논문 21-46-06-16 The Journal of Korean Institute of Communications and Information Sciences '21-06 Vol.46 No.06
https://doi.org/10.7840/kics.2021.46.6.1065

원격 헬스케어 모니터링을 위한 키 격리 기법과 스마트카드 기반 개선된 인증 및 전송 프로토콜

류 현 호◆, 김 현 성◦

Enhanced Authentication and Transmission Protocol Based on Key Insulation Mechanism and Smartcard for Remote Healthcare Monitoring System

Hyunho Ryu◆, Hyunsung Kim◦

요 약

원격 헬스케어 모니터링 시스템의 보안을 위한 다양한 연구가 진행되었다. 이 시스템에서는 네트워크를 통한 환자의 건강정보가 주기적으로 병원 서버에 전송된다. 그러나 네트워크를 통한 전송에 있어서 허가되지 않은 외부 사용자의 정보 수집으로 인한 환자의 건강기록이나 개인 식별 정보 등이 노출되지 않도록 보호되어야 한다. 이러한 문제를 해결하기 위해 최근에 Noh등은 키 격리 기법을 이용한 개선된 건강정보 전송 기법을 제안하였다. 하지만 Noh등의 기법은 훔친 검증자 공격에 대해 안전하지 않은 문제가 있다. 본 논문에서는 Noh등의 기법에 존재하는 보안 문제를 해결하기 위한 키 격리 기법과 스마트카드 기반 개선된 인증 및 전송 프로토콜을 제안한다. 제안한 프로토콜은 Noh등의 기법에 존재하는 서버 검증자 유지 문제를 해결하기 위해 스마트카드를 이용하고 안전성 보증을 위해 키 격리 기법을 활용한다. 정형화된 보안 검증을 위해 자동화 검증 툴인 ProVerif를 이용하였다. 본 논문에서 제안한 프로토콜을 토대로 보다 안전하고 프라이버시를 제공할 수 있는 원격 헬스케어 모니터링 시스템을 구축할 수 있을 것이다.

키워드 : 헬스케어, 전송프로토콜, 프라이버시, 익명성, 인증프로토콜
Key Words : healthcare, transmission protocol, privacy, anonymity, authentication protocol

ABSTRACT

Various studies have been conducted for the security of remote healthcare monitoring systems. In this system, patient's health information through the network is periodically transmitted to the hospital server. However, in the transmission through the network, the patient's health records or personal identification information should not be exposed to unauthorized external users during the data collection. To solve this problem, Noh et al. recently proposed an improved health data transmission scheme using a key isolation technique. However, it is not safe against the stolen verifier attack. In this paper, we propose an improved authentication and transmission protocol based on key insulation mechanism and smartcard to solve the security

※ 본 연구는 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2017R1D1A1B04032598)으로 수행되었습니다.
◆ First Author : Kyungil University, School of Computer Science, ryoofamily0430@gmail.com, 학생회원
◦ Corresponding Author : Kyungil University, School of Computer Science, kim@kiu.ac.kr, 정회원
논문번호 : 202102-041-C-RN, Received February 23, 2021; Revised March 26, 2021; Accepted April 4, 2021

problem in Noh et al.'s protocol. The proposed protocol uses smartcard to solve the verifier usage problem in the server in Noh et al.'s protocol and key insulation mechanism for the security validation. ProVerif, an automatic security verification tool, was used for the canonical security validation of the proposed protocol. Much secure and privacy-preserving remote healthcare monitoring systems could be established based on the proposed protocol.

Ⅰ. 서 론

지속적으로 노인인구가 증가하고 만성질환자가 빠르게 늘어나고 있다. 이로 인해 헬스케어(Healthcare) 패러다임도 질병치료 중심에서 정보통신기술을 접목하여 사전 예방적인 건강관리 강화로 전환되고 있다[1-4]. 의료산업과 정보통신기술의 융합으로 언제 어디서나 헬스케어 서비스를 제공받을 수 있는 시스템 개발은 더욱 더 중요한 이슈가 되고 있다[4]. 헬스케어 서비스를 통하여 실시간으로 환자의 상태를 모니터링할 수 있고, 이를 통하여 환자의 시간과 금전적인 관점에서 장점을 제시할 수 있다. 특히, 환자는 원격지에서 편리하게 의사로부터 진료와 처방전을 받을 수 있어서 효율적이다. 이를 위해 환자는 의료용 건강 측정 센서들을 이용하여 수집된 자신의 건강정보(Personal health information, PHI)를 네트워크를 통해 헬스케어 시스템 서버에 전송함으로서 원격 주치의에게 적절한 의료 서비스를 제공 받을 수 있다. 원격 헬스케어 서비스를 이용함으로 얻을 수 있는 이점이 많지만, 원격을 지원하기 위한 안전하지 않는 통신 채널을 통한 보안 및 프라이버시의 취약성이 존재한다. 헬스케어 서비스를 위해 전송되는 환자의 건강 정보는 매우 민감한 정보이다. 헬스케어 네트워크 상에서 전송되는 다양한 데이터를 통해 환자의 프라이버시 정보가 유출될 수 있다. 환자의 건강정보와 관련된 정보가 노출되었을 경우에는 다양한 피해로 이어질 수 있다. 최악의 경우에는 공격자를 통해 임의로 조작된 데이터가 주치의에게 전송될 경우 환자의 건강에 악영향을 미칠 수 있다. 즉, 원격 헬스케어 시스템의 실용화를 위해 프라이버시 및 보안 보증 기법의 확충은 필수적이다[5].

