한국정보전자통신기술학회논문지(jkiiect)'21-2, Vol.14 No.1
논문 21-14-01-98 http://dx.doi.org/10.17661/jkiiect.2021.14.1.98

확장성과 보안을 보장하는 IoT 디바이스 기반의 그룹통신 기법

김기영*

Scheme of Secure IoT based Group communication

Ki-Young Kim*

요 약 본 연구에서는 보안기능을 탑재한 IoT 단말로 구성된 네트워크를 구성하여 보안성과 확장성을 보장하는 그룹통신 기법을 제안한다. 네트워크상에 참여하는 단말의 수가 증가하면 네트워크 자원도 비례하여 감소되며 IoT 단말에 보안기능을 추가하면 IoT 단말에서 암호화로 인해 지연시간이 증가하게 된다. 네트워크에 발생하는 에러율이 높아지면 재전송으로 인해 네트워크 자원은 빠르게 잠식되게 된다. 따라서 보안성을 지원하면서 확장성을 보장하도록 IoT 단말을 그룹화 하여 참여 노드가 증가하여도 네트워크 자원의 소모를 감소시켜 확장성을 보장할 수 있도록 하였다. 향후 구현을 위해 IoT 단말에서 사용하는 암호화 방식은 IEEE802.5.4의 표준을 고려하였으며 표준화 동향을 조사 분류하였다. 제안하는 방식은 IEEE802.5.4 표준의 보안기능을 제공하는 IoT 디바이스를 그룹통신 기반에 적용하여 신뢰성과 확장성 보장이 가능하도록 하였다. 성능평가는 시뮬레이션을 통해 보안기능을 갖는 IoT 디바이스를 기존 방식과 그룹통신으로 구성하였을 때의 지연시간을 비교하여 제안한 방법의 효율성을 확인하였다.

Abstract In this study, we propose a group communication technique that guarantees security and expandability by configuring a network consisting of IoT terminals equipped with security functions. As the number of devices participating in the network increases, network resources are proportionally reduced, and adding a security function to the IoT device increases the delay time due to encryption in the IoT device. If the error rate that occurs in the network increases, network resources are quickly consumed due to retransmission. Therefore, IoT terminals are grouped to ensure scalability while supporting security, reducing the consumption of network resources even when the number of participating nodes increases, thus ensuring scalability. For the future implementation, the encryption method used in IoT terminals considered the standard of IEEE802.5.4, and the standardization trend was investigated and classified. The proposed method applies IoT devices that provide security functions of the IEEE802.5.4 standard to the group communication base to ensure reliability and scalability. In the performance evaluation, the effectiveness of the proposed method was confirmed by comparing the delay times when grouping IoT devices with security functions through simulation.

Key Words : Security, IoT, Scalability, IEEE802.15.4, Group Communication

1. 서론

최근 IoT기술은 데이터를 수집하고 원격지의 서버로 전송하여 빅데이터 구축과 활용을 가능하게 하고 있다. IoT기술은 원격제어를 통해 스마트팜 개발에도 적용되고 있으며 기존 사회의 인프라, 소비산업 등 전반적으로 영향을 미치고 있다[1]. IoT 디바이스가 폭넓게 통신 서비스에 적용되어 사용되자 다양한 보안취약성 등이 들어나고 있다. 그 이유로 IoT디바이스를 개발했을 때 기본적으로 IoT 디바이스에 보안모듈을 탑재하지 않았으며 그 결과 현재 다양한 보안위협 이슈

The present research has been conducted by the Research Grant of Seoil University in 2021
*Dept. of Software Engineering, Seoil University
Received February 04, 2021 Revised February 06, 2021 Accepted February 17, 2021

가 발생되고 있다[2]. 보안이슈를 해결하기 위해 IEEE802.5.4 표준을 조사하였고 확장성을 제공하는 그룹통신 기반의 IoT디바이스 네트워크 기법을 제안하였다. 기존 네트워크에 보안기술을 제공하는 IoT디바이스를 적용하였을 때와 그룹통신 기반 네트워크에 적용했을 때의 확정성에 대해 비교하였다. 본 논문에서 고려하는 그룹통신은 3계층 이상에서 구현되는 기술에 해당한다. 2절에서 IoT디바이스에서 고려해야할 보안사항 및 표준화동향 및 표준에 대해 분류 조사하고 3장에서는 확정성과 보안기능이 추가된 그룹기반의 IoT 네트워크를 제안한다. 4장에서는 보안기법이 적용된 IoT디바이스를 적용했을 때 통신효율성 분석하고 결론 및 향후 연구에 대해 기술한다.

