

A Frame-Based Architecture for Enhanced Secure IoT Communication with Ascon-128a

The First International Conference on Intelligent Aerial Access and
Applications - IAAA 2025

Huu-Tu Hoang, Duc-Hung Le

The University of Science - VNU, Ho Chi Minh City, Vietnam
Faculty of Electronics and Telecommunications

dd/MM/2025



TABLE OF CONTENTS

- ① Introduction
- ② Proposes Method
- ③ Result and Analysis
- ④ Conclusion and Future Work

1 Introduction

2 Proposes Method

3 Result and Analysis

4 Conclusion and Future Work

MOTIVATION

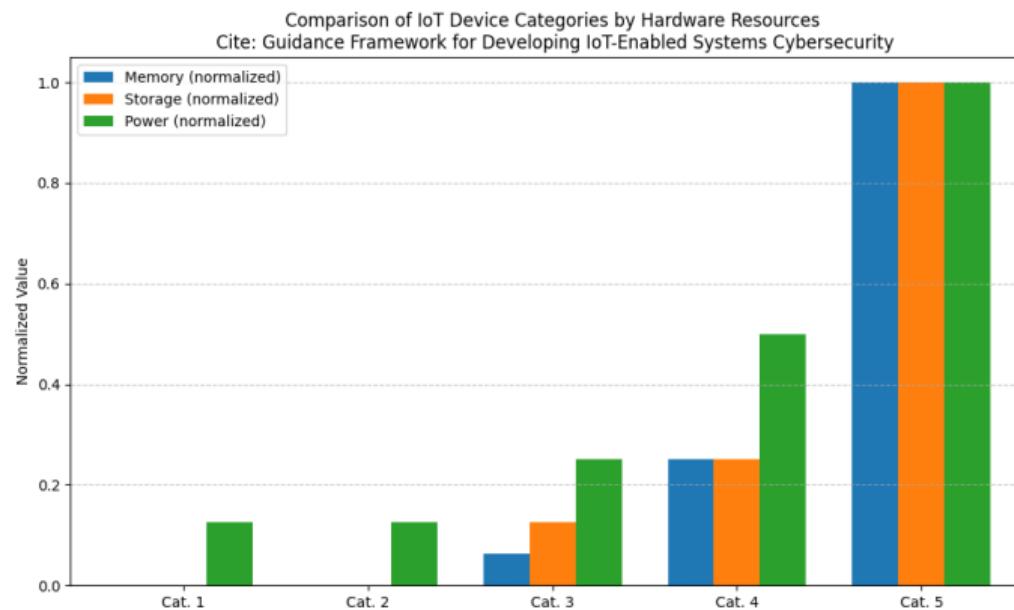
- Most IoT devices operate with constrained computational capabilities and limited resources.

Bảng 1: Classification of IoT devices based on hardware capabilities.

Category	CPU	RAM	Storage	Power	Example
Category 1	8-bit, 16 MHz	\leq 32 KB	Small	\leq 1 W	Arduino Mega
Category 2	32-bit, 80 MHz	32–80 KB	Small	\leq 1 W	NodeMCU ESP-12
Category 3	Single-core, 1 GHz	80 KB–512 MB	\leq 4 GB	1–2 W	Raspberry Pi Zero
Category 4	Quad-core, 1.2 GHz	512 MB–2 GB	\leq 8 GB	2–4 W	Raspberry Pi 3
Category 5	Quad-core, 2 GHz	\geq 8 GB	\geq 32 GB	High	Jetson TX2

MOTIVATION

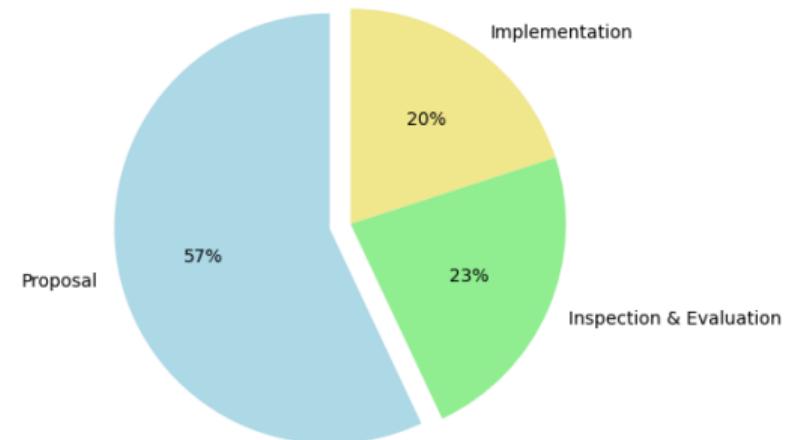
- Most IoT devices operate with constrained computational capabilities and limited resources.



