IEEE 802.11 네트워크에서의 복제된 AP 탐지 공격으로부터의 방어 대책

고윤미*, 김진희*, 권경희*
*단국 대학교 전자계산학과
e-mail : allice8105@dankook.ac.kr

Defense Tactics Against the Attack of Cloned Access Point in IEEE 802.11 Networks

Yun Mi Go*, Kyuug-Hee Kwon*
*Dept. of Computer Science, Dankook University

요 약

무선 네트워크 환경에서 합법적인 AP(Access Point)의 MAC 주소, SSID(Service Set Identifier), 채널등의 정보를 이용하여 복제된 AP(Cloned Access Point)를 만들 수 있다. 복제된 AP 는 합법적인 AP 와 연결되어 있는 무선 스테이션들의 연결 설정을 끊고 자신과 연결 설정을 하게 한다. 무선 스테이션들이 복제된 AP 와 통신을 하게 되면서 많은 공격으로부터 노출되게 된다. 본 연구에서는 복제된 AP 가 설치되었을 때 무선 스테이션들이 합법적이 AP 의 비콘 프레임과 복제된 AP 비콘 프레임의 시퀀스 번호를 이용하여 복제된 AP 을 판별하였다. 시뮬레이터 NS-2 를 이용하여 실험한 결과 본 논문에서 제안하는 메커니즘을 통해 무선 스테이션들이 복제된 AP 의 등장을 판별할 수 있게 되어 보다 안전한 무선랜 환경을 구축할 수 있게 되었다.

1. 서론

무선 네트워크 보안에서 문제 중 하나가 복제된 AP (Access Point)이다. 복제된 AP 는 합법적인 AP 에서 오는 프레임을 가지고 그 AP 의 정보를 추출하여 똑같이 복제하는 것이다. 이러한 복제된 AP 는 합법적인 AP 와 연결설정이 되어있는 무선 스테이션들의 연결설정을 강제적으로 끊고 자신과 연결 설정이 이루어 지도록 한다. 이러한 공격으로 인해 무선 스테이션과 AP 와 주고받은 중요한 정보가 외부로 유출될 문제가 생기게 된다.

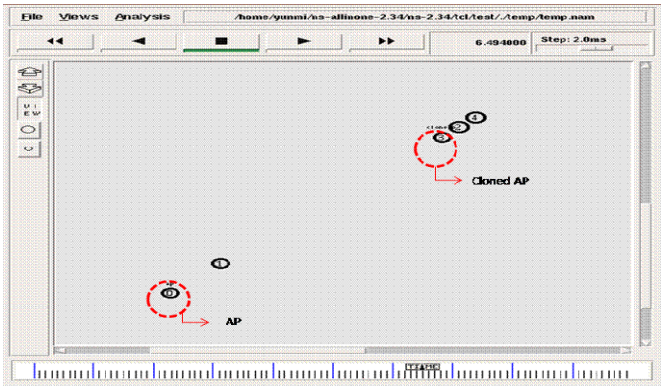
그러나 현재는 복제된 AP 설치에 대한 공격에 대해 조치를 취하고 있지 못하고 있는 현실이다. 따라서 복제된 AP 의 설치를 탐지하여 공격에 대응하는 것이 시급하다. 본 연구에서는 합법적인 AP 와 복제된 AP 에서 오는 비콘 프레임을 이용하여 복제된 AP 를 탐지한다.

2. 연구배경

공격자는 패킷 스니퍼를 이용하여 모든 프레임을 캡쳐하여 볼 수 있다. 이렇게 모든 프레임을 이용하여 무선랜 내부에 설치되어 있는 합법적인 AP 의 구성을 복제하여 복제된 AP 를 만든다. 공격자가 복제된 AP 를 설치하는 이유는 크게 3 가지고 볼 수 잇다. 첫 번째로는 복제된 AP 에 무선 클라이언트들과 연결이 이루어지게 한다. 이렇게 연결설정이 이루어진 무선 스테이션들은 복제된 AP 와 패킷을 주고 받기 때문에 이것을 통해 패킷 캡쳐와 분석을 할 수 있게 된다. 또한 복제된 AP 를 설치하게 되면 합법적인 AP 와 무선 단말들의 연결설정을 방해하게 되므로 합법적인 AP 를 고립시키는 결과를 가져온다. 마지막으로 복제된 AP 를 설치하게 되면 합법적으로 서비스를 받는 무선 스테이션들이 아닌 불법 무선 스테이션들도 서비스를 사용할 수 있게 된다.

3. 시뮬레이션 및 성능 분석

본 논문에서는 네트워크 시뮬레이터인 NS-2[1]를 이용하여 합법적인 AP 와 복제된 AP 판별하였다.



