텔레메틱스 환경에서 이동성과 보안성을 고려한 지문정보를 이용한 사용자 인증 프로토콜에 관한 연구

준회원 김 태 섭*, 정회원 오 룡*, 준회원 이 상 준*, 이 성 주**, 김 학 재**,
정회원 정 용 화**, 종신회원 조 충 호*

A Study on the Fingerprint-based User Authentication Protocol Considering both the Mobility and Security in the Telematics Environment

Tae-sub Kim* ***Associate Member***, Ryong Oh* ***Regular Member,***
Sang-Joon Lee*, Sung-ju Lee**, Hak-jae Kim** ***Associate Members***,
Yong-wha Chung** ***Regular Member***, Choong-ho Cho* ***Lifelong Member***

요 약

최근 인터넷 및 이동통신 기술의 발전과 함께 차량에서 무선 단말을 이용하여, 유선 네트워크의 서비스를 이용할 수 있는 텔레메틱스 환경이 실현되고 있다. 텔레메틱스 환경 구축에 앞서 선결해야 하는 문제로는 무선 네트워크에서 보안성을 고려한 사용자 인증의 문제, 보안성과 이동성의 상충성, 인증의 가용성 등이 있다. 본 논문에서는 텔레메틱스 환경 구축에 있어서 이러한 문제점들을 해결할 수 있는 효율적인 사용자 인증 프로토콜을 제안한다. 사용자 인증 프로토콜에서는 차량에서 사용자의 인증이 용이하고 분실, 도난 망각의 위험이 없는 생체정보(지문정보)를 이용하고, 사용자 인증 정보를 암호화하기 위한 임시키(Session Key)를 생성하기 위한 마스터키(Master Key)분배가 이루어 진다. 특히, 이동성을 고려하여 보안상 취약점을 최소화하고 보다 효율적인 시스템을 위하여 액세스포인트(Access Point)간의 인증정보를 보다 안전하게 전달할 수 있는 프로토콜을 제안한다. 또한 텔레메틱스의 여러 환경 중 무선랜 환경에서 제안한 프로토콜을 구현하였고, 제안한 프로토콜에 대한 다양한 공격으로부터의 안전성을 분석 하였다.

Key Words : User authentication protocol, Telematics, Fingerprint, Wireless LAN, Key distribution protocol

ABSTRACT

Recently, according to being advanced internet, mobile communication technique, Telematics environment which users in vehicle can use internet service in LAN(Local Area Network) via mobile device has being realized. In this paper, we propose the remote user authentication protocol to solve these issues. Additionally, we use biometrics(fingerprint) for our user authentication protocol cause it can provide to avoid critical weakness that can be lost, stolen, or forgotten and to make authentication easily. In our user authentication protocol, to protect the biometric we use session key which is generated from master key distributed in our key distribution protocol. In particular, we propose secure protocol between APs considering weakness of security in mobile environment. Based on implementation of our proposed protocol, we conform that our proposed protocols are secure from various attack methods and provide real-time authentication.

※ 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었습니다.
* 고려대학교 컴퓨터정보학과 데이터통신및네트워크 연구실(ree31206@korea.ac.kr),
** 고려대학교 컴퓨터정보학과 병렬알고리즘 연구실(peacfeel@korea.ac.kr)
논문번호 : KICS2007-06-275, 접수일자 : 2007년 06월 13일, 최종논문접수일자 : 2007년 11월 5일

Ⅰ. 서 론

최근 자동차에 컴퓨터와 이동통신이 결합되면서 자동차의 모습이 빠르게 변하고 있다. 예를 들어, 기존의 오토 PC는 라디오/DVD 조작, 연비 체크, 엔진 고장 여부, 엔진/타이어 교체 주기, 좌석 조절, 차량 실내 외 기온 제공 등 단순한 기능만을 제공하였으나, 이동통신 기술과 결합되면서 운전자에게 다양한 정보를 실시간으로 제공하는 텔레메틱스 시스템으로 발전하고 있다.

텔레메틱스 환경 구축에 앞서 안전한 서비스를 받기위해 선결해야 하는 문제로는 무선 네트워크에서 보안성을 고려한 사용자 인증의 문제, 보안성과 이동성의 상충성, 인증의 가용성 등의 문제를 해결할 수 있는 기술이 필요하다. 일반적으로 정보시스템에 접근하기 위한 사용자 인증 수단으로 패스워드, PIN(Personal Identification Number) 또는 스마트카드 등의 전통적인 방법들이 널리 이용되고 있으나, 이러한 인증수단은 분실, 도난, 망각으로 인한 위험이 존재한다. 이를 해결하기 위하여 개인의 고유한 생체정보인 신체적 또는 행동학적 특징에 따라 사람들의 신원을 확인하는 생체인증 시스템이 대두되고 있다.

