IEEE 802.11 무선랜 재밍 환경에서의 측정 기반 채널 도약 기법

준회원 정 승 명*, 정회원 정 재 민**, 종신회원 임 재 성***

Measurement-based Channel Hopping Scheme against Jamming Attacks in IEEE 802.11 Wireless Networks

Seungmyeong Jeong* *Associate Member*, Jaemin Jeung** *Regular Member*,
Jaesung Lim*** *Lifelong Member*

요 약

본 논문에서는 IEEE 802.11 무선 네트워크에서 재밍 (jamming) 공격에 효과적으로 대처할 수 있는 IEEE 802.11h 기반의 채널 도약 기법을 제안한다. IEEE 802.11h의 Dynamic Frequency Selection (DFS)은 현재 사용하는 채널에서 군 레이더와 같은 높은 간섭을 감지할 경우 임의의 채널을 선택하지 않고 전체 채널 측정을 통해 가장 좋은 채널로 도약하는 기법이다. 이러한 기법은 재밍 공격이 발생하는 환경에서는 채널 도약을 위해 모든 채널 측정을 위한 시간이 소요되며 그 시간만큼의 통신 단절이 발생해 네트워크 성능이 저하되는 단점을 가진다. 제안하는 기법에서는 기존의 기법과는 달리 재밍 공격 이전에 도약할 채널을 모든 단말이 알게 함으로써 재머에 대해 즉각적인 대처가 가능하다. 이를 위해 제안하는 기법에서는 비콘 (Beacon)을 통해 도약할 채널을 매번 갱신하며 이것은 이전 비콘 구간마다 전채널 상태 측정을 수행하는 것으로 가능하다. 다양한 환경에서의 모의 실험을 통해 제안 기법이 재머에 즉각적인 대응을 수행함으로써 네트워크 성능 저하를 완화할 수 있음을 확인할 수 있다.

Key Words : WLAN, IEEE 802.11h, DFS, Channel Hopping, Jamming Attacks

ABSTRACT

In this paper, we propose a new channel hopping scheme based on IEEE 802.11h as a good countermeasure against jamming attacks in IEEE 802.11 wireless networks. 802.11h Dynamic Frequency Selection (DFS) is a mechanism which enables hopping to a best channel with full channel measurement, not a randomly chosen channel, when the current link quality degradation occurs due to interferers such as military radars. However, under jammer attacks, this needs a time for full channel measurement before a new channel hopping and due to link disconnection during the time network performance degradation is inevitable. In contrast, our proposed schemes make an immediate response right after a jammer detection since every device is aware of next hopping channel in advance. To do this, a next hopping channel is announced by Beacon frames and the channel is selected by full channel measurement within Beacon intervals. Simulation results show that proposed scheme minimizes throughput degradation and keeps the advantages of DFS.

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원 사업의 연구결과로 수행되었음 (NIPA-2011-C1090-1121-0011)
* 아주대학교 정보통신대학원 (aflight@ajou.ac.kr)
** 아주대학교 NCW 학과 (mnsg@ajou.ac.kr)
*** 아주대학교 정보통신전문대학원 정보통신공학과 (jaslim@ajou.ac.kr)
논문번호 : KICS2011-06-268, 접수일자 : 2011년 6월 21일, 최종논문접수일자 : 2012년 1월 6일

Ⅰ. 서 론

최근 스마트폰 이용자의 급격한 증가로 인해 무선랜으로 대표되는 IEEE 802.11 프로토콜을 이용하는 단말의 숫자 또한 급격히 늘어나고 있다. 늘어나는 사용량과 함께 무선 네트워크는 많은 위험에 노출될 수 있지만 IEEE 802.11 표준은 모든 단말이 정해진 프로토콜에 따라 동작하는 것을 가정하며 네트워크의 통신을 단절시킬 수 있는 재머(jammer)와 같은 악의적인 네트워크 공격에 대처할 수 있도록 설계되지 않았다[1].

재머 공격은 계층 및 공격 대상에 따라 여러 유형으로 나누어볼 수 있다. IEEE 802.11은 무선 통신의 브로드케스트 속성에 의해 서비스거부 (DoS : Denial-of-Service)공격 유형에 취약하다[2]. 서비스 거부 공격은 현재 우리가 사용하는 무선 장비를 이용해 쉽게 구현할 수 있으며 특정 채널에 대하여 연속적으로 패킷을 전송하여 네트워크를 마비시키는 공격 유형이다.

IEEE 802.11 무선 네트워크에서 재밍 공격에 대한 효과적인 대처 방안으로 채널 도약이 알려져 있다[1,3]. 채널 도약 수행 시 재밍 공격 상황에서도 약간의 성능 저하가 있지만 여전히 네트워크 운용이 가능하다.

본래 IEEE 802.11 표준은 주파수 도약 스펙트럼 확산을 정의하고 있다. 하지만 이 기법은 802.11 a/b/g 프로토콜에서 반영되지 않았다[1]. 반면 주파수 도약 스펙트럼 확산과는 다른 [1], [3]의 채널 단위의 도약 기법은 현재 사용 중인 IEEE 802.11 네트워크 카드의 하드웨어 수정 없이 펌웨어 소프트웨어 변경만으로도 구현 가능하므로 쉽게 적용할 수 있다.

