2013년 5월 전자공학회 논문지 제 50 권 제 5 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 5, May 2013 http://dx.doi.org/10.5573/ieek.2013.50.5.165

논문 2012-50-5-19

인지무선네트워크를 위한 회전자 기반 적응형 보안프레임워크 설계

(Design of Adaptive Security Framework based on Carousel for Cognitive Radio Network)

김 현 성*

(Hyunsung Kim©)

요 약

최근 들어 IT 분야에 하나나 그 이상의 기술들이 하나의 장치에 결합되는 융합이 활발히 진행되고 있다. 특히, 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 융합기술인 인지무선 기술이 많은 관심을 받고 있다. 하지만 융합을 통해 개별적으로 제공되던 기존 서비스에 새로 개발된 기술들이 결합됨으로서 기존에는 존재하지 않았던 새로운 보안 문제들을 야기할 수 있다. 본 논문의 목적은 통신 융합응용 기술로서 인지무선네트워크를 위한 회전자 기반 적응형 보안프레임워크를 제안한다. 제안한 적응형 보안프레임워크는 위치정보에 기반한 회전자를 프라이버시 및 다양한 보안을 제공하기 위한 보안 기법들에 필요한 공유키 설정을 위한 기초로 이용한다. 본 논문에서 제안한 적응형 보안프레임워크는 인지무선네트워크 표준들을 포함한 다양한 융합응용의 보안 기반 구조로 활용될 수 있을 것이다.

Abstract

Convergence is increasingly prevalent in the IT world which generally refers to the combination of two or more different technologies in a single device. Especially, the spectrum scarcity is becoming a big issue because there are exponential growth of broadcasting and communication systems in the spectrum demand. Cognitive radio (CR) is a convergence 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. However, the very process of convergence is likely to expose significant security issues due to the merging of what have been separate services and technologies and also as a result of the introduction of new technologies. The main purpose of this research is focused on devising an adaptive security framework based on carousel for CR networks as a distinct telecommunication convergence application, which are still at the stage of being developed and standardized with the lack of security concerns. The framework uses a secure credential, named as carousel, initialized with the location related information from objects position, which is used to design security mechanisms for supporting privacy and various securities based on it. The proposed adaptive security framework could be used as a security building block for the CR network standards and various convergence applications.

Keywords : 정보보호, 보안프레임워크, 프라이버시, 위치정보기반, 회전자

* 정회원, 경일대학교 사이버보안학과
(Department of Cyber Security, Kyungil University)
※ 본 연구는 2012년도 융합/스마트/클라우드 컴퓨팅 학술대회에서 '인지무선네트워크를 위한 보안 프레임워크 설계' 제목으로 발표된 논문[17]을 확장한 것임.
※ 본 연구는 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 연구임 (한국연구재단2010-0021575).
© Corresponding Author(E-mail:kim@kiu.ac.kr)
접수일자: 2013년2월7일, 수정완료일: 2013년4월17일

Ⅰ. 서 론

인터넷과 Wi-Fi, 그리고 TV Broadcast와 같은 컴퓨터 네트워크 기술들의 빠른 성장과 함께 소비자들의 데이터 통신에 대한 의존성 및 그에 따른 요구사항 또한 증가 하고 있다. 특히, 최근 들어 차세대 통신 시스템은 여러 네트워크들의 융합 형태로 설계되고 시스템이 점점 복잡해지고 상호연동의 필요성이 점차 확대되고 있다. 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. 인지무선(Cognitive Radio) 기술은 그 지역의 특성에 맞춰 적응적이고 합리적으로 무선 주파수를 활용하게 한다. 현재 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 가지 형태가 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[5]. IEEE의 활동과는 별개로 ECMA-International은 개인/휴대기기들을 위한 인지무선 표준을 발표하였다[6~7]. 2009년 2월 FCC(Federal Communications Commission)는 TV 유휴주파수(White Space) 기기관련법안(Television Band Device (TVBDs))을 제정하였고, FCC는 이 법안에서 인지무선을 위한 고정형과 개인/휴대기기의 두 가지 형태의 기기를 정의 하였다. 개인/휴대기기의 사용은 두 가지 모드로 구성된다. 모드1은 주/종속(Master- Slave) 네트워크에서 종속 역할의 기기를 위한 모드이다. 모드 2는 주/종속 네트워크에서의 주기기 또는 동등 계층(Peer to Peer) 네트워크에서의 동등 계층 기기를 위한 모드이며, 이러한 개인/휴대기기의 사용은 별도의 채널 사용 데이터베이스의 등록을 필요로 하지 않는다.

