디지털산업정보학회 논문지 제7권 제3호-2011년 9월

인지 라디오 네트워크의 안전한 분산 스펙트럼 센싱을 위한 트랜잭션 서명기법*

김 태 경**

Transaction Signing-based Authentication Scheme for Secure Distributed Spectrum Sensing in Cognitive Radio Networks

Kim, Tae Kyung

〈Abstract〉

Cognitive radio (CR) technology is to maximize the spectrum utilization by allocating the unused spectrums to the unlicensed users. This technology enables the sharing of channels among secondary (unlicensed) and primary (licensed) users on a non-interference basis after sensing the vacant channel and as a result, it is possible to harness wireless frequency more efficiently. To enhance the accuracy of sensing, RDSS was suggested. It is a fusion mechanism based on the reputation of sensing nodes and WSPRT (weighted sequential probability ratio test). However, in RDSS, the execution number of WSPRT could increase according to the order of inputted sensing values, and the fast defense against the forged values is difficult. In this paper, we propose a transaction signing-based authentication scheme for secure distributed spectrum sensing to response the forged values. The validity of proposed scheme is provided by BAN logic.

Key Words : Cognitive Radio Network, Authentication scheme, Distributed Spectrum Sensing

Ⅰ. 서론

최근 들어 방송 및 통신 시스템의 급속한 성장과 더불어 새로운 차세대 무선 플랫폼 및 시스템 하드웨어 기술이 눈부시게 발전하고 있다. 그러나 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. 이러한 주파수 자원은 국가적으로 차세대 통신 시스템을 통해 선진 기술 시장을 창출해야하는 각국의 무형 자산으로 인식되고 있으며, 한정된 주파수 자원을 보다 효율적으로 사용할 수 있는 기술을 개발하는 것이 미래 통신 기술의 성공을 좌우하는 핵심이라 인식되고 있다[1-2].

일반적으로 무선 네트워크에서는 특정 대역에서의 주파수가 우선 사용자를 위주로 사용되기 때문에 시간적, 공간적으로 유휴 주파수가 발생할 수 있다. 그러나 이는

* 서울신학대학교 학술연구비 지원에 의한 논문임.
** 서울신학대학교 교양학부 교수

특정 사용자에게 고정적으로 할당되어있어 다른 목적으로 재사용이 불가능하다는 한계점을 가지고 있었다. 인지 라디오 (Cognitive Radio: CR)란 이러한 문제를 해결하기 위해 SDR (Software Defined Radio) 기술의 개념을 도입하여 지능화된 통신 단말기 및 네트워크를 통해 동적으로 변화하는 주파수 자원을 인지하고, 유휴 주파수를 재사용함으로써 주파수 자원의 효율성을 증대 시키는 기술이다[3-4].

이러한 인지 라디오 기술에서의 핵심 기술은 주사용자의 채널 사용 여부를 정확히 인지하는 채널 센싱 기능이라 할 수 있다. 그러나 무선 통신 환경의 다양한 영향 요소들(페이딩, 쉐도우잉 등)로 인해 한 노드의 센싱 결과는 그 정확성이 떨어질 수 있다. 따라서 센싱정확도를 보다 높이기 위해 최근에는 여러 노드가 동시에 센싱하여 그 결과를 하나로 종합하여 판단하는 분산 스펙트럼 센싱 (distributed spectrum sensing, DSS) 기술이 활발히 연구되고 있다.

그러나 분산 메커니즘들의 가장 큰 보안 취약점은 참여 노드의 공격 가능성이라 할 수 있다[5-6]. 이로 인해 위조된 센싱 결과는 최종 종합 결과의 오류를 야기할 수 있다. 최악의 경우, 한 노드의 위조된 센싱 결과를 가지고 주사용자의 채널 사용 보호와 채널 사용의 효율성 극대화라는 인지 라디오 기술의 목표를 와해시킬 수 있다. 이러한 취약점을 보완하고자 최근 안전한 분산 스펙트럼 기술들이 연구되고 있다[7-9].

