학 사 학 위 논 문

사물인터넷 환경에서의 보안, 인증에 관한 연구

지 도 교 수
이병천 교수님

중부대학교 정보보호학과
우민식

2015

목 차

연구요약

사물인터넷의 기원은 개인용 컴퓨터(PC)가 인터넷이 가능했을 때부터 일 것이다. 2차 세계대전에서 탄도미사일 계산 목적으로 개발되었던 최초의 컴퓨터 ENIAC으로부터 집적회로 반도체를 이용한 전자계산기로 발전된 수많은 컴퓨터가 서로 통신목적으로 인터넷을 사용하여 IT의 또 다른 역사가 시작되었으니 말이다. 또 음성통신만 하던 수억대의 휴대폰 단말기가 인터넷이 가능해 지면서 '스마트폰' 이라는 이름으로 또 다른 센세이션을 일으키고 있다.

우리는 사물인터넷이라는 용어는 아직 익숙하지 않지만 그 원리는 이미 오래전부터 사용되고 있었다. 이제는 정말로 사물인터넷의 시대가 본격적으로 진행되고 있다. 구글, HP, 삼성, LG, 달리웍스 등 많은 대기업과 글로벌 기업들이 사물인터넷 시장에 뛰어들고 있다. 또, 향후 10년간 총 19조 달러의 어마어마한 경제적 효과가 사물인터넷을 통해 창출될 것으로 추정된다고 Cisco에서 전하고 있다. 또 Cisco는 사물인터넷 미래전망보고서를 통해서 향후 2020년까지 500억 이상의 디바이스가 연결되는 환경이 도래한다고 예상하였다.

그리고 국내에서는 2003년 1.25 대란부터 현재까지도 여러 가지 보안문제점으로 인해 전상망의 많은 피해가 있었고 해킹으로 인한 피해가 급증하고 있다. 03년도 KT가 DNS서버 공격을 받는 1.25대란, 08년도 중국 해커의 소행으로 옥션 1860만명 개인정보유출, 09년도 청와대, 국방부 등 30개 사이트 디도스(DDOS) 대규모 공격, 2010년 신세계몰, 2011년 현대캐피탈 개인정보유출, 농협 전산망 마비, 2014년 KT 개인정보 유출 등 최근에도 이러한 해킹공격과 보안문제점으로 이제는 보안이 절실해지고 있는 실정이도 '필요'가 아니라 '필수'가 되고 있는 상황이다.

이러한 상황에서 사물인터넷의 도래와 보안문제점이 만나면 세상의 모든 인터넷 가능한 사물들은 해킹위험대상이 된다는 것이다. 일상생활 속에서 익숙하게 찾아볼 수 있는 냉장고, 전자레인지, TV, 책상, 의자, 스마트폰이 모두 해킹되고 악용된다면 그 피해는 상상도 할 수 없는 것이다. 이러한 문제점들을 해결하기 위한 보안기술은 무엇이 있을까? 또 사물인터넷의 현황과 동향 그리고 인증, 인가의 문제까지 알아보고 연구하였다. 사물인터넷에서는 센서 네트워킹 기술이 가장 핵심 기술이다. 또한 인증, 인가도 상당히 중요한 기술이다. 이러한 것들의 보안적인 측면과 기술은 어떠한 것들이 있는지 연구하였다.

기리고 국내 사물인터넷에서의 보안으로는 실제로 어떻게 쓰여지고 어떤 회사가 어떠한 사물에 어떠한 기술을 어떻게 적용하고 있는지에 대해서 연구하였다.

1장 서론

1.1 연구의 배경 및 목적

2007년 6월 29일, 스티브잡스가 아이폰을 출시할 때 얼마나 팔릴지 자신이 없어 손익분기점을 맞추기 위해 599달러라는 적지 않은 가격에 아이폰을 내놓았지만 엄청난 인기를 끌었고 두 달 만에 200달러 낮춘 399달러에 팔기 시작했으며 애플은 1년 주기로 새로운 아이폰을 내놓기 시작했다. 결과는 2011년 4월엔 아이폰 시리즈의 누적 판매량이 전 세계 1억대를 돌파했다.

이것이 사물인터넷의 발전가능성이다. 스마트폰도 넓게 보면 사물인터넷의 범주 안에 들어가 있다고 볼 수 있다. 휴대폰이라는 전자기기는 인터넷이 가능해 졌고 터치스크린의 기술과 더불어 누구나 쉽게 조작이 가능한 사용자 인터페이스와 카메라 및 동영상 재생, GPS, MP3, 수 십 만개의 애플리케이션 바다에서 원하는 애플리케이션을 내려 받아 여러 가지 편리하고 유용한 기능을 쉽게 사용할 수 있게 되었다.

처음에는 음성통화만 가능했던 휴대폰도 이렇게 발전해오고 있다. 전화기를 통한 사람과 사람 간의 통신이 이루어진 것은 약 150년 전이며, 네트워크 기기들은 이미 오래 전부터 다양한 라우팅 프로토콜(Routing Protocol)을 통해 서로 통신하며 인터넷이 원활하게 이루어지기 위한 '길'을 만들고 있었다. 따라서 사람과 사물이 주체가 되는 통신의 관점에서는 사물인터넷은 꽤 오래 전부터 이루어져온 개념이다. 다만 지금의 사물인터넷 개념은 모든 산업의 모든 제품과 서비스가 포함되는 확장된 개념이라는 점에서 관점을 달리하는 것이다.

휴대폰의 역사를 보면 이렇게 우리가 예상치 못한 전개로 인하여 기술력이 눈부시게 발전을 하고 수많은 편리와 효율성을 제공하고 우리의 삶은 다양한 방식으로 바뀌게 되었다. 이제는 그 발자취를 우리 주변에서 쉽게 볼 수 있는 냉장고, 옷, 사물함, 세탁기, 자동차, 네비게이션, TV 등 많은 현실세계의 사물들과 가전제품들이 그 뒤를 이을 것으로 보인다. 휴대폰 하나만 인터넷이 되고 어플리케이션이 되어도 세상이 이렇게 편리해지고 빠른 통신으로 초고속 정보화시대가 되었는데 이제는 또 다른 수많은 사물들이 그 뒤를 잇는다면 세상이 또 어떻게 변화되어 갈지 기대가 된다.

IT는 점점 작아지고 있으며 가벼워지고 있고 저렴해지고 있는데 놀랍게도 더 빨라지고 있고 더 대용량화 되어 가고 있고 심지어 더욱더 효율적이고 더 무궁무진한 편리함과 시너지를 제공하고 있다.

이제는 휴대폰뿐만 아니라 우리 주변에 있는 모든 것들이 인터넷과 연결되고 이를 기반으로 상상도 할 수 없을 정도로 다양하고 많은 서비스를 제공할 수 있는 인터넷 기술로서 초-연결 사회를 가능케 할 수 있다.

그리고 한국 IT업체들은 “스마트폰은 곧 범용제품이 될 것이다. 고부가가치를 내건 스마트폰이 PC처럼 저부가가치 IT기기가 될 날이 멀지 않았다. 서둘러 새로운 성장엔진을 찾아내지 못하면 한국 산업과 경제는 큰 충격을 받게 될 것이다”라고 얘기하고 있다. 미래 IT발전에 대한 경각심을 심어주는 말이다.

본 논문은 이러한 사물인터넷 환경에서 고려해야 할 보안에는 어떠한 것들이 있는지, 또 인증에는 어떠한 것들이 있는지 알아보고자 한다.

2장 이론적 고찰

2.1 사물인터넷의 정의

사물인터넷(IoT, Internet of Things)이란 사람, 사물, 공간, 데이터 등 모든 것들(Things)에 인터넷을 접목해 서로 연결되어 이것들이 정보를 생성, 수집하고 공유하고 활용하고 선용되는 것을 말한다. 현재 이처럼 인터넷에 접목되어 실제 활용되고 있는 사물은 1% 미만으로 앞으로 연결 가능한 사물이 확대된다면 IT 역사상 또 한 번의 위대한 혁신이 일어날 것으로 예상된다.

2014년 3월 영국의 데이비드 캐머런 총리와 독일의 앙겔라 메르켈 총리는 세계 최대 정보통신 박람회 세빗(CeBIT)에서 만나 PC와 스마트폰뿐 아니라 '이 세상 모든 것들이 인터넷에 연결되는 새로운 디지털 시대'의 잠재력을 깨닫고 IoT 전략을 세워 한 발 앞서 추진하고 공동 투자하기로 약속하였다.

사물인터넷의 개념은 M2M(Machine to Machine), IoT(Internet of Things)를 거쳐 IoE(Internet of Everything)로 까지 확장되고 있으며, 향후 10년간 총 19조 달러의 어마어마한 경제적 효과가 사물인터넷을 통해 창출될 것으로 추정된다고 Cisco에서 전하고 있다. 또 Cisco는 사물인터넷 미래전망보고서를 통해서 향후 2020년까지 500억 이상의 디바이스가 연결되는 환경이 도래한다고 예상하였다.

`05년 ITU가 처음으로 사물인터넷의 개념을 정립하였다. ITU는

- 언제나, 어디서나, 어느 것과도 연결될 수 있는 것이 사물인터넷 시대의 새로운 통신 환경
- 모바일 인터넷의 활성화는 인간이 정보 접속에 대해 가지고 있던 '시간의 제약'과 '공간의 제약'의 문제를 해결해주었으며, 사물인터넷의 핵심은 ITU가 제안한 PC와- PC, 인간과 인간, 인간과 사물, 사물과 사물을 연결하는 '객체의 제약을 해결하는 것에 있음

결국 사물인터넷은 M2M을 포함하여, 정보의 생산주체와 소비주체가 기기, 사람인 경우를 모두 아우르는 개념이라고 할 수 있다.

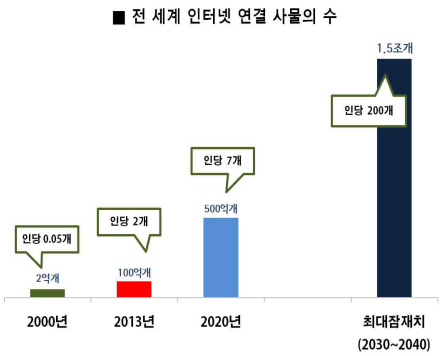
2.2 사물인터넷의 현황 및 동향

여러 미래학자들을 통해 3차 산업혁명이자 인터넷에 이은 2차 디지털 혁명이 될 것이라 예견되는 사물인터넷 시장의 성장 가능성은 무궁무진하다.

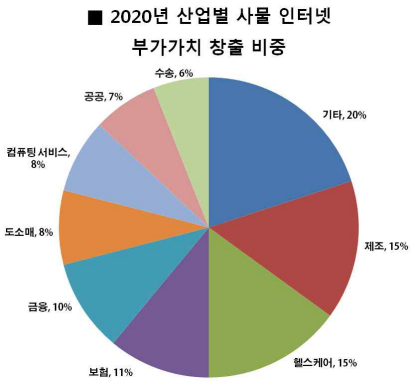
통신·미디어 전문 시장 조사 기관 아이데이트(IDATE)의 2013년 9월 자료에 따르면, 인터넷에 연결된 사물(기계, 통신장비 등)은 2010년 약 40억 개에서 2012년 약 150억 개로 증가할 전망하고 있다. 그리고 아이데이트는 현재와 같은 추세가 이어질 경우 2020년 경 약 800억 개의 사물이 인터넷에 연결될 것이라며 사물인터넷 인프라의 급격한 확대를 예고하고 있다.

세계 네트워크 장비 시장 최대 기업인 시스코(Cisco) 조사에 따르면 2010년 1인당 1.84개에 불과했던 커넥티드 디바이스(인터넷 연결 장비)가 2020년 6.58개로 예측되는 등 숫자로 헤아릴 수 없을 만큼 많은 기기가 네트워크에 연결될 전망이다.

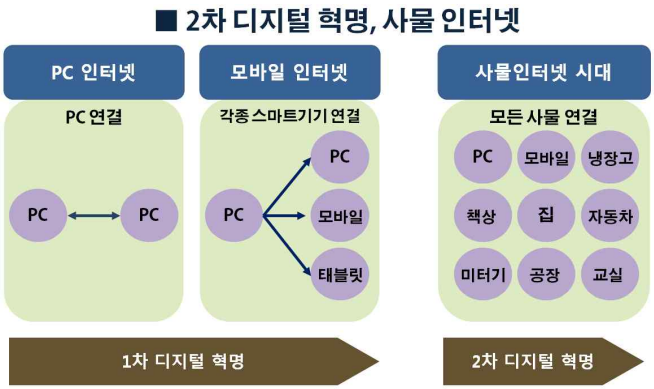
시장조사업체인 Machina Research에 따르면 2013년 기준 전 세계 사물인터넷 시장 규모는 약 2000억달러 수준으로 이 가운데 90%는 선진국이 차지하고 있는 것으로 나타났다. 이는 '기기(device)' 매출 중심으로 산정된 수치이기 때문에 실제 연관 산업을 포함한 시장 규모는 훨씬 클 것으로 예상하였으며 2020년까지 전 세계 사물인터넷 시장 규모가 1조2000억 달러 규모까지 성장될 것으로 분석했다.



< 그림 1. 전 세계 인터넷 연결 사물의 수 >

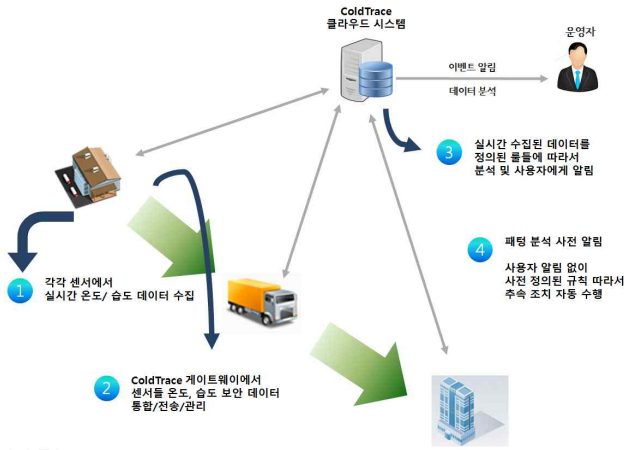


<그림 2. 2020년 산업별 사물 인터넷 부가가치 창출 비중 >

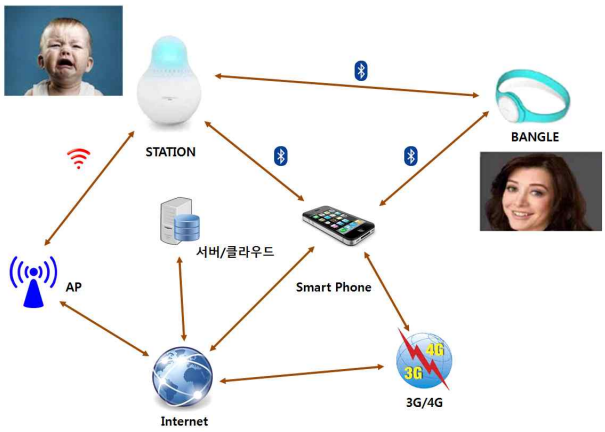


< 그림 3. 2차 디지털 혁명, 사물 인터넷 >

국내 기업들의 사물인터넷 사례를 살펴보면,



< 그림 4. 달리웍스(주)의 ColdTrace : 냉동/냉장 물류창고/차량 실시간 관리 >



< 그림 5. 모뉴엘의 배블 : 아기 울음소리 감지해 부모에게 전달 >

< 그림 6. 한스크리에이티브의 스마트보안, 에너지절감 시스템 >

그 밖에도,

* 스마트 워터 시스템 : 상하수도 센서 설치 → 40~50% 누수 방지
* 스마트 가로등 : 가로등에 센서 설치 → 연간 30% 에너지 절감
* 제조업 서비스화 : 항공, 선박 엔진에 센서 부착해 엔진고장 가능성 미리 탐

지 → 영업이익률 2.5배 증가 (롤스로이스)

* 스마트 약병 : 약 뚜껑 센서 부착, 투약시점 관리 → 98% 복약 이행

등 생활 곳곳에서 사물인터넷이 개발되고 있다.

국내외 사물인터넷의 시장 전망을 살펴보면

● (세계) `13년 2천억 달러 → `20년 1.2조 달러, 연평균 21.8% 성장 전망

● (국내) `13년 2.3조 원 → `20년 17.1조 원, 연평균 32.8% 성장 전망

		2013	2022	GAGR
디바이스	반도체 칩 (Chipsets)	58	281	19.2
	모듈(Modules)	102	477	18.7
	단말기(Terminals)	1,728	3,692	8.8
	합계	1,888	4,450	10.0
이동통신망	GSM/HSPA	31	69	9.3
	CDMA	42	78	7.1
	LTE	14	201	34.5
	기타	8	43	20.5
	합계	95	391	17.0
시스템사업자	제품기기 제조사	12	694	57.0
	시스템통합사업자	14	1,436	67.3
	특정 어플리케이션 입대 사업자	8	904	69.1
	B2B/B2C 서비스 사업자	3	521	77.4
	합계	37	3,555	66.1
서비스 및 어플리케이션	자동차 텔레매틱스	5	1,492	88.4
	차량관제	1	186	78.7
	스마트그리드 및 관리	2	215	68.2
	고정형 무선통신	1	271	86.4
	생활가전	1	1,184	119.5
	기타 분야	1	204	80.6
	합계	11	3,552	90.0
총계		2,031	11,948	21.8

< 표 1. 국내외 사물인터넷 시장 전망 > 단위 : 억 달러, %

2.3 사물인터넷 보안의 필요성

개인정보유출과 바이러스유포는 모두 보안이 취약한 PC와 서버로부터 시작되었다. 전자계산기를 개발할 때만 하더라도 이러한 개인정보유출은 모두 예견되었던 사항은 아닐 것이다. 전자계산기 개발과 네트워크의 구축은 모두 보안을 염두해 두지 않고 구축되었다. IT세상은 갑자기 보안이 절실해 졌고 IT 기반 자체가 보안을 신경 쓰지 않고 구축되었기 때문에 IT 발전이 꽤 진행되어있는 상태에서 완벽한 보안을 접목하기란 불가능에 가까웠을 것이다.

그러나 오늘도 컴퓨팅기술은 발전하고 IT는 발전하고 있을 것이다. 물론 보안기술도 발전하고 있지만 모든 정보를 완벽히 보호할 만큼의 구현이 가능할까?

이렇게 하루하루가 다르게 IT 기술은 발전하고 있지만 위험요소인 컴퓨터와 같은 디바이스 또한 늘어나고 있다. 컴퓨터가 탄생하지 않았다면 우리의 개인정보가 공유되어질 일도 없었을 것이다. 하지만 컴퓨터를 사용하지 않을 수는 없다. 그렇기 때문에 우리가 컴퓨터 보안을 더욱 연구하고 구현해 나아가는 것은 IT 발전에 있어서 큰 숙제이지 사명일 것이다.

