情 報 保 護 學 會 誌
第19卷 第5號, 2009. 10

인지무선네트워크를 위한 보안 표준화 현황 - IEEE 802.22 WRAN을 중심으로

김 현 성*

요 약

최근 들어 기학급수적으로 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(Cognitive radio) 기술이 많은 관심을 받고 있다. 본 고에서는 TV 주파수 대역 내 유휴자원(White space)을 대상으로 주파수 공유 기술인 인지무선 기술을 적용하기 위해 현재 표준화가 진행 중인 IEEE 802.22 WRAN을 중심으로 인지무선네트워크를 위한 보안 표준화 현황을 살펴본다.

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 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 데이터베이스(Database, DB)를 이용하는 방법과 스펙트럼 센싱(Spectrum sensing)을 이용하는 방법을 적용하도록 하고 있다. 채널 사용 DB는 TV대역의 인지무선을 위한 주사용자 보호 기법으로 해당대역의 좌표에서 사용 가능한 채널을 찾기 위하여 사용되는 국가 DB이다[5].

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 적용한 기법을 기본적으로 도입하고자 노력하였다[5-7]. 하지만 IEEE 802.16 보안 관련 표준은 인지무선의 기술적 속성이 고려되지 못해서 IEEE 802.22 자체를 위한 새로운 보안 기술이 제시되어야 할 필요성이 증대되고 있

본 연구는 2009년도 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2009-013-D00118)
* 경일대학교 컴퓨터공학과 (kim@kiu.ac.kr)

다. 최근에는 인지무선의 기술적 속성을 고려하기 위해서 추가로 보안서브레이어(Security sublayer)를 제시하기 위한 노력을 하고 있다[8].

지금까지 다양한 무선 응용을 위한 보안 표준들이 제안되어 왔지만, 거의 대부분의 보안 표준에서 많은 문제들이 발견되고 있고 이를 보완하기 위한 노력들이 계속 진행되고 있다. 이러한 문제가 제시되는 가장 중요한 원인은 표준 추진과정에서 보안보다는 그 표준의 기술적 내용의 실현에 대한 구체화를 표준화의 목적으로 제시하여 왔기 때문이다. 이러한 문제는 IEEE 802.22 WRAN에서도 여전히 반복되고 있고, 본 고의 목적이 여기에 있다.

본 고에서는 TV 주파수 대역 내 빈 공간을 대상으로 주파수 공유 기술인 인지무선 기술을 적용하기 위해 현재 표준화가 진행 중인 IEEE 802.22 WRAN을 중심으로 인지무선네트워크를 위한 보안 표준화 현황을 살펴본다.

본 고의 구성은 다음과 같다. Ⅱ장에서는 인지무선네트워크의 기본개념에 대해서 IEEE 802.22 WRAN을 중심으로 살펴본다. Ⅲ장에서는 IEEE 802.22 WRAN의 보안 표준화 현황에 대해서 살펴보고 Ⅳ장에서 결론을 맺는다.

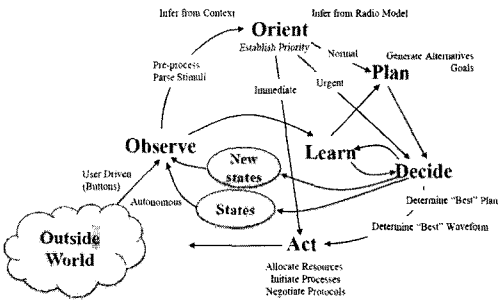
Ⅱ. 인지무선네트워크

본 장에서는 인지무선네트워크의 정의를 살펴보고 이를 위한 표준화 노력으로서 IEEE 802.22 WRAN 시스템의 개요에 대해서 살펴본다.

2.1 인지무선네트워크

인지무선네트워크(Cognitive radio network)는 라이센스(License)가 없는 네트워크 사용자에게도 지역과 시간에 따라 사용하지 않는 주파수를 자동으로 찾아 주변의 허가된 노드들을 보호하면서 목적하는 통신이 가능하도록 하기위한 네트워크이다[9].

