019
Accepted February 20, 2019
Published February 28, 2019

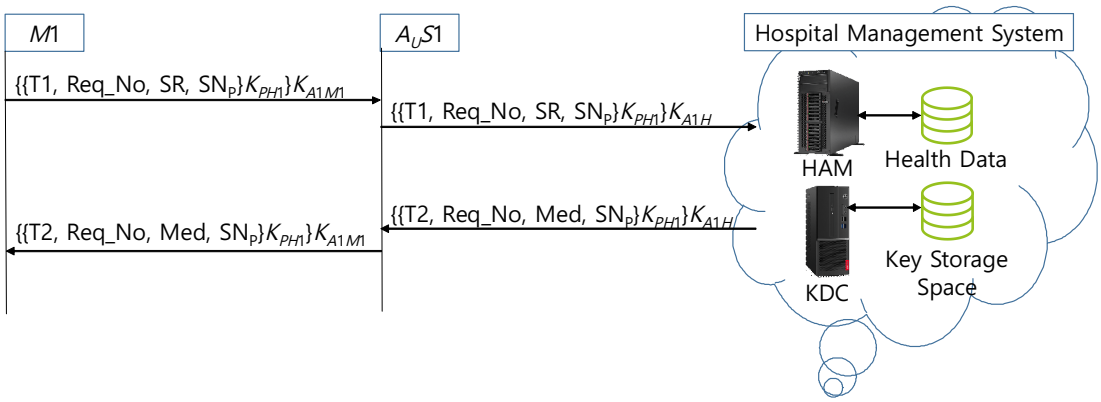

Fig. 1. Vijayakumar et al.'s Secure Communication Scheme [12]

란을 발생시킬 수 있다[3].

헬스케어시스템을 통해 환자의 안전한 원격 의료 서비스를 제공하기 위해서 센서와 같은 필수 웨어러블 장치가 환자의 신체에 내장되어 지속적으로 건강 상태를 모니터링 한다[4-6]. 센서는 해당 데이터를 지속적으로 체크하여 환자의 모바일 기기로 보낸다. 모바일 기기는 건강 분석 관리자(health analysis manager)에게 데이터를 주기적으로 전달한다. HAM은 환자로부터 수신 된 데이터를 분석하여 적절한 의료를 제공한다. 분석 결과 환자에게 약물 치료가 필요하면 HAM은 필요한 처방전을 포함하는 정보를 환자에게 보낸다. 분석 결과에 응급 상황이 발생하면 의사, 친척, 구급차, 병원 및 환자에게 비상 경보 메시지가 전송된다. 이 메시지를 여러 사람들에게 전송하기 위해 본 논문에서는 계산적으로 효율적이고 안전한 통신 기법을 제안한다. 제안 된 작업은 연산 요구량이 적기 때문에 자원의 제약이 강한 유비쿼터스 컴퓨팅 환경에 적합하다.

다양한 헬스케어시스템을 위한 보안 기법이 제안되었다[7-12]. Mark와 John은 의료 데이터 교환에 대한 안전한 기법을 제안했다[7]. 이 연구에서, 휴대 전화는 패킷을 수신하고 데이터 패킷을 전송하기 위한 도구로 이용되었다. 통신 보안을 보장하기 위해 메시지는 암호화되기 전에 서명되어 이용되었다. Othman등은 병원의 분산 무선 의료 센서 네트워크에서 데이터의 안전한 전송을 제공하는 시스템을 제안했다[8]. 이 연구에서 시스템은 지속적으로 환자의 상태를 의사에게 지속적으로 업데이트하여 환자의 신체에서 수집 한 민감한 데이터를 기반으로 요청시 응급 결정을 내린다. Han등은 인체정보네트워크를 이용하여 환자의 중요한 매개 변수를 수집하고 이를 클라우드 서버로 보낸다[9]. 이 기법은 통신의 복잡성을 줄여서 사용자 프라이버시를 제공한다. Smys와 Kumar에 의해 제안된 기법은 인체 센서 네트워크를 이용하여 환자로부터 중요한 건강 데이터를 수집하고 분석 결과를 관리인, 응급 진료 기관 및 의사에게 전달한다[10]. 이러한 시스템의 주된 한계는 메모리 가용성과 통신 복잡성을 더욱 줄이는데 있다. Liu등의 다른 연구에서는 계산 복잡도가 낮고 인증서를 사용하지 않는 안전한 인증 기법을 제안하였다[11]. 효과적인 연산과 통신 부하를 제공하고 다양한 장점을 제공한다. 최근에 Vijayakumar등은 연산의 효율성과 안전성을 위한 웨어러블 장치를 사용한 헬스케어시스템을 위한 안전한 기법을 제안하였다[12]. 특히, Vijayakumar등은 자신들의 기법이 다양한 안전성을 제시한다고 주장하였다.

