인지 무선통신 네트워크의 보안 문제 연구

문상국

목원대학교 전자공학과

A Study of Security Issues of Cognitive Radio Network

Sangook Moon

Mokwon University, Department of Electronic Engineering

E-mail : smoon@mokwon.ac.kr

요 약

인지 무선통신 네트워크는 현재까지 폭넓은 커뮤니티 중심의 오픈소스의 형식으로 연구되고 있으며, 프로그램이 가능한 플랫폼 기반의 연구 성과라는 생각에 대한 잠재적인 기대치는 매우 높다. 하지만, 이러한 무선 플랫폼의 확산과 지원하는 소프트웨어의 오픈소스적인 특성 또한 그 위험성이 매우 높다고 할 수 있다. 사용자간 (peer-to-peer) 소프트웨어가 한 때 오용되었던 것처럼, 개별 프로그래머가 저렴하고 쉽게 널리 보급할 수 있는 인지 무선통신 플랫폼을 개발하여 대중적으로 악용할 수 있는 가능성이 매우 큰 것이다. 이렇게 되면 차세대 무선 통신의 새로운 연구로 얻을 수 있는 이익보다 인지 무선통신 디바이스를 재프로그래밍하여 통신법규를 어기거나 적대적으로 악용할 수 있는 부정적인 영향이 오히려 심각해 질 수 있다. 본 고에서는 이러한 인지 무선통신 네트워크의 보안 문제를 살펴보고, 효과적인 대체방안에 대하여 분석하였다.

ABSTRACT

The cognitive radio (CR) network has been studied in the form of open source by vast number of communities, and the potential expectation is very high since the CR is based on reprogrammable platform. However, this characteristics of open-source software take high risk as well. As the peer-to-peer software has been abused, so high is the chance that the CR network can be abused public wide. Consequently, the benefit from the study of next-generation wireless network can be at risk because of the negative impact of violation of communication law or abusing the CR. In this contribution, we analyze the issues and the problems of the CR and discuss an efficient measure against security attacks.

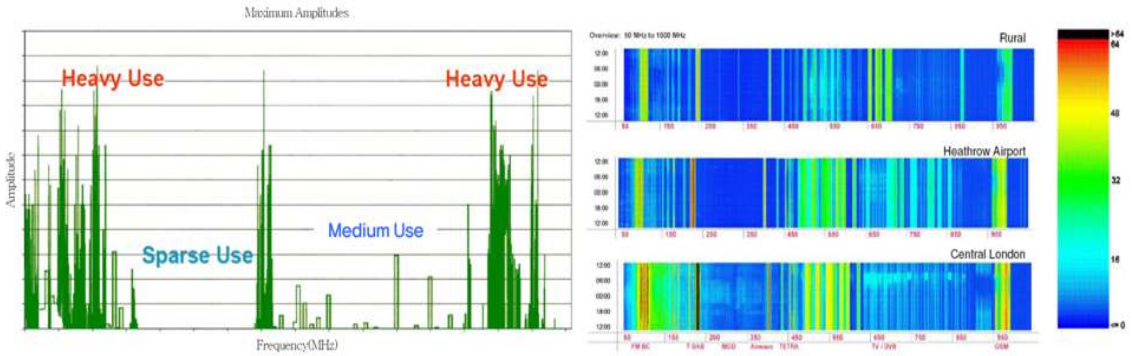
키워드

인지 무선통신, 보안, cognitive radio

Ⅰ. 서 론

유비쿼터스 시대의 도래와 더불어, 무선 통신 단말기기들은 기하급수적으로 증가하게 되었고, 이에 따른 주파수자원의 부족현상이 심각하게 대두되고 있다. 따라서 최근 무선통신에서는 무선 채널을 고정적으로 할당받아 데이터를 전송하던 기존 방식에서 벗어나, 무선 주파수 대역의 사용 현황을 스스로 인지하여 빈 채널을 찾고 해당 채널에서 데이터 통신을 수행하는 인지형 무선통신 (Cognitive Radio; CR)의 개념이 소개되었다 [1].