채널 도약은 일정 시간 간격으로 채널 도약을 수행하는 능동적 도약 (proactive hopping)과 채널 상태의 변화 등에 의해 도약을 수행하는 대응적 도약 (reactive hopping)으로 나누어 볼 수 있다. [1], [3]은 능동적인 도약 기법에 속한다. 반면 블루투스(Bluetooth)의 Adaptive Frequency Hopping (AFH), Adaptive Frequency Rolling (AFR), 그리고 Dynamic Adaptive Frequency Hopping (DAFH)는 대응적 도약에 포함될 수 있다. 재머 공격에 대해서는 대응적인 기법이 좀 더 우수한 성능을 보이는 것으로 알려져 있다[4].

재밍 공격을 회피하기 위한 [1], [3]의 채널 도약 기법은 다음 번 도약할 채널을 채널 상태와는 무관하게 임의적으로 선택한다. 같은 주파수 대역을 사용하는 단말의 숫자가 늘어남에 따라 채널 간섭이 높은 환경에서는 임의적으로 다음 도약 채널을 선택하면 주변 네트워크와 동일 채널 사용으로 IEEE 802.11의 CSMA/CA의 백오프 (back-off)가 증가하여 서로 간의 성능 저하를 유발할 수 있다.

반면에 각 채널 상태를 측정한 후 주변에서 사용하지 않는 그리고 재밍에 노출되어 있지 않은 최적의 채널을 선택하여 도약하는 기법이 있고 대표적으로는 IEEE 802.11h, 802.16h에서 정의하고 있는 DFS (Dynamic Frequency Selection)이다. 특히, IEEE 802.11h의 DFS는 본래 군 레이더나 위성이 사용 중인 5GHz 주파수 대역에서 802.11 무선 단말을 사용 할 때 레이더 신호를 검출하면 다른 채널을 선택해서 AP를 비롯한 모든 단말이 새로운 채널로 도약하는 기법이다[5]. DFS의 자세한 동작은 다음 장에서 설명하기로 한다.

본 논문에서는 IEEE 802.11의 네트워크에 AP가 존재하는 환경에서 채널측정 기반 채널 선택을 통한 주파수 도약 기법에 관한 연구로서 기존의 IEEE 802.11h DFS 알고리즘을 개선한다. 이를 위한 방법으로는 비콘 구간에 전채널을 측정하여 매번 비콘(Beacon)에 다음 도약할 채널을 갱신하여 즉각적인 재밍 대응이 가능한 기법을 제안한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 기존 IEEE 802.11h의 기존적인 DFS 알고리즘을 소개하고 재밍 환경에서의 동작을 설명한다. 3장에서는 본 논문에서 제안하는 재밍 환경의 개선된 채널 도약 기법을 소개한다. 그리고 4장에서는 제안하는 기법의 성능을 모의 실험을 통해 검증하고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

IEEE 802.11h는 5GHz Unlicensed National Information Infrastructure (U-NII) 주파수 대역의 부사용자인 IEEE 802.11 단말이 주사용자인 레이더나 위성과 주파수 간섭을 회피하여 다른 채널로 도약할 수 있는 DFS 알고리즘을 정의한다.

IEEE 802.11h의 DFS 동작은 아래의 그림과 같이 동작한다. AP가 처음에 전 채널을 검사하여 가장 좋은 채널을 선택한 후 동작을 시작하며 비콘 프레임을 통해 현재 채널을 알리면서 네트워크를 가동한다. 정상운용 (Normal Operation)에서는 일정 간격으로 현재 사용 중인 채널을 검사하며 레이더

의 등으로 인해 링크의 상태가 나빠지면 기존의 동작을 멈추고 즉시 전 주파수 측정 (Full DFS Test) 상태로 천이된다. 전 주파수 측정에서는 AP가 모든 채널 상태를 측정하며 최적 채널을 선택한다. 이 때 AP는 단말과 협력하여 채널을 상태를 측정할 수 있다. 이후 AP는 채널변경 지시 (Channel Switch Announcement)를 전송하여 선택한 채널로 즉시 혹은 특정 시간에 AP와 모든 단말이 새로운 채널로 도약한다.

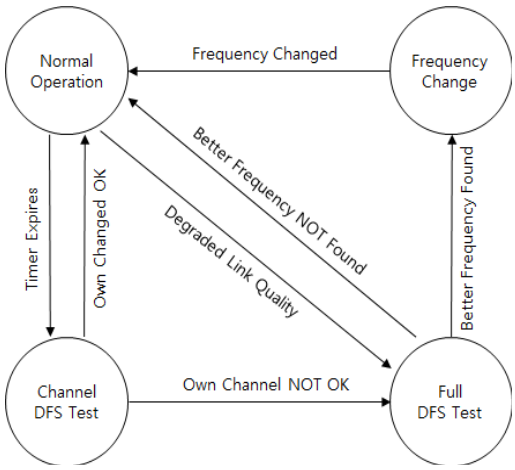


그림 1. IEEE 802.11h DFS 알고리즘

이러한 IEEE 802.11h DFS는 재밍 공격 발생 시 새로운 채널을 탐색하는 Full DFS Test 구간에 의해 재머 대응에 일정한 시간이 걸리며 그 시간 동안 통신이 두절되는 단점을 가지고 있다. 또한 새로운 채널은 전채널을 검사한 후에 이루어지므로 채널 간의 도약 시간과 전체 채널 개수에 비례하여 재머에 대응할 수 있는 시간이 늘어난다.

