WLAN 상에서의 분산 가상 재머 공격

이현록*,김광조*

*한국과학기술원 전산학과

Distributed Virtual Jammer Attack on WLAN

Hyunrok Lee* and Kwangjo Kim*

*Department of Computer Science, KAIST

요 약

최근 IEEE 802.11 (WiFi)에 기반한 많은 수의 무선 인터넷 액세스 포인트(Access Point)가 사람들이 많이 모이는 장소인 공항, 카페, 쇼핑몰 등에 핫스팟이라는 이름으로 설치되고 있다. 이런 무선 데이터 통신은 사용자의 편의성을 확대시켜 준 반면 기존의 유선망에서의 보안 문제와 더불어 무선이라는 미디어 특성으로 인한 새로운 보안 취약점 및 위협에 대해 고려해야 한다.

본 논문에서는 무선랜 상에서의 기존 서비스 거부 공격들에 대해 살펴보고 사용자의 이동성을 고려한 봇넷 공격을 기반으로 설계된 분산 가상 재머(Jammer) 공격 방식을 제안한다. 기존의 물리(Physical, PHY) 계층 및 MAC(Medium Access Control) 계층 공격에 비해 제안 공격은 별도의 재머(Jammer)가 필요 없는 한층 진보된 MAC 계층의 공격으로 이산 네트워크 시뮬레이션을 통해 해당 공격의 위험성과 강력함을 검증하고 향후 연구에 대해 논의한다.

Ⅰ. 서 론

최근 스마트폰, 태블릿 PC와 같은 모바일 기기들의 폭발적인 보급에 따라 무선 데이터 통신 또한 급속도로 증가하고 있다. 해당 모바일 기기들의 무선 데이터 통신을 지원하기 위해 IEEE 802.11 (WiFi)에 기반한 많은 수의 무선 인터넷 액세스 포인트(Access Point, AP)가 이동통신사들의 주도하에 사용자가 많은 장소인 카페, 백화점, 공항, 대학 캠퍼스 등에 경쟁적으로 설치되고 있다. 또한 개인 사용자들도 가정, 회사 등에 개인적으로 무선 공유기를 설치하여 사용함으로 인해 무선랜(Wireless Local Area Network, WLAN)의 밀집도가 높아지고 있으며, 이런 고밀집 WLAN에 대해 WiFi 정글 혹은 밀집하여 설치된 무선랜(Densely deployed WLAN)이라고 표현하고 있다. 하지만 이런 무선 인터넷 접속 가능 지역의 확장은 언제 어디서나 무선 데이터 통신을 할 수 있게 해주는 반면 여러 가지 새로운 보안 문제 또한 제기되고 있는 실정이다[1,2].

해당 보안 문제 중에서 네트워크 자원을 고갈시켜 서비스를 불능으로 만드는 서비스 거부 공격(Denial of Service, DoS)은 기존 유선랜에서도 연구가 많이 이루어진 분야이긴 하지만 무선랜에서는 무선 미디어의 작은 대역폭을 가지는 특성으로 인해 가용성의 저하가 쉬우므로 더욱 취약한 공격으로 여겨지고 있으며, 무선랜

상에서의 하나의 액세스 포인트를 MAC(Medium Access Control)계층 및 물리계층의 취약점을 이용하여 공격하는 DoS를 중심으로 한 선행 연구들이 수행되었다. 기존 연구들은 하나의 AP의 가용성 저하를 위해 고출력의 장비를 이용하거나 혹은 실험실 내부에서의 장비들을 AP에 연결한 뒤 공격기기를 지정하여 해당 AP의 서비스 거부 현상을 실험하였다. 해당 연구들은 별도의 장비가 오프라인에서 요구되거나 하나의 대상에 대한 고정 위치에서의 공격으로 다수의 모바일 기기 사용자의 이동성을 고려하지 않았을 뿐만 아니라 분산 서비스 거부 공격(Distributed Denial of Service, DDoS)가 일반화된 최근 동향을 반영하지 않고 있다. 따라서 무선 출력 신호의 강도를 가지고 해당 공격자의 위치를 파악하고 대응책을 마련할 수 있는 한계를 가진 공격 방식이다.