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 기술적 속성을 고려하지 못하고 있어 이를 고려한 추가적인 보안 연구의 필요성이 증대 되고 있다[8~19].

본 논문에서는 인지무선네트워크를 위한 회전자기반 적응형 보안프레임워크를 제안한다. 이를 위해 먼저 인지무선네트워크의 특성을 파악하고 이러한 특성에 기반한 다양한 보안 위협을 도출한다. 이러한 분석을 기반으로 일반적인 네트워크와 인지무선네트워크의 보안을 위한 기본적인 요구사항으로 유효성 (Availability)과 인증 (Authentication), 권한 인증 (Authorization), 신원확인 (Identification), 무결성 (Integrity), 기밀성 (Confidentiality), 프라이버시(Privacy)관점에 대해 정의하고 이러한 서비스를 제공하기 위한 회전자기반의 보안프레임워크를 제안한다. 본 논문에서 제안한 보안프레임워크는 이러한 기본적인 네트워크의 보안 요구사항을 만족하기 위해서 객체(Objects)의 위치정보에 기반한 회전자(Carousel)를 프라이버시 및 다양한 보안 요구사항을 제공하기 위한 보안 기법들을 설계하기 위해 필요한 보안 기초로 활용한다[16]. 이는 특히 IEEE 802.22와 같은 표준에서 요구되는 위치기반의 사용자 인증을 위한 아주 효율적인 기반구조로 활용될 수 있다. 본 논문에서 제안한 적응형 보안프레임워크는 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 인지무선네트워크의 특성을 살펴보고, Ⅲ장에서는 그러한 특성에 기반한 다양한 인지무선네트워크 보안 위협에 대해 기술 한다. 그리고 Ⅳ장에서는 인지무선네트워크를 위한 회전자기반 적응형 보안프레임워크를 제안하고, Ⅴ장에서 결론을 맺는다.

Ⅱ. 인지무선네트워크

Mitola는 1991년에 SDR(Software Defined Radio) 개념을 그리고 1998년에 인지무선 개념을 정립하였다[2]. SDR은 소프트웨어 무선으로도 불리는데, 여러 개의 무선장치와 프로토콜들을 지원하고 DSP(Digital Signal Processor)나 범용마이크로프로세서 상에서 동작하는 재구성 가능한 소프트웨어를 통해 제공되는 다주파수대역 무선을 지원한다.

인지무선은 SDR의 소프트웨어무선 플랫폼 상에서 구현되며, 통신환경을 인지하고 적응적으로 무선을 자동재구성할 수 있는 인지능력을 가진 지능형 무선이다[20~22]. 또한, 인지무선은 통신시스템의 많은 특성들을 인지기능을 이용하여 향상시킬 수 있는 SDR보다는 더

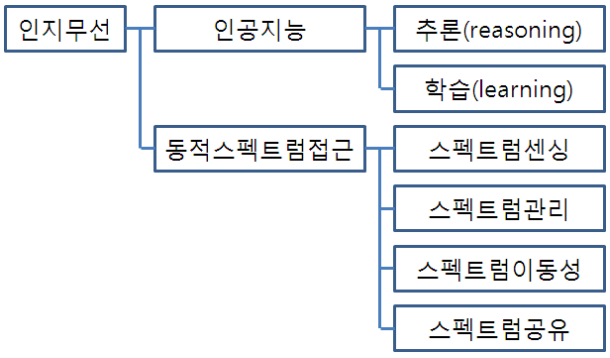

그림 1. 인지무선의 특징
Fig. 1. Properties of cognitive radio.

넓은 개념의 기술이다. 전통적인 무선 기술과 비교하여 인지무선은 인공지능 기능과 동적인 스펙트럼 접근(Dynamic Spectrum Accessing) 응용과 같은 특별한 특징을 가진다. 그림 1은 인지무선의 이러한 특징을 보여준다.

