2015년 1월 전자공학회 논문지 제 52권 제 1 호
Journal of The Institute of Electronics and Information Engineers Vol. 52, NO. 1, January 2015 http://dx.doi.org/10.5573/ieie.2015.52.1.079

논문 2015-52-1-10

인지무선네트워크를 위한 위임기반 인증 프로토콜

(Delegation-based Authentication Protocol for Cognitive Radio Network)

김 현 성*

(Hyunsung Kim©)

요 약

인지무선네트워크(Cognitive Radio Networks, CRNs)는 네트워크 환경을 인지하고 적응적으로 운용할 수 있는 지능형 무선 네트워킹을 제공하기 위한 기술로 인지되고 있다. CRN은 FCC(Federal Communications Commission)의 최근 정책으로 인해 비인가된 사용자가 네트워크의 주사용자를 방해하지 않는 한 유휴 스펙트럼을 활용할 수 있도록 허락하는 기술이다. 그러므로 CRNs의 보안 특성은 다른 네트워크와 달라야만 한다. 본 논문의 목적은 Tsai등의 위임기반 인증 프로토콜(TDAP)로부터 CRN상의 비인가된 사용자를 위한 보안의 특성을 추출함으로서 새로운 위임기반 인증 프로토콜(NDAP)을 제안하는데 있다. 먼저 TDAP에 대한 보안분석을 제시하고 비인가 사용자 인증을 위한 프로토콜 설계 목표를 설정한다. 그런 후 TDAP에 대한 보안 해결책과 CRNs를 위한 새로운 프로토콜로서 NDAP을 제안한다. 본 논문에서 제안한 NDAP은 CRNs과 다양한 융합응용의 보안 기반 구조로 활용될 수 있을 것이다.

Abstract

Cognitive radio networks (CRNs) offer the promise of intelligent radios that can learn from and adapt to their environment. CRN permits unlicensed users to utilize the idle spectrum as long as it does not introduce interference to the primary users due to the Federal Communications Commission's recent regulatory policies. Thereby, the security aspects in CRNs should be different with the other networks. The purpose of this paper is to devise a new delegation-based authentication protocol (NDAP) by extracting out the security aspects for unlicensed user authentication over CRNs from Tsai et al's delegation-based authentication protocol (TDAP). First of all, we will provide security analyses on the TDAP and set design goal for unlicensed user authentication. Then, we will propose a NDAP as a remedy mechanism for the TDAP and a new protocol for CRNs. The NDAP could be used as a security building block for the CRNs and various convergence applications.

Keywords : 정보보호, 인지무선네트워크, 인증, 위임, 프라이버시

* 정회원, 경일대학교 사이버보안학과
((Dept. of Cyber Security, Kyungil University)
© Corresponding Author (E-mail: kim@kiu.ac.kr)
※ 본 연구는 2014년도 융합/스마트/클라우드 컴퓨팅 학술대회에서 '무선 로밍 서비스를 위한 위임기반 인증 프로토콜 분석' 제목으로 발표된 논문[12]을 확장한 것임.
※ 본 연구는 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 연구임(한국연구재단2010-0021575).
접수일자: 2014년10월11일, 수정일자: 2014년12월12일
게재확정: 2014년12월23일

Ⅰ. 서 론

최근 들어 차세대 통신 시스템은 여러 네트워크들의 융합 형태로 설계되고 시스템이 점점 복잡해지고 상호연동의 필요성이 점차 확대되고 있다. 특히, 통신 기술의 발전함에 따라 주파수 자원에 대한 사용 빈도가 증가하고 주파수 고갈 문제가 심각한 상황에 이르렀다. 인지무선(Cognitive Radio) 기술은 적응적이고 합리적으로 무선

주파수를 활용하기 위한 기술이다. 다양한 환경에서 최적화된 인지무선 기술의 실용화를 위해 다양한 연구가 진행되고 있다[1~4].

인지무선을 위한 표준화는 크게 IEEE 802.22와 Ecma-International의 개인/휴대기기를 위한 표준의 두 가지가 있다[5~7]. IEEE 802.22는 광대역 무선 인터넷 서비스에 인지무선 기술을 적용하여 54~862 MHz 사이의 TV 주파수 대역에서 WRAN(Wireless Regional Area Network)서비스를 제공하기 위한 표준을 선보였다. IEEE의 활동과는 별개로 ECMA-International은 개인/휴대기기들을 위한 인지무선 표준을 발표하였다[5~7]. 지금까지의 인지무선 보안관련 연구들은 인지무선의 지능적 속성(Intelligent Behavior)으로 인하여 인지무선 자체의 보안에 대한 위협요소를 조사하기 위한 몇몇 연구들이 진행되어 왔다[8-9]. 하지만 기존 연구들은 인지 무선의 속성을 고려하지 못하고 있어 추가적인 보안 연구의 필요성이 증대 되고 있다[8~14].