2. 관련연구

2.1 IoT 보안

TCP/IP에 존재하는 보안취약성, 공격위협, 비정상 동작의 발생 등이 IoT 보안 이슈에 해당된다. 현재는 보안에 대한 책임은 IoT제조사와 IoT를 사용하는 회사에 있으며 IoT에서 보안 기술 요소는 Hashing, Encryption, Secure communication을 사용할 수 있다. IoT에서 고려해야할 보안 기능의 계층은 4계층으로 구성되며 인지(Perception), 응용(Application), 네트워크(Network) 계층으로 구분할 수 있다. IoT의 보안 구조는 지원계층의 기능을 추가하여 고려하고 있다. IoT 디바이스와 서버와의 통신 방식은 네트워크 계층을 이용하지만 클라우드, 인텔리전스 컴퓨팅 방식을 지원계층으로 분리하여 정의하고 있다. 보안 영역은 구조, 위협요소, 신뢰성, 정책으로 구분할 수 있다. 계층은 인지계층, 응용계층, 네트워크계층으로 구분할 수 있다. 인지계층은 IoT디바이스가 데이터를 수집 하는 부분이다. 불법적인 공격자로부터 인지계층의 피해를 방지하기 위해서 반드시 보안기능을 추가하는 것이 필요하다. 응용계층은 OSI7 계층과 유사한 개념으로 다양하고 복잡한 구조를 갖는 계층이다. 따라서 IoT를 제조 생산하는 디바이스 제조업체별로 서로 다르고 통일된 표준이 확립되어 있지 않다. 이와 같은 태생적인 문제로 인해 보안 관련 침해사례가 발생하기 쉬운 구조이고 표준이 없는 상태에서는 보안을 효율적으로 구축하고 운영하는 것은 불가능하다. 따라서 응용계층에서 데이터 접근 허가와 인증 기능 등을 고려해야 한다. 일반적으로 운영체제, 플랫폼의 취약성이 존재할 수 있지만 안정화된 이후에는 발생할 확률은 낮아지게 된다. 또한 취약점이 발견되어도 패치 등을 통해 신속한 대응이 가능하다. 하지만 소프트웨어에서 발생하는 취약점은 개발자, 개발회사에 따라 발생하기 때문에 운영체제, 플랫폼에서 발생하는 취약성과 다른 성격을 갖는다. IoT환경에서 보안 위협요소로 DoS, DDoS 공격 등을 고려할 수 있다. 이와 같은 공격은 기존 인터넷 서비스에서도 빈번히 발생하고 있는 공격이지만 그 대응기술의 발전으로 공격을 차단하는 확률이 높아지고 있다. IoT디바이스의 특성을 고려하여 DoS, DDos 공격을 방지하기 위해서는 IoT 보안 구조를 네 개의 계층으로 구분하여 설계해야 한다. 첫 번째 계층인 인지계층(perceptual layer)의 범위는 센서와 물리적 장치에서 다루어야 할 기능으로 정의한다. 물론 IoT디바이스의 특성상 저용량 저장 공간과 낮은 계산 기능을 갖기 때문에 기존 라우터, 스위치 등에서 사용하는 기술을 적용하는 것은 한계가 존재한다. IoT디바이스에서 발생할 수 있는 보안공격은 다양하지만 대표적인 방법을 7 가지로 구분할 수 있다. 인지계층에서의 보안 고려사항으로 첫 번째 차동 전력 분석 (DPA)암호화에 저장된 비밀 키를 공개하여 보안 장치에 저장시키는 방법을 사용한다. 이 방식은 일정형식의 텍스트의 전력추적을 위해 확률모델을 사용한다[2]. 두 번째는 게이트웨이 노드 공격으로 공격자가 쉽게 제어 할 수 있어 보안 위험을 초래하며 전체 네트워크의 보안을 침해할 수 있다[3]. 세 번째 가짜노드, 악의적 데이터 공격방식으로 시스템에 노드를 추가한 공격자가 데이터 주입, 악의적 코드 공격을 수행한다. 이와 같은 공격은 시스템에 실제 데이터 전송을 동작되지 않게 할 수 있다. 네 번째는 DoS는 보편적인 공격방법으로 서버와 네트워크 자원을 소진하게 하여 서비스를 불가능하게 만든다. 다섯 번째는 라우팅 공격으로 데이터의 전송과 중계를 담당하기 때문에 전송 중에 중간노드들의 공격이 가능하다[4]. 여섯 번째는 재연공격으로 신뢰관계인 시스템으로 가장하여 패킷을 상대 시스템에 다시 보내서