원격 헬스케어 모니터링 시스템을 위한 다양한 보안 및 프라이버시 관련 기법 개발 연구들이 진행되었다[6-9]. Lin등은 도청으로 부터 환자의 건강정보 보호 및 익명성을 보장할 수 있는 기법을 제안하였다[6]. Lin 등의 기법은 신원기반 (Identity- based) 암호를 활용함으로서 메시지 내용 프라이버시 (Content oriented privacy) 뿐만 아니라 문맥 프라이버시 (Contextual privacy)도 제공할 수 있었다. 하지만 Yang등은 Lin등의 기법에서 환자의 정보를 헬스케어 서버에 전송하는 역할을 담당하는 휴대폰과 같은 단말 장치가 분실되었을 때 비밀키 노출로 인해 다양한 공격이 가능함을 보였다. 또한, Lin등의 기법에 존재하는 문제를 해결하기 위한 키 격리 (Key insulation) 기법을 이용한 새로운 기법을 제안하였다[7-8]. 하지만, Noh등은 Yang 등의 기법에서 모든 환자에게 하나의 동일한 마스터 키를 발급함으로서 발생하는 개인키 유출 문제를 도출하였다. 또한, 이 문제를 해결하기 위해 환자마다 다른 키를 이용하는 새로운 기법을 제안하였다[9]. 하지만, 본 논문의 저자들은 Noh등의 기법에서 건강 기록 전송 단계의 안전성을 위한 환자와 서버 사이의 공유 비밀키 설립에 환자의 가명식별자를 이용하고 개인키 관련 정보가 서버에 저장되어야 하는 문제가 있음을 확인하였다. 특히, 공격자가 서버 침투 공격을 통해 서버에 저장된 검증자를 획득할 수 있고, 이러한 검증자에 저장된 정보를 활용한 다양한 공격에 취약함을 확인하였다.

본 논문에서는 Noh등의 기법에 존재하는 보안 문제를 해결하기 위한 스마트카드 기반 개선된 인증 및 전송 프로토콜을 제안한다. 제안한 프로토콜은 서버의 검증자 유지 문제를 해결하기 위해서 시스템에 중요한 데이터를 스마트카드에 저장하고 안전성을 보증하기 위해 키 격리 기법을 이용한다. 제안한 프로토콜에 대한 보안 검증을 위해 정형화된 자동화 검증 툴인 ProVerif를 이용하였다. 이러한 검증결과 본 논문에서 제안한 프로토콜이 Noh등의 기법을 포함한 관련 기법들에 존재하는 다양한 보안 및 프라이버시 문제를 효율적으로 해결할 수 있음을 확인할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 원격 헬스케어 모니터링 시스템의 네트워크 구성과 키 격리 기법 정의 그리고 관련 연구를 살펴본다. 3장은 새로운 스마트카드 기반 인증 및 전송 보안 프로토콜을 설계한다. 4장에서 제안한 프로토콜에 대한 보안 및 성능 분석을 제시하고, 5장에서 결론을 맺는다.

Ⅱ. 연구 배경

본 장에서는 헬스케어 시스템 구성과 키 격리기법의 개요를 살펴본다.

2.1 원격 헬스케어 모니터링 시스템

원격 헬스케어 시스템을 위한 네트워크 구성은 그림 1과 같고 주요 참가자 및 역할은 다음과 같다[10-12].

- 건강 모니터링 시스템(HMS): 신뢰기관으로 시스템 파라미터 생성과 네트워크 참가자들의 시스템 등록을 담당한다. 또한, 환자의 암호화된 건강정보를 수집하고 의사에게 제공하는 역할을 수행한다.
- 의사(Doctor, D_j): HMS와 동일 내부 네트워크를 이용하고 주기적으로 HMS의 데이터베이스를 통해서 자신이 담당한 환자들의 건강정보를 확인하고 적절한 의료 서비스를 제공한다.
- 환자(Patient, PT): HMS에 등록하여 원격 헬스케어 서비스를 이용하는 주체이다. 주기적으로 HMS에게 건강정보를 전송하고 주치의 D_j로부터 의료 서비스를 받는다.

제안하는 프로토콜에서 원격 헬스케어 서비스를 이용하는 PT는 안전한 서비스를 제공받기 위해서 BH와 HKU를 사용한다고 가정한다. 이들의 역할은 다음과 같다.

- BH(Body Hub): 병원에서 원격 진료를 원활히 수행하기 위해 주기적으로 PT의 건강정보를 수집하고 이를 HMS에게 전송하기 위한 장치이다. 본 논문에서는 PT가 소유한 스마트폰을 BH로 고려한다. 특히, 이러한 스마트폰은 USIM(Universal subscriber identity module)과 같은 스마트카드 활용을 가정한다.
- HKU(Helper of Key Unit): PT의 안전한 통신을 위해 주기적으로 비밀키를 업데이트 하는 주체이다. 특히, PT가 BH를 잃어버린 경우에도 HMS와 안전한 통신 회선을 설립하기 위한 역할을 수행한다. 본 논문에서 PT의 개인용 컴퓨터(Personal computer)를 HKU로 가정한다.

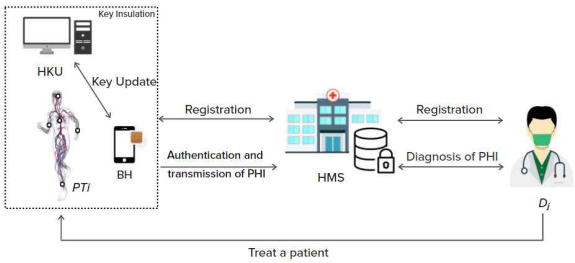

그림 1. 헬스케어 모니터링 시스템 구성
Fig. 1. Healthcare monitoring system configuration.