무선 로밍 서비스는 방문 위치 등록자 (Visited Location Register, VLR)가 홈 위치 등록자 (Home Location Register, HLR)의 도움을 받아서 이동기기(Mobile Station, MS)를 인증할 수 있도록 허락한다. Lee등이 첫 익명성을 제공하는 위임기반 인증 프로토콜을 제안하였다[15]. Lee등의 프로토콜은 프락시 서명(Proxy Signature) 기법을 이용하였다. 하지만, Lee등의 기법이 VLR 가장 공격에 취약함이 확인되었고, 다양한 연구들이 제안되었다[16]. 최근에 Tsai등은 기존 위임기반 기법들의 문제점을 도출하고 이를 해결하기 위한 안전한 위임기반 인증 프로토콜(Tsai et al.'s Delegation-based Authentication Protocol, TDAP)을 제안하였다[17]. Tsai등은 TDAP이 서비스거부공격을 포함한 다양한 보안 공격에 안전하다고 주장하였다.

본 논문에서는 Tsai등의 TDAP에 대해 살펴보고 인지무선 네트워크에 적용하기 위한 Tsai등의 TDAP에 대한 보안 분석 및 특성 분석을 제시한다. 이를 통해 인지무선네트워크를 위한 새로운 위임기반 인증 프로토콜(New Delegation-based Authentication Protocol, NDAP)을 제안한다. 본 논문에서 제안한 NDAP은 일반적인 무선 네트워크의 로밍 서비스 뿐만 아니라 인지무선네트워크의 요구사항을 만족한다. NDAP은 IEEE 802.22 및 Ecma-International의 개인/휴대기기를 위한 인지무선네트워크 표준들을 포함한 다양한 융합응용의 보안 기반 구조로 활용될 수 있을 것이다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 TDAP에 대해 살펴보고, Ⅲ장에서는 인지무선네트워크의 개요와 TDAP의 보안분석을 제시한다. Ⅳ장에서는 인지무선네트워크를 위한 NDAP을 제안한다. 그리고 Ⅴ장에서는 분석을 제시하고 Ⅵ장에서 결론을 맺는다.

Ⅱ. Tsai등의 위임기반 인증 프로토콜

Tsai등은 위임기반 인증 프로토콜 TDAP을 살펴본다[17]. TDAP에서 사용된 기호는 표 1과 같다.

표 1. 기호 정의
Table 1. Notations.

기 호	내 용
p, q	$q\|(p-1)$을 만족하는 솟수들
g	Z_p상의 생성자
ID_V, ID_H	VLR과 HLR의 식별자
$[M]_K$	키 K로 메시지 M을 위한 대칭키 암호
G	순환 덧셈군
$h()$	$Z_p \rightarrow Z_p$ 매핑을 위한 일방향 해쉬 함수
$H()$	$G \rightarrow Z_p$ 매핑을 위한 일방향 해쉬 함수
l	가칭을 위한 정수 길이
$B_l(m)$	이진문자열 m의 첫 l 비트
P	순환 덧셈군의 생성자
$\oplus$	XOR 연산
$a?=b$	a와 b가 같은지 검증 연산

가. 셋업 단계

HLR은 x와 x_v두 개의 개인키를 선택한 후, 각 키와 대응되는 공개키 $v=xP$와 $y_v=x_vP$를 계산한다. 그리고 HLR은 VLR과 K_{HV}와 x_v 그리고 v를 공유한다. HLR은 또한 난수 k를 생성하여 각 MS를 위한 프락시 키 쌍 $K=kP$와 $\sigma = x+Kh(K) \bmod q$를 계산한다. 각 MS를 위해 생성된 프락시 키 쌍(σ,K)은 HLR의 데이터베이스에 저장하고 키 쌍(σ,K)과 공개키 y_v는 대응되는 MS의 SIM 카드에 각각 저장한다.

나. 온라인 인증 단계

각 온라인 인증 세션을 위해 MS는 난수 n_1을 생성하고, $h^{(1)}(n_1)$, $h^{(2)}(n_1)$, ..., $h^{(n+1)}(n_1)$를 계산하고 데이터베이스에 저장한다. 여기서 n은 프로토콜에 의해 지원되는 오프라인 인증의 전체 횟수를 의미한다.

단계 1. MS는 VLR에게 로그인 요청을 보낸다.

단계 2. VLR은 난수 n_2를 생성하고, MS에게 (n_2, ID_V)를 보낸다.

단계 3. MS는 SIM카드로부터 $N_1=h^{(n+1)}(n_1)$을 검색하고 난수 t를 생성한 후 $r_1=tP$와 $r_2=H(ty_v)\oplus(K, N_1)$, 그리고 $s=\sigma\, h(N_1||n_2||ID_V||r_1||r_2||ID_H)+t \bmod q$를 계산한다. 그리고 MS는 ($r_1$, r_2, s, ID_H, ID_V)를 VLR에게 전송한다.