보안공격을 한다. 일곱 번째는 부채널(SCA)공격은 비밀키를 알아내고 알아낸 비밀키를 RFID 등의 보안 장비에 할당하여 정보를 획득하는 공격이다.

2.2 IoT 표준 플랫폼

IoT를 적용한 서비스 개발에 공통 플랫폼을 적용하는 것은 보안문제를 해결에도 효율적이다. 이와 같은 이유로 표준의 필요성이 대두되었으며 표준화는 IEEE에서 진행을 하였다. 관련 표준은 IEEE802.15.4는 데이터 통신에 있어서 에너지 효율과 데이터의 범위, 속도를 고려하여 정의하고 있다. IEEE802.5.4의 물리계층은 저전력 통신을 위해 6LoWPAN, CoAP와 같은 표준기술을 적용하여 사용하고 ZigBee-2006, ZigBee PRO, ISA 100.11a와 같은 WSN표준 기술도 도입하고 있다. 802.15.4 물리계층에서 다루는 무선기술은 다음 표 1과 같다.

표 1. 802.15.4 적용 무선기술
Table 1. 802.15.4 Wireless Technology

무선기술	비고
Radio Frequency	2.4Ghz 16Ch
Industrial, Scientific and Medical	
Direct Spread Spectrum(DSS)	
Ultra-Wideband(UWB)	
Chirp Spread Spectrum(CSS)	

IoT 디바이스는 FFD와 RFD로 구분할 수 있다. FFD는 네트워크 디바이스와 직접 연동이 가능한 것을 의미하고 RFD는 FDD등을 통해 네트워크 디바이스와 연동될 수 있는 것을 의미하며 IEEE802.15.4는 peer to peer를 지원하고 16비트 또는 64비트 식별자를 사용하여 디바이스를 구분 한다. 기존 주소체계와 호환성 지원을 위해 6LoWPAN은 IPv6주소를 16비트 또는 64비트 구분자로 사상할 수 있는 기법을 제공한다.

데이터의 형식은 네 가지로 데이터 프레임, 응답 프레임, 비컨 프레임 MAC 명령 프레임이다. 전송 시 발생하는 충돌 감지를 CSMA/CA기법을 사용한다.

3. 그룹통신 기반 보안 IoT 기법

3.1 IoT 보안 플랫폼

IEEE은 저전력 IoT 표준 프로토콜 스택을 정의하고 있다. 기존의 관련 통신기술과 호환을 위해 인터넷과 연결되지 않은 WSN(Wireless Sensor Networks)과 유사하지만 IoT 표준 프로토콜 스택은 기존 인터넷 표준과 상호환성을 보장할 수 있도록 설계하였다. IoT의 통신 스택은 5계층으로 구성되며 하위 2계층은 물리, 맥계층으로 인터넷 프로토콜 스택의 하부 계층이 지원하는 기능과 유사하다.

적응(Adaption)계층은 6LoWPAN을 사용한다.

