한국컴퓨터정보학회 동계학술대회 논문집 제24권 제1호 (2016. 1)

ZigBee 네트워크 키 관리 기법 조사

정성민*, 이정준O, 정영교*, 윤희용*
*O성균관대학교 전자전기컴퓨터공학과
e-mail:{gearfried, jungjune86, joung0491, youn7147}@skku.edu*O

A Survey on Key Management of ZigBee Network

Sung-Min Chung*, Jung-June LeeO, Young-Gyo Jung*, Hee-Yong Youn*
*ODept. of Electrical and Computer Engineering, Sungkyunkwan University

● 요 약 ●

ZigBee는 전력소모가 적고 근거리통신방식을 사용하며 저비용인 장점을 가지는 개인 영역 네트워크 (PAN)이다. ZigBee가 산업과 헬스케어 등의 여러 애플리케이션에서 많이 사용되면서, 최근 ZigBee에서의 보안이 중요한 문제로 다루어졌다. 본 논문에서는 ZigBee 네트워크에서의 키 관리 기법을 조사하고 보안능력 및 성능을 분석한다.

키워드: 지그비(ZigBee), 키 관리(key management), 지그비 보안(ZigBee Security)

I. Introduction

저 전력, 저 비용 무선 네트워크 프로토콜의 대표적인 표준이라 할 수 있는 ZigBee는 헬스케어, 스마트그리드 환경 및 보안 분야에서 그 활용성이 높아지고 있다. ZigBee는 IEEE 기술 표준인 802.15.4를 기반으로 만들어진 무선 개인 영역 네트워크로, ZigBee의 각 단말들은 저 전력 소모로 다수의 디바이스와 연결 가능하며, 고품질의 기능은 아니지만 센서와 연동하여 데이터 전송이 가능하도록 충분한 성능을 제공 한다[1].

II. ZigBee 네트워크 보안 및 취약점

ZigBee 네트워크 프로토콜 스택은 OSI 계층을 기반으로 그림 1과 같이 구성되어 있다.

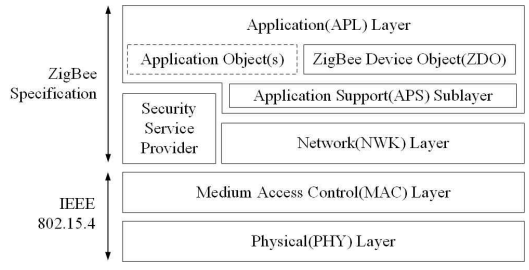

Fig. 1. ZigBee Protocol Stack Architecture

위의 그림과 같이 IEEE 802.15.4에서 정의된 두 개의 계층인 Physical(PHY) 계층과 Media Access Control(MAC) 계층을 기반으로 하며, 그 위로 ZigBee Alliance에서 정의한 두 개의 ZigBee 계층인 Network(NW) 계층과 Application(APL) 계층을 추가한 형태로 구성 된다 [2].

ZigBee의 보안 메커니즘은 데이터 암호화, Sequential Freshness, 프레임 무결성 체크, and Entity Authentication Service를 제공한다. ZigBee는 AES-128 CCM* 암호화 알고리즘을 지원하는데, CCM*은 IEEE 802.15.4에서 제공하는 AES-CCM을 확장한 것으로 암호화 기능, 인증기능을 각각 제공, 또는 두 가지 기능 모두 제공 가능하다 [3].

ZigBee 보안의 여러 가지 문제점 중 가장 핵심적인 문제는 제한된 성능으로 ZigBee 환경에서는 현재의 강한 보안성을 지닌 알고리즘을 적용하는 것이 제한된다. 때문에 ZigBee에서 선택할 수 있는 보안메커니즘은 한정되어 있고, 일정 수준 이상의 암호화가 불가능하므로 많은 위협에 노출된다.