단계 4. VLR은 (K, N_1)을 계산하기 위해서 x_v를 이용하여 $r_2\oplus H(x_v r_1)$를 계산한다. 그리고 VLR은 sP와 $h(N_1||n_2||ID_V||r_1||r_2||ID_H)(v+h(K)K)+r_1$을 계산하고, 계산된 두 값이 같은지 검증한다. 만약 검증이 성립하면 VLR은 암호키로 K_{HV}를 이용하여 $CT_1=[N_1||n_2||K]_{K_{HV}}$를 계산하고 HLR에게 ($CT_1$, ID_H, ID_V)를 보낸다. 그렇지 않으면 VLR은 로그인 요청을 거부한다.

단계 5. HLR은 비밀키 K_{HV}를 이용하여 CT_1를 복호함으로서 $N_1||n_2||K$를 확인한다. 그리고 HLR은 복호된 K에 따라 데이터베이스에서 대응되는 σ 를 찾는다. HLR은 난수 n_3를 생성하고, $SK = h(N_1||n_2||n_3||\sigma)$와 $CT_2=[N_1||n_3||ID_V]_\sigma$ 그리고 $CT_3=[CT_2||n_2||N_1||SK]_{K_{HV}}$를 계산한다. 최종적으로 HLR은 VLR에게 (CT_3, ID_H, ID_V)를 보낸다.

단계 6. VLR은 비밀키 K_{HV}를 이용하여 CT_3를 복호함으로서 $CT_2||n_2||N_1||SK$를 찾고, n_2와 N_1가 복호된 문자열 $CT_2||n_2||N_1||SK$에 존재하는지 검증한다. 만약 검증이 성립하면 VLR은 MS에게 (CT_2, ID_V)를 보낸다.

단계 7. MS는 키 σ 를 이용하여 CT_2를 복호함으로서 $N_1||n_3||ID_V$를 획득하고 N_1과 ID_V가 복호된 문자열 $N_1||n_3||ID_V$에 존재하는지 검증한다. 만약 검증이 성립되면 MS는 세션키 $SK=h(N_1||n_2||n_3||\sigma)$를 계산한다.

다. i번째 오프라인 인증 단계

MS는 자신의 데이터베이스에서 $h^{(n-i+1)}(n_1)$을 검색하고 VLR에게 $[h^{(n-i+1)}(n_1)]_C$를 보낸다. 메시지를 받은 VLR은 암호된 메시지 $[h^{(n-i+1)}(n_1)]_C$를 복호하고 $h(h^{(n-i+1)}(n_1))$를 계산한다. 그리고 VLR은 계산된 값이 자신의 데이터베이스에 저장된 값 $h^{(n-i+2)}(n_1))$과 같은지 검증한다. 만약 조건이 성립하면, VLR은 데이터베이스에 저장된 $h^{(n-i+2)}(n_1))$를 $h(h^{(n-i+1)}(n_1))$로 대체하고 세션키 $C_{i+1}=h(h^{(n-i+1)}(n_1), C_i)$계산하며, i를 1 증가시킨다.

Ⅲ. 인지무선네트워크 및 보안 요구사항

본 장에서는 인지무선네트워크의 개요를 살펴보고 Tsai등의 TDAP 분석을 제시함으로서 인지무선네트워크의 보안 요구사항을 도출한다.

가. 인지무선네트워크 개요

Mitola는 1991년에 SDR(Software Defined Radio) 개념을 그리고 1998년에 인지무선 개념을 정립하였다[1]. 인지무선은 SDR 소프트웨어 무선 플랫폼 상에서 구현되며, 통신환경을 인지하고 적응적으로 무선을 자동재구성할 수 있는 인지능력을 가진 지능형 무선이다[2-7]. 전통적인 무선 기술과 비교하여 인지무선은 인공지능 기능과 동적인 스펙트럼 접근(Dynamic Spectrum Accessing) 응용과 같은 특별한 특징을 가진다.

인지무선을 위한 표준화는 크게 IEEE 802.22와 Ecma-International의 개인/휴대기기를 표준의 두 가지가 있다[2~7]. 특히, 이들 표준들은 그림 1에서 보여주는 바와 같이 하부구조를 기반으로 하는 네트워크(Infra Structure Based)와 하부구조가 필요 없는 네트워크(Infrastructureless Structure)로 나뉠 수 있다. 하부구조 기반의 네트워크 표준을 위해 IEEE 802.22는 광대역 무선 인터넷 서비스에 인지무선 기술을 적용하여