미국 시장조사 기관인 가트너(Gartner)는 2020년에는 260억 개의 사물이 연결되어 약 1조 9천억 달러에 달하는 시장이 창출될 것이라고 예측했다. 한편, 미국 국제전략연구소(CSIS)는 해킹으로 인한 경제적 손실을 연간 약 4천 450억 달러로 추정하며 보안의 중요성을 강조했다.

지금까지는 컴퓨터와 서버가 해킹을 당했지만 새로운 플랫폼인 사물인터넷이 등장하면서 위험요소가 새롭게 등장하는 것이다.

사물인터넷이 우리의 생활에 새로운 가치를 가져다주고 더 차원 높은 서비스를 제공할 것은 의심의 여지가 없다. 하지만 컴퓨터가 우리의 생활에 필수에 가까운 매체임에 동시에 해킹을 당할 위험요소임에도 틀림이 없다.

네트워크로 연결된 사물의 개수가 증가할수록 해커의 공격 대상은 물론 공격 루트는 다양해지고, 그 피해가 기존 사이버 세계의 정보유출 및 금전피해를 넘어 인간의 생명까지 위협할 정도로 심각한 영향을 미칠 수 있다.

이렇게 IT발전과 새로운 패러다임, 플랫폼이 창조되어진다고 해서 좋아할 수만은 없는 것이다. 새로운 위험요소가 늘어나는 것뿐인 것이다. 어쩌면 그

위험의 수준이 더욱 높아질 수 있는 것이다. 왜냐하면 인터넷 연결 매체가 이제는 PC와 스마트폰을 넘어서 우리의 생활필수품인 거의 모든 사물이 인터넷 연결 매체가 되어가고 있기 때문이다. 아기를 잘 돌보기 위해서 집 안에 설치해 놓은 가정용 CCTV가 해킹 당했다고 생각해 보면 개인정보유출은 아니지만 더 심각한 사생활보호의 심각한 침해가 우려될 수 있는 것이다. 한 가지 더, 냉장고가 해킹 당했다면 냉장고 전원을 off 당하는 순간 냉장고 안의 음식물은 모두 버려야 할 것이다. 가정용 CCTV와 냉장고만 해킹 당해도 나의 일상생활이 엉망진창이 되어진다. 또, DDoS(분산서비스거부) 공격에 냉장고 및 세탁기 등의 스마트 가전제품이 좀비 PC로 이용되기도 했다. 더욱이, 글로벌 해킹 컨퍼런스인 '블랙햇(Blackhat) 2013'에서는 차량을 해킹하여 가속 페달 및 운전대를 임의 조작하는 등 생명까지 위협할 수 있음을 보여줬다.

이렇게 사물인터넷의 발전은 우리에게 새로운 가치와 서비스의 창출만 가져다주지는 않을 것이다.

우리는 카드사와 금융업, 통신사 등의 많은 기업에게 개인정보를 주고 서비스를 제공 받고 있다. 하지만 기업들의 보안기술과 수준은 우리들의 소중한 개인정보를 지키기에는 부족해 보인다.

앞으로 사물인터넷 사업과 시장이 발전함에 따라 우리가 개인정보를 주고 서비스를 제공 받아야 할 기업들이 수 없이 많아질 것이다. 하지만 우리의 개인정보가 완벽히 보호될 약속을 어느 기업에서 할 수 있을까?

이러한 문제점들 해결하고 개선해 나아가는 것이 IT업계 보안 종사자 및 전문가들이 갖고 있어야 할 숙제일 것이다.

3장 사물인터넷에서의 보안

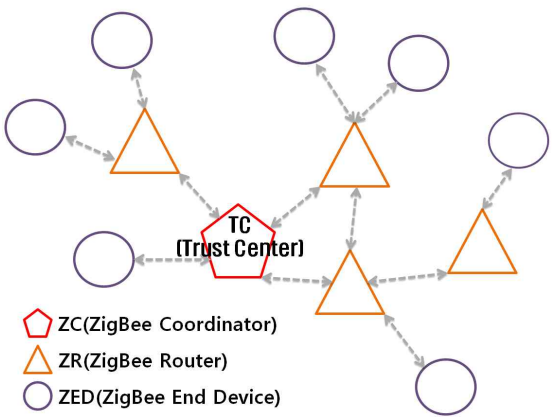
3.1 통신/네트워크 보안 기술

3.1.1 ZigBee 보안 기술

ZigBee는 센서 네트워크 기술 중 가장 대표적인 기술이다. 사물인터넷에서 센서 네트워크가 중요시 되는 만큼 센서 네트워크의 보안, 즉, ZigBee 보안 기술이야 말로 정말 중요하다고 볼 수 있다.

우선 ZigBee란 'Zigzag'와 벌을 뜻하는 'Bee'의 합성어로 벌이 꽃을 쫓아 옮겨 다니듯이 여기저기 구석구석 움직이며 통신한다는 뜻을 담고 있다. 250Kbps 이하의 저속 국제 표준인 IEEE 802.15.4 물리계층 기반의 무선 네트워킹 기술로 저전력, 저비용, 저속이 특징이다. 반경 30m 내에서 20~250kbps의 속도로 데이터를 전송하며 하나의 무선 네트워크에 최대 255대의 기기를 연결할 수 있다.

즉, 지그비는 휴대전화나 무선LAN의 개념으로, 기존의 기술과 다른 특징은 전력소모를 최소화하는 대신 소량의 정보를 소통시키는 개념이다. 작은 크기로 홈 네트워크 등 유비쿼터스 컴퓨팅을 위한 핵심 기술로 각광받고 있다. 그러나 통신할 수 있는 정보량이 한정되어 있어 높은 수준의 보안 기술을 적용하기는 어렵다는 단점이 있다.



< 그림 7. ZigBee 네트워크 구조 >

[그림 ZigBee 네트워크 구조]는 ZigBee 네트워크의 구조이다. ZigBee 네트워크는 역할에 따라서 ZC(ZigBee Coordinator)와 ZR(ZigBee Router), ZED(ZigBee End Device)로 구성이 된다.

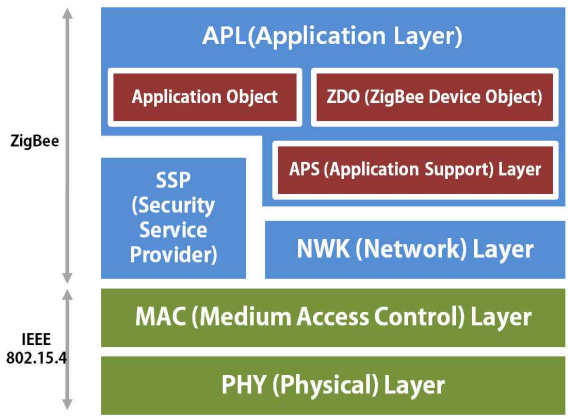
ZC는 ZigBee 네트워크 내에 하나만 존재하며, 네트워크내의 모든 장치들에 대한 정보의 관리 및 다른 ZigBee 네트워크와의 통신을 담당한다. ZC는 FFD(Full-function Device)를 사용하는데, FFD는 ZigBee에서 요구하는 정보관리, 네트워크제어, 데이터 수집 등의 모든 기능을 가지고 있는 장치로, ZigBee 네트워크 내에서 어떤 역할로도 쓰일 수 있다.

ZR은 보통 FFD로 ZigBee 네트워크 내에서 데이터전송범위가 작은 ZED의 데이터를 수집하여 전달하는 역할을 한다. ZC보다는 필요한 기능이 적어 메모리를 적게 사용하므로 상대적으로 단말기의 비용이 더 적게 들어간다.

ZED는 ZigBee 네트워크의 가장 하위에 존재하는 장치들로 데이터를 측정하여 전송하는 역할을 가지고 있다. ZED는 RFD(Reduced-function Device)를 사용하는데, RFD는 성능에 제약이 있어 ZigBee 네트워크내의 데이터의 수집이나 일방적인 데이터전송 등의 특정한 역할만을 수행할 수 있다. ZED는 ZR이나 ZC와 통신할 수 있으며, 큰 기능을 필요로 하지 않아 단말 비용이 저렴하기 때문에 네트워크 구성에 유리하다는 장점을 가지고 있다.

ZC내에 존재하는 TC(Trust Center)가 네트워크내의 모든 장치들에 대한 관리를 담당한다. TC는 ZigBee 네트워크의 모든 키를 관리하고, 주기적으로 키를 업데이트하여 전달해준다. 새로운 키는 기존의 키로 암호화되어 브로드캐스트 된다.

ZigBee 보안 기술의 구조를 보면



< 그림 8. ZigBee 스택구조 >

ZigBee는 [그림 ZigBee 스택구조]과 같이 802.15.4에서 정의된 두 개의 계층인 PHY(Physical) 계층과 MAC(Medium Access Control) 계층을 기반으로 하며, 그 위에 ZigBee Alliance에서 정의한 두 개의 ZigBee계층인 NWK(네트워크) 계층과 APL(Application) 계층을 추가한 형태로 구성된다.

ZigBee는 이 구조에서 Application object를 구동시키게 된다. ZigBee의 계층 중 APL은 보조적인 역할을 하는 두 가지의 내부계층을 포함하고 있는데, 하나는 ZDO(ZigBee 장치 Object)이고 다른 하나는 APS(Application Support Sublayer)이다. 보안서비스를 제공해주는 SSP(Security Service Provider)는 별도로 존재하며 APS와 NWK에 보안서비스를 제공한다.

ZigBee의 각각의 계층들은 모두 다른 역할을 가지고 있다. 첫 번째로 PHY는 무선통신의 기본적인 기능을 가지고 있는 계층으로 정해진 통신설정에 맞추어 데이터를 전송하는 역할을 담당한다. 두 번째로 MAC은 이웃하는 장치간의 데이터 전송을 담당하며, 802.15.4에서 정의하고 있는 보안 서비스를 지원한다. 세 번째인 NWK는 ZigBee 네트워크에 대한 신규가입 및 주소할당, 전송프레임에 대한 라우팅의 역할을 담당하고 있다. 네 번째인 APS는 프로그램이 작동하는 과정에서 Application object를 프레임으로 작성하고 이를 하위계층과 연결시키는 역할을 맡고 있다. 다섯 번 째인 ZDO는 장치들의 정보 및 정책을 결정하는 역할을 담당한다. 마지막으로 SSP는 ZigBee내에서 사용되는 보안에 대한 서비스를 제공하고 있다. 보안이 필요한 계층은 SSP로부터 서비스를 제공받아 자신의 프레임을 암호화하게 되는데, Application object를 프레임으로 작성하는 APS와 ZigBee 네트워크에서 신규가입에 대한 인증을 담당하는 NWK가 보안서비스를 필요로 한다. 위에서도 언급했듯이 ZigBee는 강력한 보안프로토콜을 사용할 수 없기 때문에, 비교적 효율적인 보안기능을 구상하여 탑재하고 있다.

ZigBee는 SSM(Standard Security Mode)이나 HSM(High Security Mode) 중에 하나로 작동한다. SSM은 낮은 수준의 보안을 요구하는 환경을 위하여 설계되었고, HSM은 높은 수준의 보안을 요구하는 환경을 위하여 설계되었다.

ZigBee의 암호화는 Open Trust Model을 사용하는데, 이는 각 장치내의 모든 계층과 모든 프로그램들 사이에서 신뢰성이 보장된다는 개념으로, 각각의 장치는 자신에 대한 신뢰성만 보장하여 다른 장치가 어떤 암호화과정을 거치는지 알 수가 없게 하는 방법이다. 결국 내부의 신뢰성은 보장이 되는 상태이기

때문에 외부로의 전송과정에서의 위협만 제어하면 된다. 이런 기본 환경에서 ZigBee는 128비트 대칭키 블록암호화 방식(AES-128)을 사용하여 키의 암호화를 제공하며, CCM* 알고리즘을 사용하여 무결성과 기밀성에 대한 선별적인 서비스를 적용할 수 있도록 하고 있다.

CCM* 알고리즘은 128비트 블록 암호화방식을 사용하여 암호화와 인증과정을 포괄적으로 제공할 수 있는 기법이다. ZigBee에서는 AES-CCM*방식을 사용하는데, 이는 IEEE에서 정의한 802.15.4에 서 제공되는 AES-CCM을 확장한 것으로 암호화기능이나 인증기능을 각각 제공할 수 있으며, 필요에 따라서 두 가지 기능을 한 번에 제공할 수 도 있다. CCM*의 암호화기능은 총 8가지가 있다.

모드	적용내용
No Security	보안 없음
AES-CBC-MAC-32(MIC-32)	32비트 메시지 인증
AES-CBC-MAC-64(MIC-64)	64비트 메시지 인증
AES-CBC-MAC-128(MIC-128)	128비트 메시지 인증
AES-CTR(ENC)	암호화만 적용
AES-CCM-32	32비트 암호화 및 메시지 인증
AES-CCM-64	64비트 암호화 및 메시지 인증
AES-CCM-128	128비트 암호화 및 메시지 인증

< 표 2. CCM* 운영모드 >

현재 사용되고 있는 보안모드는 프레임의 필드 값에서 확인할 수 있는데 먼저 기본적인 프레임 구조는

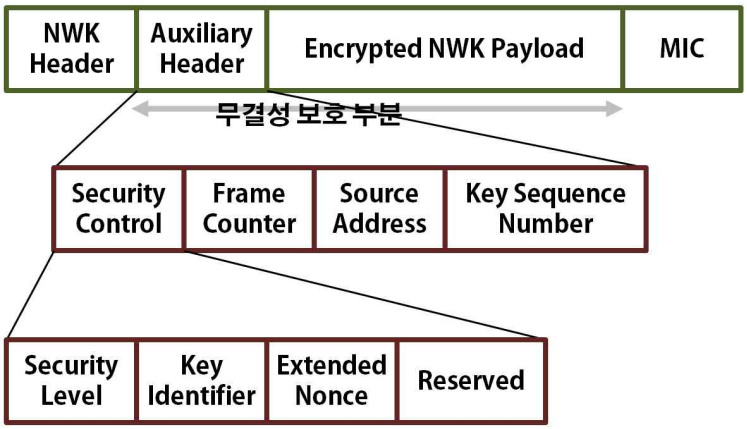
< 그림 9. ZigBee 프레임 >

보안 모드를 사용하지 않는 일반 ZigBee 프레임이다.
보안모드가 사용되기 시작하면 필요에 따라서 보조헤더(Auxiliary Header)나

MIC(Message Integrity Code)를 추가하기도 하는데, 어느 계층에서 추가되는가에 따라서 프레임의 구성이 달라진다. MIC를 사용하는 이유는 각 계층별로 헤더 및 보조헤더와 Payload가 전송과정에서 변조가 없었다는 무결성을 보장하기 위함이다. 그림4는 계층에 따라 내용이 추가된 프레임의 형태를 보여준다. [그림 ZigBee 프레임]는 NWK의 프레임을 그림 [그림 보조헤더에 MIC가 추가된 프레임]는 APS의 프레임을 나타내고 있다.

< 그림 10. 보조헤더에 MIC가 추가된 프레임 >

NWK 프레임에 대한 기밀성 및 무결성 제공



< 그림 11. APS 프레임에 대한 무결성 제공 >

APS 프레임에 대한 기밀성 및 무결성을 제공한다.

Security Level : CCM*모드 사용 여부
Key Identifier : 사용된 Key의 종류
Extended Nonce : Aux헤더 내 Source Address 포함 여부
Frame Counter : 재생 공격 방지를 위한 프레임 번호

Source Address : 송신 디바이스 주소
Key Sequence Number : Key Identifier 가 NK 일 때 사용

Security control 필드는 작동중인 CCM* 모드 값을 가지고 있는 Security level, 키의 종류를 알려주는 키 identifier, 불필요한 필드사용방지를 위하여 Source address의 포함여부를 알려주는 Extended nonce의 정보를 가지고 있으며, Frame counter 필드는 프레임의 재생공격을 방지하기 위한 프레임의 현재성을 제공하기 위하여 사용된다. 키 sequence number 필드는 Security control 필드의 identifier 보조필드의 값이 1일 때만 존재하는데, 즉, 네트워크의 모든 장치들이 공유하는 NK(네트워크 Key)의 사용 시에만 해당필드의 값이 존재한다. APS 헤더 또한 counter 필드를 가지고 있는데 이는 APS프레임의 복사를 방지하기 위함이며, 새로운 전송이 일어날 때마다 필드의 값
이 증가한다.

ZC는 NIB(네트워크 Layer Information Base)에서 NWK의 보안모드 속성 값인 nwkSecurityLevel을 확인하고, 그 값에 따라서 CCM* 모드 중 하나를 선택하여 네트워크의 보안수준을 설정한다. 만약 nwkSecurityLevel의 속성 값이 0으로 되어있다면, 네트워크는 unsecure한 상태로, 다른 값을 가지고 있으면 secure한 상태로 판단할 수 있다. 또한 AIB(Application Support Layer Information Base)에서 apsTrustCenterAddress의 속성 값 설정에 따라서 TC의 주소를 설정한다. TC의 기본 주소 값은 ZC의 고유 주소와 같다.

그리고 TC는 자신이 관리하는 ZigBee 네트워크 내에 존재하는 암호화키인 Master 키, Link 키, NK를 모두 유지, 관리한다. 각각의 키의 역할은 다음 표와 같다.

키	역활
MK (Master Key)	● Link 키 생성을 위한 Symmetric 키 Establishment Perocedure(SKKE) 에서, 두 개의 장치 사이에 초기에 공유되어야 하는 비밀 키의 역할. ● Trust Center와 노드사이에 공유되는 키를 TC-MK(Trust Center Master Key)로, 장치 간에 공유되는 키를 AP-MK(Application Layer Master Key)라고 부른다.
LK (Link Key)	● 두 개의 장치의 Application Layer사이에서 unicast로 전달되는 메시지를 암호화 ● Trust Center와 공유하는 키를 TC-LK(Trust Center Link Key)라고 부르며, 장치 간에 공유되는 키를 AP-LK(Application Layer Link Key)라고 부른다.
NK (Network Key)	● NWK의 보안을 담당 ● 네트워크 내의 모든 장치가 함께 공유 ● •SSM에서 사용되는 NK인 SSNK(Standard Security 네트워크 Key)는 암호화 시키지 않고 서도 전송되지만, HSM으로 동작할 때의 NK인 HSNK(High Security Network Key)는 암호화되어 전송된다.