III. ZigBee 네트워크의 보안 취약점

몇몇 ZigBee 네트워크 보안 취약점은 비 암호화 구간에서의 키 분배, 노드의 네트워크 탈퇴 시 탈퇴 노드의 키 제거 문제, 암호화 nonce 등이 있다. nonce는 32비트 프레임 카운터로 되어 있어 ZigBee 네트워크에서 재전송 공격을 보호하기 위한 중요한 역할을 한다. 센서 혹은 컨트롤러와 같은 디바이스는 에너지 절약을 위한 절전 모드로 전환되거나, 데이터 추가 전송을 위해 메모리에 nonce를 저장한다. 절전 모드로 전환하면서 소정의 시간 동안 네트워크 코디네이터와의 접속을 끊고 프레임 카운터 값을 0으로 초기화 한 후 다시 연결을 시작한다. 이 과정을 통해 재생성 되는 암호문(CT)은 다음과

같이 나타낼 수 있다.

$$CT_1 = [PT_1 \text{ XOR } E_{key}(n)] \quad (1)$$
$$CT_2 = [PT_2 \text{ XOR } E_{key}(n)] \quad (2)$$

이러한 암호문은 ZigBee 네트워크에서 동일한 키와 nonce로 나타낼 수 있다. [4] 에 따르면 CT_1과 CT_2이 다른 평문과 같은 암호화키, 그리고 같은 nonce를 포함할 때, 공격자는 $[CT_1 \veebar CT_2]$의 연산을 통해 $[PT_1 \veebar PT_2]$를 얻기 위해 bypass를 사용할 수 있다. 이러한 문제의 수학적 증명은 다음과 같다.

$$\text{(가정) } CT_1 \text{ XOR } CT_2 = PT_1 \text{ XOR } PT_2, \quad (3)$$

$$(PT_1 \textbf{ XOR } E_{key}(n)),$$
$$PT_1 \textbf{ XOR } PT_2 \textbf{ XOR } (E_{key}(n) \textbf{ XOR } E_{key}(n)),$$
$$PT_1 \textbf{ XOR } PT_2 \textbf{ XOR } (0 \textbf{ XOR } 0),$$
$$PT_1 \textbf{ XOR } PT_2$$

이 때 공격자는 빈도 횟수 분석을 이용하여 평문을 얻을 수 있으며 다음과 같은 식으로 키를 만들어 낼 수 있다.

$$E_{key} = CT \textbf{ XOR } PT = (PT \textbf{ XOR } E_{key}) \textbf{ XOR } PT = E_{key} \quad (4)$$

따라서 공격자는 여러 암호문의 비교를 통해 텍스트에서 어느 바이트가 바뀌었는지 발견할 수 있기 때문에 그로 인한 평문을 추측하고 키를 유추해내는 것이 가능하다.

IV. Conclusions

본 논문에서는 ZigBee 네트워크에서의 키 관리 기법을 조사하고 보안능력 및 성능을 분석하였다. 공격자는 빈도 횟수 분석을 이용하여 여러 암호문의 비교를 통해 키를 유추해내는 것이 가능하다는 문제점이 있다. 때문에 이러한 공격에 대한 추가적인 보안 서비스가 적용될 수 있는 연구가 필요하다.

Acknowledgment

본 연구는 BK21Plus 사업, 한국연구재단 기초연구사업 (2013R1A1A2060398), 삼성전자, 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신·방송 연구개발사업 (1391105003)의 일환으로 수행하였음.

References

[1] Yan, Z., & Jiaxing, Z. “Design and implementation of Zigbee based wireless sensor network for remote SpO2 monitor.” In Future Computer and Communication (ICFCC), 2010 2nd International Conference on (Vol. 2, pp. V2-278). IEEE.

[2] Yüksel, E., Nielson, H. R., & Nielson, F. “Zigbee-2007 security essentials.” In Proc. 13th Nordic Workshop on Secure IT-systems (pp. 65-82).

[3] bhkim, jmlim, and chspark. “Analysis of ZigBee Security Mechanism” Jounal of Security Engineering 9.5, 2012.

[4] Forler, C., Lucks, S., & Wenzel, J. “Designing the API for a Cryptographic Library.” In Reliable Software Technologies–Ada-Europe 2012 (pp. 75-88). Springer Berlin Heidelberg.