情報保護學會論文誌
第20卷 第1號, 2010. 2

인지무선 네트워크를 위한 프라이버시가 강화된 인증 프로토콜

김 현 성† ‡
경일대학교

Privacy Aware Authentication Protocol for Cognitive Radio Networks

Hyun Sung Kim† ‡
Kyungil University

요 약

최근 들어 기하급수적으로 증가하는 방송 및 통신 시스템으로 인해 무선 주파수 자원의 고갈 문제가 심각하게 대두되고 있다. 이와 같은 주파수 고갈과 비효율적인 주파수 사용 문제를 해결하기 위해 유휴 주파수를 합리적으로 이용하기 위한 인지무선 기술이 많은 관심을 받고 있다. Kuroda등은 인지무선네트워크를 위한 무선 독립적인 인증 프로토콜을 제안하였다. 본 논문에서는 Kuroda등의 인증 프로토콜에 존재하는 프라이버시 취약성을 보이고 이를 해결하기 위한 프라이버시가 강화된 인증 프로토콜을 제안한다.

ABSTRACT

Recently, the spectrum scarcity is becoming a big issue because there are exponential growth of broadcasting and communication systems in the spectrum demand. Cognitive radio is a technology that is envisaged to solve the problems in wireless networks resulting from the limited available spectrum and the inefficiency in the spectrum usage by exploiting the existing wireless spectrum opportunistically. Kuroda et al. proposed a radio-independent authentication protocol for cognitive radio networks. This paper first shows the privacy weaknesses in the authentication protocol by Kuroda et al. and proposes a privacy aware authentication protocol to solve the weaknesses.

Keywords: IEEE 802.22, Cognitive radio network, Authentication protocol

I. 서 론

최근 들어 방송 및 통신 시스템의 급속한 성장과 더불어 차세대 통신 시스템은 여러 네트워크들의 융합 형태로 설계되고 시스템이 점점 복잡해지고 상호연동의 필요성이 점차 확대되고 있다. 또한, 통신 기술 및 서비스가 발전함에 따라 주파수 자원에 대한 사용 빈도가 증가하고, 우수한 통신 기술 및 서비스 제공을 위해 고정적으로 특정 주파수 대역을 점유함에 따라 주파수 고갈 문제가 심각한 상황에 이르렀다. 이와 같은 주파수 자원의 고갈 문제가 세계적으로 중요하게 인식됨에 따라 미국 FCC(Federal Communications Commission)는 2008년 11월 스펙트럼 사용 효율을 높이고 새로운 서비스 도입을 용이하게 하기 위해 TV 유휴주파수(White Space)를 대상으로 주파수 공유기술인 인지무선(Cognitive Radio) 기술을 적용하기로 하고 관련 규정을 개정하였다 [1,2].

Mitola에 의해 제안된 인지무선은 통신 장치가 스스로 통신 환경을 관찰하고, 최적의 통신을 위한 동작 방식을 판단하고 선택하며, 이전의 통신경험으로부터

접수일(2009년 7월 18일), 게재확정일(2009년 9월 14일)
† 주저자, kim@kiu.ac.kr
‡ 교신저자, kim@kiu.ac.kr

향후 판단 과정에 대한 계획을 세우는 시스템을 말한다[3,4]. 즉, 비면허 대역(Unlicensed Band)에 할당되어 있는 주파수 대역 중 그 활용도가 낮거나, 시/공간적으로 사용되지 않는 유휴자원(Spectrum Hole, White Space)을 찾아 적응적(Adaptive)이고 합리적(Opportunistic)으로 이용하는 기술이다. 이때 해당 대역에 이용권한(License)을 가지고 있는 주사용자(Primary User)가 발견되면 즉시 해당 대역의 사용을 멈추거나 전송 전력을 조절하여 주사용자에게 피해가 가지 않도록 동작해야 한다. 이를 위하여 FCC에서는 데이터베이스를 이용하는 방법과 스펙트럼 센싱(Spectrum Sensing)을 이용하는 방법을 적용하도록 권고하고 있다. 채널 사용 데이터베이스는 TV대역의 인지무선을 위한 주사용자 보호를 위하여 해당대역의 좌표에서 사용 가능한 채널을 찾기 위하여 사용되는 국가 데이터베이스이다[5].

인지무선 패러다임은 기존과는 완전히 새로운 보안의 위협요소들과 어려운 문제들을 야기하였고, 강력한 보안기법을 제공하는 것 자체가 인지무선 상용화에 있어서 가장 어려운 문제 중 하나일 것이다. 인지무선의 지능적인 속성(Intelligent Behavior)으로 인하여 인지무선자체의 위협요소를 조사하기 위한 몇몇 연구들이 진행되어 왔고, 최근에는 동적인 스펙트럼 접근 상에서의 공격 및 다양한 서비스 거부공격에 대한 논문이 발표되었다[6-9]. 하지만 대부분의 인지무선 관련 연구는 최근에 본격화 되고 있고, 따라서 보안연구도 구체적인 기법을 제공하지 못하는 문제점이 제시되고 있다.

