ISSN 2383-6318(Print) / ISSN 2383-6326(Online)
KIISE Transactions on Computing Practices, Vol. 23, No. 7, pp. 397-407, 2017. 7
https://doi.org/10.5626/KTCP.2017.23.7.397

라즈베리파이를 이용한 전용 WIPS 센서 구현

(Implementing a Dedicated WIPS Sensor Using Raspberry Pi)

윤 광 욱 † 최 석 환 † 안 상 언 † 김 정 구 †† 최 윤 호 †††
(Kwang-Wook Yun) (Suck-Hwan Choi) (Sang-Un An) (Jeong-Goo Kim) (Yoon-Ho Choi)

요 약 무선 네트워크를 이용한 사용자의 업무 편의성 및 효율성이라는 순기능은 보안 위협이 발생하면 심각한 네트워크 자원 가용성의 침해와 더불어 중요한 기업 정보의 유출로 이어질 수 있다. 특히 무선 AP(Access Point)를 통해 보안 취약점을 악용한 다양한 보안 공격과 이로 이한 피해가 늘어나고 있다. 이러한 다양한 공격에 대항하고 내부망을 보호하기 위해 공공기관 및 기업에서 WIPS(Wireless Intrusion Prevention System)를 도입하는 사례가 늘어나고 있다. 하지만, WIPS 솔루션 도입시 고려해야 할 높은 비용은 개인 또는 소규모 회사에서의 WIPS 솔루션 도입을 방해하는 주요 이슈이다. 본 논문에서는 WIPS 솔루션 도입에 따른 비용 문제를 절감하고 다양한 무선랜 보안 위협들을 차단하기 위한 라즈베리파이를 이용한 WIPS 센서 구현 방안을 제안한다. 이를 통해 비교적 낮은 비용으로 기업 정보를 보호하고 서비스 연속성을 제공할 수 있을 것으로 기대한다.

키워드: 무선 네트워크, WIPS, 침입탐지, 침입차단

Abstract Wireless networks make the users' work more convenient and efficient, but such networks can impair the availability of network resources and can cause leakage of important corporate information when there are security threats. In particular, damage has increased because of security attacks that take advantage of the vulnerabilities created by a wireless AP (Access Point). Public organizations and companies have gradually selected the WIPS (Wireless Intrusion Prevention System) to block wireless security threats and protect the internal network. However, it is very costly for other organizations and companies to introduce the WIPS solution. This paper proposes implementing a WIPS Sensor by using Raspberry Pi to reduce these costs and to block the various wireless LAN security threats. This implementation would protect corporate information and provide consistent services at a relatively reasonable price.

Keywords: wireless network, WIPS, intrusion detection, intrusion protection

· 본 연구는 한국연구재단 논문연구과제(NRF-2015R1D1A1A01057888) 지원으로 수행되었습니다.

† 학생회원 : 부산대학교 전자전기컴퓨터공학부
dnr9198@gmail.com
01055335847a@gmail.com
qnfpdhrwka1@gmail.com
†† 종신회원 : 부산대학교 전자전기컴퓨터공학부 교수
kimjg@pusan.ac.kr
††† 종신회원 : 부산대학교 전자전기컴퓨터공학부 교수(Pusan Nat'l Univ.)
(Corresponding author임)
yhchoi@pusan.ac.kr

논문접수 : 2016년 11월 23일
(Received 23 November 2016)
논문수정 : 2017년 4월 10일
(Revised 10 April 2017)
심사완료 : 2017년 4월 12일
(Accepted 12 April 2017)

정보과학회 컴퓨팅의 실제 논문지 제23권 제7호(2017. 7)

1. 서 론

무선 네트워크와 무선 디바이스가 제공하는 사용상의 편리성, 이동성, 생산성, 비용 효율성, 그리고 다른 네트워크와의 통합 용이성 등으로 인해 무선 네트워크를 이용한 사용자의 서비스 이용 빈도가 나날이 증가하고 있다. 특히, 스마트폰의 높은 보급률과 BYOD(Bring Your Own Device) 현상으로 인해 무선 디바이스의 사용 및 이를 활용하여 업무를 보는 사용자가 급증하는 추세이다.

하지만 무선 네트워크를 이용한 사용자의 업무 편의성 및 효율성이라는 순기능은 올바른 네트워크 접근 제어가 이루어지지 않는다면 심각한 네트워크 자원 가용성의 침해와 더불어 중요한 기업 정보의 유출로 이어질 수 있다. 특히 무선 AP(Access Point)를 통한 사용자 단말의 내부 네트워크 연결 시 다양한 보안 취약점이 존재하며 이를 악용한 다양한 보안 공격과 이로 이한 피해가 늘어나고 있다[1-3].

예를 들어, 기업 내 보안 설정을 누락하거나 보안 정책에 위반되는 보안 설정으로 인해 보안 위협에 노출된 AP(Access Point)가 존재하는 경우 인가되지 않은 사용자가 기업 내부 네트워크에 침입하는 경우가 발생 할 수 있으며, 공격자가 인가된 AP의 MAC 주소(Media Access Control Address)와 SSID(Service Set Identifier)를 갖는 패킷을 생성하여 무선 통신을 방해하는 AP MAC 위장(AP MAC Spoofing) 공격이 발생할 수 있다. 이들 공격이 성공할 경우 기업 내부 기밀 정보의 유출과 업무 서비스의 중단 등 심각한 피해로 이어질 수 있다.

이러한 무선 AP를 이용한 다양한 공격에 대항하고 내부망을 보호하기 위해서는 접속 단말에 대한 보안 취약성 관리와 더불어 기업 내부 망에 대한 침입 탐지 및 차단을 통한 인가되지 않은 접근 혹은 인가된 사용자의 비정상적인 접근을 차단하기 위한 보안 솔루션의 도입이 필요하다. 이를 위해 최근 들어 대다수의 기업과 공공기관들은 무선 보안 솔루션인 WIPS(Wireless Intrusion Prevnetion System) 솔루션을 도입하는 추세이다.