본 논문에서는 Vijayakumar등의 기법이 서비스거부 공격에 취약하고 무결성을 제시하지 못하는 문제를 확인하고 이를 해결할 수 있는 개선된 안전한 통신 기법을 제안한다. 제안된 기법에서는 시스템의 타임스탬프(timestamp)와 해쉬 함수의 사용을 도입함으로서 기존 기법의 문제점을 해결한다. 특히, 제안한 기법은 기존의 기법에 비해서 안전하면서 연산의 부하를 효과적으로 줄일 수 있다.

2. Vijayakumar등의 안전한 통신 기법

최근에 Vijayakumar등은 웨어러블 장치를 이용한 헬스케어시스템을 위한 안전한 통신 기법을 일반상황과 응급상황의 두 가지 상황을 위한 보안 기법들을 각각 제안

했다[12]. 두 가지 기법이 비슷한 보안 속성을 공유하고 있고, 보안의 문제점 또한 공유하고 있어서 본 장에서는 이들 기법의 첫 번째 경우에 대한 상세한 리뷰를 제시한다. 이 기법은 병원관리시스템(hospital management system, HMS)이 환자가 약이 필요하고 응급상황이 발생하지 않는 경우에 이용할 수 있는 기법이다. Vijayakumar등의 기법은 등록단계와 안전한 통신 단계로 구성된다.

[등록단계] 등록단계에서 인증센터는 각 통신 참여자들 간의 공유 비밀키들을 안전하게 공유한다. M_1은 HMS와 비밀키인 K_{PH1}을 공유하고 인증서버인 A_US1과는 K_{A1M1}을 공유한다. A_US1은 HMS와 K_{A1H}를 공유한다.

[안전한 통신 단계] Fig. 1은 기법의 메시지 교환을 보여준다. 센서들은 환자의 신체정보를 읽고 이들 정보를 모바일폰 M_1에게 전송한다. M_1과 HMS간 상세 메시지 처리는 다음과 같다. 모든 비밀키는 인증센터를 통해 등록단계에서 안전하게 각 통신 참여자들에게 전송된다.

단계 1 : 센싱 데이터를 받고, M_1은 현재시간인 T1, 메시지 요청번호 Req_No, 환자의 센서정보 SR, 그리고 환자 등록번호 SNp로 메시지를 구성한다. M_1은 이 메시지를 HMS와 공유한 비밀키인 K_{PH1}을 이용하여 {T1, Req_No, SR, SNp}K_{PH1}같이 암호한다. M_1은 이 메시지를 인증서버 A_US1과 공유한 비밀키인 K_{A1M1}을 이용하여 다시 암호하고 이를 A_US1에게 보낸다.

단계 2 : A_US1은 받은 메시지를 K_{A1M1}을 이용하여 복호하고 HMS와 공유한 비밀키인 K_{A1H}를 이용하여 이를 다시 암호하여 HMS에게 보낸다.