MOTIVATION

- Research on implementing complete IoT architectures remains limited.

Research Work Distribution (2010-2020)
Citation: A decade of research on patterns and architectures for IoT security



Objectives and Contributions

This work aims to develop a complete IoT architecture that fulfills the following goals:

- ① Compatible with a **wide range** of hardware platforms.
- ② Ensures **data integrity** and **confidentiality** during transmission.
- ③ Provides mechanisms to **mitigate common attacks**.
- ④ **Implementation** on real hardware and performance benchmarking.
- ⑤ Can be used as a **reference** framework for future IoT implementations.

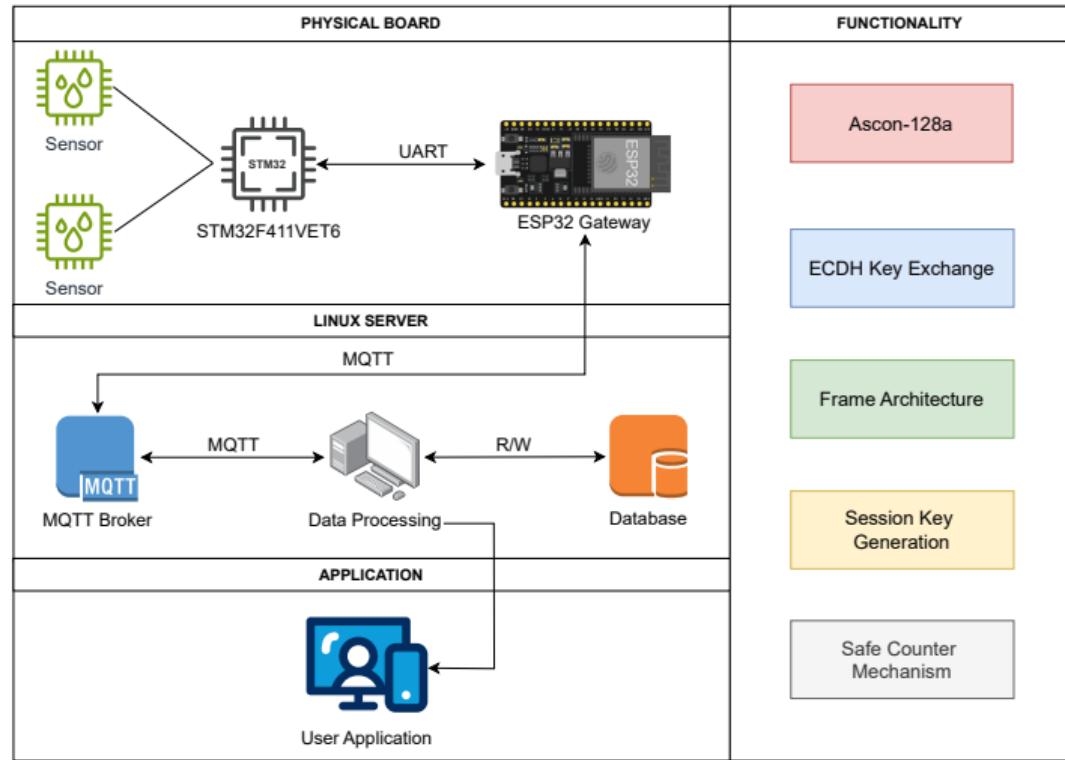
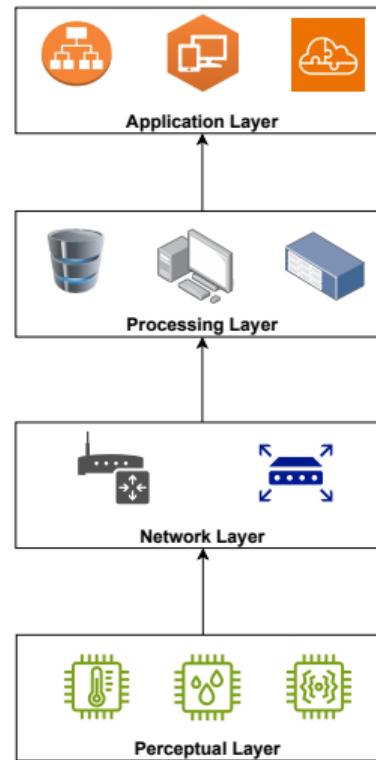
1 Introduction