WIPS 솔루션은 서버 제품과 센서 제품으로 구성되며 서버의 경우 허용된 단말에 대한 리스트인 화이트리스트(화이트리스트) 관리 등 WIPS 센서의 차단 정책 및 운영을 관리하는 기능을 담당하며 WIPS 센서의 경우 실제로 무선 AP를 통해 접근하는 인가된 혹은 비인가된 접속에 대한 관리를 수행한다.

WIPS 센서는 IEEE 802.11 상에서 사용되는 2.4Ghz (802.11b/g), 5.0Ghz(802.11a) 대역의 채널을 동시에 탐색하여 802.11 MAC 프레임을 수집한다. 다음으로, 수집된 데이터의 제어 관련 정보를 담고 있는 Frame Control 필드 내 Type과 Subtype을 분석하여 연결을 허용하거나 차단할지 결정한다. 예를 들어, 관리 유형의 데이터가 초당 4개 이상 지속적으로 발생 시 공격으로 판단(탐지)하고 해당 연결을 차단하는 기능을 수행하는 것이 가능하다.

현재가지 개발되어 상용화한 WIPS 솔루션의 경우, 예를 들어 WIPS 센서 경우 약 100만원 가량의 고가의 설치비용과 유지비용으로 인해 개인 또는 소규모 회사에서 사용하기 힘든 실정이다[4]. 본 논문에서는 저가형 초소형 컴퓨터로 알려진 라즈베리파이를 이용하여 WIPS 센서 구현 방안을 제안하고 대표적인 무선 보안 위협들에 대한 탐지 및 차단 기능을 통해 성능을 검증한다.

본 논문의 구성은 다음과 같다. 2장에서는 WIPS 센서 성능 검증을 위해 사용된 잘 알려진 무선랜 공격 유형과 WIPS 센서의 공격 탐지 및 차단 기능에 대해 기술한다. 3장에서는 3가지 WIPS 센서 구현 형태의 특징에 대해 살펴보고, 4장에서는 제안하는 시스템의 구성요소와 상세한 구현 방안에 대해 기술한다. 5장에서는 실험을 통한 성능 분석, 마지막으로 6장에서 결론짓는다.

2. 배경 지식

2.1 무선랜 보안 위협

일반적으로 WIPS는 불법 AP(Rogue AP), 비인증 결합(Unauthorized Association), 임시 연결(Ad hoc Connection) 등의 보안 위협을 탐지하고 차단하는 기능을 제공한다[5,6]. 본 논문에서 WIPS 센서의 성능 측정을 위해 사용한 무선랜 상의 주요 보안 위협을 피해 상황에 따라 분류하면 다음과 같다[7,8].

- 정보(내부 자료, 계정 정보 등) 유출
  - **불법 AP(Rogue AP):** 기업의 허가 없이 임의로 또는 악의적인 목적으로 설치한 AP
  - **잘못 설정된 AP(Mis-configured AP):** 보안 설정을 누락하거나 보안 정책에 위반되는 보안 설정으로 인해 보안 위협에 노출된 AP
  - **잘못 결합된 클라이언트(Client Mis-Association):** 인가된 클라이언트가 비인가 AP에 접속한 상황.
  - **비인증 결합(Unauthorized Association):** 비인가 클라이언트가 인가된 AP에 접속한 상황-
  - **Honeypot AP:** 내부 네트워크의 AP와 동일한 SSID를 갖도록 구성된 AP
  - AP MAC 위장(AP MAC Spoofing): 공격자가 인가된 AP의 MAC 주소와 SSID를 갖는 패킷을 생성하여 무선 상의 통신을 방해하는 상황
- 네트워크 서비스 장애
  - **임시 연결(Ad hoc Connection):** Peer-to-peer 연결을 통해 직접 접속한 단말을 경유하여 내부 네트워크에 불법적으로 접근한 상황

- **서비스 거부 공격(DoS Attack):** 대량의 데이터를 인가된 클라이언트에게 전송하여 인가된 클라이언트의 정상적인 통신을 방해하는 비인증 홍수 공격(De authentication flooding attack), AP에 과부하를 주는 결합 요청 홍수 공격(Association Request flooding attack), 그리고 클라이언트에 과부하를 주는 결합 응답 홍수 공격(Association Response flooding attack) 등으로 구성[9,10].

2.2 WIPS 센서를 이용한 공격 탐지 및 차단 원리

WIPS 센서는 일반적으로 그림 1에서 기술된 바와 같이 다음 세가지 절차를 거쳐 무선랜 상의 보안 위협을 탐지하고 차단한다: (1)무선 패킷 캡처, (2)보안 위협 탐지 및 (3)차단[11].

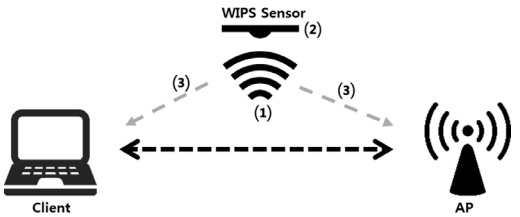

그림 1 WIPS 센서를 이용한 무선 위협 탐지 및 차단 절차
Fig. 1 Wireless threat detection and prevention using WIPS sensor

(1)무선 패킷 캡처 단계에서 libpcap과 tcpdump와 같은 패킷 캡처 라이브러리를 사용하여 무선 상의 802.11 mac 패킷을 캡처한다. 이를 위해서 모니터 모드(monitor mode)가 지원되는 무선 랜카드가 필요하다. (2)보안 위협 탐지 단계에서는 캡처한 패킷의 내용을 분석하여 상기 2.1에서 언급한 위협이 발생했는지 여부를 확인한다. 해당 패킷에서 위협 탐지 시, (3)차단 단계에서 센서는 위협이 발생한 기기와 AP로 비인증 이유 코드(De-Authentication Reason code)를 보내 자체적으로 세션을 종료하도록 유도한다.

하지만 이러한 WIPS 센서는 설치 및 관리에 있어 비용적인 문제가 있다. 실제로 현재 상용화 중인 센서의 경우에는 하나 당 약 100만원에 거래되고 있으며 설치 시에도 추가적인 비용이 지출된다. 또한 WIPS 서버와 센서를 동시에 운영하는 경우 유지비용은 연간 설치비용의 12% 달하는 것으로 알려져 있다. 이로 인해, 개인 사용자 및 소규모 회사에서는 WIPS 솔루션을 도입하기 힘든 상황이다[4].