2.2 키 격리 기법

Yang등은 환자의 개인키가 저장된 단말기의 분실로 인해 개인키가 손상될 우려가 있음을 제시하였고, 키 격리 기법을 적용한 익명 인증 기법을 제안하였다[7]. 키 격리 기법은 사용자의 마스터 비밀키를 분실 위험이 없는 안전한 곳에 저장하고, 마스터 비밀키로부터 생성된 일정 주기의 개인키를 휴대용 단말기에 저장하여 사용함으로써, 단말기 분실 시 발생할 수 있는 개인키 노출의 피해를 최소화하기 위한 기법이다[8].

Yang 등과 Noh 등의 기법에서 환자의 개인키 분실 피해를 최소화하기 위해 마스터 비밀키를 생성하고 이를 개인용 컴퓨터에 저장하여 이용한다[7, 9]. 이후 마스터 비밀키로부터 생성된 일정 시간 주기의 개인키를 만들어 환자의 단말기에 저장함으로서, 단말기를 분실하여도 서버의 도움 없이 새로운 주기의 키를 생성할 수 있게 한다.

그림 2는 본 논문에서 제안하는 프로토콜의 키 격리 기법 동작 원리를 보여준다. 헬스케어 서버인 HMS로부터 헬퍼키를 발급 받은 BH는 HKU 상에 헬퍼키를 복사한다. 헬퍼키 복사는 시스템 셋업 단계에서 한번만 수행된다. PT의 BH는 t시간 주기마다 HKU와 연동하여 새로운 개인키를 생성하여 활용한다. 키 격리 기법을 통해 일정 시간 주기별 다른 개인키를 사용함으로서 시스템의 안전성을 향상시킬 수 있다.

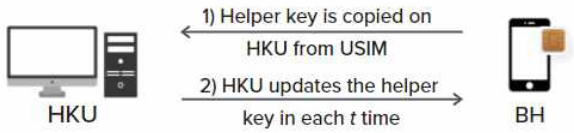

그림 2. 키 격리 기법 원리
Fig. 2. Conceptual flow of key insulation mechanism.

Ⅲ. 스마트카드 기반 건강정보 전송 보안 프로토콜

본 장에서는 기존의 키 격리 기법을 이용하는 다양한 PHI 전송 보안 프로토콜들의 문제점을 해결할 수 있는 새로운 스마트카드 기반 프로토콜을 제안한다. 제안한 프로토콜에서는 HMS가 등록 과정에서 데이터베이스의 필요성을 환자의 스마트카드 (USIM) 사용으로 대체한다. 새로운 프로토콜은 시스템 초기화,

표 1. 기호 정의
Table 1. Notations.

Notation	Descriptions
G, G_T	Cyclic groups of the same order q
P	Generator of group G
$\hat{e}()$	Bilinear pairing
$H_1()$	One-way hash function
s_0	Master key of HMS
PU_{HMS}	Public key of HMS
ID_{PTi}	Identity of patient
PW_{PTi}	Password of patient
ts	Time stamp
PHI	Personal health information
hk_{PTi}	Helper private key of HKU
HP_{PTi}	Helper public key
$\|\|$	Concatenation operation
$\oplus$	XOR operation
$KDF()$	Key derivation function
$E_{key}()$	Symmetric encryption algorithm with key
$D_{key}()$	Symmetric decryption algorithm with key

환자 등록, 키 갱신, 인증 및 전송 그리고 건강기록 진단 과정으로 구성된다. 표 1은 본 논문에서 사용하는 기호와 그 의미를 보여준다.

3.1 시스템 초기화

HMS는 겹선형 파라미터 $<q, P, G, G_T, \hat{e}()>$를 생성한다. HMS의 마스터키 $s_0 \in Z_q^*$를 랜덤하게 선택하고 공개키 $PU_{HMS}=\hat{e}(s_0, P)$를 계산한다. 일방향 해시함수 $H_1()$: $\{0, 1\}^n \rightarrow G$를 정의하고 시스템 파라미터 $<q, P, G, G_T, \hat{e}(), H_1(), PU_{HMS}>$를 시스템에 배포한다. 이후 소속된 각 의사 D_j의 개인키 $SK_{Dj}=\hat{e}(s_0, H_1(D_j))$를 생성하여 D_j에게 전달한다. 여기서 D_j와 HMS 간 통신은 안전한 내부 네트워크를 사용한다고 가정한다.

3.2 환자 등록

원격 헬스케어 모니터링 서비스에 등록하고자 하는 환자 PT는 관련 신청서를 HMS에게 제출한다.

1) PT는 자신의 식별자 ID_{PTi}와 패스워드 PW_{PTi}를 선택한다. 난수 n을 생성하고 $P_{PTi}=H_1(ID_{PTi}||n)$를 계산하고 PT의 실제 신원정보인 $REAL_{PTi}$를 이용한 메시지 $\{REAL_{PTi}, P_{PTi}\}$를 구성하여 HMS에게 제출한다.
2) HMS는 PT로부터 $\{REAL_{PTi}, P_{PTi}\}$를 받은 후 $REAL_{PTi}$의 유효성을 검사하고 등록되지 않은 PT라면 랜덤하게 가명식별자 PID_{PTi}를 생성한다.
3) HMS는 PT를 위한 헬퍼 비밀키 $hk_{PTi} \in Z_q^*$를 랜덤하게 생성하고, 헬퍼 공개키 $HP_{PTi}=\hat{e}(hk_{PTi}, P)$와 PT의 초기 $t=0$ 서비스 개인키인 $PSK^0_{PTi}=\hat{e}(s_0, H_1(PID_{PTi}))+\hat{e}(hk_{PTi}, H_1(PID_{PTi}||HP_{PTi}||t))$를 계산한다. 그리고, $V_{PTi}=H_1(P_{PTi})\oplus H_1(hk_{PTi})$와 $C_{PTi}=H_1(s_0||P_{PTi})$를 계산한다.
4) HMS는 $\{PID_{PTi}, hk_{PTi}, PSK^0_{PTi}, HP_{PTi}, V_{PTi}, C_{PTi}\}$가 저장된 USIM을 PT에게 발급한다.
5) PT는 HMS로부터 발급 받은 USIM을 BH에게 삽입하고 hk_{PTi}를 자신의 HKU에 복사한다.
6) PT는 $W_{PTi}=H_1(ID_{PTi}||PW_{PTi})\oplus n$, $X_{PTi}=hk_{PTi}\oplus H_1(ID_{PTi}||PW_{PTi})$, $Y_{PTi}=PSK^0_{PTi}\oplus H_1(ID_{PTi}||PW_{PTi})$를 계산하여 USIM에 저장하고 PSK^0_{PTi}와 hk_{PTi}를 삭제한다.
7) PT는 HMS에 소속된 의사 중 주치의 D_j를 선택한 후 $DP^j_{PTi}=\hat{e}(hk_{PTi}, H_1(D_j))$를 계산하고 이를 USIM에 저장한다.