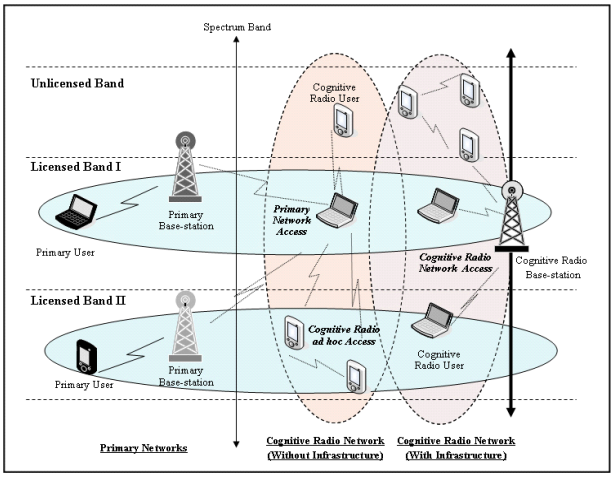

그림 1. 인지무선네트워크 구조[18]
Fig. 1. Cognitive radio network architecture[18].

54~862 MHz 사이의 TV 주파수 대역에서 WRAN서비스를 제공하기 위한 표준을 선보였다[5]. 하부구조 기반 네트워크와 하부구조가 필요 없는 네트워크의 결합형인 혼합형 네트워크를 위하여 ECMA-International은 개인/휴대기기들을 위한 인지무선 표준을 발표하였다[6~7].

2009년 2월 FCC는 TV 유휴주파수 기기관련법을 제정하였다. 이 법에는 유휴주파수 기기와 관련된 일반적인 기술규정과 간섭현상을 방지하기 위한 기술조건, 기존 서비스 이용자를 간섭으로부터 보호하기 위한 규제사항, 유휴주파수의 데이터베이스(Database)에 대한 규정 등을 포함한다. 인지무선 기기들은 위치정보를 수집하는 기능과 인가된 데이터베이스로부터 이용 가능한 채널 검색 기능, 그리고 스펙트럼 센싱(Spectrum Sensing) 기능 등을 기본요구 사항으로 명시하고 있다.

나. Tsai등의 TDAP 분석

본 절에서는 TDAP의 보안 분석 및 인지무선을 위한 인증 프로토콜에 있어서 추가로 고려될 사항에 대한 분석을 제시한다[11~12]. 먼저 TDAP이 스마트카드 침해 공격에 취약함으로 보이고, 다양한 네트워크에 적용을 위한 인증 프로토콜이 고려해야 할 사항을 네트워크 제어와 식별자관점의 분석을 제시한다.

스마트카드 침해 공격 : 다양한 인증 프로토콜에서 스마트카드(Smart card)가 부정 조작 방지 (Tamper Resistant) 가능하다는 가정 하에 제안되었다. 그러므로 논문 [19-20]에서 제시된 연구처럼 만약 스마트카드가 공격자에 의해 쉽게 조작될 수 있다면 이들 인증 프로토콜은 안전하지 않다. Tsai등의 TDAP에서도 MS는 스마트카드와 유사한 특성을 갖는 SIM 카드의 사용을 가정하고 있고, 여기에 (P, q, $h()$, $H()$, [], σ , K, y_v, ID_H, $h^{(1)}(n_1)$, $h^{(2)}(n_1)$, ..., $h^{(n+1)}(n_1)$)를 저장한다. Tsai등의 TDAP에 논문 [19-20]에서 제시된 공격 기법을 통해 침해 공격을 수행한다면, MS의 SIM으로부터 프로토콜에서 중요한 비밀키로 이용된 σ 와 K를 도출할 수 있다. 특히, 도출된 값을 통해 공격자는 인증 및 세션키와 관련된 사용자의 중요한 정보를 획득할 수 있음으로 해서 MS 가장공격을 포함한 다양한 공격을 수행할 수 있다. 즉, Tsai등의 TDAP은 스마트카드 침해 공격에 취약하다.

MS에 의한 인증 횟수 제어 : 다양한 방문자 네트워크 환경에 있어서 네트워크 제어의 모든 권한은 VLR에게 제시되어야 한다. 즉, 방문자인 MS의 인증에 대한 허용 및 인증 횟수 제어는 VLR에 의존해야 한다. 하지만 Tsai 등의 인증 기법에 있어서 인증 횟수는 방문자인 MS에 의해 결정된다. 비록 VLR이 HLR을 통해 간접적인 MS 인증을 제시하지만, 네트워크 서비스에 대한 전체적인 권한은 MS가 아닌 VLR에게 제시되어야 할 필요가 있다. Tsai등의 TDAP은 일방향 해쉬체인의 특성을 이용하여 n개의 해쉬체인을 생성하고, 생성된 해쉬체인의 역방향 순서로 해쉬값을 세션키로 활용함으로서 HLR의 오버헤드를 줄일 수 있는 오프라인 인증 기법을 제시하고 있다. 하지만 해쉬체인의 생성이 MS에 의존하고 있어서 오프라인 인증 횟수에 대한 제약을 VLR이 제시할 수 없는 문제점이 존재한다.

