IT융합분과

차세대 무선랜 침입방지 시스템 기술(무선랜 보안 기술)

Ⅰ. 제안기술 개요

기술의 내용	기술의 동향	기술의 제품화 및 시장 전망
· 수백Mbps~ 수Gbps급 초고속 무선랜 환경에서 다채널 감시, 본딩채널 감시, 실시간 자동탐지 및 차단, 무선 핑거프린트를 이용한 위장 무선공격 디바이스(AP/단말)의 식별 및 추적 등을 제공하는 무선랜 침입 방지 시스템(침입탐지/차단 센서 및 서버) 기술 · 감시 대상 무선채널 수가 급증하는 802.11ac 무선랜 AP 및 컨트롤러에 내장하여 위협 대응 센서 엔진 핵심 기술로 활용	[국내동향] · Gbps급 무선랜 특성을 고려한 무선랜 침입 방지 센서 및 침입방지형 보안 AP에 대한 기술은 현재 없음 [해외동향] · 무선랜 침해방지(WIPS) 제품의 경우, 시스코를 선두로 에어타이트, 아루바 등이 시장을 점유하고 있으며, 스마트 디바이스 증가에 따른 무선네트워크 감시, 위협 대응 관련 IPR 등이 증가 추세	· 별도의 침입 탐지 센서 기반의 기업용 WIPS 제품이 전체 시장의 80%를 차지하고 있으나, 무선랜 컨트롤러/AP에 내장된 WIPS 솔루션도 증가 추세임. · MAC 주소를 불법 복제한 위장 AP로 개인정보 유출을 유인하는 무선 피싱을 원천적으로 차단할 수 있는 침입방지센서 제품화 · 무선서비스 채널 감시, 연결 무선단말의 식별, 연결차단 등 침입 탐지/대응 보안기능을 무선랜 AP에 탑재(침입방지형 보안AP)하여 제품화

상용화단계	일반	①아이디어 ②연구단계 ③개발단계 ④개발완료(시제품) ❺제품화 단계
	의약바이오	①라이센싱 ②개발단계 ③제품화 단계
핵심키워드	한글	무선랜 침입 탐지 및 방지, 무선랜 보안
	영문	WIPS, Wireless Intrusion Prevention System, Gbps WLAN security

Ⅱ. 기술개발자 정보

기관명	한국전자통신연구원	부 서	ICT융합보안연구실
성 명	김신효	직 급	책임연구원
전화/핸드폰	042-860-5485/010-8211-5485	이메일	shykim@etri.re.kr

Ⅲ. 수행과제정보

지원지관명	미래창조과학부	연구사업명	정보통신 · 방송 기술개발
연구과제명	MTM기반 단말 및 차세대무선랜 보안 기술 개발	수행기간	2012.3.1. ~ 2015.2.28
주관기관	한국전자통신연구원	공동연구기관	㈜코나아이, ㈜유브릿지, ㈜네오인프라, ㈜제이알에스씨, 금융보안연구원, 한국정보보호시스템(주), ㈜에어큐브, 유넷시스템(주)

Ⅳ. 특허정보

특허현황	사업화대상기술관련 특허 총 3 건				
상세현황	구 분	상 태	출원(등록)일자	특허번호	특허명
	대상기술	■출원□등록	2012.12.04	10-2012-0139745	무선랜 침입 탐지 방법 및 시스템
	대상기술	■출원□등록	2012.11.05	10-2012-0124243	소프트 로그 액세스 포인트를 구동하는 공격 단말 색출 방법 및 이 방법을 수행하는 장치
	대상기술	■출원□등록	2012.12.04	10-2012-0139805	무선 침해 방지를 위한 무선 디바이스 분류 장치