3. 관련 연구

WIPS 센서 구현 형태에 따라 크게 (1) AP와 결합된 공용 WIPS 센서, (2) AP와 결합된 전용 WIPS 센서 및 (3) 독립적 WIPS 센서 형태로 구분 가능하다. 이 중, (1) AP와 결합된 공용 WIPS 센서의 경우 AP가 네트워크 연결 기능과 WIPS 기능을 번갈아 수행하므로 보안 위협을 탐지하는데 효과적이지 않으며 연결 지연 문제가 발생할 수 있어 잘 사용되지 않는다. 본 단락에서는 (2) AP와 결합된 전용 WIPS 센서 및 (3) 독립적 WIPS 센서 형태로 개발되어 보편적으로 사용되는 WIPS 센서의 장단점을 보안 위협 탐지 범위(attack discovery) 및 가격(price) 측면을 중심으로 비교 분석한다[12].

현재까지 개발된 대부분의 WIPS 센서는 단락 2.1에서 언급된 다양한 보안 위협 중 가장 기본적인 보안 위협인 불법 AP(Rogue AP), 비인증 고객 디바이스(un-authorized client devices) 및 비인증 임시 네트워크(unauthorized ad hoc networks)을 탐지하도록 설계되었다. 또한 Zebra Technologies AirDefense와 같은 일부 WIPS 제품의 경우는 DoS 공격을 탐지하고 차단하는 것이 가능하며, Cisco Adaptive Wireless IPS와 HP Mobility Security IDS/IPS 제품의 경우는 단락 2.1에서 언급한 모든 보안 위협을 탐지하고 차단하는 것이 가능한 것으로 알려져 있다. 하지만, 현재까지 개발된 상용화 제품의 경우 (2) AP와 결합된 전용 WIPS 센서 혹은 (3) 전용 WIPS 센서 관리를 위해 기본적으로 서버와 연동해야 하므로 개인 사용자 및 소규모 회사에서 사용하기 적합하지 않다.

WIPS 제품의 가격은 서버와의 연동 유무 및 구현 방식에 따라 달라진다. 소프트웨어 모듈로 구현되어 AP에 설치하여 사용하기 편리한 Aruba RFProtect의 경우는 하드웨어 모듈로 개발된 일부 제품에 비해 낮은 가격으로 사용자 및 소규모 회사에서 사용하기 적합하다. 하지만, 상용화된 WIPS 제품들은 서버 및 WIPS 센서를 구입하고 설치하는 과정에서 많은 비용이 드는 단점을 갖고 있다. 제안한 WIPS 센서는 범용 라즈베리 파이 보드를 사용하여 개발함으로써, 관리 대상 네트워크의 운영 정책에 따라 다양한 종류의 무선 안테나와 무선 랜카드 장착이 가능하기 때문에 설치 및 운영비용을 최소화하는 것이 가능하다.

3.1 기존의 저비용 WIPS 개발 사례

기존에 저비용으로 WIPS를 구현한 사례는 다음과 같다. 센서(Sensor)와 서버(Server)를 하나의 컴퓨터를 사용하여 구현 하였으며 센서(Sensor)에서 패킷을 수집한 후 서버(Server)에서 패킷을 분석하여 불법 AP(Rogue AP), 잘못 설정된 AP(Mis-configured AP), 잘못 결합된 클라이언트(Client Mis-Association), 임시 연결(Ad hoc Connection), AP MAC 위장(AP MAC Spoofing), Honey Pot AP, 서비스 거부 공격(DoS Attack)을 탐지한다. 선행연구에서 사용한 시스템 개발 환경은 표 1과 같다[13].

표 1 선행연구의 시스템 개발 환경
Table 1 System development

element	Explanation
OS	Windows 7 Professional
Development environment	- CPU : Intel Pentium III 800Mhz - Memory : At least 128MB - HDD : 100MB or more free space - Wireless LAN card
Development language	C#

선행연구와 제안 시스템을 비교해보자면 선행 연구는 센서(Sensor)에서 모든 기능을 수행하는 제안시스템과 달리 서버(Server)를 추가적으로 사용하기 때문에 대쉬보드 화면을 통해 패킷 분석정보를 손쉽게 확인 가능하다는 장점이 있고 제안시스템은 라즈베리파이를 이용하여 개발한 WIPS 센서(Sensor)에서 패킷 수집 및 분석이 모두 이루어지기 때문에 선행연구에 비해 더욱 저비용으로 WIPS 환경 도입이 가능하며 라즈베리파이의 크기를 활용하여 다수의 센서(Sensor)를 협소한 공간에 설치할 수 있고 점과 추가적으로 비인증 결합(Unauthorized Association)을 탐지할 수 있다는 장점이 존재한다.

3.2 오픈소스 소프트웨어를 사용한 WIPS 개발 사례

기존의 오픈소스 소프트 웨어를 사용한 WIPS 개발 사례는 다음과 같다. [14]는 WIDS 오픈 소스 툴인 WAIDPS를 사용하여 소규모 네트워크에 적합한 상용 WIPS 대안을 제시하였다. WAIDPS(Wireless Auditing Intrusion Detection & Prevention System)은 SYWorks Programming에서 개발한 오픈소스 소프트웨어 툴로서 PC와 시중에서 쉽게 구할 수 있는 무선 랜 인터페이스만 있으면 쉽게 구동할 수 있다.

WAIDPS는 제안 시스템과 달리 AP MAC Spoofing 및 DoS의 공격을 탐지 하지 못하고 또한, 공격 발생 시 탐지 정보를 네트워크 관리자에게 알려주는 기능은 탑재하였지만 대응기능이 포함되어 있지 않아 공격 받고 있음을 탐지하더라도 네트워크 탐지자가 직접 적절한 대처를 해야 한다는 단점이 있다. 제안시스템과 WAIDPS의 비교 내용은 표 2에서 기술한다.

