LoRa 환경에서의 Class 분류에 따른 선택적 암호화 기술

이남곤 · 김기천*

건국대학교

Selective encryption technique according to class classification in LoRa environment

Nam-gon Lee · Keecheon Kim*

Konkuk University

E-mail : a2369ya@konkuk.ac.kr

kckim@konkuk.ac.kr*

요 약

현재 데이터 통신의 세계는 단순히 유선으로 서버와 유저간의 통신이 아닌, 무선 환경을 이용하여 더 넓고 다양한 환경에서 다양한 디바이스가 통신을 주고받으며 대량의 데이터들을 만들어 내고 있다. 이러한 환경에서 IoT는 이제 우리 삶 깊숙한 곳에 자리를 잡고 있고, 많은 업무에서 IoT 기술들이 이용이 되고 있지만, IoT 안에서 사용되는 데이터들은 악의적인 행위로부터 충분한 보호를 받지 못하고 고스란히 노출이 되어 있는 상황이다. 이러한 디바이스들 대부분 악의적인 공격에 대처할 수 있는 충분한 컴퓨팅 파워를 보유하고 있지는 못한 상황이다. 본 논문에서는, 단순한 센서부터 충분한 컴퓨팅 파워 및 안전성을 가져야 하는 디바이스 모두가 상황에 맞춰 보안성을 갖출 수 있도록 하는 것을 목표로 한다. 제안하는 기술은 디바이스의 중요도와 컴퓨팅 파워를 중심으로 Classing을 하고, 그것을 통하여 선택적으로 암호화 기술을 선택, 보안성을 강화할 수 있는 방안을 마련하는 것이다.

ABSTRACT

Currently, the world of data communication is not simply communication between server and user in a wired way, but using wireless environment, various devices communicate with each other in a wider and diverse environment to generate a large amount of data. In this environment, IoT is now located deep in our lives, and IoT technologies are used in many tasks, but the data used in IoT is exposed without sufficient protection from malicious behavior. Most of these devices do not have enough computing power to cope with malicious attacks. In this paper, we aim to make all devices that have sufficient computing power and safety from simple sensors to be able to have security according to the situation. The proposed technology is based on the importance of the device and computing power, and it is possible to select the encryption technology selectively and to improve security.

키워드

LoRa, IoT, Classing, Authentication, Encryption

Ⅰ. 서 론

스마트폰과 무선 네트워크 환경의 발달에 힘입어 폭발적인 성장을 거두기 시작한 IoT는 이제 생활 곳곳에 자리 잡고 있을 뿐만 아니라, 사회 전반에 걸쳐 다양한 곳에서 우리의 생활의 질을 높이는 데에 이바지하고 있다. 지속적으로 다양한 IoT 기술이 생겨나고 있지만 근래에 가장 각광받는 기술로서는 LPWAN(Low Power Wide Area Network)이 있다. 글자 그대로의 뜻인 저전력 광

범위 네트워크로서, 하나의 도시나 거대한 공장 등에서 여러 센서 네트워크를 중심으로 하여 체계적으로 도시 및 공장의 인프라 및 시스템을 관리하는 용도로 사용되고 있다. 다양한 LPWAN 기술 가운데서 본 논문에서는 LoRa[1]라는 기술을 다뤄보고자 한다. LoRa(Long Range)는 라이센스 없이도 사용이 가능하며, 무엇보다 LPWAN 기술 중에서도 몇 없는 보안성을 제공하는 프로토콜이다. 하지만 LoRa는 AES-128 암호화만을 제공하기 때문에 보안 기술의 다양성이 낮고 또한 AES-128은 상대적으로 보안에 취약하다. 그렇기에 본 논문에서는 LoRa환경에서의 단말 Classing과 그것을 이용한 선택적 암호기술을 제안하여 LoRa 통신에서의 비도를 증가시키고자 한다.

II. LoRa

LoRa는 이름에서도 알 수 있듯이 장거리 통신을 위해 개발된 기술로서 약 10km까지 통신이 가능하도록 설계가 되어 있으며, 그와 더불어서 LPWAN 특성상 저전력 기능 또한 갖추고 있어 센서 노드에 대해 10년 정도의 라이프타임을 가질 수 있다. 10년이라는 기간 동안 노드를 쓸 수 있는 것는 LoRa의 특유한 통신 방식에 기인한다. LoRa는 노드 측에서의 업링크라 불리 우는 통신 세션을 통하여 서버로의 데이터 전송을 시도 특성이 있다. 이 특성을 때문에 서버로의 데이터 전송이 없으면 서버 측에서는 노드 측으로 데이터 전송 세션을 먼저 만들 수 없는 또 다른 특성이 생긴다. 이러한 특성들을 이용하여 노드가 데이터 수신을 위해 수신 슬롯을 열어 대기하는 시간을 없앰으로서 저전력 특성을 만드는 것이다.