이와는 달리 TV 유효주파수를 이용하여 광대역 무선 인터넷 서비스를 제공하기 위해 IEEE 802.22 WG(Working Group)은 WRAN(Wireless Regional Area Network) PHY/MAC 표준 재정을 진행하면서 프라이버시 및 보안을 위해서도 IEEE 802.16 표준의 X.509를 이용한 공개키 인증 알고리즘을 적용 한 기법을 기본적으로 도입하고자 노력하고 있다[10, 11]. 하지만 IEEE 802.16 보안 관련 표준은 인지무선의 기술적 속성을 고려하지 못하고 있어서 IEEE 802.22 자체를 위한 새로운 보안 기술이 제시되어야 할 필요성이 증대되고 있다. 최근에 Kuroda 등은 인지무선을 위한 무선 독립적인 인증 프로토콜(EAP-CRP)을 제안하였다[12]. EAP-CRP는 EAP (Extensible Authentication Protocol)를 지원하고 현재 사용하는 무선 프로토콜과 독립적인 인증을 제공하는데 그 목적이 있다.

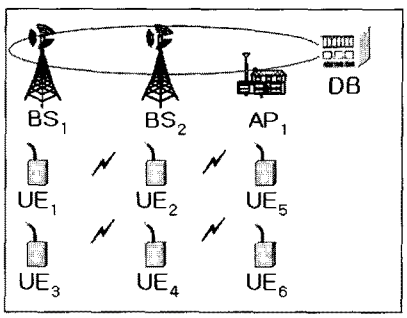
본 논문에서는 인지무선 네트워크에서 프라이버시의 필요성에 대하여 논하고 Kuroda등이 제안한 EAP-CRP에 대한 식별자 프라이버시와 위치 프라이버시에 대한 취약성을 보인다. 또한, EAP-CRP의 프라이버시 취약성 문제를 해결하기 위한 프라이버시가 강화된 인증 프로토콜을 제안한다. 본 논문에서 제안한 프로토콜은 IEEE 802.22의 인지무선 네트워크 구조를 위한 효율적인 인증을 제시할 수 있을 것이다.

II. 관련연구

본 장에서는 Kuroda등의 무선 독립적인 인증프로토콜(EAP-CRP)에 대해 기술한다[12]. 먼저 프로토콜의 기반이 되는 Kuroda등의 논문에서 활용한 인지무선 네트워크(Cognitive Radio Network) 환경에 대해서 살펴보고, EAP-CRP에 대해서 상세히 설명한다.

2.1 인지무선 네트워크

인지무선 네트워크는 라이센스가 없는 네트워크 사용자에게도 지역과 시간에 따라 사용하지 않는 주파수를 자동으로 찾아 주변의 허가된 노드들을 보호하면서 목적하는 통신이 가능하도록 하기위한 네트워크이다. 인지무선 기술은 현재 IEEE 802.22 WRAN 시스템을 기본 구조로 기술 규격 표준화에 많은 노력을 기울이고 있다. Kuroda등의 연구는 그림 1의 IEEE 802.22 네트워크 환경에 초점을 맞추고 있다.



[그림 1] IEEE 802.22 시나리오

IEEE 802.22 WRAN 시스템은 VHF/UHF TV 주파수 대역을 사용하여 넓은 영역에 다양한 형태의 음성 및 데이터 서비스를 제공하기 위한 시스템이다. 이 시스템은 셀 반경 내에 하나의 기지국(Base

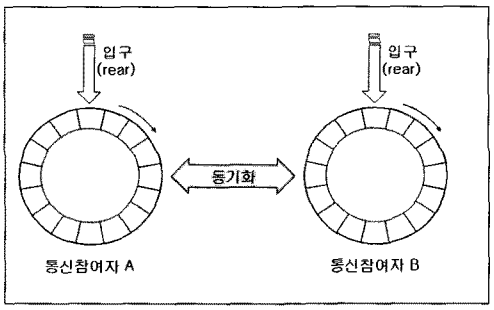
Station, BS)과 다수의 사용자 장치(User Equipment, UE, 이동노드)가 고정된 점대다점(Point to Multi-point) 형태로 구성되고 해당 대역에 이용권한을 가지고 있는 주사용자의 위치에 대한 정보를 담고 있는 데이터베이스(Database, DB)가 존재한다.