4. 제안하는 시스템

본 단락에서는 확장성이 뛰어난 범용 개발 보드인 라즈베리파이를 이용하여 단락 2.1에서 언급한 무선 보안 위협들을 탐지하고 차단하기 위한 WIPS 센서 구현 방안에 대해 기술한다. 제안하는 WIPS 센서는 화이트리스트를 사용하여 인가된 AP와 디바이스의 항목을 관리 유지한다. 3.2절에서 기술하는 공격 탐지 알고리즘에 대한 이해를 돕기 위해 관련 용어에 대한 설명을 표 3에서 기술한다.

4.1 시스템 구성 요소

시스템 구성 형태는 그림 2와 같으며, 시스템 구성 요소는 다음과 같다.

표 2 제안시스템과 WAIDPS[14] 비교
Table 2 Comparison of proposed system and WAIDPS[14]

Attack Type	Proposed System		WAIDPS	
	Detection	Prevention	Detection	Prevention
Rogue AP	○	○	○	×
Mis-configured	○	○	○	×
Client Mis Association	○	○	○	×
Unauthorized Association	○	○	○	×
Ad-Hoc	○	○	×	×
Honeypot AP	○	○	○	×
AP MAC Spoofing	○	○	×	×
DoS	○	○	×	×

표 3 용어 설명
Table 3 Terminology

element	Explanation
DSAP (Destination Service Access Point)	The individual or group address for the address into the upper layers of the network protocol stack.
SSAP (Source Service Access Point)	The individual address for access into the upper layers of the network protocol stack.
SNAP (Sub-Network Access Protocol)	Extension of the IEEE 802.2 Logical Link Control (LLC) to distinguish much more protocols of the higher layer than using of the 8-bit Service Access Point fields (LSAP) present in the IEEE 802.2 header.

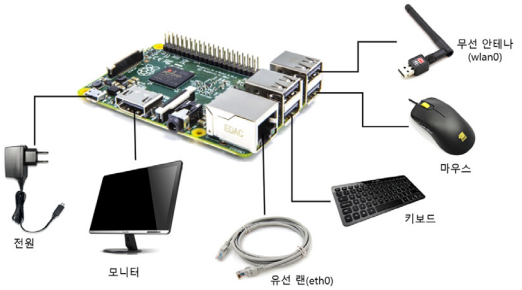

그림 2 시스템 구성도
Fig. 2 System configuration

• 하드웨어
  - 무선 안테나 : RT5370 USB Wi-Fi Adapter
  - 유선 랜 : 외부 유선망과 연결(100Mbps)
  - 전원 : 5V-2000mA
  - 보드 : Raspberry Pi-2
• 소프트웨어
  - 운영체제 : RASPBIAN jessie 2015-11-21 (kernel 4.1.7+)
  - 패킷 캡처 라이브러리 : Libpcap v1.5.3

4.2 채널 변경 및 패킷 스니핑

4.2.1 채널 변경

제안 시스템은 모니터링시 전체 채널을 탐지하기 위하여 채널 스위칭을 수행한다. 채널 스위칭은 1초 간격으로 수행된다. 그 이유는 서비스 거부 공격(DoS Attack) 탐지 시 1초 동안의 관리 패킷의 수를 사용하기 때문에 1초 동안 동일 채널에서 생성되는 패킷을 모두 캡쳐하기 위함이다. 채널 변경은 “iwconfig” 명령어를 코드 상에서 실행하여 수행한다.

4.2.2 채널 스캐닝 및 패킷 스니핑

제안 시스템은 리눅스의 네트워크 트래픽 포착용 API로 널리 알려진 libpcap 라이브러리를 사용하여 현재 설정된 채널을 스캐닝하고 패킷을 캡쳐한다. 패킷 캡쳐 시 공격 탐지에 필요한 802.11 MAC 프레임은 암호화 되지 않은 상태로 무선상에 전송되기 때문에 손쉽게 패킷의 해당 필드들을 스니핑할 수 있다.

4.3 공격 탐지 방안

4.3.1 화이트리스트 구성

화이트리스트는 관리자로부터 보안성을 인증 받은 AP와 기기들의 항목들로 유지된다. 화이트리스트는 AP 화이트리스트, Dev 화이트리스트 형태로 관리되며, 화이트리스트의 관리 대상 항목을 표 4와 5에서 기술한다.

4.3.2 무선 위협 별 분석 802.11 field

공격탐지는 공격 종류에 따라 802.11 MAC 프레임의 필요한 필드를 분석하여 수행한다. 공격 종류별 사용되는 분석 필드는 표 6과 같다.

표 4 디바이스 화이트리스트 구성 요소
Table 4 Components of device whitelist

element	Explanation
MAC	Physical address
SSID_length	SSID length of Dev
SSID	SSID of Dev

표 5 AP 화이트리스트 구성 요소
Table 5 Components of AP whitelist

element	Explanation
MAC	Physical address
SSID_length	SSID length of AP
SSID	SSID of AP
security policy	The security policy that a is using
Sequence_number	latest Sequence_number of AP
management_count	Number of management packet per second
Connect_Dev_MAC[]	mac address of Dev connected to AP

표 6 공격별 분석 필드
Table 6 Analysis field

Attack Type	Analysis Field
Rogue AP	frame_control
	DSAP
	SSAP
	frame_body
	sender_address
Mis-configured AP	Privacy
	RSN Information
	WPA Information
Client Mis-association	reciver_address
	sender_address
Unauthorized Association	reciver_address
	sender_address
Ad hoc Connection	frame_control
	ESS
	IBSS
Honeypot AP	frame_control
	SSID
	sender_address
AP MAC Spoofing	frame_control
	SSID
	sender_address
	sequence_number
DoS Attack	frame_control_type
	reciver_address

4.3.3 불법 AP(Rogue AP) attack detection

알고리즘 1에서 기술된 바와 같이 불법 AP(Rogue AP)는 ARP 패킷의 특성을 이용하여 탐지한다. ARP

패킷은 AP가 유선상의 정보를 무선 네트워크로 forward 해주는 특성이 있다. ARP 패킷을 이용한 불법 AP (Rogue AP)의 탐지는 다음과 같은 4단계 과정을 거친다. (1)센서(Sensor)는 ARP 패킷을 유선 네트워크상에 방송(Broadcast) 한다. (2)유선네트워크에 연결된 AP들은 전달받은 ARP 패킷을 자신에게 연결된 기기들에게 전달하기 위하여 무선 네트워크에 Forward 한다. (3)센서(Sensor)는 AP들이 Forward한 무선 ARP 패킷을 캡처하여 AP들의 MAC 주소를 확인한다. (4)확인한 MAC주소가 AP 화이트리스트 항목에 존재하지 않는 경우 불법 AP(Rogue AP)로 판단한다. 이 후, 센서는 비인증 패킷(De-Authentication packet)을 전송하여 불법 AP(Rogue AP)와 연결된 모든 디바이스의 세션을 종료한다.

