Comparative Study of Encryption Algorithms in Battery Powered Thread Networks for Smart Homes

Simeon Tran David C. Harrison

Baskin School of Engineering, University of California, Santa Cruz

Contribution

Energy consumption in Thread© Sleepy End Devices (SEDs) is not adversely affected by replacing standard OpenThread with a version modified to use the ASCON-128a and ASCON-128 AEAD algorithm; suggesting manufacturers can use ASCON without negative impact on battery life.

Introduction

Internet of Things (IoT) devices are often resource-constrained, with many operating on low power. Lightweight encryption algorithms are necessary to secure these devices.

ASCON is a lightweight cipher suite composed of AEAD and hashing algorithms designed for resource-constrained use cases. It is endorsed and now standardized by the National Institute of Standards and Technology (NIST).

Thread© is a wireless mesh IoT protocol built on top of 802.15.4, and is designed for smart homes and buildings. OpenThread is an open-source implementation of Thread© created and maintained by Google.

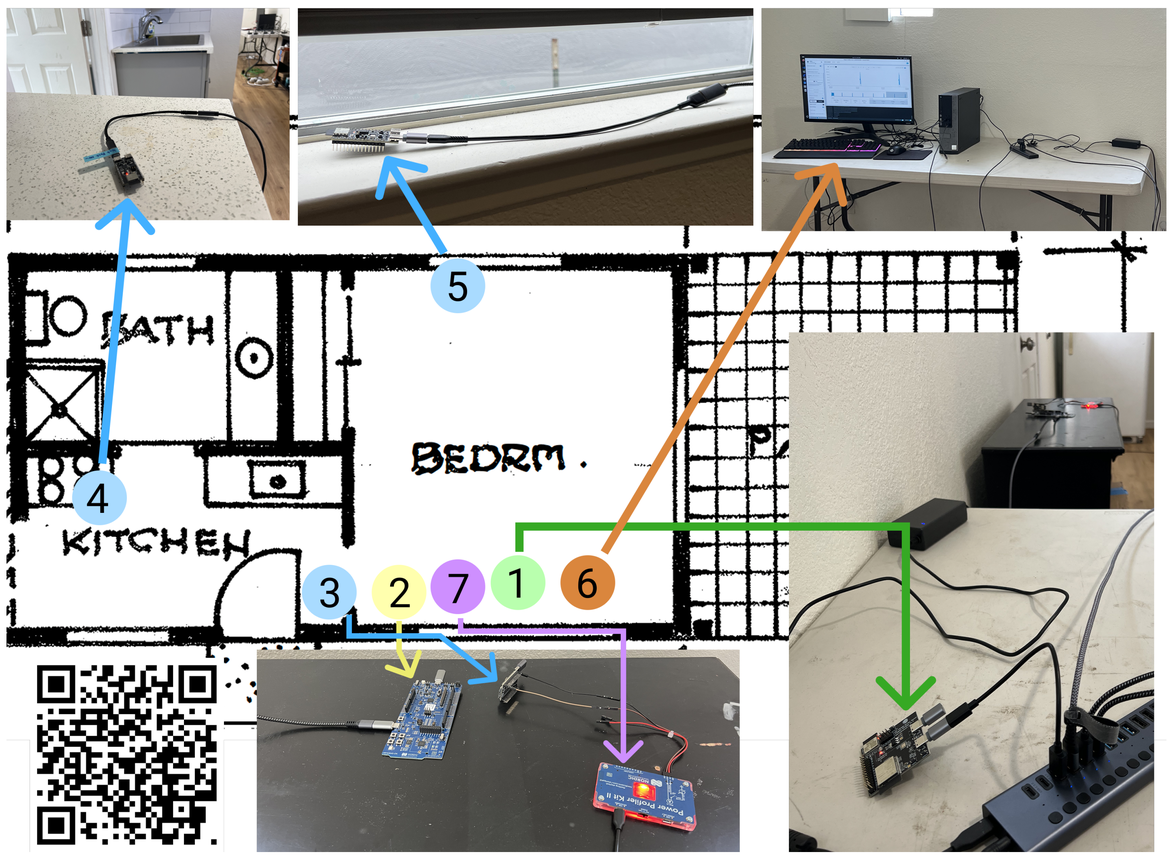
Evaluation

Our comparative study took place in a simulated smart home environment within a single story ADU.