2 Proposes Method

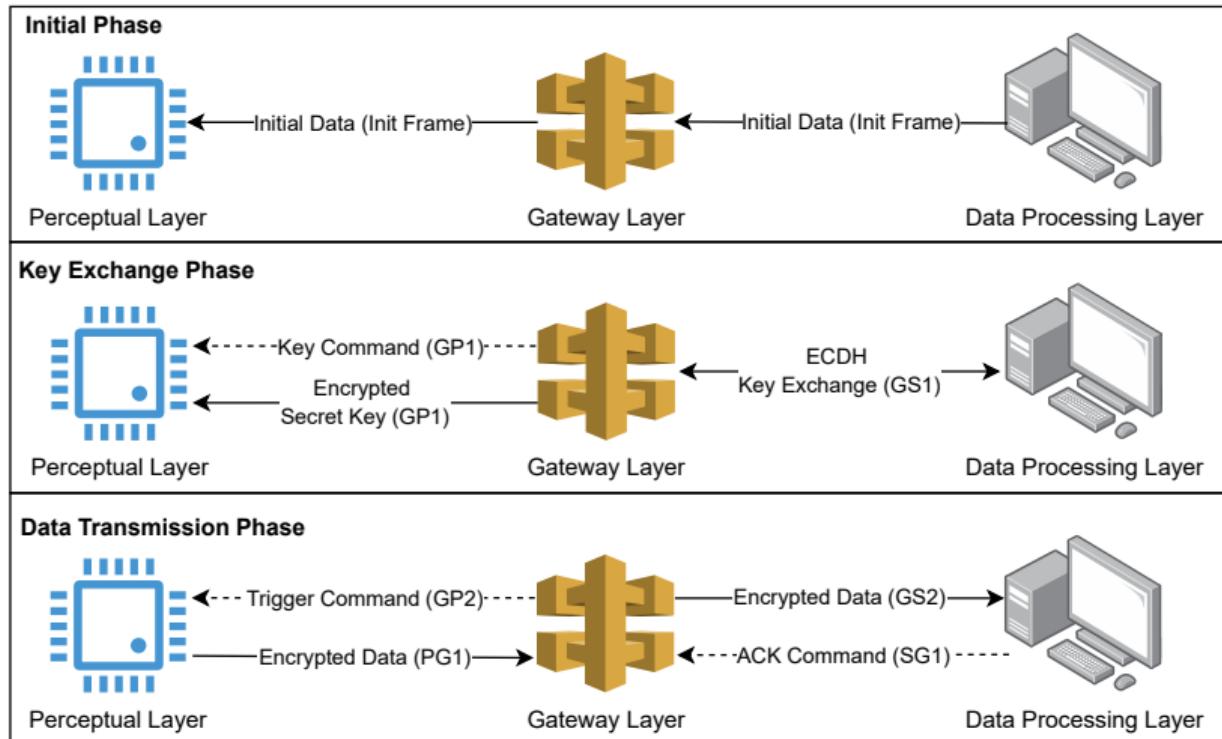
3 Result and Analysis

4 Conclusion and Future Work

SYSTEM ARCHITECTURE



COMMUNICATION MODEL



FRAME ARCHITECTURE

Initial Frame

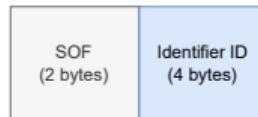


Perceptual to Gateway Frame

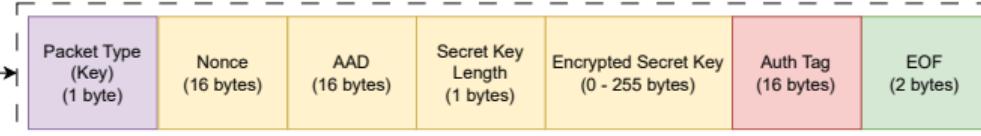
Frame for transmitting encrypted data (PG1)