모든 BS는 DB를 통하여 초기화 과정에서 유휴채널에 대한 센싱 후 후보채널을 찾고 자원관련 정보에 대한 자문을 통하여 채널을 할당 받는다. 각 BS는 할당된 채널 상에서 인지무선 기지국 역할을 수행한다. UE는 통신을 시작하고자 할 때 유휴채널을 찾기 위해서 자신에게 미리 할당된 채널리스트를 조사하거나 모든 채널을 조사하고, 인접한 BS와 연결을 설립하며, 업링크(Uplink)와 다운링크(Downlink) 채널들과 파워레벨과 같은 자원관련 파라미터를 획득한다. 초기화 후 BS들과 UE들은 통신상태에 놓이게 되고 주기적으로 자원관련 정보를 DB에 보고한다. 권고된 자원관련 정보에는 UE의 위치정보와 파워레벨, 전송대역(Transmission Band), 모듈화 형식, 그리고 잡음비(Signal to Noise Ratio) 등이 있다. 이러한 정보를 획득한 후 DB는 BS들과 UE들의 환경을 재설정한다. 각 BS는 DB에 대한 접근을 통하여 자신의 영역에 속해있는 UE들을 제어하고 충돌이 발생하지 않도록 스펙트럼의 사용을 관리하며 좀더 강력하고 효율적인 모듈화와 코딩(Modulation and Coding)을 위한 설정을 수행한다.

UE들은 가용한 유휴채널 중 특정한 하나의 채널을 이용하기 위해 환경을 설정한 후 그 무선 시스템(Radio System)을 이용하기 위해서 시스템에서 요구하는 인증 절차를 수행해야 한다. 여기서 중요한 점은 각각의 무선 시스템에서 사용하는 인증기법은 각 시스템의 프로토콜 요구사항에 의존적이라는 것이다. 또한 현재 IEEE 802.22 초안(Draft)에도 인지무선의 플랫폼이 다른 무선 시스템으로 바뀔 때마다 인증을 수행하도록 요구하고 있다.

2.2 EAP-CRP

Kuroda등은 인지무선의 무선 시스템 의존성을 갖는 인증 방법을 해결하기 위한 무선 독립성(Radio Independent)을 제공하는 인증기법을 제안하였다. 무선 독립성을 제공하기 위해서는 인지무선 플랫폼이 사용할 수 있는 모든 무선 기술에 범용적으로 이용할 수 있는 정보를 사용할 필요가 있다. Kuroda등은 이러한 정보로서 이동노드(Mobile Node)의 위치정보(Location Information)를 선택하였다. 이 위치정보를 네트워크 참여자간의 비밀 값(Secret Value)을 추출하기 위한 수단으로 이용함으로서 AAA (Authentication Authorization Accounting) 서버의 참여를 배제하고 이를 통해 통신 오버헤드를 줄이기 위한 인증기법으로 EAP-CRP를 제안하였다.



〔그림 2〕 위치정보-회전자

〔표 1〕 기호정의

기 호	설 명
MN, AUi	이동노드와 인증자 i
LR	위치등록 서버
IDi	노드 i의 식별자
PIDi	노드 i의 익명 식별자
h()	일방향 해쉬 함수(one-way hash function)
Loc	위치정보
R, Ri	임의의 난수와 i번째 생성된 난수
L	등록된 위치정보 L=h(Loc, R)
CRi	노드 i의 위치정보-회전자 CR
Ki	노드 i가 위치정보-회전자를 통해 생성한 비밀키
{}K	비밀키 K를 이용한 데이터{}의 관용암호 연산
MAC	메시지 인증 코드(message authentication code)
||	문자열 결합 연산(concatenation)
→	메시지 전송

EAP-CRP는 위치정보 활용을 위하여 그림 2에서 보여 준 것과 같은 통신 참여자간에 동기화된 환영큐(Circular Queue)형태의 위치정보-회전자(Location Carousel) 자료구조를 이용한다. 위치정보-회전자의 각 셀은 위치정보 Loc와 R이 결합된 해쉬 정보인 $L=h(Loc, R)$을 저장한다.

인증에 참여하는 참여자 간 공유키를 생성하기 전에 위치정보-회전자는 동기화(Synchronization) 되어야 한다. 위치정보-회전자는 인증이 수행될 때마다 한 번씩 회전한다. 상호인증은 동기화된 위치정보-회전자로부터 생성된 인증키를 이용하여 수행된다. 본 논문에서 사용하는 기호에 대한 정의는 표 1과 같다.