단계 3 : HMS의 일원인 건강분석관리자(health analysis manager, HAM)가 A_US1로부터 메시지를 받고 이것을 키분배센터(key distribution center, KDC)에게 포워드하면 KDC는 K_{A1H}를 이용하여 그 메시지를 복호하고 HAM에게 전달한다. HAM은 환자로부터 받은 센서 데이터를 처리하여 그 환자가 약처방이 필요하지만 응급한 상황이 아님을 확인한다. 그러므로 HAM은 약을 처방하고 현재시간 T_2, 받은 요청번호 Req_No, 처방전 Med, 환자 등록번호 SNp를 KDC에게 보낸다. KDC는 그 내용을 K_{PH1}을 이용하여 암호하고 K_{A1H}를 이용하여 다시 암호하여 A_US1에게 보낸다.

단계 4 : A_US1은 K_{A1H}를 이용하여 그 메시지를 복호하고 K_{A1M1}을 이용하여 다시 암호하고 M_1에게 보낸다.

단계 5 : 마지막으로 M_1은 먼저 K_{A1M1}을 이용하여 메시지를 복호하고 다시 K_{PH1}을 이용하여 실제 내용을 확인한다.

3. Vijayakumar등의 기법 취약점 분석

본 장에서는 Vijayakumar등의 안전한 통신 기법에 대한 보안 분석을 서비스거부공격과 무결성 관점에서 제시한다.

[서비스거부공격] 서비스거부공격은 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격이다[13]. Vijayakumar등의 기법의 안전성은 두 번의 암호를 통해 제공된다. 특히, 통신 참여자들은 각각 두 번의 암호나 복호를 진행해야 해당 메시지가 제대로 된 메시지인지에 대한 확인을 할 수 있는 문제가 있다. 즉, Vijayakumar등의 기법에서 주고받는 메시지 각각에 대한 안전성은 두 번의 비밀키 암호 연산의 오버헤드를 갖는다. 이러한 문제로 인해서 공격자는 적법한 메시지 크기와 동일한 임의의 연속된 랜덤메시지를 통신 참여자들에게 보냄으로서 아주 쉽게 서비스거부공격을 수행할 수 있는 문제점이 있다. 즉, 랜덤메시지를 수신 받은 통신 참여자들은 메시지의 적법성을 두 번의 복호연산을 수행해야만 확인할 수 있다. 이러한 상황에서 메시지의 수가 증가함으로서 자연스럽게 컴퓨팅 능력의 범위를 벗어나고 시스템이 중지되는 문제가 발생할 수 있다.

[무결성] 무결성은 컴퓨팅 분야에서 데이터의 정확성과 일관성을 유지하고 보증하는 것을 가리킨다[14]. Vijayakumar등의 기법은 무결성을 제시하지 못한다. 메시지의 안전성은 단지 기밀성 기법인 암호화에 의존하고 있다. 따라서 메시지의 내용을 확인함으로서 무결성에 대한 체크를 단지 제시하고 있다. 하지만 이러한 기법은 연산의 비효율성을 제시하고 있고, 서비스거부공격에서 제시한 문제가 도출할 수 있는 가능성이 크다.

따라서 Vijayakumar등의 기법은 이러한 서비스거부공격과 무결성을 확인할 수 있는 기법으로의 보완이 필요하다.