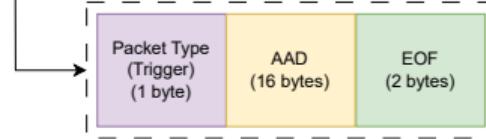
Gateway to Perceptual Frame



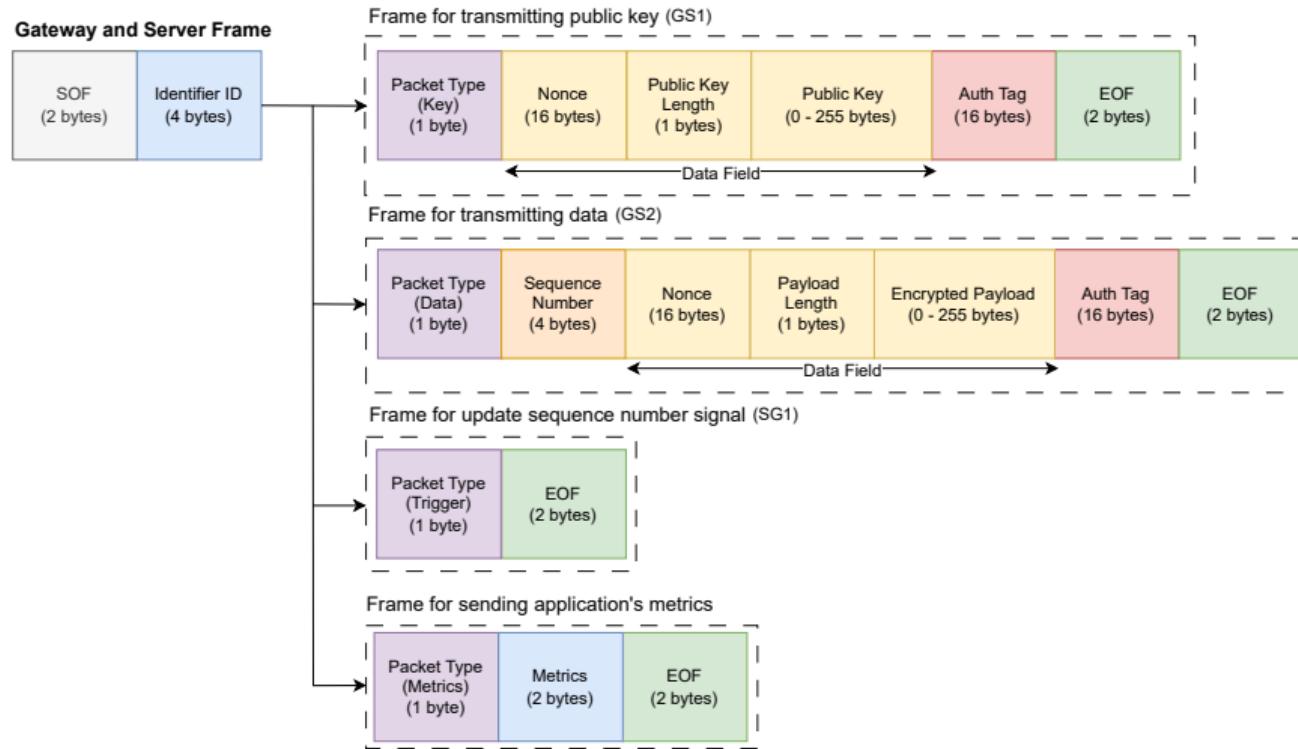
Frame for transmitting encrypted secret key (GP1)



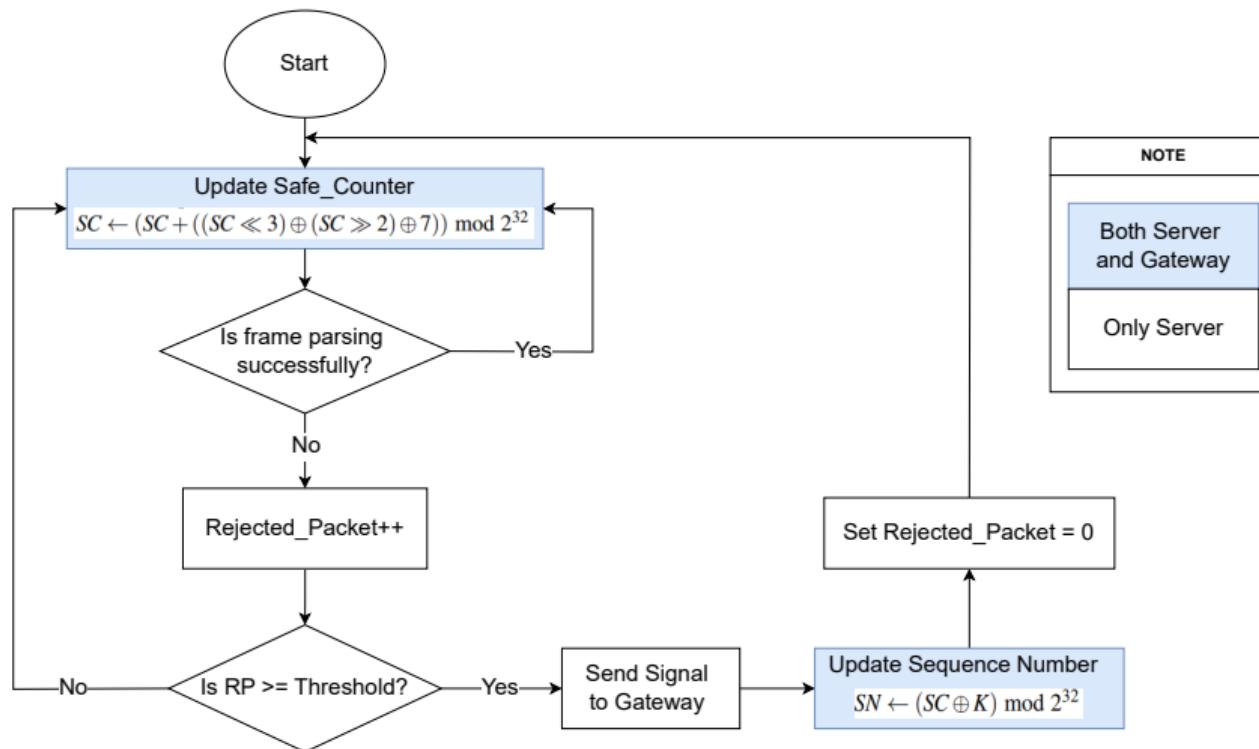
Frame for trigger signal (GP2)