Algorithm 1. Rogue AP detection

```
불법 AP(Rogue AP) Detection
input : ieee80211 ieee MAC frame
set check to true;
if frame_control is data_type then
  if DSAP is SNAP and
    SSAP is SNAP then
      if frame_body is ARP then
        for(i = 0 to size of AP_whitelist){
          if MAC_sender is
          AP_whitelist[i]->MAC then
            set check to false;
        }
        if check then
          deauth_packet_send(
          MAC_sender, Broadcast);
```

4.3.4 잘못 설정된 AP(Mis-configured AP) 공격 탐지

잘못 설정된 AP(Mis-configured AP) 공격은 비콘 패킷의 내부 프레임 값을 비교하여 판단한다. AP의 보안정책 판단은 아래 그림 3과 같은 결정트리 형식 판단을 통해 결정한다. 먼저, (1)Capebility 정보의 privacy 비트를 확인하여 0이면 보안정책이 설정되지 않은 OPEN AP로 판단한다. 다음으로, (2)privacy 비트가 1이고 가변필드에 WPA2에서 필수 요소로 사용하는 AES-CCMP의 RSN 정보가 존재한다면 WPA2 보안정책을 사용하는 AP로 판단한다. 또한, (3)가변 필드에 WPA 정보 요소가 존재한다면 WPA 보안정책을 사용하는 AP로 판단하고 그렇지 않다면 WEP 보안정책을 사용하는 AP로 판단한다. 이 후, 관리자가 선정한 보안정책을 사용하지 않는 AP 탐지 시 알람 메시지를 발생한다.

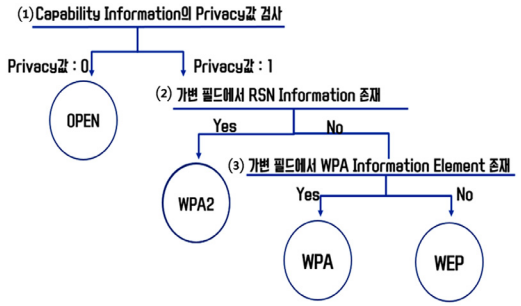

그림 3 잘못 설정된 AP(Mis-configured AP) 탐지 규칙
Fig. 3 Mis-configured AP detection rules

4.3.5 잘못 결합된 클라이언트(Client Mis-Association) 탐지

알고리즘 2에서 기술된 바와 같이 캡쳐 된 패킷의 출발지 주소와 목적지 주소 field 확인을 통해 인가된 디바이스가 비 인가된 AP와 통신하는 것을 확인하면 잘못 결합된 클라이언트(Client Mis-Association) 발생을 탐지한다. 이 후, 센서는 해당 디바이스와 AP로 비인증 이유 코드(De-Authentication Reason code)를 전송하여 세션을 종료한다.

Algorithm 2. Client mis-association detection

```
detect_ClientMisAssociation
input : ieee80211 ieee MAC frame
set Dev_check to false;
set AP_check to false;

if MAC_reciver is Broadcast then
else
    for(i = 0 to size of Dev_Whitelist){
      if MAC_sender is Dev_Whitelist[i]
      ->MAC then
        set Dev_check to true;
        for(j = 0 to size of AP_Whitelist){
          if MAC_reciver is AP_Whitelist[j]
            ->MAC then
              set AP_check to true;
        }
    }
    if Dev_check is true and AP_check is false then
      deauth_packet_send(MAC_sender, MAC_reciver);
```

4.3.6 비인증 결합(Unauthorized Association) 공격 탐지

알고리즘 3에서 기술된 바와 같이 잘못 결합된 클라이언트(Client Mis-Association)와 유사하게 캡처된 패

킷에서 출발지 주소와 목적지 주소 field를 확인하여 인가된 AP와 비 인가된 디바이스가 통신하는 것을 확인하면 비인증 결합(Unauthorized Association)로 탐지한다. 이 후, 센서는 해당 AP와 디바이스로 비인증 이유 코드(De-Authentication Reason code)를 전송하여 세션을 종료한다.

Algorithm 3. Unauthorized association detection

```
detect_UnauthorizedAssociation
input : ieee80211 ieee MAC frame
set Dev_check to false;
set AP_check to false;

if MAC_reciver is Broadcast then
else
    for(i = 0 to size of AP_Whitelist){
      if MAC_sender is AP_Whitelist[i]->MAC
      then
        set AP_check to true;
        for(j = 0 to size of Dev_Whitelist){
          if MAC_reciver is Dev_Whitelist[j]
            ->MAC then
              set Dev_check to true;
        }
    }
    if AP_check is true and Dev_check is false
    then
      deauth_packet_send(MAC_sender, MAC_reciver);
```

4.3.7 임시 연결(Ad hoc Connection) 공격 탐지

알고리즘 4에서 기술된 바와 같이 Transmitter가 STA이고, transmitter가 IBSS에 속하는 패킷이 탐지된다면 임시 연결(임시 연결(Ad hoc Connection)) 상태로 판단한다. 즉, 비콘 및 프로브 응답 패킷의 능력 정보 중 ESS bit가 0이고 IBSS bit가 1인 경우 임시 연결(임시 연결(Ad hoc Connection))으로 판단하고 센서(Sensor)는 해당 기기들에게 비인증 이유 코드(De-Authentication Reason code)를 전송하여 세션을 종료한다.