인지무선을 위한 표준화는 크게 IEEE 802.22와 Ecma-International의 개인/휴대기기를 표준의 두 가지가 있다. 특히, 이들 표준들은 그림 2에서 보여주는 바와 같이 하부구조를 기반으로 하는 네트워크(Infra Structure Based)와 하부구조가 필요없는 네트워크(Infrastructureless Structure)로 나뉠 수 있다. 하부구조 기반의 네트워크 표준을 위해 IEEE 802.22는 광대역 무선 인터넷 서비스에 인지무선 기술을 적용하여 54~862 MHz 사이의 TV 주파수 대역에서 WRAN서비스를 제공하기 위한 표준을 선보였다[5]. 하부구조 기반 네트워크와 하부구조가 필요없는 네트워크의 결합형인 혼합형 네트워크를 위하여 ECMA-International은 개인/휴대기기들을 위한 인지무선 표준을 발표하였다[6~7]. IEEE 802.22 표준은 고정형 기기를 이용하여 도시 외각 지역에서의 서비스를 제공하는 반면에, Ecma-International 산업표준의 경우 고정형 기기와 개인/휴대기기의 혼합형 네트워크를 통해 홈 네트워크를 위한 서비스를 제공하는데 그 목적이 있다.

2009년 2월 FCC는 TV 유휴주파수 기기관련법안을 제정하였다. 이 법안에는 주로 유휴주파수 기기와 관련된 일반적인 기술규정과 간섭현상을 방지하기 위한 기술조건, 기존 서비스 이용자를 간섭으로부터 보호하기 위한 규제 사항, 유휴주파수의 데이터베이스(Database)에 대한 규정 등을 포함한다. FCC는 이 법안에서 인지무선을 위한 고정형과 개인/휴대기기의 두 가지 형태의 기기를 정의 하고 있다. 인지무선 기기들은 위치정보를 수집하는 기능과 인가된 데이터베이스로부터 이용 가능

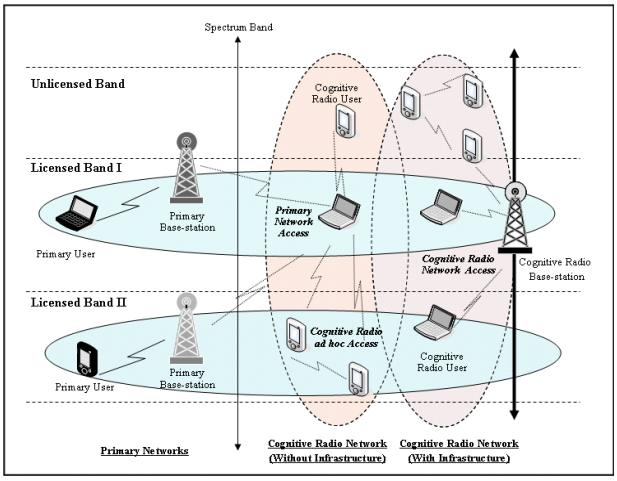

그림 2. 인지무선네트워크 구조 [18]
Fig. 2. Cognitive radio network architecture [18].

한 채널 검색 기능, 그리고 스펙트럼 센싱(Spectrum Sensing) 기능 등을 기본요구 사항으로 명시하고 있다. 특히, 고정형 기기는 3, 4, 37번을 제외한 채널 2~51번을 사용할 수 있으며, 개인/휴대기기는 Radio astronomy와 Wireless telemetry service가 이용 중인 채널 37번을 제외한 채널 21~51번을 사용할 수 있다. 고정형 기기의 최대 송신 출력은 4W EIRP이며 개인/휴대기기는 100W EIRP이다[6]. 단, 고정형 기기의 경우 서비스 인접 채널에서 사용이 불가능한 반면 개인/휴대기기의 경우 40W EIRP 이하의 송신 출력으로 서비스 인접채널에서도 사용이 가능하다. 개인/휴대기기의 사용은 두 가지 모드로 구성된다. 모드1은 주/종속 네트워크에서 종속 역할의 기기를 위한 모드로서 스펙트럼 센싱의 기능을 요구하며, 데이터베이스에 접속이 가능한 고정형 기기의 제어를 받거나 모드 2로 동작하는 개인/휴대기기의 제어를 받아 동작한다. 모드 2는 주/종속 네트워크에서의 주기기 또는 동등 계층 네트워크에서의 동등 계층 기기를 위한 모드로서, 독립적인 데이터베이스를 통해 스스로 사용가능한 채널을 결정하는 기능을 가진 모드이며, 이러한 개인/휴대기기의 사용은 별도의 채널 사용 데이터베이스의 등록을 필요로 하지 않는다.