또한 재머(Jammer) 장비를 이용하여 무선망 자체를 무력화시키는 공격이 적대국가 및 테러리스트 등에 의해 시도되고 있으며 심지어 개인도 인터넷을 통해 쉽게 고출력의 재머를 구입하고 설치하여 공격 할 수 있는 상황이다[3]. 해당 공격에 대한 심각성은 인정하고 있지만 국내 전파법 제 58조에 의해 법적인 제제가 가능하고 별도의 장비가 필요하며 국지적인 공격이라는 한계 때문에 무선랜 상에서의 보안 문제를 다룰 때 후순위로 취급되는 경우가 많은 실정이다. 해당 공격에 있어 별도의 장비가 없이도 재머가 방해전파를 발생시키는 것만큼의 효과를 얻을 수 있는 공격방식이 있다면 해당 보안 위협은 심각성의 인지의 문제가 아닌 우선순위가 높은 보안 문제로 다뤄져야 할 것이다.

본 논문에서는 기존 연구들에서 제안한 방식들보다 한층 진보된 방식인 분산 가상 재머(Distributed Virtual Jammer) 공격을 제안한다. 기존의 공격에 비해 제안 공격 방식은 별도의 재머가 필요 없을 뿐만 아니라 실제 사용자들의 모바일 기기들에 감염된 봇넷을 기반으로 낮은 출력, 즉 공격자의 위치를 파악할 수 없을 정도로 낮은 신호 강도로 MAC 계층에서 분산 서비스 거부 공격을 수행하는 공격 방식이다. 해당 공격 방식은 이산 네트워크 시뮬레이션을 통해 특정 지역에 분포된 액세스 포인트 그룹 자체를 불능화시켜 해당 지역의 무선랜 서비스가 불가능한 상황까지 되는 위험성과 강력함이 있음을 검증한다. 시뮬레이션 결과 실제 많은 사용자가 모바일 기기를 통해 사용하고 있는 VoIP(Voice over IP) 서비스 및 VOD(Video On Demand) 스트리밍 서비스는 해당 공격을 통해 서비스가 불가능한 정도로 패킷 손실률(Packet Drop Ratio)이 높아지는 것을 보인다.

본 논문의 구조는 다음과 같다. 먼저 II 장에서 관련 연구를 살펴보고, III 장에서 본 논문의 제안 공격 방식에 대하여 기술한다. IV 장에서는 제안 공격을 시뮬레이션하고 분석하였으며, 마지막으로 V 장에서 본 논문의 결론과 향후 연구에 대하여 기술한다.

Ⅱ. 관련 연구

1. 국내 무선랜 현황

먼저 무선랜은 액세스 포인트의 운영방법에 따라 크게 중앙 관리 무선랜, 자유 설치 무선랜 두 가지로 나뉜다. 중앙 관리 무선랜은 학교 캠퍼스 혹은 큰 규모의 회사 사옥 등에 하나의 SSID를 가지는 AP를 설치하여