3.3 키 갱신

본 논문에서 제안한 시스템은 미리 정해진 시간 주기마다 서비스 개인키를 생성하여 이용한다. 주기 $t+1$의 새로운 서비스 개인키는 다음과 같이 생성한다.

1) PT의 HKU는 헬퍼키 $TK^{t+1}_{PTi}=\hat{e}(hk_{PTi}, H_1(PID_{PTi}||HP_{PTi}||t+1)-H_1(ID_{PTi}||HP_{PTi}||t))$를 생성하여 PT의 BH에 전달한다.
2) BH의 USIM에서 $PSK=Y_{PTi}\oplus H_1(ID_{PTi}||PW_{PTi})$를 통하여 $PSK^{t+1}_{PTi}=PSK+TK^{t+1}_{PTi}$를 계산한 후에 헬퍼키 TK^{t+1}_{PTi}와 USIM에서 Y_{PTi}를 삭제하고 새로운 주기 $t+1$의 개인키인 $Y_{PTi}=PSK^{t+1}_{PTi}\oplus H_1(ID_{PTi}||PW_{PTi})$를 계산하여 USIM에 새로 저장한다. 즉, t 주기의 서비스 개인키 PSK^t_{PTi}는 새로운 시간 주기에서는 더 이상 사용하지 않는다.

3.4 인증 및 전송

헬스케어 모니터링 서비스에 등록된 PT는 일정 주기마다 BH를 통해 수집된 건강 정보를 HMS에 전송한다. 이를 위해 BH는 먼저 USIM의 소유자 인증을 수행하고, 인증에 성공된 PT만 HMS와 통신을 할 수 있다. 특히, 통신의 안전성과 프라이버시 보증을 위해 세션 의존적인 타임스탬프와 난수를 사용한다. 그림 3은 본 논문에서 제안한 프로토콜의 인증 및 전송 단계의 개념적 흐름도를 보여준다. 자세한 단계는 아래와 같다.

1) PT는 자신의 건강정보를 HMS에게 전송하기 위해서 USIM에 ID_{PTi}와 PW_{PTi}를 입력한다. USIM은 $n' = W_{PTi}\oplus H_1(ID_{PTi}||PW_{PTi})$, $P_{PTi}' = H_1(ID_{PTi}||n')$, $hk_{PTi}' = X_{PTi}\oplus H_1(ID_{PTi}||PW_{PTi})$, $V_{PTi}' = H_1(P_{PTi}')\oplus$

$H_1(hk_{PTi}')$를 계산한다. 이후 V_{PTi}와 V_{PTi}'이 동일한지 확인한다. 두 값이 일치하지 않으면 USIM은 세션을 종료한다.

2) USIM은 난수 r을 생성하고 $R_{PTi}=\hat{e}(PU_{HMS}, r)$, $B_{PTi}=\hat{e}(P, r)$, $PSK=Y_{PTi}\oplus H_1(ID_{PTi}||PW_{PTi})$, $VID_{PTi}=R_{PTi}\oplus P_{PTi}'$, $VSK_{PTi}=R_{PTi}\oplus PSK$를 계산한다.

3) 현재 주기가 t라고 할 때 D_j와 비대화식으로 공유 비밀키 $K_{PTi\text{-}Dj}=\hat{e}(PSK'_{PTi}, H_1(D_j))$를 생성하고 $K_{PTi}=KDF(K_{PTi\text{-}Dj}||0)$를 계산한다.

4) USIM은 수집된 PT의 PHI를 안전하게 HMS에게 전송하기 위해 현재시간 ts를 이용하여 암호문 $C_1=E_{KPTi}(\text{PHI}, ts)$, $C_2=H_1(PID_{PTi}||C_{PTi}||HP_{PTi}||ts||D_j||C_1)$, $C_3=E_{KPTi\text{-}H}(HP_{PTi}, DP^j_{PTi}, C_{PTi}, D_j, C_1, C_2)$를 계산한다. HMS와 공유할 키 $K_{PTi\text{-}H}=KDF(\hat{e}(PSK'_{PTi}, H_1(PU_{HMS})))$를 이용하여 C_3를 계산한다. 이후 $\{B_{PTi}, VID_{PTi}, PID_{PTi}, C_3\}$를 HMS에게 전송한다.

