u-Work 환경에서 ZigBee 네트워크의 효율적인 보안기법 설계

김철중*, 명대희*, 박석천*
*경원대학교 소프트웨어학부

Design of Efficient Security Technique of ZigBee Network in u-Work Environment

Kim, Chul-Joong, Myoung, Dae-Hee, Park, Seok-Cheon
Kyungwon University
E-mail : huntcjk@empal.com, daehee@ku.kyungwon.ac.kr, scpark@kyungwon.ac.kr

요 약

현재 전 세계적으로 IT기술이 급속도로 발전함에 따라 유비쿼터스 환경으로 급속히 변화하고 있다. 이러한 유비쿼터스 환경에서는 근로자가 언제, 어디서나 고도의 유무선 정보통신 기술을 활용하여 업무를 수행할 수 있는 u-Work 환경이 도래될 전망이다. u-Work를 보다 발전된 방향으로 구축하려면 센서 네트워크가 중요하며 그 중 ZigBee가 가장 유용하고 사회적으로 대두되어 개발이 많이 되고 있는 기술 중 하나이다. 따라서 본 논문에서는 보다 나은 사무환경 조성을 위해 u-Work와 ZigBee 기술을 조사하고 u-Work 환경에서 ZigBee 네트워크의 효율적인 보안기법 설계를 하였다.

1. 서론

현재 전 세계가 유비쿼터스 환경으로 변화하고 있으며 이로 인해 근로자가 언제, 어디서나 유무선 정보통신 기술을 활용하여 업무를 수행할 수 있는 u-Work 환경이 도래될 전망이다. 이러한 u-Work를 보다 발전된 방향으로 구축하려면 사무실 내외의 환경을 잘 조성해야 하고 이를 잘 제어 할 수 있는 센서 네트워크가 중요하지 않을 수 없다. 현재 ZigBee는 가장 유용하고 사회적으로 대두되어 개발이 많이 되고 있는 센서 네트워크 기술 중 하나이다. 이러한 기술이 적용이 되어 유비쿼터스 환경으로 변화할수록 중요하게 생각하고 대처해야하는 부분이 바로 보안이다. 현 상태에서 네트워크를 구축하게 되면 이러한 보안문제가 큰 이슈 중 하나가 되며 앞으로 보안이라는 부분은 현 사회에서 없어서는 안 되는 부분이다[1].

따라서 본 논문에서는 u-Work 환경에서 ZigBee 네트워크의 효율적인 보안기법을 위해 2장에서는 u-Work와 ZigBee 기술, 그리고 ECC 알고리즘에 대해서 조사하였고 3장에서는 조사한 내용을 바탕으로 ZigBee 네트워크 보안 설계를 위해 시스템 구성과 보안 인증 알고리즘을 설계하였으며 마지막 4장에서 결론을 정리하였다.

2. 본론

2.1 u-Work 란?

정보사회로의 전환과 함께 '노동의 유연성 확보'를 목표로 1980년대부터 선진국을 중심으로 급속하게 확산되고 있는 u-Work란 '유비쿼터스 환경에서 근로자가 언제, 어디서나 고도의 유무선 정보통신 기술을 활용하여 근무시간의 일정부분을 전통적인 사무실 이외의 환경에서 효율적이고 안전하게 업무를 수행할 수 있는 환경을 제공하는 것'으로 국외에서는 Telework(일본), e-Work(유럽) 등으로 부르고 있다[2]. u-Work는 기존의 텔레워크,

재택근무, 유럽의 e-Work의 개념으로 존재하던 근무형태가 사회적 환경 변화, 근로에 대한 가치관 변화, 기업 비즈니스의 국제협력 강화 등으로 인하여 유비쿼터스 사회의 업무방식에 맞는 새로운 업무방식으로 등장하게 되었다[3].

2.2 ZigBee 기술

Zigbee는 센서 네트워크 영역에서 경쟁력 있는 단거리 무선 통신 기술로 전력 소모가 적은 것이 특징이다. ZigBee 송수신기를 센서와 결합하면 센서 네트워크를 구성할 수 있게 해준다. 이러한 센서네트워크에서는 대용량 정보 전달이 요구되지 않는 반면, 긴 배터리 시간과 일정 거리 이상의 전송 커버리지 확보가 필요하다[4]. 다음 <표 1>은 ZigBee와 타 기술과의 비교를 나타낸 것이다.

