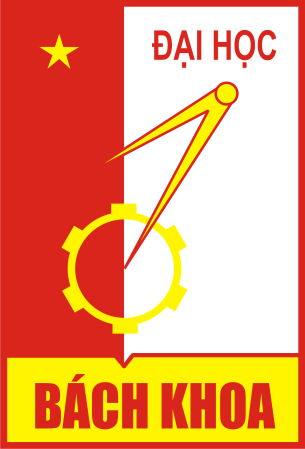
**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**TRƯỜNG ĐIỆN - ĐIỆN TỬ**

**KHOA TỰ ĐỘNG HÓA**



**BÁO CÁO ĐỒ ÁN MÔN HỌC MẠNG CẢM BIẾN KHÔNG DÂY**

**Đề tài: Giám sát nhiệt độ môi trường trong các điều kiện**

Giảng viên hướng dẫn: Th.S Đào Đức Thịnh

Danh sách thành viên nhóm 3:

|  |  |
| --- | --- |
| Họ và tên | MSSV |
| 1. Ngô Đức Dũng | 20202345 |
| 1. Hoàng Minh Khánh | 20181548 |
| 1. Bùi Thanh Tùng | 20202563 |

Hà Nội, 1/2024

Contents

[GIỚI THIỆU ĐỀ TÀI 2](#_Toc127971938)

[CHƯƠNG 1: TỔ CHỨC THỰC HIỆN 1](#_Toc127971939)

[**I.** **Yêu cầu của dự án** 1](#_Toc127971940)

[**II.** **Giới thiệu thành viên dự án** 2](#_Toc127971941)

[**III.** **Kế hoạch thực hiện của dự án** 2](#_Toc127971942)

[**1.** **Kế hoạch thực hiện chung của dự án** 2](#_Toc127971943)

[**2.** **Kế hoạch và nội dung thực hiện của từng thành viên** 2](#_Toc127971944)

[**IV.** **Đánh giá tỷ lệ đóng góp của từng thành viên** 6](#_Toc127971945)

[CHƯƠNG 2: NỘI DUNG THỰC HIỆN 7](#_Toc127971946)

[**I.** **Phân tích các yêu cầu của dự án** 7](#_Toc127971947)

[**II.** **Tìm hiểu các nghiên cứu, dự án liên quan** 7](#_Toc127971948)

[III. Lựa chọn giải pháp và lên phương án thiết kế 8](#_Toc127971949)

[**1.** **Lựa chọn giải pháp** 8](#_Toc127971950)

[**2.** **Tìm hiểu công nghệ sử dụng** 12](#_Toc127971951)

[**3.** **Thử nghiệm và đánh giá và hoàn thiện sản phẩm** 35](#_Toc127971952)

[**4.** **Kết luận và hướng phát triển** 42](#_Toc127971954)

# GIỚI THIỆU ĐỀ TÀI

Trong quá trình học môn Mạng Cảm Biến Không Dây, nhóm chúng em đã tiếp cận và nghiên cứu về các công nghệ không dây đang được ứng dụng mạnh mẽ trong lĩnh vực Internet of Things (IoT). Chúng em cũng đã tìm hiểu về các yêu cầu và yếu tố quan trọng để xây dựng một mô hình mạng không dây. Được hưởng lợi từ cách mạng công nghiệp 4.0, nhiều cơ hội mới mở ra, đặc biệt là trong lĩnh vực công nghiệp. Các ứng dụng như vườn thông minh, giám sát độ bụi và nhiệt độ đã trở nên phổ biến. Tuy nhiên, chúng em đã nhận thức được nhiều thách thức, bao gồm vấn đề bảo mật, đồng bộ hóa dữ liệu, và khả năng kiểm soát các tham số môi trường.

Trong báo cáo của chúng tôi, chúng em tập trung vào việc xây dựng một mạng cảm biến không dây sử dụng công nghệ LoRa để đo lường nhiệt độ trong một khu vực cụ thể. Chúng tôi đã nghiên cứu một cách tổng quan về các công nghệ và mô hình mạng cảm biến không dây phổ biến hiện nay. Qua đó, chúng em đã lựa chọn các loại cảm biến và công nghệ phù hợp để tích hợp vào mô hình mạng, xây dựng một mạng cảm biến thử nghiệm để đánh giá tính khả thi của giải pháp.

Trong quá trình triển khai, chúng em đã đặc biệt chú ý đến các khía cạnh như hiệu suất, độ tin cậy và khả năng mở rộng của mạng. Những thông tin này đã giúp chúng em hiểu rõ hơn về ưu và nhược điểm của mô hình mạng cảm biến không dây của mình. Nhìn chung, dự án của chúng em không chỉ tập trung vào việc áp dụng kiến thức lý thuyết từ môn học mà còn đặt ra những thách thức thực tế trong triển khai một hệ thống cảm biến không dây cho môi trường công nghiệp 4.0.

Ngoài ra thì chúng em cũng tìm cách lưu trữ và hiển thị dữ liệu một cách trực quan qua phần mềm máy tính và qua một server để có thể dễ theo dõi cũng như đưa ra cảnh báo khi cần thiết để có biện pháp thay đổi nhiệt độ kịp thời.

