홈 네트워크 디바이스에서 ZigBee기반의 안전한 인증 메커니즘

최지훈, 김정재, 전문석
숭실대학교 일반대학원 컴퓨터학과
e-mail : czih@nate.com, argniss@nate.com, mjun@ssu.ac.kr

HAN(Home Area Network) in Zigbee Safety Authentication Mechanism for Zigbee Device

Ji-Hoon Choi, Jung-Jae Kim, Moon-Seog Jun
Dept of Computer Science, Soong-Sil University

요 약

Zigbee는 단말에 대한 경제성이 뛰어나고 저 전력통신을 이용하기 때문에 수명이 길다. Mesh, Tree, Star 등 다양한 방식의 토플리지 구조를 지원 하며 확장성이 뛰어나 군사적인 용도, 환경 모니터링 시스템 등 많은 분야에 사용되고 있다. 최근 스마트그리드환경을 구축함에 있어 Zigbee는 HAN(Home Area Network)에 표준으로 사용될 예정이며 현재는 Zigbee를 이용한 AMR(Automatic Meter Reading)을 시범 중에 있다. 일반적으로 ZIgbee Network은 ZC(Zigbee Coordinator), ZCH(Zigbee Cluster Head), ZE(Zigbee End Device) 3가지로 구성되며, Zigbee Network에서 발생할 수 있는 취약점은 허가되지 않은 디바이스의 접근, 라우터의 흐름을 조작하는 방법, ZC(Zigbee Coordinator)와 ZE(Zigbee End Device)사이의 키 전송 시 안전하지 않은 채널을 이용하여 전송되는 문제가 발생된다. 본 논문에서는, TCP(Third Party Center)를 이용함으로써, ZE와 ZC간의 키 생성 시 발생하는 취약점을 보완하였다. 또한 인증절차를 강화함으로써 ZE(Zigbee End Device)에서 발생 할 수 있는 취약점을 보완하고자 하였으며 RS(Register Server)를 이용하여 HAN에 존재하는 디바이스에 대하여 실시간 모니터링이 가능하게 하였다.

1. 서론

전력망과 정보통신의 융합기술인 스마트 그리드 정책이 가속화됨에 따라 스마트 그리드의 핵심 기술인 AMI(Advanced Metering Infrastructure)를 구축 하는데 관심이 집중되고 있다. AMI에 대한 관심이 고조됨에 따라 HAN의 환경에서 Zigbee의 활용도가 높아질 전망이다. ZigBee는 IEEE 802.15.4 기반으로 만들어진 WPAN(Wireless Personal Area Network)영역에 속하는 저 비용, 저 전력, 저속을 특징으로 하는 근거리 무선통신 표준으로 Tree, Mesh, Star방식의 여러 가지 네트워크 토플로지 구성이 가능하고 최대 약65000개의 디바이스를 수용할 수 있다. 이러한 많은 장점에도 불구하고 보안에 대한 문제점 또한 존재한다. ZigBee에서 발생되는 문제점으로는 ZED(Zigbee End Device)가 ZC(Zigbee Coordinator)와 키를 교환 시 안전하지 않은 채널을 이용하여 전송될 때 때문에 MITM(Man In The Middle Attack)같은 중간자 공격이 발생될 시 ZC까지 위협받을 수 있는 문제점, 키 교환과 인증을 동시에 하는 방식을 사용하므로 허가되지 않은 ZED가 Zigbee Network에 합류하는 문제점 (ACL(Aceess List Contorl)을 사용하여 인증을 하는 방식도 있으나 모든 방식에서는 지원하지 않고 있다). Router에 대한 트래픽을 조작하는 Router Jamming Attack, ZC가 키 생성 및 관리 삭제를 수행하는 TC(Trust Center)역할을 수행하기 때문에 오버헤드가 발생되는 문제점이 있다.[2]

본 논문에서는 이러한 문제점들을 개선하기 위하여 허가되지 않은 디바이스에 대하여 디바이스에 존재하는 유일한 부분을 이용하여 인증을 개선하고자 하였으며, HAN과 외부 망 사이에 TPS(Third Party Server)를 구성하여, ZC에서 하는 역할을 분산함으로써 ZC에서 발생되는 오버헤드를 줄이고 키 교환 시 문제점을 개선하고자 하는 방법을 제안한다. 또한 TPS앞 영역에 RS(Register Server)를 이용하여 특정 디바이스의 사용량에 대하여 모니터링 하는 방법도 제안한다.