Ⅲ. 인지무선네트워크 보안 위협

그림 3은 인지무선의 상황인지라는 새로운 개념 도입으로 파생되는 인지무선네트워크의 잠재적인 내부 및 외부 공격들에 대한 개념적인 개요도를 보여준다[7, 9, 19].

인지무선네트워크는 다른 네트워크와는 다른 인지무선네트워크에 국한된 다음과 같은 기본적인 공격속성들

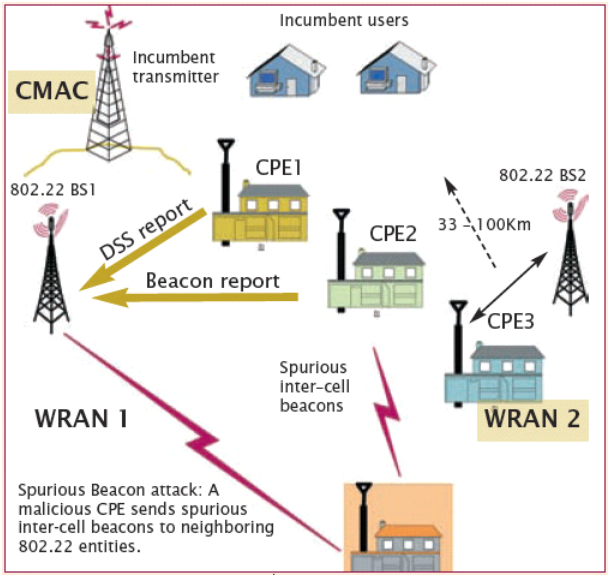

그림 3. 인지무선네트워크의 보안 위협 요소 [19]
Fig. 3. Security threats over CRNs [19].

을 가지고 있다. 이러한 인지무선네트워크만이 가지고 있는 속성들을 분석하고 다른 네트워크 공격 속성들과의 차이점을 분석함으로서 인지무선네트워크의 잠재적인 내부 및 외부 공격에 대한 예측을 수행할 수 있다[15~17].

- 공격자는 잠재적으로 인지무선네트워크에 접근하기 어렵고 일단 공격권 획득 시 공격이 오래 지속되는 특성을 가짐(인지무선에서는 현재 네트워크 사용 지 역을 중심으로 수집되고 교환된 네트워크 환경 정보가 향후 네트워크 환경에 미칠 영향을 구축하는데 이용됨)
- 간단한 스펙트럼 조작(신호의 생성)을 통하여 네트워크 성능과 속성에 지대한 영향을 미칠 수 있는 가능성이 있음
- 특히, 인지무선네트워크는 비면허 대역(Unlicensed band)에 할당되어 있는 주파수 대역 중 그 활용도가 낮거나, 시/공간적으로 사용되지 않는 유휴자원을 찾아 적응적이고 합리적으로 이용하는 기술임. 이러한 비면허 대역의 사용에 있어서 해당 대역에 이용권한(License)을 가지고 있는 주사용자로 사칭하는 공격은 네트워크 전체에 치명적인 영향을 미칠 수 있음

Ⅳ. 회전자 기반 적응형 보안프레임워크

본 장에서는 이전 장들에서 파악된 인지무선네트워크의 특성과 다양한 보안 위협에 대한 문제점을 해결할 수 있는 회전자(Carousel)기반의 보안프레임워크를 제안한다.

가. 적응형 보안 프레임워크

인지무선시스템에서는 기밀성과 프라이버시 기법들이 데이터 뿐 만 아니라 민감한 스펙트럼 소유 정보와 BS가 CPE들의 작업을 구성하는데 이용되는 스펙트럼 관리 정보들에 대해서도 보호되어야 한다. 특히, FCC가 제정한 TV 유휴주파수 법안에서 제시된 기기간 간섭현상을 방지하기 위한 기술 조건으로서 제시된 인지무선 기기들의 위치정보를 활용한 기법을 통해 다양한 보안 관련 문제에 대한 해결책을 제시할 수 있어야 한다. 이를 위해 본 논문에서 제안한 회전자기반 적응형 보안프레임워크는 그림 4에서 보여준다. 본 논문에서 제안한 적응형 보안프레임워크는 위치정보를 기반으로한 회전자를 활용하여 IEEE 802 표준들의 기본적인 보안기법인 보안서브레이어1에 더하여 인지무선의 속성에 대한 보안기법을 위한 보안서브레이어2를 추가로 제시하는 형태를 고려한다. 이러한 적응형 보안프레임워크를 통하여 인지무선네트워크 시스템의 인지기능과 함께 비인지 기능에도 초점을 맞춘 두 개의 보안 서브레이어가 공존된 보안프레임워크를 구성한다.