IoT 디바이스는 블루투스, Wi-Fi 무선기술을 사용하여 연결하고 보안 기능은 링크계층에서 지원하도록 설계했다. 하지만 IEEE802.15.4는 링크 계층에서 보안 기능을 제공하지 않고 IoT디바이스 MAC계층에서 제공하도록 했다. MAC계층에서 보안 기능을 제공하는 방법은 상위 계층의 프로토콜 스택에 구현하는 것보다 시스템을 단순하게 할 수 있는 장점이 있다. 이와 같은 이유로 대칭암호화를 하드웨어에서 지원하도록 고안하였다. 센서네트워크 플랫폼에 사용되는 텍사스 인스트루먼트의 c2420과 크로스보우의 TelosB는 MAC계층인 하드웨어에서 AES기반의 보안기능을 제공한다[5]. IoT단말에서 사용할 수 있는 AES, ECC알고리즘은 일반적인 방식이 아닌 경량화된 AES[7], ECS[8,9]알고리즘을 사용하고 있다.

3.2 그룹통신기반 보안 지원 IoT 네트워크

경량화된 보안 알고리즘을 적용하여도 암호화에 따른 오버헤드가 발생하며 이는 전송지연시간의 형태로 나타난다. 암호화 지연시간은 상수이기 때문에 가변적으로 네트워크 지연을 감소시켜 전체 전송 지연시간을 감소시킬 수 있도록 그룹통신 기반의 IEEE802.15.4 표준 보안 플랫폼을 사용하는 IoT 디바이스로 구성된 네트워크 기법을 제안한다.

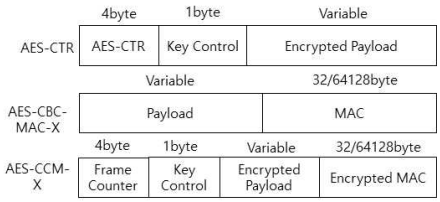

그림 1. IEEE802.15.4보안 페이로드 형식
Fig. 1. IEEE802.15.4 Security Payload

IEEE802.15.4 보안표준은 링크계층 데이터 프레임의 보안설정 비트 필드를 사용하여 보호 프레임을 구분한다. IEEE802.15.4 링크계층 데이터 프레임의 헤더 앞부분은 2byte에 프레임 제어(Frame Control)필드가 위치하며 부가 보안 필드 내의 3비트 플래그 비트인 보안설정 비트로 보호 프레임을 구분할 수 있도록 하고 있다. 그림 1의 두 번째 프레임은 부가(Auxiliary) 보안헤더로 보안기능을 사용할 때 비트를 설정하여 프레임에 적용된 보안모드를 나타낸다. 보안모드에 따라 페이로드의 필드 값과 위치가 상이하며 세부 내용은 그림 1과 같다. IEEE802.5.4 보안표준을 지원하는 그룹통신은 IoT 디바이스들이 각각 인터넷과 무선으로 연결되어 통신을 하는 기존 네트워크 방식과 달리 일정 지역 내의 IoT 디바이스 중에서 지정노드(Designated Node)를 통해 연격지에 위치한 서버와 통신을 하도록 하여 네트워크 상에서 발생하는 지연시간을 감소시킬 수 있다. 지연시간은 흐름제어, 오류제어로 발생되는 시간을 의미한다.

표 2. 보안 알고리즘
Table 2. Security Algorithm

알고리즘	용도
Advanced encryption standard(AES)	confidentiality
Rivest shamir adelman(RSA)/Elliptic curve cryptography(ECC)	Digital signatures key transport
Diffie-hellman(DH)	Key agreement
SHA-1/SHA0256	Integrality

보안구조의 인지계층은 IoT 디바이스의 무선통신 계층으로 RFID, ZigBee, WSN,Wi-Fi 등과 같은 물리적 방식을 사용한다. 인식 계층에서 센서를 통해 수집된 정보를 정보 처리 시스템을 통해 다른 통신 네트워크로 전송하는 미들웨어 계층은 네트워크 계층 사이에 위치하며 응용 프로그램 계층은 데이터 저장, 서비스 관리 등의 기능을 담당한다. 미들웨어 계층에서 발생하는 공격으로는 Dos공격, 데이터 공격 등이 있으며 응용계층에서의 보안은 환경에 따라 서로 다르고 응용계층 상에서 구현해야하는 보안서비스 비용은 큰 편이다. 예상되는 공격을 방지하기 위한 보안 알고리즘은 표 2와 같다.