본 논문에서는 텔레메틱스의 여러 환경 중 이동통신 기술의 하나인 WLAN(Wireless Local Area Network)환경을 가정하였다. WLAN은 무선 네트워크 카드를 장착한 무선 단말에서 LAN(Local Area Network)과 WLAN을 연결해 주는 AP(Access Point)를 통하여 WLAN 상의 장치에서LAN 상의 정보시스템을 이용할 수 있게 해주는 기술이다. WLAN 기술을 이용하면 이동 전화 기술을 이용할 경우에 비해 속도가 빠르고, 장비의 비용이 10배정도 저렴하기 때문에 무선인터넷 시장에서 경쟁력을 갖추고 있다고 보여지며, 향후 더 많은 이용이 예상되고 있다. 그러나, WLAN은 편리함과 동시에 두 가지 보안상 문제를 가지고 있다. 첫 번째는 승인된 사용자에게만 접속을 허용하는 접속(Access)에 관한 보안이며, 다른 하나는 스니퍼(Sniffer) 등을 이용해 WLAN을 통해 전송되는 내용을 도청하는 행위를 방지하는 것이다. 특히 유선 네트워크와 달리 무선랜에서는 AP만 설치되어 있는 곳이면 누구나 쉽게 AP를 통해 네트워크를 이용할 수 있다. 따라서, WLAN 환경에서 LAN 상의 정보시스템에 접근 하기 위한 사용자 인증 및 보안 프로토콜이 필요하다. 또한 무선랜은 그 특성상 단말의 이동이 빈번하게 발생하여, 핸드오프시(Handoff)마다 반복되는 인증으로 많은 오버헤드를 야기시킨다. 따라서 이동성을 고려하여 보안상 취약점을 최소화하고 보다 효율적인 시스템을 위하여 AP간의 인증정보를 보다 안전하게 전달할 수 있는 프로토콜이 필요하다.

이에 따라 본 논문에서는 생체정보 중 가장 보편적으로 사용되는 지문정보를 이용하고, 전송채널에서 안전하게 전송할 수 있도록 기밀성과 무결성을 보장하는 사용자 지문인증 프로토콜 및 마스터 키 분배 프로토콜 그리고 이동단말의 보안 프로토콜을 제안한다. 간단한 실험환경 구축을 통하여 텔레메틱스 환경에서 편리하고 안전한 인증시스템을 확인하였다.

본 논문의 구성을 살펴보면 2장에서는 시스템 환경 및 프로토콜 구현 시 요구사항에 대해 알아보고, 3장에서는 텔레메틱스 환경에서 사용자 인증을 위한 프로토콜에 대해 제안한다. 4장에서는 제안한 프로토콜의 구현 및 보안성 평가를 하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 시스템 환경 및 요구사항

2.1 시스템 환경

본 논문의 시스템 환경은 그림 1과 같다. 그림 1의 시스템 환경은 LAN(Local Area Network)상에 있는 사용자 인증을 위한 서버인 AS(Authentication Server)와 키를 분배해 주기 위한 KDC(Key Distribution Center) 그리고 AP 무선으로 연결되어 서비스를 받고 있는 단말을 지닌 자동차로 구성이 되어 있다.

기존 다수의 무선 환경에서 인증에 대한 연구에서 패스워드 방식을 통해 접근을 인증 받았으나, 텔레메틱스 환경에서 운전자의 편의를 고려하여 비교

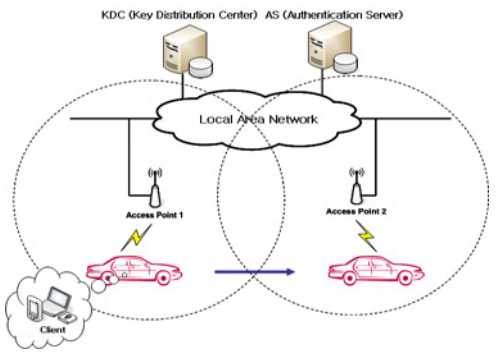

그림 1. 사용자 인증 시스템 환경

적 인증이 용이한 지문정보를 선택했다. 지문 정보를 이용한 인증에서는 사람의 지문정보는 유한하기 때문에, 안전하지 않는 네트워크를 통해 지문정보를 전송할 때 지문정보를 보호하기 위한 보안이 필수적이다. 따라서, 본 논문의 시스템 환경에서는 사용자의 지문정보를 암호화하기 위해서 사용자가 인증을 요청 시마다, 임시키를 생성하여 지문정보를 보호한다.

임시키를 생성하기 위해 키 생성을 위한 정보가 임시키를 공유하는 개체들 사이에서 사전에 교환되어야 한다. 암호화 알고리즘은 비대칭키(Asymmetric Key)와 대칭키(Symmetric Key) 알고리즘이 있는데, 전자의 경우 후자에 비해 암호화를 수행하는 속도가 느리지만 수학적으로 보안의 강도가 높다. 따라서, 임시키를 생성하기 위한 데이터는 데이터 크기가 비교적 작기 때문에 느리지만 보안성이 비교적 높은 비대칭키 알고리즘을 이용하여 보안성를 높여서, 부정당한 사용자가 임시키를 생성하지 못하게 할 수 있다. 지문 정보의 경우 상대적으로 데이터 크기가 크기 때문에 임시키를 이용하여 비교적 속도가 빠른 대칭키 방식으로 암호화를 수행한다.

비대칭키 알고리즘으로 암호화된 데이터 교환을 하는 개체들은 서로의 공개키(Public Key)를 가지고 있어야 한다. WLAN과 LAN상에 있는 개체들은 서로를 신뢰할 수 없기 때문에, 공개키를 네트워크 상에서 공유하기 위해서, 키 분배 프로토콜이 필요하다. 따라서, 본 논문에서 제안하는 시스템에서 공개키를 공유하기 위한 제반 사항은 다음과 같다. 첫째, 모든 개체들(i.e., 사용자 단말, AP, AS)은 장치가 초기화되기 전에 각자의 공개키와 개인키(Private Key)를 가지고 있어야 한다. 둘째, 모든 개체의 공개키는 신뢰할 수 있는 제 3자(Trust Third Party) 기관인 KDC의 데이터베이스에 보관이 되고, LAN 상의 KDC를 통해 공개키 분배가 일어난다.