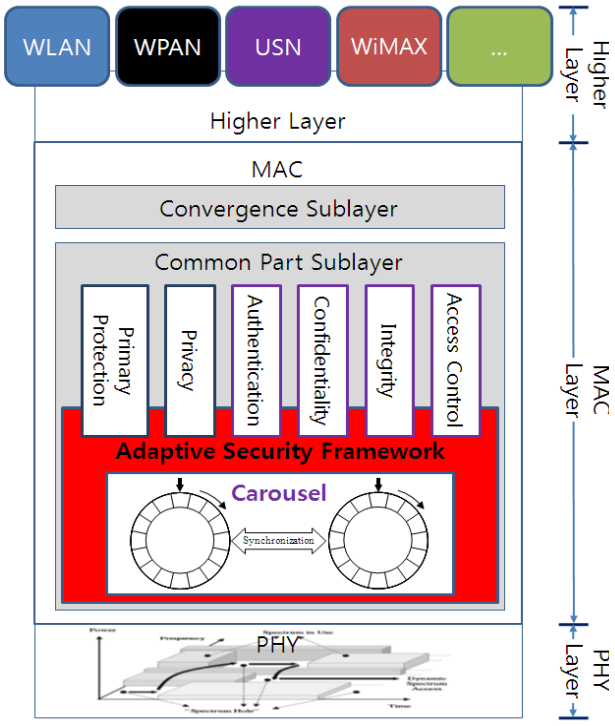

그림 4. 인지무선네트워크 적응형 보안프레임워크
Fig. 4. Adaptive security framework over CRN.

그림 4에서 보여준 바와 같이 본 논문에서 제안한 보안프레임워크는 인지무선네트워크의 기본적인 네트워크의 보안 요구사항을 만족하기 위해서 객체의 위치정보에 기반한 회전자(Carousel)를 프라이버시 및 다양한 보안 요구사항을 제공하기 위한 보안 기법들을 설계하기 위해 필요한 보안 기초(Security Credential)로 활용한다[16].

나. 위치정보 기반의 회전자

인지무선네트워크에서 위치정보는 객체들의 보안레벨을 결정하는데 있어서 아주 중요한 정보이다[16]. 이러한 이유는 FCC가 제정한 TV 유휴주파수 법안에서 제시된 기기간 간섭현상을 해결하기 위한 방안으로서 위치정보에 기반한 데이터베이스의 활용에 대한 권고에서도 확인할 수 있다.

이러한 요구사항을 반영하기 위해서 본 논문에서 제안한 적응형 보안프레임워크는 다양한 보안 기법을 위한 보안기초로서 환형큐(Circular Queue)형태의 위치정보에 기반한 회전자 자료구조를 이용한다. 회전자는 Kuroda등에 의해 제안되었고, 다양한 보안기법들의 보안기초로 활용되었다[16]. 그림 5는 통신 참여자간에 동기화된 회전자 구조를 보여준다.

환형큐 형태의 회전자의 각 셀은 개체의 위치정보 Loc와 난수 R이 결합된 정보를 단방향함수인 해쉬함수를 적용하여 $L=h(Loc, R)$로 초기화 한다. 보안기법을 활용하기 위한 참여자들은 보안기법을 수행하기 전에 회전자 동기화(Synchronization)를 먼저 수행해야 한다. 회전자 동기화는 각 참여자들 간에 동일한 정보의 공유를 보장한다. 회전자는 보안기법이 수행될 때마다 한번씩 미리 정해진 방향으로 회전한다. 보안기법들은 동기화된 회전자로부터 생성된 키를 이용하여 다양한 보안 서비스를 제공한다.