< 표 3. 암호화키의 종류 및 역할 >

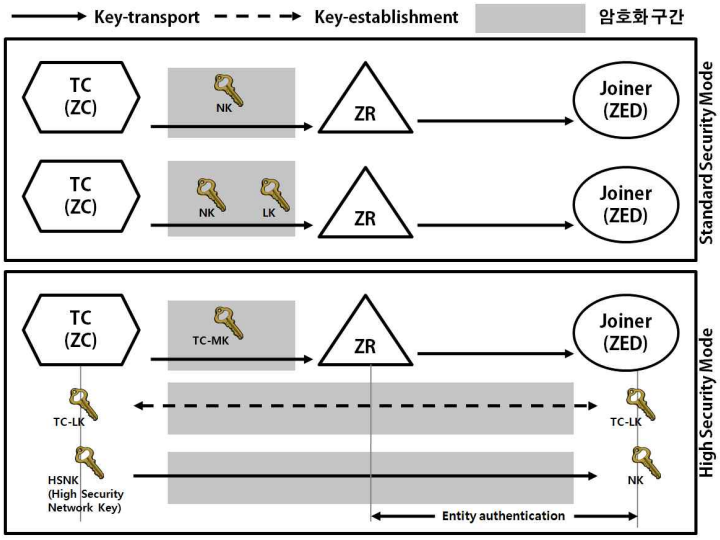
다음은 키 전달 과정이다.

ZigBee 장치들은 설정된 보안모드 내에서 이 3가지 종류의 키들을 사용하여 암호화작업을 수행해야 하는데, 각각의 키들은 서로 다른 방법을 통하여 획득될 수 있다. ZigBee 네트워크에서는 키를 얻을 수 있는 방법이 3가지가 있다. 첫 번째 방법은 key-transport로써 무선통신을 이용하여 다른 ZigBee 장치(ZC(TC), ZR)로부터 키를 전달받는 방법이다. 네트워크 내에서 가장 일반적으로 사용되는 방법이지만 전달과정에서 도청이 이루어지면 키가 노출될 수 있다는 문제점이 있기 때문에 전달과정에서의 암호화를 필요로 한다. 두 번째 방법은 key-establishment로 먼저 두 장치가 상호간에 신뢰성을 확인한 다음, 확인과정에서 주고받은 데이터를 가지고 새로운 키를 만들어내는 방법이다. 신뢰성의 확인은 기존에 설정되어있는 key를 사용하며, 확인과정에서 추가적으로 생성되는 정보를 혼합하여 새로운 key를 계산해낸다. ZigBee에서는 MK를 사용하여 LK를 도출하는 방법을 사용하고 있다. 세 번째 방법은 Pre-installation으로 미리 ZigBee 장치 안에 네트워크에서 사용가능 한 키를 미리 입력해놓는 방식이다. 주로 생산과정에서 키를 주입하는 방법이나 설치시에 관리자가 직접 키를 주입하는 방식을 사용한다. 다음의 표는 위에서 설명된 방식을 가지고 각각의 key 들을 얻을 수 있는 경우를 나타낸다.

	MK	LK	NK
key-transport	YES	YES	YES
key-establishment	NO	YES	NO
Pre-installation	YES	YES	YES

< 표 4. 키 종류별 획득방법 >

ZigBee 네트워크에서는 가입하려는 장치의 키의 설정에 따라서 키의 전달과정이 달라질 수가 있다. 새로 가입하는 장치를 joiner라고 하자. 만약 joiner안에 현재 네트워크에서 사용 중인 NK나 TC-MK 혹은 TC-LK가 Pre-installation되지 않은 상태라면, 프로그램을 암호화되지 않은 경로를 통하여 전달되는 TC-MK나 TC-LK 또는 사용 중인 NK중 하나를 전달받을 때까지 대기해야한다.

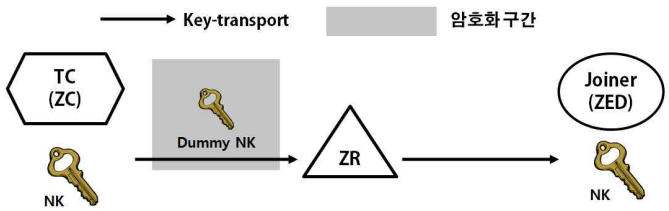


< 그림 12. ZigBee Security mode 별 키 전달 과정 >

<그림 12 >에서는 프로그램의 NK가 Pre-installation되지 않은 상황에서

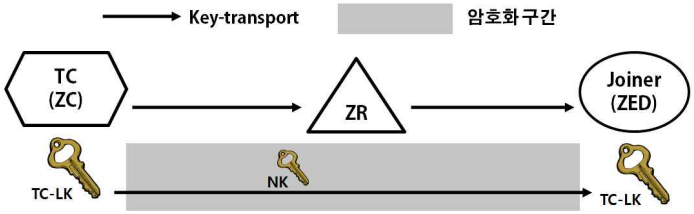
joiner가 가입할 때의 상황을 나타낸 것이다. 이 경우에 joiner는 사용 중인 NK나, TC-MK 또는 TC-LK를 알 수가 없다. 따라서 joiner는 위에서 언급했듯이 비 암호화된 경로를 통하여 키를 전달받을 때까지 대기해야한다. SSM에서는 비 암호화된 경로를 통하여 NK를 전송하거나 TC-LK를 사용하여 NK를 암호화하고 이를 전송하게 된다. HSM에서는 TC가 ZR를 거쳐서 TC-MK를 joiner에게 전달하게 되면, 전달된 TC-MK을 사용하여 TC와 joiner사이에 TC-LK 키를 설정하게 된다. 이렇게 설정된 TC-LK를 통하여 TC로부터 joiner로 NK(High security 네트워크 key)가 전송되며, 전송된 NK를 가지고 ZR과 joiner간의 개체인증을 진행하게 된다.

반대로 joiner에 키가 Pre-installation이 되어있는 경우도 존재할 수 있다. 이 경우에는 어떤 키가 미리 설정되었는가에 따라서 진행과정이 달라진다. Pre-installation에서 설정되는 키는 인증과정 시에 비 암호화경로를 따라서 전달되던 정보들을 미리 저장해 두는 것이다.



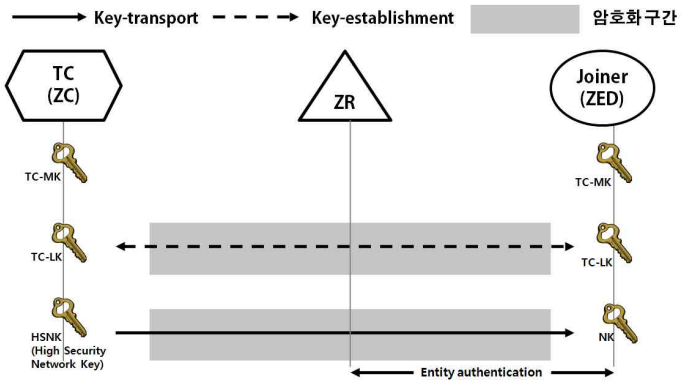
< 그림 13. NK의 Pre-installation >

< 그림 13 >과 같이 SSM에서 NK가 미리 설정되어 있다면, NK를 위한 출력 frame counter를 0으로 설정하고, 입력 frame counter를 비워둔 다음, TC로부터 Dummy NK가 전달되는 것을 기다리게 된다. Dummy NK는 모두 0으로 채워져 있게 된다.



< 그림 14. TC-LK의 Pre-installation >

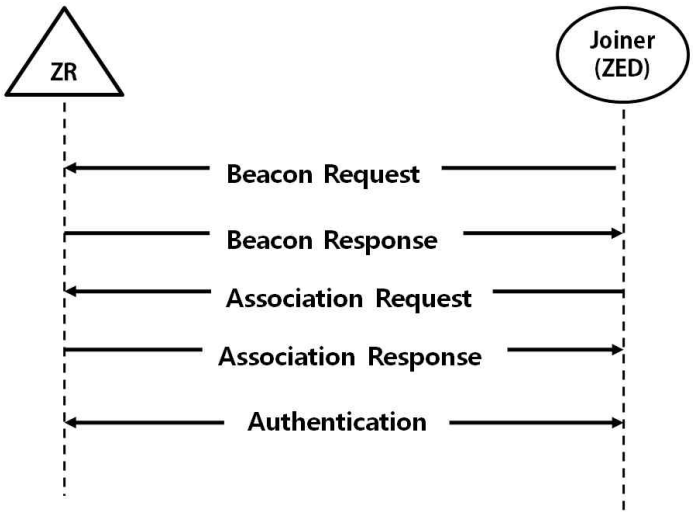
< 그림 14 >과 같이 SSM에서 TC-LK 키가 설정되어 있다면, TC-LK로 암호화된 NK를 TC에서 joiner로 바로 전달하게 된다. 사전설정이 안되어 있을 때는 ZR를 거쳐서 키가 전달되었지만, TC-LK가 설정되어 있다면, joiner로 바로 암호화된 NK가 전송될 수 있다.



< 그림 15. TC-MK의 Pre-installation >

< 그림 15 >와 같이 HSM에서 TC-MK가 설정되어 있다면, 바로 TC와 joiner사이에 TC-LK키 설정이 이루어진다. TC Link 키가 설정되고 나면 이 키를 사용하여 NK(High Security NK)를 joiner로 전송하게 된다.

인증과정에서는, joiner가 secured 네트워크의 가입을 하려고 할 때, joiner는 router와 그림9와 같은 가입과정을 거쳐야 한다.



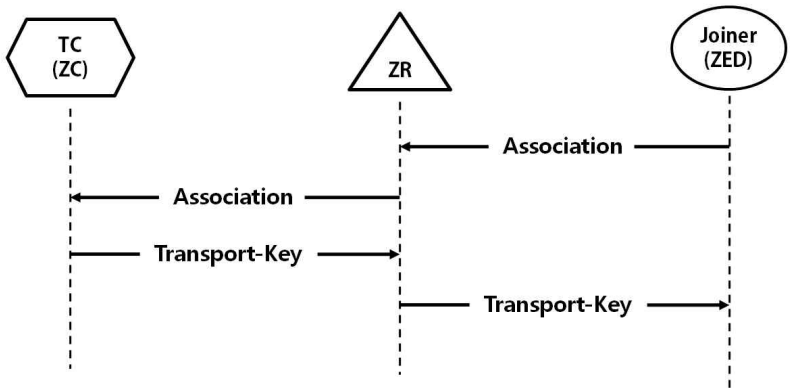
< 그림 16. Secured 네트워크의 가입과정 >

joiner는 Beacon을 사용하여 가입에 대한 신호를 보내고 이 응답이 도착하면 ZR과 Joiner사이에 인증절차가 시작된다. Beacon을 사용하는 이유는 ZigBee네트워크의 특성 때문인데, 각각의 장치는 평소에는 대기상태로 있다가 작업할 일이 있을 경우에만 깨어나 작업을 하게 된다. 이는 저 전력을 구현하기 위함으로, 대기상태에 있을 경우 일반적인 신호를 보내면 즉각적인 응답이 불가능하므로 Beacon을 써서 작업을 요청해 두면 장치가 깨어났을 때 이 Beacon신호를 확인하고 해당 Beacon이 어떤 요청인지 확인한 후 작업을 수행하게 된다. ZR이 가입하겠다는 Beacon에 대한 응답을 보내게 되면, joiner는 인증과정을 진행하게 된다. ZR은 joiner로부터의 가입인증에 대한 응답을 보냄으로써 ZR과 joiner사이에 인증이 이루어지게 된다. 인증과정에서 가장 중요한 부분은 전달된 키를 가지고 이후에 필요한 키를 어떻게 계산해 내는가이다. ZigBee에서는 MK를 사용하여 LK를 계산하는 과정을 필요로 하는데, 키를 계산하는 과정을 간단히 표현하면 다음과 같다.

$$TCLK = h(TCMK(U \| V \| R_u R_v))$$

여기서 U와 V는 상호간에 LK를 만들려는 두 장치의 ID이고, R_u와 R_v는 두 장치가 각자 만들어서 전달하는 난수이다. 각각의 장치는 서로의 ID와 난수를

TC-MK로 암호화한 다음 그 결과를 다시 해시함수에 넣어 결과 값을 구하고 이것을 LK로 사용한다. 전달된 난수에 따라 계산결과가 달라지기 때문에 상호간에 정확한 값이 전달되지 않는다면 키를 계산해 낼 수 없다. 따라서 자신이 보내준 난수를 정확히 알고 있는 가를 통하여 상대방에 대한 인증도 가능하게 된다. 이 과정은 일반적으로 새로 가입하려는 장치들이 거치는 과정이지만, 작동중임에도 키 업데이트에 실패한 네트워크내의 모든 장치도 가장최신의 NK를 수신하기 위해서 이 과정을 거치게 된다. 이 과정을 거치게 되면 joiner는 NK를 획득하여 ZigBee 네트워크를 사용할 수 있게 된다. 다음의 < 그림 17 >은 인증 과정에서 장치의 등록과 키의 전달을 그림으로 표현한 것이다.



< 그림 17. 장치목록 업데이트 및 키 전송 >

joiner가 ZR과의 가입인증과정을 끝내고나면 ZR은 이를 TC에 알리게 된다. TC는 네트워크내의 모든 장치들에 대한 관리를 하고 있기 때문에 새로 네트워크에 가입한 장치를 목록에 추가한 후, ZR에게 필요한 키를 전송한다. 전송된 키는 ZR를 거쳐 joiner에게 전달되며 joiner는 전달받은 키를 가지고 네트워크에서 원하는 작업을 할 수 있게 된다.

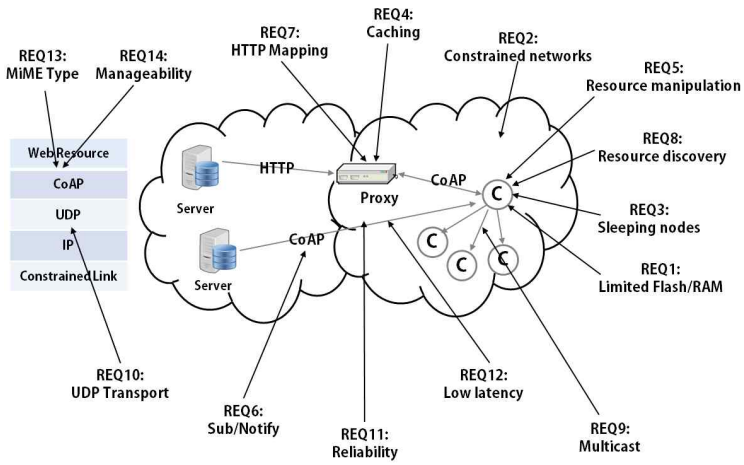
3.1.2 CoAP 보안 기술

사물인터넷은 다양한 기기가 서로 연결되는 네트워크이다. 거기에는 컴퓨터와 스마트폰처럼 높은 처리용량과 메모리를 가지고 있는 노드도 있지만 센서와 같이 작은 메모리와 낮은 처리 성능을 가진 노드들도 인터넷에 연결된다. 이에 인터넷 표준화 단체인 IETF는 다양한 노드를 수용할 수 있는 사물인터넷 프로토콜을 만들기 시작하였고, 그 중 하나가 기존의 HTTP 웹 프로토콜에 대응되는 CoAP(Constrained Application Protocol) 프로토콜이다.

앞으로 CoAP(Constrained Application Protocol)은 차세대 센서 접속 프로토콜의 핵심 역할을 할 것으로 기대되고 있다.

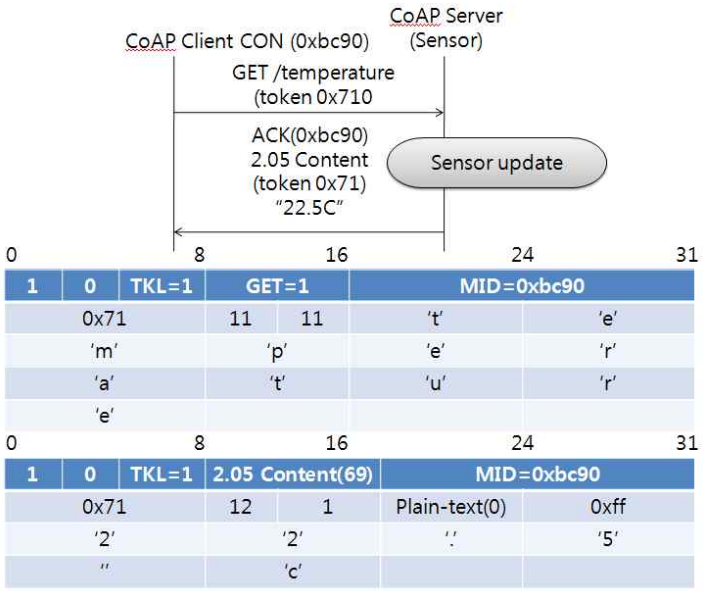
사물인터넷 관련 표준화로는 ITU 및 ETSI가 서비스 모델, 서비스 연동 등 큰 그림을 담당하고 있으며, IETF에서 IP 기반 프로토콜 표준화를 주도하고 있다. 그 밖에 IPSO(Internet Protocol of Smart Objects), OMA 등 기관에서도 사물인터넷 관련 표준 적용을 지원하고 있다.

IETF CoRE 워킹그룹에서는 사물인터넷 노드 사이에 통신할 수 있는 CoAP을 개발하고 있다. < 그림 18 >은 CoRE 워킹그룹의 표준화 범위를 나타내고 있으며, 노드 및 네트워크의 제약사항에 관한 정리, 리소스 등록 및 탐색, 신뢰성 있는 전달, 이벤트 통지, 멀티캐스트, 프록시, 메시지 포맷, 보안 등을 고려하고 있다.



< 그림 18. IRTF CoRE WG 표준화 범위 >

CoAP 프로토콜은 기본적으로 IP 계층 위에 UDP 트랜스포트 계층을 가정하고 있지만, 하위 계층과 독립적으로 설계되어 다른 네트워크 계층 및 트랜스포트 계층에서도 동작할 수 있다. < 그림 19 >는 CoAP에서 제공하는 메시지 포맷의 예를 보인다. CoAP은 기본적으로 작은 메시지 크기 및 쉬운 인코딩, 디코딩을 위해 바이너리 인코딩 방식을 사용한다. CoAP은 확인(acknowledgement) 메시지를 받아야만 재전송을 멈추는 확인형(confirmable) 메시지와 응답이 안와도 상관없는 비확인형(Non-confirmable) 메시지를 선택적으로 지원한다. 또한, CoAP 클라이언트가 CoAP 서버(센서노드)를 주기적으로 조회하는 폴링(Polling) 방식 외에 추가로 이벤트가 발생할 경우에 바로 CoAP 서버(센서노드)가 CoAP 클라이언트로 메시지를 전송하는 푸시(push)방식도 지원한다. CoAP 에서는 이를 Observe 확장이라고 한다. CoAP에서는 요청 메시지에 따른 즉시 응담이 곤란한 경우, 지연된 응답 기능이 가능하고, 그 밖에 CoAP서버가 제공하고 있는 목록을 확인할 수 있는 링크 포맷 기능, 큰 데이터를 나누어서 전송할 수 있는 블록단위 전송 기능, 보안 기능 등이 있다.