5) HMS는 수신한 $\{B_{PTi}, VID_{PTi}, PID_{PTi}, C_3\}$로부터 $R_{PTi}'=\hat{e}(s_0, B_{PTi})$를 계산하여 $PSK'_{PTi}'=VSK_{PTi}\oplus R_{PTi}'$를 알아낸 뒤 $K_{PTi\text{-}H}=KDF(\hat{e}(PSK'_{PTi}',$

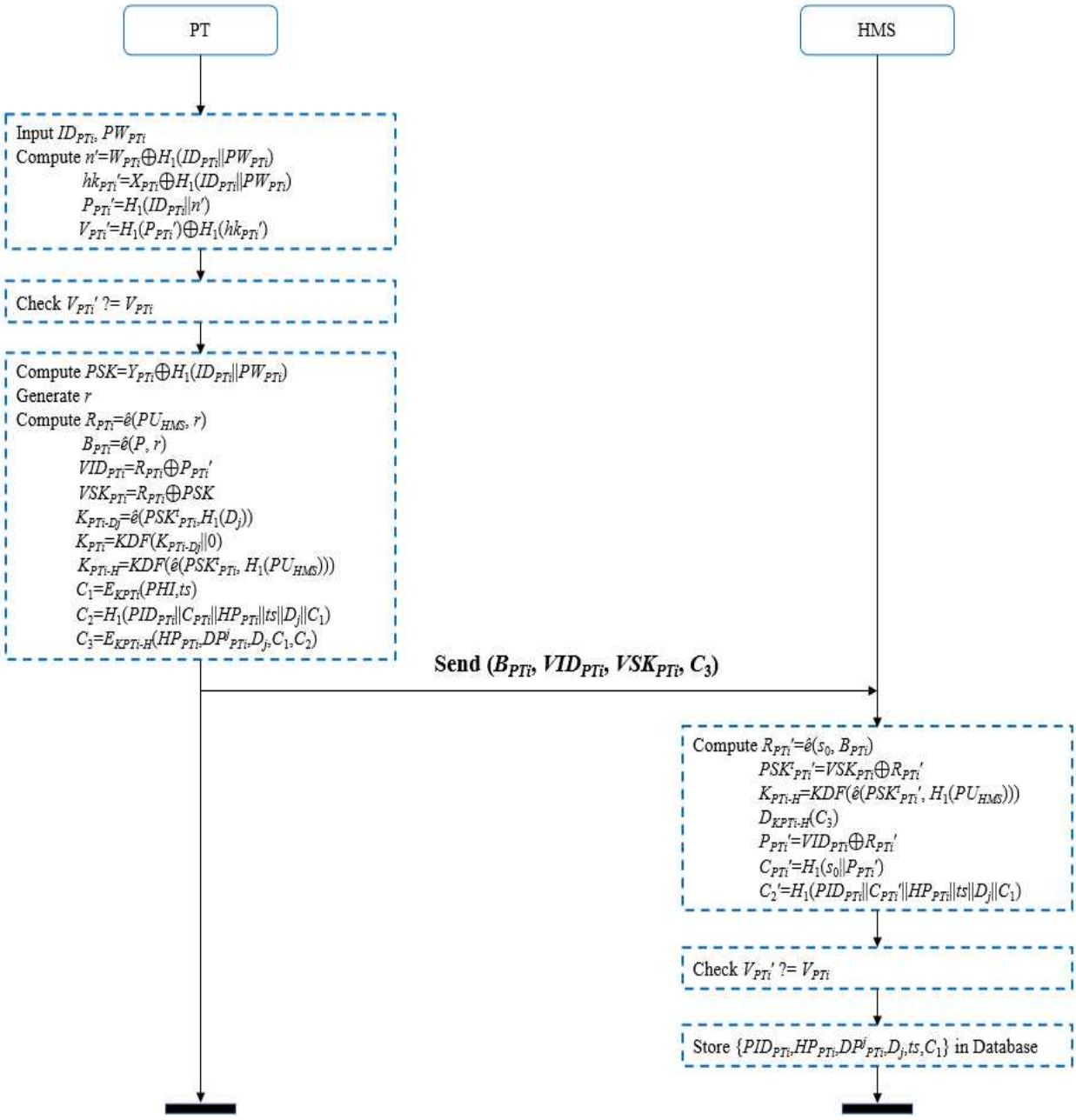

그림 3. 인증 및 전송 단계
Fig. 3. Authentication and transmission phase.

$H_1(PU_{HMS})$))를 계산하여 C_3를 복호한다. 이후 $P_{PTi}' = VID_{PTi} \oplus R_{PTi}'$를 통해 $C_{PTi}' = H_1(s_0 \| P_{PTi}')$를 계산한 후에 $C_2' = H_1(PID_{PTi} \| C_{PTi}' \| HP_{PTi} \| ts \| D_j \| C_1)$을 도출하고 C_2'과 C_2가 서로 동일한지 검증한다. 만일 두 값이 다르다면 HMS는 해당 세션을 종료한다.

6) HMS는 $M = \{PID_{PTi}, HP_{PTi}, DP^j_{PTi}, D_j, ts, C_1\}$을 구성하여 자신의 데이터베이스에 저장한다.

3.5 건강기록 진료

D_j는 HMS에게 적절한 인증 과정을 거친 후, HMS의 데이터베이스에 접근하여 PT의 환자 건강 정보를 확인한 후 적절한 진단을 제시한다.

1) D_j는 HMS에 저장된 PT의 정보에 접근하기 위해서 적절한 인증 과정을 수행한다. 성공적인 인증 후 HMS에 저장된 PT의 정보$\{PID_{PTi}, HP_{PTi}, DP^j_{PTi}, D_j, ts, C_1\}$를 이용하여 비밀키 $K_{PTi\text{-}Dj}' = \hat{e}(H_1(PID_{PTi}), SK_{Dj})\hat{e}(H_1(PID_{PTi} \| HP_{PTi} \| t), DP^j_{PTi}))$를 통해 $K_{PTi}' = KDF(K_{PTi\text{-}Dj}' \| 0)$을 도출한다.
2) D_j는 $D_{KPTi}'(C_1)$를 통해 PT의 PHI를 확인하고 적합한 진단을 제시한다. 이때 PT와 추가적인 통신에 $K_{PTi\text{-}Dj}'$를 이용한 안전한 통신을 진행한다.