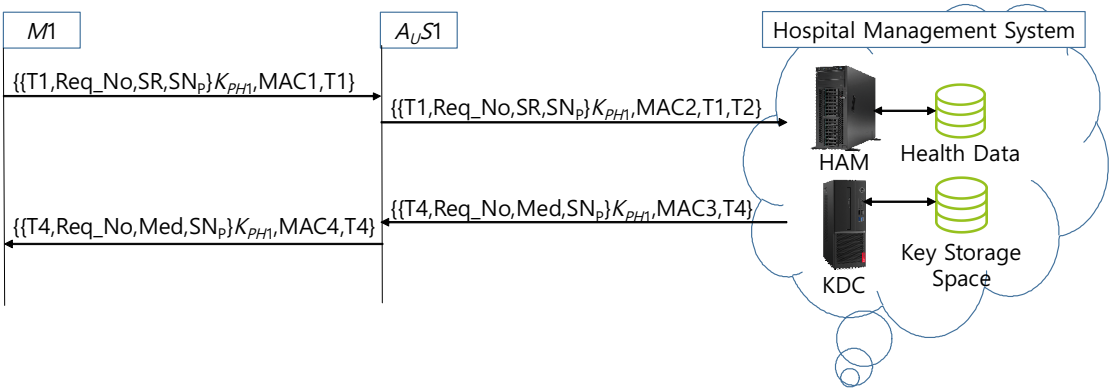

Fig. 2. Normal Status Phase of Proposed Secure Communication Scheme

4. 개선된 안전한 통신 기법

본 장에서는 Vijayakumar등의 기법의 보안 문제점을 해결할 수 있는 웨어러블 장치를 이용한 헬스케어시스템을 위한 개선된 안전한 통신 기법을 제안한다. 제안한 기법은 해쉬 함수에 기반한 무결성을 제공하고 서비스거부 공격에 안전할 수 있다. 본 논문에서 제안한 개선된 안전한 통신 기법의 모든 가정은 Vijayakumar등의 기법과 동일하다. 제안한 개선된 기법도 일반상황과 응급상황의 두 가지 상황을 위한 보안 기법들을 각각 제안한다. 제안한 기법은 등록단계와 일반상황 단계와 응급상황 단계로 구성된다.

[등록단계] 등록단계에서 인증센터는 각 통신 참여자들 간의 공유 비밀키들을 안전하게 공유한다. $M1$은 HMS와 비밀키인 K_{PH1}을 공유하고 인증서버인 A_US1과는 K_{A1M1}을 공유한다. A_US1은 HMS와 K_{A1H}를 공유한다. 특히, 이때 응급상황 발생 시 필요한 연락할 보호자 휴대폰 번호, 응급 레벨(α), 보호자와 환자, 그리고 A_US1은 HMS가 공유할 그룹키(GK)를 등록한다. 그리고 A_US1은 보호자와 응급상황에 사용할 비밀키 K_{A1Mi}를 공유한다. 또한, 진보된암호표준(advanced encryption standard, AES) 128비트 알고리즘과 해쉬 함수 H()를 통신 참여자들과 공유한다.

[일반상황 단계] Fig. 2는 제안한 개선된 안전한 통신 기법의 일반상황 단계의 메시지 교환을 보여준다. 센서들은 환자의 신체정보를 읽고 이들 정보를 모바일폰 M_1에게 전송한다. M_1과 HMS간 상세 메시지 처리는 다음과 같다.

단계 1 : 센싱 데이터를 받고, M_1은 현재시간인 T1, 메시지 요청번호 Req_No, 환자의 센서정보 SR, 그리고 환자 등록번호 SNp로 메시지를 구성한다. M_1은 이 메시지를 HMS와 공유한 비밀키인 K_{PH1}을 이용하여 {T1, Req_No, SR, SNp}K_{PH1}같이 암호한다. M_1은 이 메시지를 인증서버 A_US1과 공유한 비밀키인 K_{A1M1}을 이용하여 무결성 검증을 위해 MAC1=H(K_{A1M1}||{T1, Req_No, SR, SNp}K_{PH1})을 계산하고 {{T1, Req_No, SR, SNp}K_{PH1}, MAC1, T1}를 A_US1보낸다. 여기서||는 문자결합 연산자이다.

단계 2 : A_US1이 메시지를 받은 시점이 T2라면 T2 - T1 < △T을 통해서 전송지연 허용시간인 △T를 활용하여 재전송 공격의 가능성을 검증한다. 이를 통과한 메시지는 비밀키 K_{A1M1}을 이용하여 H(K_{A1M1}||{T1, Req_No, SR, SNp}K_{PH1})을 계산하고 이를 받은 MAC1과 비교하여 무결성 체크와 사용자 인증을 실시한다. 검증에 실패하면 통신을 끝내고 성공하면 MAC2=H(K_{A1H}||T2||{T1, Req_No, SR, SNp}K_{PH1})을 계산하고 {{T1, Req_No, SR, SNp}K_{PH1}, MAC2, T1, T2}를 HMS에게 보낸다.