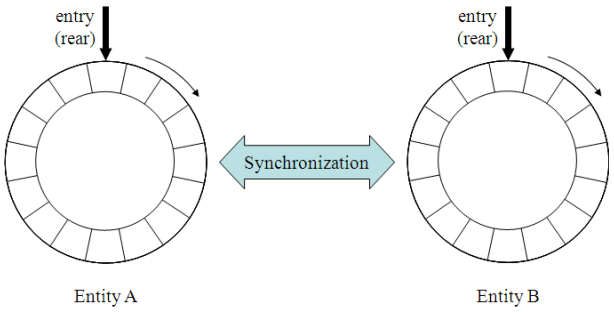

그림 5. 회전자 구조
Fig. 5. Carousel Structure.

다. 보안기법들을 위한 요구사항

일반적인 네트워크와 인지무선네트워크 보안기법들을 위한 기본적인 요구사항은 유효성과 인증, 권한인증, 신원확인, 무결성, 기밀성, 프라이버시를 통해서 제공된다. 특히, 이러한 보안 요구사항을 제공하기 위해서 본 논문에서 제안한 보안프레임워크 상의 다양한 보안기법들은 위치정보에 기반한 회전자를 보안 기초로 활용한다. 본 절에서는 이들 보안 요구사항에 대한 개요와 이를 제공하기 위한 보안기법들의 요구사항들을 인지무선네트워크 관점에서 살펴본다[15-17].

(1) 유효성

유효성은 어떠한 네트워크에서나 중요하게 제시되어야 할 속성이다. 네트워크가 특별한 서비스나 보안 기법 때문에 신뢰를 잃는다면 최종사용자들이나 인지무선네트워크 이용자들은 그 네트워크를 더 이상 이용하지 않을 것이다. 인지무선네트워크에서 유효성은 BS(Base Station)가 유효한 스펙트럼을 적절히 센싱 할 수 있고 그 스펙트럼을 유효한 CPE(Customer Premise Equipment)들에게 제공할 수 있는 능력을 말한다. 즉, BS가 회전자 보안기초를 활용한 다음과 같은 내장 보안 기법(Built-in Security Mechanism)을 제공할 수 있음을 말한다.

- 네트워크 주사용자와 부사용자들에게 스펙트럼의 유효성
- BS나 CPE, 그리고 IEEE 802.22.1 비컨을 생성하는데 사용되는 장치를 포함하는 다양한 장치들에 제시된 임의의 DoS(Denial of Service)형태 공격들에 대한 해결책

(2) 인증

인증은 송신자나 수신자, 즉, 통신에 참여하는 당사자들이 그들이 주장하는 존재임을 보증하는 기능을 제공한다. 인지무선네트워크의 인증에서는 스펙트럼의 유효한 주사용자와 부사용자들 간의 구별 기능이 추가로 제시될 수 있어야 한다. 이를 위해서 인지무선네트워크 장치들은 회전자를 보안기초로 활용하여 다음 기능들을 제공할 수 있어야 한다.

- TV 시그널과 무선 마이크 비컨을 확인 기능
- 유효 스펙트럼을 갈취하기 위한 중간자 공격과 비슷한 형태의 공격에 대한 해결책
- 스푸핑 공격과 비슷한 형태의 공격에 대한 해결책

- 지리정보를 인증할 수 있는 기능
- 이웃하는 인지무선네트워크 시스템들의 공존 정보를 인증할 수 있는 기능
- 다른 CPE들로부터의 가짜 트래픽 전송을 탐지하고 레포트 할 수 있는 기능

(3) 권한인증

다양한 네트워크 구성요소들은 다양한 권한 레벨을 갖는다. 예를 들어 BS는 네트워크로부터 CPE의 간섭을 제거할 수 있는 권한을 가질 수 있다. 또한, BS는 스펙트럼의 유효성을 센싱하고 유효한 스펙트럼에 대한 사용을 판단하며, 그러한 판단에 대한 실행을 CPE에게 제시하는 권한을 가진다. 이를 위하여 인지무선네트워크는 회전자를 보안기초로 활용한 다음과 같은 주요 기능들을 제공할 수 있어야 한다.

