Poster Abstract: Comparative Study of Encryption Algorithms in Battery Powered Thread© Networks for Smart Homes

Simeon Tran, David C. Harrison
University of California, Santa Cruz
Santa Cruz, California, USA
{siatran, dcharris}@ucsc.edu

***Abstract*—In response to the security challenges inherent in the Internet of Things (IoT), in 2023, the National Institute of Standards and Technology (NIST) has endorsed ASCON, a cipher suite designed to secure the communications between resource-constrained IoT devices. Thread, a popular wireless mesh protocol designed for smart homes and smart buildings, does not currently support ASCON. We modified OpenThread, the open source implementation of Thread, to support ASCON. Compared to the original version of OpenThread, we show that the energy consumption of battery powered smart home devices are not negatively impacted when OpenThread is secured by ASCON encryption. To the best of our knowledge, we are the first to investigate the potential of ASCON in securing the communications of smart home devices operating under OpenThread.**

I. Introduction

In February 2023, NIST announced its endorsement of the ASCON lightweight encryption scheme for securing resource-constrained IoT devices, and has published official versions of ASCON encryption and hashing in August 2025 [1]. The IEEE Standards Committee is updating 802.15.4 to enable it to be secured by ASCON; the standards proposal to add this encryptions scheme: P802.15.4ae, is expected to be submitted for revisions in December 2026 [2]. Previous research has separately examined the energy consumption of Thread devices [3] and the impacts in power and computation when resource-constrained devices are secured by ASCON AEAD [4, 5]. To our knowledge, there has not been any research yet which has explored the feasibility of ASCON in securing battery powered Thread devices.

For our extended abstract, we describe a comparative study showing that when OpenThread [6] is modified to support ASCON encryption, the energy consumption of battery powered Thread devices is not significantly impacted when compared to using the original version of OpenThread. Such results highlight the feasibility for smart home device manufacturers to follow NIST recommendations in using ASCON AEAD while not having to be concerned about any adverse impacts in the functionality and performance of their devices when doing so. The source code for our modified implementation of OpenThread and the driver code for our experiments is publicly available at: https://github.com/UCSC-ThreadAscon.

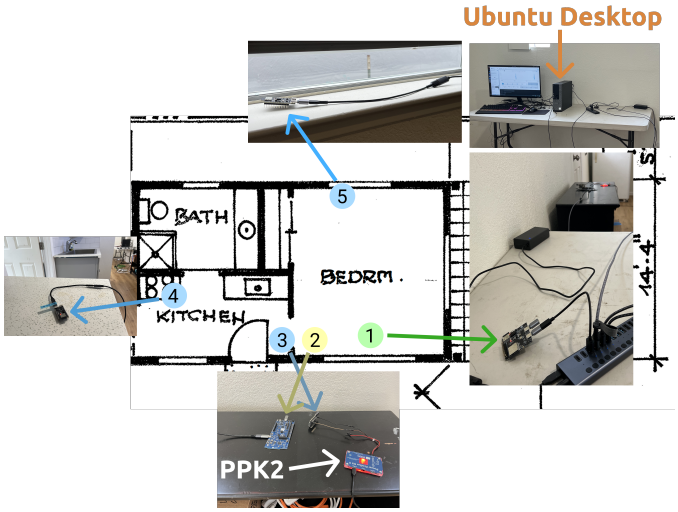

Figure 1. The experimental setup. The green circle labelled 1 corresponds to the location of the Border Router. The yellow circle labelled 2 corresponds to the location of the nRF52840 802.15.4 sniffer. The blue circles labelled 3, 4, and 5, corresponds to the locations of the sensor for the front door, the air quality monitor, and the window sensor, respectively. All data collected by the Power Profiler Kit II (PPK2) was saved to an Ubuntu desktop computer.

II. Evaluation

Our comparative study took place in a simulated smart home environment within a single story ADU. Three ESP32-H2 development kits were programmed to operate as battery powered Sleepy End Devices (SEDs), with each playing the role of a window sensor, front door motion sensor, and air quality monitor. The ESP32 Thread Border Router board functioned as the gateway. A nRF52840 development kit, running the nRF 802.15.4 sniffer software, captured all packets sent by the devices during the experiments.

For each experiment, the independent variables were:

- The encryption algorithm used by OpenThread: ASCON-128a, ASCON-128, AES-CCM (which is built into OpenThread), or no encryption algorithm.
- The TX power used by the devices: 20 dBm, 9 dBm, or 0 dBm.

Our modified implementation of OpenThread supports the use of ASCON-128a, ASCON-128, and plaintext communi-

cations, while we ran the original version of OpenThread when using AES-CCM. The dependent variable was the energy consumption of the front door motion sensor, measured in milliampere-hours (mAh). The Nordic Semiconductors Power Profiler Kit II (PPK2) was used to measure its energy consumption at a rate of 10k samples per second.

Each experiment simulated 365 days, or 1 year's, worth of smart home network activity in a short period of time. The timescale in the experiments were compressed by equating 30 seconds to represent 1 day's worth of smart home network activity; thus, each experiment lasted for $(30 \text{ seconds} \cdot 365 \text{ days})$ seconds $\div$ 60 minutes $= 182.5$ minutes, which we rounded up to 183 minutes.