그림 1에서 차량이 AP1(Old AP)에서 인증이 수행된다면, 차량이 AP2(New AP)로 이동한 후에는 재인증 과정이 필요 없이 AP1과 AP2간의 안전한 보안 프로토콜을 이용하여 유선망에서 인증이 수행된다. 이 경우, 단말의 이동 시 AP의 경로가 바뀔 때마다 무선망에서 사용자의 중요한 인증 정보인 지문정보가 불필요하게 노출되지 않고, 인증 과정을 새로 시작하는 것 보다 AP간의 통신이 상대적으로 빠르게 수행되기 때문에 보다 안전하고 효율적이다.

2.2 지문인증 시스템

지문인식시스템은 그림2과 같이 등록(Enrollment)과 검증(Verification)과정으로 구분된다. 오프라인에서 지문의 등록은 지문영상 전처리(Pre-Processing), 지문 특징점 추출(Minutiae Extraction), 그리고 서버에 저장(Store)하는 순으로 진행된다. 그리고 온라인에서의 지문 검증은 지문 입력 센서로부터 입력된 영상에서 추출된 특징과 데이터베이스(System DB)에 저장된 특징을 정합하여 본인 여부를 확인한다. 본 논문에서는 사용자 지문인식시스템에서 전처리 및 지문의 특징 추출을 무선 단말에서 수행하고 WLAN을 통해 AP로 전송되고, LAN 상의 지문 인증 서버에서 인증 받을 사용자 ID와 지문 특징점을 지문 인증 서버에 등록된 데이터베이스와 매칭을 한다. 지문정보를 이용하여, 사용자 인증을 함으로써, 기존 패스워드의 기반 인증의 보안상 취약성(i.e., 전수조사 공격), 망각, 분실, 도난 등의 위험을 해결할 수 있다.

일반적으로 공격 포인트에 따라서 시스템 내부 모듈을 공격(i.e., Trojan Horse), 시스템 데이터 베이스에 대한 공격, 통신 채널(WLAN/LAN) 상에서 공격(i.e., Replay Attack)으로 나눌 수 있다. 본 논문에서는 프로토콜을 통하여 통신 채널 상에서의 공격에 대비한 방법에만 국한해서 언급한다.

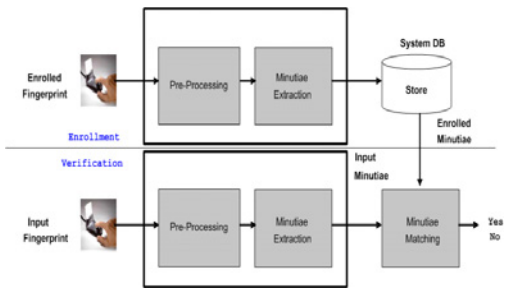

그림 2. 일반적인 지문인식 과정

Ⅲ. 제안한는 사용자 인증 프로토콜

앞 장에서 언급한 시스템의 환경 및 요구사항을 바탕으로 키 분배 프로토콜, 사용자 인증 프로토콜, 이동단말을 고려한 AP간의 보안프로토콜을 제안한다.

우선 제안하는 프로토콜을 살펴보기 이전에 각 개체들 사이에서 쓰이는 용어에 대하여 알아볼 필요가 있다. 표 1과 같이 각 용어와 용어에 대한 설명이 되어있다.

표 1. 용어에 대한 설명

용 어	용어설명	용 어	용어설명
C	클라이어트(Client)	Kc-as	C와 AS의 공유 세션키(Session Key)
AS	인증서버(Authentication Server)	Kap-as	AP와 AS의 공유 세션키(Session Key)
AP	액세스포인트(Access Point)	Fingerprint Minutiae	지문의 특징점 정보
KDC	키 분배센터(Key Distribution Center)	UID	지문 소유자의 ID
IDx	x의 장치 ID(Device Identifier)	Hash(x)	일방향 해쉬 함수
Nx	임의의 수(Random Value)	AP1	Access Point 1(Old AP)
f(x)	임의의 수를 바꾸기 위한 함수	AP2	Access Point(New AP)
KUx	x의 공개키(Public Key)	BSSID1	AP1 MAC address
KRx	x의 개인키(Private Key)	Kap-s	AP1과 AP2간의 세션키(Session Key)

그림 3. 4는 임시키를 생성하기 위해 사용자, AP가 신뢰할 수 있는 제 3자 KDC를 통해 AS와 키를 공유하는 프로토콜이다. 본 프로토콜은 AP와 단말이 처음 초기화될 때, 단 한번만 일어나며 한번 분배된 공개키는 AS의 데이터베이스에 저장된다.