단계 3 : HMS의 일원인 HAM이 A_US1로부터 메시지를 받고 이것을 KDC에게 포워드하면 KDC는 메시지를 받은 시점인 T3를 이용하여 T3 - T2 < △T을 통해서 재전송 가능성을 체크한다. 이를 통과한 메시지는 비밀키 K_{A1H}

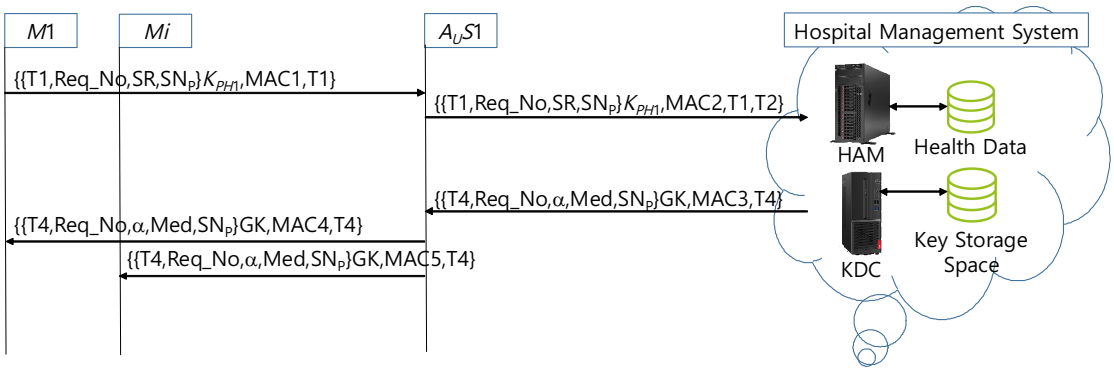

Fig. 3. Emergency Status Phase of Proposed Secure Communication Scheme

과 T2를 이용하여 H(K_{A1H}||T2||{T1, Req_No, SR, SNp}K_{PH1})을 계산하고 이를 받은 MAC2와 비교하여 무결성 체크 및 개체 인증을 실시한다. 검증이 성공했을 때만 받은 메시지를 K_{PH1}을 이용하여 복호하고 HAM에게 전달한다. HAM은 환자로부터 받은 센서 데이터를 처리하여 그 환자가 약처방이 필요하지만 응급한 상황이 아님을 확인한다. 그러므로 HAM은 약을 처방하고 현재시간 T4, 받은 요청번호 Req_No, 처방전 Med, 환자 등록번호 SNp를 KDC에게 보낸다. KDC는 그 내용을 K_{PH1}을 이용하여 암호하고 K_{A1H}를 MAC3=H(K_{A1H}||{T4, Req_No, Med, SNp}K_{PH1})을 계산하고 {{T4, Req_No, Med, SNp}K_{PH1}, MAC3, T4}를 A_US1에게 보낸다.

단계 4 : A_US1은 메시지를 받은 시점이 T5라면 T5 - T4 < △T를 통해서 재전송 가능성을 체크한다. 이를 통과한 메시지는 비밀키 K_{A1H}를 이용하여 H(K_{A1H}||{T4, Req_No, Med, SNp}K_{PH1})을 계산하고 이를 받은 MAC4와 비교하여 무결성 체크 및 개체 인증을 실시한다. 검증이 성공했을 때만 MAC4=H(K_{A1M1}||{T4, Req_No, Med, SNp}K_{PH1})을 계산하고 {{T4, Req_No, Med, SNp}K_{PH1}, MAC4, T4}를 $M1$에게 보낸다.

단계 5 : 마지막으로 M_1은 먼저 K_{A1M1}을 이용하여 H(K_{A1M1}||{T4, Req_No, Med, SNp}K_{PH1})을 계산하고 이를 받은 MAC4와 비교하여 무결성 체크 및 개체 인증을 실시한다. 검증이 성공했을 때만 K_{PH1}을 이용하여 메시지를 복호하고 실제 내용을 SMS로 표시한다.