MS의 식별자 부재 : 다양한 인증 프로토콜에서 사용자의 식별자는 아주 중요한 정보로 활용된다. 하지만 Tsai등의 TDAP에서는 MS의 식별자를 이용하지 않는다. 이렇게 함으로서 사용자의 익명성(Anonymity)을 기반으로 하는 프라이버시(Privacy)를 제공할 수 있지만, 다양한 네트워크 환경에서 사용자 식별자의 활용은 다양한 응용 요구사항을 지원하기 위해서 필수적이다.

Ⅳ. 새로운 위임 기반 사용자 인증 프로토콜

본 장에서는 인지무선네트워크를 위한 새로운 위임기반 사용자 인증 프로토콜(New Delegation-based Authentication Protocol, NDAP)을 제안한다. 인지무선네트워크는 비면허 대역(Unlicensed band)에 할당되어 있는 주파수 대역 중 그 활용도가 낮거나, 시·공간적으로 사용되지 않는 유휴자원을 찾아 적응적이고 합리적으로 이용하는 기술이다. 이러한 비면허 대역의 사용에 있어서 해당 대역에 이용권한(License)을 가지고 있는 주사용자(Primary User)를 보호하면서 비면허자(Nonlicense Holder)가 유휴대역을 활용할 수 있는 보안 기술의 개발은 필수적이다.

본 장에서는 인지무선 인증에 있어서 제시해야 할 보안 요구사항을 정의하고 이를 만족하기 위한 인지무선 네트워크를 위한 NDAP을 제안한다. 제안한 기법 또한 셋업과 로그인, 그리고 오프라인 인증 단계로 구성된다.

가. 인지무선 인증 기법 보안 요구사항

인지무선시스템에서는 기밀성과 프라이버시 기법들

이 데이터 뿐 만 아니라 민감한 스펙트럼 소유 정보 등 다양한 정보가 보호되어야 한다. 이절에서는 사용자 인증을 위한 무등록(No Registration)과 비추적성(Untraceability) 관점의 두 가지 보안 측면에 대한 논의를 제시한다.

무등록 : 다양한 방문자 네트워크 환경에서 그 네트워크 사용 권한이 없는 방문자는 주사용자를 보호하면서 VLR을 통한 서비스를 제공받을 수 있어야 한다. 이때 VLR은 HLR과의 연계를 통해 사용자에 대한 인증을 실시할 수 있어야 한다.

비추적성 : 네트워크 환경에서 통신의 추적성은 아주 민감한 프라이버시 문제를 야기할 수 있다. 따라서 방문자가 방문자 네트워크나 비면허 대역 이용 시 세션간의 연계관계를 제시할 수 없도록 프로토콜이 설계될 필요가 있다. 하지만, 이들 방문자들이 주사용자의 보호 책무를 저해할 경우 조건부 식별자 확인 가능성을 제시할 필요가 있다.

Ⅲ장의 TDAP 분석과 본 절의 내용을 토대로 인지무선네트워크의 인증 기법이 제시하여야 할 보안 속성은 표 2와 같이 요약할 수 있다.

표 2. 인증 프로토콜의 보안 속성
Table 2. Security Aspects in Authentication Protocol.

속성 \ 프로토콜	TDAP [17]	인지무선네트워크 인증
스마트카드 보안(Smartcard Security Protection)	Not Support	Support
인증제어(Authentication Control)	MS	VLR
무등록(No Registration)	Support	Support
비추적성(Untraceability)	Required	Required
MS식별자(Identification)	Not Required	Required

나. 셋업 단계

HLR은 x와 x_v두 개의 개인키를 선택한 후, 각 키와 대응되는 공개키 $v=xP$와 $y_v=x_vP$를 계산한다. 그리고 HLR은 VLR과 K_{HV}와 x_v 그리고 v를 공유한다. HLR에 등록을 원할 경우 MS는 난수 d를 생성하고 자신의 식별자 ID_{MS}와 패스워드 PW_{MS}를 이용하여 $AID_{MS}=h(ID_{MS}||d)$와 $APW_{MS}=h(PW_{MS}||d)$를 계산한 후 $\{AID_{MS}, APW_{MS}\}$를 HLR에 전송한다. HLR은 난수 k를 생성하여 각 MS를 위한 프락시 키 쌍 $K=kh(AID_{MS})P$와 $\sigma=x+Kh(K) \bmod q$를 계산한다. 각 MS를 위해 생성된 프락시 키 쌍(σ, K)은 HLR의 데이터베이스에 저장하고 키 쌍(σ, K)을 이용해 $W=h(AID_{MS}||APW_{MS})\oplus(\sigma||K)$을 계산 후 W와 공개키 y_v를 저장한 SIM카드를 MS에게 발급한다. MS는 $D=h(ID_{MS}||PW_{MS})\oplus d$를 계산하여 SIM카드에 저장한다.