**CHƯƠNG 1: TỔ CHỨC THỰC HIỆN**

1. **Yêu cầu của dự án**

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | **Phương pháp thực hiện** | **Mức độ ưu tiên** |
| - Dải đo: 25oC ÷ 150oC  - Độ chính xác: 1oC  - Độ phân giải hiển thị: 0.1oC | Thiết kế linh kiện đo nhiệt độ phù hợp(digital, analog) | 1 |
| Nguồn pin, thời gian hoạt động của thiết bị là 4h (nâng cao: 8h). Pin có thể sạc trực tiếp trên máy hoặc tháo ra ngoài | Dùng pin Li-Po dung lượng khoảng 2100mAh | 1 |
| - Kích thước (dự kiến): 70x50x100 mm (kiểu trụ để dễ lắp vào các thiết bị giám sát)  - Trọng lượng (dự kiến): <150g. | Vẽ mạch PCB kết nối hệ thống và lắp pin | 1 |
| - Thời gian đo một mẫu : <20s. (nâng cao < 5s) | Thời gian đo khoảng 5s | 1 |
| - Kết nối máy tính: RF Khoảng cách truyền trong phạm vi 20m từ hệ thống đo đến trạm thu RF có nối nguồn và mạng | Sử dụng công nghệ LoRa truyền thông tin các node cảm biến đến gateway và WiFi để đưa data lên server | 2 |
| Quản lý tối thiểu cho 11 thiết bị đo. (nâng cao: phương án mở rộng số thiết bị với khoảng cách từ thiết bị đến trạm tiếp nhận có thể lên tới 100m) | Cấu trúc hình sao, gồm 11 thiết bị với 1 gateway và 10 node  Phát hiện được các node thêm và thoát khỏi mạng | 2 |
| - Phần mềm máy tính: thu thập giá trị đo từ thiết bị đo, quản lý dữ liệu, xuất báo cáo dạng excel, giao diện theo mẫu thống nhất. | Hiển thị thông qua 1 webserver thông qua MQTT | 2 |
| OTA (nâng cao) | Chưa hoàn thành cho tới 20/1, sẽ cố gắng hoàn thành vào ngày 2/2 | 3 |

1. **Giới thiệu thành viên dự án**

|  |  |
| --- | --- |
|  | * Họ và tên: Hoàng Minh Khánh * MSSV: 20181548 * Phụ trách công việc:   - Thiết kế phần cứng dựa trên các task phải làm của sản phẩm. Thiết kế mạch PCB |
|  | * Họ và tên: Bùi thanh Tùng * MSSV: 20202563 * Phụ trách công việc: * Chuyển giao tín hiệu từ gateway lên websever(thingboard) * Hỗ trợ thiết kế phần cứng |
|  | * Họ và tên: Ngô Đức Dũng * MSSV: 20202345 * Phụ trách công việc:   - Tìm hiểu về cảm biến, xây dựng code đọc cảm biến, LoRa  - Thiết kế dashboard hiển thị web |

1. **Kế hoạch thực hiện của dự án**
   1. **Kế hoạch thực hiện chung của dự án**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nội dung** | **Kết quả cần đạt** | **Thời gian (tuần)** | **Ghi chú** |
| Tìm hiểu, phân tích nội dung bài toán | Phân tích các yêu cầu của dự án | 1-5 |  |
| Tìm hiểu các dự án liên quan | Lựa chọn công nghệ truyền thông, kiến trúc mạng, module, … phù hợp | 5-6 |  |
| Lên phương án sơ bộ | Sơ đồ khối chức năng, yêu cầu,…  Tính toán công suất  Lựa chọn linh kiện | 6-9 |  |
| Thực hiện dự án | Thiết kế mạch PCB | 8-9 |  |
| Thiết kế phần mềm | 10-13 |  |
| Kết nối phần mềm trên máy tính | 10-13 |  |
| Thử nghiệm, hiệu chỉnh | So sánh kết quả thu được so với yêu cầu đặt ra | 14-15 |  |
| Nộp dự án | Quay video, hoàn thành báo cáo và slide | 17 |  |

* 1. **Kế hoạch và nội dung thực hiện của từng thành viên**

**Bùi Thanh Tùng - 20202563**

|  |  |  |  |
| --- | --- | --- | --- |
| Nội dung | Mô tả (tính năng, thông số,…) | Kết quả cần đạt | Thời gian thực hiện (theo tuần) |
| Tìm hiểu các phần mềm máy tính, sever thu thập và lưu trữ dữ liệu | * Thu thập và lưu trữ dữ liệu * Hiển thị dữ liệu trên phần mềm máy tính và server online | * Tiến hành thu thập được dữ liệu mẫu * Hiển thị dữ liệu dưới dạng bảng (đồ thị) bằng phần mềm máy tính . * Gửi dữ liệu lên Server online | T4: Tìm hiểu về cách lưu trữ và xử lý dữ liệu  T5: Lập trình ứng dụng hiển thị và xuất dữ liệu mẫu dạng file excel trên máy tính  T6: Gửi dữ liệu mẫu lên server |
|  |  |  |  |
| Tìm hiểu các phương pháp quản lý thiết bị đo | * Quản lý các nút cảm biến * Thêm hoặc xóa một nút cảm biến trong mạng * Nhận biết các nút cảm biến đúng | * Có thể thêm hoặc xóa một nút cảm biến trong mạng (quản lý 10 thiết bị) * Mạng có khả năng nhận biết một nút cảm biến có phải là nút cảm biến đúng hay không | T9: Lập trình thêm/xóa một nút cảm biến trong mạng  T10: Lập trình quản lý các nút cảm biến (lập trình nút trung chuyển)  T11-T12: lập trình gateway |
| Thử nghiệm hoàn thiện dự án |  | Hoàn thiện dự án môn học | T14 – T15 |
| Demo dự án |  | T16 |

**Ngô Đức Dũng - 20202345**

|  |  |  |  |
| --- | --- | --- | --- |
| Nội dung | Mô tả (tính năng, thông số,…) | Kết quả cần đạt | Thời gian thực hiện (theo tuần) |
| Tính chọn phần cứng | * Dải đo, độ phân giải cảm biến * Tốc độ VĐK, bộ nhớ chương trình, hỗ trợ hđh, vv * Chọn các linh kiện khác, xây dựng BOMList | * Chọn được cảm biến phù hợp * Dự trù bộ nhớ của chương trình, tốc độ xử lý, IO, vv để chọn được VĐK thích hợp. | T4-T6: Chọn cảm biến, VĐK  T7-T8: Chọn linh kiện, xây dựng BOMLish |
| Tìm hiểu lập trình truyền nhận LoRa | * Lập trình truyền nhận bản tin * Phân vùng dữ liệu cho node cảm biến (vùng phủ) | * Node và gateway có thể giao tiếp được với nhau * Thời gian cập nhật tối đa 2 phút | T4-T8: Tìm hiểu về LoRa  T8-T12: Viết chương trình truyền nhận LoRa  T8-T10: Tính vùng phủ của node |
| Thiết kế PCB | * Mạch PCB 2 lớp * Có đèn chỉ thị * Có công tắc bắt đầu đo | * kích thước mạch < 100x70mm | T8-T10: vẽ sơ đồ nguyên lý  T11-T13: Vẽ và đặt mua PCB |
| Thử nghiệm hoàn thiện dự án |  | Hoàn thiện dự án môn học | T10 – T15 |
| Demo |  | T16 |