대표적인 안전한 분산 스펙트럼 메커니즘인 RDSS[7]는 주변 센싱노드들로부터 센싱값을 모아 최종 결정을 내리는데, WSPRT(weighted sequential probability ratio test) 가설 검정 테스트를 사용하였다. 일반적인 SPRT와 달리 센싱값의 정확성에 따라 평판값(reputation)을 조정하여 가중치(weight)로 사용함으로써 변조된 센싱값에 의한 공격의 영향을 줄이고자 하였다. 그러나 해당 퓨전 메커니즘은 입력되는 센싱값의 순서에 따라 많은 WSPRT 반복 횟수를 요구할 수 있고, 소수의 위조된 센싱값으로 최종의 이상결과를 유도해 낼 수 있다. 또한 공격 노드로부터의 영향을 줄이기 위해 상당한 시간이 요구될 수도 있다[10].

본 논문에서는 이러한 RDSS의 단점을 보완하여 위조된 센싱값에 안정적으로 대응하기 위한 트랜잭션 서명기법을 제안한다. 제안된 기법은 RDSS가 평판값에 따라 WSPRT를 수행하되, 변조된 센싱값에 의한 공격의 영향을 방지하여 안정적인 기능을 수행하도록 하였다. 본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 관련연구와 RDSS에 대해 설명하며, 3장에서는 본 논문에서 제안하는 트랜잭션 서명기법에 대해 기술하였다. 4장에서는 제안한 기법에 대한 성능평가를 하였으며, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 스펙트럼 센싱 메커니즘

IEEE 802.22 네트워크는 하나의 기지국(BS)을 통해 중앙 집중적 MAC(media access control) 프로토콜을 사용하여 사용자의 채널을 관리하며 서비스를 제공한다. IEEE 802.22 네트워크는 사용 가능한 각 채널들에 대해 모든 노드가 전송을 중지하는 침묵기간(quiet period)을 탐지하기 위해 센싱을 수행한다[11]. 기지국은 노드들의 센싱결과를 수집하여 최종 센싱 결과를 도출하고 이를 바탕으로 채널 사용을 위해 스케줄링한다. 사용 가능한 센싱 방법으로는 에너지 검출 기법과 특성 검출 기법이 있다[12].

분산 스펙트럼 센싱(DSS) 메커니즘의 가장 중요한 문제는 수집한 결과를 가지고 어떻게 최종결과를 얻는가 하는 퓨전 기술이라고 할 수 있다. 가장 기본적인 방법으

로는 OR, AND, Majority 퓨전 방법이 있다. 전체 센싱 노드의 수를 N 이라고 했을 때, 시그널이 존재한다고 판정한 노드의 수가 k 이상인 경우 최종 시그널이 있다라고 결정하는 방법이다. 각 방법의 k 값은 1, N, 그리고 ceil(N/2)이다. 그러나 이러한 방법은 미탐지율과 센싱정확도의 두 성능 측도에 모두 좋은 성능을 나타내는 것은 아니다[7]. 이에 좀 더 정확한 센싱 결과를 제공하기 위한 분산 스펙트럼 센싱 연구(Soft Decision)가 활발히 진행되어 왔다[13-15].

2.2 안전한 분산 스펙트럼 센싱 메커니즘

정확성 측면의 분산 스펙트럼 센싱의 연구가 활발히 진행되면서 해당 메커니즘에서의 안전성 측면의 문제가 점차 제기 되었는데 이는 참여하는 센싱 노드의 센싱값이 위조된 경우에 최종적으로 실제 상황과 상이한 결과가 도출될 수 있다는 것이다.