증가하는 무선 통신에 대해 사용자의 요구를 만족시키기 위해서는 충분한 주파수 대역의 확보가 필수적이다. 하지만 통신에 활용 가능한 무선 주파수 대역은 한정적일 뿐 아니라, 대부분이 기존의 무선 통신 서비스 (선순위 사용자; primary user)에 이미 할당되어 있기 때문에 추가적인 통신 서비스를 위한 주파수 대역의 확보가 매우 어려운 실정이다. 그러나 실제로 미국의 FCC (federal communications commission) 등 연구단체에서 선순위 사용자에게 분배된 주파수의 이용효율을 측정해 본 결과, 주파수 대역의 이용효율



(a) 미국 스펙트럼 이용현황 측정 (b) 영국 지방별 주파수 사용 현황

그림 1. 미국과 영국의 주파수 사용 현황.

이 매우 떨어지며, 특히 도시 외곽이나 인구밀도가 낮은 지역에서 두드러진 경향을 보인다는 사실이 보고된 바 있다. 미국에서의 주파수 이용 효율은 평균적으로 30% 이하로 나타나고 있고 (그림 1-(a)) [2], 이는 영국도 크게 다르지 않다. 그림 1-(b)는 영국의 인구복잡도를 기준으로 한 세 지역에서 측정한 주파수 사용현황을 보인 것이다. 특히 그림 윗부분 전원 지방에서 주파수 대역 중 많은 부분이 낭비되는 것을 볼 수 있다 [3].

이와 같이 이용되지 않고 있는 주파수 자원이 많지만 선순위 사용자가 해당 주파수 대역을 선점하고 있기 때문에 해당 대역을 새로운 무선통신 서비스에 재할당하기란 매우 어렵다. CR 기술은 이러한 주파수 자원을 효율적으로 이용하기 위한 기술로, 소프트웨어 정의 무선 통신 기술 (SDR; Software Defined Radio)을 기반으로 스펙트럼 센싱 기능을 활용하여 가용한 주파수를 인식하고 선정하여 통신하는 기본적인 기능과 여러 가지 환경 파라미터를 지속적으로 업데이트 하는 인지 알고리듬이 합쳐진 미래 무선통신의 핵심 기술이다. 이 기술을 활용하는 CR 네트워크가 실현되기 위해서 효과적인 채널 센싱과 채널 변경 기법의 연구가 미국을 중심으로 진행되고 있으며, 한국에도 2006년 경 소개되어 연구의 필요성을 깨닫기 시작하였다.

II. 소프트웨어 기반의 CR 검증과 보안 측정 체계

CR에서의 임베디드 소프트웨어 검증방식은 시스템 전반에 걸쳐 테스팅을 수행하는 기존 소프트웨어 시스템의 검증방식과는 기본적으로 다르다. 프로그램 코드의 모든 경우를 검증하는 대신, CR이 네트워크의 통제 정책 (regulation policy)에 명시된 조항을 따르는 것에 대한 보장의 여부가 검증의 핵심이다. 기존의 기능 검증이 디버깅에 의존하는 것에 비해, CR의 검증은 모든 CR 디바이스가 통제 주체 (regulation entity)로부터 규정된 정책을 위반하지 않으면 되는 것이다.

송신 파워가 반드시 송신 주파수에 관계된 함수값 미만이어야 한다는 정책을 따르는 규칙을 예로 들어보자. 우리는 CR을 제어하는 소프트웨어가 이 규칙을 위반하지 않는 본질적인 방안을 강구해야 한다. 본 과제에서 우리가 제안하는 방법은 본질적으로 다음과 같은 해법을 제시할 수 있다. “프로그램 코드의 송신 파워의 산출계산과 관련된 모든 코드들의 가능한 모든 경우를 고려해도, 송신 파워가 허용량보다 항상 작도록 모든 경우를 보장”하면 된다. 이러한 방식은 기존 분석방식에서 제거할 수 없었던 세부적인 잠재적인 악성 코드를 제거할 수 있게 한다. 또한, 다소 과감한 가지치기를 통하여 대상 프로그램 자체의 기능이 상실되지 않도록 주의해야 할 것이다. 이러한 새로운 검증을 위하여 소프트웨어적인 측면에서는 두 가지 개념을 제안한다.