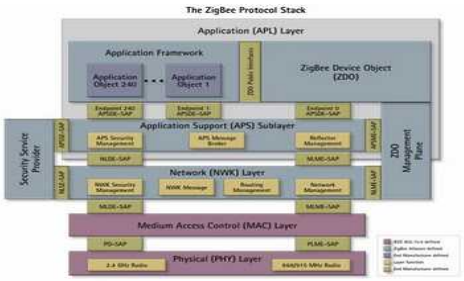
본 논문의 구성은 다음과 같다. 2장에서 관련연구로는

ZigBee의 스택구조와 보안적인 문제점에 대하여 설명하고, 3장에서는 제안하는 ZigBee에서의 인증 방식, 키 교환 방식, 모니터링 방식에 대하여 설명하며 4장에서는 결론을 맺는다.

2. 관련연구

2.1 ZigBee 스택구조

ZigBee 스택구조는 OSI의 7계층 표준모델을 기반으로 하며 각 계층은 상위계층에 서비스들을 제공 하는 SAP(Service Acess Point)을 통하여 인터페이스를 제공한다. ZigBee의 하위계층은 IEEE 802.15.4 표준에서 정의된 PHY와MAC계층과 ZigBee연합에서 네트워크(NWK)계층과 응용(APP)계층의 스펙을 정의하였으며, 응용계층 부분 중에는 ZDO(ZigBee Device Object)와 응용객체(Application Object)부분에 대한 정의도 하였다. ZigBee 스택 구조는 [그림 1]과 같다.



[그림 1] ZigBee 스택 구조

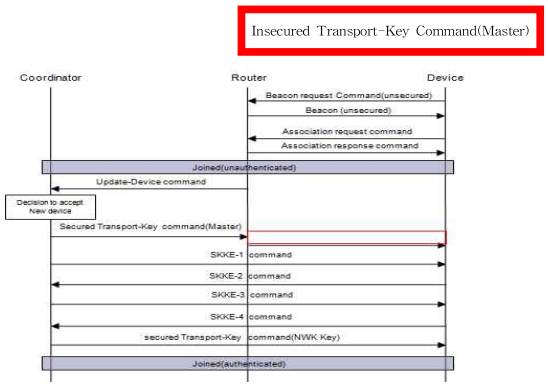
PHY(Physical Layer)계층은 무선으로 직접 데이터를 다루는 물리계층으로 2.4G에서 16개, 902~928MHz 사이에 10개 868~870MHz에 하나의 주파수대역을 사용하며, 최대 전송률은 각각 250Kbps, 40Kps와20Kbps 이다. CSMA(Carrier Sense Multiple Access) 방식을 사용하며 신뢰성을 지원하기 위하여 ACK를 사용하며 네트워크 결합과 분리에는 AES-128bit 암호화가 지원된다. MAC(Medium Access Contorl Layer) 계층은 CSMA/CA(Carrier Sense Multiple Access with Avoidance)를 사용하여 무선채널을 통제하며 비컨 프레임의 전송, 동기관리, 신뢰성 있는 전송 메커니즘을 제공하며, PAN에 대한 가입 및 가입해체에 대한지원 기기에 대한 보안을 지원한다. NWK(Network Layer)계층은 네트워크에 가입하거나 탈퇴하는 방식, 전송프레임에 대한 보안을 제공, 라우팅을 지원하고 라우팅 경로를 찾고 관리기능도 담당하며, 새로 접근하는 기기에 대하여 주소를 부여하는 기능을 수행한다. APL(Application Layer)응용계층은 APS(Application Support Sub layer)와 응용프레임워크, ZDO(Zigbee Device Object)로 구성 된다. APL은 기기들 간의 바인딩을 관리하고, 바인딩 테이블을 유지한다. ZDO는 네트워크 내에서 기기의 역할을 정의하고 기기사이에 바인딩 요구에 대한 처리와 기기간의 보안 관계를 설정한다. ZDO는 네트워크에서 기기들을 탐색하고 각 기기들이 제공하는 응용서비스를 결정하는 기능을 제공한다. [1]

2.2 ZigBee의 문제점

ZigBee에서 문제점은 허가 되지 않은 디바이스가 접근하여 발생되는 문제점과 ZC와 ZED에서 키를 생성할 시 안전하지 않은 채널을 이용한 Master Key의 전송 시 발생되는 문제점 Router의 흐름을 조작하는 Router Jamming Attack 등이 있다. 또한 ZigBee네트워크에서 ZC는 오직 하나만 존재하며 FFD(Full Function Device)의 하나이며 ZigBee 네트워크에서 네트워크 관리자인 TC의 역할을 수행하므로 새로운 디바이스에 대한 인증 및 키 생성 및 관리를 수행하게 되므로 모든 트래픽이 ZC에 집중되어 오버헤드가 발생되는 문제점이 발생된다.