**Hoàng Minh Khánh - 20181548**

|  |  |  |  |
| --- | --- | --- | --- |
| Nội dung | Mô tả (tính năng, thông số,…) | Kết quả cần đạt | Thời gian thực hiện (theo tuần) |
| Thiết kế firmware nút cảm biến | * Đọc nhiệt độ môi trường từ cảm biến * Đo dung lượng pin * Có nút bấm kiểm tra dung lượng pin | * Đọc được nhiệt độ môi trường * Kiểm tra được dung lượng pin của node * Thời gian đo 1 mẫu < 20s   pin | - T4-T5: Lập trình giao tiếp cảm biến nhiệt độ với vi điều khiển  - T6-T7: Lập trình node cảm biến chế độ active mode  T12-13: Lập trình firmware hoàn thiện cho node cảm biến |
| Tính toán phần nguồn cho node cảm biến | * Node cảm biến có khả năng sử dụng năng lượng pin * Node cảm biến có thể sạc pin trực tiếp hoặc thay pin | * Thời gian dùng khoảng 8h * Thời gian sạc trung bình khoảng 4h | - T8-T9: Tính toán công suất tiêu thụ của node cảm biến  - T10-T11: Tính toán và lựa chọn phần nguồn cho node cảm biến (pin, mạch bảo vê, mạch sạc) |
| Thử nghiệm hoàn thiện dự án |  | Hoàn thiện dự án môn học | T14 – T15 |
| Demo dự án |  | T16 |

1. **Đánh giá tỷ lệ đóng góp của từng thành viên**

|  |  |  |
| --- | --- | --- |
| Người thực hiện | Tỷ lệ | Những vấn đề sẽ giải quyết trong dự án |
|  | 34% | Thiết kế phần cứng dựa trên các task phải làm của sản phẩm. Thiết kế mạch PCB  Phát triển phần mềm, lập trình các task |
|  | 33% | Chuyển giao tín hiệu từ gateway lên websever(thingboard)  Hỗ trợ thiết kế phần cứng |
|  | 33% | Tìm hiểu về cảm biến, xây dựng code đọc cảm biến, LoRa  Thiết kế dashboard hiển thị web |

**CHƯƠNG 2: NỘI DUNG THỰC HIỆN**

1. **Phân tích các yêu cầu của dự án**

Yêu cầu tổng quan dự án:

* Có khả năng giám sát nhiệt độ trong môi trường.
* Dải đo của thiết bị phải nằm khoảng 10°C - 40°C
* Do nhiệt độ thiết bị đo phải có độ chính xác nhỏ (1°C)
* Để kiểm soát nhiệt độ không thay đổi một cách đột ngột thì thiết bị đo phải có thời gian đo 1 mẫu ngắn (cỡ < 20s)
* Có khả năng mở rộng giám sát nhiều node.
* Do cần đo nhiệt độ trong khu vực rộng, số lượng nhiều nên thời gian sử dụng của thiết bị phải lâu để tránh việc mất thời gian khi thay pin hay sạc lại thiết bị

1. **Tìm hiểu các nghiên cứu, dự án liên quan**

* **Phát triển mạng cảm biến không dây (**[**Luận văn thạc sỹ kỹ thuật điều khiển và tự động hóa – Đại học Bách Khoa Hà Nội**](https://dlib.hust.edu.vn/ViewOnline?bitstid=b0030d2f-8f51-46f0-b253-b7833a08232c&type=1)**)**
* Nghiên cứu về mạng cảm biến không dây và các ứng dụng
* Nghiên cứu về công nghệ bluetooth
* Thiết lập mạng cảm biến không dây
* **Công nghệ Lora cho các ứng dụng IOT (**[**Luận văn thạc sỹ chuyên ngành kỹ thuật viễn thông – Đại học Bách Khoa Hà Nội**](https://dlib.hust.edu.vn/ViewOnline?bitstid=f53a8ef2-dedc-43fa-b3db-cd9903dfc493&type=1)**)**
* Các vấn đề chung về IOT, mạng LoRaWAN và thành phố thông minh
* Phân tích công nghệ LoRa
* ứng dụng LoRa ở Việt Nam, các dự án đang nghiên cứu và thực hiện
* **Mạng cảm biến không dây ứng dụng cho nông nghiệp công nghệ cao (**[**Đại học quốc tế, Đại học Quốc gia Thành Phố Hồ Chí Minh**](http://stdjns.scienceandtechnology.com.vn/index.php/stdjns/article/view/704)**)**
* Phương pháp thiết kế các thành phần trong mạng cảm biến
* Ưu điểm của công nghệ Lora trong việc phát triển mạng cảm biến không dây
* Thử nghiệm mô hình mạng cảm biến trong thực tế

## Lựa chọn giải pháp và lên phương án thiết kế

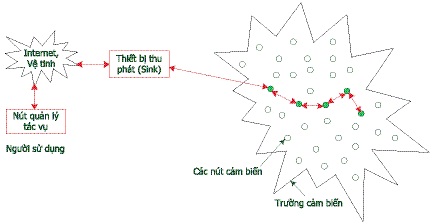
1. **Lựa chọn giải pháp**
   1. **Giới thiệu về mạng cảm biến không dây**

Mạng cảm biến không dây (Wireless Sensor Network) bao gồm một tập hợp các thiết bị cảm biến sử dụng các liên kết không dây (vô tuyến, hồng ngoại hoặc quang học) để phối hợp thực hiện nhiệm vụ thu thập thông tin dữ liệu phân tán với quy mô lớn trong bất kỳ điều kiện và ở bất kỳ vùng địa lý nào.

