Penerapan Keamanan Komunikasi pada Jaringan LoRa(*Long Range*) Menggunakan Algoritma *Advanced Encryption Standard*(AES) dan *Message Authentication Code*(MAC)

Putri Apriyanti Windya[1], Vera Suryani[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]putriawindya@students.telkomuniversity.ac.id, [2] verasuryani@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstract

Internet of Things (IoT) is a popular thing nowadays. The use of IoT is increasing every year especially the use of LoRa, as well as the development of IoT *device*s. One of the characteristics of IoT *device*s is limited resources. This *device* is often referred to as IoT-constrained *device*s. Along with the increasing use of LoRa, the communication security aspect of the LoRa network must also be considered. However, the limited resources possessed by IoT *device*s are a challenge in choosing the appropriate security method. Therefore, to overcome this problem an appropriate security method is needed namely the use of AES algorithms and MAC. Variants of AES algorithm used in this research are AES128 and AES256. Meanwhile, the MAC algorithm used is Hash-based Message Authentication Code (HMAC). Based on the results of the security analysis that has been done, this methode is able to guarantee aspects of confidentiality, integrity and authentication. In addition, this study also performs overhead analysis on IoT constrained *device*s class 0 and class 2. The results of the overhead analysis show that this method is suitable to be implemented on IoT constrained *device*s class 0 and class 2.

Keywords: ***Long Range, constrained devices, CIA, AES, HMAC***