다. 온라인 인증 단계

방문자 네트워크 환경에서 그 네트워크 사용 권한이 없는 방문자는 주사용자를 보호하면서 VLR을 통한 서비스를 제공받기 위해 온라인 인증 단계가 필요하다. 온라인 인증 세션을 위해 MS는 VLR의 난수 n_1과 자신의 난수 n_2를 이용하여, $h^{(1)}(n_1||n_2)$, $h^{(2)}(n_1||n_2)$, ..., $h^{(n+1)}(n_1||n_2)$를 계산하고 데이터베이스에 저장한다. 여기서 n은 VLR에 의해 제공되는 NDAP에 의해 지원되는 오프라인 인증의 전체 횟수를 의미한다.

단계 1. MS는 VLR에게 로그인 요청을 보낸다.

단계 2. VLR은 난수 n_1을 생성하고, 오프라인 인증 횟수 n을 포함한 메시지 $\{n_1, n, ID_V\}$를 MS에게 보낸다.

단계 3. MS는 자신의 식별자 ID_{MS}와 패스워드 PW_{MS}를 SIM카드에 입력한다. SIM카드는 난수 n_2를 생성하고 해쉬체인을 생성한 후 $N_1=h^{(n+1)}(n_1||n_2)$을 검색한다. D를 통해 d를 찾고, W를 통해 키 쌍(σ, K)을 유도한 후, 난수 t를 생성하며 $r_1=tP$, $r_2=H(ty_v)\oplus(K, N_1)$, $s=\sigma\, h(N_1||n_2||ID_V||r_1||r_2||ID_H)+t \bmod q$, $V_1=h(N_1||r_1||r_2||s||ID_H||ID_V)$를 계산한다. 그리고 MS는 $\{r_1, r_2, s, ID_H, ID_V, V_1\}$를 VLR에게 전송한다.

단계 4. VLR은 (K, N_1)을 계산하기 위해서 x_v를 이용하여 $r_2\oplus H(x_vr_1)$를 계산한다. 그리고 VLR은 $V_1?=h(N_1||r_1||r_2||s||ID_H||ID_V)$과 $sP?= h(N_1||n_2||ID_V||r_1||r_2||ID_H)(v+h(K)K)+r_1$을 검증한다. 만약 검증이 성립하면 VLR은 암호키로 K_{HV}를 이용하여 $CT_1=[N_1||n_2||K]_{K_{HV}}$과 $V_2=h(N_1||CT_1||ID_H||ID_V)$ 계산하고 HLR에게 $\{CT_1, ID_H, ID_V, V_2\}$를 보낸다. 그렇지 않으면 VLR은 로그인 요청을 거부한다.

단계 5. HLR은 비밀키 K_{HV}를 이용하여 CT_1를 복호함으로서 $N_1||n_2||K$를 확인한다. 그리고 HLR은

V_2?=$h(N_1||CT_1||ID_H||ID_V)$을 검증한다. 검증이 성공하면, 복호된 K에 따라 데이터베이스에서 대응되는 σ 를 찾는다. HLR은 난수 n_3를 생성하고, $SK=h(N_1||n_2||n_3||\sigma)$, $CT_2=[N_1||n_3||ID_V]_\sigma$, $CT_3=[CT_2||n_2||N_1||SK]_{K_{HV}}$를 계산한다. 최종적으로 HLR은 VLR에게 $\{CT_3, ID_H, ID_V\}$를 보낸다.

단계 6. VLR은 비밀키 K_{HV}를 이용하여 CT_3를 복호함으로서 $CT_2||n_2||N_1||SK$를 찾고, n_2와 N_1이 복호된 문자열 $CT_2||n_2||N_1||SK$에 존재하는지 검증한다. 만약 검증이 성립하면 VLR은 MS에게 $\{CT_2, ID_V\}$를 보낸다.

단계 7. MS는 키 σ 를 이용하여 CT_2를 복호함으로서 $N_1||n_3||ID_V$를 획득하고 N_1과 ID_V가 복호된 문자열 $N_1||n_3||ID_V$에 존재하는지 검증한다. 만약 검증이 성립되면 MS는 세션키 $SK=h(N_1||n_2||n_3||\sigma)$를 계산한다.