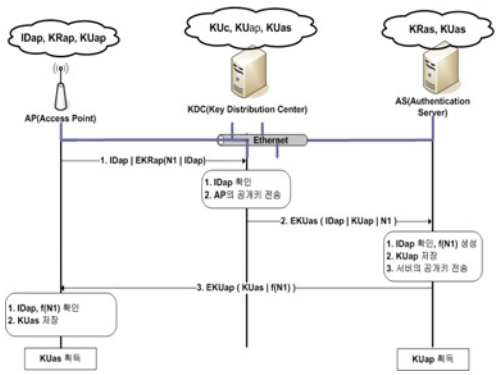

그림 3. AP의 키 분배 프로토콜

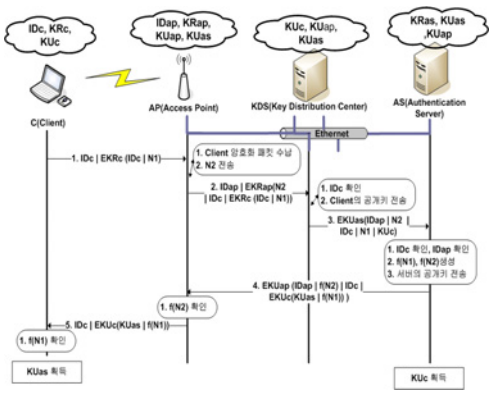

그림 4. 사용자의 키 분배 프로토콜

3.1 AP의 키 분배 프로토콜

3.1.1 키 분배 요청

(1) AP에서 KDC로의 메시지 : IDap | EKRap(N1 | IDap)
LAN상에서 AP 는 임의의 수 N1(메시지의 안전한 전송 및 회신 메시지의 유효성을 확인)를 생성하여 KDC에게 인증 받을 장치 고유번호와 함께 자신의 개인키로 전자 서명(KDC에게 AP의 신뢰성를 입증)을 해서 KDC로 전송한다.

3.1.2 키 분배 응답

(1) KDC에서 AS로의 메시지 : EKUas(IDap | KUap | N1)
KDC에서 해당 장치 식별번호(IDap)로 확인한 KUap를 AS의 KUas로 암호화하여, AS에게 전송한다. 또한, AP가 자신의 키 분배 요청이 안전하게 전송되었는지 확인할 수 있도록 AP가 생성한 N1을 암호화 하여 전송한다.

(2) KDC에서 AS로의 메시지 : EKUas(IDap | KUap | N1)
KDC에서 해당 장치 식별번호(IDap)로 확인한 KUap를 AS의 KUas로 암호화하여, AS에게 전송한다. 또한, AP가 자신의 키 분배 요청이 안전하게 전송되었는지 확인할 수 있도록 AP가 생성한 N1을 암호화 하여 전송한다.

3.1.3 키 분배 완료

AP는 3의 메시지를 전송 받은 후, AS의 KUas를 저장한다.

3.2 사용자의 키 분배 프로토콜

3.2.1 키 분배 요청

(1) C에서 AP로의 메시지 : : IDc | EKRc(IDc |N1)
WLAN상에서 C의 임의의 수 N1과 IDc를 자신의 개인키로 전자 서명을 해서 LAN과 WLAN의 매개체인 AP로 전송을 한다.

(2) AP에서 KDC로의 메시지 : IDap | EKRap{N2 | IDc | EKRc(IDc | N1) }
C로부터 전송 받은 키 분배 요청 메시지를 AP가 보증을 하는 의미에서 1의 메시지를 IDap와 AP가 생성한 임의의 수N2와 함께 자신의

KRap로 전자 서명을 해서 KDC로 전송한다.

3.2.2 키 분배 응답

(1) KDC에서 AS로의 메시지 : (IDap | N2 | IDc | N1 | KUc)
KDC에서 AP로부터 전송 받은 2.의 메시지를 AP의 KUap로 복호화 함으로써 검증하고, C의 메시지KRc(IDc | N1) 또한 IDc로 KUc를 찾아서, KUc로 복호화 함으로써 유효성을 검증한다. 이 두 검증이 정당할 때, AP와 C로부터 전송받은 N1과 N2와 AS에서 AP와 C의 정보를 저장할 수 있도록 IDc, IDap를 KUas로 암호화한다.

(2) AP에서 AP로의 메시지 : { IDap | f(N2) | IDc | EKUc(KUas | f(N1)) }
AS에서 KDC로 받은 키 분배 응답 메시지를 복호화하여 KUc를 IDc와 함께 데이터베이스에 저장하고, N1과 N2를 이용해 f(N1), f(N2)를 생성한다. AP에서 C에게 전송할 메시지의 기밀성을 보장하기 위해서 AP에게 전송할 암호화 메시지(i.e., KUap로 암호화된 메시지) 내부에 C로 전송할 암호화 메시지(i.e., KUc로 암호화된 메시지 : : KUas와 f(N1)을 암호화)를 암호화하여 수납한다. 따라서, AP는 IDap와 f(Nc)만을 확인할 수 있고, KUc로 암호화되어 수납된 메시지는 C에게 무결성이 보장된 상태로 전송된다.

3.2.3 키 분배 완료

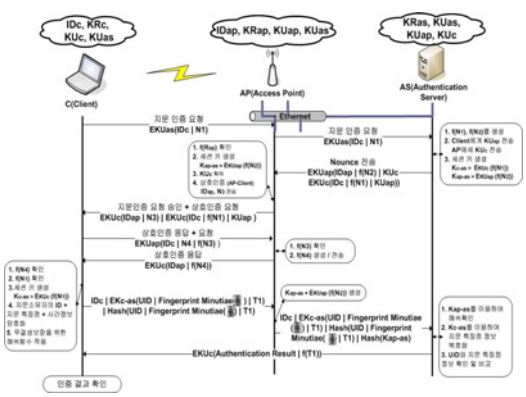

그림 5. 사용자 인증 프로토콜

(1) AP에서 C로의 메시지 : IDc | EKUc(KUas | f(N1))
AP는 3.의 메시지를 복호화 후에, f(N2)를 통해 유효성을 확인하고, C의 KUc로 암호화되어 수납된 메시지를 C에게 전송하고, C는 AP로부터 전송받은 5.의 메시지로부터f(N1)을 통해 유효성을 확인하고 AS의 KUas를 저장한다.