EAP-CRP는 인지무선 네트워크에서 BS의 역할을 하는 두개의 인증자(Authenticator) AU_1과 AU_2 그리고 DB 역할을 하는 위치등록 서버(Location Registry) LR이 있음을 가정하고 이들 간에 안전한 통신경로가 설정된 것을 가정한다. 또한, 위치정보-회전자에 대한 초기 설정은 이동노드(MN)와 위치등록 서버(LR) 간에 안전한 방법을 통하여 오프라인(Off-line)으로 수행된다고 가정한다. 이때 위치정보-회전자는 안전한 방법으로 생성된 난수로 모든 셀이 초기화 된다. LR은 이동노드에 대한 데이터를 가지거나 이 데이터를 소유한 AU의 위치정보를 유지함으로서 위치정보-회전자를 관리한다. EAP-CRP의 구체적인 과정은 다음과 같다.

단계1) $AU \rightarrow MN$: IdentityREQ();
AU는 MN에게 식별자 요구메시지 IdentityREQ()를 보낸다.

단계2) $MN \rightarrow AU$: AuthREQ(ID_{MN});
MN은 자신의 식별자 ID_{MN}을 IdentityREQ()에 대한 응답메시지로 보낸다. 이 과정에서 MN은 AU에게 위치정보-회전자를 이용한 상호인증을 요청한다.

단계3) $AU \rightarrow LR$: InqREQ(ID_{MN})
AU는 LR에게 이동노드의 식별자 IDMN을 통하여 MN의 위치정보-회전자 정보를 요청한다. LR은 위치정보-회전자 정보를 자신이 가지고 있지 않으면 다른 인증자로부터 이 정보를 가져온다.

단계4) $LR \rightarrow AU$: InqREP(ID_{MN}, CR_{MN});
LR은 AU에게 위치정보-회전자 CR_{MN}을 보낸다.

단계5) $AU \rightarrow MN$: RotateREQ($\{R_1||MAC_1\}K_{AU}$);
AU는 위치정보-회전자로부터 인증키 K_{AU}를 생성하고 MN에게 도전(Challenge)메시지를 보낸다. AU는 도전메시지를 보내기 위해서 먼저 위치정보-회전자를 임의의 수만큼 회전시킨다. 회전된 위치정보-회전자의 최 상위 셀(Rear)을 통하여 인증키 K_{AU}를 생성하고, 난수 R_1과 메시지 인증코드 MAC_1(예, $MAC_1=h(R_1)$)을 생성한 후 K_{AU}를 이용하여 R_1과 MAC_1을 암호(Encryption)한다.

단계6) $MN \rightarrow AU$: RotateREP($\{R_1||R_2||MAC_2\}K_{MN}'$);
MN은 도전메시지에 대한 응답(Response)메시지를 보낸다. MN은 위치정보-회전자에 의해 생성된 인증키를 이용하여 받은 메시지를 복호(Decryption)한다. 만약 암호된 메시지에 대한 복호가 실패하면 성공할 때까지 위치정보-회전자를 임의의 횟수 회전시킨 후 인증키를 유도하고 복호를 시도한다. MN은 R_1에 대응하는 난수 R2와 메시지 인증코드 MAC_2(예, $MAC_2=h(R_2)$)를 생성한 후 현재위치 Loc와 R1을 이용하여 $L=h(Loc, R_1)$을 계산하고 이를 위치정보-회전자의 현재 셀(Rear)에 저장한다. MN은 생성된 L을 이용하여 인증키 K_{MN}'을 생성하고 이 키를 이용하여 응답메시지를 암호한다.

단계7) $AU \rightarrow MN$: AuthREP($\{R_2||MAC_2\}K_{AU}'$);
AU는 MN의 새로운 위치정보와 자신이 생성한 R_1을 이용하여 $L=h(Loc, R_1)$을 계산하고 이를 위치정보-회전자의 현재 셀(Cell)에 저장한다. AU는 L을 이용하여 인증키 K_{AU}'을 생성하고 MN으로부터 받은 응답메시지를 복호한다. 받은 메시지가 성공적으로 복호되었을 때 MN에게 인증 성공에 대한 메시지를 전송한다.

단계8) $AU \rightarrow LR$: Notify(ID_{MN}, Loc);
AU는 MN의 위치정보를 LR에게 알린다.

MN과 AU는 상호인증이 끝난 후 EAP에서 제안한 방법에 따른 안전한 통신 채널을 설립하기 위하여 뒤따르는 통신에 필요한 키들을 생성한다[13].

III. EAP-CRP의 프라이버시에 대한 분석

본 장에서는 인지무선 네트워크의 프라이버시에 대한 기본적인 요구사항을 분석하고, 이를 토대로 Kuroda등이 제안한 EAP-CRP의 프라이버시에 대한 문제점을 분석한다.