[응급상황 단계] Fig. 3은 제안한 개선된 안전한 통신 기법의 응급상황 단계의 메시지 교환을 보여준다. 이때 단계 1~2번까지의 처리는 일반상황 단계와 동일하다. 하지만, 단계 3의 환자의 신체정보 확인 후 처리과정은 다음과 같이 응급상황을 취한 처리를 수행한다.

단계 3 : HAM은 환자로부터 받은 센서 데이터를 처리하여 그 환자가 응급한 상황임을 확인한다. 이를 위해 환자 등록시 건강 데이터베이스에 등록된 기관이나 사람에게 적절한 연락을 취하기 위해, HAM은 환자 등록시 수집된 휴대폰 번호, 응급 레벨 α, 그룹키 GK, 그리고 응급 정보를 KDC에게 보낸다. KDC는 그 내용을 GK를 이용하여 암호하고 K_{A1H}를 MAC3=H(K_{A1H}||{T4, Req_No, α, Msg, SNp}GK)을 계산하고 {{T4, Req_No, α, Msg, SNp}GK, MAC3, T4}를 A_US1에게 보낸다. 이때 인증기관은 여러기관이 될 수 있다.

단계 4 : A_US1은 메시지를 받은 시점이 T5라면 T5 - T4 < △T를 통해서 재전송 가능성을 체크한다. 이를 통과한 메시지는 비밀키 K_{A1H}를 이용하여 H(K_{A1H}||{T4, Req_No, α, Msg, SNp}GK)을 계산하고 이를 받은 MAC4와 비교하여 무결성 체크 및 개체 인증을 실시한다. 검증이 성공했을 때만 M1을 위해서 MAC4=H(K_{A1M1}||{T4, Req_No, α, Msg, SNp}GK)와 보호자인 Mi를 위해서

MAC5=H(K_{A1Mi}||{T4, Req_No, α, Msg, SNp}GK)을 계산하여 M1에게 {{T4, Req_No, α, Msg, SNp}GK, MAC4, T4}와 Mi에게 {{T4, Req_No, α, Msg, SNp}GK, MAC4, T4}를 보낸다.

단계 5 : 마지막으로 $M1$은 먼저 K_{A1M1}을 이용하여 H(K_{A1M1}||{T4, Req_No, α, Msg, SNp}GK)을 계산하고 이를 받은 MAC4와 비교하여 무결성 체크 및 개체 인증을 실시한다. 검증이 성공했을 때만 응급상황임을 확인하고 GK를 이용하여 메시지를 복호하고 실제 내용을 SMS로 표시한다. 보호자 Mi도 H(K_{A1Mi}||{T4, Req_No, α, Msg, SNp}GK)을 계산하여 이를 받은 MAC5와 비교하여 무결성 체크 및 개체 인증을 실시한다. 검증이 성공했을 때만 GK를 이용하여 메시지를 복호하고 응급상황에 따른 적절한 대처를 간구한다.

5. 보안 및 성능 분석

본 장에서는 개선된 안전한 통신 기법의 보안 및 성능을 Vijayakumar등의 기법[12]과 비교하여 제시한다.

[보안 분석] 제안한 기법에서는 해쉬 함수와 시스템의 타임스탬프를 이용하여 메시지의 신선성에 기반한 무결성을 제시하였고, 이중 암호의 문제를 해결하였다. 이를 통하여 기존에 Vijayakumar등의 기법에 존재하는 서비스거부공격에 대한 문제와 무결성을 제공하지 못하는 문제를 효과적으로 해결하였다. 따라서 본 논문의 보안 분석도 기밀성, 서비스거부공격과 무결성에 초점을 맞추도록 한다. Table 1은 제안한 기법과 Vijayakumar등의 기법에 대한 안전성에 대한 비교를 제시한다.

① 기밀성 : 제안한 기법의 메시지 기밀성은 AES 알고리즘의 안전성에 기반한다. 즉, AES-128 알고리즘을 이용하여 모든 메시지가 암호화 되어 있기 때문에 공격자는 통신 참여자들 간에 주고받는 메시지의 내용을 확인할 수 있는 방법이 없다. 따라서 본 논문에서 제안한 개선된 보안 기법은 기밀성을 제공한다.