- 인증된 BS만이 스펙트럼 메니저를 위한 환경설정을 할 수 있고 인증된 CPE만이 스펙트럼 자동화를 위한 환경설정을 할 수 있는 기능
- 환경설정 정보들이 식별될 수 있고 보호될 수 있는 기능
- BS는 주사용자에 대한 간섭을 초래한 CPE를 발견했을 때 네트워크로부터 그 CPE를 제거할 수 있는 기능

(4) 신원확인

신원확인은 통신 참여자들이 알려진 주사용자나 부사용자임을 확증하는 인증과 상호작용한다. 이를 위해 인지무선네트워크는 회전자를 보안기초로 활용한 다음과 같은 기능을 제공할 수 있어야 한다.

- 데이터를 전송하거나 수신하는 BS나 CPE 장치를 식별할 수 있는 기능
- 사용된 신원확인 기법이 공모나 비슷한 형태의 공격을 통한 타협이 불가능하도록 하는 기능
- 이전에 전송된 유효한 식별자를 이용한 재전송형태의 공격에 대한 해결책

(5) 무결성

무결성은 네트워크를 통해 전송된 정보가 원래 목적지에 변경 없이 전송됨을 보증하는 기법이다. 이를 위해 무결성은 내용에 대한 쓰기 방지 기능을 제공한다. 무선네트워크 상에서 무결성을 제공하는 것은 전송되는 형태의 제어불가능성으로 인해서 특히 어렵다. 또한 데이터의 특정부분이 전송 도중에 변경되어야만 하는 문제는 어려움을 가중시킨다. 인지무선네트워크는 회전자를 보안기초로 활용한 다음 기능들을 제공할 수 있어야 한다.

- 공존을 위한 비컨과정(Co-existence Beaconing)의 위조에 대한 해결책
- 이전에 전송된 유효 데이터를 이용한 재전송 형태의 공격에 대한 해결책

(6) 기밀성/프라이버시

기밀성은 데이터에 대한 읽기보호와 함께 쓰기보호를 제공하기 위해 무결성과 밀접하게 협력해야 한다. 기밀성은 링크계층이나 더 높은 계층에서 동작할 수 있는 암호화를 통해 일반적으로 수행된다. 특히, 무선장치가 쉐도윙(Shadowing)과 신호감쇄현상(Fading), 그리고 의도적이지 않은 간섭과 같은 영향 때문에 전송 오류에 더 민감함을 고려할 수 있어야 한다. 이 민감성이 암호화된 복잡한 데이터를 엉망으로 만들 수 있고 여러 번의 재전송을 발생시킴으로서 해당 대역폭의 낭비를 초래할 수 있다. 인지무선네트워크에서는 부사용자에 의한 스펙트럼의 기회적 이용과 스펙트럼의 사용이 보증되지 못하는 특성 때문에 특히 이 민감성은 중요한 문제이다. 그러므로 인지무선네트워크는 회전자를 보안기초로 활용한 다음 기능들을 제공할 수 있어야 한다.

- 견고한 암호기법
- 스펙트럼 경쟁자나 해커들의 도청으로부터 WRAN 이용자의 스펙트럼 유효성을 보증하기 위한 기법

V. 결론 및 향후 연구 방향

방송 및 통신 시스템의 급속한 성장과 더불어 주파수 자원의 고갈 문제가 세계적으로 중요하게 인식됨에 따라 스펙트럼 사용 효율을 높이고 새로운 서비스 도입을 용이하게 하기 위해 TV 유휴 주파수를 대상으로 주파수 공유기술인 인지무선 기술에 대한 관심이 증대되고 있다. 하지만, 인지무선의 상용화에 있어서 보안은 가장 큰 걸림돌로 작용하고 있고, 다양한 융복합 네트워크를 위한 보안은 아주 중요한 문제이다. 이러한 문제를 해결하기 위해서 본 논문에서는 인지무선네트워크를 위한 회전자기반 적응형 보안프레임워크를 설계하였다. 이러한 적응형 보안프레임워크를 설계하기 위해서 인지무선

네트워크의 보안 위협에 대해 분석하고 이를 토대로 보안 요구사항을 도출한 후 이러한 속성을 제공할 수 있는 회전자기반 적응형 보안프레임워크의 기본구조를 제안하였다.

향후 본 연구에서 제안된 적응형 보안프레임워크를 위한 회전자기반의 구체적인 보안 기법들에 대한 설계가 추가로 제시되어야 하고, 이러한 보안 기법들은 본 논문에서 제시된 보안 요구사항을 만족하기 위한 형태로 제안되어야 할 것이다.