중앙에서 채널 정보 및 사용자를 제어하고 관리하는 방식을 말하고, 자유 설치 무선랜은 개인 혹은 단체가 임의의 SSID를 부여하고 원하는 위치에 설치하여 사용하는 방식이다. 두 방식 모두 네트워크를 개방 혹은 폐쇄 방식으로 운영할 수 있으며, 개방형의 경우에 사용자는 자신의 모바일 기기를 해당 AP에 연결하여 자유롭게 사용할 수 있다. 반면 폐쇄형의 경우에는 AP의 SSID를 숨기거나 무선랜 보안 방식인 MAC 주소 인증, WEP, WPA, WPA2 등을 적용하여 사용자의 접근제어를 하는 방식으로 대부분의 유료 핫스팟에서 채용하고 있는 방식이기도 하다. JiWire사에서는 각국의 WiFi 핫스팟에 대한 정보를 수집하여 관리하고 있는데 〔표 1〕은 현재 해당 회사의 "WiFi Finder"〔4〕에서 파악하고 있는 국내 핫스팟의 지역별 분포와 총 개수이다. 또한 (그림 1)은 방송통신위원회와 한국정보화진흥원에서 제공하는 앱인 Wi-Fi Explorer에서 서울 강남구 대치동의 AP 위치를 표시한 화면이다. 해당 자료들에서는 개인에 의해 운영되는 개별적인 AP에 대한 정보는 대부분 누락되어 있는 상태로 해당 부분까지 포함하면 현재 국내의 핫스팟은 굉장한 밀집도를 가진 네트워크 인프라스트럭쳐가 구성되어 있는 상황이다.

표 1. 국내 WiFi 핫스팟 지역 분포

지역	핫스팟 개수
서울특별시	54591
경기도	34149
인천광역시	16062
부산광역시	15080
대구광역시	10382
경상북도	7859
충청남도	7213
전라남도	7213
대전광역시	7203
경상남도	7177
전라북도	6355
강원도	5383
충청북도	5037
울산광역시	2692
제주도	2584
기타	1
총 합	186759

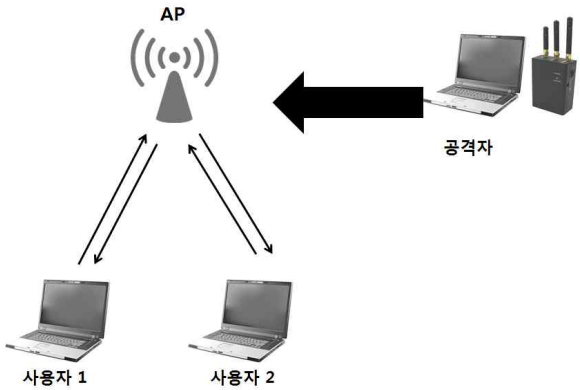
(그림 1) 방송통신위원회 WiFi Explorer

2. 무선랜에서의 PHY/MAC 계층 DoS/DDoS

기존에 일반적인 인터넷 서비스에 대한 DoS/DDoS 공격, 검출 및 대응책에 대한 연구들이 대부분이었으며 무선랜에 대한 해당 공격 연구는 IEEE 802.11 표준이 제정 후에 수행되었으며, 유선랜에 비해 상대적으로 많은 연구가 이루어지지 못한 분야로 최근 많은 연구가 진행되고 있다.

J. Bellardo와 S. Savage〔5〕는 802.11 MAC 계층의 DoS 취약점들에 대하여 조사하였으며, 총 4대의 클라이언트와 1대의 공격자를 둔 상황에서 Deauthentication 공격 및 가상 캐리어-센스 공격을 제안하고 실험으로 검증하였다. M. Bernash 등〔6〕은 액세스 포인트 자체의 취약점에 집중하여 다양한 상용 액세스 포인

트 제품들을 대상으로 서비스 거부 공격을 수행하고 하나의 악성 단말로 해당 공격이 성공적으로 수행되었음을 보였다. K. Bicakci와 B.Tavli[7]는 기존에 연구된 무선랜 상의 서비스 거부 공격들을 네트워크 계층 전반에 걸쳐 조사, 분류, 비교하였으며 가능한 대응책을 분류하였다. 위의 해당 연구들은 (그림 2)와 같은 실험환경에서의 서비스 거부 공격에 대한 연구로 고정된 단일 액세스 포인트에 대한 가용성 저하에 초점을 맞춘 연구이며, 단일의 공격기기를 통한 공격으로 모바일 기기 사용자의 이동성과 다수의 사용자를 고려하지 않았다. 또한 고밀집 무선랜 환경에서의 해당 공격 효율성에 대한 분석이 제외되어 있는 실정이다. 그리고 해당 공격에 대하여 알려진 무선랜 보안 솔루션을 통해 DeAuthentication, DeAssociation 공격 등의 대응책을 비교적 잘 마련할 수 있으며, Probe Request Flooding 경우에도 무선 출력 신호의 강도를 가지고 해당 공격자의 위치를 파악하는 등으로 적절한 대응책을 강구할 수 있다.