이러한 공격에 대응하기 위한 연구로서 PU(primary user)의 시그널 패턴에 대한 사전 지식을 통해 각 노드의 의심레벨(suspicious level)을 계산하고, 그 레벨이 높은 센싱값을 제외하고 나머지 값을 OR 퓨전하는 방법이 제안되었다[8]. 그러나 이 방법에서 가정한 PU 시그널 패턴은 실험적으로 정확히 측정하여 구하기 어려운 단점이 있다. 이외에도 로그 노멀 쉐도우잉 거리손실모델(log-normal shadowing model)에 기반하여 센싱값의 수신 시그널 모델을 설립하고 이를 이용하는 ADSP 방법이 제안되었다[9]. ADSP 방법에서는 센싱 노드들 사이에 클러스터를 구성하여 클러스터 내 센싱값의 유사성을 비교해 보고, 유사 정도가 낮은 센싱값은 퓨전 시 제외시켜 공격의 영향을 줄이고자 하였다. 그러나 이 방법은 클러스터 내 1/3 이상의 노드가 공격당한 경우에는 대처할 수 없다는 단점이 있다[10].

2.3 RDSS

위조된 센싱값에 의한 공격에 대응하는 또 하나의 방법으로서 RDSS[7]가 제안되었다. RDSS에서는 ADSP[9]와 유사하게 PU 시그널 패턴에 대한 사전 지식을 요구하지 않는다. 대신 쉐도우잉에 기반하여 PU 시그널 전파 모델을 설립하고, PU와 센싱노드 사이의 거리값을 가지고 이 모델을 이용해 각 센싱노드의 PU 시그널 수신 세기를 추정한다. 이에 기반하여 수신한 센싱값(0 또는 1)의 조건부 확률비를 구하고, 이들을 곱하여 임계치에 다다르게 되면 최종 결정에 이르게 되는 weighted SPRT를 수행한다. 이 때 각 센싱노드의 센싱값 정확도에 따라 평판값을 계산하여 조건부 확률비에 대한 가중치(weight)로 사용함으로써 위조된 센싱값으로부터 영향을 줄이고자 하였다. 그러나 RDSS에서는 다음과 같은 단점들이 존재한다.

1. WSPRT 반복 시, 공격자는 위조된 센싱값을 초기에 입력하게 함으로써 적은 노드 수의 공격으로도 쉽게 최종의 이상결과를 유도해 낼 수 있다.
2. 평판값이 높은 노드가 공격 당하면, 해당 공격의 영향을 줄이기 위해 상당한 시간이 요구될 수 있다.

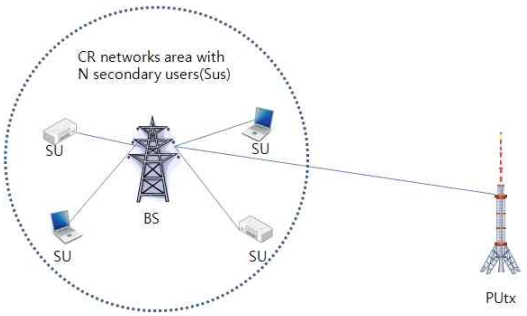
본 논문에서는 이러한 단점을 보완하여 사전에 공격 가능성을 차단하여 위조된 센싱값을 방지하므로 안정적인 사용이 가능하도록 하는 서명기법 인증 매커니즘을 제안하였다.

Ⅲ. RDSS 트랜잭션 서명기법

3.1 RDSS 네트워크 모델

RDSS 네트워크 모델은 여러 SU(secondary user) 노드들은 기지국(base station, BS)을 중심으로 애드혹 인지

라디오 네트워크를 구성하고, TV 송신탑과 같은 주사용자 전송기(primary user transmitter, PUtx)의 송신 시그널 존재 여부를 주기적으로 센싱을 수행한다.



<그림 1> RDSS 네트워크 모델

이러한 RDSS 네트워크 모델에서 가정하는 공격 유형은 PUtx 시그널의 센싱 값을 반대로 만드는 공격이다. 즉 시그널을 감지하면 "1"의 값을 전송해야 하는데 "0"을 전송하거나, 시그널이 감지되지 않으면 "0"의 값을 전송해야 하는데 "1"의 값을 전송하는 것을 의미한다.