라. i번째 오프라인 인증 단계

MS는 자신의 데이터베이스에서 $h^{(n-i+1)}(n_1||n_2)$을 검색하고 VLR에게 $[h^{(n-i+1)}(n_1||n_2)]_C$를 보낸다. 메시지를 받은 VLR은 암호된 메시지 $[h^{(n-i+1)}(n_1)]_C$를 복호하고 $h(h^{(n-i+1)}(n_1))$를 계산한다. 그리고 VLR은 계산된 값이 자신의 데이터베이스에 저장된 값 $h^{(n-i+2)}(n_1||n_2))$과 같은지 검증하고 허락된 n세션을 초과하지 않는지 확인한다. 만약 조건이 성립하면, VLR은 데이터베이스에 저장된 $h^{(n-i+2)}(n_1||n_2))$를 $h(h^{(n-i+1)}(n_1||n_2))$로 대체하고 세션키 $C_{i+1}=h(h^{(n-i+1)}(n_1||n_2), C_i)$를 계산한 후 i를 1 증가시킨다.

V. 분 석

본 장에서는 NDAP에 대한 보안 분석과 인지무선네트워크를 위한 속성 분석을 제시한다. 표 3은 TDAP과 NDAP의 비교를 보여준다.

표 3. 인증 프로토콜 간 속성 비교
Table 3. Property Comparisons between Authentication.

속성 \ 프로토콜	TDAP [17]	NDAP
스마트카드 침해 공격	Unsecure	Secure
비연결성	Support	Support
인증 제어 주체	MS	VLR
무등록	Support	Support
MS식별자 활용	Not Support	Support

가. 보안 분석

NDAP에 대한 보안 분석은 스마트카드 침해공격과 비연결성 관점에서 살펴본다.

스마트카드 침해 공격 : 논문 [19~20]의 가정인 스마트카드가 공격자에 의해 쉽게 조작될 수 있다고 하더라도 NDAP은 안전하다. NDAP에서 MS의 SIM 카드는 $(P, q, h(), H(), [], D, W, y_v, ID_H)$를 저장한다. 하지만, NDAP에 논문 [19~20]에서 방법을 통해 침해 공격을 수행한다고 하더라도 공격자는 MS의 SIM으로부터 프로토콜에서 중요한 비밀키로 이용된 σ 와 K를 도출할 방법이 없다. 이는 해쉬함수의 일방향성에 기인할 수 있다. 그러므로 NDAP 프로토콜에서 주고받는 메시지를 통해 공격자는 어떠한 유용한 정보도 습득할 수 있는 방법이 없다.

비연결성 : NDAP은 세션간 비 연결성을 제공하기 위해서 MS, VLR, HLR에 의한 신선성(Freshness)을 제공할 수 있는 난수 n_1, n_2, n_3, t를 이용한다. 공격자가 세션의 메시지 캡춰 공격을 통하여 추적공격을 제시하고자 하더라도 주고 받는 메시지 $\{n_1, n, ID_V\}$, $\{r_1, r_2, s, ID_H, ID_V, V_1\}$, $\{CT_1, ID_H, ID_V, V_2\}$, $\{CT_3, ID_H, ID_V\}$, $\{CT_2, ID_V\}$를 통해 세션 간 연계관계를 제시할 수 있는 어떠한 정보도 유추할 수 없다. 즉, NDAP에서는 임의의 두 세션 메시지들을 통해 어떤 특정 MS의 메시지들인지 확인할 수 있는 방법이 없다. 그러므로 NDAP은 비연결성을 제공한다.

나. 속성 분석

NDAP은 Ⅳ장에서 제시한 다양한 인지무선네트워크 인증 프로토콜 요구사항을 만족함을 표 3을 통해 확인할 수 있다. 본 절에서는 속성 분석을 VLR에 의한 인증 제어와 MS의 식별자 사용 관점에 대해 제시한다.

VLR에 의한 인증 횟수 제어 : NDAP에서 네트워크 제어의 모든 권한은 VLR에게 있다. 이를 위해 VLR은 인증에 이용될 정보와 횟수 정보를 MS에게 전달한다. 적절한 인증 횟수를 위해 MS와 VLR은 상호 통신이 필요할 것이다.

MS의 식별자 활용 : NDAP은 HLR이 MS에 대한 등록 시 식별자를 활용한다. 이렇게 함으로서 MS가 비권한 네트워크 상에서 어떤 문제를 발생시켰을 시 부인

봉쇄(Nodrepudiation)을 제공할 수 있는 방안을 제시할 수 있다. 이는 인지무선네트워크에 있어서 주사용자 보호를 위한 아주 중요한 관점이라 할 수 있다.

Ⅵ. 결 론

본 논문에서는 인지무선네트워크를 위한 새로운 위임기반 인증 프로토콜 NDAP을 제안하였다. 먼저, 인지무선네트워크 인증 프로토콜이 만족해야 할 속성을 도출하기 위하여 Tsai등이 제안한 TDAP에 대한 분석을 제시하였다. 이를 통해 인지무선네트워크를 위한 인증 프로토콜이 갖추어야 할 속성을 도출 한 후, TDAP의 문제점을 해결하면서 보다 안전한 NDAP을 제안하였다. 본 논문에서 제안한 NDAP은 IEEE 802.22 및 Ecma-International의 개인/휴대기기를 위한 인지무선네트워크 표준들을 포함한 다양한 융합응용의 보안 기반 구조로 활용될 수 있을 것이다.