(그림 2) WLAN 환경의 DoS 공격 모델

재머 장비를 이용하여 무선망 자체를 무력화 시키는 공격은 X. Wu 등[8]이 4 가지 공격 방식으로 분류하였다. 첫째, Constant Jammer(CJ)는 연속적으로 랜덤 값을 가진 라디오 신호를 무선 미디어에 방출하는 방식이고, 둘째 Deceptive Jammer(DJ)는 CJ와 유사한 방식이지만 전송되는 라디오 신호의 비트가 랜덤 값이 아닌 경우이다. 셋째, Random Jammer(RJ)는 공격자가 라디오 신호를 특정 시간동안 방출하다가 특정 시간 동안 중지하는 것을 랜덤하게 반복하는 공격방식이고, 마지막 Reactive Jammer(RJ)는 무선 채널을 지속적으로 감시하고 있다가 전송 패킷 신호를 검출하게 되면 라디오 신호를 방출하는 방식이다. 재밍 공격은 국내 전파법으로 금지되고 있고 별도의 장비가 필요한 공격으로 라디오 신호 출력이 작은 경우 한정된 지역에 대한 공격만 이루어 질 수 있으며, 넓은 지역에 영향을 주기 위해서는 고가의 고출력 장비가 필요한 방식이다.

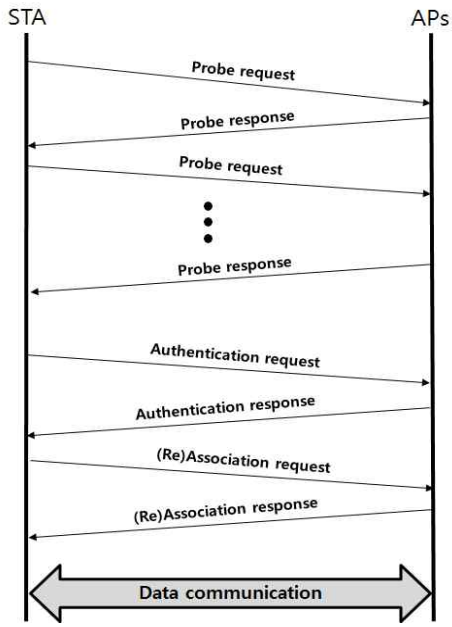
Ⅲ. 제안 공격 방식

1. Probe Request Flooding(PRF)

본 논문의 분산 가상 재머 공격에서 사용되는 MAC 계층의 취약점은 Probe 요청/응답을 기반으로하는

PRF 공격이다. MAC 계층의 공격 방식은 1) Authentication Request Flooding, 2) Association Request Flooding, 3) Probe Request Flooding 이 있는데, 1)은 무선랜에 참여하기 위해 사용자 인증을 위해 보내는 AUTH_REQ 메시지를 연속적으로 보내기만 하여 가용자원을 고갈 시키는 방식이고, 2)는 무선랜에 주소를 할당받기 위해 ASSOC_REQ 메시지를 연속적으로 보내기만 하여 가용자원을 고갈 시키는 방식이다. 1), 2) 방식은 IEEE 802.11i 보안표준에서 해당 공격의 대응책을 제시하고 있다. 하지만 3)PRF의 경우에는 보안표준 제정 시에도 논외로 취급된 공격 방식으로, 원천적이지만 강력한 MAC 계층 공격 방식이다.