그림 3을 보면 재밍 공격에 의해 높은 채널 간섭을 감지한 AP는 Full DFS Test를 수행한다. 이 시간 동안 네트워크의 모든 통신은 단절된다. 전채널을 검사한 AP는 새로 도약할 채널을 선택하고 이 채널을 비콘 프레임, 프로브응답 프레임 (Probe Response frame) 그리고 채널변경지시 프레임 (Channel Switch Announcement frame)을 통해 알려줄 수 있다. 하지만 현재 채널이 여전히 재밍 공격을 받고 있으며 이로 인해 채널 변경 지시 프레임을 수신하지 못하면 단말은 비콘이나 프로브 응답을 통해 기존AP 혹은 다른 AP와 연결될 수 있다.

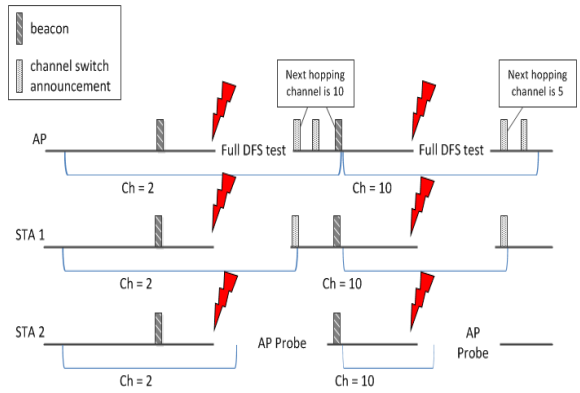


그림 2. IEEE 802.11h DFS 동작 예시

본 논문에서는 여러 재머 모델 중 스마트 재머(smart jammer)를 가정한다[1]. 여기서의 스마트 재머는 일정 시간 간격으로 IEEE 802.11 무선 네트워크 전체 채널의 사용 여부를 판단하여 사용하지 않는 채널일 경우 다음 채널을 검사하면서 사용 중인 채널을 찾아낸다. 사용 중인 채널을 찾아내면 그 채널로 일정 시간 연속적인 패킷을 전송하는 공격을 가하며 채널은 사용할 수 없게 된다. 모든 채널을 순회하며 공격을 가하는 재머 모델로써 구현이 단순하면서도 재머로써의 성능이 높다.

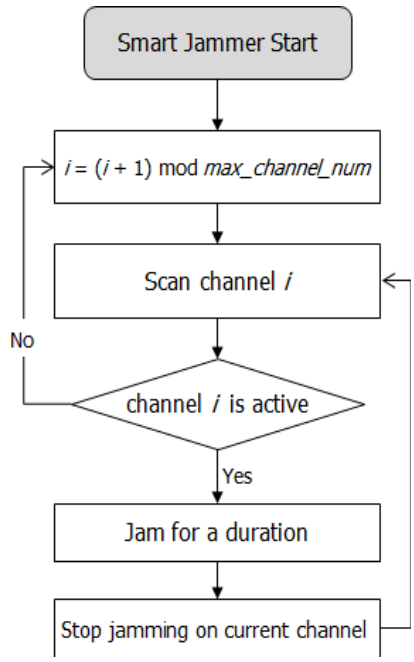


그림 3. 스마트 재머 동작 알고리즘

Ⅲ. 제안하는 기법

제안하는 기법은 AP를 포함한 모든 단말이 다음 도약할 채널 정보를 미리 공유하여 재머 공격 발생 시 즉시 채널 도약을 수행하는 기법과 비콘 구간 (Beacon Interval) 사이에 전체 채널을 검사하는 기법으로 구성된다.

3.1. 재밍 공격 후 즉각적인 채널 도약

재밍 환경에서 기존의 IEEE 802.11h는 Full DFS Test 수행 시간 이후에 AP에 의해 새로운 채널이 선택되고 다른 단말이 AP의 새로운 채널을 인식하는 데 추가적인 시간이 소요될 수 있다. 이와 같은 느린 재머에 대한 반응은 재머 공격 유형에 따라 네트워크 성능이 크게 저하될 수 있는 가능성이 있다.

제안하는 기법은 재밍 공격이 발생하기 전에 미리 AP와 모든 단말이 다음 도약할 채널 정보를 공유하는 기법이다. 이 기법이 가능하기 위해서는 재밍 공격 이전에 도약할 후보 채널의 상태를 측정하여야 하며 자세한 방법은 다음 절에 설명한다.

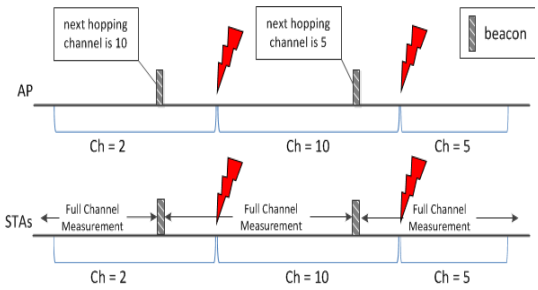


그림 4. 도약 채널 사전 공유를 통한 즉각적 채널도약

그림 4를 보면 처음에 네트워크에서 2번 채널을 사용 중이며 비콘을 통해 다음 번 도약할 채널이 10번임을 공유하였다. 이후 재밍 공격이 탐지되면 AP를 포함한 모든 단말이 10번 채널로 도약한다.