3.3 사용자 지문 인증 프로토콜

3.3.1 지문 인증 요청

(1) C에서 AP를 거쳐 AS로의 메시지 : EKUas(IDc | N1)
WLAN상의 C에서 사용자 인증을 받기 위해서 AP를 통해 IDc와 임시키를 생성하기 위한 임의의 수 N1을 키 분배 프로토콜에서 획득한 AS의 KUas로 암호화를 해서 AP를 통해 AS로 전송한다.

3.3.2 지문 인증 요청 응답

(1) AS에서 AP로의 메시지 : EKUap{IDap | N2 | KUc | KUc(IDc | f(N1) | KUap) }
AS는 AP로부터 전송 받은 C의 지문 인증 요청 메시지를 복호화하여 N1을 획득한다. 키 분배 프로토콜을 통해 AS는 KUap와 KUc를 가지고 있다. 따라서, N1을 이용해서, f(N1)을 KUc로 암호화하여 KUc-as를 생성한고, 임의의 수 N2를 생성하여, AP와의 임시키 공유를 위해, f(N2)를 KUap로 암호화해서 KUap-as를 생성한다. KUap-as는 차후 AP에서 AS로 정당한 AP인지 확인할 때 인증자 역할을 한다. 인증 받을 지문 정보를 C가 AS로 전송하기 전에 C와 AP가 서로 믿을 수 있어야 한다. 따라서, AS는 C에게 AP의 KUap를 AP에게 C의 KUc를 분배하여, C와 AP 사이에서CHAP(Challenge Response)과정을 가능하게 해준다. 따라서, AS에서 AP에게 IDap, N2, KUc, C에게 기밀성 있는 전송을 위해 KUc로 암호화한 메시지EKUc(IDc, f(N1), KUap)를 수납하고 KUap로 암호화 하여 전송한다.

3.3.3 AP와 C의 상호 인증과정 (Challenge/Response)

(1) AP에서 C로의 메시지 : EKUc(IDap | N3) | EKUc(IDc | f(N1) | KUap)
AS로부터 전송 받은 메시지를 KRap를 이용해

복호화하고 임시키를 생성하기 위한 N2를 획득 후, f(N2)를 자신의 KUap로 암호화 하여, 임시키 Kap-as를 생성한다. 또한, AS로부터 전송 받은 KUc를 이용해C와 상호인증을 할 수 있다. 상호 인증을 위해 임의의 수 N3를 생성하고, KUc를 이용해 IDap와 N3를 암호화한다. AS에서 C에게 전송하는 암호화 메시지 EKUc(IDc | f(N1) | KUap)와 같이 상호인증 메시지(EKUc(IDap | N3))를 C에게 전송한다.

(2) C에서 AP로의 메시지 : EKUap(IDc | N4 | f(N3))
AP로부터 AS의 사용자 인증 응답 메시지와 AP의 상호 인증 요청 메시지를 받는다. AS로부터 받은 메시지를 복호화하여, 임시키를 생성하기 위한 정보(f(N3))를 이용해 KUc로 암호화하여 임시키(KUc-as)를 생성하고, AP와 상호인증을 위한 AP의 KUap를 획득한다. AP에게 C가 정당한 사용자 임을 확인시키기 위해, C의 장치 고유번호(IDc)와 AP로부터 전송 받은 N3를 이용해, f(N3)를 생성하여 AP에게 C가 정당한 개체임을 확인시킨다. 또한, C가 생성한 임의의 수 N4를 생성해 AP가 정당한 개체인지 확인하기 위해, f(N3), IDc와 함께 KUap로 암호화하여 AP에게 전송한다.

(3) AP에서 C로의 메시지 : EKUc(IDap | f(N4))
AP는 C부터 전송 받은 메시지를 KRap로 복호화하여 f(N3)를 이전 4의 메시지에서 보냈던 N3와 비교하여 유효성을 확인하고, C가 AP가 정당한 개체인지 확인하기 위한 N4를 이용해 f(N4)를 생성하여, AP의 장치 고유번호(IDap)와 함께 C에게 전송한다. C는 이 메시지를 복호화하여 유효성을 판단한 후에, 상호 인증을 완료한다.

3.3.4 지문 정보 전송

(1) C에서 AS로의 메시지 : IDc | EKc-as(UID | Fingerprint Minutiae | T1) | Hash(UID | Fingerprint Minutiae | T1)
3).의 과정을 통해서 상호 인증이 성공되면, C는 WLAN 상에서 중개자 AP를 신뢰할 수 있고, AP에게 지문 정보 메시지를 AS에게 전달할 수 있게 된다. C는 사용자의 단말에 장착된 센서로부터 입력 받은 지문 이미지의 특징점을 추출하여 인증 받을 지문의 소유자 식별자(UID)와 함께, Kc-as를 이용해 대칭키 암호화를 한다. 여기서, C에서 인증이 요청되는 매 세션(Session)마다 임시키는 바뀌지만, 동일 세션 내에서 암호화된 지문정보의 재전송이 C에서 AS로 전송이 되면, 암호화된 메시지의 보안이 떨어질 수 있다(i.e., 부정당한 사용자가 암호화된 지문정보를 획득하여, 임시키 혹은 지문 정보를 획득할 수 있음), 따라서, 동일 세션에서 지문 이미지를 암호화 할 때, 세션의 시간 정보(T1: Time Stamp)를 지문 정보와 함께 암호화해서 전송을 한다. 또한, 암호화된 지문 정보의 무결성을 보장하기 위해, 일방향 해쉬 함수를 적용한다.