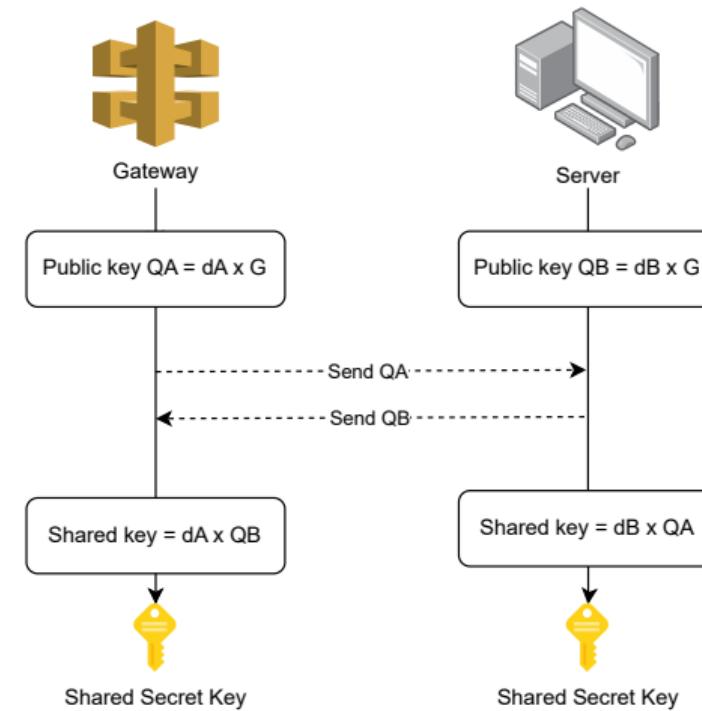
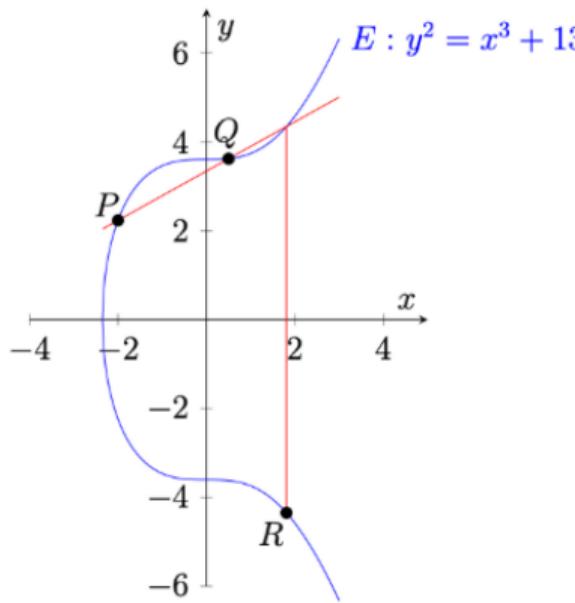
FRAME ARCHITECTURE