다양한 유형의 재밍 공격을 탐지할 수 있는 기법은 대표적으로 패킷전달비율 (PDR : Packet Delivery Ratio)과 신호세기를 동시에 이용하는 방법 등 다양한 기법 들이 연구되고 있다 [7]. 재밍 탐지 기법은 본 논문의 연구 범위 밖으로 별도로 다루지 않고 모든 단말에서 즉각적인 재밍 공격을 탐지할 수 있다고 가정한다.

IEEE 802.11 무선 네트워크 환경에서는 재머의 신호 세기에 따라 위의 그림과 같이 부분적인 영향을 받을 수도 있다. 경우 1에서는 AP가 재밍 공격을 탐지하지 못했다. AP가 채널 도약을 수행하지 않고 계속 재밍 공격을 당하고 있으면 도약을 수행한 단말 2와 3은 AP와 연결이 끊어져 통신이 불가능하다. 따라서 단말 2와 단말 3이 채널 도약을 수행하기 전에 채널변경지시 프레임을 전송하여 AP와 단말 1도 미리 알고 있는 채널로 도약한다. 경우 2에서는 단말 1과 2와 같은 일부 단말만 재밍을 탐지하지 못했다. 이 경우에는 앞선 경우 1과 같이 AP와 단말 3이 채널 도약을 알려주는 방법을 통해 단말 1과 2가 다음 채널로 도약할 수 있다. 또한 단말 1과 2가 다시 AP 프로브를 수행하는 경우에 비콘 프레임 혹은 프로브응답 프레임에 의해 다시 AP와 연결될 수 있다.

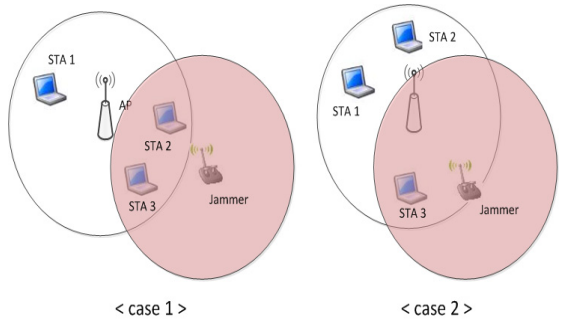


그림 5. 재머 공격에 대한 Hidden Terminal

3.2. 비콘 구간내 후보 채널 측정

제안하는 기법은 비콘 구간에서 현재 채널을 포함한 전체 채널의 상태를 측정한다. AP는 단말에 IEEE 802.11h의 동작 프레임 (Action frame)인 측정요구 프레임 (Measurement Request frame)을 통해 측정해야할 채널을 할당한다. 단 현재 채널에서 레이더와 같은 주사용자를 피해 다른 채널을 사용해야 하므로 현재 사용 중인 채널은 반드시 주기적인 측정을 수행해야 한다.

채널 측정을 요청받은 단말은 IEEE 802.11h의 비콘 프레임과 프로브응답 프레임을 통해 알려진 휴지간격 (Quiet Interval)을 이용해 각 채널에 대한 측정을 수행한다. 휴지간격은 휴지시간 (Quiet Duration)의 간격을 말하며, 휴지시간은 모든 단말이 전송을 중지하는 구간이므로 현재 채널을 적어도 현재 네트워크의 간섭 없이 측정할 수 있다.

측정된 결과는 특정 채널에 재머 공격이 있는지에 대한 정보를 포함하며 측정 응답 (Measurement Response)을 통해 AP로 전송된다. 단말로부터 각 채널의 정보를 수집한 AP는 우선 재머가 존재하지 않고, 레이더나 다른 네트워크로 인한 간섭량 및 채널 사용량이 가장 적은 채널을 선택한다.

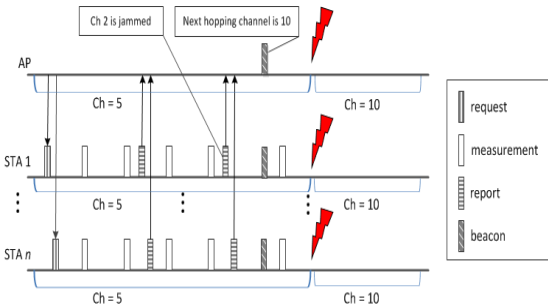


그림 6. 제안하는 채널 상태 측정 방법

측정을 통해 위와 같이 최적의 채널을 선택하는 경우 밀집한 네트워크 환경에서는 근거리에 위치한 AP 끼리 같은 채널을 선택할 수 있다. 이 경우 같은 채널을 사용하는 단말의 숫자가 늘어나면 백오프가 늘어나고 재머의 영향과는 무관하게 네트워크 성능이 저하된다. 또한 같은 채널을 사용하면 재머의 공격에 동시에 노출되는 단점이 있다. 때문에 AP가 다음 도약할 채널을 선택할 때는 채널 상태 정보를 수집 후 임계치 이상의 좋은 채널들에서 임의로 채널을 선택한다.

현재 채널이 아닌 도약 후보 채널의 상태 측정에는 IEEE 802.11h DFS에 비해 휴지시간이 더 길게 설정되어야한다. 왜냐하면 후보 채널에 대한 상태 측정을 위해서는 그 채널 도약했다가 다시 돌아오는 추가적인 시간이 필요하기 때문이다. 이는 곧 재밍이 없는 환경에서는 제안하는 기법이 오버헤드를 유발할 수 있기에 재머 공격에 대해 적응적으로 채널 측정을 수행할 필요가 있다.