(2) AP에서 AS로의 메시지 : IDc | EKc-as(UID | Fingerprint Minutiae | T1) | Hash(UID | Fingerprint Minutiae | T1) | Hash(Kap-as)
AP는 C의 지문 정보를 AS에게 보낼 때, AS가 AP를 신뢰할 수 있게 AP에서 생성한 Kap-as에 일방향 해쉬를 적용하여, C의 메시지에 수납하고, AS에게 전송한다.

3.3.5 지문 인증 응답

(1) AS에서 AP로의 메시지 : EKUc(Authentication Result | f(T1))
AS는 AP로부터 전송 받은 메시지에서 Kap-as를 일방향 해쉬를 적용해서, 정당한 AP로부터 받은 메시지인지를 확인한 후에, C에서 전송한 메시지에서 암호화된 지문 정보 메시지(EKc-as(UID | Fingerprint Minutiae | T1))에 일방향 해쉬를 적용하여 메시지의 무결성을 검사한다. 전송 받은 메시지가 위/변조되지 않았다면, IDc와 공유했던 Kc-as를 찾아서 암호화된 지문 정보 메시지를 복호화하고, T1을 확인해서 유효한 시간 안에 전송된 메시지인지 확인하고, C의 사용자의 UID와 지문 특징점 정보를 획득한다. 획득한 정보는 앞 장에서 소개간 지문 인식 과정을 통해, AS의 데이터베이스에 있는 사용자 특징점 정보(오프라인 상에서 등록한)와 정합한다. 정합 후에, 인증된 결과를 전송 받은 T1을 이용해 f(T1)을 생성하여, 인증 결과를 AP를 통해서, KUc로 암호화하여 C에게 전송한다. T1을 인증 결과와 함께 암호화함으로써, 인증 성공 혹은 실패에 메시지가 일정한 패턴으로 C에게 전송되는 것을 막을 수 있다 (i.e., 키 값

은 KUc로 동일할 때, 인증 여부는 성공 혹은 실패이므로 암호화 메시지의 패턴도 인증 여부에 따라 오직 두 가지임). AS에서 전송된 인증 결과는 C에게 전송되고, C는 메시지를 KRc로 복호화하여, 사용자 지문 인증 과정을 완료한다.

3.4 이동환경에서 사용자 인증 메커니즘

3.4.1 재접속 요청

(1) C에서AP2를 거쳐 AS로의 메시지 : EKUc(IDc | BSSID1)
C 가 이동하여 AP2로의 재접속을 위해 AP2를 거쳐 AS로 C의 공개키(KUc)를 이용하여 IDc와 BSSID1(MAC address)을 암호화하여 전송한다.

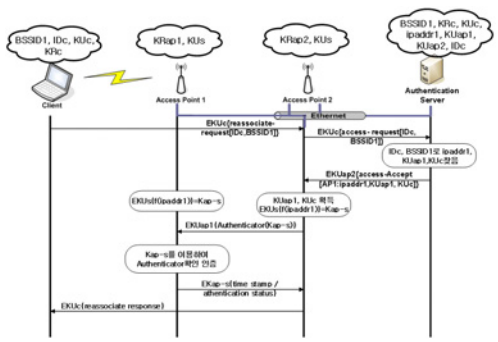

그림 6. 이동시 사용자 인증 프로토콜

3.4.2 재접속 요청 응답 및 확인

(1) AS에서 AP2로의 메시지 : EKUap2(ipaddr1 | KUap1 | KUc)
AS는 C의 개인키(KRc)로 IDc와 BSSID1을 획득하여 해당 클라이언트 ID와 MAC address에 대응되는 AP1의 IP address와 현재 AP1의 공개키(KUap1)와 단말의 공개키(KUc)를 AP2의 공개키(KUap2)로 암호화 하여 AP2로 전송한다.

(2) AP2에서 AP1로의 메시지 : EKUap1(Kap-s | Authenticator)
AP2는 받은 메시지에서 KUc와 KUap1를 획득하고 AS의 공개키(KUs)와 AP1의 IP address를 가지고 세션키 Kap-s를 생성하여, Authenticator를 만들어 AP1의 공개키(KUap1)로 암호화하여 AP1으로 전송한다.

(3) AP1에서 AP2로의 메시지 : EKUap-s(time stamp | authentication status)
AP1은 이 Authenticator를 이용하여 정당한 AP인지를 확인하고, 세션키 Kap-s를 이용하여 AP1이 가지고 있던 정보를 전달하게 된다. 전달되는 메시지에는 Time Sync로 재전송 공격(Replay Attack)을 예방하기 위한 Time Stamp 값을 가지고, 무선단말의 인증여부를 판단하기 위한 Authentication Status를 메시지 안에 넣어 전송하게 된다. 이는 액세스포인트에 대한 DoS(Denial of Service) 공격과 위장 단말(Rogue Statins)을 사전에 예방할 수 있다.

3.4.3 C에 인증 결과 전송

(1) AP2에서 C로의 메시지 : EKUc(result)
C에 대한 재접속 응답 메시지를 보내어 인증의 성공여부를 전송하게 된다.

