Abstract

LoRa or Long Range with LoRaWAN technology is a new example of a network class and is being used on a large scale in several countries. The weakness of the LoRaWAN network is that there is no encryption process in the data payload. When the process of sending messages is running between devices, the sniffing process can find out all the messages sent and received by the device, so there is a big possibility that attacks can occur from the sniffing process that causes no privacy in the data payload. This study uses a digital signature method to secure messages sent by LoRaWAN network devices using the Advanced Encryption Standard (AES) algorithm in the message encryption and decryption process, and using the Ed25519 algorithm in the signature process, this study also analyzes the overhead of applying the digital signature method. The purpose of implementing digital signatures in this system is to verify that the data payload sent is original and does not change during the transmission process, as well as guaranteeing the confidentiality of the data payload. The addition of security mechanisms on the LoRaWAN network such as encryption, decryption and verification results has resulted in overhead in several aspects. After the analysis, there was an increase in size for several aspects when the digital signature method was applied.

Keywords: LoRaWAN, sniffing, digital signature, AES, overhead.