1. 기술성 분석

1. 기술의 내용 및 특징

○ 무선랜 침입방지 시스템((WIPS: Wireless Intrusion Prevention System)이란 무선랜 통신 채널을 모니터링하여 위장, 복제 또는 인가되지 않은 무선장비를 이용한 해킹(피싱 또는 DoS) 공격 시도를 자동으로 탐지 및 차단하여 안전한 무선랜 이용 환경을 제공하는 보안 시스템으로 센서와 이를 관리 제어하는 서버로 구성

· (센서) 다수의 무선 채널 스케줄링을 통하여 수신 가능한 통신 트래픽을 센싱(수집)하고 DoS, 피싱 등 다양한 공격발생 여부를 분석하여 무선 침입을 탐지하고 차단하는 무선침입 감시 및 대응(차단) 장치

· (서버) 무선랜 보안서비스(분류, 인가, 탐지, 차단, 관리, 관제 등) 정책을 설정하고, 그 정책에 따라 무선 기기, 센서, 및 무선랜 보안상태를 중앙에서 분석 및 모니터링하고 제어하는 보안 서버

· 본 기술의 주요 특징 : 다채널 무선감시용 스마트 스케줄러, 실시간 자동탐지 및 차단, 무선 핑거프린트를 이용한 무선공격 단말기 식별 및 추적, 무선랜 보안 위협관제 등

○ WIPS는 무선랜의 유형에 따라 802.11a/b/g(저속)과 802.11n/ac(고속)방식이 있고, 침입탐지 기능의 구현방식에 따라 독립형(Stand-alone) 센서 방식, 무선AP(Access Point) 또는 무선랜 컨트롤러 내장 방식으로 구분되며, **최근에 802.11ac Gbps급 무선랜 등장(감시 대상 무선채널 수 급증)으로 내장 방식의 요구도 증가**

2. 기술의 수준

○ 에어타이트, 시스코, 에어디펜스, 아루바 등이 무선랜 침입방지(WIPS) 기술 선도, **Gbps 무선전송 특성(다채널, 대용량 트래픽, 채널본딩 등)에 대한 고려없이** 기존의 저속 무선침입탐지 기술을 적용한 수준임

○ 또한, 채널을 순차적으로 스캐닝함으로써, 특정 시점에 미(未)탐지될 수 있는 구조적 한계, **MAC 주소 등 불법 복제한 위장 AP/단말의 공격 유무를 판별하지 못함**

○ 침해방지형 보안 AP**(무선 AP 또는 컨트롤러에 무선침입 방지 기능이 내장)에 대한 제품은 없음**

3. 기술의 필요성

○ 무선 통신 환경이 수십Mbps급 802.11a/b/g 저속 무선랜에서 ⇒ **수Gbps급 802.11n/ac 무선랜 환경으로 전환되는 시점에서 무선 침입을 방지하는 보안 핵심기술의 적용**이 시급함

○ 무선랜이 유선만큼 안전하지 않으며, 무선해킹에 취약하다는 이유로 관리적 측면에서 무선랜 보안 지침 및 규제를 강화하고 있으나, 기술적 조치의 한계로 실효성 저하

○ 스마트 기기 폭증, 스마트오피스, 모바일 클라우드, 콘텐츠 공유 등 무선AP를 이용한 서비스 확산으로, 무선/모바일 보안 제품 수요 증가와 정부의 무선랜 보안 지침/규제가 무선보안 시장성장의 원동력 역할을 함

1. 기술성 분석

※ Wi-Fi 무선랜 관련 국내규제: 백화점, 보험사, 병원 등 준용사업자 무선랜 보안조치 강화(행안부), 금융회사의 무선랜보안 통제강화(무선보안시스템의무도입, 금융감독원) 공공기관 '보안관제전문업체 지정제도' 시행(지경부), 유비쿼터스도시의 건설 등에 관한 법률(유무선통합보안관제, 국토부), 정보통신망법, 개인정보보호법, 무선랜 보안가이드(행안부), 무선랜보안대책/의무법검토(방통위) 등이 국내 무선보안 시장 성장에 영향