0	8	16	24	31
1	0	TKL=1	GET=1	MID=0xbc90
0x71		11	11	't'	'e'
'm'		'p'		'e'	'r'
'a'		't'		'u'	'r'
'e'					

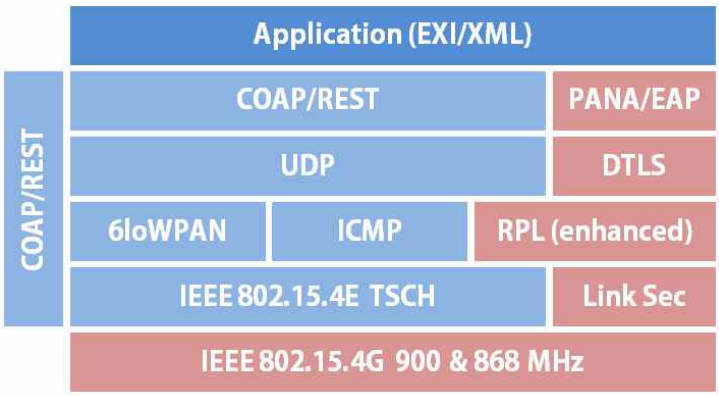
0	8	16	24	31
1	0	TKL=1	2.05 Content(69)	MID=0xbc90
0x71		12	1	Plain-text(0)	0xff
'2'		'2'		'.'	'5'
''		'c'			

< 그림 19. CoAP 메시지 포맷 >

여기까지가 CoAP 프로토콜의 기술이다. 그리고 또 IETF 에서는 표준 CoAP 프로토콜에서는 보안을 위해 DTLS를 사용할 것을 강력히 권고하고 있다. 그 이유는 사물인터넷에는 제약된 환경에서 제한된 자원을 가진 센서 디바이스들이 존재하는데 상호 작용을 위해 각 디바이스들은 Client/Server 두 가지 모델을 모두 수행할 수 있어야 한다. 이러한 디바이스가 응용 계층에서 데이터를 전송할 수 있어야하기 때문이다.

앞에서 다룬 봐와 같이 CoAP 은 HTTP와 유사하지만, 전송의 효율을 고려하여 TCP 대신 UDP를 전송 프로토콜로 사용한다. 그래서 보안 관점에서는 HTTP가 클라이언트와 서버 간 안전한 데이터 전송을 위해 TLS(Transport Layer Security)를 사용하듯, CoAP에서는 TLS의 UDP 기반 버전인 DTLS(Datagram TLS)를 사용하도록 권고하고 있다.

DTLS 프로토콜은 데이터그램 프로토콜을 위한 통신 프라이버시를 제공한다. 이 프로토콜은 클라이언트/서버 응용 프로그램이 통신하는 과정에서 도청, 간섭, 위조를 방지하기 위해서 설계되었다. DTLS 프로토콜은 전송 계층 보안(TLS) 프로토콜에 바탕을 두고 있으며 동등한 안전성을 보장한다. 기초적인 전송의 데이터그램 시멘틱은 DTLS 프로토콜에 의해 보호된다. 이 표준은 사용자 데이터그램 프로토콜(UDP: User Datagram Protocol)을 사용하는 모든 네트워크에 사용할 수 있는 규격이다. 본 표준은 전송 계층에서 데이터 무결성, 단대단 인증, 기밀성 등의 보안 서비스를 제공하며 UDP를 이용하는 모든 통신 및 응용 서비스에 사용할 수 있다.



< 그림 20. 무선 디바이스 상에서의 프로토콜 구조 >

< 그림 20 >은 무선 디바이스 상에서의 프로토콜 구조를 나타내고 있다. 그림에서 볼 수 있듯이 UDP를 사용하기 때문에 DTLS를 사용하는 것을 볼 수 있다. 이러한 점은 IoT 환경에서도 적용이 된다고 할 수 있다.

DTLS는 TLS를 기반으로 설계된 프로토콜이기 때문에 보통 TLS를 사용하기 위해 OpenSSL을 사용하는 것처럼 DTLS를 사용하고자 하는 유저들은 OpenSSL을 사용한다. 그러므로 OpenSSL상에서의 취약점도 그대로 DTLS에서도 나타나게 된다.

특히나 최근 2014년에 Heartbleed 취약점, Recursion flaw 취약점, Invalid fragment 취약점 등 많은 취약점이 보고되고 있고 이러한 취약점은 고스란히 DTLS를 기반으로 한 IoT 디바이스에 적용되므로 쉽게 공격에 대상이 될 수 있다.

DTLS에서 사용되는 대표적인 암호 알고리즘은 AES 알고리즘이라고 할 수 있다. 하지만 이 AES 알고리즘은 자원이 제한적인 IoT 디바이스에 사용하기에는 비용과 성능 면에서는 부적합하다고 할 수 있다. 최근에 제시된 LEA 알고리즘은 AES 보다 빠른 연산속도를 가지지만 일부 보고서에서는 IoT 환경에 적용은 지속적인 검토가 요구된다고 보고 있다. 그러므로 본 논문에서는 DTLS에서 ChangeCipherSpec의 암호 알고리즘 중 하나로 기존의 경량 암호 알고리즘으로 제안된 PRINCE 알고리즘 및 개량된 Extended PRINCE를 사용할 것을 제안한다. PRINCE는 다른 알고리즘에 비해 하드웨어 최적화가 잘 되어 있는 알고리즘이라고 할 수 있다. PRINCE를 하드웨어로 구현 시 AES-128보다 면적 부분에서 최대 16.35배 정도의 면적을 덜 차지하며 전력 부분에서는 최대 84.8배 정도 전력을 덜 소비한다. PRINCE는 다른 암호 알고리즘인 PRESENT, LED에 대해서도 마찬가지로 면적과 전력 면에서 우수한 성능을 보여주고 있다. 이러한 부분에서 PRINCE는 IoT 디바이스에 사용하기에 알맞은 경량 알고리즘 이라고 할 수 있다.

3.1.3 WiFi 보안 기술

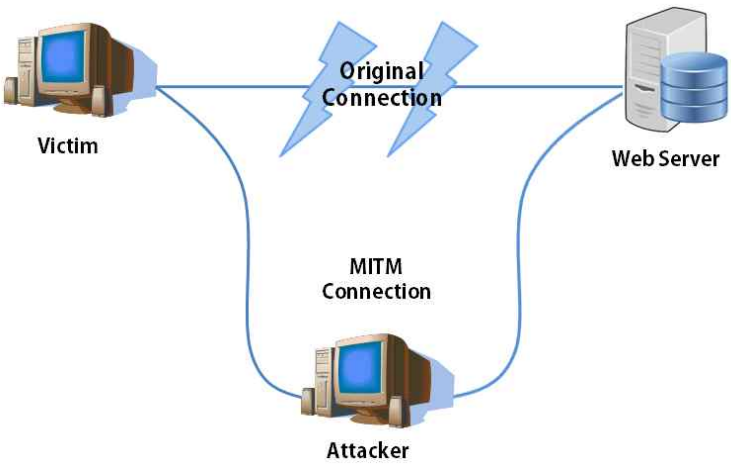
공기를 물리적 매개체로 하는 Wi-Fi는 사용자에게 이동성이나 사용편리성 등 다양한 이점을 제공하지만 각종 해킹이나 정보유출 시도에 노출되기 쉽다는 근본적인 취약성을 갖고 있다. 특정 보안기술이 설정되어 있지 않으면 무선랜 카드가 탑재된 무선기기를 사용하고 있는 사람은 누구나 주변에 설치된 유•무선 공유기나 AP를 이용해 네트워크에 접속할 수 있고, 사용자가 원치 않더라도 건물 내•외부의 네트워크에 자동으로 단말기에서 접속될 수 있어 공격을 받거나 내부정보가 유출될 위험성도 크다. 최근 국내에서도 금융기관의 내부 네트워크 및 시스템을 무선랜을 이용하여 해킹을 시도하다 적발된 사례가 발생하고 있으며, 무선랜 사용자의 사생활 보호, 법적 지위 보호 및 재산권 보호 등 무선랜 보안의 중요성은 점차 증대되고 있는 추세이다. 그러나 여전히 무선랜 보안에 쏟는 투자는 전반적으로 부족하다는 지적과 보도가 많고, 대부분의 기업들이 무선랜을 통해 고객의 정보를 전송하더라도 보안 투자를 안 하거나 얼마든지 위협에 노출될만한 초보단계의 보안기술을 적용해 운영하고 있는 실정이라는 평가다. 또한 방송통신위원회가 지난 4월 발표한 보고서에 따르면 공중 및 사설 AP 총 500만대 중 74%가 무보안 상태인 것으로 파악되어 국내에서의 보안문제는 더욱 심각한 실정이다.

무선랜을 위협하는 주요 공격유형들을 살펴보면, 외부 해커들에 의한 데이터 유출, 비인증 AP(rogue AP),3) 접속 허점, 핫스팟 해킹 등이 주를 이루고 있다. 각각의 보안 침해유형들을 살펴보면 다음과 같다.

첫 번째로 패킷 스니핑(Packet Sniffing)은 네트워크 상에서 자신이 아닌 다른 상대방이 네트워크 트래픽을 도청하는 과정을 말하는 것으로, 해커들은 건물외부에서도 Wi-Fi 기기와 네트워크 간에 전송되는 모든 데이터 패킷을 복사하는 프로그램을 운영할 수 있고, 무료 소프트웨어 툴을 이용해 이 패킷들을 해독할 수도 있다. 이때 유출될 수 있는 정보는 패스워드를 비롯하여 개인들의 사적인 정보 및 기업 비밀까지도 가능한 것으로 알려져 있다.

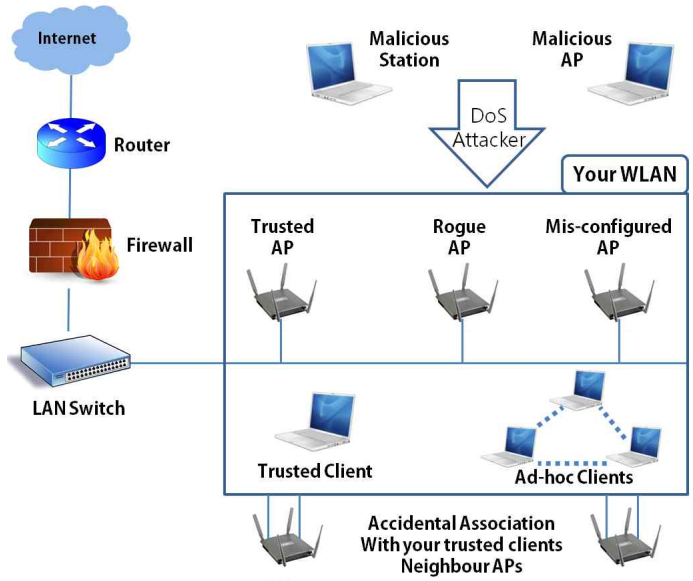
두 번째로 MITM(Man-in-the-Middle 또는 bucket-brigade attack, Janus attack) 공격, MITM 공격은 해커가 메시지를 주고받는 두 사용자 간의 메시지를 마음대로 읽고 조작하는 것으로 이때 당사자들은 해킹을 당하고 있다는 사실을 모른 채 개인정보들을 유출당할 수 있다. MITM 공격을 당한 기기의 작업

은 해커의 컴퓨터에서 모두 확인할 수 있으며, 패킷 스니핑 보다도 훨씬 장기간 더 많은 정보들이 유출 가능성이 있다.

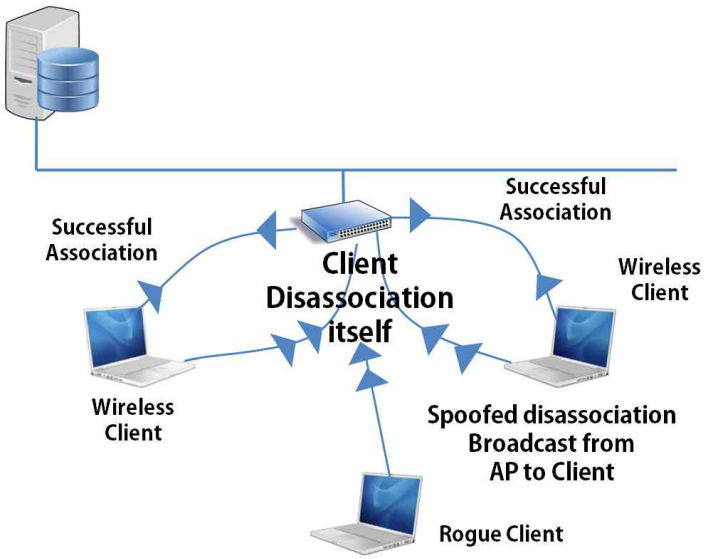


< 그림 21. Man-in-the middle 공격(lllustration of man-in-the-middle attack) >

세 번째는 Evil twin 공격(Wi-Fi 피싱)이다. Wi-Fi 피싱으로 알려진 에빌트윈 공격은 해커가 진짜 AP를 흉내내 암호화되지 않은 가짜 AP를 구축해 발생한다. 가짜 AP는 진짜 AP보다 훨씬 더 강한 신호를 보내 컴퓨터들이 무선 네트워크에 접속을 시도하면 자동으로 가짜 AP에 접속하게 하고, 사용자들은 진짜 AP가 아닌 가짜 AP에 로그온하게 되어 자신도 모르는 사이에 패스워드, 파일, 이메일 계정, 신용카드 정보, 은행 계좌와 같은 개인 데이터들을 해킹 당하게 된다. 에빌트 윈 형태의 공격 위험을 최소화하려면 사용자는 무선 네트워크에 접속하지 않을 때에는 반드시 네트워크 인터페이스 카드를 비활성화해야 한다.



< 그림 22. Wi-Fi 피싱 '에빌트윈' 공격 >



< 그림 23. 비인증 클라이언트가 SSID를 가지고 AP처럼 동작 >

네 번째는 Wardriving, Warwalking, Warchalking 이다.

워드라이빙(Wardriving)은 차량으로 이동하면서 타인의 무선 구내 정보 통신망(LAN)에 무단으로 접속하는 행위로, 광범위한 무선 LAN에서 인터넷을 통해 자료와 자원에 접근하는 경우나 자가 위성 위치 확인 시스템(GPS)을 장착한 차량으로 지역별 무선 액세스 상태를 파악하여 시스템 지도를 만드는 경우에 이용한다. 걸어다니며 이같은 행위를 하는 경우를 Warwalking이라고 부른다.

워초킹(Warchalking)은 불특정 다수에게 무선 인터넷 접속이 가능한 장소, 즉 핫스팟의 위치를 알려주는 기호를 < 그림 24 >와 같이 무선망 접속지점에 표시하여 다른 사람들이 자유로이 무선 인터넷 접속을 할 수 있도록 건물 외벽이나 인도, 빌딩, 표지판, 나무 등에 분필로 표시하는 행위를 말한다. 기업체 빌딩 안에 설치된 무선망 접속점을 이용해 무료로 접속하는 것이 보통이며, 그곳에 분필로 접속점이 있다는 것을 표시해 둔다.

< 그림 24. Warchalking >

다섯 번째로 암호사전 공격(Dictionary Attack)은 일반적으로 패스워드로 많이 사용되는 수천 개의 패스워드를 입력해 하나가 맞을 때까지 계속 시도하는 방식을 말한다. 최근에 이용되고 있는 WPA는 설계 방식 때문에 이 같은 암호

사전공격으로 WPA 네트워크를 공격하는 것은 굉장히 많은 시간이 걸릴 수 있다는 분석이 있었으나, 지난해 보도된 'WPA Cracker'라는 서비스는 $34만 지불하면 20분만에 해킹이 가능하며 일반 가정이나 소규모 사무실에서 많이 사용하는 PSK(Pre-shared Key, 사전공유키) 네트워
크의 취약점을 이용하여 특정 WPA 네트워크를 해킹하는 것으로 알려졌다.

이러한 무선랜 취약점 보안 기술 개발로 초기의 802.11 표준은 원치 않는 무선 네트워크 액세스에 대한 보호의 수단으로 WEP(Wired Equivalent Privacy)를 채택하였으나, 2001년 초 암호학자들이 WEP로 암호화된 데이터를 쉽게 해독될 수 있는 등 WEP 자체의 구조적 취약점을 발견하게 된다. 이에 IEEE는 이러한 약점을 해결하기 위한 802.11i 팀을 새로 만들었고, 2003년 Wi-Fi Alliance에서는 뒤에 나올 802.11i 수정안의 일부였던 WPA(Wi-Fi Protected Access)가 WEP를 대체하게 되었다고 발표했다. 2004년에는 802.11i 표준안(일명 WPA2)이 완전히 비준되었고, IEEE는 WEP-40 및 WEP-104 모두 원래의 보안 목적을 달성하지 못하여 추천하지 않는다고 선언하였다. 현재는 Wi-Fi 보안을 위해 WPA, IEEE 802.11i(WPA2), TKIP, AES 등 다양한 보안기술이 사용되고 있고, 이외에 MAC 인증, 키값 입력 등의 방법이 이용되고 있다.

WEP(Wired Equivalent Privacy)는 무선 LAN 표준을 정의하는 IEEE 802.11 규약의 일부분으로 무선 LAN 운용 간의 보안을 위해 사용되는 기술로서, 대부분의 가정과 소규모 기업에서는 설치가 편리한 WEP를 사용하였다. 그러나 WEP는 데이터 암호화를 위해 RC4 암호를 사용하고, 메시지 인코딩과 디코딩을 위해 40비트 키를 사용하기 때문에, WEP를 적절히 사용하지 않으면 위험에 노출되기 쉽다. 또한 WEP에 사용되는 암호키의 값이 노출되는 경우에는 누구나 통신의 내용을 해독해서 볼 수 있다는 단점이 있으며, 암호키의 값을 모르는 경우에도 이미 널리 알려진 방법을 통해 누구나 데이터의 내용을 해독할 수 있는 취약점이 존재한다.

WPA(Wi-Fi Protected Access)는 Wi-Fi Alliance 및 IEEE(Institute of Electrical and Electronics Engineers)에 의해 제정된 보안 표준으로 Wi-Fi Alliance의 감독 하에 수행하는 인증 프로그램이다. 2002년에 이전의 WEP 방식의 취약점을 보완하기 위한 대안으로 Wi-Fi Alliance에 의해 개발되었으며,

WEP 방식에서는 제공되지 않던 새로운 보안 기능들이 추가되었다. WPA 방식은 TKIP(Temporal Key Integrity Protocol) 및 MIC(Message Integrity Check) 암호화 방식을 사용하며, TKIP는 WEP에서 암호화를 위해 사용했던 RC4 알고리즘을 동일하게 채택하고 향상된 키 관리 방식과 효과적인 메시지 무결성 체크 방식이 추가되었다. WPA 방식의 도입으로 WEP나 802.11 표준에서 제공하던 다른 나머지 보안 기능들이 효과적으로 대체된 바 있다.