참 고 문 헌

[1] B. Fette, *Cognitive Radio Technology-second edition*, Academic Press, 2009.
[2] J. Mitola, "Cognitive Radio for Flexible Mobile Multimedia Communications," *Mobile Network and Applications,* Vol. 6, No. 5, pp.435-441, 2001.
[3] I. F. AKyildiz, W. Y. Lee, M. C. Vuran and S. Mohanty, "A survey on Spectrum Management in Cognitive Radio Networks," *IEEE Communications Magazine*, Vol. 46, pp. 40-48, Apr. 2008.
[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] Ecma-International, MAC and PHY for operation in TV white space, *standard ECMA-392,* Dec. 2009.
[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, 2008.
[9] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," *CrownCom 2008*, pp. 1-8, 2008.
[10] R. Chen, J. Park, "Ensuring trustworth spectrum sensing in cognitive radio networks," *IEEE Workshop on Networking Technologies for SDR 2006*, pp. 110-119, 2006.
[11] 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, 2007.
[12] J. Mitola, "Cognitive INFOSEC," *IEEE wireless and microwave technology symposium 2003*, Vol. 2, pp. 1051-1054, 2003.
[13] Y. Yuan, P, Bahl, R. Chandra, P. A. Chou, J. I. Ferrell, T. Moscibroda, S. Narlanka, and Y. Wu, "KNOWS: Cognitive Networking Over White Spaces," *Proceedings of IEEE DySPAN*, 2007.
[14] J. L. Burbank, "Security in cognitive radio networks : the required evolution in approaches to wireless network security," *Proc. of CrownCom 2008*, pp. 1-7, 2008.
[15] 김현성, "인지무선네트워크를 위한 보안 표준화 현황-IEEE 802.22 WRAN을 중심으로", *정보보호학회지*, Vol, No. 5, pp. 65-69, 2009.
[16] H. S. Kim, "Location-based authentication protocol for first cognitive radio networking standard," *Journal of Network and Computer Applications*, Vol. 34, pp. 1160-1167, 2011.
[17] 김현성, "인지무선네트워크를 위한 보안프레임워크 설계," *2012년도 융합/스마트/클라우드 컴퓨팅 학술대회*, pp. 23-27, 2012.
[18] BWN Lab. GeorgiaTech, http://www.ece.gatech.edu/research/labs/bwn.
[19] ARIAS VirginiaTech, http://www.arias.ece.vt.edu/.
[20] 백준호, 이종환, 오형주, 황승훈, "인지무선환경에서 스팩트럼 센싱을 위한 에너지 검출기의 성능개선:시간지연을 이용한 확인과정," *전자공학회논문지-TC*, Vol. 45, No. 1, pp. 72-77, 2008.
[21] 이소영, 이재진, 김진영, "인지무선 시스템을 위한 거리기반 가중치가 적용된 협력 스펙트럼 센싱," *전자공학회논문지-TC*, Vol. 47, No. 7, pp. 45-50, 2010.
[22] 박창현, 송명선, "인지 무선 시스템을 위한 채널 집한 관리기의 개발 및 성능 분석," *전자공학회논문지-CI,* Vol. 45, No. 5, pp. 8-14, 2008.
[22] 강해린, 유혜인, 김낙명, "Relay Station 시스템의 Throughput 향상을 위한 Auction 기반 계층적 링크 할당 알고리듬," *전자공학회논문지-TC*, Vol. 46, No. 6, pp. 11-18, 2009.

저 자 소 개

김 현 성(정회원)

1996년 경일대학교 컴퓨터공학과 공학사 졸업.
1998년 경북대학교 컴퓨터공학과 공학석사 졸업.
2002년 경북대학교 컴퓨터공학과 공학박사 졸업.

2002년～2011년 경일대학교 컴퓨터공학과 교수
2012년～현재 경일대학교 사이버보안학과 교수
2012년～현재 경일대학교 학술정보원 원장
2010년～현재 경일대학교 정보융합보안연구소 소장
2002년～현재 한국정보보호학회 논문지 편집위원
2009년 더블린시립대학 컴퓨팅학과 방문교수
<주관심분야 : 인지무선네트워크 보안, 네트워크 보안, 암호 프로토콜, 암호구현, 정보보호>