가. 새로운 집단지성 (Swarm-Intelligence) 기반의 프로그램 추상화

첫 번째로 제안하는 것은, 새로운 집단지성 방식에 의한 프로그램의 추상화이다. 즉, Ant Colony Optimization (ACO) [4]를 응용한 추상화 기술을 응용하여 프로그램 코드에서 가장 먼저 조사하여야 된다고 추정되는 부분을 식별하도록 할 것이다. ACO는 실제 개미의 습성을 에뮬레이션하는 가상 개미들의 협력과 적응방식을 통하여 최적의 해답과 문제점을 찾는 집단지성 기반의 인지 알고리듬이다. ACO의 원래 용도인 테스트 데이터를 생성하는 것과는 달리, 본 과제에서는 소프트웨어 검증을 위한 path level 추상화 작업을 단순화 하기 위하여 ACO를 수정하고 확장한다. 기본적인 개념은 다음과 같다. 검증해야 할 특성이 주어졌을 때, 인공 개미들은 프로그램의 흐름을 따라 이동하게 되는데 이동 중

특성을 위반하면서 보내지는 상태공간 (state space)이 발견될 수 있다. 그 개미들에 의하여 추적된 자취는 초기 프로그램 under-approximation으로 사용할 수 있고, 다수의 프로그램 코드로 실험한 결과 상당 부분을 감소시킬 수 있었다.

나. 프로그램 변수의 취약성 평가를 위한 코드 레벨의 측정체계 (metric)

시스템 레벨에 초점을 맞추는 전통적인 안전성 측정체계와는 달리, 우리는 프로그램 디자인 단계에서 가능한 빨리 취약한 코드를 식별하기 위해 선취적이고 비용대비 효율적인 방식을 제안한다. 만약 시스템 레벨이 아닌 코드 레벨로 초점을 맞추면 안전성에 위협이 될 수 있는 오류를 찾아내고 고치는 데 대한 노력을 줄일 수 있을 것이다. 이러한 개념은 보안 취약점을 소프트웨어가 자리잡기 전에 제거함으로써, 소프트웨어 보안강화도를 높이고, 악의적인 공격을 어렵게 하는 데 그 의미가 있다.

취약한 프로그램 변수는 가장 대표적인 공격 목표가 된다. 그림 2의 코드를 보면, 스칼라 변수인 range, count와 어레이변수 deststr, nums는 모두 잠재적인 공격 대상이다. 일반적인 공격 형태는 두 가지의 시나리오를 가지고 있다. 첫 번째, deststr과 같이 변수 자체가 직접적인 공격 대상인 경우이다. la 행의 strcpy 함수가 배열에 대하여 자동적으로 범위 처리를 하지 않기 때문에, 입력 버퍼 inputstr의 길이가 목적 버퍼의 deststr에 할당된 크기를 넘는다면 deststr 변수는 오버플로우 된다. 두 번째, 변수들은 간접적으로 range나 count 같은 다른 목표에 대한 공격에 영향을 받을 수 있다. 지역변수 스택의 일반적인 구조에 따르면, 두 개의 스칼라 변수의 값들은 이웃하는 어레이 변수 deststr의 오버플로우에 의해 간접적으로 겹쳐써지는 (overwritten) 것이 가능하다. 하지만, 모든 경우에 있어서 변수값의 변경이 프로그램의 보안 문제를 야기하는 것은 아니다. 오히려 count 변수와 비교하면 range가 안전성 측면에 있어서 더 중요하다. 왜냐하면 유효성 검증이 없다면, 행 lb의 부적절한 range의 값은 또한 배열변수 nums에 대한 오버플로우를 일으키기 때문이다. 반대로 count 값을 악의적으로 변경해도 range가 미치는 영향에 비하면 미미하다.