본 논문에서 제안하는 것은 기존의 로컬 네트워크에 표준 플랫폼을 준수하는 IoT 디바이스를 확장성을 보장하면서 연결하는 것이다. IoT 디바이스와 연결되는 원격 서버의 수가 증가하면 확장성이 낮아 질 수 있다. 확장성 지원을 위해 IoT 디바이스는 그룹 단위로 통신하도록 구성하였다.

4. 성능평가

제안하는 기법은 기존의 일반적인 IoT디바이스 네트워크와 달리 IoT 디바이스를 지정 노드로 그룹화 하여 확장성을 보장하는 논리 토폴로지 방식이다. 성능분석을 위해 보안기술을 적용한 IoT 디바이스를 적용한 로컬 네트워크 환경은 그림2와 같이 가정하였다.

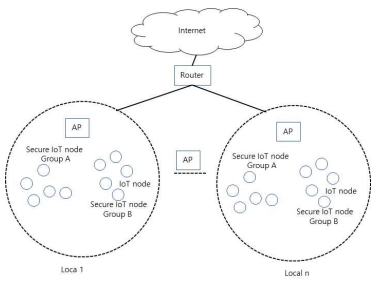

그림 2. 실험환경
Fig. 2. Simulation Environment

보안 플랫폼 기술을 적용한 네트워크 환경에서의 네트워크 지연시간을 $Dtime_{nt}$, 게이트웨이의 지연시간을

$Dtime_{gw}$, 보안기술이 적용된 IoT 디바이스 지연시간을 $Dtime_{SIoT}$ 라고 표시하면 기존 IoT 네트워크 환경에 보안 IoT 디바이스의 전체 지연시간은 avg_{time}은 다음 수식 1과 같다.

$$avg_{time} = Dtime_{SIoT} + Dtime_{nt} + Dtime_{gw} * \lambda + Dtime_{gw*}(1-\lambda) \quad (1)$$

수식 1에서 λ는 오류발생 확률을 나타낸다. 보안 플랫폼 기술을 사용하는 SIoT 네트워크 환경에서의 지정노드의 계수 G를 적용하면 전체 지연시간은 수식 2와 같다.

$$G-avg_{time} = \frac{Dtime_{SIoT} + Dtime_{nt} + Dtime_{gw} * \lambda + Dtime_{gw*}(1-\lambda)}{G} \quad (2)$$

그룹화 하지 않은 네트워크에 암호기능이 없는 IoT 디바이스와 보안이 지원되는 IoT의 지연시간은 보안기술을 적용한 IoT 디바이스로 구성한 네트워크의 지연시간은 다소 증가하였으며 기울기의 커진 것을 확인할 수 있었다.

보안을 위해 암호화에 소요되는 시간의 증가로 인해 지연시간이 증가하였다. 불법적인 정보침해를 방지하기 위해 보안기능이 있는 IoT 디바이스는 필요하기 때문에 이에 따른 지연시간의 증가는 허용할 수 있는 범위 내에 있어 지연에 따른 문제가 발생하지 않는다. 하지만 오류율이 높아지면 재전송으로 인한 지연시간이 증가하게 되고 참여하는 노드가 증가하게 되면 지연시간은 허용 범위를 넘어서게 된다.

그림 3. 그룹화 지연시간
Fig. 3. Grouping delay time

그림 3은 그룹화 하지 않은 IoT 디바이스 네트워크와 그룹화한 IoT 디바이스 네트워크의 지연시간을 나타낸다. 그룹화하지 않은 네트워크와 그룹화한 네트워크에서 사용하는 IoT 디바이스는 모두 보안기능을 지원하는 IoT 디바이스다. 더욱이 IoT 디바이스는 센싱 정보 등의 수집에 있기 때문에 실시간 데이터 통신에 민감한 지연시간보다 허용할 수 있는 지연시간에 상대적으로 민감하지 않는다는 점을 고려하면 기존 방식의 지연시간과 비교하여 감내할 수 있는 수준임을 알 수 있다.

