ABSTRACT

Wireless Sensor Network (WSN) is a wireless network of several nodes that perform sensing and can control the environment. In general, the components used in building a WSN are sensor nodes, gateway nodes and server nodes. The three components communicate with each other using LoRa (Long Range) wireless technology. Communication between nodes with wireless technology raises security issues on WSN such as sniffing, man-in-the-middle attacks and data forgery that can affect aspects of data integrity and confidentiality. This research applies security to the data to be sent via WSN using two sequential cryptographic algorithms. The first algorithm is RSA 2048 which implements asymmetric encryption where the encryption process uses a public key and the decryption process uses a private key. The second algorithm is SHA-3 hash function which is used to determine whether the data has been modified or not. RSA 2048 is an algorithm that guarantees the security aspects of authentication and non-repudiation. Meanwhile, SHA-3 is a hash function that does not have a collision attack because of the application of a sponge function at the time of the formation of the hash so that it can fulfill the security aspects of integrity. After testing by sending data packets from the sensor node to the server node with several variations of the distance based on the delay measurement, the average delay of data delivery without encryption is 2,066 seconds, while the delivery data with encryption get an average delay of 21,973 seconds. In data security testing, the results showed that encrypted data could not be read by unauthorized parties.

Keywords: WSN, RSA 2048, SHA-3, LoRa.