제안하는 채널 측정 기법은 재머 공격이 없을 때는 현재 채널만을 측정하고 공격이 발생하면 앞서 설명한 바와 같이 후보 채널을 측정한다. 따라서 공격이 없는 경우에는 IEEE 802.11h DFS와 같은 짧은 휴지시간이 설정되므로 불필요한 성능 저하를 방지할 수 있다. 물론 처음에는 후보 채널에 대한 측정을 수행하지 않으므로 최초의 재머 공격에 대한 도약을 수행하기 위해서는 기본 도약 채널을 AP가 임의로 설정하고 모든 단말이 이를 알고 있어야 한다. 또한, AP가 선택한 채널을 비콘을 통해 알려줄 때는 재머에 의한 도청의 위험이 있으므로, 해당 네트워크의 그룹키로 암호화하여 전송하여야 한다.

3.3. AP 및 단말 동작 순서도

앞서 설명한 제안 기법을 AP와 단말 관점에서 동작 순서도로 정리하면 다음과 같다. 그림 7과 8에서의 AP와 단말의 기본 동작은 IEEE 802.11 프로토콜의 기본 동작 이외에도 IEEE 802.11h의 측정요구 및 측정보고 프레임을 송수신하는 동작을 포함한다.

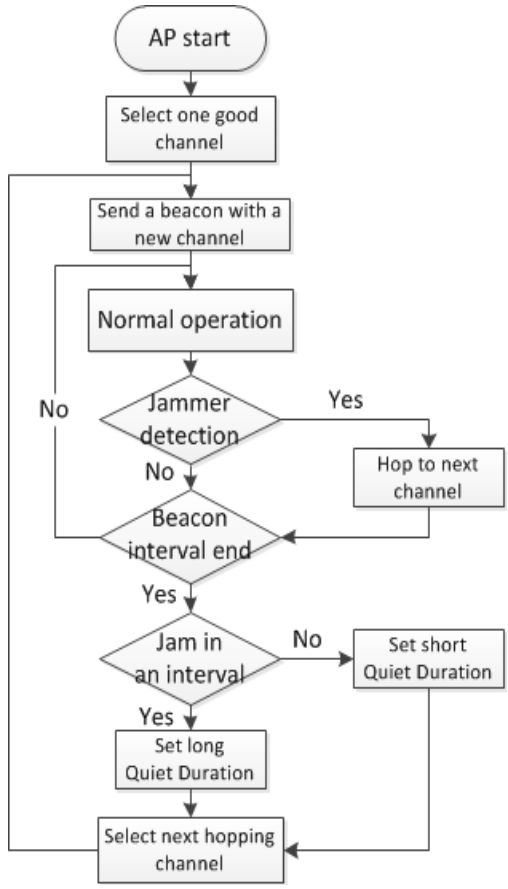


그림 7. AP 동작 순서도

AP는 처음에 전 채널을 검사하여 가장 좋은 채널을 선택한다. 선택한 채널을 비콘이나 프로브응답을 통해 다음 도약 채널 정보와 휴지간격에 대한 정보를 함께 알려주어 채널을 측정을 위한 주기적인 시간을 모든 합법적인 단말들이 알 수 있게 그룹키로 암호화 하여 전송한다. 일반적인 AP의 동작을 수행하면서 현재 채널에 재머의 공격이 있는지

검사한다. 만약 재머가 검출되면 사전에 정의된 채널로 도약을 수행한다. 지난 비콘 구간 동안 재머 공격이 있으면 다음 구간 내에 다른 채널을 측정할 수 있도록 휴지시간을 길게 설정한다. 반면 재머 공격이 없었으면 현재 채널만 측정하도록 휴지시간을 설정한다. 수집된 채널 정보가 있는 경우에는 그 정보를 바탕으로 다음 도약할 채널을 선택하여 다음 비콘을 통해 다시 알려준다.

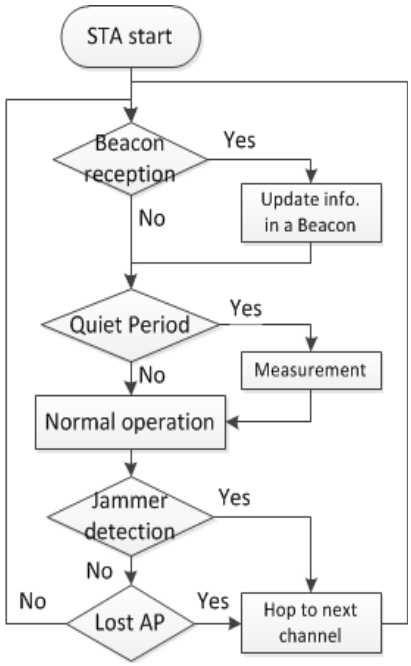


그림 8. 단말 동작 순서도

단말은 비콘을 수신하면 다음 도약할 채널 정보뿐만 아니라 휴지기간 (Quiet Period) 즉 휴지간격 및 휴지시간 등에 대한 정보를 갱신한다. 짧게 설정된 휴지시간에 대해서는 현재 채널에 대한 측정을 수행하고 다른 채널 측정에 필요한 시간만큼 길게 설정된 구간에서는 AP로부터 할당받은 채널에 대한 측정을 수행하여 일반 동작 구간에서 보고한다. 재밍 공격을 탐지하지 못했는데 만약 AP와 연결이 끊어진 경우는 현재 단말과는 달리 AP는 재밍 공격을 탐지하여 채널 도약을 수행한 경우이다. 따라서 이 때는 간접적으로 재머 공격을 인식하여 약속된 채널로 도약을 수행한다. 반면에 직접 재머 공격을 탐지한 경우에는 약속된 채널로 도약을 수행한다. 여기서는 단말이 재밍 공격이 없는데 있는 것으로 인식하는 탐지 에러 (False Alarm)는 없는 것으로 가정한다.