Algorithm 4. Ad hoc connection detection

```
detect_adhoc
input : ieee80211 ieee MAC frame
if frame_control is probe_response or beacon
then
    if ESS is false and IBSS is true then
      deauth_packet_send(MAC_sender, MAC_reciver);
```

4.3.8 Honeypot AP 공격 탐지

알고리즘 5에서 기술된 바와 같이 Honeypot AP는 비콘 패킷의 frame 총 2단계에 거쳐 확인하여 판단한다. 먼저, 캡처한 패킷의 SSID와 일치하는 화이트리스트상의 AP의 SSID가 있는지 확인한다. 동일한 SSID가 존재하는 경우, 캡처한 패킷의 BSS ID와 해당 AP의 mac 주소를 비교한다. 캡처한 패킷의 BSSID와 AP의 mac 주소가 일치하지 않을 때 Honeypot AP attack이 발생하였다고 판단한다. 센서는 Honeypot AP와 연결되어있던 모든 디바이스에 비인증 패킷(De-Authentication packet)을 전송하여 세션을 종료한다.

Algorithm 5. Honeypot AP detection

```
detect_HoneypotAP
input : ieee80211 ieee MAC frame
if frame_control is beacon then
    for(i = 0 to size of AP_whitelist){
      for(j = 0 to AP_whitelist[i].SSID_length){
        if SSID[j] is AP_whitelist[i]->SSID[j]
        then
          if MAC_sender is not AP_whitelist[i]->MAC
          then
          deauth_packet_send(MAC_sender,
          MAC_reciver);
      }
    }
```

4.3.9 AP MAC 위장(AP MAC Spoofing) 공격 탐지

알고리즘 6에서 기술된 바와 같이 AP MAC 위장(AP MAC Spoofing) 공격은 AP에서 보내는 패킷의 순차 번호(Sequence number)가 1씩 순차적으로 증가한다는 특성을 이용하여 탐지한다. Honeypot AP 공격과 마찬가지로, 캡처한 패킷의 SSID와 일치하는 화이트리스트상의 AP의 SSID가 있는지 확인한다. 동일한 SSID가 존재하는 경우, 캡처된 패킷의 BSS ID와 해당 AP의 mac 주소를 비교한다. 위의 두 항목이 모두 일치한다면 화이트리스트에 저장되어있는 AP의 순차 번호(Sequence number)와 캡처한 패킷의 순차 번호(Sequence number)를 비교한다. 순차 번호(Sequence number)가 순차적으로 증가하는 경우 화이트리스트의 순차 번호(Sequence number)를 업데이트 하고, 순차적이지 않을 경우에는 MAC 위장 공격으로 판단한다. 센서는 불법 AP(Rogue AP)와 연결된 모든 디바이스에 비인증 패킷(De-Authentication packet)을 전송하여 세션을 종료한다.

Algorithm 6. AP MAC spoofing detection

```
detect_MacSpoofing
input : ieee80211 ieee MAC frame
if frame_control is beacon then
  for(i = 0 to size of AP_whitelist){
    for(j = 0 to AP_whitelist[i].SSID_length){
      if SSID[j] is AP_whitelist[i]->SSID[j]
      then
        if MAC_sender is AP_whitelist[i]->MAC
        then
          if sequence_number is
          (AP_whitelist[i]->sequence_number)+1
          then
            set AP_whitelist[i]->sequence_number++;
          else
            deauth_packet_send
            (MAC_sender, MAC_reciver);
    }
  }
```

4.3.10 서비스 거부 공격(DoS Attack) 탐지

서비스 거부 공격(DoS Attack)은 화이트리스트에 속해있는 각 AP와 디바이스가 초당 수신하는 관리 패킷의 개수를 확인하여 탐지한다. 탐지과정은 알고리즘 7에서 기술된 바와 같이 DoS 탐지를 위한 데이터를 수집하는 과정과 알고리즘 8에서 기술된 바와 같이 1초에 한번 씩 수집된 데이터를 이용하여 DoS 공격을 탐지하는 과정으로 나누어진다. 해당 AP가 초당 5개 이상의 관리 패킷을 수신한다면 서비스 거부 공격(DoS Attack)으로 판단한다. 이후 센서는 공격을 받고 있는 AP에 연결된 디바이스들에게 CTS 패킷을 전송하여 AP의 서비스를 정상적으로 받을 수 있도록 한다.

Algorithm 7. DoS data collection

```
collect_DoS_data
input : ieee80211 ieee MAC frame
set Dev_MAC_check to false;

if frame_control_type is management then
  for(i = 0 to size of AP_whitelist){
    if MAC_reciver is AP_whitelist[i] ->MAC
    then
      (AP_whitelist[i]->management_count)++;
      for(j = 0 to size of AP_whitelist[i].
Connect_Dev_MAC){
        if MAC_sender is AP_whitelist[i].
Connect_Dev_MAC[j] then
          set Dev_MAC_check to true;
          break;
      }
      if Dev_MAC_check is flase then
        Add MAC_sender to AP_whitelist[i].
Connect_Dev_MAC;
  }
```

Algorithm 8. DoS attack detection

```
detect_DoS
input : ieee80211 ieee MAC frame
sleep(1);

for(i = 0 to size of AP_whitelist){
  if AP_whitelist[i]->management_count is
  greater than 5 then
    for(j = 0 to size of
    AP_whitelist[i].Connect_Dev_MAC){
      CTS_packet_send(AP_whitelist[i].
      Connect_Dev_MAC[j]);
    }

  set AP_whitelist[i]->management_count to 0;
}
```

4.3.11 탐지 결과 분석

앞에서 설명한 무선 랜 공격 차단을 위한 보안 위협 탐지 방법에 따른 탐지 결과와 분석 내용은 표 7에서 기술한다.

5. 실험 및 성능분석

5.1 실험 환경 및 방법

실험은 쉴드룸 환경에서 3개의 인증 AP와 1개의 공격 AP 그리고 3개의 인증 디바이스와 1개의 비인증 디바이스, 1개의 ad-hoc attack AP, 마지막으로 1개의 WIPS 센서를 사용하여 진행하였고 각 기기들의 배치 구조는 그림 4와 같다. 실험 방법은 각 공격 종류별 임의의 채널을 사용하여 공격을 진행하고 공격 시작 시간부터 WIPS의 탐지 시간 및 차단시간까지의 시간차와 탐지거리를 총 20번 씩 수행하여 측정한다.