이러한 악성 코드에 감염되거나 혹은 악의적인 의도를 가진 SU들을 사전에 차단하기 위해서는 악의적인 센서인지를 판단하는 인증작업이 필요하다. 이러한 인증작업 통해서 인증받지 못한 센서의 값을 제외함으로 잘못된 정보를 전달하는 것을 사전에 예방할 수 있다.

3.2 트랜잭션 서명기법

위조된 센싱값을 해결하기 위해 <그림 2>와 같은 인증서기반의 트랜잭션 서명기법[16]을 제안하였다. PU 시그널 수신 세기를 측정하는 각 센서는 자신의 인증서를 소유하고 있으며, 센서 메시지를 입력으로 하는 트랜잭션 기반의 인증방식을 나타내고 있다. <그림 2>에서 사용된 기호의 정의는 다음과 같다.

<표 1> 기호의 정의

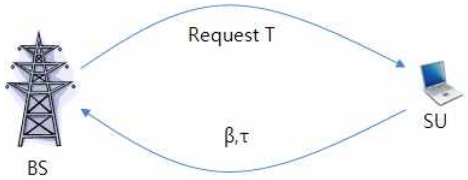
기호	의미
H_k	일방향 해쉬함수
K	공유키
T	경로 강화 메시지 정보
T_p	T의 부분 정보
$T \supseteq T_p$	센서 노드의 개인키
SK(A)	BS 노드의 공개키
PK(A)	BS 노드의 개인키
ρ	노드의 PIN 값

SU 노드에서는 토큰 정보 K를 사용하여 해쉬 작업을 수행한다.

$$\alpha = MAC1 = H_K(T_P, \rho, \zeta) = f(K, T_P, \rho, \zeta)$$

또한 이 정보를 대상으로 $SK_{(B)}$를 사용하여 서명작업을 수행한다.

$$\beta = sign_{SK(B)}(\alpha)$$



<그림 2> 트랜잭션 서명기법

마지막으로, $PK_{(A)}$를 사용하여 T의 정보를 암호화한다.

$$\gamma = E_{PK_{(A)}}(T)$$

센서 노드는 BS 노드로 β, γ의 정보를 전송하면 BS 노드에서는 γ를 복호화하며, α를 생성하고 마지막으로 β를 검증하는 작업을 수행한다.

이러한 방식은 일반적인 OTP 기반의 트랜잭션 서명 방식과 유사하다. 센서 노드는 OTP 지원 모듈과 공인인증서를 저장하고 있기 때문에 OTP 생성을 위한 키(k)를 가지고 α을 생성하고, 인증서에 포함된 개인키를 이용하여 서명해 β를 생성하고 BS 노드에 전송한다.

1: All i, $r_i = 0$
2: For each spectrum sensing attempt made by N_0 {
3: i=0, $W_n - 1$
4: Request T verification {
5: $\alpha = MAC1 = H_K(T_P, \rho, \zeta) = f(K, T_P, \rho, \zeta)$
6: $\beta = sign_{SK(B)}(\alpha)$
7: $\gamma = E_{PK_{(A)}}(T)$
8: Verification α, β {
9: Get all spectrum sensing reports $u_i\, s$ from N_i
10: $W_n = W_n \bullet (\frac{P[u_i|H_1]}{P[u_i|H_0]})^{f(r_i)}$
11: If $n_0 < W_n < n_1, i = (i+1) \bmod (m+1)$, *Go* to 9
12: If $W_n \geq n_1$, $accept\, H_1$, $i.e.\, output\, u = 1$, *Go* to 14
13: If $W_n \leq n_0$, $accept\, H_0$, $i.e.\, output\, u = 0$
14: For each sampled u_i, $set\, r_i = r_i + (-1)^{u_i + u}$

<그림 3> RDSS 트랜잭션 서명기법

β와 경로 강화 메시지(T)를 베이스노드의 개인키로 암호화한 γ를 수신한 PU 노드는 등록된 PIN(ρ), 공유키(k) 그리고 동기정보(ζ)를 사용하여 $f(k, T_P \rho, \zeta)$을 생성하여 검증하고, β를 복호화한다. BS 노드는 공개키로 서명된 β를 검증하여 α와 동일하면 경로 강화 메시지의 정보를 정상적인 정보로 인지하고 WSPRT 정보에 반영한다[17].