Mạng cảm biến không dây có thể liên kết trực tiếp với nút quản lý giám sát trực tiếp hay gián tiếp thông qua một điểm thu phát (Sink) và môi trường mạng công cộng như Internet hay vệ tinh. Lợi thế chủ yếu của chúng là khả năng xử lý tốc độ cao, triển khai hầu như trong bất kì loại hình địa lý nào kể cả các môi trường nguy hiểm không thể sử dụng mạng cảm biến có dây truyền thống.

#### **Cấu trúc của mạng cảm biến không dây**

Một mạng cảm biến không dây bao gồm số lượng lớn các nút được triển khai dầy đặc bên trong hoặc ở rất gần đối tượng cần thăm dò, thu thập thông tin dữ liệu. Vị trí các cảm biến không cần định trước vì vậy nó cho phép triển khai ngẫu nhiên trong các vùng không thể tiếp cận hoặc các khu vực nguy hiểm. Khả năng tự tổ chức mạng và cộng tác làm việc của các cảm biến không dây là những đặc trưng rất cơ bản của mạng này. Với số lượng lớn các cảm biến không dây được triển khai gần nhau thì truyền thông đa liên kết được lựa chọn để công suất tiêu thụ là nhỏ nhất (so với truyền thông đơn liên kết) và mang lại hiệu quả truyền tín hiệu tốt hơn so với truyền khoảng cách xa.

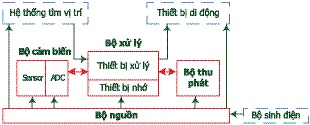


Hình : Cấu trúc cơ bản của mạng cảm biến không dây

Các nút cảm biến được triển khai trong một trường cảm biến (sensor field). Mỗi nút cảm biến được phát tán trong mạng có khả năng thu thập thông số liệu, định tuyến số liệu về bộ thu nhận (Sink) để chuyển tới người dùng (User) và định tuyến các bản tin mang theo yêu cầu từ nút Sink đến các nút cảm biến. Số liệu được định tuyến về phía bộ thu nhận (Sink) theo cấu trúc đa liên kết không có cơ sở hạ tầng nền tảng (Multihop Infrastructureless Architecture), tức là không có các trạm thu phát gốc hay các trung tâm điều khiển. Bộ thu nhận có thể liên lạc trực tiếp với trạm điều hành (Task Manager Node) của người dùng hoặc gián tiếp thông qua Internet hay vệ tinh (Satellite).

Mỗi nút cảm biến bao gồm bốn thành phần cơ bản là: bộ cảm biến, bộ xử lý, bộ thu phát không dây và nguồn điện. Tuỳ theo ứng dụng cụ thể, nút cảm biến còn có thể có các thành phần bổ sung như hệ thống tìm vị trí, bộ sinh năng lượng và thiết bị di động. Các thành phần trong một nút cảm biến được thể hiện trên hình 2. Bộ cảm biến thường gồm hai đơn vị thành phần là đầu đo cảm biến (Sensor) và bộ chuyển đổi tương tự/số (ADC). Các tín hiệu tương tự được thu nhận từ đầu đo, sau đó được chuyển sang tín hiệu số bằng bộ chuyển đổi ADC, rồi mới được đưa tới bộ xử lý. Bộ xử lý, thường kết hợp với một bộ nhớ nhỏ, phân tích thông tin cảm biến và quản lý các thủ tục cộng tác với các nút khác để phối hợp thực hiện nhiệm vụ. Bộ thu phát đảm bảo thông tin giữa nút cảm biến và mạng bằng kết nối không dây, có thể là vô tuyến, hồng ngoại hoặc bằng tín hiệu quang. Một thành phần quan trọng của nút cảm biến là bộ nguồn. Bộ nguồn, có thể là pin hoặc ắcquy, cung cấp năng lượng cho nút cảm biến và không thay thế được nên nguồn năng lượng của nút thường là giới hạn. Bộ nguồn có thể được hỗ trợ bởi các thiết bị sinh điện, ví dụ như các tấm pin mặt trời nhỏ.

Hầu hết các công nghệ định tuyến trong mạng cảm biến và các nhiệm vụ cảm biến yêu cầu phải có sự nhận biết về vị trí với độ chính xác cao. Do đó, các nút cảm biến thường phải có hệ thống tìm vị trí. Các thiết bị di động đôi khi cũng cần thiết để di chuyển các nút cảm biến theo yêu cầu để đảm bảo các nhiệm vụ được phân công.



Hình 2: Các thành phần của nút cảm biến

#### **Đặc điểm của mạng cảm biến không dây**

* Kích thước vật lý nhỏ gọn
* Kích thước và công suất tiêu thụ luôn chi phối khả năng xử lý, lưu trữ và tương tác của các thiết bị cơ sở.
* Hoạt động đồng thời với độ tập trung cao
* Khả năng liên kết vật lý và phân cấp điều khiển hạn chế
* Tính đa dạng trong thiết kế và sử dụng
* Hoạt động tin cậy

#### **Ứng dụng của mạng cảm biến không dây**

**Giám sát và điều khiển công nghiệp**

Phục vụ việc thu thập thông tin, giám sát trạng thái hoạt động của hệ thống, như trạng thái các van, trạng thái thiết bị, nhiệt độ và áp suất của nguyên liệu được lưu trữ; hệ thống điều khiển không dây ánh sáng quảng cáo.