The SEDs functioned only sent packets in the following two scenarios, both of which were based on the classification of smart home traffic by Betzler et al. [7]:

1) **Scenario 1:** The SEDs sent packets to the border router to report the status of their battery life exactly *once* per day. This corresponds to sending a packet once every 30 seconds the border router in our experiments.
2) **Scenario 2:** The SEDs sent packets informing the border router when an event has occurred. In our experiments, we suppose that the front-door motion sensor, window sensor, and air quality monitor detects an event uniformly 36, 10, and 12 times per year, respectively; each of these are the exact number of event packets that each respective device sends to the border router in each experiment.

III. Results & Discussion

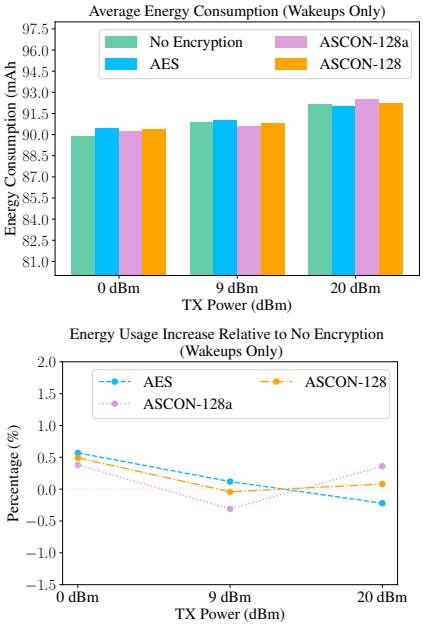

Figure 2. The average energy consumption of the front-door motion sensor. The deep sleep currents are *not* included in the calculations of the averages.

Encryption and decryption only occurs when the device is *on wakeup*; the deep sleep current always remains the same regardless of the encryption algorithm used. Therefore, we only display the average energy consumption of the device when it was awake in Figure 2.

The results show no significant difference in energy consumption when the encryption algorithm was varied. The TX power was the factor that made a noticeable difference in the energy usage of the SED – which is to be expected, as the most power intensive component of a resource-constrained device is its transceiver. Although the results themselves are non-significant, they are nonetheless still important: they entail *no adverse impact* on the battery lifetimes of battery powered Thread smart home devices when secured by ASCON encryption instead of AES-CCM. Therefore, smart home device manufacturers can be confident in securing their devices using ASCON without any noticeable effect on their battery lives.

IV. Conclusion & Future Work

In this extended abstract, we showed that there is no significant adverse impact in the energy consumption of ESP32 Thread Devices running a version of OpenThread modified to replace AES-CCM with ASCON AEAD. This result suggests ASCON AEAD is a viable alternative to AES-CCM in any Thread implementation.

NIST has already standardized the algorithms defined in the ASCON cipher suite [1]. However, the research described in this extended abstract was completed *before* NIST's standardization of ASCON. Instead, we modified our implementation of OpenThread to support a third-party implementation of ASCON: LibAscon [8]. Repeating this research using the official implementations of the standardized ASCON AEAD algorithm is left for future work.

References

[1] M. Sonmez Turan, "Ascon-Based Lightweight Cryptography Standards for Constrained Devices," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-232, 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.pdf

[2] IEEE Standards Committee, "P802.15.4ae: Amendment to IEEE Standard 802.15.4-2020." [Online]. Available: https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/11985

[3] E. Azoidou, Z. Pang, Y. Liu, D. Lan, G. Bag, and S. Gong, "Battery Lifetime Modeling and Validation of Wireless Building Automation Devices in Thread," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 2869–2880, Jul. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8106811/

[4] J. Avery, B. Fraelich, W. Duran, A. Lee, A. Sullivan, Z. Mechalke, M. B. Birrer, S. Dick, and J. Cochran, "Analysis of Practical Application of Lightweight Cryptographic Algorithm ASCON." [Online]. Available: https://csrc.nist.gov/csrc/media/Events/2022/lightweight-cryptography-workshop-2022/documents/papers/analysis-of-practical-application-of-lwc-cryptographic-algorithm-ascon.pdf

[5] M. Nooruddin and D. Valles, "An Advanced IoT Framework for Long Range Connectivity and Secure Data Transmission Leveraging LoRa and ASCON Encryption," in *2023 IEEE World AI IoT Congress (AIIoT)*, Jun. 2023, pp. 0583–0589. [Online]. Available: https://ieeexplore.ieee.org/document/10174401

[6] Google, "OpenThread," Jul. 2023. [Online]. Available: openthread.io

[7] A. Betzler, C. Gomez, I. Demirkol, and J. Paradells, "A Holistic Approach to ZigBee Performance Enhancement for Home Automation Networks," *Sensors*, vol. 14, no. 8, pp. 14 932–14 970, Aug. 2014, number: 8 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1424-8220/14/8/14932

[8] "TheMatjaz/LibAscon," Mar. 2024, original-date: 2020-05-21T17:25:26Z. [Online]. Available: https://github.com/TheMatjaz/LibAscon