3.3 RDSS에 제안 기법의 적용

RDSS의 프로시저에<그림 3>과 같이 적용할 수 있다. 여기에서 n_0는 BS 노드를 의미하며, n_i는 i번째 센싱노드를 나타낸다.

각 센싱노드로부터 센싱값들을 수집하기 전에 각 노드들이 위조된 정보를 제공하는 악의적인 노드인지 정상적인 기능을 수행하는 노드인지를 판별하기 위해서 트랜잭션 서명기법을 사용하여 각 노드들에 대한 정당성 여부를 점검하게 된다. 만약 적정한 노드로 판별되면, SPRT는 각 센싱노드들로부터의 센싱값(u_i=1 또는 0)에 따라 PU 시그널 존재 여부(존재 H_1, 부재 H_0)의 조건부 확률비를 곱하여 계산하고 그 값이 임계치에 다다르게 되면 최종결과를 내고($S_n \geq n_1$이면 H_1 결정, $S_n \leq n_0$이면 H_0 결정), 그렇지 않은 경우 다른 센싱값을 다시 적용하여 계산한다.

여기서 n_1과 n_0는 다음과 같이 값을 산정할 수 있다. 단, P_{01}은 허용된 오탐지율(tolerated false alarm probability)이고, P_{10}은 허용된 미탐지율(tolerated miss detection probability)이다.

$$n_1 = \frac{1 - P_{01}}{P_{10}}, \quad n_0 = \frac{P_{01}}{1 - P_{10}}$$

또한 <그림 3>의 10번째 스텝에서 각 센싱노드의 센싱값의 정확성에 따라 평판값 r_i에 의한 가중치 $f(r_i)$가 사용된다[7].

Ⅳ. 성능평가

본 논문에서는 BAN 로직을 이용하여 제시한 메커니즘을 정형 명세하고, 검증작업을 수행하였다.

4.1 BAN 로직

본 절에서는 BAN 로직을 소개하고자 하며, 세부적인 내용은 M. Burrows[18]의 논문에서 언급되고 있다. BAN 로직의 핵심 요소는 통신 주체들 간에 전송되는 메시지가 최근의 것이고 적절한 키를 사용하여 암호화가 되었다면 인증될 수 있다는 정의에서부터 시작된다. 이 정의는 암호화에 사용되는 알고리즘이 안전하다는 것을 가정하고 있으며, 많은 보안 프로토콜에 대한 분석과 암호 분석을 위한 도구로서 사용되고 있다.

BAN 로직의 주요 구조 및 본 논문에서 사용하는 기호는 다음의 표기를 사용하여 기술된다.

A : BS노드의 인증 서버,

B : 센서노드,

ρ : PIN 값,

ζ : 동기정보로 사용되는 시간 값

A|≡X : A는 X를 신뢰해도 된다.

A|~X : A는 X에게 메시지를 전송한다.

A◁X : A는 X를 확인한다.

#X : X메시지는 최근의 것이다.

$\xrightarrow{K}A$: K는 A의 공개키이다. (개인키 K^{-1}은 A만이 가지고 있다.)

$A \overset{K}{\longleftrightarrow} B$: A와 B는 안전한 통신을 위해 공유키 K를 사용할 수 있다.

$A \overset{K}{\Longleftrightarrow} B$: A와 B 사이에 공유하는 비밀값 K가 존재한다.

$\{X\}_K$: 메시지 X는 키 K를 사용하여 암호화 되었다.

$<X>_Y$: X는 비밀값 Y와 결합되었다.