**Tự động hoá gia đình và điện dân dụng**

Mục đích lớn của các mạng cảm biến không dây trong gia đình được mong chờ là mức tiêu thụ điện thấp. Ứng dụng khác trong gia đình là việc hỗ trợ các dịch vụ gia đình trên ôtô: ổ khoá không dây, các cảm biến cửa ra vào và cửa sổ, và các bộ điều khiển bóng đèn không dây, chủ nhà có một thiết bị tương tự như một key-fob với một nút bấm. Khi bấm nút, thiết bị khoá tất cả các cửa ra vào và cửa sổ trong nhà, tắt hầu hết các bóng đèn trong nhà (trừ một vài bóng đèn ngủ), bật các bóng đèn an toàn ngoài nhà, và thiết lập hệ thống HVAC đến chế độ ngủ. Người sử dụng nhận một tiếng beep một lần hồi đáp thể hiện tất cả đã thực hiện thành công, và nghỉ ngơi hoàn toàn, như vậy ngôi nhà an toàn. Khi một cánh cửa hỏng không thể mở, hoặc vấn đề tồn tại, một màn hình hiển thị trên thiết bị chỉ thị nơi bị hỏng.

**Triển vọng của mạng cảm biến không dây trong quân sự**

Vì các mạng cảm biến dựa trên cơ sở triển khai dày đặc với các nút giá rẻ và chỉ dùng một lần, việc bị địch phá huỷ một số nút không ảnh hưởng tới hoạt động chung như các cảm biến truyền thống nên chúng tiếp cận chiến trường tốt hơn. Một số ứng dụng của mạng cảm biến là: kiểm tra lực lượng, trang bị, đạn dược, giám sát chiến trường, trinh sát vùng và lực lượng địch, tìm mục tiêu, đánh giá thiệt hại trận đánh, trinh sát và phát hiện các vũ khí hóa học - sinh học - hạt nhân.

**Mạng cảm biến không dây trong y tế và giám sát sức khoẻ**

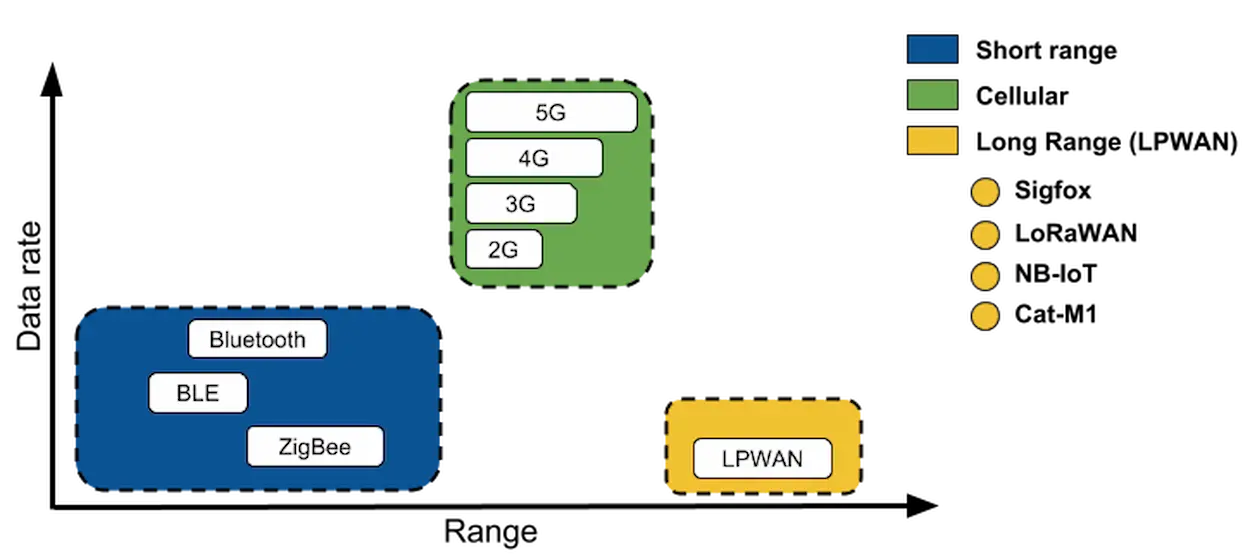
Một số ứng dụng trong y tế của mạng cảm biến không dây là cung cấp khả năng giao tiếp cho người khuyết tật; kiểm tra tình trạng của bệnh nhân; chẩn đoán; quản lý dược phẩm trong bệnh viện; kiểm tra sự di chuyển và các cơ chế sinh học bên trong của côn trùng và các loài sinh vật nhỏ khác; kiểm tra từ xa các số liệu về sinh lý con người; giám sát, kiểm tra các bác sĩ và bệnh nhân bên trong bệnh viện.