② 서비스거부공격 : 제안한 기법은 시스템의 타임스탬프를 통해서 메시지 재전송 공격에 대해 가장 먼저 체크한다. 또한, 해쉬 함수를 통해 무결성 체크를 제시함으로서 Vijayakumar등의 기법에서 발생할 수 있는 연산에 대한 과부하를 해결할 수 있었다. 즉, 모든 통신 참여자들은 한 번의 해쉬 함수를 수행함으로서 서비스거부공격을 체크할 수 있음으로 시스템의 안정성을 제시할 수 있다.

③ 무결성 : 제안한 기법의 무결성은 해쉬 함수를 통해 제시된다. 특히, 등록단계에서 안전하게 통신 참여자들 간에 공유된 비밀키가 해쉬 함수의 입력으로 활용됨으로서 메시지의 무결성 뿐만 아니라 메시지 인증도 제시할 수 있다. 즉, 인가된 통신 참가자들만 유효한 메시지 인증 코드를 생성할 수 있음으로서 잠재적인 메시지 수정과 삽입 그리고 삭제 공격에 안전하게 대응할 수 있다.

Table 1. Security Comparison

Security Scheme	Con.	DoS	Int.
Vijayakumar et al.	Yes	No	No
Proposed	Yes	Yes	Yes

[성능 분석] 제안한 기법에서는 Fig. 3에서 보여준 것처럼 통신 참가자들은 모두 한 번의 해쉬 함수와 암호 및 복호 연산의 오버헤드만 갖는다. 구체적인 연산속도의 비교 분석을 위해서 논문 [15]의 구현에 따른 오버헤드인 암호 및 복호 연산 T_S와 해쉬 함수 T_H를 고려한다. 논문 [15]에 따르면 T_S와 T_H는 각각 0.0214835 ms와 0.005174 ms를 요구한다. Table 2는 제안한 기법과 Vijayakumar등의 기법에 대한 안전상황 단계 연산의 복잡도에 대한 비교를 제시한다. 즉, 본 논문에서 제시한 개선된 기법은 Vijayakumar등의 기법보다 40%정도의 연산 오버헤드를 줄일 수 있는 효율성을 제시할 수 있다.

Table 2. Computational Cost Comparison

Entity Scheme	M1	AUS1	HAM
Vijayakumar et al.	$4T_S$ =0.08593	$2T_S$ =0.04297	$4T_S$ =0.08593
Proposed	$2T_S+2T_H$ =0.05332	$2T_H$ =0.01035	$2T_S+2T_H$ =0.05332

6. 결론

본 논문에서는 Vijayakumar등이 최근에 제안한 웨어러블 장치를 이용한 헬스케어시스템을 위한 안전한 통신 기법이 서비스거부공격에 취약하고 무결성을 제시하지 못하는 문제를 먼저 분석하였다. 또한, 이러한 보안 문제를 해결하기 위하여 해쉬 함수와 시스템의 타임스탬프를 이용한 개선된 안전한 통신 기법을 제안하였다. 본 논문에서 제안한 개선된 안전한 통신 기법의 안전성은 해쉬 함수의 일방향성과 비밀키암호시스템의 안전성에 기반한다. 특히, 분석에서 제시한 바와 같이 본 논문에서 제시한 기법이 Vijayakumar등의 논문에서 발생하는 문제를 효율적으로 해결하면서 연산의 효율성도 40%정도 개선하는 효과를 확인할 수 있었다.

REFERENCES

[1] H. Kim, E. K. Ryu & S. W. Lee. (2011). Security Considerations on Cognitive Radio based on Body Area Networks for u-Healthcare. *Journal of Security Engineering, 10(1),* 9-20.

[2] S. Y. Mun, Y. M. Yun, T. H. Han, S. E. Lee, H. J. Chang, S. Y. Song & H. C. Kim. (2017). Public Awareness of Digital Healthcare Services. *Journal of Digital Convergence, 15(4),* 621-629.