○ 사용자의 무선랜 보안 실태 조사시 무선랜 보안 설정 적용(82%), 보안 필요성 인식 82%로 조사되고 , 무선랜 구축시 신뢰성(35%) 다음으로 보안성(32%)을 중요하게 생각
- 무선랜 보안실태 조사(방통위 자료 2013년 1월) 및 Forrester Report 자료

○ 사업화 추진 필요성

· **시장 환경 변화에 따른 사업화 추진 필요** : 무선랜을 이용한 스마트 서비스 확산, BYOD 보급에 따른 무선보안 이슈, 무선 ICT를 활용한 융합 산업(자동차, 의료, 스마트 그리드, 산업용 제어시스템 등) 제품의 수요 증가

· 네트워크 인프라 보호에 **안전한 국산 장비 도입 니즈**

· 무선 침입공격 방지와 무선 스위치 기능이 내장된 **프리미엄 AP(보안 AP)에 대한 시장의 요구 증가와 유무선통합보안서비스 시장 확대** 예상

활용분야(제품/서비스)	관련 시장 규모(5년), 단위:억원				
	2015년	2016년	2017년	2018년	2019년
보안AP제품	303	336	372	413	458
유무선통합보안서비스	500	600	700	800	900

4. 기술의 차별성

○ Gbps급 고성능 무선랜에서는 모니터링하고 탐지해야 하는 채널수가 많아서 보다 스마트한 채널 스케줄러, 신속한 위장 AP탐지 알고리즘 등이 핵심 기능으로써, 성능에 미치는 비중이 큼.

○ 무선랜 기기의 고유한 특성(무선 핑거프린트)을 이용하여 **불법복제 또는 위장AP에 의한 무선침해 공격시도를 원천적으로 차단**할 수 있는 무선침입방지 센서 기술

※ 기존의 무선지문 추출/분석 기술은 고가의 계측기를 이용한 연구 실험용이나, 본 기술은 무선랜 침입방지 **센서 레벨에서 무선 지문을 추출/분석하고 디바이스를 식별**함으로써 MAC 주소 복제를 탐지하는 기술임

○ 채널 본딩, 다채널 등의 초고속 전송 특성을 갖는 Gbps급 무선랜 특성을 고려한 무선랜 침입 방지 센서 및 침해방지형 보안 AP에 대한 기술은 현재 없으며, 본 기술은 **침입방지형 보안 AP의 핵심 센서엔진**으로 활용 가능

· 센서엔진 : 칩셋 독립적인 동적 채널할당(Fair Channel Hopping), 다채널 감시(동시 4채널), 1.5초이내 연결 해제를 통한 침입 차단 성능 제공

○ **무선/모바일 통합 보안관리** 지원을 통한 위협 대응 성능 향상

· 무선망 감시용 WIPS와 모바일 단말 관리용 MDM를 지원하는 보안정보 공유 프레임워크 **(WIPS-MDM 연계 제품 및 서비스 없음)**

2. 특허성 분석

1. 국내외 특허 동향

○ 무선랜 보안 특허의 경우 총 879(국내 53건)건의 특허가 공개/등록 되어 있으며, 국내 특허는 본과제의 개발기술인 무선 침입방지 관련 특허 보다는 무선랜 네트워크 보안관리 방법, 무선랜 통신 보안 및 망연동 등의 관리 방법, 스마트디바이스 제어와 무선랜 관련 서비스 특허가 주류임. (특허검색 사이트 윕스 검색 결과임)

	무선 보안관리	무선랜 통신 보안/망연동	스마트디바이스제어	무선랜 기반서비스
국내 공개/등록 특허(건)	21	26	3	3

○ 무선랜 침입 탐지 및 방지 관련 국내 등록 특허의 경우, 총 3건으로 환경에서 센서 및 시스템, 불법AP검출 방법, 스마트 디바이스 감시 방법 관련 IPR로 **차세대 무선랜 환경에 특화된 특허는 등록된바 없음**