Ⅳ. 보안 및 성능분석

본 장에서는 제안한 프로토콜의 보안 검증을 위해 ProVerif 자동 검증 툴을 활용한다[13]. 또한 제안한 프로토콜과 관련된 Yang등의 기법과 Noh등의 기법의 보안 속성에 대한 비교 분석을 제시한다. 마지막으로 관련된 프로토콜들 간 성능에 대한 분석을 제시한다.

4.1 ProVerif 보안 검증

ProVerif 는 보안 프로토콜에 대한 자동화된 검증 툴이다[13]. 특히, 보안 검증을 위해서 Dolev-Yao 공격 모델[14]을 가정한다. ProVerif를 통해서 상호 인증과 보안성 및 프로세스들 간의 등가성과 같은 인증 기법의 보안적 특성들을 확인해 볼 수 있다.

제안한 프로토콜의 보안 검증을 위하여 다음과 같은 단계로 진행하였다. 먼저 환자와 HMS간의 공개 통신 채널인 ch를 정의하였다. 한 세션에 의존성이 있는 R_{PTi}의 안전성을 검증하기 위하여 svalueA와 svalueB가 사용되었다. 또한 제안한 프로토콜의 상호 인증을 검증하기 위하여 4개의 이벤트 SUbegin(entity), USbegin (entity), SUend(entity), USend(entity)를 이용하였다. 그런 후, PT와 HMS 각

```
ProVerif text output:

Completing equations...
Completing equations...
-- Process 1-- Query inj-event(SUend(e)) ==> inj-event(SUbegin(e)) in process 1
Translating the process into Horn clauses...
Completing...
Starting query inj-event(SUend(e)) ==> inj-event(SUbegin(e))
RESULT inj-event(SUend(e)) ==> inj-event(SUbegin(e)) is true.
-- Query inj-event(USend(e)) ==> inj-event(USbegin(e)) in process 1
Translating the process into Horn clauses...
Completing...
Starting query inj-event(USend(e)) ==> inj-event(USbegin(e))
RESULT inj-event(USend(e)) ==> inj-event(USbegin(e)) is true.
-- Query not attacker(svalueA[]); not attacker(svalueB[]) in process 1
Translating the process into Horn clauses...
Completing...
Starting query not attacker(svalueA[])
RESULT not attacker(svalueA[]) is true.
Starting query not attacker(svalueB[])
RESULT not attacker(svalueB[]) is true.

--------------------------------------------------------------
Verification summary:

Query inj-event(SUend(e)) ==> inj-event(SUbegin(e)) is true.

Query inj-event(USend(e)) ==> inj-event(USbegin(e)) is true.

Query not attacker(svalueA[]) is true.

Query not attacker(svalueB[]) is true.

--------------------------------------------------------------
```

그림 4. ProVerif 검증 결과
Fig. 4. Result of ProVerif analysis.

각의 인증 단계에 대한 데모(Demo)를 진행하였다. 마지막으로 전체 프로토콜에 대한 모델을 제시함으로서 그림 4와 같이 제안한 프로토콜의 안전성 검증을 성공적으로 수행하였다.

4.2 보안 분석

본 논문에서 제안한 프로토콜의 보안 속성 분석 및 Yang등의 기법과 Noh등의 기법과의 비교 분석을 제시한다. Yang등의 기법에서 모든 환자가 같은 마스터 비밀키를 이용함으로서 보안에 문제점이 제시되었다. Noh등의 기법은 환자마다 다른 마스터 비밀키를 부여함으로서 Yang등의 기법에 존재하는 문제를 해결하였으나, HMS의 데이터베이스에 환자의 개인키와 마스터 비밀키를 저장함으로서 보안에 취약했다. 표 2는 본 논문에서 제안한 프로토콜과 관련된 기법간의 보안 속성에 대한 비교를 보여준다. 본 절에서는 보안 속성에 대한 분석을 제시한다.

- 단일 헬퍼키 문제

Yang등의 기법은 시스템에 존재하는 모든 환자들에게 동일한 헬퍼 비밀키를 부여함으로서 임의의 사용자의 BH를 다른 사용자가 습득하였을 경우 자신이

표 2. 보안 속성 비교
Table 2. Security feature comparison.

Scheme / Security feature	Yang et al. in [7]	Noh et al. in [9]	Proposed
Key insulation	X	□	□
Security of PHI	X	X	□
Safety of key	X	X	□

보유한 헬퍼키를 이용하여 새로운 주기의 서비스 개인키를 생성할 수 있는 문제가 있었다. 이를 해결하기 위해서, 제안한 프로토콜에서도 Noh등의 기법과 동일하게 환자마다 다른 헬퍼 비밀키를 부여함으로써 BH를 분실한 경우 발생할 수 있는 보안 문제를 해결하였다. 즉, 본 논문에서 제안한 프로토콜에서 비밀키의 생성에 필요한 서비스 개인키의 갱신은 HKU를 소유하고 있는 환자 자신만이 가능함을 보증할 수 있다.

- 의사 신원정보의 기밀성

환자의 익명성이 보장되더라도 환자의 의료정보 관련 데이터로부터 의사의 신원정보가 노출된다면 환자의 병력 관련 프라이버시 침해 문제가 발생할 수 있다. 제안한 프로토콜은 환자의 PHI 관련 정보를 C_3를 통해 HMS에게 전송한다. 특히 C_3는 K_{PTi-H}를 이용하여 암호되어 전송된다. 즉, 프라이버시가 포함된 환자의 PHI 관련 정보는 HMS도 알 수 있는 방법이 없다. 즉, 본 논문에서 제안한 프로토콜은 의사 신원정보의 기밀성을 제공한다.