Ⅳ. 구현 및 보안성 평가

4.1 제안 프로토콜 구현

3장에서 소개한 키 분배 프로토콜(사용자 키 분배, AP 키 분배), 사용자 지문 인증 프로토콜, 효율적인 핸드오프 프로토콜을 그림 7, 8과 같이 구현하였다. 사용자 단말과 지문 인증 서버는 Window XP환경에서 구현하였고, 지문 정보 처리 관련 모듈

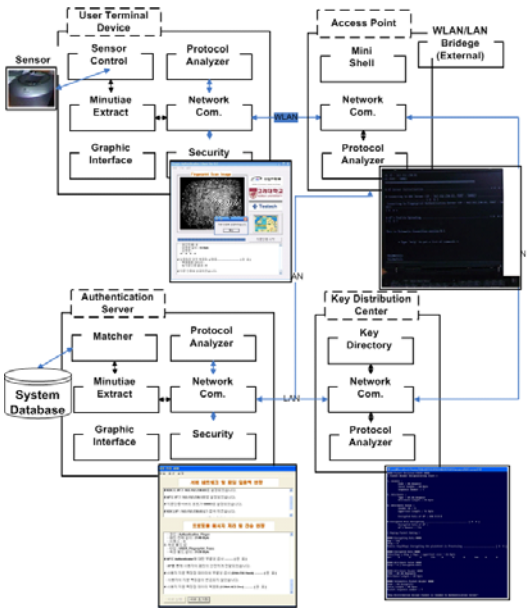

그림 7. 사용자 인증 시스템 세부 구성도

그림 8. 지문을 이용한 사용자 인증 시스템 구현

(Minutiae Extract), 보안 모듈(Security: SHA-256, AES, RSA), 네트워크 패킷 송수신 모듈(Network Com.), 프로토콜 처리 모듈(Protocol Analyzer)이 공통적으로 구성되어 있고, 지문 인증 서버에는 정합모듈(Matcher)을 사용자 단말에는 지문 센서와 통신할 수 있는 센서 제어 모듈(Sensor Control)로 구성되어 있다. AP와 KDC는 Linux Redhat 9.0 환경에서 구현하였고, AP의 Linux 커널에는 WLAN과 LAN의 브릿지 환경을 구성하는 모듈을 포팅(Porting)하였다. AP에는 키 분배 및 AP 초기화 설정을 할 수 있는 미니 쉘(Mini Shell)을 KDC에는 키 관리를 위한 키 디렉토리 모듈(Key Directory)로 구성하였다.

4.2 보안성 평가

4.2.1 오프라인 사전 공격(Off-line password Dictionary Attack) 예방

기존의 패스워드 기반 인증 프로토콜(i.e., IEEE 802.1x EAP-MD5, Kerberos 등)들의 취약점은 전수 공격(Brute force)을 통해 패스워드가 노출될 수 있었지만, 본 논문에서는 개인의 지문 정보를 이용해서 인증을 했다. 따라서, 사용자가 지문 센서를 통해 지문을 입력하면, 매번 다른 지문 이미지가 생성이 되고, 지문 특징점 정보를 추출할 때 정보가 변하게 된다. 물리적인 방법으로 지문 정보가 유출되지 않는다면 기존 자릿수에 의존하는 패스워드 기반의 인증 방식보다 강인하다.

4.2.2 전방향 안정성 제공

지문 인증서버, AP, 사용자 단말 사이에서 인증에 사용될 지문 정보를 암호화하기 위해 임시키를 분배할 때, 키 분배 프로토콜에서 공유한 공개키 방식을 기반으로 하여, 임의의 수(i.e., 임시키 생성을 위한 정보)를 공유한다. 공개키 기반 방식으로 임시키를 암호화하기 때문에 보안의 강도는 공개키 방식 암호화의 수학적 보안성 강도를 따라간다. 또한 매 인증 시, 임의의 수를 생성하기 때문에, 공격자가 임시키를 획득하더라도, 다음 인증에 해당 세션키를 사용할 수 없다.

4.2.3 Denning-Sacco(DS) 공격 예방

DS 공격은 공격자가 이전 임시키를 안다고 할 때 암호화된 지문정보를 알아내는 공격이다. 제안한 프로토콜은 공격자가 임시키를 획득하더라도 T1(인증 세션 시간)안에 인증을 성공하지 못한다면, 다음 인증 세션에서 획득한 임시키를 재사용할 수 없다(i.e., 임의의 수로 N1, N2을 이용해 매 인증 세션마다 새로운 임시키를 생성).

4.2.4 능동적 중간자 공격(Positive Man in the Middle Attack) 및 재생 공격(Replay Attack)

능동적 중간자 공격은 가장 공격(Impersonation Attack)과 동일하다. 제안한 프로토콜에서 WLAN과 LAN상의 재생 공격이 가능한데, WLAN상에서 AP와 사용자 터미널 장치는 장치의 고유번호(IDx)와 지문 인증 서버에게서 받은 공개키를 통해 질의/응답 과정을 통해 상호 인증을 하고, 사용자 단말은 임시키를 AP가 아닌 지문 인증서버와 공유를 하기 때문에, 공격자가 중간(WLAN)에서 암호화된 지문 정보메시지를 획득하더라도 임시키가 없다면 지문 정보를 획득 할 수 없다. LAN 상에서도 또한 공격자가 AP와 지문 인증서버 사이의 교환 메시지를 획득하더라도, 지문 인증서버에서 사용자 단말에게 전달되는 메시지는 사용자 단말의 공개키(KUc)를 통해 암호화가 되어 AP의 공개키(KUap)로 암호화되어 전송되는 메시지 안에 수납되기 때문에, 부정당한 방법에 의해 메시지 획득이 어렵다. 또한, AP는 지문 인증 서버 에게 사용자 단말의 암호화된 지문 정보를 전송할 때, AP와 지문 인증서버 사이에서 공유된 임시키(Kap-as)를 일방향 해쉬를 적용한 값이 수납되고, 지문 인증서버는 이 값을 검증하기 때문에, 공격자가 AP로 가장해서 지문 인증서버에게 인증을 받는 것은 어렵다.