(그림 1) 네트워크 모델

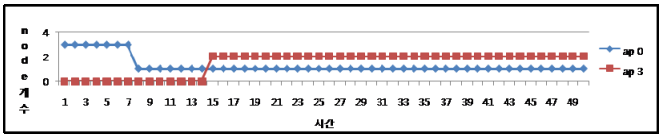
(그림 1)은 시뮬에이션에 사용된 네트워크 모델이다. 5 개의 노드가 위치해 있고 0 번 노드는 합법적인 AP 이고, 3 번 노드는 복제된 AP 이다. 나머지 1.2.4 노드는 무선 스테이션으로 이루어져 있다. 합법적인 AP 인 0 번 노드는 2 초 후부터 비콘 프레임을 보내기 시작한다. 그 후 1.2.4 번 노드 무선 스테이션들은 0 번 노드와 연결설정이 이루어진다. 합법적인 AP 인 0 번노드를 복제한 복제된 AP 3 번 노드는 7 초 후 비콘 프레임을 보내게 된다. 이때 복제된 AP 3 번 노드는 합법적인 AP 0 번 노드 보다 신호강도가 세게 설정하였다. 시뮬에이션에 사용된 무선 구간이 대역폭과 지연, 시뮬레이션 총 시간등 표 1 에 나타난 바와 같다.

<표 1>시뮬레이션 환경

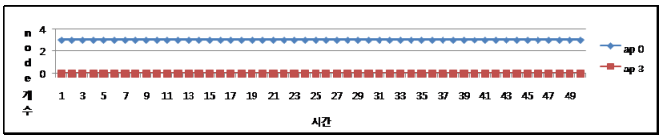
파라미터	설정값
Simulator	NS-2.34
Application	TCP,CBR
MAC	802.11 DSSS (Direct Sequence Spread Spectrum)
채널 접근방식	CSMA/CA
비콘간격	100ms
토폴로지	670*670 grid
총 시뮬레이션 시간	50s

시뮬레이션에서 합법적인 AP 와 무선 스테이션의 연결설정과정은 스캐닝을 통해 신호 강도가 가장 강한 AP 를 하나 선택한 후 무선 스테이션이 네트워크에 결합 하기전 인증과정을 거친 후 결합한다. 이때 네트워크의 존재를 알리는 비콘 프레임[2]의 MAC 헤더 부분에는 시퀀스제어필드가 있다. 이 필드는 12 비트의 시퀀스 번호 필드가 있고 이 시퀀스 번호는 처음 시작된 비콘 프레임 시퀀스 번호로부터 순차적으로 증가한다. 무선 스테이션이 프레임을 수신하였을 때 시퀀스 번호를 조사해 보면 전 프레임과 지금 수신한 프레임의 차이가 1 일 경우가 88.8%, 2 일 경우와 0 일 경우 7.9% [3][4]이다. 따라서 합법적인 AP 에서 오는 비콘 프레임에서 전 프레임과 지금 수신한 프레임의 시퀀스 차이는 2 보다 작다.

시뮬레이션에서 복제된 AP 가 설치되면 복제된 AP 도 비콘 프레임을 브로드캐스트 한다. 무선 스테이션들은 이 프레임을 수신하게 된다. 이때 이때 합법적인 AP 에서 오는 프레임과 복제된 AP 에서 오는 프레임의 소스 주소는 같은 MAC 으로 표시된다. 그러나 프레임에 표기된 시퀀스 번호가 전 프레임과 지금 수신한 프레임의 차이가 2 이상인 다른 번호가 나타나게 된다. 이러한 현상을 이용하여 무선 스테이션들이 기존에 받았던 합법적인 AP 들의 비콘 프레임을 기준으로하여 복제된 AP 의 비콘 프레임을 판별할 수 있게 된다. 이에 본 논문에서 제안하는 메커니즘은 복제된 AP 의 프레임을 받게 되면 무선 스테이션들은 이 프레임을 무시한다. 그 결과 복제된 AP 는 어떤 무선 스테이션들과 연결설정이 이루지지 않게 하여 고립상태에 빠지게 만든다. (그림 2)은 현재 복제된 AP 가 설치 되었을 때 합법적인 AP 0 과 연결설정을 끊고 신호 강도가 강한 복제된 AP3 으로 연결설정이 이루어지고 있다. 본 논문에서 제안한 메커니즘을 이용하였을 때 복제된 AP3 을 발견하여 연결설정이 이루어지지 않고 있음을 (그림 3) 를 통해 확인할 수 있다.



(그림 2) AP 에 연결된 노드 개수



(그림 3) 제안하는 메커니즘에 사용할 때 AP 에 연결된 노드 개수

4. 결론

IEEE 802.11 무선네트워크 환경에서 무선 클라이언트들은 합법적인 AP 인지 아닌지 인증하지 않아 복제된 AP 에 대한 공격에 취약하다. 논문에서는 복제된 AP 에 대한 탐지 및 공격을 무효화 시키는 방법을 제안하였다.

향후 연구 과제로는 본 논문에서 고려 되지 않은 상황인 공격자가 합법적인 AP 의 비콘 프레임의 시퀀스 번호까지 복제하였을 때에 대한 복제된 AP 탐지 및 방어에 대한 메커니즘을 찾는 것이다.

참고문헌

[1] Network Research Group, Lawrence Berkeley Nation Laboratory Network simulator version 2(NS-2) URL : http://www.isi.edu/nsnam/ns

[2] IEEE802.11,"Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specification,"June.2007.

[3] F.Guo and T.cker Chiueh, "Sequence number-based MAC address spoof detection" in Proceeding of the 8th International symposium on Recent Advances in Intrusion Detecion, Seattle, WA,USA,Sept.2005

[4]Bansl.R, Tiwari.S , Bansl.D."Non-cryptograaphic methods of MAC spoof detection in wireless LAN " 16th IEEE international Conferences , ICON , Dec.2008.