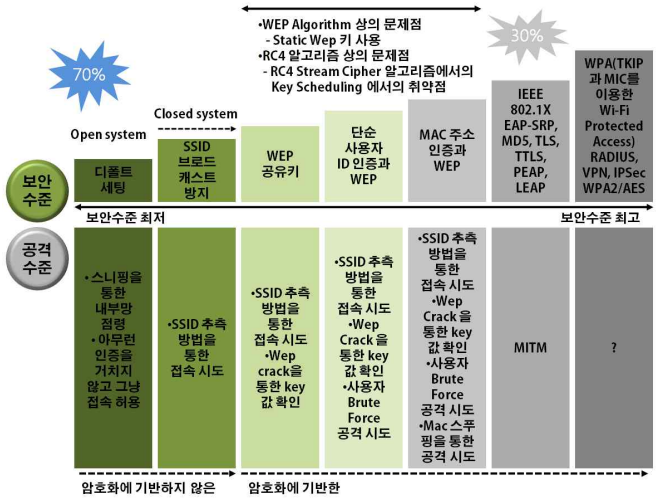
WPA의 향상된 암호화 방식은 공공 핫스팟과 같이 서로 다른 형태의 다양한 802.11 메시지 무결성 체크(MICs)를 처리해야 하는 무선 네트워크에 이상적이라는 평가로, 대부분의 무선 액세스 포인트 장비 및 칩셋 제조사들은 WPA를 지원하고 있다. 그러나 모든 새로운 솔루션은 기존의 문제점들에 대해서는 해결할 수 있지만 완벽한 해결책이 되지는 못하며, WPA 또한 특정 공격에 의해네트워크 전체가 마비될 수 있다는 등의 새로운 문제점들이 계속 발견되었다.

WPA의 후속 버전인 WPA2(Wi-Fi Protected Access 2)는 미 정부 보안 요건인 FIPS140-2을 충족하기 위해 기존 TKIP 암호화 방식을 128비트의 AES(Advanced Encryption Standard) 암호화 방식으로 대체했다. AES 암호화 방식을 채택해 보안 기능이 더욱 강화됐지만, WPA2를 사용하기 위해서는 데이터의 암호화 및 복호화 처리를 위한 전용 칩이 필요하다. WPA2가 제공하는 강력한 보안 기능을 무선 네트워크에 적용하기 위해서는 기존의 무선 장비를 새로운 하드웨어로 업그레이드해야 한다.

SSID(Service Set Identifier)는 무선랜을 독특하게 인식시켜주는 32자의 알파벳 키로, 다른 무선장비가 일시적 혹은 의도적으로 접속하는 것을 막아주는 역할을 한다. 무선기기가 통신하기 위해서는 SSID의 동일성이 인식되어야만 한다. 라우터나 AP에 SSID가 자동으로 전파되는 설정을 해제하면 해당 기기의 SSID는 다른 기기에서 볼 수 없고 수동으로 이를 입력해야만 한다. 그러나 SSID는 강력한 보안책은 아니므로 WEP나 WPA와 같은 다른 보안기술과 함께 사용되어야 한다.

SSID에는 ESSID(the Extended Service Set Identification)와 BSSID(the Basic Service Set Identification)의 두 종류가 있다. 비록 아직은 막연한 의미에서 SSID로 동일하게 사용되지만, AP가 없는 Ad-hoc 네트워크는 BSSID를 사용하고, ESSID는 AP를 포함하여 무선네트워크 인프라 구조에서 사용된

다.



< 그림 25. WLAN 보안 및 공격기술의 발달추이 >

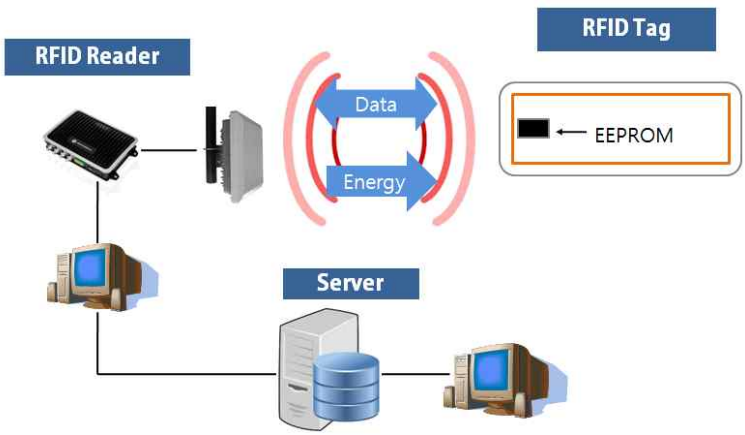
3.1.4 RFID 보안 기술

우선 RFID(Radio Frequency Identification)란 칩과 무선을 통해 식품, 동물, 사물 등 다양한 개체의 정보를 관리할 수 있는 인식 기술을 지칭한다. '전자태그'혹은 '스마트 태그', '전자 라벨', '무선식별' 등으로 불린다. 대상이 되는 사물 등에 RFID 태그를 부착하고 전파를 사용하여 해당 사물 등의 식별정보 및 주변 환경정보를 인식하여 각 사물 등의 정보를 수집·저장·가공 및 활용하는 시스템을 말한다.

RFID 시스템은 정보를 저장하거나 처리하는 태그와 전파를 이용하여 태그정보를 송·수신하는 리더기 및 리더기로부터 정보를 받아 태그정보를 관리하는 백엔드 시스템으로 구성된다.

또, RFID 기술은 상품·동물을 비롯해 일반적인 물체의 자동인식 및 추적을 위해 사용되며 기존 광학기술 기반의 식별 방식인 바코드에 비해 다음과 같은 장점이 있다.

1) 인식속도가 0.01~0.1ch 정도로 바코드에 비해 빠르다.
2) 수십m의 원거리에서도 인실이 가능하다
3) 99.0% 이상의 높은 인식률을 갖는다.
4) 대용량 정보저장이 가능하고 재기록이 용이하다
5) 패스워드 등 보안기술 적용이 가능하다.



< 그림 26. RFID 개념도 >

RFID는 지금까지 유통분야에서 일반적으로 물품관리를 위해 사용된 바코드를 대체할 차세대 인식기술로 꼽힌다. RFID는 판독 및 해독 기능을 하는 판독기(reader)와 정보를 제공하는 태그(tag)로 구성되는데, 제품에 붙이는 태그에 생산, 유통, 보관, 소비의 전 과정에 대한 정보를 담고, 판독기로 하여금 안테나를 통해서 이 정보를 읽도록 한다.

활용범위도 무궁무진하다. 도난과 복제 방지를 위한 목적으로 사용할 수도 있고, 도서관에서는 도서 출납에 이용할 수도 있다. 현재 월-마트를 필두로 베네통, 독일의 유통체인인 메트로 등에서 상용화를 추진 중이다. 우리나라의 경우 RFID는 대중교통 요금징수 시스템은 물론, 그 활용 범위가 넓어져 유통분야뿐 아니라, 동물 추적장치, 자동차 안전장치, 개인 출입 및 접근 허가장치, 전자요금 징수 장치, 생산관리 등 여러 분야로 활용되고 있다.

RFID “태그”라 함은 사물 등에 내장 또는 부착되어 해당 사물에 관한 정보 또는 그 밖의 정보를 기록하고 전파를 이용하여 이들 정보를 송·수신하는 장치를 말한다. 태그는 정보를 저장·처리하기 위한 하나의 마이크로 칩(IC Chip)과 정보를 전송하기 위한 안테나로 구성된다. 태그를 결정하는 주요 요소는 식별자, 전원공급 방식, 동작주파수 등이다.

모든 RFID 태그는 고유 식별자를 가지고 있다. 주로 사용되는 EPCglobal의 전자상품코드 (EPC : Electronic Product Code)는 헤더, 기관명, 상품분류 일련번호 등 네 개의 요소로 구성된다.

< 그림 27. RFID 태그 고유 식별자 >

태그는 전원 공급방식에 따라 능동형과 수동형으로 분류할 수 있다.

1) 능동형 태그(Active Tag)는 자체 전원장치를 가지고 있으며 메모리와 계산능력을 갖추고 있어 원거리 통신이 가능하다. 항만물류 컨테이너 추적 등에 주로 이용된다.
2) 수동형 태그(Passive Tag)는 자체 전원장치가 없는 태그로 RFID 리더기가 보

내는 전파로부터 전원을 공급받아 동작하는 태그이다. 통신거리가 짧으나 소형, 저가로 다양한 분야에서 널리 쓰이는 태그이다.

동작주파수 대역에 따른 태그의 종류는 대략 5가지 정도로 분류된다.

① 저주파 대역 RFID 태그

- 태그 사용 주파수 : 125KHz, 134KHz
- 인식거리 : 60cm 이하
- 동작방식 : 수동형
- 특징 : 액체 등 비금속 장애물 투과성 우수
- 주요 사용분야 : 출입통제, 동물관리
- 보안 기능 : 태그정보 쓰기 금지

  * 보안기능을 강화하기 위해서는 13.56MHz 태그 사용을 권고한다.

< 그림 28. RFID 동물관리 >

< 그림 29. RFID 출입통제 >

② 고주파 대역 RFID 태그(비접촉식 스마트카드 포함)

- 태그 사용 주파수 : 13.56MHz
- 인식거리 : 60cm 이하
- 동작방식[3] : 수동형
- 특징 : 액체 등 비금속 장애물 투과성 우수
- 주요 사용분야 : 출입통제, 도서관리, 전자지불 (교통카드, 복지카드 등)
- 보안 기능 : 리더기 인증, 전송 정보의 암호화

< 그림 30. RFID 전자지불 >

< 그림 31. RFID 도서관리 >

③ 극초단파 대역 능동형 RFID 태그
- 태그 사용 주파수 : 443MHz
- 인식거리 : 50 ~ 100m

3) 능동형 태그도 부분적으로 사용되고 있다.
- 동작방식 : 능동형
- 특징 : 대형 물류 관리에 사용
- 주요 사용분야 : 항만물류
- 보안 기능 : 리더기 인증, 전송 정보의 암호화

< 그림 32. RFID 물류관리 >

④ 극초단파 대역 수동형 RFID 태그
- 태그 사용 주파수 : 908.5 ~ 914MHz[4)]
- 인식거리 : 60cm 이하

- 동작방식[5] : 수동형
- 특징 : 저가, 금속 ·액체 투과성 낮음
- 주요 사용분야 : 유통·물류관리
- 보안 기능 : 태그정보 소거[6], 접근·잠금 패스워드

⑤ 마이크로파 대역 RFID 태그
- 태그 사용 주파수 : 2.45GHz
- 인식거리 : 1m ~ 10m
- 동작방식 : 능동형 또는 수동형
- 특징 : 고가
- 주요 사용분야 : 지폐·상품권, 고가품
- 보안 기능 : 태그정보 쓰기 금지 또는 잠금 기능 등

< 그림 33. RFID 지폐 >

RFID 리더기라 함은 태그의 정보를 활용하기 위해 태그와 송·수신하거나 태그에서 수집된 정보를 백엔드 시스템으로 전소하는 장치를 말한다. 리더기는 수동형 태그에 통신신호를 통해 전원을 공급하고 정보를 교환한다. 또한 능동형 태그가 주기적으로 보내는 신호를 처리하여 정보를 전송한다.

태그와 리더기는 다음 두 가지 방법으로 통신을 개시한다.

1) 리더기가 먼저 신호를 보내는 방식(ITF, Interrogators Talk First)으로 신호를 수신한 태그가 이에 응답함으로써 통신이 이루어니다. 대부분의 수동형 태그가 이 통신방식을 사용한다.
2) 태그가 먼저 신호를 보내는 방식(TTF, Tag Talk First)으로 신호를 받은 리

더기는 태그의 존재를 알 수 있다. 대부분의 능동형 태그가 이 방식을 사용한다. 수동형 태그에도 적용할 수 있는데, 이 경우에는 리더기로부터 전원을 공급받은 후 신호를 보낼 수 있다. TTF방식은 태그가 인증되지 않은 리더기에도 신호를 보내게 되어 보안에 취약할 수 있다.

RFID 시스템의 호환성을 위하여 국제표준기구(ISO/IEC)와 EPCglobal 등에서 국제 및 산업계 표준화를 주도하고 있다.

< 표 5. ISO, IEC 국제 표준 현황 >

표준분야	표준번호	내 용	비 고
명령어, 데이터 형식	15961	명령어 형식	리더기 ↔ 백엔드
	15961	데이터 형식	리더기 정보 대상
고유식별자	15961	UID 형식	태그 대상
무선통신방식	18000-1	18000시리즈 용어	용어정의 규정
	18000-2	134kHz 이하 RFID	동, 식물 관리
	18000-3	13.56MHz RFID	도서관리
	18000-4	2.45GHz RFID	진품확인
	18000-5	860~960MHz RFID	물류유통
	18000-6	433MHz RFID	항만물류
응용 요구사항	TF180001	응용 S/W 요구사항	RFID 응용 대상
스마트카드	14443 15693	비접촉식 카드	근접 카드

1) ISO/IEC에서 제시한 표준 중 14443, 15693과 18000-2·3·4는 단순 잠금 기능[12]만 있다. 18000-7은 잠금 패스워드[13] 설정이 가능하고 18000-6은 태

그정보 소거, 잠금·접근 패스워드 설정까지 가능하다.

2) EPCglobal은 산업계 표준으로 Class 0·1·2가 있으며 주로 사용되는 규격은 Class1Gen2[14]이다. 여기에는 태그정보 소거, 잠금·접근 패스워드 설정의 보안 기능이 있다.

따라서, 소통정보를 보호하기 위해서는 ISO/IEC 18000-6 또는 EPCglobal Class1Gen2 규격의 태그를 사용할 것을 권장한다.

RFID의 보안기술을 살펴보면 물리적 보안, 패스워드 보안, 암호화 보안을 살펴볼 수 있다. 먼저 물리적 보안으로는

가. Faraday Cage

1) 전파의 발산을 차단하는 특수 물질로 만든 용기를 이용하여 태그를 감싸는 방법이다.
2) 정당하지 않은 리더기가 태그정보를 읽는 것을 막기 위하여 알루미늄이나 은박지 등의 금속 또는 망으로 만들어진 용기에 태그를 넣어 보관하거나 이동한다.

나. Active Jamming

1) 강력한 방해전파를 발산하는 기기를 이용하여 기기근처에 있는 모든 RFID 리더기의 작동을 방해하는 기술로 태그정보의 유출을 차단하기 위하여 한시적으로 사용할 수 있다.
2) 이 기술은 원래 정상적인 태그와 리더기간 통신을 방해하는 공격기술로 사용되고 있지만 역으로 근처에 있는 정당하지 않은 리더기에 의해 태그정보가 노출되는 것을 막기 위한 방어기술로도 이용 가능한 방법이다.

다. Kill 명령어

1) 리더기에서 패스워드(8bit)를 포함한 Kill 명령어를 전송하여 태그의 기능을 정지시키는 기법으로 사용자의 프라이버시를 보호하기 위해 사용하는 가장 일반적인 방법이다.
2) 그러나, Kill 명령어가 적용된 후에는 재사용이 안 되기 때문에 제한적인 환경에서만 적용이 가능하다. 예를 들어, 상품 판매 후에는 Kill 명령어를 통해 태

그의 동작을 중지시킴으로써 프라이버시를 보호할 수 있지만 반품 등의 경우에는 작동이 되지 않는 단점이 있다.

라. Blocker 태그

1) 의미 없는 신호를 발생하여 주변 태그의 통신을 방해하는 특수 태그로 정당하지 않은 리더기에 의한 태그정보 유출을 차단하기 위하여 사용한다.
2) 예를 들면, 태그부착 의약품 구입시 Blocker 태그를 사용한 용기에 의약품을 넣으면 어떤 리더기라도 태그정보를 읽을 수 없어 의약품 구입 등의 개인정보를 보호할 수 있다.

마. Clipped 태그

1) 태그 내부의 안테나 연결선을 일부 절단시킴으로써 태그의 통신거리를 줄이는 방법으로 Kill 명령어의 단점을 보완하기 위하여 개발된 태그이다.
2) 이 기술을 적용할 경우 태그의 정보저장 기능은 그대로 유지한 채 정보 송신거리를 대폭 줄임으로써 원거리에서 위치추적 등을 통한 프라이버시침해 가능성을 줄일 수 있다.

4-2. 패스워드 보안기술

가. 접근 패스워드

리더기가 태그정보를 읽으려고 하는 경우 패스워드가 일치하지 않으면 응답하지 않음으로써 태그의 정보유출을 차단하는 기술이다.

나. 잠금 패스워드

태그의 특정 정보만을 보호하기 위하여 그 부분만 패스워들 설정하는 기술로 불법 리더기에 의한 정보유출을 차단하기 위한 방법이다.

다. Kill 패스워드

태그를 더 이상 사용할 필요가 없을 경우에 패스워드를 통해 Kill 명령어를 적용하는 방법이다. 이는 Kill 명령어를 적용할 경우 재상이 안되기 때문에 Kill 명령어 실행 시 다시 한 번 확인하기 위함이다.

4-3. 암호화 보안기술

가. 인 증

1) 인증이란 일반적으로 패스워드, 공개키 암호, 생체정보 등을 이용하여 상대 개체의 정당성을 식별하는 기술로써 RFID 시스템에서는 태그와 리더기의 정당성 확인 등에 적용된다.
2) 인증방법으로는 태그가 정당한 리더기인지를 확인하거나 리더기가 정당한 태그인지를 확인하는 방법, 태그와 리더기간 상호 인증하는 방법 등이 있다.
3) 안전성 측면에서 보면 태그와 리더기간 상호 인증하는 방식이 가장 좋으며 태그의 위·변조 방지, 불법 리더기를 이용한 태그정보 추출을 차단할 수 있다.
4) 현재 비접촉식 스마트카드(13.56MHz)의 경우 주로 Challenge-Response 방식의 인증기술이 적용되고 있다.
5) 수동형 태그에는 메모리와 컴퓨팅 능력 제한 등으로 인하여 인증기술이 보편적으로 적용되지 못하고 있다.
   * 현재 경량화 된 해수함수를 이용하는 인증기술이 연구되고 있으며 태그에 식별 정보를 직접 저장하지 않고 태그 제작시 디지털 회로의 신호출력 값을 고유 식별정보로 활용하는 태그 복제방지 기술도 활용되고 있다.