Ⅳ. 모의 실험

우리는 OPNET 네트워크 시뮬레이터를 통해 제안하는 채널 도약 모델을 모델링하여 실험 결과를 얻었다. OPNET Modeler에서 기본적으로 제공하는 무선랜 MAC 모델을 변경하여 채널 도약을 수행하는 IEEE 802.11 단말을 구현하였다.

재머 모델은 앞서 설명한 스마트 재머를 모델링하여 사용하였다. 이 재머는 순차적으로 각 채널의 사용여부를 검사하면서 사용 중인 채널에만 재밍 공격을 가한다. 이를 위해 기존에 OPNET에서 제공하는 재머 모델에 채널을 검사하여 사용 중인 채널만 연속적으로 공격하도록 수정하였다. 이러한 환경에서 제안하는 채널 도약 기법과 IEEE 802.11h DFS와의 성능을 비교하였다.

4.1. 모의 실험 환경

기본적인 모의 실험 변수 값은 아래의 표와 같다. 재머 탐지 (Jammer Sesing) 시간은 재머가 현재 채널의 사용 여부를 다시 검사하는 시간으로 5ms을 가정하였다. 또한 채널도약 시간은 현재까지 상용화된 대부분 기기가 수 밀리초 내에 채널 도약을 수행할 수 있다 [8]. 본 논문에서는 이 시간을 5ms를 가정하였고 IEEE 802.11a의 12개 직교 채널을 사용는 것을 가정하여 수행하였다.

표 1. 실험 환경변수

환경변수	값
재밍 공격 시간	50 msec
재머 탐지 시간	5 msec
채널 도약 시간	5 msec
비콘 간격 시간	100 msec
채널 수	12개
스마트 재머 수	1 개
클라이언트 수	8 개
네트워크 트래픽	Poisson(λ=1) 분포 1024KB 패킷

4.2. 모의 실험 결과

그림 9는 2 ~ 9초 사이에 재머 공격이 발생할 때의 처리량을 나타낸다. 재밍 환경에서 제안하는 기법의 처리량은 재밍이 없을 때 처리량의 50% 이

상의 높은 성능을 보인다. 같은 기법 내에서도 휴지간격 (QI)에 따라 성능이 다른 것을 확인할 수 있다. 먼저 제안하는 기법에서는 휴지간격이 높을수록 더 높은 처리량을 보인다. 휴지간격이 좁게 설정될수록 채널 측정에 대한 오버헤드가 증가하기 때문이다. 반면에 IEEE 802.11h DFS에서는 재밍 공격이 없을 때는 휴지간격 값이 클수록 오버헤드가 덜 발생하지만 재머 공격이 있을 때는 휴지간격 값이 클수록 공격을 탐지하는 데 지연이 발생할 수 있어 지연 시간 만큼의 성능 감소가 발생한다. 재밍이 발생하지 않는 구간에서는 두 기법이 비슷한 성능을 보이는데 재밍이 시작되는 구간에서 즉각적인 재밍 탐지가 가능한 제안 기법이 근소한 차이로 높은 성능을 보인다.

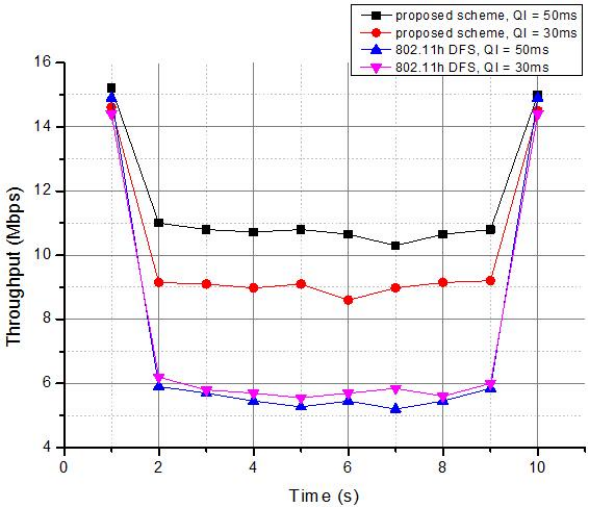


그림 9. 재머 공격시 네트워크 처리량

그림 10은 그림 9와 같은 동일한 실험에서 재머 공격에 따른 채널 도약 횟수를 시간의 경과에 따라 보여준다. 결과를 보면 채널 도약 횟수는 제안하는 기법이 IEEE 802.11h DFS에 비해 더 많다. 이러한 결과는 IEEE 802.11h DFS에서는 재머에 의해 공격될 때마다 Full DFS TEST를 수행하는 구간에서는 통신이 이루어지지 않기 때문에 재머에 의해 공격 당할 수 없는 구간이다. 따라서 채널 도약을 많이 수행하는 것이 단말의 에너지 관점에서 손해로 생각될 수 있지만 네트워크의 생존성 측면에서 생각하면 재머의 공격하에서도 네트워크를 계속 운용하는 기법이 더욱 접합하다고 판단할 수 있다.