3.1 인지무선 네트워크의 프라이버시

다양한 크기의 지능형 장비 개발과 다양한 유/무선 네트워크의 융합 기술 개발을 통하여 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경의 현실화가

점점 가까워지고 있다. 하지만 유비쿼터스 컴퓨팅에 대한 프라이버시는 논란의 주된 이슈가 되고 있고, 프라이버시는 유비쿼터스 컴퓨팅의 성공적 실현을 위해서 넘어야 할 최대의 장벽으로 고려되고 있다. 프라이버시란 개인이나 그룹이 그들 자신이나 그들에 관한 정보를 제 삼자로부터 격리하고 선택적으로 그런 정보를 노출할 수 있는 능력을 말한다[14]. 특히, 정보통신에서 프라이버시 보호라 함은 노드의 통신 참여자에 대한 정보나 상대적인 위치 및 거리에 대한 정보를 제 삼자에게 드러나지 않도록 하는 것을 말한다. 2장에서 설명한 바와 같이 인지무선 네트워크에서는 서비스를 제공하기 위해 사용자의 위치정보를 하나의 중요 정보로 활용한다. 본 논문에서는 인지무선 네트워크의 프라이버시를 위한 가장 기본적인 고려로서 식별자 프라이버시(익명성)와 위치 프라이버시를 고려한다.

- ⊙ 식별자 프라이버시 : 통신 참여자의 실제 식별자(Identification)를 제 삼자가 모르게 한다.
- ⊙ 위치 프라이버시 : 통신 참여자의 상대적인 위치를 제 삼자가 모르게 한다.

3.2 EAP-CRP의 프라이버시 취약점

본 소절에서는 EAP-CRP의 프라이버시 문제점에 대한 분석을 제시한다. EAP-CRP는 식별자 프라이버시와 위치 프라이버시를 제공하지 못하는 문제가 있다.

EAP-CRP는 단계2에서 단계4까지의 메시지와 단계8의 메시지에서 이동노드의 식별자 ID_{MN}를 변형 없이 그대로 이용한다. 공격자는 노출된 통신 참여자의 식별자 정보를 통해서 식별자 프라이버시 관련 공격을 수행할 수 있다.

또한, EAP-CRP는 논문[12]에서 기술된 내용과는 달리 위치 프라이버시를 제공하지 못한다. EAP-CRP의 단계8에서 *AU*는 *LR*에게 Notify (ID_{MN}, *Loc*)메시지를 보낸다. 비록 가정에서 제시한 것처럼 *AU*와 *LR*간에 안전한 채널의 설립을 통한 메시지의 전송이 제시된다고 하더라도 인지무선 네트워크의 보안은 MAC(Medium Access Control)계층에서 고려되기 때문에 소스와 목적지 노드 사이에 있는 중간 노드에 대한 이동노드 위치 프라이버시 노출은 추가적으로 고려되어야 할 중요한 요소이다.

마지막으로, EAP-CRP의 단계6에서는 AU는 이동노드의 현재위치인 *Loc*와 R_1을 통해서 $L=h(Loc, R_1)$을 계산하고 계산된 *L*을 통해 생성된 인증키 K_{MN}'를 이용하여 응답메시지를 암호한다. 하지만 프로토콜에서는 *AU*가 위치정보-회전자 시스템에서 아주 중요한 정보인 이동노드의 위치 정보인 *Loc*을 획득하기 위한 방법을 제공하지 못하고 있다.

IV. 프라이버시가 강화된 인증 프로토콜

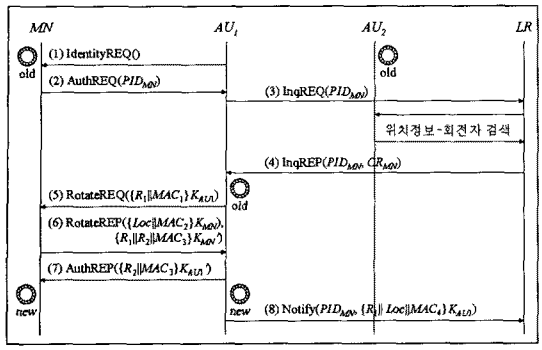
본 장에서는 IEEE 802.22의 인지무선 네트워크 구조를 위한 프라이버시가 강화된 인증 프로토콜을 제안한다. 본 논문에서 제안한 프로토콜은 EAP-CRP의 프라이버시 취약성을 효율적으로 해결하는데 그 목적이 있다. 이를 위해 본 논문에서 제안한 프로토콜은 익명 식별자를 이용하고 위치프라이버시를 제공하기 위해서 이동노드의 위치정보는 항상 암호하여 전송한다. 본 논문에서도 Kuroda등의 논문에서와 동일한 가정을 고려한다. 즉, 인지무선 네트워크에서 AU1과 AU2 그리고 LR 간에 안전한 통신경로가 설정되고 MN은 LR을 통해 위치정보-회전자를 동기화 된다고 가정한다.