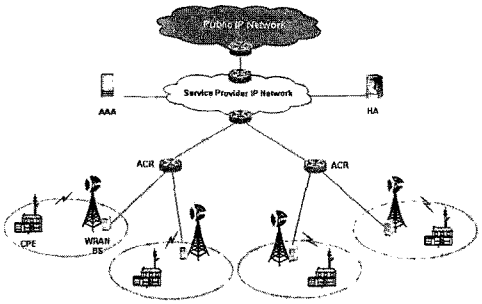
인지무선네트워크는 [그림 1]과 같이 6단계로 구성된 인지사이클(Cognition cycle)을 기반으로 운용된다. 인지사이클은 관측(Observe), 인지(Orient), 계획(Plan), 결정(Decide), 동작(Act), 그리고 학습(Learn)의 단계로 구성되며, 외부 환경에 대한 분석을 위해 이 6단계를 운영한다.



〔그림 1〕 인지무선네트워크의 인지사이클[9]

2.2 IEEE 802.22 WRAN

IEEE 802.22 WRAN 시스템은 VHF/UHF TV 주파수 대역을 사용하여 넓은 영역에 다양한 형태의 음성 및 데이터 서비스를 제공하기 위한 시스템으로서 인지무선 기술이 처음으로 접목된 시스템이다. [그림 2]에서 보여주는 바와 같이 이 시스템은 셀 반경 내에 하나의 기지국(Base Station, BS)과 다수의 비면허 사용자 장치(Customer Premise Equipment, CPE)가 고정된 점대다점(Point to Multi-point) 형태로 구성되고 해당 대역에 이용권한을 가지고 있는 주사용자(Primary user)의 위치에 대한 정보를 담고 있는 데이터베이스(Database, DB)가 존재한다[10].



〔그림 2〕 WRAN시스템의 서비스 시나리오[5]

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. CPE는 통신을 시작하고자 할 때 유휴채널을 찾기 위해서 자신에게 미리 할당된 채널리스트를 조사하거나 모든 채널

을 조사하고, 인접한 BS와 연결을 설립하며, 업링크(Uplink)와 다운링크(Downlink) 채널들과 파워레벨과 같은 자원관련 파라미터를 획득한다. 초기화 후 BS들과 CPE들은 통신상태에 놓이게 되고 주기적으로 자원관련 정보를 DB에 보고한다. 권고된 CPE의 자원관련 정보는 다음과 같다[11].

- 위치정보(Geolocation) : 위도, 경도, 높이(height above average ground level)
- 장치식별자 : 제품식별자(FCC ID)와 시리얼번호(MAC주소가 대체될 수 있음)
- 장치타입 : 고정형, 이동모드

이러한 정보를 획득한 후 DB는 BS들과 CPE들의 환경을 재설정한다. 각 BS는 DB에 대한 접근을 통하여 자신의 영역에 속해있는 CPE들을 제어하고 충돌이 발생하지 않도록 스펙트럼의 사용을 관리하며 좀더 강력하고 효율적인 모듈화와 코딩(Modulation and coding)을 위한 설정을 수행한다.

Ⅲ. IEEE 802.22 보안 서브레이어

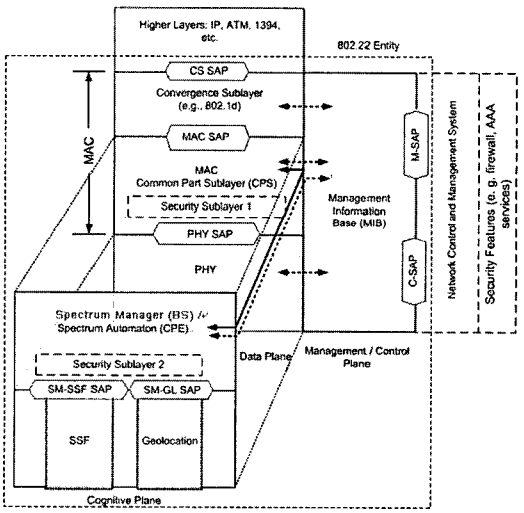
IEEE 802.22 WRAN MAC(Medium Access Control) 계층에 대한 표준화는 2005년 11월에 시작되었고, 보안도 MAC의 서브레이어(Sublayer)에 두기로 결정되었다. 보안(Security)에 대한 연구는 2008년 4월에 시작되었다. 본 장에서는 IEEE 802.22 WRAN 초안(Draft) v1.0의 MAC 보안 서브레이어와 v2.0을 위한 추진현황에 대해서 살펴본다.