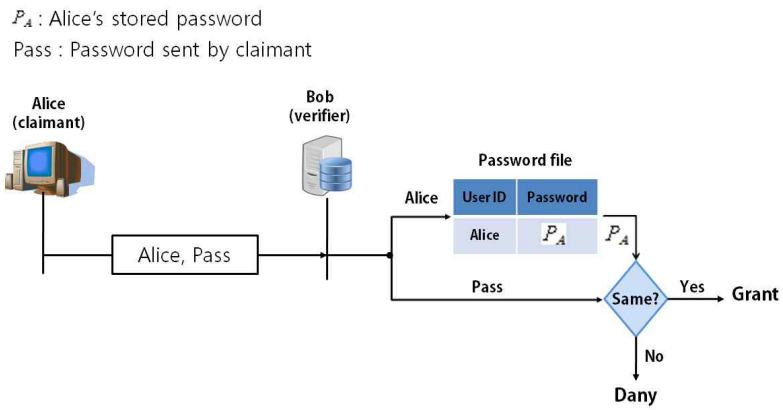
나. 암호화

1) 중요 정보를 보호하기 위하여 평문내용을 제3자가 알아볼 수 없도록 변환시키는 기술로 블록암호, 스트림암호 등을 이용한다.
2) 블록암호란 정보를 일정 크기의 블록 단위로 암호화하는 기술로 AES, 3-DES 등이 널리 사용되고 있으며 국내에는 SEED가 사용 표준으로 제정되어 있다.
3) 현재 비접촉식 스마트카드는 블록암호를 이용한 보안기술의 적용이 가능하며 국가기관에서 사용하기 위해서는 '국가기관용 표준암호' 탑재가 필요하다.
4) 스트림암호는 랜덤 넘버라 불리는 난수열을 이용하여 평문 내용을 비트(bit) 또는 문자 단위로 암호화하는 기술로 일반적으로는 암호화 속도가 블록암호에 비해 빠르다고 할 수 있다. 최근에는 극소형의 RFID 칩에서 동작이 가능한 경량화 된 스트림암호의 개발·적용 노력이 진행되고 있다.

3.1 사물인터넷에서의 인증/인가

3.3.1 ID/PW 기반 인증

ID/PW 기반 인증기술은 인증 기술 중 가장 기본적인 인증 방식으로 주로 서버/클라이언트 인증에서 사용되는 기술이다. 서버는 클라이언트의 최초 등록 시 ID와 PW를 저장하고 있으며, 클라이언트가 접속 시도 시 해당 클라이언트 ID에 해당하는 PW가 서버가 저장하고 있는 ID의 PW와 일치하는 지 확인하는 방식의 인증이다.



< 그림 34. ID/PW 인증 서식도 >

ID/PW 인증 기술은 서버에 패스워드 리스트가 저장되므로 서버에 저장된 클라이언트의 패스워드 리스트가 노출될 경우 인증이 무력화 될 수 있다. 따라서 이를 방지하기 위하여 서버에서 패스워드를 저장할 때 해쉬 함수를 통하여 해쉬값을 저장하며, 인증 시도가 이루어질 경우 서버는 클라이언트가 제출한 PW의 해쉬값을 계산하여 저장된 해쉬값과 검증하는 방식을 채택하는 경우가 많다.

현재 사용되고 있는 ID/PW 기반 인증 시스템은 “약한 인증(Weak Authentication) 시스템”이다. 약한 인증 시스템이란 제3의 공인 기관

(Trusted 3rd Party)에 의존하지 않고, 사전에 교류가 없는 집단과 통신을 하는 인증 프로토콜을 의미한다. 또한 약한 인증 시스템은 네트워크상에 프로토콜이 그대로 노출되거나, 패스워드를 암호화 하지 않은 채 평문으로 통신하거나 해쉬값을 통신하는 경우 역시 약한 프로토콜에 속한다.

"강한 인증 시스템"으로는 EKE(Encrypted Key Exchange) 프로토콜, DH-EKE(Diffie-Hellman Encrypted Key Exchange) 프로토콜 등이 있다. EKE 프로토콜은 패스워드의 인증 시, 대칭키 암호 방식과 공개키 암호 방식을 결합한 메커니즘을 통하여 제3의 공인 기관 없이도 안전성을 제공하며, 사전 공격에 강한 특징을 갖는다. 또한 이후 DH-EKE 프로토콜은 Diffie Hellman이 제안한 키 교환 방식에 기반한 EKE 프로토콜로, 키 교환 프로토콜에서 분배되는 패스워드로 메시지가 암호화되어 통신하는 방식의 프로토콜이다. 또한, Diffie Hellman의 키 교환에 기반하며, 세션 키(Session Key) 생성함수를 통하여 패스워드가 생성되는 SPEKE(Simple Password Exponential Key Exchange)가 등이 제안되고 있다.

ID/PW 기반 인증 시스템은 네트워크 등을 통해 연결된 각종 임베디드 환경에서 역시 사용되고 있는 추세이다. 현재 사용되고 있는 ID/PW 기반 인증 서비스들은 다음과 같다.

가. SSID(Service Set IDentifier) 숨김

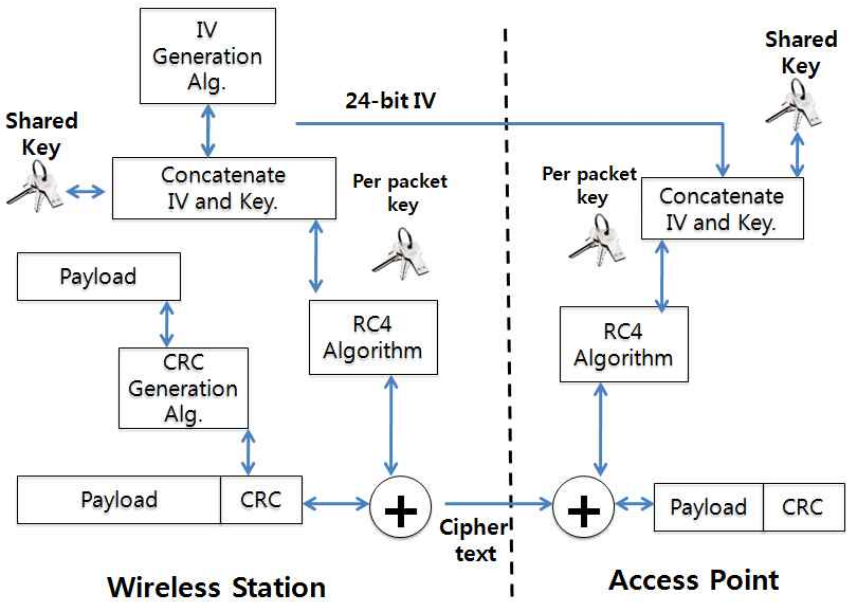
무선 네트워크 환경에서 클라이언트와 AP(Access Point) 간 통신 시, 무선 네트워크 고유 ID인 SSID(Service Set IDentifier)를 공유하여 인증하는 방식이다. 이러한 환경에서 SSID를 알 경우 인증되지 않은 클라이언트가 접속할 수 있는 문제가 있어 SSID를 숨겨주는 기능인 Secure Access를 이용하는데 이를 SSID 숨김이라고 한다. SSID 숨김의 경우 SSID의 이름을 알지 못할 경우 연결할 수 없으므로 보다 안전하다. 그러나 AP와 클라이언트간 통신이 일어나고 있는 동안은 스니핑(Sniffing)을 할 경우 SSID가 노출되는 취약성이 있어 강력한 인증이라고 할 수 없다.

나. 무선 디바이스와 AP(Access Point)간 WEP키 이용

WEP(Wired Equivalent Privacy)는 무선 인터넷 표준을 규정하고 있는

IEEE 802.11 규약에서 명시하고 있는 무선 LAN 인증 방식으로, 무선 디바이스와 AP간 인증 시, 패스워드 방식에 기반을 두고 있는 인증방식이다. WEP 방식은 RC4 Stream Cipher를 이용한 암호프로토콜 방식이지만, WEP 키(Key)라는 비밀 정보를 공유한다는 측면에서 ID/PW 인증기술이라고 보는 견해도 있다.

WEP 키 인증 방식은 AP가 디바이스에게 Challenge 패킷을 보내고, 디바이스가 올바른 WEP 키를 보유하고 있으면 이를 통해 패스워드를 암호화하여 다시 AP로 Response를 하는 Challenge-Response 방식을 통하여 인증한다. 디바이스가 잘못된 WEP 키를 가지고 있거나 WEP 키를 가지고 있지 않다면, 적절한 Response를 생성하지 못하여 인증에 실패하게 된다.

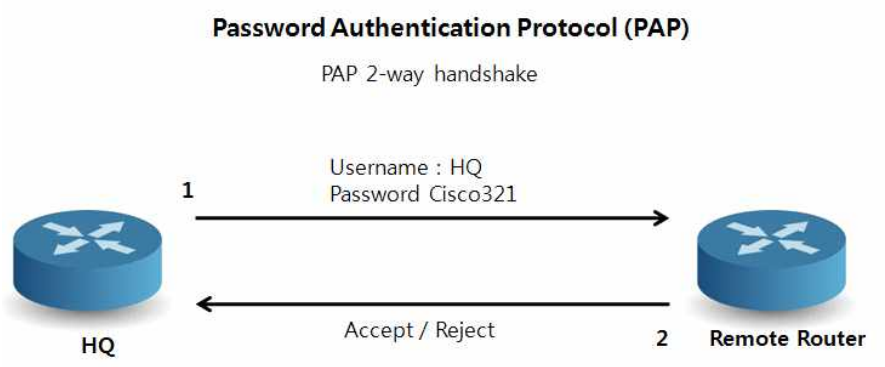


< 그림 35. WEP 인증 서식도 >

다. PAP 인증 방식

PAP(Password Authentication Protocol) 인증 방식은 단대 단 통신 규약

(Point-to-Point Protocol)로, Unix 시스템에서 서버와 클라이언트간 인증 시 사용되는 프로토콜이다. PAP 프로토콜은 클라이언트에게 기존에 설정된 패스워드를 이용하여 자동으로 인증을 제공하는 기술이다. 클라이언트는 자신의 ID와 PW를 서버에 보내고, 서버와 보유하고 있는 ID/PW 정보와 비교를 통하여 인증하는 방식의 프로토콜이다.



< 그림 36. PAP 인증 서식도 >

PAP 프로토콜은 서버-클라이언트뿐만 아니라, 서버와 서버간의 인증에도 사용되고 있다. 서버-서버 간 인증 역시 서버-클라이언트 방식과 마찬가지로 Challenge-Response 방식으로 인증을 하며, 호스트네임과 PW 정보의 일치 여부를 통해 인증하는 방식이다. 홈 네트워크 환경에서 역시 PAP를 통하여 홈 게이트웨이 간 상호 인증 시, 호스트네임과 PW를 통하여 상호 인증이 가능하다.

라. RFID 태그와 RFID 리더 간 인증 (EPC Global)

RFID(Radio Frequency IDentification)는 RFID 태그와 리더, 그리고 인증 서버로 구성되어 있다. RFID 태그는 메모리 용량과 연산량, 그리고 전력 등의 한계로 인하여 상대적으로 계산량이 적은 인증 프로토콜을 사용해야 한다. 이로 인하여 RFID 환경에서 태그와 리더 간 인증 시에는 태그 고유의 키를 이용하여 인증한다. 이러한 RFID 인증 프로토콜에는 Hash lock, Randomized Hash lock, Hash-chain 기법 등이 있다. Hash lock 인증방식은 태그의 유일한 비밀키를 해쉬화한 metaID를 통해 이루어진다. 리더는 태그의 metaID에

해당하는 비밀키 값을 서버로부터 전달 받는다. Randomized Hash lock 인증 방식은 태그에서 아이디 이외에 랜덤한 값을 선택하여 리더에게 보내어 인증하는 방식이다. Hash-chain 인증방식에서는 태그에 저장된 비밀키를 Hash-chain을 이용하여 바꾸어 주는 방식을 이용하였다. 이러한 RFID 태그-리더 간 인증 방식은 태그에 저장된 아이디 또는 패스워드 이용하여 인증을 수행하기 때문에 이 정보가 노출되지 않도록 해야한다. 또한 태그 패스워드의 길이는 8비트이므로 공격자로 하여금 쉽게 패스워드를 추측 가능하다.

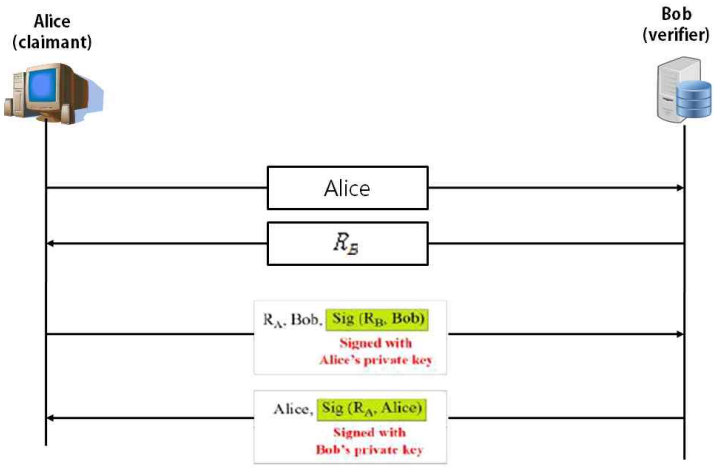
ID/PW 기반 인증기술은 서버-클라이언트 환경에서 클라이언트가 사전에 자신의 ID와 이에 해당하는 PW를 설정하고, 이에 대하여 서버가 인증을 하는 방식의 인증 프로토콜이다. ID/PW 기반 인증기술은 ID/PW만 설정이 되면 범용적으로 어느 환경과 어떤 기기에서든 사용이 가능하며, 각 기기들이 등록된 ID/PW 리스트만 관리하면 되기 때문에 관리가 쉬우며, 요구하는 자원이 크지 않다는 장점이 있다. 하지만 서버-클라이언트가 사전에 반드시 ID/PW를 공유해야 하며, 서버와 같이 여러 주체들을 인증해야 하는 경우 각 주체들의 모든 ID/PW를 저장해야 하는 단점이 있다. 이와 같은 단점으로 인하여, 대규모 환경에서 적용할 경우 관리와 저장의 문제가 있으며, 다량의 인증을 동시에 처리해야 할 경우 부하가 걸리는 문제가 예상된다.

사물통신 환경은 대규모의 기기들이 사람의 개입이 없거나 최소화된 상태에서 상호 통신하는 환경이다. 이러한 환경에서 ID/PW 방식은 서버의 관리 및 부하가 예상되며, 새로운 기기를 추가하거나 수정을 하는 데 있어 사람의 개입이 전제 되어야 하는 문제점이 있다. 또한 ID/PW 인증 방식은 부인방지 기능을 제공하지 못하여 과금 서비스 혹은 강력한 보안이 필요로 하는 분야에 적용할 경우 통신 사실 등을 부인할 수 있어 인증기술로는 큰 단점이 존재한다.

3.3.2 인증서 기반 인증

인증서 기반 인증기술은 공개키 기반의 암호기술을 이용하는 전자서명(Digital Signature)을 통하여 인증하는 방식의 인증기술로, 인증서에 전자서명을 위한 정보를 수록하여 이를 기반으로 인증하는 기술을 의미한다. 공개키 기반의 암호기술은 한 주체가 본인만이 알 수 있는 비밀키(Private Key)를 생성하고, 이에 대응하는 공개키(Public Key)를 생성하여 이를 공개하는 과정을 통하여 암호화 통신을 한다. 즉, 한 주체(B)가 다른 주체(A)에게 그 주체만이 알 수 있도록 암호화하여 메시지를 보내야 할 경우 이 주체(A)가 공개한 공개키를 통하여 암호화하여 전송한다. 이 주체(B)로부터 암호화된 메시지를 전달받은 주체(A)는 자신이 보유한 비밀키를 통하여 원 메시지를 복호화 할 수 있다.

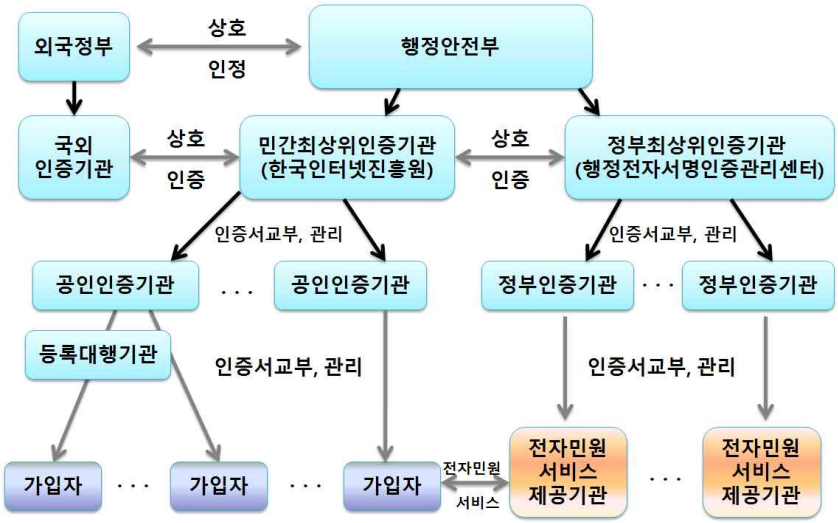
전자서명을 통한 인증 방식은 이 공개키 암호시스템을 이용하여 인증하는 방식이다. 즉 인증 받고자 하는 주체인 청구인(Claimant) 검증자(Verifier)에게 인증을 위한 메시지를 요청한다. 검증자는 검증메시지(Challenge Message)를 청구인에게 전송한다. 이를 수신한 청구인은 이를 자신만의 비밀키로 암호화하는 전자서명 과정을 통하여 검증 메시지를 암호화하여 다시 검증자에게 전송한다. 이 암호화된 메시지를 수신한 검증자는 사전에 청구인이 공개한 공개키로 이 메시지를 복호화하여 자신이 최초에 전송한 검증메시지와 일치하는 지 여부를 확인한다. 이 메시지가 서로 일치할 경우 검증자는 이 청구인이 적합한 청구인임을 검증할 수 있다. 이 방식이 '전자 서명'이라고 불리는 이유는 일반적인 서명과 동일한 검증을 할 수 있기 때문이다. 즉 청구인은 청구인 자신만이 유일하게 할 수 있는 서명을 하고, 이 서명은 누구나 검증할 수 있으므로 일반적인 서명과 동일한 검증 기능을 제공한다.



< 그림 37. 전자서명을 통한 인증 방식 >

인증서에는 전자서명을 위한 일련번호, 주체, 서명 알고리즘, 발행자, 유효기간, 공인키, 지문, 지문 생성 알고리즘 등의 정보가 포함되어 전자서명 시 인증서를 통하여 전자서명이 이루어진다.