본 장에서는 프라이버시 제공을 위해 기본적으로 고려될 이동노드의 익명 식별자에 대해 설명하고 익명 식별자를 활용한 본 논문에서 제안한 프라이버시가 강화된 인증 프로토콜에 대한 자세한 설명을 단계별로 제시한다.

4.1 익명 식별자의 초기화 및 갱신

본 논문에서 제안한 프라이버시가 강화된 인증 프로토콜은 이동노드 MN이 위치등록 서버 LR과 위치정보-회전자에 대한 초기화와 동기화를 수행할 때 자신의 익명 식별자 *PIDi*(예, $PID_i=h(ID_i, R)$)도 같이 제출한다. 여기서 R은 위치정보-회전자를 초기화할 때 사용한 난수와 동일하다. 이때 위치등록 서버는 필요에 따라 이동노드의 실제 식별자를 추가로 요구할 수 있다.

인증 프로토콜에 사용되는 익명 식별자는 세션(Session) 간 메시지의 비연결성을 제공하기 위해서 통신 세션마다 새로운 값으로 갱신되어야 할 필요가 있다. 본 논문에서 *MN*과 *LR*은 인증이 성공적으로 종료된 후, 다음 세션을 위해 새로운 익명 식별자 PID_{i+1}(예, $PID_{i+1}=h(PID_i, R_1)$)을 생성한다.



〔그림 3〕 프라이버시가 강화된 인증 프로토콜

4.2 제안한 인증 프로토콜

그림 3은 본 논문에서 제안한 프라이버시가 강화된 인증 프로토콜의 개념적인 수행과정을 보여주며 구체적인 동작과정은 다음과 같다.

단계1) $AU_1 \rightarrow MN$: IdentityREQ();
AU_1은 MN에게 식별자 요구메시지 IdentityREQ()를 보낸다.

단계2) $MN \rightarrow AU_1$: AuthREQ(PIDMN);
MN은 자신의 현재 세션의 식별자 PID_{MN}을 IdentityREQ()에 대한 응답메시지로 보낸다. 이 과정에서 MN은 AU_1에게 위치정보-회전자를 이용한 상호인증을 요청한다.

단계3) $AU_1 \rightarrow LR$: InqREQ(PID_{MN})
AU_1은 LR에게 이동노드의 식별자 PID_{MN}을 통하여 MN의 위치정보-회전자 정보를 요청한다. LR은 위치정보-회전자 정보를 자신이 가지고 있지 않으면 다른 인증자로부터 이 정보를 가져온다.

단계4) $LR \rightarrow AU_1$: InqREP(PID_{MN}, CR_{MN});
LR은 AU_1에게 위치정보-회전자 CR_{MN}을 보낸다.

단계5) $AU_1 \rightarrow MN$: RotateREQ($\{R_1||MAC_1\}K_{AU1}$);
AU_1은 위치정보-회전자로부터 인증키 K_{AU1}를 생성하고 MN에게 도전메시지를 보낸다. AU_1은 도전메시지를 보내기 위해서 먼저 위치정보-회전자를 임의의 수만큼 회전시킨다. 회전된 위치정보-회전자의 최상위 셀(Rear)을 통하여 인증키 K_{AU1}을 생성하고, 난수 R_1과 메시지 인증코드 MAC_1(예, $MAC_1=h(R_1)$)을 생성한 후 KAU를 이용하여 R_1과 MAC_1을 암호한다.

단계6) $MN \rightarrow AU_1$: RotateREP($\{Loc||MAC_2\}K_{MN}$, $\{R_1||R_2||MAC_3\}K_{MN}'$);
MN은 위치정보-회전자로부터 인증키 K_{MN}과 K_{MN}'을 생성하고 AU_1에게 도전메시지에 대한 응답메시지를 보낸다. MN은 위치정보-회전자에 의해 생성된 인증키를 이용하여 받은 메시지를 복호한다. 만약 복호가 실패하면 성공할 때까지 위치정보-회전자를 임의의 횟수 회전시킨 후 인증키 K_{MN}을 유도하고 복호를 시도한다. MN은 자신의 새로운 위치정보 Loc와 R_1을 이용하여 $L=h(Loc, R_1)$을 계산하고 이를 위치정보-회전자의 현재 셀(Rear)에 저장하며 L을 이용하여 인증키 K_{MN}'을 생성한다. MN은 현재 위치정보 Loc와 메시지 인증코드 MAC_2(예, $MAC_2=h(Loc)$)를 K_{MN}을 이용하여 암호하고, R1에 대응하는 난수 R2를 생성하며 이에 대한 메시지 인증코드 MAC3(예, $MAC_3=h(R_2)$)를 생성한 후 K_{MN}'을 이용하여 $\{R_1||R_2||MAC_3\}$메시지를 암호한다.

