**PROJECT No. ISNE P706-1/2568**

# Design and Implementation of a Lightweight Secure Communication System for IoT Using LoRa and MicroPython


**Ritthanupahp Sitthananun 650615030**
**Piyawut Buncharoen 650615024**
**Siripa Aungwattana 650615032**


**A Report Submitted in Partial Fulfillment of Project Survey Course**
**as Required by the Degree of Bachelor of Engineering**

**Department of Computer Engineering**
**Faculty of Engineering**
**Chiang Mai University**

**2025**

| | |
|---|---|
| Project Title | : Design and Implementation of a Lightweight Secure Communication System for IoT Using LoRa and MicroPython |
| Name | : Ritthanupahp Sitthananun 650615030 |
| | Piyawut Buncharoen 650615024 |
| | Siripa Aungwattana 650615032 |
| Department | : Computer Engineering |
| Project Advisor | : Asst. Prof. Kampol Woradit, Ph.D. |
| Degree | : Bachelor of Engineering |
| Program | : Information Systems and Network Engineering |
| Academic Year | : 2025 |

---

The Department of Computer Engineering, Faculty of Engineering, Chiang Mai University has approved this project to be part of the degree of Bachelor of Engineering (Information Systems and Network Engineering)

..... Department chair
(Assoc. Prof. Santi Phithakkitnukoon, Ph.D.)

Project examination committee:

..... Main advisor / Chair
(Asst. Prof. Kampol Woradit, Ph.D.)

..... Committee member
(Assoc. Prof. Anya Apavatjrut, Ph.D.)

..... Committee member
(Sasin Janpuangtong, Ph.D.)

# Contents

# Chapter 1
# Introduction

## 1.1 Project rationale

LoRa (Long Range) is a low-power wireless communication technology widely used in Internet of Things (IoT) applications such as environmental monitoring, infrastructure systems, and smart home appliances. Despite its advantages, LoRa lacks strong built-in security mechanisms. This leaves signals exposed to attacks such as eavesdropping, reply attacks , and message injections [1], [2]. Traditional encryption methods can mitigate these risks but are often too resource-intensive for low-power devices like the ESP32.

## 1.2 Objectives

To address this challenge, this project avoids static, pre-stored keys and instead generates encryption keys that are dynamic and constantly changing. RSSI (Received Signal Strength Indicator) values are used as the basis for key generation. Since RSSI values are unique between two devices and vary with environmental conditions, the resulting keys are never fixed. Unlike a static key, RSSI-based keys change over time, making them more difficult for an attacker to predict or reuse.

This project presents a lightweight secure communication framework for IoT systems using LoRa and MicroPython, focusing on encryption and dynamic key management. Session keys are updated using RSSI values. Both devices share a predefined keyword and an RSSI interval for adjustment. The communication process begins with the sender transmitting a verification message while the receiver measures the RSSI and iteratively adjusts its interpretation within the agreed interval until the message is correctly decrypted and the keyword matches. This ensures that both devices converge on the same session key despite natural fluctuations in signal strength. Furthermore, by using RSSI values with two-decimal precision and combining measurements across multiple LoRa channels, the system significantly increases resistance to interception and eavesdropping. Overall, the framework provides a practical balance between security and performance for securing IoT communication [3],[4].

### 1.3 Project scope

#### 1.3.1 Hardware scope

#### 1.3.2 Software scope

### 1.4 Expected outcomes

### 1.5 Technology and tools

#### 1.5.1 Hardware technology

#### 1.5.2 Software technology

### 1.6 Project plan

### 1.7 Roles and responsibilities

### 1.8 Impacts of this project on society, health, safety, legal, and cultural issues

# Chapter 2
# Background Knowledge and Theory

## 2.1 Internet of Things (IoT)

The Internet of Things (IoT) refers to a network of interconnected devices that can sense, process, and exchange data with minimal human intervention. These devices are widely deployed in applications such as smart homes, healthcare monitoring, environmental sensing, transportation systems, and industrial automation. While IoT enables efficiency and automation, it also introduces security challenges. Many IoT devices are resource-constrained in terms of processing power, memory, and energy supply, making it difficult to implement traditional, computation-heavy cryptographic techniques. As a result, IoT networks are often vulnerable to attacks such as eavesdropping, replay, and message injection.