이외에도 서명기법을 증명하기 위해 BAN로직에서 다음의 공리들을 사용하였다.

1. 공개키 암호 메시지 규칙

K가 B의 공개키일 때, A는 B가 K^{-1}을 사용하여 암호화한 메시지 X를 확인이 가능하다면, A는 메시지 X가 B로부터 전송된 메시지라는 것을 믿을 수 있다.

2. 대칭키 암호 방식에 대한 메시지 규칙

A가 B와 대칭키 K를 공유하고 있을 때, A는 B가 K을 사용하여 암호화한 메시지 X를 확인이 가능하다면, A는 메시지 X가 B로부터 전송되었다는 것을 믿을 수 있다.

3. 비밀키 암호 방식에 대한 메시지 규칙

A가 B와 비밀키 Y를 공유하고 있을 때, A는 B가 Y을 사용하여 암호화한 메시지 $<X>_Y$를 확인이 가능하다면, A는 메시지 X가 B로부터 전송되었다는 것을 믿을 수 있다.

4. 비표(Nonce) 검증 규칙

특정 통신 주체가 메시지를 전송하였고, 그 메시지가 최근의 것이라면 비표를 신뢰할 수 있다.

4.2 서명기법에 대한 검증

앞서 기술한 서명기법을 BAN 로직의 규칙에 따라 서명인증 기법을 정규화하면 다음의 식과 같이 정리할 수 있다.

$$\beta = \alpha = \{<X,\zeta>_\rho,\rho\}_{K_k},\ \left\{A \overset{K_k}{\longleftrightarrow} B\right\},\left\{A \overset{\rho}{\Longleftrightarrow} B\right\},\ \left\{A \overset{\zeta}{\Longleftrightarrow} B\right\},\left\{\xrightarrow{K_{(B)}} B\right\}_{K_B^{-1}},\left\{\gamma = M,\left\{\xrightarrow{K_{(A)}} A\right\}\right\}_{K_{(A)}} \quad (1)$$

식(2)부터 식 (7)까지는 BAN 로직에 의해 증명하기 위한 가정들을 정규식으로 표현하고 있다[18].

$$A| \equiv A \overset{K_k}{\longleftrightarrow} B \quad (2)$$

$$A| \equiv A \overset{\rho}{\Longleftrightarrow} B \quad (3)$$

$$A| \equiv A \overset{\zeta}{\Longleftrightarrow} B \quad (4)$$

$$A| \equiv \xrightarrow{K_{(A)}} A \quad (5)$$

$$A| \equiv \xrightarrow{K_{(B)}} B \quad (6)$$

$$B| \equiv (\zeta) \quad (7)$$

정규화된 프로토콜을 가정과 공리를 사용하여 로직을 다음과 같이 검증할 수 있다.

- Step 1: A는 가정 (2), (3), (4), (7)가정에 의해 K_k와 ρ를 가지고 있으며, 시드(seed) 정보로서 ζ을 가지고 있다.
- Step 2: 가정 (5)와 BAN 로직의 message-meaning rule의 공개키 암호 메시지 규칙으로부터 BS 노드는 센서 노드가 전송한 γ를 읽을 수 있고, 트랜잭션 X를 확인할 수 있다.
- Step 3: (2)의 가정과 비표 검증 규칙의 공리로부터 BS 노드는 최근의 ζ을 생성하고 (2), (4)의 가정에 의해 동일한 α를 생성할 수 있다. 이 때 BS 노드는 message-meaning rule 대칭키와 비밀키 암호 방식에 대한 메시지 규칙 공리에 의해 센서 노드로부터 생성된 트랜잭션이라는 것을 확인할 수 있다.
- Step 4: 베이스 노드는 (1)의 가정과 비표 검증 규칙의 공리에 의해 센서 노드의 개인키(K^{-1})로 서명된 β를 센서 노드의 공개키(K)를 사용하여 검증하고, 센서 노드가 최근에 거래 요청한 트랜잭션서명이란 것을 믿을 수 있다.