단계7) $AU_1 \rightarrow MN$: AuthREP($\{R_2||MAC_3\}K_{AU1}'$);
AU_1은 MN으로부터 받은 메시지의 첫 번째 암호화 된 값을 K_{AU1}을 이용하여 MN의 새로운 위치 정보를 확인한다. 그리고 $L=h(Loc, R_1)$을 계산한 후 이를 위치정보-회전자의 현재 셀에 저장하고 생성된 L을 이용하여 인증키 K_{AU1}'을 유도하여 두 번째 암호된 값을 복호한다. MN으로부터 받은 메시지가 모두 성공적으로 복호되었을 때 MN에게 인증 성공에 대한 메시지를 전송한다.

단계8) $AU1 \rightarrow LR$: Notify(PID_{MN}, $\{R_1||Loc||MAC_4\}K_{AU1}$);
AU_1은 MN의 현재 세션 난수 R_1과 현재 위치정보 Loc를 인증키 K_{AU1}을 이용하여 LR에게 알린다.

MN과 AU_1은 상호인증이 끝난 후 EAP에서 제안한 방법에 따른 안전한 통신 채널을 설립하기 위하여 뒤따르는 통신에 필요한 키들을 생성한다. 그리고 MN과 LR은 다음 세션을 위해 새로운 익명 식별자

PID_{i+1}을 생성한다.

V. 안전성 분석

본 장에서는 제안된 프라이버시가 강화된 인증프로토콜에 대한 안전성 분석을 제시한다. 본 논문의 안전성 분석도 Kuroda등의 분석과 비슷하여 프라이버시에 대한 분석을 강화하여 제시한다.

5.1 위치정보-회전자에 대한 위치 프라이버시 분석

위치정보-회전자의 각 셀은 이동노드의 위치정보 Loc와 난수 R을 이용한 해쉬 값인 $L=h(Loc, R)$을 저장한다. 공격자가 위치정보-회전자를 획득한다고 하더라도 해쉬 된 정보 L을 통해 이동노드의 위치정보를 확인할 수 있는 방법은 해쉬 함수의 일방향성에 의존한다. 난수를 이용한 해쉬 연산은 비슷한 위치의 다른 이동노드와는 다른 L의 사용을 보증한다[12]. 즉, 본 논문에서 제안한 인증 프로토콜은 해쉬된 값인 L을 위치정보-회전자에 저장함으로서 위치 프라이버시를 제공할 수 있다.

5.2 식별자 프라이버시 분석

식별자 프라이버시는 통신 참여자의 실제 식별자를 제 삼자가 모르게 함으로서 제공할 수 있다. 특히, 본 논문 환경의 인증 프로토콜에서 식별자 프라이버시는 이동단말(사용자)의 식별자에 대한 제 삼자에게의 익명성을 의미한다. 본 논문에서 제안한 강화된 인증 프로토콜은 이동단말의 실제 식별자 ID_i 대신에 익명 식별자 PID_i를 이용함으로서 프라이버시를 제공한다. 또한 논문에서 제안한 프로토콜에서는 매 세션 새로운 익명 식별자를 사용함으로서 세션 간 메시지의 비연결성도 제공한다.

5.3 기밀성에 대한 분석

본 논문에서 제안한 프라이버시가 강화된 인증 프로토콜은 위치정보-회전자를 이용하여 유도된 인증키를 사용하기 때문에 인증키의 기밀성 분석은 필수적이다. 위치정보-회전자를 통해 생성된 키에 대한 기밀성 공격은 위치정보-회전자의 추론(Inferring)과 이동노드의 추적을 통해서 제시될 수 있을 것이다[15]. 이동노드의 추적을 통한 공격은 공격자가 이동노드가 이동한 지역을 모두 추적할 수 있다는 가정 하에서 진행되어야 하고 이는 매우 어려운 일이므로 본 소절에서는 추론을 통한 공격에 초점을 맞춘다. 공격에 대한 분석을 제시하기 위해서 위치정보-회전자의 각 셀이 공격자에게 알려지지 않은 난수에 의해 채워졌다고 가정하고 공격자는 이동노드의 위치변경에 대해 한번만 모니터 할 수 있다고 가정한다[12]. 이러한 가정을 통해서 공격자는 자신이 모니터한 이동노드의 위치정보 Loc를 통해 위치정보-회전자의 한 셀 정보인 $L=h(Loc, R)$을 알 수 있을 것이다. 하지만 본 논문에서 제안한 강화된 인증 프로토콜의 안전성은 위치정보-회전자에 공격자가 모니터링 한 정보와 연계된 정보가 위치정보-회전자의 어느 위치에 저장되는지 알지 못하는데 근거하고 있다.