· 무선랜 보안 및 침해방지 기술 관련하여 국내에서는 ETRI가, 미국은 에어타이트사가 구조 및 기능 관련 핵심 등록 특허 보유

2. 선행특허분석

특허번호	0628325	0874015	2013-0007848 US	1429177
특 허 명	무선 네트워크에 대한 공격을 탐지하기 위한 침입 탐지센서 및 무선 네트워크 침입 탐지 시스템 및 방법	무선랜 침입 방지 시스템 및 방법	MONITORING OF SMART MOBILE DEVICES IN THE WIRELESS ACCESS NETWORKS	불법 A P 검출 시스템 및 그의 검출 방법
출 원 인	한국전자통신연구원	스큅정보통신	AirTight Networks	유넷시스템
기술요약	무선 침입 탐지 센서는 독자적인 무선랜 신호 감시 외에 액세스 포인트로부터 이벤트 관련 정보를 수신하여 무선 네트워크 상에서 발생되는 다양한 공격의 효과적 탐지 및 체계적 관리 방법	보안영역 내에 설치된 복수의 센서로부터 무선랜 기기의 감시 정보를 수신하고, 복수의 무선랜 감시 정보를 바탕으로 무선랜 기기가 악성 무선랜 기기인지를 판단하여, 기기의 위치 정보를 생성하고, 통신 차단 메시지를 생성	무선 로컬 영역 네트워크와 연결된 무선 클라이언트를 검출하고 무선 클라이언트를 스마트 모바일 장치로 식별하는 방법	보안 모드 및 라우터 모드의 무선 환경에서도 비인가 불법 AP가 자신의 네트워크 통신망에 연결되어 있는지를 확인 및 검출하는 방법
관련도 분석	A	A	A	A
	* 관련도 : X - 관련높음, Y - 관련있음, A - 관련은 없으나 참고할 자료 * X, Y - 주요참증에 해당, A - 참고참증에 해당			
조사결과	본 제안기술은 무선랜 침입방지 등 차세대 무선랜 보안기술에 관한 것으로, 이와 관련한 선행특허 문헌조사결과, 한국등록특허 0628325/한국전자통신연구원, 0874015/스큅정보통신, 1429177/유넷시스템, 미국 공개 특허 [2013-0007848] 등이 선행 특허로 조사됨			

3. 사업성 및 시장성 분석

1. 사업화 제품화

- ○ 무선 응용 제품시장 확대 기대감으로 삼성전자 등 대기업에서 무선보안 전략사업 분야로 시장진입. 그러나 에어타이트, 지러스 등 세계 1등/일류 기업이 기술 전문화된 중소 벤처기업이고, 무선랜 기술진화에 따른 지속적인 핵심 기술력 확보가 사업화 제품화 등 시장 경쟁력의 핵심
- ○ BYOD, IoT, Cloud 등 모바일 디바이스를 통한 무선랜 활용이 확대되면서 무선랜 보안 위협이 심화되어 더욱 큰 사회적, 국가적 위험을 야기할 것으로 예상되며, 무선랜 서비스를 제공하면서 보안위협 탐지/차단하는 '보안AP'시장은 지속성장 예상
- ○ 초고속무선랜(802.11n/ac) 모니터링 지원, 무선디바이스 식별, 무선랜 관리프레임 보호 지원 등 차별화 보안기능을 탑재한 보안 AP 제품화
- ○ WIPS에 무선랜 취약성 분석 기능과 네트워크 포렌식 기능을 내장한 제품 또는 서비스
- ○ 기존 유선 보안 관제 서비스와 연동하여 유무선 통합 보안 서비스 제공에 활용