즉, 1에서 4까지의 단계를 통해서 베이스 노드는 센서 노드가 "Always-False" 공격을 시도하는 악의적인 노드인지 혹은 적당한 권한을 가진 정당한 센서 노드인지를 인증할 수 있다.

4.2 악의적인 노드 공격에 대한 대응 분석

악의적인 노드는 거짓 정보를 전달하기 위해 센싱 메시지 M을 위조하여 M'로 변경한 공격을 시도한다. 공격자는 $\gamma' = \left\{M', \left\{\xrightarrow{K_{(A)}} A\right\}\right\}_{K_{(A)}}$ 를 생성하여 Always-False 공격을 시도한다. BS 노드는 단계 2에서 M'를 추출하고 단계 3을 수행한다.

여기서 BS 노드가 생성한 α'는 다음과 같다.

$$\alpha' = \{< M', N >, \rho\}_{K_k}$$

그러나 실제로 센서 노드가 시도한 α는 다음과 같다.

$$\alpha = \{< M, N >, \rho\}_{K_k}$$

그러므로 해당 트랜잭션은 거절이 되어 거짓 센서 정보는 거절된다.

이러한 공격 이외의 합법적이지 않은 노드들로부터의 임의의 센싱값에 의한 삽입(injecting) 공격은 기본적인 인증 메커니즘(예, MAC(message authentication code) 검증 혹은 RF fingerprint[19])에 의해 대응 가능하다. 또한 과거에 전송된 센싱값을 캡쳐하여 재전송하는 재생(replaying) 공격은 타임스탬프나 시퀀스번호 삽입을 통해 탐지 가능하다. 물리계층의 재밍 공격은 기본적인 재밍방해(jamming-resistant) 기법인 FSSS(frequency hopping spread spectrum) 혹은 DSSS(direct sequence spread spectrum) 기법 등으로 대응이 가능하다[20-21].

Ⅴ. 결론

인지 라디오 네트워크 기술의 중요성은 점점 더 확대되고 있다. 이는 한정된 주파수 자원에 비해 그 사용량이 크게 확대되고 있기 때문이다. 본 논문에서는 이러한 인지 네트워크 상에서 주파수 탐지 기능을 원활하게 수행하기 위한 인증기술을 제안하였다.

이러한 인증기술은 SU 노드와 BS 노드 사이에 일어나는 트랜잭션을 기반으로 한 서명기법으로 인증함으로써 임의의 SU 노드가 악성코드에 의해 잘못된 정보를 전달하려고 할 때 그에 대한 효과적인 대응을 할 수 있다. 즉 인

지 라디오 네트워크의 RDSS에서 WSPRT 반복 시, 공격자의 위조된 센싱값을 통해 적은 노드 수의 공격으로도 쉽게 최종의 이상결과를 도출하거나, 평판값이 높은 노드가 공격당하면, 해당 공격의 영향을 줄이기 위해 상당한 시간이 요구되는 등의 문제점을 근원적으로 해결할 수 있다.

참고문헌

[1] 김창주, "Cognitive Radio 기술 및 응용," 한국전자파학회지 전자파기술, 제17권, 제2호, 2006년 4월, pp. 3-8.

[2] 김창주, "Cognitive Radio 기술동향," 전자통신동향분석, 제21권, 제4호, 2006년 8월, pp. 62-69.

[3] J. Mitola III, and G. Q. Maguire, "Cognitive radio: making software radios more personal," IEEE Personal Communications, Vol. 6, No. 4, 1999, pp. 13-18.

[4] Z. Kostic, and N. Sollenberger, "Performance and implementation of dynamic frequency hopping in limited-bandwidth cellular systems," IEEE Transactions on Wireless Communications, Vol. 1, No. 1, Jan., 2002, pp. 28-36.