무선랜을 발견하고 사용하기 위해서는 능동모드, 수동모드 두 가지의 모드가 존재하는데 수동모드는 거의 쓰이지 않는 방식이고 사용자 기기에서 AP를 발견하기 위해 먼저 Probe 요청 신호를 보내는 능동모드가 현재 일반적인 방식이다. (그림 3)에 나타난 것처럼 사용자 기기(STA)는 AP들에게 제일 처음 Probe Request를 브로드캐스트하게 되면 AP들은 Probe Response를 보내고 이를 받은 STA는 AP에게 이후의 과정을 처리하게 된다. 하지만 Probe 요청 신호만 지속적으로 보내게 되면 네트워크 자원이 고갈되어 통신 불능 상태에 빠지게 된다.



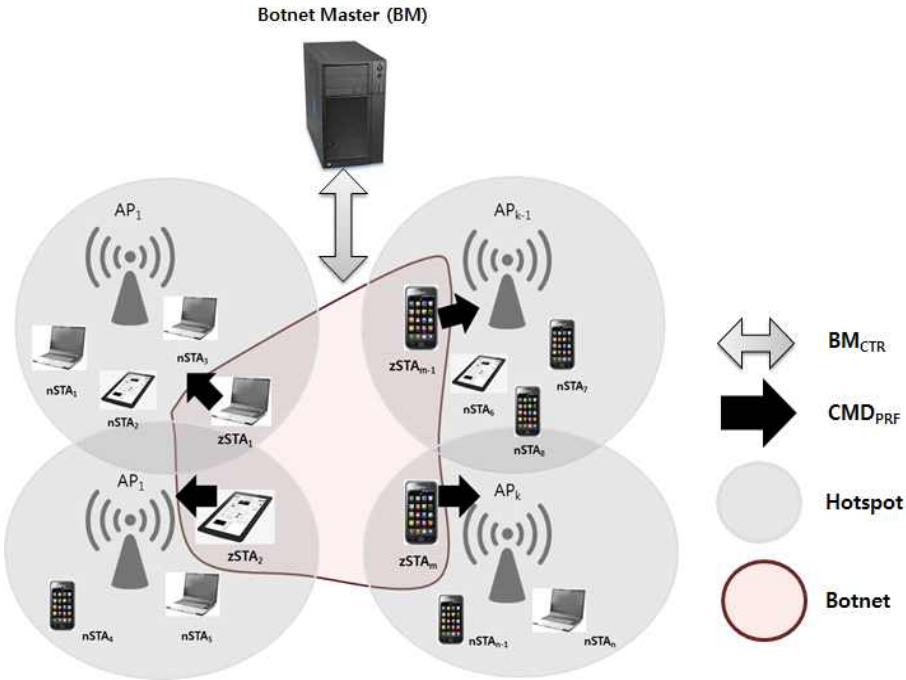
(그림 3) WiFi에서 사용자기기(STA)와 액세스 포인트 간의 통신을 위한 절차

2. 제안 공격 모델

분산 가상 재머 공격은 (그림 4)와 같은 공격 모델을 구성하게 된다. 해당 공격 모델에서 액세스 포인트는 AP_1부터 AP_k까지 존재 가능하며 각 AP들에 정상적인 사용자인 1부터 n개의 nSTA가 일반적인 무선 통신을 수행하고 있는 것으로 가정한다. 또한 각 nSTA는 이동성을 가지고 있으며 특정 시간 이후에는 이동하고 다른

AP와도 통신 가능한 개방형 구조이다. 해당 모델에서 zSTA는 악성 봇에 감염된 1부터 m개의 좀비 STA로 가정하였으며, 해당 zSTA들은 봇넷 마스터 BM에 의해 BM_{CTR} 명령전달 채널로 제어된다. 이때 nSTA, zSTA는 사용자가 일반적으로 사용하는 노트북 PC, 태블릿 PC, 스마트 폰 등으로 가정하였다.