- 훔친 검증자 공격 안전성

Noh등의 기법에서는 HMS가 등록 과정에서 환자와 관련된 $<PID_{PTi}, PSK^0_{PTi}, hk_{PTi}, HP_{PTi}>$를 데이터베이스에 저장하여 인증에 활용한다. 하지만 이는 공격자가 훔친 검증자 공격을 통해 HMS 데이터베이스에 저장된 정보를 획득할 수 있다[15]. 이후 공격자는 데이터베이스 정보로부터 $TK^{t+1}_{PTi}=\hat{e}(hk_{PTi}, H_1(PID_{PTi}||HP_{PTi}||t+1)-H_1(ID_{PTi}||HP_{PTi}||t))$를 계산하고 새로운 개인키 $PSK^{t+1}_{PTi}=PSK^t_{PTi}+TK^{t+1}_{PTi}$를 생성할 수 있는 취약성이 존재한다. 이를 해결하기 위해 제안한 프로토콜은 HMS가 데이터베이스를 유지하지 않고 필요한 정보를 USIM에 저장하도록 하였다. 또한 USIM에 저장된 정보는 적법한 소유자 인증을 통과한 사용자만 이용할 수 있다. 즉, 본 논문에서 제안한 프로토콜은 훔친 검증자 공격에 안전하다.

- 환자의 PHI 기밀성

HMS에게 전송된 환자의 PHI는 PT와 D_j 간 공유된 비밀키 K_{PTi-D_j}로 암호되어 전송된다. 즉, PT의 PHI는 암호된 $C_1=E_{KPTi}(\text{PHI}, ts)$, 과 $C_3=E_{KPTi-H}(HP_{PTi}, DP^j_{PTi}, C_{PTi}, D_j, C_1, C_2)$를 통해 HMS에게 전송된다. 이 과정에서 HMS도 PHI 관련 정보를 확인할 수 없다. 즉, 제안한 프로토콜은 환자의 PHI 기밀성을 제공한다.

- 전송된 정보의 무결성

인증과 전송 단계에서 만약 공격자가 메시지 $<B_{PTi}, VID_{PTi}, VSK_{PTi}, C_3>$를 도청했다고 가정하면, PT의 PHI가 포함된 C_3는 $K_{PTi-H}=KDF(\hat{e}(PSK^t_{PTi}', H_1(PU_{HMS})))$를 이용하므로 PT의 개인키 PSK^t_{PTi}'을 알아야만 확인할 수 있다. 이는 VSK_{PTi}로 부터 계산할 수 있지만 HMS의 마스터키인 s_0를 획득할 수 있는 방법이 없기 때문에 공격자는 공격에 성공할 수 없다. 만약 공격자가 위조된 정보를 통해 HMS에게 전달할 경우 C_3 관련 정보의 진위는 C_2 검증을 통해 확인할 수 있다. 또한, 세션의 시간인 ts를 매개변수로 이용함으로서 메시지의 신선성도 보증할 수 있다.

4.3 성능 분석

제안한 프로토콜의 성능 분석을 위해서는 인증 및 전송 단계에 초점을 맞춘 분석을 제시한다. 구현 환경은 Dual CPU E2200 2.2GHz의 CPU와 2GB 용량의 메모리와 Ubuntu 운영체제를 활용하였다. 성능 분석을 위해 네트워크 참여자 각각의 프로토콜 수행에 따른 연산 요구량을 고려한다. 특히, 본 논문에서 제안한 프로토콜과 Noh등의 기법, 그리고 Yang등의 기법과의 비교도 제시한다. 명확한 연산량 분석을 위한 중요한 지표로서 겹선형 페어링(T_p)과 대칭키 암호·복호(T_s) 그리고 일방향 해쉬함수(T_h) 연산을 고려한다. 표 3은 프로토콜 간 연산에 대한 비교를 제시한다.

제안한 프로토콜의 구체적인 연산 오버헤드를 위한 주요 연산 T_p, T_s, T_h에 초점을 맞춘 연산의 수행시간은 각각 5.811 ms, 0.0046 ms, 0.0023 ms가 필요하였다. 그림 5에서 보여주는 바와 같이 Yang등의 기법과 Noh등의 기법은 각각 40.7322 ms와 34.9051 ms가 필요하였다. 본 논문에서 제안한 프로토콜은 52.3473 ms의 시간이 필요하다. 표 3과 그림 5에서의 결과를 보았을 때, 본 논문에서 제안한 프로토콜이 기존의 노등의 기법보다 17.4422 ms정도 연산의 부하가 필요하였지만, 이것은 보안 분석으로 보았을 때 제안한 프로토콜의 보안과 프라이버시 보증을 위한 부하로 고려될 수 있다.

표 3. 성능 비교
Table 3. Performance comparison.

Scheme \ Entity	PT(BH)	HMS	D_j
Yang et al. in [7]	$2T_p+2T_h+3T_s$	$3T_p+4T_h+3T_s$	$2T_p+2T_h+2T_s$
Noh et al. in [9]	$2T_p+2T_h+3T_s$	$1T_p+1T_h+1T_s$	$3T_p+2T_h+2T_s$
Proposed	$4T_p+6T_h+2T_s$	$2T_p+4T_h+1T_s$	$3T_p+3T_h+1T_s$

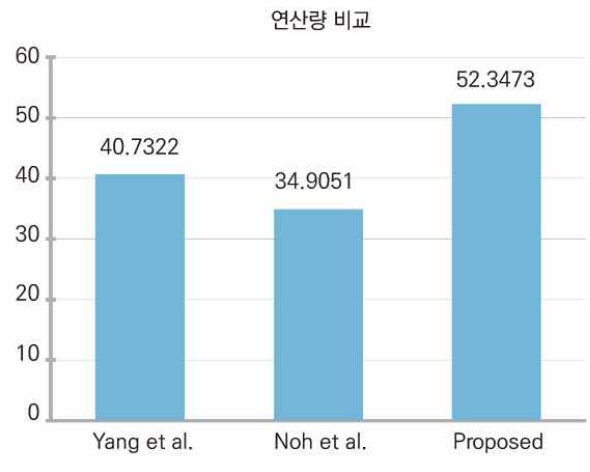

그림 5. 연산량 비교
Fig. 5. Computational overhead comparison.