## 2.2 LoRa Technology

LoRa (Long Range) is a low-power wide-area network (LPWAN) communication technology that enables devices to transmit data over several kilometers while consuming minimal energy. This makes it suitable for IoT applications where devices must operate on battery power for extended periods. LoRa achieves long-distance communication using Chirp Spread Spectrum (CSS) modulation, which provides robustness against noise and interference. However, LoRa's primary limitation is its lack of built-in security mechanisms. The physical layer itself does not provide strong confidentiality or integrity protection. While LoRaWAN (the higher-layer protocol) introduces some security features, lightweight LoRa implementations—such as those used in simple ESP32 + LoRa projects—are highly vulnerable to interception, spoofing, and key extraction if insecure practices (e.g., hardcoded keys) are used.

## 2.3 Received Signal Strength Indicator (RSSI)

The Received Signal Strength Indicator (RSSI) measures the power level of a received wireless signal, typically expressed in decibels relative to one milliwatt (dBm). In LoRa systems, RSSI is automatically measured at the receiver whenever a packet is received. Normally, RSSI is used to evaluate link quality or assist in adaptive communication strategies. In the context of security, RSSI can also be leveraged as a source of entropy for key generation. Since RSSI values fluctuate depending on distance, obstacles, interference, and environmental conditions, they are inherently dynamic and difficult for an attacker to predict without being physically co-located in the communication channel. By using RSSI values as a basis for session key generation, IoT devices can avoid reliance on static, pre-shared keys that are easy to compromise.

## 2.4 Lightweight Cryptography

Lightweight cryptography refers to cryptographic techniques designed specifically for devices with limited computational and memory resources. Unlike traditional algorithms such as AES-256 or RSA, which require significant processing power, lightweight algorithms are optimized for efficiency while maintaining an acceptable level of security. Typical strategies include reducing key sizes, minimizing memory overhead, or designing algorithms tailored for 8-bit or 32-bit microcontrollers. For IoT applications using devices like the ESP32, lightweight cryptography is essential to balance security with system performance. The challenge is to implement schemes that protect data confidentiality and integrity without exceeding constraints such as 10 KB of program memory or 300 bytes of RAM.

## 2.5 Key Management in IoT

Key management is one of the most critical aspects of securing IoT networks. Traditional approaches rely on pre-shared static keys, which pose significant risks: once an attacker obtains the key, they can decrypt all subsequent communications. Dynamic key management schemes provide stronger protection by regularly updating session keys. One promising approach is to derive session keys from physical-layer metrics, such as RSSI. Since each device independently measures RSSI during communication, keys can be generated locally without transmitting sensitive information over the air. To ensure synchronization, both devices agree on an adjustment interval and use a shared keyword for verification. This method significantly reduces the risk of interception and makes it difficult for attackers to reuse keys, thereby enhancing overall IoT security.

### 2.5.1 Subsection heading goes here

Subsection 1 text

#### Subsubsection 1 heading goes here

Subsubsection 1 text

#### Subsubsection 2 heading goes here

Subsubsection 2 text

## 2.6 Third section

Section 3 text. The dielectric constant at the air-metal interface determines the resonance shift as absorption or capture occurs is shown in Equation (2.1):

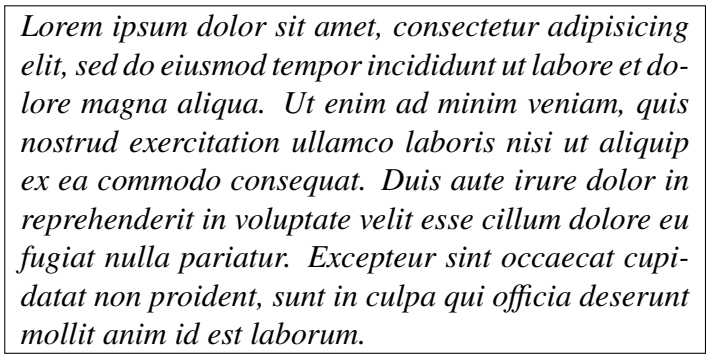


Figure 2.1: This figure is a sample containing lorem ipsum, showing you how you can include figures and glossary in your report. You can specify a shorter caption that will appear in the List of Figures.

$$k_1 = \frac{\omega}{c(1/\varepsilon_m + 1/\varepsilon_i)^{1/2}} = k_2 = \frac{\omega \sin(\theta)\varepsilon_{air}^{1/2}}{c} \tag{2.1}$$

where $\omega$ is the frequency of the plasmon, $c$ is the speed of light, $\varepsilon_m$ is the dielectric constant of the metal, $\varepsilon_i$ is the dielectric constant of neighboring insulator, and $\varepsilon_{air}$ is the dielectric constant of air.