**Mạng cảm biến không dây với môi trường và ngành nông nghiệp**

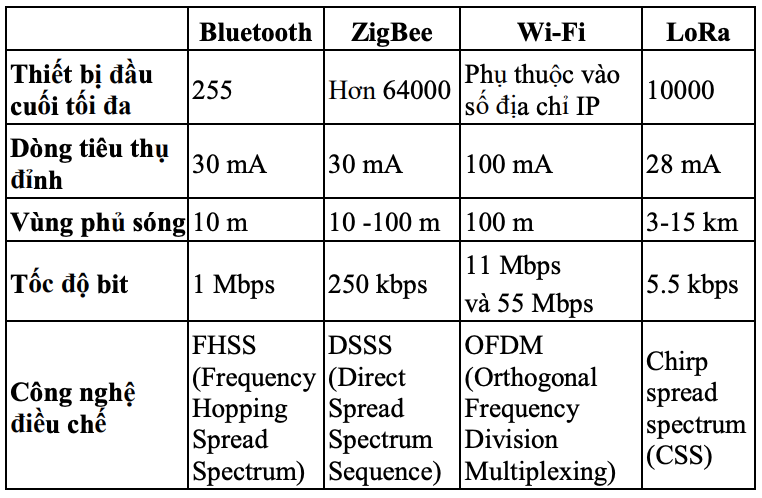
Theo dõi sự di chuyển của các loài chim, loài thú nhỏ, côn trùng; kiểm tra các điều kiện môi trường ảnh hưởng tới mùa màng và vật nuôi; tình trạng nước tưới; các công cụ vĩ mô cho việc giám sát mặt đất ở phạm vi rộng và thám hiểm các hành tinh; phát hiện hóa học, sinh học; tính toán trong nông nghiệp; kiểm tra môi trường không khí, đất trồng, biển; phát hiện cháy rừng; nghiên cứu khí tượng và địa lý; phát hiện lũ lụt; vẽ bản đồ sinh học phức tạp của môi trường và nghiên cứu ô nhiễm môi trường. Các ứng dụng của các mạng cảm biến không dây cũng được sử dụng trên các trang trại chăn nuôi. Người chăn nuôi có thể sử dụng các mạng cảm biến trong quá trình quyết định vị trí của động vật trong trang trại và với các cảm biến được gắn theo mỗi động vật, xác định yêu cầu cho các phương pháp điều trị để phòng chống các động vật ký sinh. Người chăn nuôi lợn hoặc gà có các đàn trong các chuồng nuôi mát, thoáng khí. Mạng cảm biến không dây có thể được sử dụng cho việc giám sát nhiệt độ khắp chuồng nuôi, đảm bảo an toàn cho đàn.

#### **1.5 Lựa chọn giải pháp công nghệ phù hợp với yêu cầu của dự án**

Có rất nhiều công nghệ truyền thông không dây được sử dụng phổ biến hiện nay như: Wifi, Bluetooth, LoRa, Zigbee, … Mỗi công nghệ lại có những ưu nhược điểm riêng và phù hợp với từng ứng dụng mục đích và ứng dụng khác nhau. Ta có hai bản so sánh một số công nghệ phổ biến như sau:



Hình 3: So sánh một số công nghệ không dây phổ biến



Từ các thông số ở trên và dựa theo yêu cầu của dự án thì công nghệ LoRa là công nghệ phù hợp nhất vì:

* + Khoảng cách truyền nhận lớn (lớn hơn 1km)
  + Thiết bị có thể hoạt động ổn định trong thời gian dài (công suất thấp)
  + Không yêu cầu tốc độ truyền nhận cao
  + Chi phí thấp
  + Có độ tin cậy, an toàn và bền vững trong thời gian dài
  + Có khả năng mở rộng để quản lý một lượng lớn các đối tượng

1. **Tìm hiểu công nghệ sử dụng**

#### **2.1** **Sơ lược về LPWAN**

Một loại hình công nghệ không thể phục vụ tất cả các ứng dụng và dự ​án ​của IoT. WiFi và BLE là những tiêu chuẩn được áp dụng rộng rãi và phục vụ khá tốt cho các ứng dụng liên quan đến giao tiếp giữa thiết bị cá nhân. Công nghệ di động Cellular rất phù hợp cho các ứng dụng cần một lượng dữ liệu cao và phải cần nguồn điện. Với LPWAN, thì nguồn pin thiết kế dùng được trong nhiều năm và được dùng cho các cảm biến và các ứng dụng khi cần gửi một lượng nhỏ dữ liệu trong khoảng cách xa vài lần trong một giờ từ các loại môi trường khác nhau.

Ảnh có chứa bàn

Mô tả được tạo tự động

Các yếu tố quan trọng nhất trong LPWAN là:

* Cấu trúc mạng
* Phạm vi giao tiếp
* Tuổi thọ của pin và công suất
* Khả năng chống nhiễu
* Số nút tối đa trong một mạng
* An ninh mạng, bảo mật thông tin
* Giao tiếp 1 chiều, 2 chiều
* Nhiều phần mềm hỗ trợ

LoRa và cảm biến LoraWAN thuộc về loại giao thức và trình phát mạng truyền thông không dây LPWAN phi di động (non-cellular), hoạt động trong phổ tần số không có giấy phép.

Lora sử dụng kỹ thuật điều chế gọi là Chirp Spread Spectrum, và Lora vẫn duy trì được các đặc tính công suất thấp giống như điều chế FSK ngoài ra còn tăng đáng kể phạm vi truyền thông. Chirp Spread Spectrum đã được sử dụng trong lĩnh vực quân sự và vũ trụ trong nhiều thập kỷ do khoảng cách giao tiếp tầm xa có thể đạt được và khả năng can thiệp mạnh mẽ, và LoRa cũng là ứng dụng với mức chi phí thấp đầu tiên được sử dụng cho mục đích thương mại.

Lợi thế nhất của LoRa là ở khả năng tầm xa của công nghệ. Một gateway hoặc một trạm gốc có thể bao phủ toàn bộ thành phố hoặc hàng trăm km vuông. Phạm vi phụ thuộc nhiều vào môi trường hoặc vật cản tại một vị trí nhất định, nhưng LoRa và LoRaWAN có tầm liên kết (Link Budget) rộng hơn so với bất kỳ công nghệ truyền thông tiêu chuẩn nào khác. Tầm liên kết, thường được tính bằng decibel (dB), là yếu tố chính để xác định phạm vi liên kết trong một môi trường nhất định.

LoRaWAN được định nghĩa là một kiến trúc hệ thống và giao thức truyền thông trong mạng, trong khi đó LoRa là lớp vật lý (physical layer) cho phép thiết lập các kết nối truyền thông tầm xa. Giao thức và kiến ​​trúc mạng có ảnh hưởng lớn nhất đến việc xác định thời lượng pin của một nút, dung lượng mạng, chất lượng dịch vụ, bảo mật và nhiều loại ứng dụng được phục vụ bởi mạng.