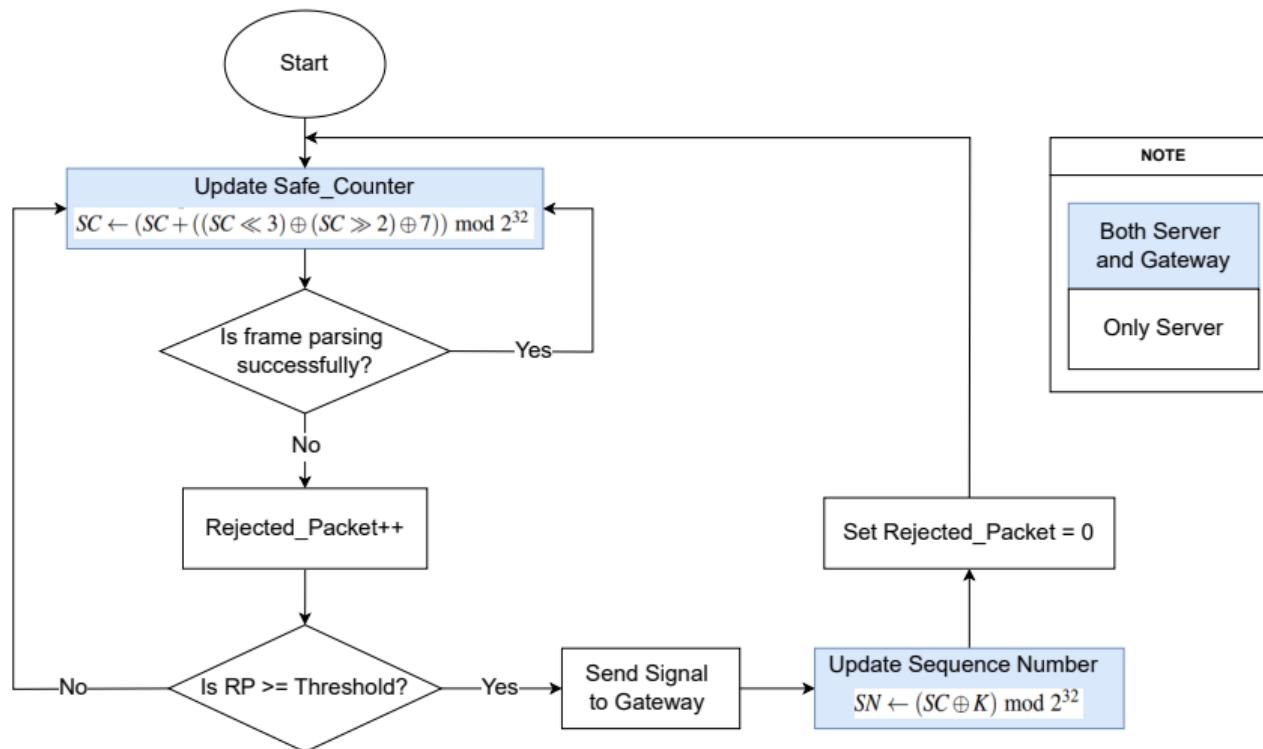
FRAME PARSING PROCESS



ELLIPTIC CURVE DIFFIE-HELLMAN KEY EXCHANGE



SAFE COUNTER MECHANISM



1 Introduction

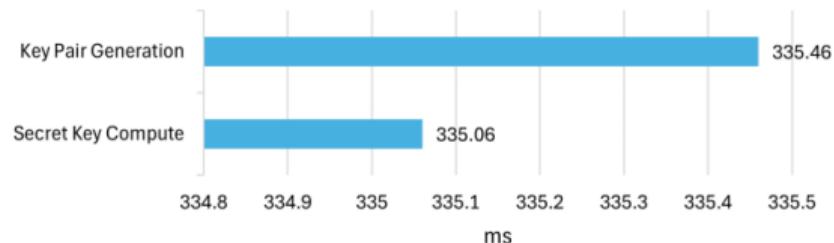
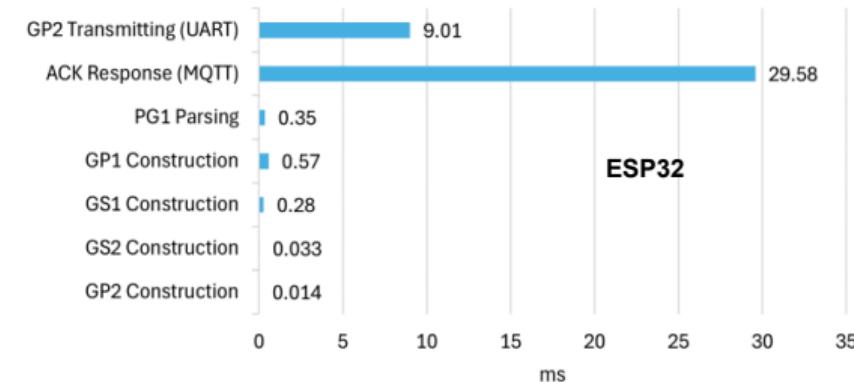
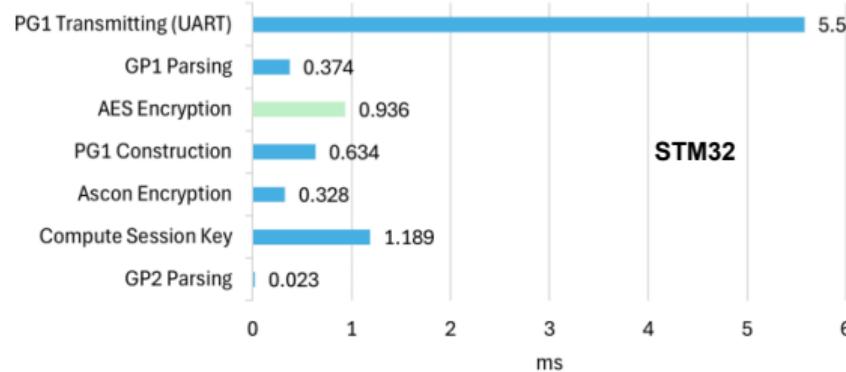
2 Proposes Method