V. 결 론

본 논문에서는 Noh등이 제안한 개선된 개인정보 전송 기법의 보안 취약점인 훔친 검증자 공격을 해결할 수 있는 스마트카드 기반 인증 및 개인정보 전송 프로토콜을 제안하였다. Noh등의 기법은 HMS 서버에 검증자 테이블을 유지해야 하는 문제가 있었다. 하지만 검증자 테이블 기반 프로토콜은 훔친 검증자 공격에 대한 안전성을 제공하지 못하는 문제점이 다양한 연구에 의해서 도출되었다. 따라서 제안한 프로토콜은 HMS에 검증자를 유지해야 할 필요가 없는 스마트카드를 이용한 기법으로 설계함으로서 안전성을 보장하였다. 이를 통해 보다 안전하고 프라이버시를 보증할 수 있는 새로운 프로토콜을 제안할 수 있었다. 하지만, 보안성 및 프라이버시 강화를 통해 기존의 기법보다 연산의 부하가 발생하였다. ProVerif를 통한 정형화된 툴을 이용한 보안성 검증을 제시하였다. 본 논문에서 제안한 프로토콜을 토대로 보다 안전하고 프라이버시를 보증할 수 있는 원격 헬스케어 모니터링 시스템을 구축할 수 있을 것이다.

References

[1] M. Hussain, T. Ali, J. Hussain, F. A. Satti, U. Akhtar, J. Bang, T. Heo, S. Kang, B. Kang, and S. Lee, "Intelligent medical platform: IMP," *KICS Inf. & Commun. Mag.*, vol. 37, no. 9, pp. 3-17, 2020.

[2] T. D. Subash, T. D. Subha, A. Nazim, and T. Suresh, "Enhancement of remote monitoring implantable system for diagnosing using IoMT," *Materialstoday*, 2021, https://doi.org/10.1016/j.matpr.2020.09.816

[3] J. Bang, T. Heo, and T. Ali, "Intelligent-knowledge authoring tool (I-KAT)," *KICS Inf. & Commun. Mag.*, vol. 37, no. 9, pp. 18-27, 2020.

[4] H. Kim and S. Moon, "Design and implementation of an active risk situation estimation system in smart healthcare using bio and environmental sensors," *J. KICS*, vol. 45, no. 5, pp. 914-925, 2020.

[5] H. Kim, "Freshness-preserving non-interactive hierarchical key agreement protocol over WHMS," *Sensors*, vol. 15, pp. 23742-23757, 2014.

[6] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE J. Sel. Areas in Commun.*, vol. 27, no. 4, pp. 365-378, 2009.

[7] H. Yang, H. Kim, and K. Mtonga, "An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system," *Peer-to-Peer Netw. and Appl.*, vol. 8, no. 6, pp. 1059-1069, 2014.

[8] P. Gopal and P. V. Reddy, "Efficient id-based key-insulated signature scheme with batch verifications using bilinear pairing over elliptic curve," *J. Discrete Math. Sci. and Cryptography*, vol. 18, no. 4, pp. 385-402, 2015.

[9] S. Noh, Y. Park, and K. Rhee, "An enhanced secure health data transmission protocol using key insulation in remote healthcare monitoring system," *J. Korea Multimedia Soc.*, vol. 19, no. 12, pp. 1981-1991, 2016.

[10] H. Toral-Cruz, D. He, A. D. Mihovsak, K. R. Choo, and M. K. Khan, "Reliable and Secure e-Health networks," *Wirel. Pers. Commun.*, vol. 117, no. 1, pp. 1-6, 2021.

[11] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi, "A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks," *Wirel. Pers. Commun.*, vol. 117, no. 1, pp.

47-69, 2021.

[12] X. Yuan, X. Wang, C. Wang, J. Weng, and K. Ren, “Enabling secure and fast indexing for privacy-assured healthcare monitoring via compressive sensing,” *IEEE Trans. Multimedia*, vol. 18, no. 10, pp. 2002-2014, 2016.

[13] B. Blanchet, “An efficient cryptographic protocol verifier based on prolog rules,” in *Proc. 14th IEEE Wkshps. Comput. Secur. Foundations*, pp. 82-96, Novia Scotia, Canada, 2001.

[14] D. Dolev and A. C. Yao, “On the security of public key protocols,” *IEEE Trans. Info. Theory*, vol. IT-29, no. 2, pp. 198-208, 1983.

[15] Y. Chang and C. Chang, “Authentication schemes with no verification table,” *Applied Math. and Computation*, vol. 167, no. 2, pp. 820-832, 2005.

류 현 호 (Hyunho Ryu)

2020년 3월~현재 : 경일대학교 컴퓨터사이언스학부 사이버보안전공

2020년 3월~현재 : 경일대학교 정보보호 연구 실 연구원

<관심분야> 정보보호, 헬스케어 보안, 블록체인, 네트워크 보안, 인공지능 보안, 암호 프로토콜, 자율주행 보안

[ORCID:0000-0002-2860-1612]

김 현 성 (Hyunsung Kim)

2002년 2월 : 경북대학교 컴퓨터공학과 공학박사

2002년 3월~현재 : 경일대학교 컴퓨터사이언스학부 정교수

2015년 12월~현재 : 말라위대학교 수학과 방문교수

2008년 12월~2010년 2월 : 더블린시립대학교 방문교수

<관심분야> 인지무선네트워크 보안, 네트워크 보안, 암호 프로토콜, 암호구현, 정보보호

[ORCID:0000-0002-7814-7454]