프로토콜의 기밀성에 대한 분석을 보다 명확하게 제시하기 위해서는 MN이 특정 AU와의 통신 세션에서 공유한 위치정보-회전자의 한 셀과 공격자가 모니터링 한 정보가 동일할 확률에 대해 고려하는 것이다[12]. 위치정보-회전자가 초기화 될 때 안전한 절차에 의해 생성된 값에 의해 초기화 되고, 초기 난수 값의 비예측성(Uncertainty) 때문에 모든 셀의 정보가 위치 정보로 업데이트 되지 않는 한 공격자는 이동노드와 동일한 위치정보-회전자를 생성할 수 있는 가능성이 없다. 또한, 모든 셀의 정보가 위치 정보로 업데이트 된다고 하더라도 공격자가 이전 세션들에서 사용한 이동노드의 정확한 위치를 추적하는 것은 거의 불가능함으로 기밀성에 대한 공격은 실패할 것이다.

VI. 결 론

본 논문에서는 IEEE 802.22를 기반으로 하는 인지무선 네트워크에서 프라이버시의 필요성에 대하여 논의 하였고, Kuroda등이 제안한 EAP-CRP가 식별자 프라이버시와 위치 프라이버시에 대해 취약함을 보였다. 그리고 EAP-CRP의 프라이버시 취약성을 해결하기 위한 새로운 프라이버시가 강화된 인증 프로토콜을 제안하였다. 본 논문에서 제안한 프로토콜은 IEEE 802.22의 인지무선 네트워크를 위한 효율적인 인증을 위해 활용될 수 있을 것이다.

향후 연구로는 인지무선 네트워크의 특성에 적합한 프라이버시 관련된 다양한 속성들을 정리하고 이를 만족할 수 있는 보안 인프라구조에 대한 연구가 수행될 필요가 있을 것으로 사료된다.

참 고 문 헌

[1] 고광진, 박창현, 송명선, 엄중선, 유성진, 임선민, 정회윤, 황성현, "TV White Spaces에서의 CR 기술 동향," 전자통신동향분석, 24(3), pp. 91-102, 2009년 6월.

[2] FCC, ET Docket No. 08-260, Second Report and Order and Memorandum Opinion and Order, Nov. 2008.

[3] J. Mitola and G. Maguire, "Cognitive radio: Making software radios more personal," IEEE Pers. Commun., vol. 6, no. 4, pp. 13-18, Aug. 1999.

[4] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," Proc. of IEEE Workshop on Mobile Multimedia Comm., pp. 3-10, 1999.

[5] IEEE 802.22, "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," IEEE P802.22-D1.0, 2008.

[6] J.L. Burbank, "Security in cognitive radio networks : the required evolution in approaches to wireless network security," Proc. of CrownCom 2008, pp. 1-7, May 2008.

[7] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Journal on selected areas in communications, vol. 26, no. 7, pp. 25-37, Jan. 2008.

[8] T. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi- dimensional analysis and assessment," Proc. of CrownCom 2008, pp. 456-464, May 2008.

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

[10] IEEE 802.22, "Recommended Text for Security in 802.22," IEEE 802.22-08/0174r17, 2009.

[11] IEEE 802 ECSG on WS, "Security Tutorial," IEEE 802ECSGonWS-09/0045r01, 2009.

[12] M. Kuroda, R. Nomura, and W. Trappe, "A Radio-independent Authentication Protocol (EAP-CRP) for Networks of Cognitive Radios," Proc. of SECON'07, pp. 70-79, June 2007.

[13] D. Stanley, J. Walker, and B. Aboba, "EAP Method Requirements for Wireless LANs," RFC 4017, Mar. 2005.

[14] D. Wright, S. Gutwirth, M. Friedewald, P.D. Hert, M. Langheinrich, and A. Moscibroda, "Privacy, trust and policy-making:Challenges and responses," Computer Law & Security Report, vol. 25, no. 1, pp. 69-83, 2009.

[15] R. Nomura, M. Kuroda, and D. Inoue, "Location-based Key Management for Ubiquitous Wireless Network," IWS 2005/WPMC'05, pp. 51-55, Sep. 2005.

〈著者紹介〉

김 현 성 (Hyun Sung Kim) 종신회원
2002년 2월: 경북대학교 컴퓨터공학과 박사
2002년 3월~현재: 경일대학교 컴퓨터공학과 교수
2002년 3월~현재: 한국정보보호학회 논문지 심사위원
2009년 1월~현재: 더블린시립대학 컴퓨팅학과 방문교수
〈관심분야〉 인지무선네트워크 보안, 네트워크 보안, 암호프로토콜, 암호구현, 정보보호