Available online at www.sciencedirect.com

ScienceDirect

Energy Procedia 141 (2017) 540–544

Energy Procedia

www.elsevier.com/locate/procedia

4th International Conference on Power and Energy Systems Engineering, CPESE 2017, 25-29 September 2017, Berlin, Germany

Design and Implementation for Data Protection of Energy IoT utilizing OTP in the Wireless Mesh Network

Sanghoon Lee[a], Byeongkwan Kang[a], Keonhee Cho[a], Dongjun Kang[a], Kyuhee Jang[a], Leewon Park[a], and Sehyun Park[a] *

[a]*School of Electrical and Electronics Engineering, Chung-Ang Univ, Seoul 156-756, Repulic of Korea*

Abstract

An OTP(One Time Password) is an authentication method using a randomly generated nonce. Its purpose is to overcome security vulnerabilities that occur from using the same password for every transaction. When using a nonce as an encryption key for an encryption algorithm, for every data exchange a new random number is generated, thus creating an enhanced security process. Through utilizing this, authorization and data between Energy IoT(Internet of Things), Gateway, and User Device that exist in the same WPAN(Wireless Personal Area Network) can be protected.

Peer-review under responsibility of the scientific committee of the 4th International Conference on Power and Energy Systems Engineering.

Keywords: Energy IoT; Wireless Mesh Network; Security; OTP; ZigBee WLAN 802.11ac

1. Introduction

Recently, core wireless network technologies that configure WPAN are WLAN(Wireless Local Area Network), Bluetooth, ZigBee, etc. Among those, the most common Energy IoT Mesh Network configuring method is through WLAN and ZigBee [1]. When forming a network in the range up to tens of meters, WLAN escapes the wired environment of twisted pair cables and coaxial cables that connect the switch/hub and user. Instead WLAN, a wireless access network, provides a conventional Internet service through radio waves or infrared rays in a wireless environment. This allows users to move around within a local coverage area and still be connected to the network, and connects users to the wider Internet. Applications include wireless light switches, electrical meters with in-

* Corresponding author. Tel.: +82-02-822-5338-; fax: +82-02-826-5338.
E-mail address: shpark@cau.ac.kr

1876-6102
Peer-review under responsibility of the scientific committee of the 4th International Conference on Power and Energy Systems Engineering.
10.1016/j.egypro.2017.11.116

home- displays, traffic management systems, and other consumer and industrial equipment that require short-range low-rate wireless data transfer. Therefore, the technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPAN, such as Bluetooth or Wi-Fi [2]. Its low power consumption is limited to a transmission distance between 10 to 100 meters, depending on power output and additional environmental characteristics. ZigBee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. ZigBee is best suited for intermittent data transmissions from a sensor or input device. If the Energy IoT Mesh Network is configured with the two methods mentioned above, it is possible to form WPAN that has an efficient coverage with low power consumption [3].

In this paper, an Energy IoT Mesh Network Test-bed with the following conditions was configured and additional enhanced security processes were applied to the Test-bed. The network consists of Energy IoT, Gateway and User Device. ZigBee is used as the communication method between the Energy IoT and Gateway, and WLAN 802.11ac, one of the WLAN methods, was used between the Gateway and User Device. Two kinds of enhanced security process were applied. First, an OTP synchronized between Energy IoT and Gateway was used as a key of the encryption algorithm. Second, a synchronized OTP was applied to the Gateway and User Device. The device requested to be authorized to access the Energy IoT device, and the Gateway and User Device OTP value were compared. If the two values are equal, then the device was given access for use.

2. Enhanced Security System in the Energy IoT Mesh Network

2.1. Data Encryption Method for the Energy IoT Mesh Network using OTP

Wireless network system using IoT in a mesh network is built on WLAN 802.11ac and ZigBee. WLAN 802.11ac was applied to the user`s device and the gateway-to-gateway [4]. ZigBee was applied to the communications between the gateway device and the IoT [5]. Two methods above have been used as a technical element that can perform effective low power and high-speed communication.

The data encryption method of the current Energy IoT Mesh Network uses the same encryption method of wireless communications. This is not a security method that is fit for Energy IoT Mesh Networks. We suggest a new encryption algorithm that uses OTP to complement the weaknesses of Energy IoT Mesh Networks. Through OTP, an encrypted key value created through the synchronization between the Energy IoT device, Gateway, and User Device is used for encryption, decoding, and user authentication. This method escapes the current Server-Client formations such as Energy IoT device-Gateway, and Gateway-User Device, which is often Gateway-oriented, instead forming a multilateral formation and thus constructing an enhanced security system [6].

2.2. Configuration of the Enhanced Security System

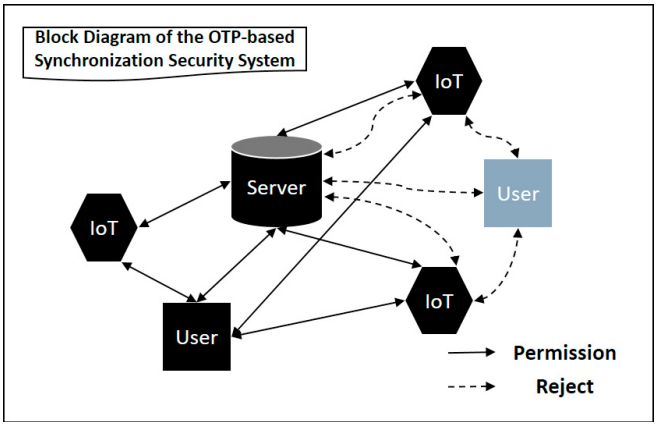

Fig. 1. Block Diagram of the OTP-based Synchronization Security System.