5. 결론

IoT환경에서 신뢰성을 보장을 위해서는 기존 네트워크 장비의 보안기술 외에 IoT 디바이스 단에서 보안을 지원해야 한다. 본 논문에서는 IoT 환경에서 발생할 수 있는 취약성과 필요 보안기술 표준 기술 프로토콜을 그룹통신 기반에 적용하였다. 그룹통신은 확장성을 보장할 수 있는 통신 토폴로지로 보안기술이 적용된 IoT 디바이스 중에서 그룹대표를 선출하고 인증을 위임받아 처리하도록 하였다. 보안기능을 탑재한 IoT 단말로 구성된 네트워크를 구성하여 보안성과 확장성을 보장하는 그룹통신은 L3상에서 흐름제어, 에러제어를 그룹화하는 통신방법으로 통신지연시간을 감소시켜주는 통신기법이다. 네트워크상에 참여하는 단말의 수가 증가하면 네트워크 자원도 비례하여 감소되어 통신지연은 노드가 늘어남에 따라 증가한다. 또한 IoT 단말에 보안 기능이 추가되면 통신지연시간은 증가하게 된다. 따라서 본 논문에서는 IEEE802.5.4표준에서 정의한 보안기능을 준수하여 IoT네트워크를 구성하고 통신지연시간은 낮출 수 있는 방법으로 그룹통신기반의 IoT네트워크 기법을 제시하였다. 제안한 기법은암호화 방식은 IEEE802.5.4의 표준을 고려하였으며 표준화 동향을 조사 분류하였다. 제안하는 방식은 IEEE802.5.4 표준의 보안기능을 제공하는 IoT 디바이스를 그룹통신 기반에 적용하여 신뢰성과 확장성 보장이 가능하도록 하였다. 성능평가는 시뮬레이션을 통해 보안기능을 갖는 IoT 디바이스를 기존 방식과 그룹통신으로 구성하였을 때의 지연시간을 비교하여 제안한

방법의 효율성을 확인하였다. 그룹의 지정노드의 선정에 따라 성능에 영향을 미치기 때문에 향후 연구로 지정노드 선정기법에 관한 연구가 필요하다.

REFERENCES

[1] Jang-Won Kim, "A Study on Smart Door Lock using Internet of Things", Korea Information Electron Communication Technology Journal of Korea Institute of Information, Electronics, and Communication Technology 13(6), pp.539-544, 2020.

[2] I. Yaqoob and al. Internet of Things Architecture: Recent Advances, Taxonomy, Req , IEEE Wireless Communications, vol. 24, no 3, pp. 10 16, 2017.

[3] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, Goals, RFC 4919, 2007.

[4] ZigBee Alliance, ZigBee specification, pp. 344-346, 2006.

[5] S. A. Kumar, "Security in Internet of Things: Challenges, Solutions and Future Directions", pp. 5772-578, 2016.

[6] S. Chen, Z. Honggang and L. Xian, "Energy Group based Random Access Method for M2M Communications," 2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Qingdao, pp. 1-5, 2018.

[7] "IEEE Draft Standard for Low-Rate Wireless Networks Amendment Defining Support for Advanced Encryption Standard (AES)-256 Encryption and Security Extensions," in IEEE P802.15.4y/ D2, October 2020 , vol., no., pp.1-20, 2020.

[8] K. Sarwar, S. Yongchareon and J. Yu, "Lightweight ECC with Fragile Zero-Watermarking for Internet of Things Security," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, pp. 867-872, 2018.

[9] E. Gyamfi, J. A. Ansere and L. Xu, "ECC Based Lightweight Cybersecurity Solution For IoT Networks Utilising Multi-Access Mobile Edge Computing," 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, pp. 149-154, 2019.

저자약력

김 기 영(Ki-Young Kim) **[종신회원]**

- 2004년 3월~현재 : 서일대학교 소프트웨어공학과 교수

〈관심분야〉 빅데이터, IoT, ITS, 네트워크보안