3 Result and Analysis

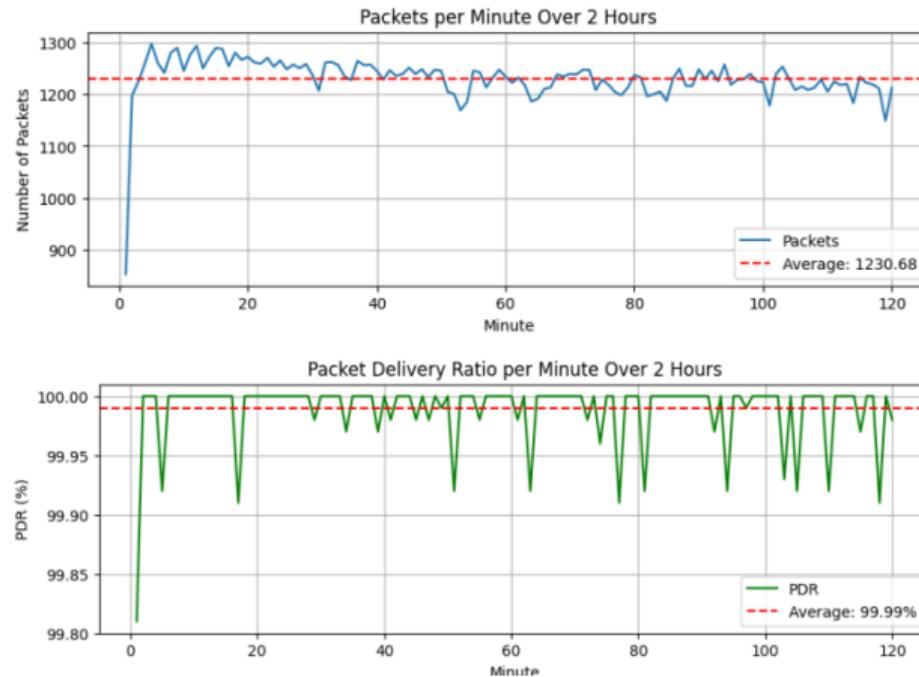
4 Conclusion and Future Work

TIME EXECUTIONS

Thời gian truyền trung bình đạt 51.08 ms.