보안 부분에서 LoRa는 두 가지의 파트로 나뉘게 되는데 하단의 그림1과 같다. 네트워크 부분의 MIC 검증과 어플리케이션 부분에 대한 AES 암호화가 그것이다. MIC는 네트워크의 기본적인 통신에 들어가는 헤더들에 대한 무결성 검증을 위한 것으로 사용되며 키는 노드가 가지고 있는 여러 정보들을 조합하여 NwkSKey라는 네트워크용 키를 만들어 낸다. AES는 위에서도 설명을 했듯이 AES-128을 표준으로 하고 있으며, 암호화에 필요한 키는 AppSKey로서 네트워크에 사용되는 MIC와 마찬가지로 노드에 들어있는 정보들을 조합하여 만들어 낸다.

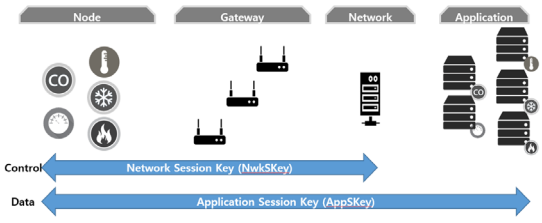

그림 1. LoRa의 보안키 사용 영역

III. 경량 AES

LoRa는 저전력 장거리 통신망이기에 현재 AES-128을 표준으로서 제정하여 사용하고 있다. 하지만 노드가 취급하는 데이터의 수준에 따라서 AES-128은 충분한 보호 조치가 될 수 없을 수 있다. 이에 대한 대책으로서는 더 상위의 AES 버전을 사용하는 것이지만 더 높아지는 연산 복잡도에 의해 노드들의 라이프타임의 감소와 딜레이등의 문제가 발생할 수 있다. 그렇기에 다양한 경량 암호 알고리즘[2]을 연구하여 IoT 환경에 적합한 암호를 찾는 것이 중요하다. LoRa'는 AES를 사용하고 있으므로 그 중에서도 경량화된 AES를 주 목적으로 하여 기술을 고안해 보기로 한다.

경량화된 AES의 경우의 문제점으로는 주로 라운드 수를 줄임으로서 스케쥴링의 복잡도가 줄어들기 때문에 나타나는 관계키 공격[3]을 꼽게 된다. 경량 암호 관련 논문 중에는 AES의 관계키 공격 취약점을 피하면서도 AES-128 대비 컴퓨팅 파워와 시간은 낮추고 키의 확산성 보다 높게 가져감으로서 경량화 한 el_AES[4] 등을 사용하여 AES-256 보다 암호 강도는 조금 약한데 반하여 빠른 시간과 낮은 컴퓨팅 파워를 가지기 때문에 해당 기술을 사용하여 기술을 제안해보고자 한다.

IV. 제 안

LoRa가 암호화하는 프레임은 앞서 설명했듯 특정 어플리케이션에 대한 데이터가 들어가는 페이로드만을 암호화한다. 각 노드들은 식별을 위한 맥, 프레임 헤더 등은 암호화하지 않고 MIC를 이용한 무결성 검증에 이용된다. 이러한 특성을 사용하여 헤더에 담기게 되는 정보를 분류 및 식별, 즉 Classing을 하여 노드의 중요도에 맞춘 암호화를 제공하는 것을 목적으로 한다.

Classing 방법은 2가지로 나눌 수 있다. 하나는 DevEUI와 DevAddr 테이블에 따른 분류와 맥 헤더 부분의 RFU 부분을 사용하는 방법이다.

DevEUI와 DevAddr을 사용하는 방법은 DevAddr을 관리자가 마음대로 설정이 가능한 것을 이용한 방법으로서, 경량 AES-256을 사용하는 노드의 DevAddr을 등록을 해둠으로서 노드를 빠르게 식별하고 경량 암호를 제공하는 방식을 취한다. 네트워크 서버에 경량 AES-256을 사용할 노드의 DevEUI에 대한 정보를 테이블에 올려두고 최초 Join-Request를 받았을 때에 해당 EUI 정보가 들어오면 DevAddr을 배정함과 동시에 AES-Table에 정보를 삽입하고 해당 정보를 어플리케이션 서버에 동시에 전달하여 어플리케이션 서버에서 또한 해당 테이블을 이용하여 노드의 경량 AES-256의 사용 상황을 알 수 있도록 한다. 추후 노드들의 통신이 있을 때에 해당 테이블을 확인하여 DevAddr이 일치하면 경량 AES-256의 키를

빠르게 불러와 복호화 및 무결성 검증을 실행할 수 있는 방식이다. 순서도는 아래 그림2와 같다.