2.2.1 인증 방식과 키 전송 시의 문제점

ZigBee Network에서 ZED는 라우터를 이용하여 접근을 요청 한다. ZC는 접근하는 디바이스에 대하여 받아들이고 라우를 통하여 ZED에게 Master Key를 전송하게 되면 ZC와 ZED는 각각 Master Key를 이용하여 SKKE(Symetric-Key Key Establishment)프로토콜을 이용하여 Link Key를 생성한다. 생성된 Link Key를 이용하여 ZC는 NWK(Network) Key를 암호화 하고 ZED는 Link Key를 복호화 하여 NWK Key를 획득하게 되면 인증 과 키 연결 과정이 끝나게 되며 ZC와 ZED는 안전한 채널을 이용하여 통신을 수행하게 된다.[2][4]



[그림 2] ZigBee에서의 인증 및 키 연결 과정

위 과정에는 문제점이 존재한다. ZC는 네트워크에 최초로 합류하는 디바이스에 대하여 인증하는 매커니즘이 존재하지 않음을 알 수 있다. 이러한 문제점은 ZigBee 보안 시스템의 심각한 문제점이라고 할 수 있겠다. 또한 새롭게 합류하는 디바이스가 Master Key를 가지고 있지 않을 경우에는 [그림 2]에서와 같이 ZR과 ZED사이에는 안전하지 않은 채널을 이용하여 전송되게 되므로 MITM(Man In The Middle Attack)같은 중간자 공격이 수행된다면 Master Key를 획득하게 될 것이고 Master Key를 획득하게 된다는 것은 또한 Link Key와 NWK Key까지 생성 할 수 있다는 위협이 따른다. 또한 Link Key를 이용하여 ZC에게 접근하게 될 경우 모든 ZED에 대한 컨트롤이 가능하게 되어 다수의 ZED를 이용한 DDoS(Distributed Denial of Service)공격으로도 이어질 수도 있다.

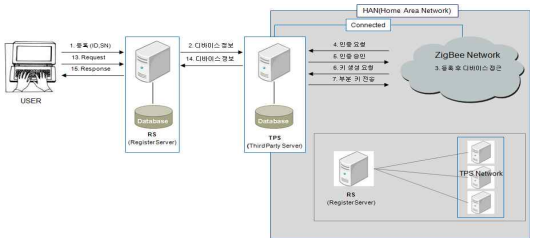
3. 제안 시스템

3.1 제안하는 디바이스 인증방법 과 키 생성 방법

제안하는 시스템은 각 디바이스 마다 존재하는 유일한 값을 이용한다. ZigBee Network에 합류를 원하는 디바이스는 ZigBee Network에 접근하기 전 User는 RS(Register Server)에 먼저 등록 시킨 후 사용 하도록 하였다. 또한 ZR에서 ZED로 전송되는 Master Key에 대한 노출 문제를 난수를 생성하여 키를 생성하는 방법을 제안하였다.

3.2 제안 시스템 구성도

제안 시스템은 [그림 3]과 같은 방식으로 구성되며 USER, RS(Register Server), TPS(Third Party Server), ZigBee Network로 구성되며 RS하부에는 TPS Network로 구성된다. TPS는 각 가구 당 배치되며 ZC와 시리얼 방식으로 연결되어 있다. TPS는 Multi-Homed 방식으로 구성된다. 또한 RS는 다수의 TPS를 관리 하는 방식으로 구성된다.