zSTA는 PRF를 BM이 지정한 순간에 CMD_{PRF}를 통해 실시하게 되는데 이때 m개의 충분한 zSTA가 존재하는 경우에는 정상적인 Probe 요청 주기를 가지고 요청을 하더라도 PRF 공격의 목적을 달성할 수 있는 모델이다. 이때 정상적인 Probe 요청 주기는 [9]에 따르면 MinChannelTime(MinCT)가 10ms에서 25ms의 범위를 가지고, MaxChannelTime(MaxCT)는 20ms에서 50ms의 범위를 가진다. 따라서 본 모델에서는 기존 무선랜의 서비스 거부 공격에 사용되는 굉장히 빠른 시간 내에 많은 양의 Probe 요청에 의한 무선 네트워크 가용성 저하는 고려하지 않고 최소 10ms 최대 50ms의 정상적인 Probe 요청만으로도 네트워크 자원의 고갈을 유도할 수 있는 강력한 공격 방식을 제안한다. 또한 해당 공격 모델은 기존의 재머와 같은 별도의 장비의 설치가 필요 없기 때문에 공격자는 BM을 이용하여 온라인상에서 재머를 가동시키는 것과 같은 효과를 가지고 공격 가능한 모델이다. 더불어 정상적인 Probe 요청 주기 내에서 분산된 공격을 하게 됨으로 인해 무선 신호의 강도 측정을 통한 zSTA의 검출이 매우 어려운 공격이다.



(그림 4) 분산 가상 재머 공격 모델

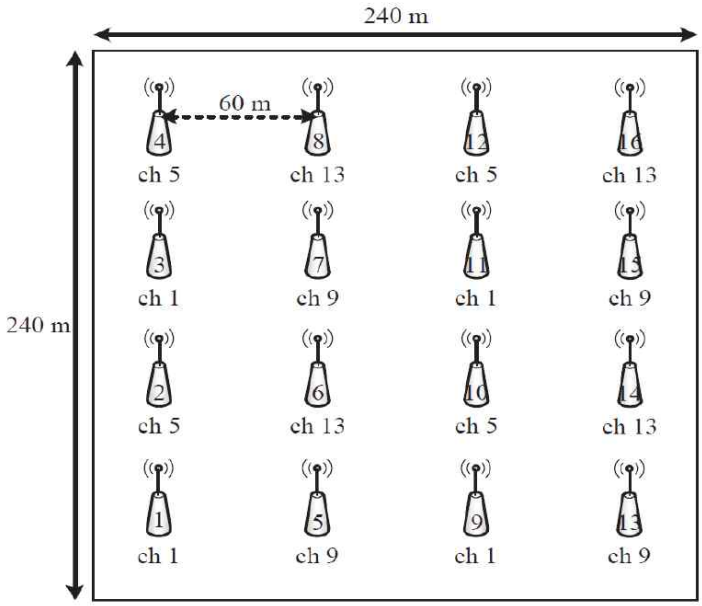
Ⅳ. 제안 공격 모델 분석

1. 시뮬레이션 모델

본 논문에서 제안한 분산 가상 재머 공격 모델을 분석하기 위해 이산 네트워크 시뮬레이터 EXata[10]를 사용하여 MAC 계층에서의 처리율(throughput), 패킷 손실율(Packet loss rate), 단대단 지연시간(end to end delay), 패킷 드랍(packet drop)에 대한 평가를 실시하였다. 해당 평가에는 모바일 기기들에서 가장 많이 활용되는 서비스인 VoIP 및 VOD 스트리밍 서비스를 고려하여 해당 서비스가 제공될 수 있는 수준인가를 판단하여 해당 네트워크의 가용성이 충분한지를 판별한다. 해당 시뮬레이션에 사용된 파라메터는 [표 2]와 같으며, 사용된 토폴로지는 그리드(Grid) 방식으로 (그림 5)와 같이 배치하였다.