우리나라는 1999년 전자서명법을 제정하였으며, 민간에서 사용하는 공인인증서 발급 체계 및 관리와 관련된 규정을 마련하였다. 이 체계는 최상위 인증기관인 Root CA(Certificate Authority) 하에 공인인증기관을 두고 이 기관들을 통하여 공인인증서를 발급하는 체계이다. 전자서명법 제25조에 근거하여 한국인터넷진흥원 (Korea Internet & Security Agency, KISA)을 최상위 인증기관으로 지정하고, 한국정보인증(주), (주)코스콤, 금융결제원, 한국전자인증(주), 한국무역정보통신, 한국정보사회진흥원을 전자서명법 제4조의 규정에 근거한 공인인증기관으로 지정하였다. 한국정보사회진흥원은 2008년 6월 한국정보인증(주)로 이관되어 현재 5개의공인인증기관을 통하여 인증서의 발급 및 인증이 이루어지고 있다.



< 그림 38. 국내 전자서명 체계 >

전자정부 환경에서 행정관련 전자문서 송·수신 등에 있어 기관 및 공무원 신원확인, 그리고 문서의 위·변조 등을 방지하기 위하여 행정전자서명(Government Public Key Infrastructure, GPKI)이 운영되고 있다. 전자정부법 제29조 및 전자정부법 시행령 제11조에서 제17조에 의거하여 발급 및 운영이 되고 있다. 행정안전부 산하 행정전자서명 인증관리센터가 최상위 인증기관으로 이 센터를 통하여 인증기관인 교육과학기술부, 국방부, 대검찰청, 병무청, 대법원(법원 행정처)을 통하여 행정전자서명이 발급되고 있다.

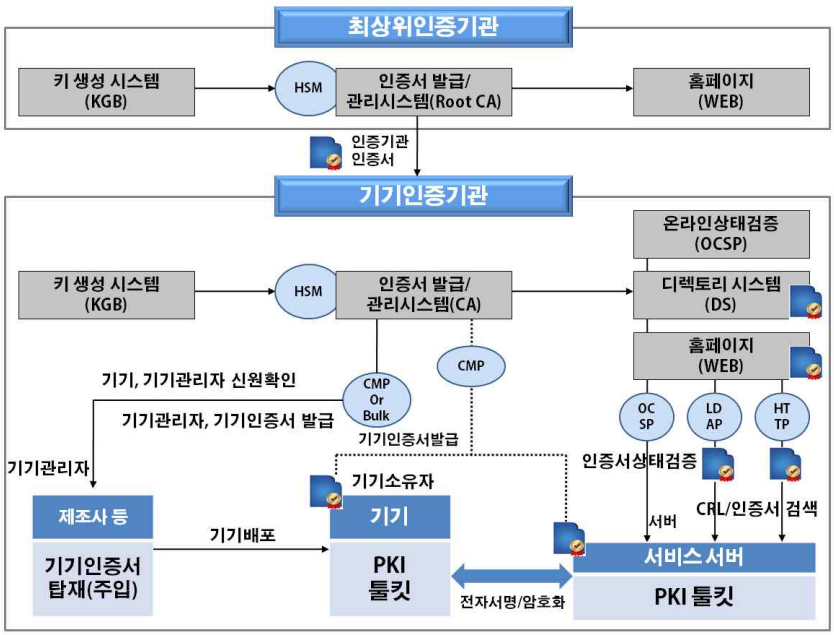
사물통신 환경에서의 인증서 기반 인증기술은 현재 국내에서 운영되고 있는 개인용 NPKI(National Public Key Infrastructure), 행정전자서명 GPKI(Government Public Key Infrastructure)와 같이 PKI(Public Key Infrastructure) 기반의 기기인증서를 통하여 인증하는 기술이다. 인증서의 대상이 개인 혹은 법인이 아닌 사물이라는 차이가 있으며, 인증서 발급 구조, 유효기간 등 에서 다음 표와 같은 차이가 존재한다.

구분	공인인증서	기기인증서
서비스 대상	자연인, 법인	네트워크에 접속되는 모든 기기
서비스 내용	인터넷뱅킹 등 전자거래 시 본인확인	특정 서비스(인터넷 전화망, 케이블 TV망 등)에 접근권한 확인
인증서 사용목적	본인확인, 전자문서 무결성 등	기기식별, 암/복호화 등
이해 당사자	공인인증기관, 전자거래 서비스 업체, 가입자	기기인증기관, 네트워크 서비스 운영자, 기기 제조업체, 기기
신원확인 절차	직접대면을 통한 확인	기기 제조업체 등을 통한 기기 진위성 확인
인증서 구성	성명 등 개인정보 포함	제조업체명, 기기 식별정보(시리얼 번호, MAC Address) 등
인증서 발급	개별적으로 개인에게 발급	수천~수만 장 단위로 벌크(Bulk)로 선발급
인증서 저장	PC. USB 등에 저장	기기 제조과정 중 해당 기기에 탑재
인증서 관리	갱신, 재발급 빈번히 발생	갱신 재발급 없이 기기의 사용연한과 동일(유효기간 ↑)

< 표 6. 공인인증서와 기기인증서 비교 >

현재 한국인터넷진흥원은 '기기인증관리체계를 위한 최상위인증기관 인증업무 준칙'을 제정하고 기기에 대한 인증서 정책, 인증서 발급·관리 등 기기인증관리체계 운영 등에 있어 필요한 사항을 규정하고 있다.40) 동 준칙에서 한국인터넷진흥원은 기기인증서를 기기의 진위여부를 식별하고 기기에서 송수신되는 정보를 안전하게 전달하기 위해 공인인증기관이 발급하는 전자적 정보로 규정하고 있다. 또한 기기인증서 발급 및 운영업무를 하는 각 공인인증기관의 인증(공인인증기관 공인인증서) 업무에 대하여 규정하고 있다. 한국인터넷진흥원

은 기기인증서의 발급체계를 다음 도식도와 같이 예상하고 있다.



< 그림 39. 기기인증서시 발급체계 예상 도식도 >

인증서 기반 인증기술은 강력한 인증 기능을 제공하여 높은 안전성을 제공한다. 또한 인증서 기반 인증 기술에서 사용되는 전자서명은 본인만이 서명이 가능하기 때문에 부인방지 기능을 제공한다. 이는 과금 및 책임소재 등에 있어 중요한 기능을 제공한다.

반면, 인증서 기반 인증기술은 반드시 사전에 키 교환이 필요하다는 단점이 있다. 또한 구현에 있어 인증서의 발급·갱신·폐기 등 인증서의 관리가 필요하다. 기기인증서의 경우 인증서 유효기간을 30년으로 늘려 이러한 불편을 최소화하고자 하는 노력이 있지만, 기본적으로 제품의 생산 시 기기인증서를 탑재하여야 하며, 폐기리스트(Certification Revocation List, CRL)를 관리해야 하는 등 여전히 관리상의 불편함이 있다. 또한 인증서의 경우 각 인증기관과의 인증 업무가 호환되지 않을 경우, 다른 국가 등 다른 도메인에서 사용 시 호환

성의 문제가 있다. 인증서 기반 인증기술에서 사용되는 서명 알고리즘 등 기기 인증서 처리 S/W 및 알고리즘은 연산 처리량이 많고 무거워 기기에 적용하기 어려운 문제점은 기기인증서의 가장 큰 단점이다.

사물통신 환경에서 인증서 기반 인증기술은 강력한 인증 및 부인방지를 제공함에 따라 높은 보안수준을 요구하는 분야에서 역시 사용이 가능하다. 또한 부인방지 기능이 요구되는 과금이 필요한 환경에서 역시 사용이 가능하다는 장점이 있다. 하지만 인증서 기반 인증기술은 높은 연산량을 요하는 단점이 있다. 사물통신 환경은 기기들의 특성상 저전력 적은 저장공간 등의 환경에서 적합한 인증기술이 필요하다. 따라서 사물통신 환경에서 인증서 기반 인증기술을 적용할 경우 사물통신 환경에 적합한 기기 인증서의 개발이 선행되어야 할 것이다. 또한 인증서 기반 인증기술은 ID/PW, MAC Address, 암호 프로토콜 기반 인증기술 들과 달리 특정 처리 소프트웨어, 발급 및 인증 체계 등이 필요하다. 사물통신 환경에서 인증서 기반 인증기술은 기기의 고장, 변경, 수리 등에 따라 잦은 변화와, 기기에서 인증서를 추출하여 위장(Masquerade)하는 공격 등을 방지하기 위한 인증서의관리가 필요하다.

사물통신은 인간의 개입이 최소화된 상태에서 인증이 이루어져야하기 때문에, 서로 다른 환경·서로 다른 인증기술·서로 다른 도메인 간 호환이 어려운 문제 역시 해결해야할 것이다. 이와 같은 발급체계, 인증체계 들로 인하여 인증서 기반 인증기술은 다른 인증기술에 비하여 많은 비용이 요구됨에 따라, 인증서 기반 인증기술은 일반적인 사물통신 환경보다는 높은 보안성을 요구하는 환경에서 사용할 것으로 예상할 수 있다.

4장 국내 사물인터넷의 보안 현황

4.1 국내 사물인터넷에서의 보안 현황

4.1.1 모바일 보안 KNOX

KNOX는 국내 기업 삼성의 모바일 보안 솔루션으로 차세대 보안 안드로이드 플랫폼으로 하드웨어 보안 기능을 활용하여 부담 없는 가격으로 운영 체제 및 애플리케이션을 여러 단계를 거쳐 보호할 수 있도록 되어 있다.

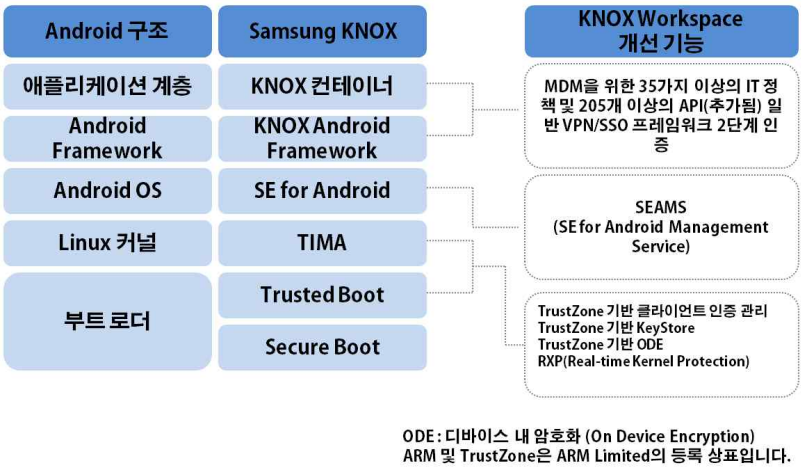
KNOX는 하드웨어 보안기능을 활용하여 강력한 보안과 사용 편의성을 제공한다. 또한, 차세대 보안 안드로이드 플랫폼으로 하드웨어 보안 기능을 활용하여 부담 없는 가격으로 운영 체제 및 애플리케이션을 여러 단계를 거쳐 보호할 수 있도록 하였다.

철저한 보안 플랫폼은 빈틈없는 보안 플랫폼으로 디바이스의 무결성을 향상하고 인증 및 허가된 기기만 오픈하여 민감한 자산을 보호한다. 그리고 커널코드가 악의적으로 변조되지 않도록 실시간 시스템 보호와 사용자 악성코드에 의한 데이터를 유출 방지 하도록 설계되었다.

뛰어난 모바일의 생산성으로 유연한 컨테이너 옵션지원과 기업 또는 공공 보안 유지 및 최적화된 사용자 환경을 제공한다. 또한 KNOX EMM의 웹 및 모바일 애플리케이션을 위한 보안 SSO를 지원한다.

포괄적 관리성으로 클라우드 기반 포괄적 제어가 가능하고 등록 절차가 간단한 SEG 및 UMC를 통한 간편해진 배포 및 사용자 관리 등 배포된 앱의 다양한 제어 및 관리가 가능하다.

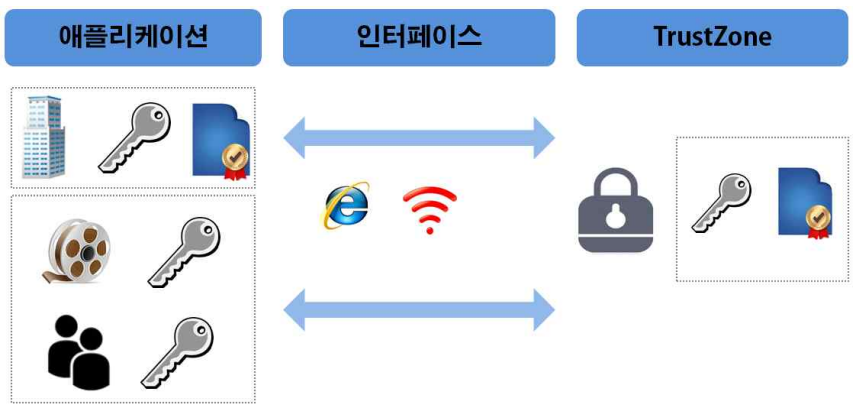
< 그림 38>을 보면 빈틈없는 보안 플랫폼 구조를 보여주고 있다. KNOX workspace의 개선된 플랫폼은 디바이스의 무결성을 향상시키도 있다.



< 그림 40. KNOX의 보안 플랫폼 >

또 KNOX는 인증 및 허가된 기기만 오픈하는데 이는 최고 수준의 보안을 요구하는 곳에 철저한 보안을 확보할 수 있다. Trusted Boot는 인증 및 하가된 OS만 부팅을 허용하는 보안이다. 따라서 정부/국방 등 최고 수준의 보안을 요구하는 공공분야에 사용될 수 있다.

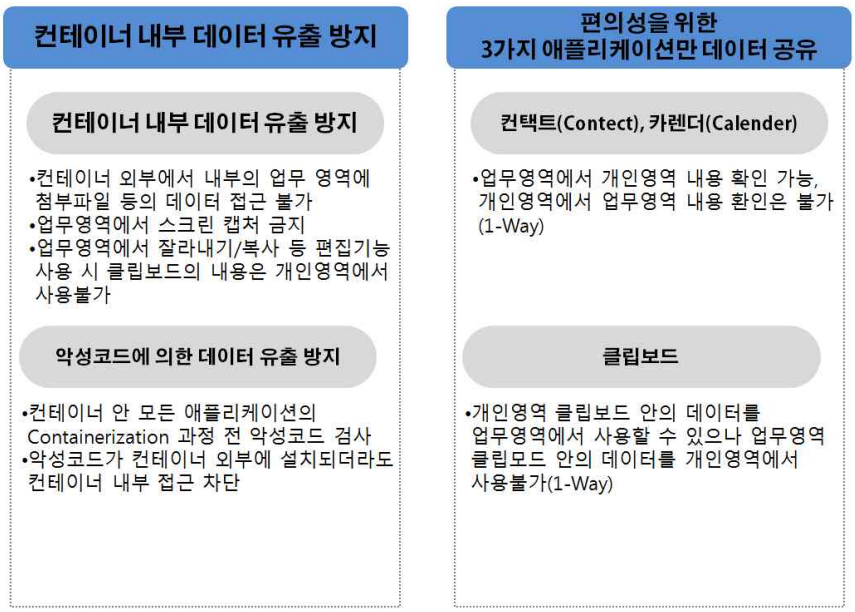
기업은 TrustZone 기반의 보안 기능을 통해 디바이스의 민감한 자산을 보호할 수 있다. 그리고 TrustZone은 AP(CPU) 안에 존재하는 H/W 기반의 보안 영역으로, Trustzone 안에 작동하는 S/W는 외부의 보안 위협으로부터 차단된다.



< 그림 41. KNOX 허가된 기기만 오픈 >

KNOX는 실시간으로 시스템을 보호한다. RKP(Real Time Kernel Protection)가 커널 코드, 핵심 커널 데이터, 시스템 파티션에 대한 변조를 관찰함으로써 커널에 대한 무단 변경을 감지 및 예방하여 실시간 시스템을 보호한다. 또 TIMA RKP는 디바이스 백 그라운드에서 실행되다가 TIMA가 감지하면 디바이스 사용자에게 알림 메시지를 보낸다.

그리고 데이터 유출 방지 및 공유를 한다. 사용자 악성코드에 의한 컨테이너 내부 데이터 유출을 방지하며, 편의성을 위한 3가지 애플리케이션에서만 데이터가 공유되도록 하여 안전하게 데이터를 관리할 수 있다.

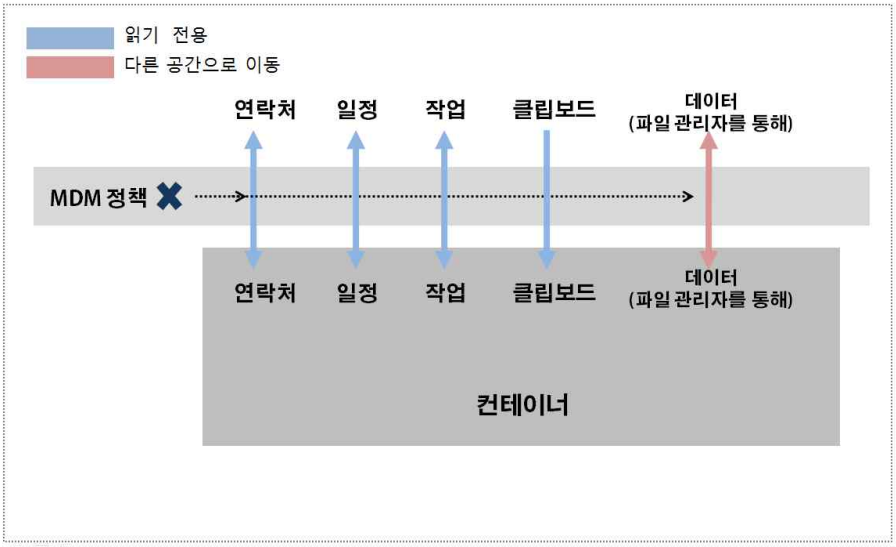


< 그림 42. KNOX 데이터 유출 방지 및 공유 >

KNOX는 유연한 컨테이너 옵션을 지원한다. 이중 컨테이너를 통해 멀티태스

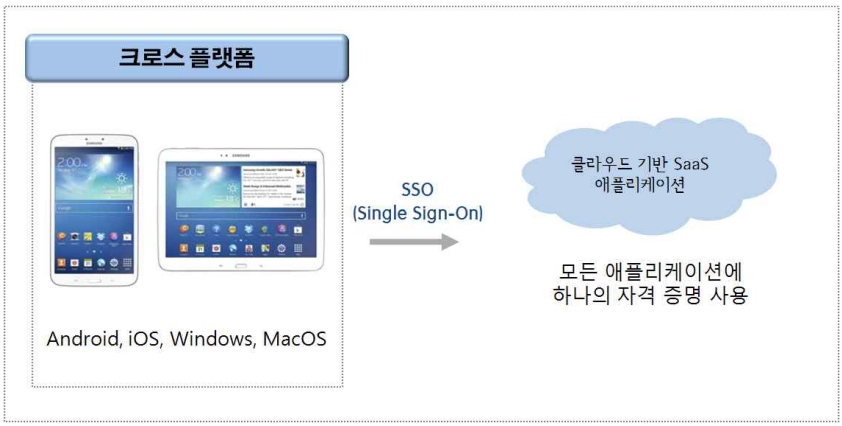
킹을 효율적으로 수행할 수 있다. 여러 그룹에 걸쳐 다양한 업무를 수행하는 멀티태스킹 작업자와 서로 다른 고객 그룹에 유사한 서비스를 제공하는 전문가(의사 및 변호사)에게 유용하다. 그리고 로우엔드부터 하이엔드 디바이스에 이르기까지 다양한 디바이스의 요구 사항을 충족한다.