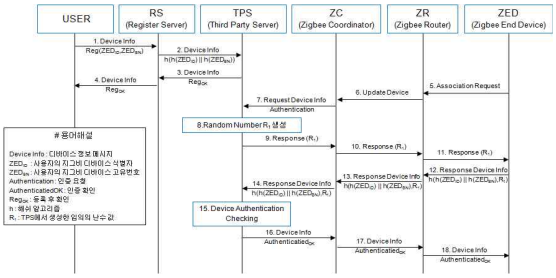
[그림 3] 시스템 전체 구성도

USER는 사용을 원하는 디바이스의 (ID, SN)같은 디바이스의 유일한 값을 RS에 등록하게 되면 RS는 디바이스의 값을 Hash하여 TPS에게 보낸다. 이렇게 하게 됨으로써 디바이스의 TPS는 디바이스는 ID와 SN 값을 알 수가 없게 된다. TPS에 등록이 완료되면 USER는 디바이스를 ZigBee Network에 물리적으로 접근 시킨다. Network에 합류하기를 원하는 디바이스는 디바이스에 대한 인증을 거치기 위하여 ZC에게 인증 요청메시지를 보내게 되면 ZC는 TPS에게 디바이스에 대한 인증을 요청한다. TPS는 인증 메커니즘을 거친 후 디바이스에 대한 접근을 허용하는 메시지를 ZC에게 보내고 키 생성을 진행한다. 키 생성 시에는 TPS에 부분키를 전송하며 부분키를 받은 ZC는 부분키에 난수 값을 생성한 후 ZED에게 키를 전송하게 된다. 실시간 모니터링은 디바이스를 인증할 시 사용된 Hash값을 주소로 사용하여 ZED에서 ZC로 ZC에서 TPS로 TPS에서 RS로 보내게 되고 RS는 사용자에게 요청한 디바이스의 사용량을 Table View형식으로 보여 주게 된다.

3.3 상세 프로토콜

3.3.1 디바이스 인증

디바이스 인증 프로토콜은 [그림 4]와 같은 방식으로 진행 된다.



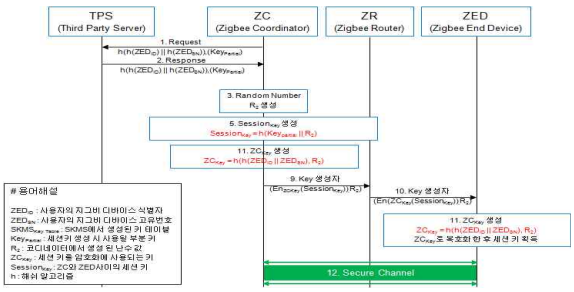
[그림 4] 디바이스 인증 프로토콜

USER는 등록을 원하는 디바이스에 대한 ID와 SN같은 디바이스의 유일한 값을 RS에 등록 한다. USER가 등록한 디바이스의 고유한 값을 h(ZED$_{ID}$ || ZED$_{SN}$)하여 TPS에게 보내고 이 값을 등록 TPS는 등록 완료 메시지를 RS와USER에게 보내게 되고 이 메시지를 확인 한 USER는 실제적으로 디바이스를 ZigBee 네트워크에 합류 시키게 된다. ZED는 ZR을 통하여 ZC에게 메시지를 보내게 되면 ZC는 TPS에게 인증을 요청하게 된다. 메시지를 받은 TPS는 난수 R$_1$을 생성하여 ZC를 거쳐ZED에게 전송하게 되고 이 값을 받은 ZED는 자신의 ID와SN을 Hash하여 h(ZED$_{ID}$ ||

ZED_{SN})값을 만들고 TPS에서 보낸 값을 추가하여 h(h(ZED_{ID} || ZED_{SN}), R_1)을 만든 후 TPS에게 보내게 된다. 이렇게 생성된 값이 TPS에서 생성된 값과 일치 할 경우 인증확인 메시지가 ZC와 ZED에게 전송됨으로써 인증이 완료 된다. TPS에서 난수 값을 생성하여 ZED에서 보내게 됨으로써 디바이스의 Hash 값이 네트워크가 노출 되지 않기 때문에 MITM이나 Router Jamming Attack에 대하여 안전하다고 할 수 있다.

3.3.2 키 생성

인증된 디바이스는 ZC와 안전한 채널을 구성하여 데이터를 주고받기 위해 키 생성을 하게 된다. 키 생성 프로토콜은 [그림 5]와 같은 방식으로 진행된다.

