Protecting End-Device from Replay Attack on LoRaWAN

Woo-Jin Sung*, Hyeong-Geun Ahn*, Jong-Beom Kim*, Seong-Gon Choi*

**Information & Communication Engineering, ChungBuk National University, Cheongju-si Chungcheongbuk-do, Korea*

sungwoojin@cbnu.ac.kr, gudrhf@cbnu.ac.kr, dragonslash@cbnu.ac.kr, choisg@cbnu.ac.kr

***Abstract*— In this paper, we propose a method to protect end-device by using RSSI and Hand-Shaking technique using Proprietary Message. One of the frequently used attacks in LoRaWAN is replay attack. It is so easy to sniff packets in a wireless network environment. If an attacker intrudes a service provided by LoRaWAN, the usage pattern of the end-device may be exposed, or a replay attack may cause a problem in connection with the user. To prevent replay attack, LoRaWAN standard uses user identification method by using the value known as DevNonce, but this is not a complete countermeasure. In order to complement these vulnerabilities, we propose a method to protect users by using the physical characteristics of a network called RSSI and a new technique called Proprietary Hand-Shaking.**

***Keyword*— DevNonce, Internet of Things, LoRaWAN, Network Security, Proprietary Hand-Shaking, Received Signal Strength Indicator, Replay Attack**

Woo-Jin Sung is currently a B.S. & M.S. candidate in School of Electrical & Computer Engineering, Chungbuk National University, Korea in 2017. His research interest is network security.