### 2.7 About using figures in your report

Using `\label` and `\ref` commands allows us to refer to figures easily. If we can refer to Figures 3.1 and 2.1 by name in the LaTeX source code, then we will not need to update the code that refers to it even if the placement or ordering of the figures changes.

*Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.*

*Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.*

*Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor*

Table 2.1: Sample landscape table

| Year | A | B |
|---|---|---|
| 1989 | 12 | 23 |
| 1990 | 4 | 9 |
| 1991 | 3 | 6 |

*in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.*

*Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.*

*Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.*

### 2.8 Overfull hbox

When the `semifinal` option is passed to the `cpecmu` document class, any line that is longer than the line width, i.e., an overfull hbox, will be highlighted with a black solid rule:

juxtaposition

### 2.9 ISNE knowledge used, applied, or integrated in this project

### 2.10 Extracurricular knowledge used, applied, or integrated in this project

# Chapter 3
# Project Structure

## 3.1 Alice in Wonderland

### 3.1.1 The Black Kitten

One thing was certain, that the WHITE kitten had had nothing to do with it:—it was the black kitten's fault entirely [1]. For the white kitten had been having its face washed by the old cat for the last quarter of an hour (and bearing it pretty well, considering); so you see that it COULDN'T have had any hand in the mischief.

The way Dinah washed her children's faces was this: first she held the poor thing down by its ear with one paw, and then with the other paw she rubbed its face all over, the wrong way, beginning at the nose: and just now, as I said, she was hard at work on the white kitten, which was lying quite still and trying to purr—no doubt feeling that it was all meant for its good.

But the black kitten had been finished with earlier in the afternoon, and so, while Alice was sitting curled up in a corner of the great arm-chair, half talking to herself and half asleep, the kitten had been having a grand game of romps with the ball of worsted Alice had been trying to wind up, and had been rolling it up and down till it had all come undone again; and there it was, spread over the hearth-rug, all knots and tangles, with the kitten running after its own tail in the middle.

### 3.1.2 The Reproach

'Oh, you wicked little thing!' cried Alice, catching up the kitten, and giving it a little kiss to make it understand that it was in disgrace. 'Really, Dinah ought to have taught you better manners! You OUGHT, Dinah, you know you ought!' she added, looking reproachfully at the old cat, and speaking in as cross a voice as she could manage—and then she scrambled back into the arm-chair, taking the kitten and the worsted with her, and began winding up the

Figure 3.1: The Walrus and the Carpenter

ball again. But she didn't get on very fast, as she was talking all the time, sometimes to the kitten, and sometimes to herself. Kitty sat very demurely on her knee, pretending to watch the progress of the winding, and now and then putting out one paw and gently touching the ball, as if it would be glad to help, if it might.

'Do you know what to-morrow is, Kitty?' Alice began. 'You'd have guessed if you'd been up in the window with me—only Dinah was making you tidy, so you couldn't. I was watching the boys getting in stick for the bonfire—and it wants plenty of sticks, Kitty! Only it got so cold, and it snowed so, they had to leave off. Never mind, Kitty, we'll go and see the bonfire to-morrow.' Here Alice wound two or three turns of the worsted round the kitten's neck, just to see how it would look: this led to a scramble, in which the ball rolled down upon the floor, and yards and yards of it got unwound again.

'Do you know, I was so angry, Kitty,' Alice went on as soon as they were comfortably settled again, 'when I saw all the mischief you had been doing, I was very nearly opening the window, and putting you out into the snow! And you'd have deserved it, you little mischievous darling! What have you got to say for yourself? Now don't interrupt me!' she went on, holding up one finger. 'I'm going to tell you all your faults. Number one: you squeaked twice while Dinah was washing your face this morning. Now you can't deny it, Kitty: I heard you! What that you say?' (pretending that the kitten was speaking.) 'Her paw went into your eye? Well, that's YOUR fault, for keeping your eyes open—if you'd shut them tight up, it wouldn't have happened. Now don't make any more excuses, but listen! Number two: you pulled Snowdrop away by the tail just as I had put down the saucer of milk before her! What, you were thirsty, were you?

# Chapter 4
# System Evaluation

## References

[1] Lewis Carroll. *Alice's Adventures in Wonderland*. George MacDonald, 1865.