Ảnh có chứa bàn

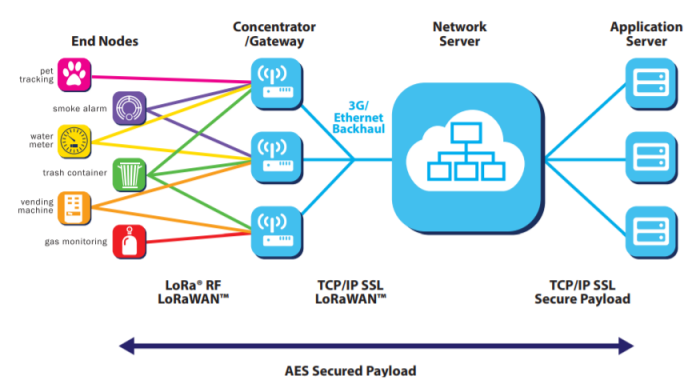
Mô tả được tạo tự động

Hình : Kiến trúc hệ thống LoRaWAN

#### **2.2 Công nghệ LoRaWAN**

##### **2.2.1 Cấu trúc mạng**

Hiện nay trên thị trường có nhiều hệ thống mạng sử dụng kiến ​​trúc mạng lưới. Trong một mạng lưới, các End-node chuyển tiếp thông tin độc lập tới các nút khác để nhằm tăng phạm vi truyền thông và kích thước ô của mạng. Vì điều này làm tăng phạm vi của nó nên cũng làm tăng thêm độ phức tạp, giảm dung lượng mạng và giảm thời lượng pin do các nút nhận và chuyển tiếp thông tin từ các nút khác có thể không liên quan đến chúng. Kiến trúc hình sao có ý nghĩa nhất là để bảo tồn thời lượng pin khi có thể đạt được kết nối tầm xa.



Hình : Mô hình mạng LoRaWAN

Trong một mạng LoRaWAN, các nút mạng không được liên kết với một gateway cụ thể. Thay vào đó, dữ liệu được truyền bởi một nút thường được nhận bởi nhiều gateway. Mỗi cổng sẽ chuyển tiếp gói tin đã nhận từ nút cuối đến máy chủ mạng dựa trên đám mây thông qua một số loại backhaul (mạng di động, Ethernet, vệ tinh hoặc Wi-Fi). Sự thông minh và phức tạp đó sẽ được đẩy lên server, nơi quản lý hệ thống mạng và lọc các gói đã nhận dư thừa, thực hiện kiểm tra bảo mật, lập lịch báo nhận thông qua cổng tối ưu và thực hiện tốc độ dữ liệu thích ứng, v.v. Nếu một nút di động hoặc đang di chuyển thì không cần chuyển giao từ gateway đến gateway, đây là một tính năng quan trọng để kích hoạt các ứng dụng theo dõi vật thể – một ngành ứng dụng chính cho IoT.

##### **2.2.2 Tuổi thọ pin**

Các nút trong mạng LoRaWAN không đồng bộ và giao tiếp khi chúng có dữ liệu sẵn sàng để gửi dù theo hướng Event hay theo lịch trình định sẵn. Loại giao thức này thường được gọi là phương pháp Aloha. Trong mạng lưới hoặc với mạng đồng bộ, chẳng hạn như mạng di động, các nút thường xuyên phải ‘đánh thức’ để đồng bộ hóa với mạng và kiểm tra thông báo. Việc đồng bộ hóa này tiêu tốn năng lượng đáng kể và là nguyên nhân số một làm giảm tuổi thọ của pin. Trong một sô nghiên cứu và so sánh gần đây được thực hiện bởi GSMA về các công nghệ khác nhau trong đó có LPWAN, LoRaWAN và họ cho thấy lợi thế gấp 3 đến 5 lần so với tất cả các lựa chọn công nghệ khác.

##### **2.2.3 Dung lượng mạng**

Để làm cho một mạng hình sao tầm xa có thể tồn tại, gateway phải có dung lượng rất cao hoặc khả năng nhận thông điệp từ một lượng rất lớn các nút. Dung lượng mạng cao trong mạng LoRaWAN đạt được bằng cách sử dụng tốc độ dữ liệu thích ứng và bằng cách sử dụng bộ thu phát đa mô-đun đa kênh trong gateway để có thể nhận được các thông báo đồng thời trên nhiều kênh. Các yếu tố quan trọng ảnh hưởng đến dung lượng là số lượng kênh hiện thời, tốc độ dữ liệu (thời gian truyền trực tuyến), độ dài tải trọng truyền và tần suất truyền của các nút. Vì LoRa là một điều chế Spread Spectrum, các tín hiệu thực tế là trực giao với nhau vì các hệ số lan truyền được sử dùng là khác nhau. Khi hệ số lan truyền thay đổi, tốc độ dữ liệu hiệu quả cũng thay đổi. Các gateway tận dụng đặc tính này bằng cách có thể nhận nhiều tốc độ dữ liệu khác nhau trên cùng một kênh cùng một lúc. Nếu một nút có liên kết tốt với một gateway ở gần đó, thì không có lý do gì để nó luôn sử dụng tốc độ dữ liệu thấp nhất và lấp đầy phổ khả dụng hơn mức cần thiết. Bằng cách thay đổi tốc độ dữ liệu cao hơn, thời gian truyền trực tuyến được rút ngắn, mở ra nhiều không gian tiềm năng hơn cho các nút khác để truyền tải.

Tốc độ dữ liệu thích ứng cũng tối ưu hóa thời lượng pin của một nút. Để tốc độ dữ liệu thích ứng hoạt động, thì phải có tính đối xứng giữa việc dùng dữ liệu để uplink và downlink phải phù hợp với dung lượng mạng. Các tính năng này cho phép mạng LoRaWAN có dung lượng rất cao và làm cho mạng có thể mở rộng. Một mạng có thể được triển khai với số lượng cơ sở hạ tầng tối thiểu và khi cần dung lượng và gateway nhiều hơn thì có thể được thêm vào, tăng tốc độ dữ liệu, giảm số lượng tiếp nhận cho các gateway khác và mở rộng dung lượng lên 6-8 lần. Các lựa chọn thay thế LPWAN khác không có khả năng mở rộng của LoRaWAN do đánh đổi công nghệ, điều này làm hạn chế dung lượng downlink hoặc làm cho phạm vi downlink không đối xứng với uplink.