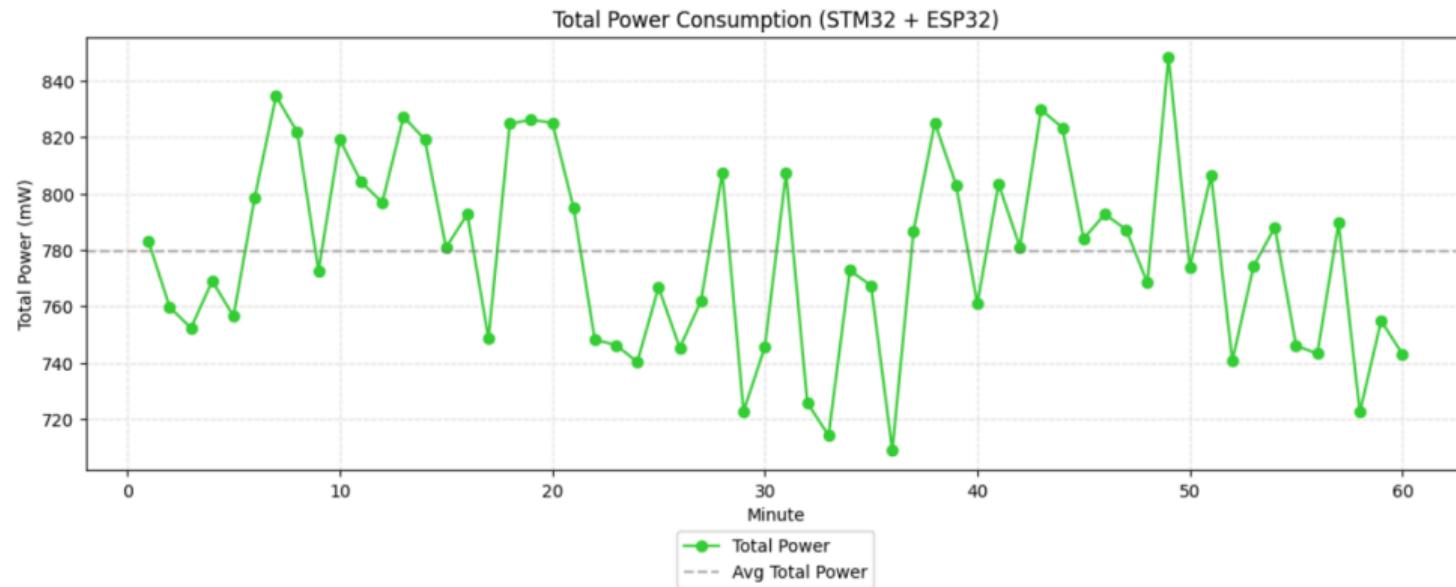


PACKET DELIVERY RATIO



POWER CONSUMPTION

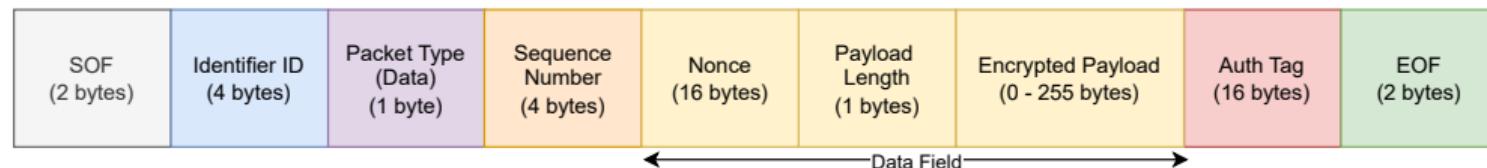
Công suất tiêu thụ trung bình là 779.43 mW.



PAYLOAD EFFICIENCY

Dánh giá dựa trên khung truyền GS2 và kích thước dữ liệu là 3 bytes.

Frame for transmitting data (GS2)



Với 3 bytes dữ liệu, tổng kích thước khung truyền là 49 bytes.

⇒ Hiệu suất tải dữ liệu là $\frac{3}{49} \approx 6.12\%$

PAYLOAD EFFICIENCY

Bảng 2: Hiệu suất tải với các kích thước tải khác nhau

Payload Length	Total Frame Size	Efficiency
3 bytes	49 bytes	6.12%
10 bytes	56 bytes	17.85%
20 bytes	66 bytes	30.30%
50 bytes	96 bytes	52.08%

⇒ Payload càng lớn thì hiệu suất tải dữ liệu càng cao

- 1 Introduction
- 2 Proposes Method
- 3 Result and Analysis
- 4 Conclusion and Future Work

ACHIEVEMENTS

Các kỹ thuật được triển khai thành công trên phần cứng và máy chủ.

- ① Các kỹ thuật giao tiếp được triển khai theo đúng yêu cầu đặt ra.
- ② Xây dựng kiến trúc khung truyền linh hoạt bao gồm cấu trúc và phân giải.
- ③ Kỹ thuật trao đổi khóa trên đường cong Elliptic.
- ④ Kỹ thuật tọa khóa phiên dựa trên hàm băm Ascon-Hash.
- ⑤ Mật mã hóa nhẹ Ascon-128a.
- ⑥ Cơ chế bảo mật *Safe Counter*.

DISADVANTAGES

Các kỹ thuật được triển khai thành công trên phần cứng và máy chủ.

- ① Các kỹ thuật giao tiếp được triển khai theo đúng yêu cầu đặt ra.
- ② Xây dựng kiến trúc khung truyền linh hoạt bao gồm cấu trúc và phân giải.
- ③ Kỹ thuật trao đổi khóa trên đường cong Elliptic.
- ④ Kỹ thuật tọa khóa phiên dựa trên hàm băm Ascon-Hash.
- ⑤ Mật mã hóa nhẹ Ascon-128a.
- ⑥ Cơ chế bảo mật *Safe Counter*.

FUTURE WORK

Các kỹ thuật được triển khai thành công trên phần cứng và máy chủ.

- ① Các kỹ thuật giao tiếp được triển khai theo đúng yêu cầu đặt ra.
- ② Xây dựng kiến trúc khung truyền linh hoạt bao gồm cấu trúc và phân giải.
- ③ Kỹ thuật trao đổi khóa trên đường cong Elliptic.
- ④ Kỹ thuật tọa khóa phiên dựa trên hàm băm Ascon-Hash.
- ⑤ Mật mã hóa nhẹ Ascon-128a.
- ⑥ Cơ chế bảo mật *Safe Counter*.

Thank you for your attention!