REFERENCES

[1] J. Mitola, "Cognitive Radio for Flexible Mobile Multimedia Communications," *Mobile Network and Applications*, Vol. 6, No. 5, pp. 435-441, 2001.

[2] H. Kim, "Security Standard Status for Cognitive Radio Networks-focused on IEEE 802.22 WRAN," *Review of KIISC*, Vol, 19, No. 5, pp. 65-69, 2009.

[3] H. Kim, S. W. Lee, "Investigations of Security Framework for Cognitive Radio Network focused on IEEE 802.22 WRAN," *Journal of Security Engineering*, Vol. 6, No. 1, pp. 25-38, 2009.

[4] I. F. Akyildiz, W. Lee, and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks," *AD hoc networks*, Vol. 7, pp. 810-836, 2009.

[5] IEEE 802.22, IEEE P802.22/D1.0 draft standard for wireless regional area networks part 22: Cognitive wireless RAN medium access control(MAC) and physical layer(PHY) specifications: Policies and procedures for operation in the TV bands, Apr. 2008.

[6] J. Wang, M. S. Song, S. Santhiveeran, K. Lim, S. H. Hwang, M. Ghosh, V. Gaddam, and K. Challapali, "First Cognitive Radio Networking Standard for Personal/Portable Devices in TV White Spaces," *Ecma/TC48-TG1/2009/132*, white paper, 2009.

[7] D. Jang, H. Kim, "Security Standardization Status of Ecma-International for Personal/ Portable Devices supporting Cognitive Radio Networking," *Journal of Security Engineering*, Vol. 8, No. 5, pp. 553-565, 2011.

[8] T. C. Clancy, N. Goergen, "Security in cognitive radio networks: Threats and mitigation," *Proc. of CrownCom 2008*, pp. 1-8, 2008.

[9] R. Chen, J. Park, "Ensuring trustworth spectrum sensing in cognitive radio networks," *IEEE Workshop on Networking Technologies for SDR 2006*, pp. 110-119, 2006.

[10] H. Kim, "Design of Security Framework for Cognitive Radio Network," *Proc. of 2012 Conference on Convergence/Smart/Cloud computing*, pp. 23-27, 2012.

[11] H. Kim, "Security Aspects Analysis for Secondary User Authentication over Cognitive Radio Network," *Proc. of 2013 Conference on Convergence/Smart/Cloud computing*, pp. 56-59, 2014.

[12] H. Kim, "Analysis on Delegation-based Authentication Protocol for Wireless Roaming Service," *Proc. of 2014 Conference on Convergence/Smart/Cloud computing*, pp. 83-86, 2014.

[13] H. Kim, "Design of Adaptive Security Framework based on Carousel for Cognitive Radio Network," Journal of The Institute of Electronics Engineers of Korea, Vol. 50, No. 5, pp. 165-172, 2013.

[14] H. Kim, "Location-based authentication protocol for first cognitive radio networking standard," *Journal of Network and Computer Applications*, Vol. 34, pp. 1160-1167, 2011.

[15] W. B. Lee, C. K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," *IEEE Transactions on Wireless Communications*, Vol. 4, No. 1, pp. 57-64, 2005.

[16] C. Tang, D. O. Wu, "An efficient mobile authentication scheme for wireless networks," *IEEE Transactions on Wireless Communications*, Vol. 7, No. 4, pp. 1408-1416, 2008.

[17] J. L. Tsai, N. W. Lo, T. C. Wu, "Secure Delegation-Based Authentication Protocol for Wireless Roaming Service," *IEEE Communications Letters*, Vol. 16, No. 7, pp.

1100-1102, 2012.
[18] BWN Lab. GeorgiaTech, http://www.ece.gatech.edu/research/labs/bwn.
[19] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis”, *Lecture Notes in Computer Science*, Vol. 1666, pp. 388-397, 1999.
[20] F. X. Standaert, T. G. Malkin, M. Yung, “A unified framework for the analysis of side-channel key recovery attacks,” *Lecture Notes in Computer Science*, Vol. 5479, pp. 443-461, 2009.

저 자 소 개

김 현 성(정회원)
1998년 경북대학교 컴퓨터공학과 공학석사 졸업
2002년 경북대학교 컴퓨터공학과 공학박사 졸업
2002년～2011년 경일대학교 컴퓨터공학과 교수
2012년～현재 경일대학교 사이버보안학과 교수
2010년～현재 경일대학교 정보융합보안연구소 소장
2009년 더블린시립대학 컴퓨팅학과 방문교수
<주관심분야 : 인지무선네트워크 보안, 네트워크 보안, 암호 프로토콜, 암호구현, 정보보호>