ESP32-H2 devkits operated as the window sensor (5), front door motion sensor (3), and air quality monitor (4). The ESP32 Thread Border Router board (1) functioned as the gateway.

A nRF52840 devkit (2) ran the nRF 802.15.4 sniffer software to capture all in-flight packets. The Nordic Semiconductors Power Profiler II (PPK2) (7) measured the current of the front-door motion sensor in milliamperes (mA) at a rate of 10k samples per second. All data collected by the PPK2 was saved to a workstation (6).

For each experiment, we averaged the instantaneous current measurements of the device in wake state and converted it into milliampere-hours (mAh). Each experiment simulated a year's worth of smart home network activity where 30 seconds represented 1 day.

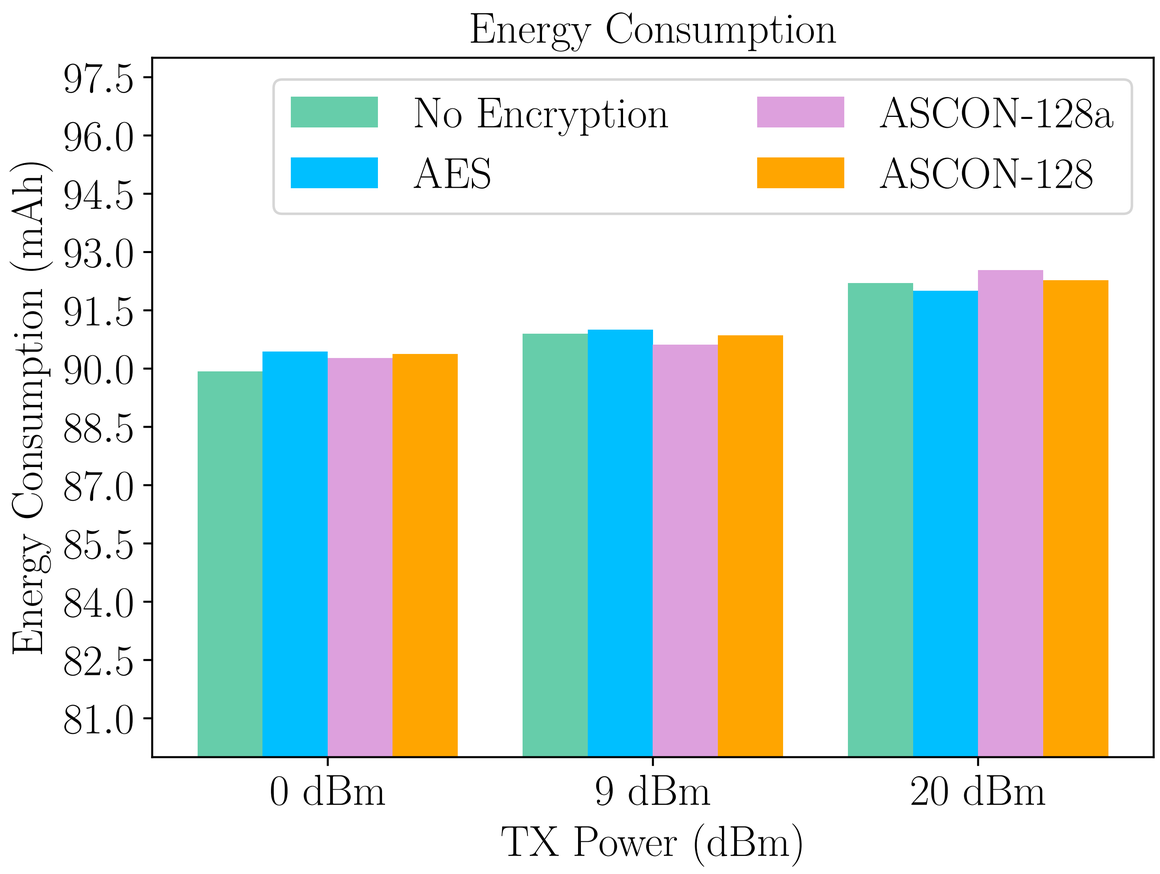


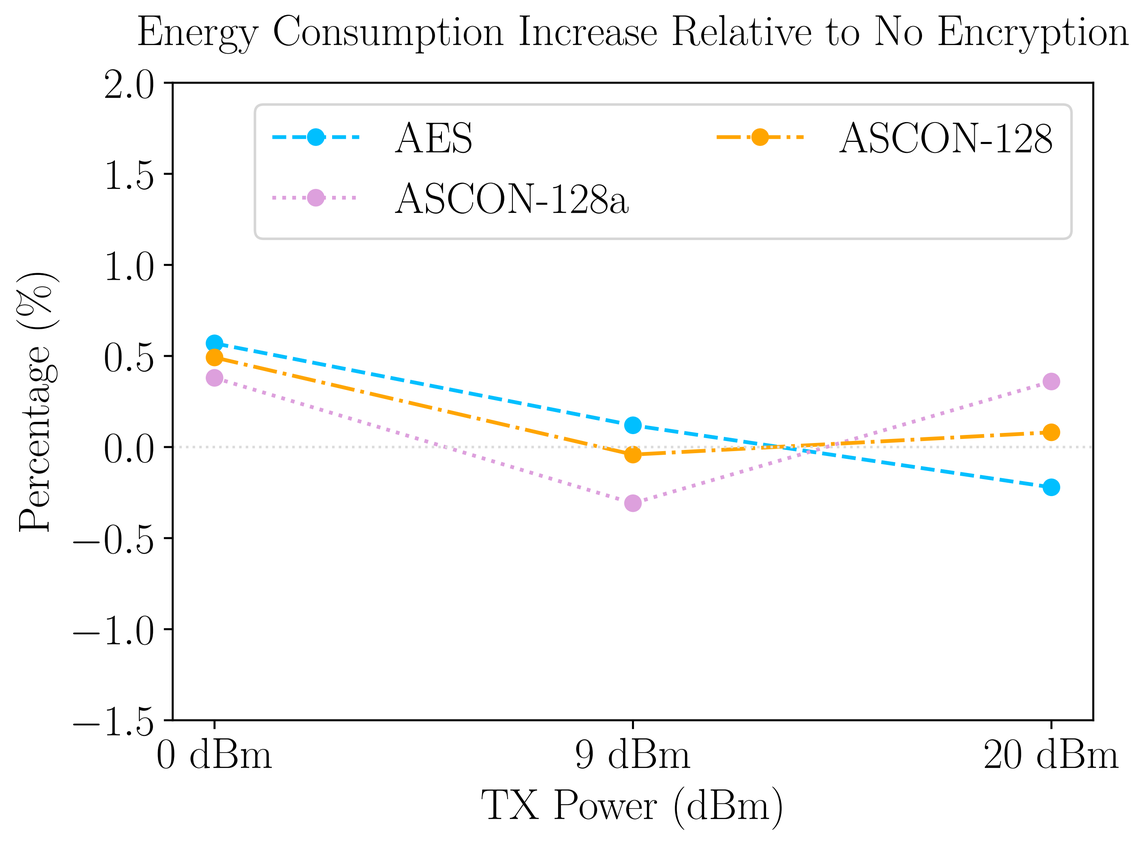
Simulated Network Traffic

Battery Lifetime Report: The SEDs informed the Border Router the status of their battery life once per day (every 30 seconds).

Event Notification: The SEDs informed the Border Router whenever an event has occurred. The front-door motion sensor, window sensor, and air quality monitor detects an event uniformly 36, 10, and 12 times per year, respectively (in each experiment).

Results





Additional Contributions

We also evaluated the Delay, Throughput, and Packet Loss of Full Thread Devices (FTDs), with similarly positive results.

Future Work

Repeating this research using the standardized ASCON AEAD algorithm: Ascon-AEAD128, is left for future work.