5.2 성능 분석 및 비교

실험을 통한 성능 분석은 탐지시간, 차단시간, 탐지거리 기준으로 진행한다. 먼저 제안한 시스템의 각 공격별 탐지성능을 측정한 후 기존의 상용 WIPS 제품과의 비

표 7 공격 유형 별 탐지 결과
Table 7 Detection results by attack type

Attack Type	Detection Result	Explanation
Rogue AP	Rogue AP Attack Detection!!!! Rogue AP : bc 6c 19 21 42 42	Output the mac address of the detected Rogue AP
Mis configured	Mis-configured AP attack Detection!!!! security policy : WPA2 Mis-configured AP : bc 6c 19 21 42 42 Mis-configured AP security policy : WPA	When detecting an attack, the security policy specified by the current Sensor and the mac address of the AP not comply to the security policy and the security policy to be used are output.
Client Mis Association	Client Mis Association Attack Detection!! Authorized Device : 48 59 29 ec 21 7d Unauthorized AP : 90 9f 33 2a 60 b8	When detecting an attack, the mac address of the unauthenticated device connected to the authenticated AP is output
Unauthorized Association	Unauthorized Association Attack Detection !! Authorized AP : 00 26 66 f2 04 bc Unauthorized Device : 48 59 29 ec 21 7d	When detecting an attack, it outputs the mac address of the device directly connected to each other.
Ad-Hoc	ad hoc Connection Attack Detection!!!! Dev1 : 5c f5 da d8 e9 1b Dev2 : bc 6c 19 21 42 42	When detecting an attack, it outputs the mac address of the unauthenticated device connected with the authenticated AP.
Honeypot AP	Honeypot AP Attack Detection!!!! SSID : wook Whitelist AP : 7c f5 da d8 e9 1b Honeypot AP : bc 6c 19 21 42 42	When detecting an attack, it outputs the forged SSID, the mac address of the authentication AP, and the mac address of the honeypot AP.
AP MAC Spoofing	AP MAC Spoofing Attack Detection!!!! Whitelist AP : 7c f5 da d8 e9 1b Whitelist AP Sequence number : 373 Capture Sequence number : 103	When detecting an attack, the mac 주소 of the authenticated AP, the current 순Sequence number and Sequence number of the captured packet are output.
DoS	DoS Attack Detection!!!! whitelist AP : 7c f5 da d8 e9 1b management Packet Num : 23	It outputs the mac address of the authenticated AP that was attacked when an attack was detected and the number of captured Management packets for 1 second.

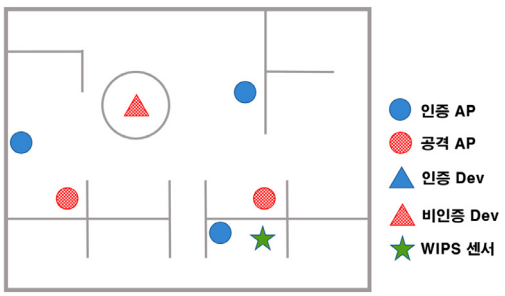

그림 4 실험 환경
Fig. 4 Experimental setup

표 8 공격 유형 별 성능
Table 8 Performance by attack type

Attack Type	detection time(sec)	block time(sec)
Rogue AP	120	105
Mis-configured AP	30	40
Client Mis-association	20	27
Unauthorized Association	20	27
Ad hoc Connection	27	32
Honeypot AP	20	27
AP MAC Spoofing	180	190
DoS Attack	330	540

교를 통해 성능을 분석한다. 비교에 사용되는 시간 값은 실험으로 측정된 시간의 최대값과 최소값의 평균값을 사용한다.

5.2.1 성능 분석

제안시스템의 공격 유형별 탐지 시간 및 차단 시간은 표 8에서 기술한다. 비교적 탐지가 쉬운 공격인 잘못 설정된 AP(Mis-configured AP), 잘못 결합된 클라이언트(Client Mis-Association), 비인증 결합(Unauthorized Association), Honeypot AP, 임시 연결(Ad hoc Connection)은 평균 25초의 시간안에 탐지가 가능하고 평균 32초의 시간안에 차단이 가능하다. 하지만 불법 AP(Rogue AP)는 센서가 유선상으로 ARP 패킷을 보내는 시간이 추가적으로 소요되기 때문에 평균 3분 정도의 시간이 탐지 시간이 걸리고 평균 2분정도의 탐지 및 차단시간이 걸린다. 그리고 AP MAC 위장(AP MAC Spoofing)의 경우에도 Sequence number가 순차적으로 올라가는지를 확인 할 때 중간에 캡쳐되지 못하고 누락된 패킷이 있다면 공격으로 판단을 하여 오탐율이 높아 탐지 및 차단에 오랜 시간이 걸렸다. 또한 서비스 거부공격(DoS Attack)의 경우에도 1초 동안의 관리 패킷의 수를 확인 하여 공격을 탐지하기 때문에 공격이 이루어지고 있는 채널이 아닌 타 채널을 스캐닝하고 있는 과정에서 DoS 공격이 발생한다면 탐지를 할 수 없어 탐지 시간이 평균 5분 30초로 오래 걸리고 차단시간 또한

표 9 WIPS 성능 비교
Table 9 WIPS performance comparison

Classification	detection time(sec)	block time(sec)	detection distance
Company WIPS A	20	45	50m
Company WIPS B	150	165	25m
Proposed System	90	110	15m

CTS 메시지를 공격받고 있는 AP와 연결된 모든 디바이스들에게 전송하여 정상화를 시켜야하기 때문에 평균 9분으로 오래 걸렸다.