3.1 초안 v1.0 - 단일 서브레이어

IEEE 802.22 WG은 2008년 5월 초안 v1.0을 완성하였다. 초안 v1.0에 정의된 보안 서브레이어는 CPE와 BS사이에 전송될 MAC 데이터(MPDU)에 암호학적 변형을 제시함으로서 기밀성과 인증 그리고 데이터무결성 서비스를 제공하고자 작성되었다[7]. 이를위해 IEEE 802.16 표준의 X.509를 이용한 공개키 인증 알고리즘을 적용 한 기법을 기본적으로 도입하였다. 보안 서브레이어는 캡슐화 프로토콜(Encapsulation protocol)과 프라이버시 키 관리 프로토콜(Privacy key management protocol, PKM)로 구성된다. 캡슐화 프로토콜은 데이터 암호화와 인증 알고리즘들의 쌍과 같은 지원되는 암호학적 기법들의 집합과 이들 알고리즘이 MPDU에 적용되기 위한 규칙을 정의한다. PKM은 BS가 CPE들에게 키를 설립하는데 필요한 정보를 안전하게 분배하는 것을 보증하는 프로토콜이다.

3.2 초안 v2.0 - 여러개의 서브레이어

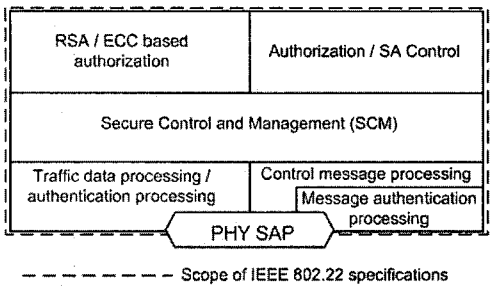
초안 v1.0의 보안 서브레이어는 인지무선의 기술적인 속성을 고려하지 못하고 있어서 이를 보완하기 위한 노력이 꾸준히 제시되고 있다. 아직 초안 v2.0이 완성되지 않았으므로 본 소절에서는 현재까지 IEEE 802.22 WRAN에서 진행된 보안 표준화 현황을 표준화 문서[12]를 통하여 제시하고자 한다.



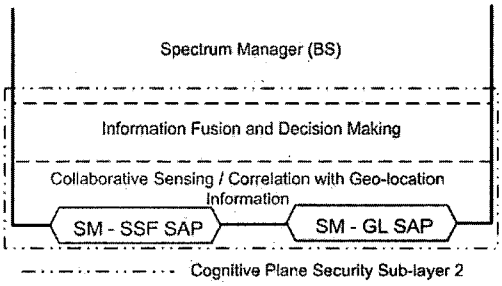
〔그림 3〕 IEEE 802.22 참조구조[12]

인지무선 기술에 의존적인 속성에 대한 보안기법 제시를 위해서 IEEE 802.22 보안 WG은 하나의 보안 서브레이어를 두 개의 서브레이어로 확장하기 위한 노력을 제시하였다. 즉, [그림 3]에서 보여준 바와 같이 초안 v2.0을 위해서 시스템의 인지기능과 함께 비인지기능에도 초점을 맞춘 두 개의 보안 서브레이어를 제안하고 이를 구체화하기 위한 작업을 현재 진행하고 있다.

[그림 4]는 초안 v2.0을 위한 보안 서브레이어의 구체화된 내용을 보여준다[12]. 초안 v2.0 보안 서브레이어를 위한 문서는 BS와 CPE간의 키 설립 정보 분배를 위한 인증된 클라이언트/서버 키 관리 프로토콜(An



(가) 보안 서브레이어 1



(나) 보안 서브레이어 2

〔그림 4〕 초안 v2.0의 IEEE 802.22 보안 서브레이어

authenticated client/server key management protocol)을 제안했다. 또한 v1.0에서와 같이 키 관리 프로토콜의 보안을 강화하기 위하여 디지털 인증서 기반의 CPE 장치 권한체크(digital certificate based CPE device authorization) 기능의 사용을 권고하고 있다.