[3] J. E. Song, S. H. Kim, M. A. Chung & K. I, Chung. (2007). Security issues and its technology trends in u-Healthcare. *Electronics and Telecommunications Trends, 22(1),* 119-129.

[4] T. M. Song & S. H. Jang. (2011). u-Healthcare : Issue and Research Trends. *Korea Institute for Health and Social Affairs,* 119-129.

[5] C. B. Roh & J. B. Song. (2015). Hybrid Healch Care System Designs in a Wireless Network Environment, *Journal of Digital Convergence, 13(3),* 457-462.

[6] J. E. Yoon & C. J. Suh. (2018). Research Trend Analysis on Smart Healthcare by using Topic Modeling and Ego Network Analysis. *Journal of Digital Convergence, 16(5),* 981-993.

[7] L. Mark & F. John. (2011). Remote control of medical devices using instant messaging infrastructure. *U.S. Patent CA2718696 A1, Dec. 8.*

[8] S. B. Othman & A. Trad. H. (2014). Youssef, Security artchitecture for at-home medical care using wireless sensor network, *Proc. of International conference on wireless communications and mobile computing conference 2014,* 304-309.

[9] S. Han, S. Q. Li, C. H. Ju & W. Zhou. (2016). PPM-HDA:Privacy-preserving and multifuntional health data aggregation with fault tolerance, *IEEE Transactions on Information Forensics and Security, 11(9),* 1940-1955.

[10] S. Syms & A. D. Kumar. (2016). Secured WBANs for pervasive m-healthcare social networks. *Proc. of 10th International Conference on Intelligent Systems and Control.*

[11] J. Liu, Z. Zhang & K. S. Kwak. (2014). Certificateless remote anonymous authentication schemes for wireless body area networks. *IEEE Transactions on Parallel and Distributed Systems, 25(2),* 332-342.

[12] P. Vijayakumar, P. Pandiaraja, M. Kaaruppiah & L. J. Deborah. (2017). An efficient secure communication for healthcare system using wearable devices. *Computers and Electrical Engineering, 63,* 232-245.

[13] Wikipedia, Denial of service attack, https://ko.wikipedia.org/wiki/Denial of service attack.

[14] Wikipedia. Data integrity, https://ko.wikipedia.org/wiki/Data integrity.

[15] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah & R. Baliyan. (2016). A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. *Security and Communication Networks, 9,* 3527-2542.

최 해 원(Choi, Hae Won) [정회원]

- 2000년 2월 : 경북대학교 컴퓨터공학과(공학석사)
- 2009년 2월 : 경북대학교 컴퓨터공학과(공학박사)
- 2016년 2월 : 대구경북과학기술원(DGIST) MOI
- 2006 ~ 2017년 : 경운대학교 항공컴퓨터학과 교수
- 2018년 3월 ~ 현재 : DGIST 기술벤처경영 겸직교수
- 2016년 10월 ~ 현재 : ㈜티에이싱크 대표
- 관심분야 : 알고리즘, 유비쿼터스 컴퓨팅, 보안
- E-Mail : chw@ikw.ac.kr

김 상 진(Kim, Sang Jin) [정회원]

- 1994년 2월 : 계명대학교 컴퓨터공학과 (공학사)
- 1996년 2월 : 경북대학교 컴퓨터공학과 (공학석사)
- 2000년 8월 : 경북대학교 컴퓨터공학과 (공학박사)
- 1999년 9월 ~ 현재 : 경운대학교 항공컴퓨터학과 교수
- 관심분야 : 알고리즘, 게임이론, 보안
- E-Mail : sjkim@ikw.ac.kr

류 명 춘(Ryoo, Myung Chun) [정회원]

- 1989년 2월 : 영남대학교 컴퓨터학과(공학사)
- 1991년 2월 : 영남대학교 컴퓨터공학과(공학석사)
- 2009년 2월 : 영남대학교 컴퓨터공학과(공학박사)
- 1997년 3월 ~ 현재 : 경운대학교 항공컴퓨터학과 교수
- 관심분야 : 지능정보시스템, Bioinformatics, 보안
- E-Mail : mcryoo@ikw.ac.kr