최적화된 사용자 환경을 제공한다. 기업 또는 공공에서 보안을 유지하면서 뛰어난 상용자 생산성을 지원할 수 있다. 사용자의 기본 설정에 기반한 애플리케이션 및 데이터 공유 관리 기능을 제공한다. 또 기업의 IT 관리자가 규정한 제한 사항을 적용하여 관리할 수 있다.



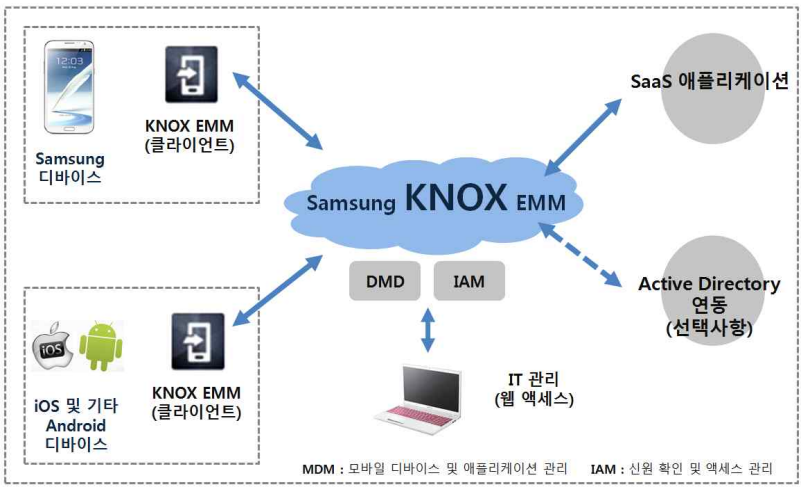
< 그림 43. KNOX 컨테이너 >

기업용 애플리케이션이 확대되고 있다. KNOX EMM은 웹 및 모바일 애플리케이션을 위한 보안 SSO(Single Sign-On)을 지원한다. 한 번의 클릭으로 2,000개가 넘는 승인된 애플리케이션 및 모바일 SaaS 애플리케이션에 액세스 가능하다. 또 매월 추가 요금으로 사용할 수 있는 무제한 애플리케이션에 대한 프리미엄 SSO 기능 및 서비스를 제공한다.



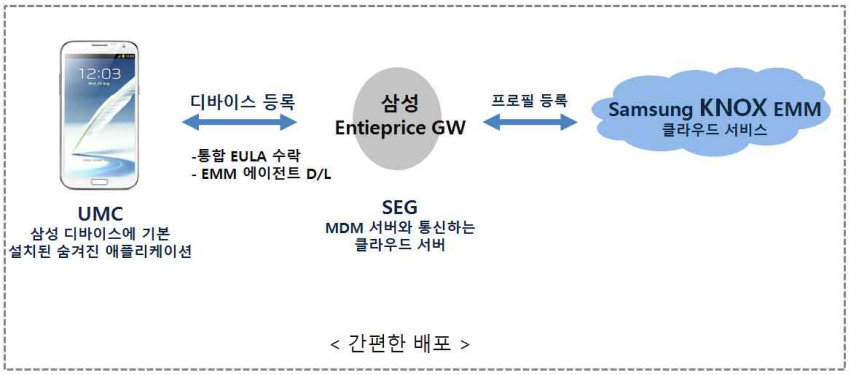
< 그림 44. 기업용 애플리케이션 확대 >

클라우드 모바일 관리가 가능하다. KNOX EMM(Enterprise Mobility Management)로 IT 관리자가 모바일 뿐만 아니라 사용자 신원 정보와 애플리케이션까지 관리할 수 있도록 해주는 클라우드 기반 솔루션을 제공한다. 또 KNOX 클라우드 기반 MDM 및 IAM(SSO+디렉토리 서비스)을 제공하며 크로스 플랫폼도 지원한다.



< 그림 45. KNOX 클라우드 모바일 관리 >

간편한 배포 및 관리가 가능하다. SEG 및 UMC는 한 번만 등록하면 되기 때문에 등록 절차가 간단하다. 그리고 기업 또는 기관에서는 컨테이너 범위를 제한해 직원의 개인정보를 보호한다.



< 그림 46. KNOX 간편한 배포 및 관리 >

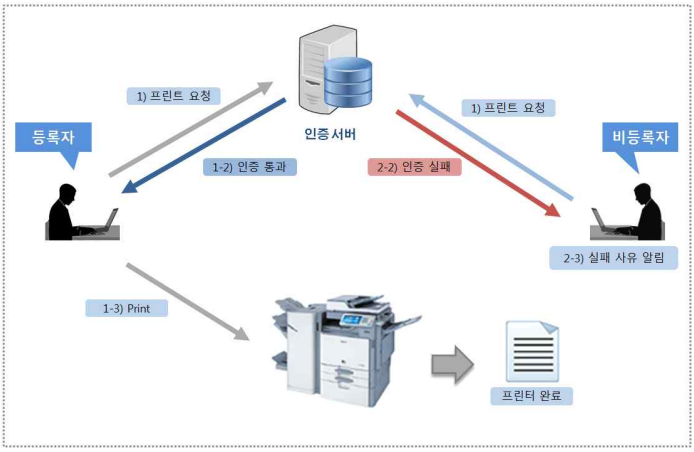
4.1.2 프린팅 인증, 출력 보안 SecuThru

SecuThre 솔루션은 정보유출에 취약한 종이매체를 위한 통합 출력보안 솔루션이다. 업무 필수 요소인 종이 출력물 정보를 지키는 출력 보안 솔루션은 다양한 기업환경에 맞는 확정성과 비용절감을 제공한다. PC에서 전송, 출력하는 종이문서는 물론, 복합기의 복사, 스캔, 팩스, 프린터 문서까지 강력한 보안 설정으로 정보를 지킬 수 있는 출력 보안 솔루션이다.

SecuThru는 출력문서 실명제 정책수립, 인증을 통한 외부인 출력 제한, 전사적 출력물 이력 통합관리, 출력물의 회사 자산화(watemark), 출력물 로그 원본(Image, Text) 저장, 사내 보안의식 고취 등으로 보안을 강화하였다. 그리고 각 부서별/개인별 출력물 통계 기능, 출력 비용계산 기능을 통한 관리, 업무 이외의 출력물 감소 효과, 불필요한 출력물 관리 기능, 기술적 제어를 통한 출력 제한 기능 탑재로 비용을 많이 절감 하였다. 다양한 프린터 및 드라이버를 지원하고 Role 기반의 워터마크/복합기 정책 및 모니터링 툴 지원으로 편리한 관리가 이루어진다.

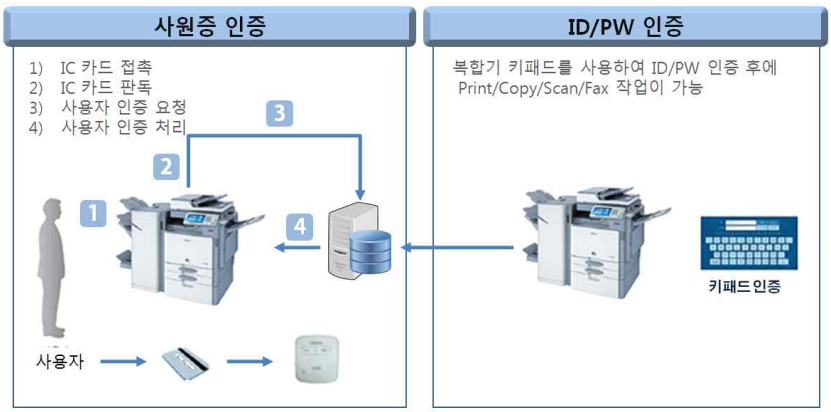
또한, 철저한 인증절차를 통해 문서, 이미지 등을 출력할 수 있으며 출력물 이력관리, 보안 키워드 관리 등을 통해 보다 철저한 보안 업무를 수행한다.

주요기능으로 첫 째는 인증관리기능이다. 사용자 PC에 Agent를 설치하여 등록되어 있는 사용자만 프린트가 가능하며 등록되지 않은 사용자에게는 프린트를 제한한다. 또한, 사용자 정보에 따라 작업이 허가되거나 거절될 수 있도록 제한한다.



< 그림 47. SecuThru 복합기 인증 관리 >

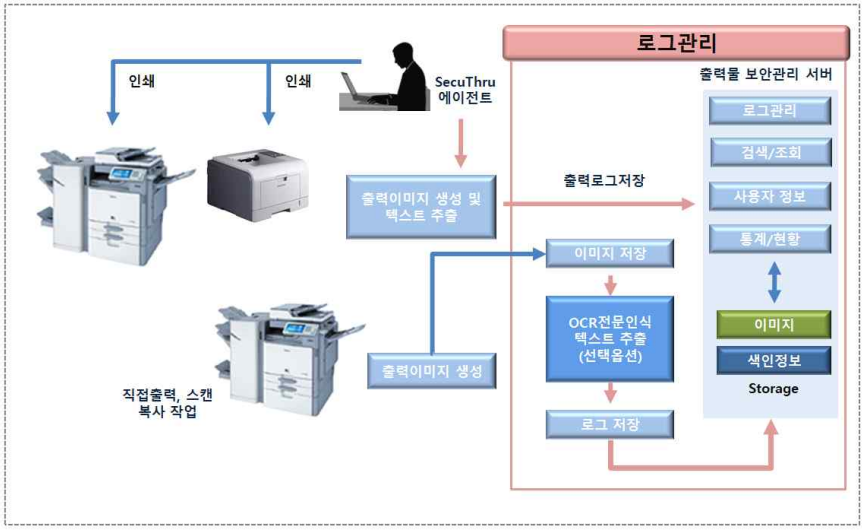
복합기로 프린트/복사/스캔 사용 시 사원증 인증 후 문서 출력 및 복합기를 사용할 수 있으며 사원증이 없는 경우 복합기의 키패드를 사용하여 ID/PW를 입력 인증 후 복합기를 사용할 수 있다.



< 그림 48. SecuThru 복합기 사원증 인증 >

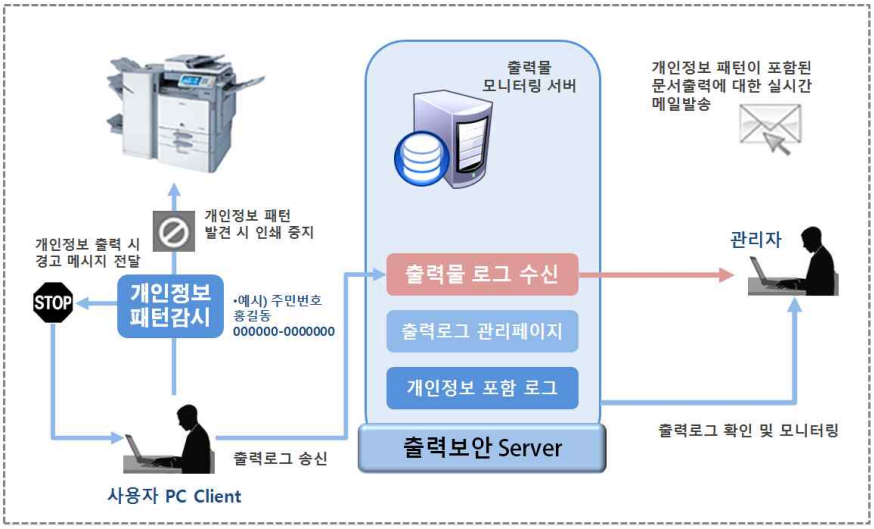
출력물 실명제를 사용하는데 출력IP, 사용자명, 시간 등 출력정보가 출력 시마다 삽입되는 출력 실명제가 구현되어 사용자에게 보안에 대한 경각심을 심어주고 보다 적극적인 문서보안 환경을 구축하게 된다.

출력물 모니터링은 PC에서 출력 시 출력물의 이미지와 추출이 가능한 텍스트, 출력 정보를 서버로 송신하여 출력물 DB에 저장한다. 이를 통해 관리자가 모니터링이 가능하도록 별도 관리한다.



< 그림 49. SecuThru 출력물 모니터링 >

개인정보 패턴분석은 출력 시 수집된 출력로그 내에 개인정보(주민번호, 카드번호)가 존재하는지 패턴을 분석하여 사용자에게 경고 메시지 팝업 전달, 인쇄 강제종료, 관리자에게 메일 발송 및 별도 로그관리 기능을 지원한다.



< 그림 50. SecuThru 개인정보 패턴분석 >

5장 결론

사물인터넷에서의 가장 중요한 네트워킹은 센서 네트워킹 이라는 것이다. ZigBee기술, RFID기술, CoAP기술, WiFi기술 등 모두 무선 센싱 네트워크 기술이다. 사물인터넷에 이러한 무선 네트워크 기술이 쓰이는 이유는 우리 사람의 편리함을 위해서 시공간의 제약이 없어야 한다는 점이다. 모든 통신이 물리적인 케이블로 연결을 한다면 안 하는게 나을 것이다.

그 결과로 지금 가장 많이 사물인터넷의 무선 통신 네트워킹기술이 쓰이고 있는 사례를 보면 물류배달과 차량 실시간 관리, 출입통제, 전자결제, 도서관리, 위조지폐방지 등이 있다. 그렇기 때문에 앞으로 사물인터넷 기술은 무선 네트워크 통신이 주를 이을 것으로 보이고 그에 따른 기술들의 보안이 필요할 것으로 보인다.

70년대 초 개인컴퓨터의 시작으로 21세기에 들어서 IT시대의 급격한 성장과 함께 IT제품, 기술의 여러 가지 혁신과 눈부신 발전이 있었지만 항상 안일하게 생각하고 아쉬운 결과를 낳았던 것은 보안문제점이다. 국내 IT기술도 인터넷 보급수준과 통신기술은 전 세계적으로 뛰어난 편이지만 보안수준은 국민적으로 많은 실망감을 안겨주었다. 보안수준을 고려해 봤을 때 또 다른 인터넷 탑재 디바이스의 세상을 맞이하고 있는 시점에서는 아주 위험한 세상을 맞이하고 있는 것이다. 우리의 일상생활의 편리함과 수준을 높여주는 사물인터넷 제품이 많이 출시되는 시대가 도래함은 해킹과 바이러스의 위협에 대상이 되는 위험요소제품이 지배하는 시대가 온다는 것과 같기 때문이다.

하지만 지금은 사물인터넷 시장이 시작 단계이고 많은 결과가 나와 있는 것은 아니기 때문에 보안기술과 사물인터넷 제품이 많이 나와 있는 상황은 아니다. 이제 막 시작 단계이고 성장가능성이 높기 때문에 국내외 여러 기업들이 관심을 가지고 연구, 개발에 착수하고 있다. 다시 한 번 말하면 앞으로 IT시대의 경쟁력은 사물인터넷의 발전 수준에 따라 나뉘어질 가능성이 크다고 볼 수 있다. 사물인터넷 그리고 보안수준이 그 나라의 경제력을 좌지우지하게 될 것이다.

국내에서 사물인터넷 시장에 뛰어든 기업은 상당히 많다. 삼성, LG, 달리웍스, 에스원, 퓨처시스템, 시큐아이 등이 있다. 하지만 출시한 제품은 많지 않고 IoT 제품에 접목한 보안기술 또한 정교하지 못한 상태이다. 앞으로 사물인터넷이 우리의 일상생활에 깊숙이 자리 잡는다면 제품의 기술과 그에 따른 보안기술이 세밀하고 정교하여 우리의 생활수준을 높여줄 것이라 기대하고 있다.

표/그림 목차

참고문헌

[1] <거의 모든 IT의 역사>, 정지훈 지음, 메디치.
[2] <모든 것이 연결되는 세상 사물인터넷>, 매일경제 IoT혁명 프로젝트팀 지음, 매일경제 신문사.
[3] 최성찬 외 3명(전자부품연구원), “사물인터넷 플랫폼 및 서비스 동향”
[4] 이재호 외 2명(한국정보화진흥원), “모든 것이 연결되는 초연결사회의 도래와 사물인터넷”
[5] 서화정 외 4명(부산대학교), “사물인터넷상에서의 보안과 프라이버시 보호”
[6] 강남희 (덕성여자대학교), “사물인터넷 보안을 위한 표준기술 동향”
[7] 김호원 (부산대학교), “사물인터넷 환경에서의 보안/프라이버시 이슈”
[8] 김동희 외 2명(한국인터넷진흥원), “IoT 서비스를 위한 보안”
[9] 김호원 (부산대학교), “사물인터넷 보안 및 프라이버시 이슈”
[10] 장봉임 외 1명, “사물인터넷 보안 기술 연구”
[11] 김봉환 외 2명, “ZigBee 보안 메커니즘 분석”
[12] 고석갑 외 3명, “사물인터넷 표준 CoAP 기술 및 구현 동향”
[13] 권력진 외 1명, “사물인터넷에서 장치 간 DTLS 적용 시 에너지 소비량 분석”
[14] 박재경(한국전파진흥원), “Wi-Fi 보안 침해 및 보안기술 현황”
[15] 한국정보보호학회, “사물통신에서의 정보보호를 위한 효율적 인증시스템 연구”
[16] 하정훈 (특허청), “사물인터넷 시대, 보안 없이 사물도 없다”
[17] 네이버 지식백과,
http://terms.naver.com/entry.nhn?docId=1691375&cid=42171&categoryId=42184
[18] 네이버 지식백과,
http://terms.naver.com/entry.nhn?docId=932676&cid=43667&categoryId=43667
[19] 네이버 지식백과,
http://terms.naver.com/entry.nhn?docId=2063772&cid=42107&categoryId=42107

[20] 네이버 지식백과,
http://terms.naver.com/entry.nhn?docId=75167&cid=43667&categoryId=43667
[21] 위키백과,
http://ko.wikipedia.org/wiki/%EA%B3%84%EC%82%B0%EA%B8%B0