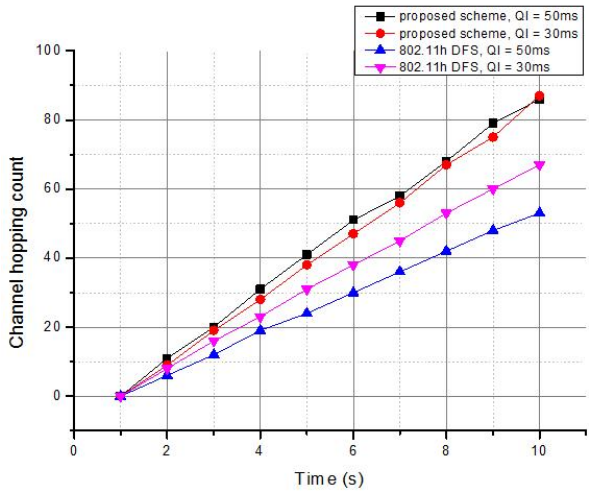


그림 10. 재머 공격시 채널 도약 횟수

그림 11은 채널 개수에 따른 처리량 비교이다. 여전히 1개 네트워크에 1개의 스마트 재머 동작하고 있다. 결과를 보면 제안하는 기법이 채널 개수에 상관 없이 더 훨씬 우수한 처리량을 보인다. 채널 개수가 많아짐에 따라 재머에 공격받을 확률은 비교 기법에 상관없이 낮아지지만 재머 공격 후 즉각적인 도약을 수행할 수 있는 제안 기법은 높은 처리율을 보이는 반면, IEEE 802.11h DFS는 Full DFS Test 소요 시간도 선형적으로 늘어남에 따라 처리율 상승 폭이 미미한 것을 확인할 수 있다. 앞의 그래프와 마찬가지로 휴지기간이 클수록 제안하는 기법에 유리하다.

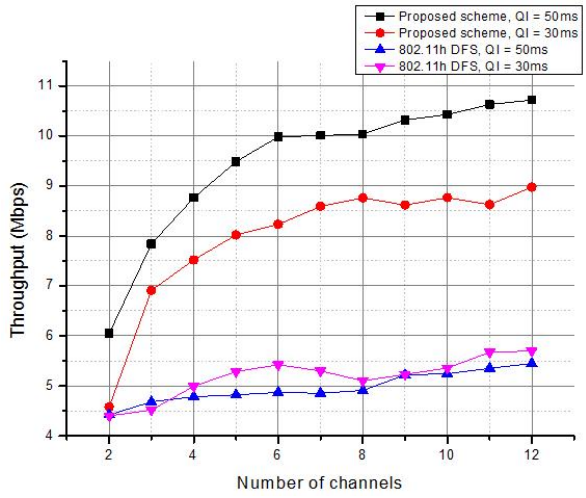


그림 11. 채널수에 따른 처리량

그림 12는 휴지기간을 좀 더 여러 구간으로 나누어 모의 실험을 수행하였다. 휴지기간이 작아질수록 두 기법의 성능이 비슷해지는 것으로 보일 수 있지

만 전체적으로는 처리량이 급속히 감소하는 현상이다. 따라서 채널 측정 신뢰도를 유지할 수 있는 범위의 휴지기간 값이 클 때 최적의 네트워크 처리량을 가져올 수 있다. 재머의 공격 시간을 비교해보면 재머가 한 번 채널을 공격하는 시간이 길수록 전체적으로 재밍되는 횟수가 줄어들기 때문에 보다 높은 성능을 보인다.

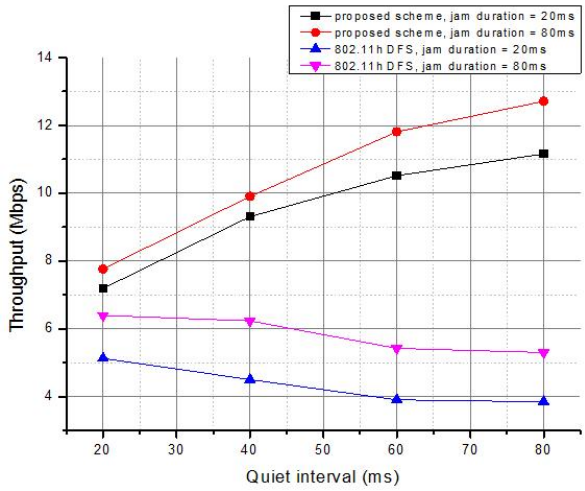


그림 12. 휴지기간 (QI)에 따른 처리량

그림 13은 앞에서 언급한 재밍 공격 시간에 따른 성능 비교이다. 전체적으로 재머의 공격 시간이 늘어날수록 재머에 공격당하는 횟수가 줄어들기 때문에 처리량이 상승하는 것을 확인할 수 있다. 재머의 속성과는 무관하게 여전히 처리량은 제안하는 기법이 우수하다. 또한 채널 개수에 따른 성능을 비교하면 채널 개수가 많을수록 재머에 노출될 확률이 낮기 때문에 더 높은 성능을 보이는 것을 확인할 수 있다.