[표 2] 시뮬레이션 파라메터

파라메터 (Parameters)	값 (Values)
Radio Type	802.11a/g
Propagation	TwoRayGround
Antenna	Omni-directional
Data Rate	54 Mbps
RTS/CTS	Disabled
No. of Channels	4 Channels in 2.4 GHz bandwidth (1,5,9,13)
Attack Interval	10, 50ms
Mobility	Random Way Point (Pause Time : 30sec)
Application	VOD Streaming, mVoIP
# of Attackers	Varying
Simulation Time	600sec



(그림 5) 시뮬레이션 토폴로지

해당 토폴로지 상에 AP는 고정된 16개를 설치하고 시뮬레이션의 단순화를 위해 각 AP마다 nSTA가 하나씩 있도록 설정하고, zSTA는 악성봇의 감염이 시간이 흐르면 늘어나는 것을 고려하여 가변적으로 설정할 수 있도록 하였다. 인접한 AP간의 거리는 75m로 하였고 대역폭은 ISM(Industrial, Scientific, and Medical)밴드의 2.4GHz로 설정하였으며 4개의 채널을 사용하였다. zSTA는 이동성을 고려하여 사람의 보행속도인 1m/sec 혹은 2m/sec 중 랜덤하게 선택하고, 30초간 머무는 시간 뒤에 다시 이동하는 모델을 적용하였다. 무선 라디오 타입은 현재 가장 많이 보급되어 있는 54Mbps의 IEEE 802.11g를 사용하고, 시뮬레이션 시간은 600초로 설정하여 실험하였다.

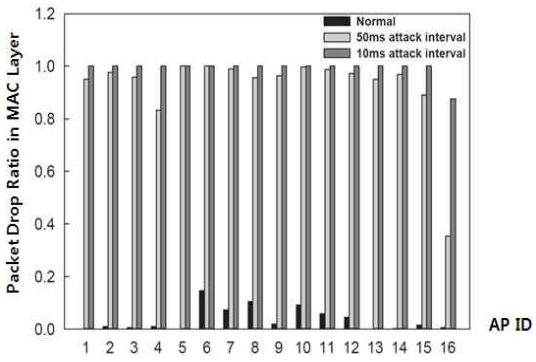
2. 시뮬레이션 결과 및 분석

zSTA의 수를 0부터 증가시켜 나가면서 개별 시뮬레이션 결과 악성봇에 감염된 20개의 zSTA가 있는 경우 BM으로부터 PRF 명령을 받아서 정상적인 Probe 요청 주기의 최소값으로 설정했던 10ms, 최대값으로 설정했던 50ms 주기로 공격했을 때, 모든 AP에서 서비스 불능상황에 도달하였다. VOD 스트리밍 서비스의 경우에는 10ms, 50ms PRF 공격시 평균적으로 88% 이상의 패킷이 유실되어 서비스가 불가능했으며, VoIP 서비스에서는 10ms PRF 공격시 평균 98%의 패킷 유실이 있었으며, 50ms PRF 공격시에는 평균 90%의 손실이 발생했다. 따라서 해당 시뮬레이션 환경에서 20개의 zSTA가 존재할 경우 분산 가상 재밍 공격이 성공하는 것을 알 수 있었다. 해당 시뮬레이션의 상세 결과를 정리하면 〔표 3〕과 같다.

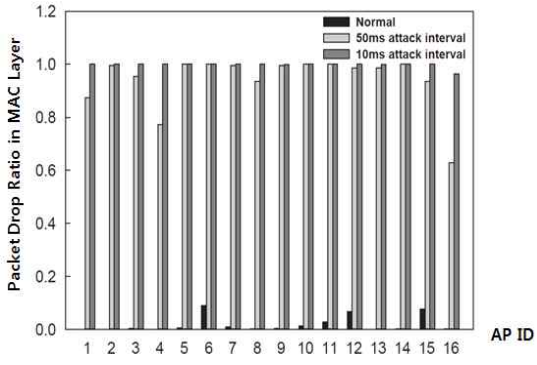
〔표 3〕 시뮬레이션 상세 결과 (20 zSTA)