2. 사업화 방법 및 성공요인

- ○ 사업화 방법 : 차별화 보안기능을 AP에 탑재하고, CC인증 등 공신력 있는 보안성 제공을 통한 제품 안전성 확보 필요
- ○ 성공 요인 : 고가의 외산 제품에 견줄만한 순수 국산 기술로, 합리적인 비용으로 무선 보안 AP의 프리미엄(차별화된 기능 탑재) 제품화

3. 국내외 시장전망

1) 국내외 시장 규모 및 동향

- ○ 기업망 환경에서 스마트폰 등의 스마트 기기의 사용 일반화, 모바일 데이터 트래픽 폭증으로 무선랜 활용이 증가되면서 무선/모바일 악성코드와 무선해킹 공격이 증가. 이러한 무선환경에서 DoS, 피싱 등을 이용한 정보유출을 방지하는 무선랜 침입방지시스템(WIPS) 시장이 부상하고 있음
- ○ 현재는 802.11a/b/g/n 무선랜용 WIPS 센서 제품이 전체 시장의 80%를 차지하고 있으며, 무선랜 컨트롤러/관제시스템에 내장된 WIPS 솔루션도 증가 추세임. 최근 Gbps급 802.11ac무선랜 등장으로 고성능(다채널감시, MIMO/본딩채널 감시, 악성 트래픽 차단, 위장AP탐지 핑거프린트 센싱, 위치추적 등) 침입탐지 및 차단 기술에 대한 시장 수요가 빠르게 증가 예상됨.
- ○ 최근 스마트그리드 등 M2M, IoT용 저전력 무선통신 방식으로 저전력(Power saving), 장거리 무선랜 802.11ah 표준 규격이 마무리 단계에 들어감에 따라, 향후 2~3년 내에 사물네트워크용 무선랜 침입방지시스템에 대한 급속한 시장 확대가 예상됨에 따라, 관련 핵심기술 확보시 새로운 시장 진입 및 경쟁력 확보의 기회를 가져다 둘 것으로 예상됨

3. 사업성 및 시장성 분석

2) 시장의 구조, 경쟁강도 및 진입장벽

○ 무선랜 침해방지(WIPS) 제품의 경우, 시스코, 에어타이트, 아루바, 모토로라 등이 시장을 점유하고 있음.

<무선랜 침입방지시스템 제품 시장경쟁 현황>

구 분	경쟁 현황				
기업 \ 경쟁수준	Strong Nagative	Caution	Promising	Positive	Strong Positive
AirTight Networks					x
Aruba Networks				x	
Cisco				x	
Fluke Networks(AirMagnet)				x	
Meraki (Cisco 자회사)			x		
Motorola(AirDefense)				x	

○ 무선침입방지시스템 수요가 증가하면서 시장 확대와 함께 **기존 외산 솔루션 중심의 시장에 국내 기업들이 가세하면서 업체 간 경쟁이 가열되는 추세**. 그러나 **제품의 탐지/대응/관제/추적 성능 핵심 기술력 및 신뢰성이 진입장벽**으로 존재

4. 사업화 성공 가이드

1) 사업화 후보기업 요건

○ 무선랜 관련 업체 또는 무선 보안 업체

○ WIPS, 유무선 보안관제, 무선랜 인증 기술 등 관련 기술 또는 제품군 보유 업체

2) 사업화 투자비용

○ 무선침입 방지 센서 엔진 기능 고도화 기술 추가 개발 비용

○ CC인증(보안성 평가), 전파인증, GS인증 등 제품 평가·인증을 위한 비용

○ 국외 수출을 위한 제품 홍보 및 판매 준비, 협력 체계 구축 및 운영 비용 등

3) 법적 검토사항

○ 기술이전 및 실시권 계약 범위 / 라이센싱 및 공동연구 범위 협의

○ 수익성 배분 협의 등

4) 희망 파트너쉽

① 기술이전 (○) ② 라이센싱 (○) ③ 공동연구 (○)

④ 기술출자 ( ) ⑤ 기타 ( )