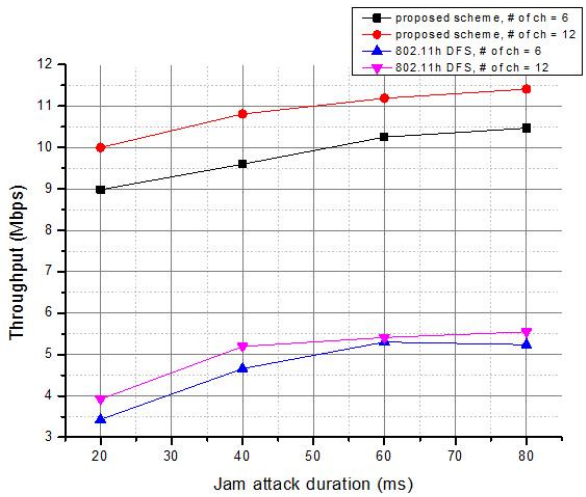


그림 13. 재머 공격 시간에 따른 처리량

본 논문에서 수행한 다양한 환경에 대한 모의 실험 결과를 종합적으로 살펴보면 표 2와 같다. 표2는 IEEE 802.11h의 네트워크 처리량을 1로 설정하였을 때 각 변수에 대한 상대적 처리량을 표시하고 있으며, 제안하는 기법이 재밍 환경에서 1.2 ~ 2배 정도 처리량이 향상됨을 확인할 수 있다.

표 2. 실험 결과 비교

변수	IEEE 802.11h	제안기법
채널 수	1	1.2 ~2.0
휴지 간격	1	1.2 ~2.0
재밍 시간	1	1.2 ~2.0

Ⅵ. 결 론

본 논문에서는 IEEE 802.11h의 DFS 알고리즘의 측정 기반의 채널 도약 기법이 재머 공격에 발생하는 성능 손실을 감소시키기 위한 즉각적인 채널 도약기법을 제안하였다. IEEE 802.11h의 DFS는 모든 채널을 측정한 후 채널을 다음 도약 채널을 선택하지만, 재머의 공격 시 전채널 측정에 오랜 시간이 소요되고 이후의 도약할 채널 정보를 전달하기 힘든 단점이 있다.

제안하는 기법은 앞으로 도약할 후보 채널로써 전체 채널을 매 비콘 구간에서 측정한다. 측정 후 비콘을 통해 도약할 채널을 지속적으로 갱신하며 재밍 시 그 채널로 즉각적으로 도약한다. 이를 통해 재머에 의한 네트워크 성능 손실을 최소화한다. 또한 재머의 공격이 없을 때에는 전체 채널을 측정하지 않고 기존의 IEEE 802.11h와 같이 현재 채널만을 측정한다. 이와 같은 두 가지 동작을 재머의 유무에 따라 적응적으로 취함으로써 높은 네트워크 처리량을 보장한다. 다양한 환경의 모의 실험을 통해 우리는 제안하는 기법이 기존의 기법에 비해 우수한 성능을 보임을 확인하였다.

참 고 문 헌

[1] Vishnu Navda, Aniruddha Bohra, Samrat Ganguly, and Dan Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in Proc. of INFOCOM '07, pp.2526~2530.

[2] K. Bicakci and B. Tavli, “Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks,” Computer Standards & Interfaces, vol. 31, no. 5, pp. 931‐941, 2009.

[3] Ramarkishna Gummadi, David Wetherall, Ben Greenstein, and Srinivasan Seshan, ″Understanding and mitigating the impact of RF interference on 802.11 networks,″ ACM SIGCOMM, vol. 37, pp.385-396, 2007.

[4] S. Khattab, D. Mosse, and R. Melhem, ″Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive?,″ in Proc. of the 4th international Conference on Security and Privacy in Communication Networks (SecureComm), pp.1-10, 2008.

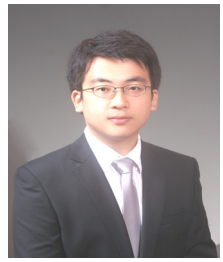
[5] IEEE 802.11h Std. IEEE 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe, 2003.

[6] IEEE 802.15 WG, ″Liaison Statement on the Compatibility between IEEE 802.11a and Radars in the Radio Location and Radion Avigation Service in the 5250-5350 MHz and 5470-5725 MHz Bands,″ IEEE 802.15-01/072, Jan. 2001.

[7] W. Xu, W. Trappe, Y. Zhang and T. Wood, ″The feasibility of launching and detecting jamming attacks in wireless networks,″ in Proc. ACM Mobi-Hoc, pp.46-57, 2005.

[8] A. Mishra, V. Shrivastava, D. Agarwal, S. Banerjee, S. Ganguly, “Distributed Channel Management in Uncoordinated Wireless Environments,” In Proc. Mobicom, pp.170-181, Sep. 2006.

정 승 명 (Seungmyeong Jeong) 준회원



2009년 8월 아주대학교 정보 및 컴퓨터공학부 학사

2009년 8월~현재 아주대학교 정보통신대학원 석사

<관심분야> Cognitive Radio, 국방전술통신

정 재 민 (Jaemin Jeung) 정회원

1998년 3월 육군사관학교 중국어학과 학사

2005년 3월 국방대학원 전산정보 석사

2009년 3월~현재 아주대학교 NCW학과 박사과정

<관심분야> Anti-jamming, Security, 국방전술통신

임 재 성 (Jaesung Lim) 종신회원

1983년 2월 아주대학교 전자공학과 학사

1985년 2월 KAIST 영상통신 석사

1994년 8월 KAIST 디지털통신 박사

1998년 3월~현재 아주대학교 정보통신전문대학원 교수

2006년 8월~현재 아주대학교 국방전술네트워크 연구센터장

<관심분야> 이동통신, 무선네트워크, 국방전술통신