	공격 주기(ms)	패킷손실(%)	처리율(bps)	단대단 지연(ms)	MAC 패킷 손실 수
VOD 스트리밍	No attack	3.7	394661	2.9	1101
	50ms	88.0	45726	1128.9	26374
	10ms	88.9	48944	4672.9	27211
VoIP	No attack	1.9	62775	1.6	577
	50ms	90.6	738	1163.5	27049
	10ms	98.8	5978	2844.3	27236

해당 데이터를 기반으로 zSTA가 시뮬레이션 환경에 전혀 존재하지 않는 상황, zSTA의 PRF가 10ms, 50ms 간격으로 이루어질 때의 패킷 손실율에 대하여 각 AP별로 계산하여 그래프로 나타내면 VOD 스티리밍 서비스에서의 손실율은 (그림 6)과 같고, VoIP 서비스에서의 경우는 (그림 7)과 같으며, 각 AP에서의 손실율이 서비스 종류에 관계없이 1.0에 근접하여 제안한 분산 가상 재머 공격이 성공적으로 이루어졌음을 알 수 있으며, 서비스 불능 상황임을 판단할 수 있다.



(그림 6) 패킷 손실율(VOD 스트리밍)



(그림 7) 패킷 손실율 (VoIP)

V. 결 론 및 향후 연구

본 논문에서는 IEEE 802.11 (WiFi)에 기반한 무선랜 상에서 기존의 서비스 거부 공격이나 재머 공격보다 진보된 MAC 계층에서의 분산 가상 재머 공격 방식을 제안하였고, 이산 네트워크 시뮬레이터를 통해 해당 공격이 유효함을 검증하고 분석하였다. 제안 공격 방식은 정상적인 Probe 요청 주기 내에서 수행되기 때문에 기존의 무선랜 보안 대책으로 감지 및 방어가 매우 힘든 공격이며, 또한 별도의 장치가 없이도 공격자가 온라인상에서 봇넷 마스터만을 조정하여 재밍의 효과를 낼 수 있는 새로운 공격 방식이다.

향후 연구로는 실제 네트워크 환경과 동일한 토폴로지를 생성하여 동일 공격을 시뮬레이션하여 해당 공격의 유효성을 달성하고, 실제 테스트 베드 구성을 통하여 실험결과를 얻는 과정이 남아 있다. 또한 해당 공격을 효과적으로 막을 수 있는 대응책에 대한 연구도 반드시 필요하다.

참 고 문 헌

[1] R. Housley and W. Arbaugh, "Security problems in 802.11-based networks", *Communications of the ACM*, 46(5):31-34, 2003.

[2] O.P. Sarmiento, F.G. Guerrero, and D.R. Argote, "Basic security measures for IEEE 802.11 wireless networks", *Revista Ingenieria E Investigacion*, 28(2):89-96, 2008.

[3] theJammerWorld, "http://www.thejammerstore.com/".

[4] JiWire Wi-Fi Finder, "http://v4.jiwire.com/search-hotspot-locations.htm".

[5] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks : Real vulnerabilities and practical solutions", USENIX Security Symposium, pp. 15-28, Washington, D.C., US, August 2003.

[6] M. Bernaschi, F.Ferreri, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks", *Wireless Networks*, 14(2):159 - 169, Kluwer Academic

Publishers, 2008.

[7] K. Bicakci and B. Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks", *Computer Standards & Interfaces*, 31:931 - 941, Elsevier, 2008.

[8] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", in MobiHoc 05, pp 46-57, Urbana-Champaign, Illinois, USA, May 25-27, 2005.

[9] Castignani G, Montavont N, Arcia-Moret A. "Analysis and evaluation of WiFi scanning strategies", *Proceedings of the 5th Conference on Electrical Engineering*, Merida, 2010.

[10] EXata 2.1. "http://www.scalable-networks.com/exata/".