[5] T. Newman, T. Clancy, "Security threats to cognitive radio signal classifiers," Virginia Tech Wireless Personal Communications Symposium, Blacksburg, Va, USA, June 2009.

[6] T. Clancy, N. Goergen, "Security in cognitive radio networks: threats and mitigation," CrownCom, Singapore, May 2008.

[7] R. Chen, J. M. Park, K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," INFOCOM, Apr. 2008, pp. 1876-1884.

[8] W. Wang, H. Li, Y. Sun, Z. Han, "Securing Collaborative Spectrum Sensing against Untrustworthy Secondary Users in Cognitive Radio Networks," EURASIP Journal on Advances in Signal Processing, vol. 2010, Article ID 695750, 2010.

[9] A. W. Min, K. G. Shin, X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," ICNP, Oct. 2009, pp. 294-303.

[10] 김미희, 추현승, "인지 라디오 네트워크에서 안전한 분산 스펙트럼 센싱을 위한 향상된 평판기반 퓨전 메커니즘," 한국인터넷정보학회 논문지, 11권, 6호, 2010. 12.

[11] W. S. Jeon, D. G. Jeong, J. A. Han, G. Ko, M. S. Song, "An efficient quiet period management scheme for cognitive radio systems," IEEE Trans. Wireless Commun., Feb. 2008, vol. 7, no. 2, pp. 505-509.

[12] H. Kim, K. G Shin, "In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?," ACM international Conference on Mobile Computing and Networking (MobiCom), Sep. 2008, pp. 14-25.

[13] E. Visotsky, S. Kuffher, R. Peterson, "On collaborative detection of TV transmissions in support of dynamic spectrum sharing," IEEE DySPAN, Nov. 2005, pp. 338-345.

[14] A. Ghasemi, E. S. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," Journal of Communications, 2007, vol. 2, no. 2, pp. 71-82.

[15] G. Ganesan, Y. Li, "Cooperative spectrum sensing in cognitive radio, part II: multiuser networks," IEEE Transactions on Wireless Communications, 2007, vol. 6, no. 6, pp. 2214-2222.

[16] 임형진, 이정근, 김문성, "안전한 인터넷 뱅킹을 위한 트랜잭션 서명기법에 관한 연구," 한국 인터넷

정보학회, 9권, 6호, 2008년, pp. 73~79.

[17] 김태경, "디렉티드 디퓨젼 기반의 무선 센서 네트워크에서의 싱크홀 공격을 막기 위한 트랜잭션 서명 기법에 관한 연구", 디지털산업정보학회, 6권, 3호, 2010. 9.

[18] M. Burrows, M. Abadi, R. Needham: A logic of authentication. ACM Transactions on Computer Systems, 8(1):18-36, February, 1990.

[19] W. C. Suski, M. A. Temple, M. J. Mendenhall, R. F. Mills, "Using Spectral Fingerprints to Improve Wireless Network Security," GLOBECOM, Dec. 2008, pp. 1-5.

[20] M. Strasser, C. Popper, S. Capkun, "Efficient uncoordinated FHSS anti-jamming communication," International Symposium on Mobile Ad Hoc Networking and Computing, May 2009, pp. 207-218.

[21] Y. Liu, P. Ning, H. Dai, A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," IEEE INFOCOM, Mar. 2010, pp. 1-9.

논문접수일 : 2011년 8 월 17 일
수 정 일 : 2011년 8 월 29 일
게재확정일 : 2011년 9 월 3 일

■ 저자소개 ■

김 태 경
Kim, Tae Kyung

2008년 3월~현재
서울신학대학교 교양학부 교수
2006년 3월~2008년 2월
서일대학 정보전자과 교수
2005년 8월 성균관대학교 전기전자 및 컴퓨터공학과 (공학박사)
2001년 8월 성균관대학교 정보통신공학과 (공학석사)
1997년 2월 단국대학교 수학교육과 (이학사)

관심분야 : 네트워크보안, USN, 클라우드 컴퓨팅
E-mail : tkkim@stu.ac.kr