<표 1> ZigBee와 타 기술과의 비교

항목	ZigBee	Bluetooth	Wireless LAN
변조방식	DSSS	FHSS	DSSS/FHSS
통신거리	10M	10-100M	150M MAX
Device/ Network	65536개	7개	1개
전송속도	2.4GHz: 250kbps 915MHz: 40kbps 868MHz: 20kbps	2.4GHz : 1~3Mbps	
채널	2.4GHz: 11~26 915MHz: 1~10 868MHz: 0	2.4GHz : 79	

ZigBee 스펙은 국제민간단체인 ZigBee Alliance가 IEEE 802.15.4를 기반으로 표준 스펙을 제정한 것이다. ZigBee와 IEEE 802.15.4의 관계는 ZigBee가 IEEE 802.15.4를 모두 포함하고 있다. ZigBee는 계층구조를 이루는데, 하위계층이 IEEE 802.15.4이며 상위계층이 ZigBee로 구성이 된다.

ZigBee는 송수신의 활동이 필요한 경우에만 Sleep 모드에 있는 노드들을 활동 상태로 변경하는 방식을 채택함으로써 전력소모를 극소화하였다[5]. 네트워크 및 시스템과의 간섭에 Robust한 기능을 수행할 수 있도록 무선 LAN에서 사용하는 DSSS 방식을 제안하였고, 2.4GHz 대역에서 O-QPSK 변조 방식을 채택하였다. 채널 할당에는 CSMA/ CA 방식을 채택하였고 선택적으로 GTS 할당 방식을 적용하고 있다[6].

2.3 ECC 알고리즘

ECC 알고리즘은 공개키 암호시스템 즉, 유한체 위에서 정의된 타원곡선 군에서의 이산대수 문제에 기초한 암호 시스템이다. Diffie-Hellman 키 분배나 ElGamal 암호는 이산대수문제에 근거한 방식이며, 그러한 방식에 대응하는 암호 키 분배를 타원 이산대수 문제상에서 구성할 수 있다. 타원 이산대수 문제는 키의 크기를 비교적 작게(100~200 비트)할 수 있는 실용상의 이점이 있다[6].

ECC 알고리즘은 p개의 원소를 갖는 유한체 GF(p)에서 p>3인 경우 암호 알고리즘으로서 실효성을 가지며 다음과 같은 방정식을 만족한다.

$$E: y^2 = x^3 + ax + b \pmod p \quad \text{식 (1)}$$
$$\left(where,\ p > 3\ AND\ prime,\ a, b \in GF(p)\right)$$

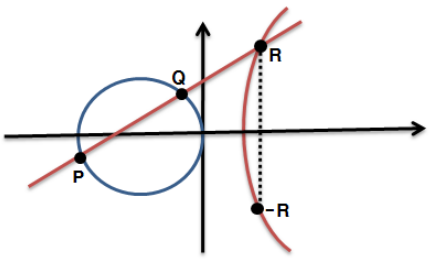
식 (1)은 타원 곡선 방정식을 만족하는 점들이고 무한대 점을 포함하는 집합은 식(2)를 만족해야 한다.

$$4a^3 + 27b^2 \neq 0 \pmod p \quad \text{식 (2)}$$

위의 식 (1), (2)을 만족하는 암호 알고리즘에서는 덧셈과 뺄셈을 통해 암·복호화를 한다. 이 때 타원곡선상의 점 P, Q에 대한 덧셈 연산 $R(x_3,y_3)$은 다음 식 (3), (4)와 같다.

$$\begin{cases} x_3 = \alpha^2 - x_1 - x_2 \\ y_3 = -y_1 + \alpha(x_1 - x_3) \end{cases} \quad \text{식 (3)}$$

$$\alpha = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & P = Q \end{cases} \quad \text{식 (4)}$$



<그림 3> ECC 알고리즘

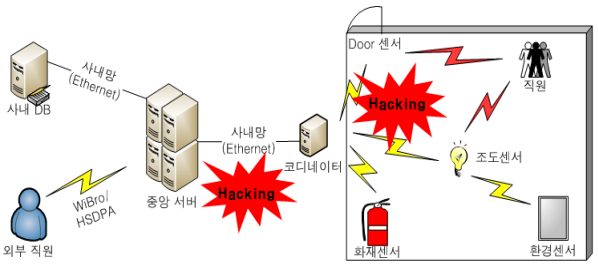
식 (3)은 타원곡선상의 점 $P=(x_1,y_1)$와 $Q=(x_2,y_2)$의 덧셈 연산의 결과인 <그림 3>의 $P+Q=R(x_3,y_3)$로 정의한다. 식 (4)에서 P와 Q가 다를 경우는 두 점이 다른 경우를 나타내며 P와 Q가 같은 경우는 본 논문에서 사용하는 두 점이 같은 경우를 나타

내는 것이다. 이 경우에는 타원 곡선상의 한 점 P의 덧셈 연산 P+P로서 2P=R(x_3,y_3)가 되는 것이다. 이로써 3P,....,NP를 구할 수 있다. 복호화는 P+(-P)=0 을 이용하여 P의 역원을 구하여 위의 식들과 같이 덧셈연산을 함으로써 구할 수 있다. 이러한 ECC 알고리즘의 특징은 타원곡선 군의 임의의 점을 잡고 스칼라 곱셈을 무수히 하여도 임의의 타원 군위의 점이 되는 것이다. 본 논문에서는 P+P=2P의 성질을 이용하여 미리 타원곡선 위의 점 G를 정의하고 이를 이용 암·복호화에 사용한다.