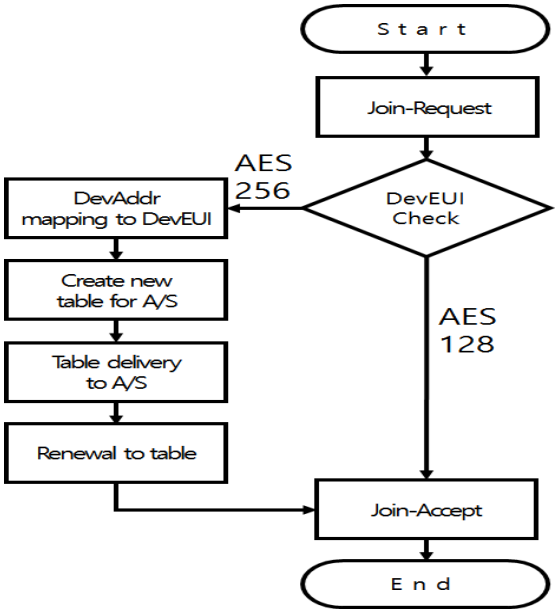

그림 2. DevEUI와 DevAddr을 이용한 순서도

두 번째 방식은 MHDR(MAC Header)에 있는 예약 비트인 RFU를 사용하는 방법이다. MHDR의 구조는 그림3과 같다. 해당 방법은 아직 표준화가 이루어지지 않은 Classing을 이용한 선택적 암호화 기술을 적용에 대해서는 회의적이지만 사용할 수 있다면 효과적일뿐더러 추후 경량 AES-256을 사용하는 LoRa망의 표준화를 시작할 때에도 충분히 좋은 조건이 될수 있으리라고 생각한다. 해당 방식은 MHDR 부분은 MIC를 이용한 무결성 검증만을 할 뿐 실질적인 암호화가 이루어지지 않는 다는 점을 이용하는 것이다. 헤더 부분에 있는 RFU 비트가 1이면 경량 AES-256으로 암호를 처리하게 코드를 구성을 하는 것이다. 해당 방식을 사용하면 RFU의 비트만 가지고도 해당 노드의 암호 방식을 파악할 수 있고 테이블을 만들고 관리함에 있어서 나타날 수 있는 테이블 변형에 의한 복호화가 불가능한 문제 등이 없어 훨씬 효율적일 것으로 예상이 된다. 또한 미래에 센서 노드들의 컴퓨팅 파워와 배터리의 수명이 증가하게 된다면 다른 암호 기술을 추가함에 있어서도 훨씬 용이할 것으로 판단된다.

Bit#	7..5	4..2	1..0
MHDR bits	MType	RFU	Major

그림 3. MHDR의 구조

V. 결 론

LoRa는 중장거리 IoT 기술 중에서 몇 되지 않는 보안 기능을 가진 IoT 기술이다. 하지만 센서의 중요도에 비해 낮은 보안성을 갖추는 경우가 있다. 이에 본 논문에서는 경량 암호 및 Classing을 통해 노드의 중요도에 맞추어 선태적인 암호화를 제공할 수 있는 기술을 제안하였다.

추후 해당 기술을 구현 및 기존 노드와의 소모 전력 및 암호 강도에 대한 비교 분석하는 것을 기획하고 있으며 이를 홈 IoT 등에 적용하는 방안 등에 대해서도 모색해 볼 예정이다.

참고문헌

[1] LoRa_Alliance, LoRaWAN_102-20161012_1398_1

[2] RSM Joshitta, L Arockiam, Authentication in IoT Environment:A Survey, Researchgate, 11,2016

[3] Alex Biryukov, Dmitry Khovratovich, "Related-Key Cryptanalysis of the Full AES-192 and AES-256", 2009

[4] 김준태, 김기천, 라운드 축소를 통한 경량 AES 블록 암호 알고리즘의 보안성 강화 연구, 한국통신학회 학술대회논문집, 23-24, 11.2015

ACKNOWLEDGMENT

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00279,안전한 IoT 전용망 구축을 위한 LPWAN 침해 방지 기술 개발)