Security and Encryption

Introduction

Security is an important aspect of an IoT communication platform. After all, if a network is not properly secured, any attacker can sniff data from the sensors, or send potentially disruptive commands to the actuators, causing damage to the system.

The security of any SPRN network revolves around a pre-shared, 240-bit network secret that is stored in every device once it is configured via UART. This secret is then used to generate a packet key for every sent packet. Due to the hardware implementation of the AES-128 in ESP32 devices, and the relatively low throughput of the radio network, this encryption scheme does not create a bottleneck for packet transmission.

The general key-creation process for each payload packet, with the packet header acting as IV is as follows:

$$K_i = E_{IV}\left(S_i S_{i+1} \ldots S_{i+15}\right)$$

This creates a maximum of 15 distinct keys, which are sufficient for a maximum of 240 bytes of payload.