3. u-Work 환경에서 ZigBee 네트워크 보안 설계

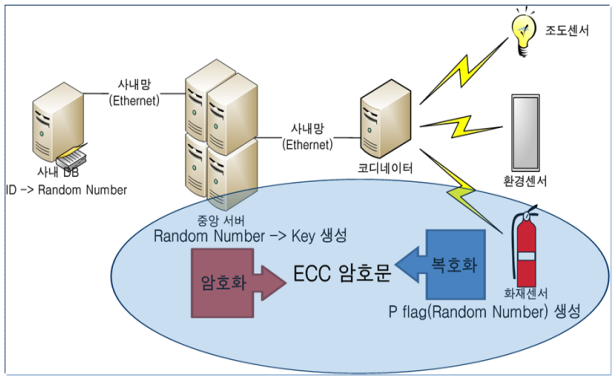
3.1 시스템 구성

본 논문은 u-Work 환경에서 ZigBee를 이용한 사무환경 시스템으로 주요 장치들은 크게 센서들에게 정보를 받고 관리하는 코디네이터, 센서 데이터를 받아 알맞은 처리를 하는 중앙서버, 데이터를 저장하고 상태를 저장하는 사내 DB로 구성된다. 중앙 서버에서는 센서정보를 바탕으로 그에 알맞은 제어명령을 제공하고 각 사무실의 상태를 UI로 보여준다. 이동 중에서 사무실 상황을 파악하고 제어 할 때는 휴대폰·PDA 등을 통해 먼저 인증을 받은 후 각 사무실 상태와 상황을 제공받고 제어 명령을 서버로 전송한다. 저장된 일련의 데이터들은 관리자에 의해 사내 관리 화면에서 명령을 내리게 되고 명령된 정보는 각 사무실의 ZigBee 모듈에 전달되어 실행된다. 예를 들어 데이터를 전송할 때 외부의 악의적인 침입자가 인가되지 않은 센서를 접속시켜 회사의 상태 제어에 혼란을 야기시킬 수 있다. 이러한 상황에서 사무환경의 보안에 관한 침입 시나리오를 살펴보면 <그림 4>와 같다.



<그림 4> ZigBee 사무환경 침입 시나리오

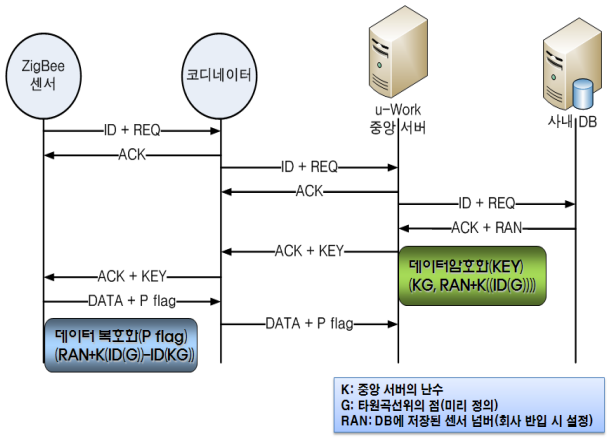
이에 따라 ZigBee 네트워크 보안 시스템 개요도를 살펴보면 다음 <그림 5>와 같다.



<그림 5> ZigBee 네트워크 보안 시스템 개요도

3.2 보안 인증 알고리즘

초기 ZigBee 센서에서 측정정보가 생성이 되면 ZigBee 코디네이터에 통보를 하고 각 센서들의 정보들을 모아서 u-Work 중앙 서버에 전송한다. 전송 받은 사무실의 센서정보는 중앙서버에서 사내망을 통해서 사내 DB에 저장된다. 이 때 위 <그림 4>와 같이 악의적인 목적 또는 허가되지 않은 센서가 거짓 정보를 보낼 수 있으므로 다음과 같이 보안 인증 절차를 거친다. <그림 6>은 보안 인증 Flow Diagram을 나타낸 것이다.