V. 결 론

최근 인터넷 및 이동통신 기술의 발전과 함께 차량에서 무선 단말을 이용하여, 유선 네트워크의 서비스를 이용할 수 있는 텔레메틱스 환경이 실현되고

있다. 본 논문에서는 텔레메틱스 환경에서 안전하고 효율적인 사용자 인증 프로토콜을 제안했다. 사용자 인증 프로토콜에서는 차량에서 사용자의 인증이 용이하고 분실, 도난, 망각의 위험이 없는 생체 정보를 이용하였다. 또한 제안한 프로토콜은 사용자 인증 정보를 암호화하기 위한 임시 키(Session Key)를 생성하기 위한 마스터키 분배가 이루어지며 단말의 이동간에 취약점을 고려하여 AP간의 보안통신을 통하여 보다 안전성 있는 시스템을 제안하였다.

시스템 구현을 통하여 편리하고, 실시간 인증이 가능함을 확인하였다. 또한 전송채널을 통해서 전송되는 인증정보를 보호하기 위하여 암호학적 알고리즘 RSA, AES, SHA1을 이용하여 기밀성과 무결성을 보장하였고, 다양한 공격에 대하여 안전한 프로토콜을 확립하였다. 이동환경에서의 실험에서는 텔레메틱스의 여러 환경 중 무선랜 환경을 사용하였다. 단말이 새로운 AP 영역으로 이동하여 인증서버를 통해서 전에 서비스 받던 AP의 정보를 얻어 이동해온 단말이 정당한 단말이라는 것을 확인할 수 있었다. 추후 Mobile IP를 이용한 실험을 계획하고 있고, 핸드오프 동안에 지문 정보가 손실되었을 경우에 대한 연구가 필요하다.

참 고 문 헌

〔1〕 W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2003

〔2〕 A. Jain, R. Bole, and S. Panakanti, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.

〔3〕 D. Maltoni, et al., Handbook of Fingerprint Recognition, Springer, 2003.

〔4〕 M. Ilyas, S. Ahson, Handbook of Wireless Local Area Networks: Applications, Technology, Security, and Standards, CRC, 2005.

〔5〕 IEEE, IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 TM Operation, IEEE Std 802.11f, 2004.

〔6〕 T. Moore and B. Aboba, "uthenticated Fast Handoff" IEEE 802.1-01/553, November 2001.

〔7〕 Y. Chung, et al., " Secure Fingerprint Authentication System on an Untrusted Computing Environment" LNCS 3592 - TrustBus, pp. 299-310, 2005.

〔8〕 U. Uludag, S. Pankanti, and A. Jain, "uzzy Vault for Fingerprints,"LNCS 3546 - Proc. of AVBPA, pp. 310-319, 2005.

김 태 섭 (Tae-sub Kim) 준회원

2006년 2월 고려대학교 전산학과 졸업 학사

2007년 현재 고려대학교 전산학과 석사 과정

<관심분야> 이동통신, 메쉬네트워크, 무선랜 보안

오 룡 (Ryong Oh) 정회원

2003년 2월 고려대학교 전산학과 (학사)

2005년 2월 고려대학교 전산학과 (석사)

2005년 3월~현재 고려대학교 전산학과 (박사과정)

<관심분야> 이동통신, QoS, 스케줄링, 텔레메틱스, 홈네트워크 보안

이 상 준 (Sang-Joon Lee) 준회원

2006년 2월 고려대학교 전산학과 졸업 학사

2007년 현재 고려대학교 전산학과 석사 과정

<관심분야> 무선자원관리, 메쉬네트워크, 이동통신

이 성 주 (Sung-ju Lee) 준회원

2006년 2월 고려대학교 전산학과 졸업 학사

2007년 현재 고려대학교 전산학과 석사 과정

<관심분야> 정보보호, 바이오메트릭, 패턴 인식

김 학 재 (Hak-jae Kim) 준회원

2007년 2월 고려대학교 전산학과 졸업 학사

2007년~현재 고려대학교 전산 학과 석사 과정

<관심분야> 정보보호, 바이오메트릭, 병렬 구조

정 용 화 (Yong-wha Chung) 정회원

1984년 한양대학교 전자통신 공학과 학사

1986년 한양대학교 전자통신 공학과 석사

1997년 미국 Univ. of Southern California 전기공학과(컴퓨터 공학 전공) 박사

1986년~2003년 한국전자통신 연구원 생체인식기술연구팀장

2003년~현재 고려대학교 컴퓨터정보학과 부교수

<관심분야> 생체인식, 정보보호, 생체정보 보호

조 충 호 (Choong-ho Cho) 종신회원

1981년 고려대학교 공과대학 산업공학과 (학사)

1983년 고려대학교 산업공학과 (석사)

1986년 프랑스 INSA de Lyon 전산학과 (석사)

1989년 프랑스 INSA de Lyon 전산학과 (박사)

1990~1994년 순천향대학교 전산통계학과 조교수

1994~현재 고려대학교 전산학과 교수

<관심분야> 통신망 트래픽 관리기술, 무선통신 시스템, 멀티미디어통신, 인터넷 비즈니스