5.2.2 성능 비교

상용 WIPS 제품을 판매하는 A, B사의 제품과 제안 시스템의 성능을 비교해 보았다. 성능비교 결과는 표 9에 기술하였다. 쉴드룸 환경에서 A사의 경우에는 탐지시간 20초, 차단시간 45초, 탐지 거리 45m이며 B사의 경우 탐지시간 2분 30초, 차단시간 2분 35초, 탐지거리 25m 이다[15]. 제안된 시스템은 탐지 시간 90초, 105초, 탐지 거리 15m로 A사 제품 보다는 낮고 B사 제품보다는 높은 성능을 보여주었다. 하지만 저가의 안테나를 사용하는 만큼 탐지 거리가 A, B사 모두보다 떨어지는 성능을 보여주는 것을 볼 수 있다. 따라서 개인이나 소기업과 같은 소규모의 공간에서만 사용 가능하다는 단점이 있다.

6. 결 론

본 논문에서는 저가형 초소형 컴퓨터로 알려진 라즈베리파이를 이용한 WIPS 센서 구현 방안에 대해 기술하였다. 이를 이용하여 대표적인 무선 보안 위협들에 대한 탐지 및 차단 기능을 구현하였다. 제안하는 시스템은 범용 개발 보드인 라즈베리파이를 사용하여 WIPS 센서를 구현함으로써 구현 가격이 저렴하고 사용자가 자유롭게 원하는 기능을 추가하는 것이 가능하다. 하지만, 실험 결과에 따르면, 상용 WIPS와 비교를 해보았을 때 탐지시간 및 차단시간에는 차이가 없었지만 탐지 거리 면에서 성능이 떨어지는 것을 볼 수 있었다. 따라서 개인 또는 소규모 회사와 같은 소규모의 공간에서 발생 가능한 주요 보안 위협 해소 방안으로 적용 가능 할 것으로 예상된다. 향후, 성능이 좋은 안테나로의 변경과 WIPS 센서(Sensor)와 연동하는 서버 구현 및 서버에 동적으로 화이트리스트를 업데이트 하는 기능을 탑재하여 대규모 네트워크에도 적용가능도록 연구를 진행해 나갈 예정이다.

References

[1] Kim Ji-an, 2014, "wireless Network Security Threat Countermeasures WIPS," Available:http://www.boannews. com/media/view.asp?idx=39719

[2] A. Scarfò, "New security perspectives around BYOD," *Proc. 7th Int. Conf. Broadband, Wireless Computing, Commun., Applicat. (BWCCA)*, pp. 446-451, Victoria, Canada, Nov. 2012.

[3] Robert Mitchell, Ing-Ray Chen, "A survey of intrusion detection in wireless network applications," *Journal Computer Communications archive Volume* 42 pp. 1-23, Apr. 2014.

[4] Jungsoo Park, Minho Park, Souhwan Jung, A whitelist-Based Scheme for Detecting and Preventing Unauthorized AP Access Using Mobile Device, KICS 13-08, Vol. 38B, Aug. 2013.

[5] AirTight Network, "Airtight network wireless security," AirTight White Paper, 2012.

[6] Lee Gi Hyouk, Young Jae Dong, "A Study on the Construction instance of the Wireless Intrusion Prevention System for illegal AP detection threat preventions," *Proc. of Symposium of the Korean Institute of communications and information Sciences*, pp. 1004-1015, November, 2008

[7] Md. Waliullah, Diane Gan, "Wireless LAN Security Threats & Vulnerabilities : A Literature Review," *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 5, No. 1, 2014.

[8] Sushma, Deepak Nandal, Vikas Nanda, "Security Threats in Wireless Sensor Networks," *International Journal of Computer Science & Management Studies(IJCSMS)*, Vol. 11, Issue 01, May 2011.

[9] Bellardo J, Savage S, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," *USENIX security* (pp. 15-28), Aug. 2003.

[10] Aslam, Baber, M. Hasan Islam, and Shoab A. Khan, "802.11 disassociation DoS Attack and its solutions: A survey," Mobile Computing and Wireless Communication International Conference, 2006. MCWC 2006, *Proc. of the First. IEEE*, 2006, Sep. 2006.

[11] Onat I, Miri A, "An intrusion detection system for wireless Sensor networks," *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, 2005, Vol. 3, pp. 253-259. IEEE, Aug, 2005.

[12] Karen Scarfone, "Comparing the top wireless intrusion prevention systems," *Wireless intrusion prevention systems: A buyer's guide,* Scarfone Cybersecurity, 2016.

[13] Han-Kil Kim, Su-Jin Kim, Hwan-Kyu Lee, Hoe-kyung Jung, Light-weight System Design & Implementation for Wireless Intrusion Detection System, *Journal of the Korea Institute of informaion and*, Vol. 18, No. 3, pp. 602-608, Mar. 2014.

[14] Woo-Hyuk Jung, Seung-hyung Lee, "Detecting and responding to security attacks about AP, The Journal of The Korean Institute of Communication

Sciences," 2016.
[15] Sansung, "Samsung wireless Enterprise sanmsung security AP, WHITE PAPER," 2013.

윤 광 욱
2011년~현재 부산대학교 정보컴퓨터공학부 학사과정. 관심분야는 네트워크 보안, 지능형 자동차 IT 보안 등

최 석 환
2016년 부산대학교 정보컴퓨터공학부 졸업(학사). 2016년~현재 부산대학교 전기전자컴퓨터공학과 석사과정. 관심분야는 네트워크 보안, IDS 등

안 상 언
2017년 부산대학교 정보컴퓨터공학부 졸업(학사). 2017년~현재 부산대학교 사물인터넷 연구센터 연구원

김 정 구
1988년 경북대학교 전자공학과 공학사
1991년 경북대학교 전자공학과 공학석사
1995년 경북대학교 전자공학과 공학박사
1995년~현재 부산대학교 정보컴퓨터공학부 교수. 관심분야는 정보 및 부호이론, 디지털통신 시스템, IoT 시스템

최 윤 호
2008년 서울대학교 전기컴퓨터공학부 박사. 2010년 펜실베니아 주립대학교 박사후 연구원. 2012년 삼성전자 네트워크사업부 책임연구원. 2014년 경기대학교 융합보안학과 조교수. 2016년 부산대학교 전기컴퓨터공학부 조교수. 2016년~현재 부산대학교 전기컴퓨터공학부 부교수. 관심분야는 모바일 보안, 유무선 네트워크 침입탐지, IoT 보안 프로토콜, 경량 암호, 지능형 자동차 IT 보안 등