<그림 6> 보안 인증 Flow Diagram

보안 인증 알고리즘 절차는 다음과 같다. 여기서 G는 ECC 알고리즘의 타원곡선 위의 점으로서 센서와 서버 간에 미리 정의된 수식에 의해 설정한다. 먼저 ZigBee 센서의 기 저장된 ECC 알고리즘

을 통해 자신의 ID로 ID(G)를 생성하여 코디네이터와 중앙서버를 통해 DB에 전송한다. 전송 시 ACK는 10초 이내에 발생하고 10초 이내에 ACK를 받지 못하면 전송을 다시 실행한다. 하나의 프레임에 대해 3번까지 반복하고, 3번 반복하여서도 ACK를 받지 못하면 해당 프레임의 전송을 중단한다. 프레임 전송이 중단되면 관리자에게 해당 사실을 알리고 데이터 전송 프레임에 오류(Checksum Error)가 있다면, 데이터 전송을 받은 Device는 해당 프레임을 무시한다. DB에서는 수신한 ID와 해당 센서의 기 등록된 Random Number를 비교해 인증 절차를 거친다. Random Number와 ID가 일치하면 중앙서버에 전송한다. 중앙서버에서는 난수 K를 생성해 ECC 알고리즘으로 KG를 생성하고 센서로부터 받은 ID(G)값으로 K(ID(G))를 생성하여 ACK와 함께 KEY인 (KG, RanNum+K(ID(G)))를 전송한다. 센서에서도 역시 ECC 알고리즘으로 복호화하여 (P flag=RanNum+K(ID(G)) - ID(KG)) RanNum인 P flag를 찾아내고 보내려하는 DATA와 함께 중앙서버로 전송을 한다. 중앙서버에서는 RanNum과 P flag를 비교해 허가된 센서인지를 판별해 악의적인 센서를 차단한다. 이 때 중앙서버에서도 암호화 KEY를 전송 후 10초 이내에 DATA+P flag를 받지 못하면 3번까지 전송을 다시 실행한다. 프레임 전송이 중단되면 관리자에게 해당 사실을 알리고 데이터 전송 프레임에 오류가 있다면, 데이터 전송을 받은 서버는 해당 프레임을 무시한다. 이와 같은 방법으로 ZigBee 네트워크를 이용한 사무환경에서 센서를 인증하고 보안 시스템을 구축한다. 본 시스템에서 사용되는 프레임 포맷은 다음 <표 3>과 같다. 여기서는 기존 데이터 포맷에 P flag를 삽입 하였다.

<표 3> ZigBee 모듈 통신의 데이터 프레임 포맷

Name	Size (Byte)	Description
Command Code	1	프레임 설명 코드
Length	2	Data Length Field 확인
ID	8	Source MAC Address
Type	1	센서 유형
P flag (DB Random Number)	2	암·복호화 Data
Data	N	센싱 정보 Data
Check	1	Frame Error Check
EOF	1	End of Frame

4. 결론

유비쿼터스 사회가 도래함에 따라 u-Work가 국내·외적으로 활발히 개발되고 있다. u-Work는 다양한 정보화 기기들과 이들을 연결하는 네트워크 기술이 상존한다. 앞으로 u-Work 환경이 되면 정부에서는 에너지 절감 및 IT 산업 활성화는 물론이고 관련 소프트웨어, 하드웨어 등의 표준화를 앞당길 수 있게 될 것이다. 근로자 측에서도 출퇴근 시간을 줄일 수 있고 여유로운 근무환경으로 삶의 질을 향상시키는 일거양득의 성과가 기대된다. 이러한 u-Work의 중요한 인프라는 센서 네트워크이며 그 중 ZigBee가 가장 유용하고 개발이 많이 되고 있는 기술 중 하나이다. 이에 따라 ZigBee 네트워크를 이용한 사무환경에서 보안 측면의 중요성이 대두되고 있다. 따라서 본 논문에서는 u-Work와 Zigbee 기술을 조사·분석하고 기존 암호화 알고리즘보다 가벼운 ECC 알고리즘을 도입하여 u-Work 환경에서 Hacking 가능 지역에 보안 인증 알고리즘을 설계하였다. 이러한 시스템 구현은 아직 초기단계에 있으나 ZigBee의 사용영역이 더욱 다양화, 보편화 되고 사용자 요구가 많아질수록 제안한 보안 시스템 등의 활용도가 높아지고 개선될 수 있을 것으로 보인다. 또한 사무정보 측정 단말기, 코디네이터, 중앙 서버, 사내 DB, 외부 직원 간의 메시지 통신 보안 방법도 효율적인 방안으로 구체화될 것으로 기대된다.

[참고문헌]

[1] 충북대학교, “u-Work 환경 구현 모델 개발을 위한 선행 연구”, NIA, 2005.12.

[2] 남장현, “u-Work 동향분석”, KT BcN본부 기업서비스 개발부, 2005.12.

[3] (주) 폴리소프트, “u-Work 서비스 관련 최근 시범사업 및 기술개발 동향”, KETI, 2006.06.

[4] 심재창 외 1명 “ZigBee”, 국립안동대학교, 2006. 09.

[5] 전호인, “IEEE 802.15.4 WPAN 기술”, 경원대학교, 2005.05.

[6] 고훈, “타원곡선 알고리즘을 이용한 XML 문서 암호 구현”, 2006.07.