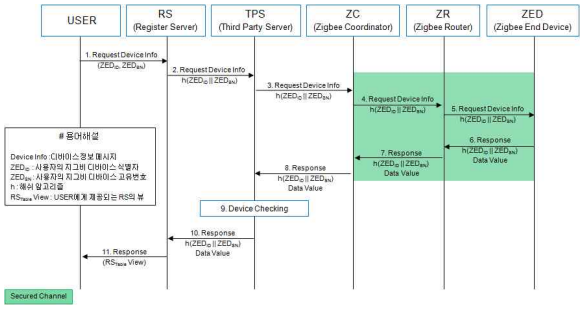


[그림 5] 키 생성 프로토콜

ZC는 ZED와 키를 생성하기 위하여 TPS는 인증 시 사용된 디바이스의 Hash값과 부분키를 ZC에게 전송하게 되고 응답을 받은 ZC는 난수 R_2를 생성한 후 다음과 같은 방식으로 h($Key_{Partial}$ || R_2) R_2와 Key_{Partia}을 Hash한 값으로 ZED와 ZC에서 사용 할 세션 키와 세션 키를 암호화 하여 보낼 ZC_{Key}를 생성한다. ZC_{Key}키는 다음과 TPS로 받은 h(ZED_{ID} || ZED_{SN})와 난수 R_2를 이용하여 생성한다. 생성된 ZC_{Key}를 이용하여 ZED와 ZC에서 사용될 키를 암호화 하여 보내고 ZED는 ZC에서 사용한 동일한 방법으로 하여 키를 생성하고 복호화 하여 세션 키를 획득하여 ZC와 ZED사이에 안전한 채널을 생성 한다. TPS에서 받은 부분키에 대하여 ZC에 생성한 난수 값을 사용하게 됨으로써 TPS는 ZC와 ZED가 사용하는 키 값에 대하여 알지 못하므로 ZC와 ZED의 유일한 키를 생성 할 수 있다.

3.3.3 실시간 모니터링

USER는 실시간으로 모니터링을 수행할 수 있으며, 모니터링은 ZC와 ZED사이의 안전한 채널이 생성된 이후에만 가능하다. 모니터링의 상세 프로토콜 진행은 [그림 6]과 같다.



[그림 6] 실시간 모니터링

USER가 사용 중인 디바이스에 대하여 모니터링을 요청하려면 디바이스의 ID와 SN을 입력한 후 RS에게 모니터링을 요청하면 RS는 디바이스에 대한 확인을 수행한 후, 등록된 디바이스 일 경우, TPS에게 요청하게 되는데 TPS에게 보내기 전 디바이스 정보에 대하여 Hash를 수행하고 TPS에게 보내게 된다. 요청 메시지를 받은 TPS는 ZC에게 디바이스의 해시 값을 보내어 모니터링을 요청 한다. ZC는 이전에 TPS에게 부분키를 요청할 때, 디바이스의 Hash값을 전송 받았기 때문에 ZC에서 관리 하는 디바이스 테이블을 참고하여 해당 디바이스가 세션을 찾고 안전한 채널을 이용하여 디바이스에게 요청을 보내게 된다. 요청을 확인한 디바이스는 자신의 사용량을 Data Value에 포함시켜 안전한 채널을 이용하여 ZC에게 보내게 되면 ZC는 TPS에게 보내고 TPS는 디바이스에 대한 체킹을 수행한 후 RS에게 보낸다. RS는 USER에게 테이블 View형식으로 보여주게 된다.

4. 결론 및 향후 연구과제

스마트 그리드 정책이 진행되고 있음에 따라 HAN에서 ZigBee의 활용도는 높아질 추세이다. ZigBee는 많은 장점을 가지고 있는 반면 많은 취약점이 존재한다. 활용도가 증가할 ZigBee에 대하여 더욱 강력한 보안 메커니즘이 절실히 요구되며, 인가된 디바이스에 한하여 키를 생성하는 방식을 도입해야 한다. 메시지 조작에 대한 공격에 대한 방어책 또한 고려해야 될 대상이다. 본 논문에서는 AMI에서의 HAN의 모델 구성 부분을 참고하여 시스템을 구성해 보았다. 저자는 시스템의 구조보다는 이러한 인증 방식의 매커니즘을 제안하고자 한다. 향후 과제로는 일반적인 ZC에서 발생되는 트래픽 량과 저자가 제안한 시스템에서 사용되는 ZC에대한 트래픽 량을 비교 분석 할 예정이며, 인증

시 사용도니 알고리즘과 기존의 일반적으로 사용되는 AES-128bit의 CCM기법에 대하여 안전성과 속도에 대하여 비교 분석 할 예정이다.

참고문헌

[1] 심재창 외 2명, "jshim-ZigBee-Draft1" September 15, 2006

[2] 김현주 외"시스템 ID를 이용한 USN의 보안 취약성 개선" 2009년 2월 전자공학회 논문지 제 46권 TC편 제 2호

[3] 김근영 외 "통신사업자 홈네트워크 기반의 스마트 그리드" AMI(Automatic Metering Infrastructure) 구축방안

[4] Ember Inc.," EmberZNet 3.1 New Features and Changes," April 2008.

[5] Robert Cragie외 ZigBee Security