인지무선시스템에서는 기밀성과 프라이버시 기법들이 데이터 뿐 만 아니라 민감한 스펙트럼 소유 정보와 BS가 CPE들의 작업을 구성하는데 사용되는 스펙트럼 관리 정보들에 대해서도 보호되어야 한다. 이를 위해서 초안 v2.0은 인지기능에 관한 보안 속성들과 기법들을 위해서 유효성(Availability), 인증, 권한부여(Authorization), 식별(Identification), 무결성, 기밀성 그리고 프라이버시를 포함하기 위해 노력했다. 그 결과로 초안 v2.0에서는 IEEE 802.22의 인지기능에 대한 보안을 향상시키기 위해서 보안 서브레이어 2가 추가되었다. 이 보안기법들은 협동적인 센싱(Collaborative sensing)과 협동적인 결정(Collaborative decision)과 같은 기법을 도입함으로서 네트워크의 주사용자와 2차 사용자(Secondary user)들에 대한 스펙트럼의 유효성을 보증한다. 보안서브레이어 2는 서비스 거부공격을 피하기 위해 거주자 센싱 정보(Incumbent sensing information)에 대한 인증과 보안 속성을 활용한 802.22.1 비컨 프레임의 인증, 위치정보와 공존(Coexistence)정보의 인증을 포함한 다양한 인증들을 제시한다. 스펙트럼 센싱 기능, 위치정보, 스펙트럼 관리자, 스펙트럼 자동화, 관리를 위한 절차와 함수들을 포함한 다양한 인지기능 보안과 연계된 기법들은 IEEE 802.22 시스템 구현에 요구되는 다른 인지 기능들의 중요한 한 부분을 차지한다.

Ⅳ. 결 론

인지무선 기술은 다가올 미래 주파수 자원의 수요 급증에 대응할 수 있는 가장 효율적인 기술로 인식되고 있다. 본 고에서는 TV 주파수 대역 내 빈 공간을 대상으로 주파수 공유 기술인 인지무선 기술을 적용하기 위해 표준화가 진행 중인 IEEE 802.22 WRAN을 중심으로 인지무선네트워크를 위한 보안 표준화 현황을 살펴보았다. IEEE 802.22 WRAN은 WLAN, WPAN, 유비쿼터스 센서 네트워크를 포함한 다양한 차세대 무선 응용 기술에 적용될 수 있고, 고정 및 이동 통신 서비스 등 넓은 범위에 적용될 수 있을 것으로 기대된다.

하지만 IEEE 802.22 WRAN을 위한 보안 연구는 아직도 초기단계에 머물러 있고, 프라이버시에 대한 문제점도 지적되고 있다[13]. 지금까지 다양한 무선 응용을 위한 보안 표준화 과정을 통해서도 확인한 것처럼, 지금이 인지무선 기술을 위한 표준화의 초기과정이고 보안 연구에 초점을 맞추기 위한 가장 적합한 시기가 아닌가 생각한다.

참고문헌

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

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

[3] J. Mitola III and G. Maguire, "Cognitive radio: Making software radios more personal", *IEEE Pers. Commun.,* 6(4), pp. 13-18, August 1999.

[4] J. Mitola III, "Cognitive radio for flexible mobile multimedia communications", *Proc. of IEEE*

Workshop on Mobile Multimedia Comm., pp. 3-10, Nov. 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] IEEE 802 ECSG on WS, *Security Tutorial,* IEEE 802ECSGonWS-09/0045r01, 2009.

[7] K. Bian and J. M. Park, "Security vulnerabilites in IEEE 802.22," *WICON'08,* Article No. 9, Nov. 2008.

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

[9] J. Mitola III, *Cognitive radio: An integrated agent architecture for software radio architecture,* Ph.D. Dissertation, Royal Institute of Technology (KTH), May 2000.

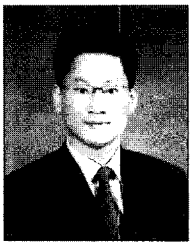
[10] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer, and W. Caldwell, "IEEE 802.22:The first cognitive radio wireless regional area network standard," *IEEE Communications Magazine,* pp. 130-138, Jan. 2009.

[11] IEEE 802.22, *802.22 Database Service Interface,* IEEE 802.22-09/00123r6, July 2009.

[12] IEEE 802.22, *Recommended Text for Security in 802.22,* IEEE 802.22-08/0174r18, May 2009.

[13] IEEE 802.22, *Privacy concerns,* IEEE 802.22-09/0114, July 2009.

〈著者紹介〉



김 현 성 (Hyun Sung Kim)
종신회원

1996년 2월: 경일대학교 컴퓨터공학과 학사
1998년 2월: 경북대학교 컴퓨터공학과 석사
2002년 2월: 경북대학교 컴퓨터공학과 박사
2002년 3월~현재: 경일대학교 컴퓨터공학과 교수
2002년 3월~현재: 한국정보보호학회 논문지 편집위원
2009년 1월~현재: 더블린시립대학 컴퓨팅학과 방문교수
<관심분야> 인지무선네트워크 보안, 네트워크 보안, 암호 프로토콜, 암호구현, 정보보호