위의 예로 알 수 있는 것은 변수 레벨에서의 안전성에 대한 위험도의 순위를 매김으로써 프로그램 코드 내의 취약한 부분을 찾는 데 활용할 수 있다는 것을 알 수 있다. 또한 알 수 있는 것은, 변수 레벨의 안전성 측정방법에서 얻을 수 있는 확신을 향상시키기 위하여 프로그램 구조의 포괄적인 분석은 물론 정확한 보안 공격 영향에 대한 모델링이 요구된다는 사실이다. 따라서, 부분적인 프로그램 행동을 기초로 한 기존 방식인 시뮬레이션을 기초로 하는 공격 모델은 코드 레벨 안전성 검증에 효율적이지 않을 것이다. 본 연구에서는 변수 레벨의 안전성 민감도를 계산하고 순위를 매기기 위해, 보안 특성을 통과하는 빈도와 그에 상응하는 보안 가중치를 동시에 고려한다. N개의 보안 특성 spi (i는 정수 | 1 <= i <= N)가 있다고 할 때, 각각의 spi는 보안 가중치 swi와 연관되어있다고 가정하자. 검증 후보 변수 v@l (l행의 변수 v)이 주어졌고, 이는 알고리듬의 첫 번째 단계 이후 Ns개의 안전한 집합 (보안 특성 spsi, 1 <= i <= Ns)과 Nv개의 취약한 집합 (보안 특성 spvi, 1 <= i <= Nv)으로 떨어진다고 가정하자. 단, 1 <= Ns, Nv <= N이고 Ns + Nv = N이다. 이제 l행의 변수 v의 보안 취약성은 다음과 같은 식으로 계산될 수 있다.

$$varSec[v@l] = (\sum_{v_1}^{v_{N_v}} sw_{vi} - \sum_{s_1}^{s_{N_s}} sw_{si})/N \qquad (1)$$

식 (1)에서 보이듯이, 변수의 보안 취약성은 그 변수가 공격당했을 때 전체적인 시스템의 안전성에 영향을 미치는 결합적인 안전성 손상에 의해 결정된다. 위 식은 공식화하여 모델 체크의 한 요소로 사용될 것이다. 건드리지 않는 보안 특성이 많을수록, 그 변수는 안전성에 둔감하다. 즉, 위반하는 보안 특성이 많을수록, 그 변수는 보안에 매우 위협적이다.

```
proc foo(char *inputstr){
        int range, count;
        char deststr[50];
      int nums[20];
      …
      range = 40;
 la:    strcpy(deststr, inputstr);
 lb:    for (int i = 1; i < range; i++) {
          nums[i] = fun1(nums[i-1]);
      }
      count+= fun2();
}
```

그림 2. 변수 공격에 대한 코드의 예

Ⅳ. 결 론

CR 기술은 향후 무선통신 전반에 걸쳐 적용될 것으로 예상된다. 미 국방성에서 수행하고 있는 XG 프로젝트는 군사용 장비의 CR 네트워크화에 대한 것인데, 군사용 장비의 경우 전쟁이

세계 어디서나 발생할 수 있고, 이 때 무선 통신 장비의 주파수가 고정되어 있다면 장비를 사용할 수가 없는 경우가 생기기 때문에 CR 기술을 이용하여 비어 있는 주파수를 이용하여 작전을 수행할 수 있기 때문이다. 또한 공공 안전 통신의 경우 재난이 발생한 경우에는 많은 주파수 대역이 필요하지만 평상시에는 최소한의 대역만 요구된다. 따라서 CR 기술을 지원하는 장비라면 평상시에는 public safty 대역을 사용하다가 재난 등의 위급 상황으로 우선 사용자가 사용하는 것을 감지하면 주파수를 놓아줌으로써 주파수의 이용 효율을 높일 수 있다. 이렇 듯 향후 CR 기술은 무선 통신 기술에 필수적으로 빠른 시일 내에 도입되어야 할 기술이며, 또한 CR은 그 인지능력의 특성상 보안에 취약할 수밖에 없기 때문에 이에 관한 보안 안전성 문제는 반드시 선행 연구가 수반되어야 한다.

참고문헌

[1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," IEEE J. Sel. Areas Commun., vol. 23, no. 2, pp. 201-220, Feb. 2005.

[2] 김창주, “Cognitive Radio 기술 동향,” 전자통신동향분석 제 21권 제 4호 2006년 8월.

[3] http://www.ofcom.org.uk/research/technology/research/emer_tech/cograd/

[4] http://iridia.ulb.ac.be/mdorigo/ACO/ACO.html.