##### **2.2.4 Các lớp thiết bị – Không phải tất cả các nút đều được cấu tạo như nhau**

Thiết bị End-Devices phục vụ các ứng dụng khác nhau và có các yêu cầu khác nhau. Để tối ưu hóa nhiều loại cấu hình của thiết bị end-node, LoRaWAN ™ sử dụng các lớp thiết bị khác nhau. Các lớp thiết bị đánh đổi tốc độ xử lý downlink của mạng so với thời lượng pin. Trong ứng dụng kiểu điều khiển hoặc cơ cấu chấp hành, tốc độ xử lý downlink là một yếu tố quan trọng.

Ảnh có chứa văn bản

Mô tả được tạo tự động

Hình : Các lớp thiết bị trong LoRaWAN

**Lớp A:** Truyền nhận dữ liệu hai hướng: Các thiết bị thuộc Loại A cho phép truyền nhận theo hai hướng, theo đó mỗi lần truyền uplink của các end-device sẽ được theo sau bởi hai đường nhận downlink. Tiến trình truyền nhận được thiết lập bởi end-devices dựa trên nhu cầu giao tiếp của riêng nó thông qua sự biến thiên thời gian (dựa trên cấu trúc giao thức ALOHA). Lớp A hoạt động với các hệ thống end-device tiêu thụ công suất thấp, phù hợp cho các ứng dụng chỉ yêu cầu giao tiếp downlink từ server sau khi end-device đã thiết lập đường truyền uplink. Giao tiếp downlink từ máy chủ vào bất kỳ thời điểm nào khác sẽ phải đợi cho đến khi uplink theo lịch trình tiếp theo.

**Lớp B:** End-devices truyền nhận dữ liệu theo 2 hướng với việc tiếp nhận (receive slots) được thiết lập theo lịch trình. End-devices theo lớp B sẽ mở cửa sổ nhận theo thời gian đã được thiết lập, nó sẽ nhận được một tín hiệu báo đồng bộ từ Gateway. Điều này cho phép Server biết được khi nào end-device đang lắng nghe.

**Lớp C:** End-devices truyền nhận dữ liệu theo 2 hướng với tiến trình “nhận” (receive slots) tối đa, mang lại độ trễ nhỏ nhất. End-devices thuộc Class C sẽ liên tục mở luồng nhận và chỉ đóng khi thực hiện việc truyền dữ liệu.

##### **2.2.5 Security**

Điều cực kỳ quan trọng đối với bất kỳ LPWAN nào là tính bảo mật. LoRaWAN ™ sử dụng hai lớp bảo mật: một cho mạng và một cho ứng dụng. Bảo mật mạng đảm bảo tính xác thực của nút trong mạng trong khi lớp bảo mật ứng dụng đảm bảo nhà khai thác mạng không có quyền truy cập vào dữ liệu ứng dụng của người dùng cuối. Mã hóa AES được sử dụng với trao đổi khóa bằng cách sử dụng số nhận dạng IEEE EUI 64. Có sự đánh đổi trong mọi lựa chọn công nghệ nhưng LoRaWAN ™ có các tính năng trong kiến ​​trúc mạng, các lớp thiết bị, bảo mật, khả năng mở rộng cho dung lượng và tối ưu hóa cho tính di động giải quyết nhiều loại ứng dụng IoT tiềm năng nhất.

**2.2.6 Ưu điểm và nhược điểm của LoRaWAN**

**Ưu điểm của LoRaWAN**

* Các cảm biến được dùng với công suất thấp và vùng phủ sóng ở tầm diện rộng km.
* Hoạt động trên tần số miễn phí (không có giấy phép), không cần chi phí cấp phép trả trước để sử dụng công nghệ.
* Nguồn điện cấp thấp nên đồng nghĩa với thời lượng pin lâu dài cho các thiết bị. Pin dùng cho cảm biến có thể kéo dài từ 2–5 năm (Loại A và Loại B).
* Các cổng Gateway được thiết kế để tiếp nhận hàng nghìn thiết bị End-device hoặc các nút.
* Dễ dàng triển khai do kiến ​​trúc mạng đơn giản.
* Nó được sử dụng rộng rãi cho các ứng dụng M2M / IoT
* Dung lượng đường truyền lên đến (100 byte), so với SigFox là 12 byte
* Tính “Mở”: một công nghệ mở và một tiêu chuẩn mở so với đối thủ cạnh tranh SigFox
* Không hạn chế số lượng thông điệp tối đa mỗi ngày (so với giới hạn của SigFox là 140 / ngày)
* LoRaWAN có các lợi ích với cách tiếp cận Mở thay vì độc quyền (SigFox).
* Tầm xa cho phép các giải quyết các ứng dụng phạm vi rộng trong thành phố.
* Băng tần thấp khiến LoRaWAN trở nên lý tưởng cho các ứng dụng IoT thực tế với ít dữ liệu hơn hoặc với việc truyền dữ liệu không liên tục.
* Chi phí kết nối thấp.
* Không dây, dễ cài đặt và triển khai nhanh chóng.
* Bảo mật: một lớp bảo mật cho mạng và một lớp cho ứng dụng với mã hóa AES.
* Hoàn toàn giao tiếp hai chiều.
* Được hỗ trợ bởi CISCO, IBM và 500 công ty thành viên khác của LoRa Alliance.

**Nhược điểm của LoRaWAN**

* Không dành cho các ứng dụng truyền dữ liệu lớn, giới hạn trong tầm 100 byte.
* Không dùng để giám sát liên tục (trừ thiết bị loại C).
* Không phù hợp cho các ứng dụng thời gian thực yêu cầu độ trễ thấp và các yêu cầu về rung giật giới hạn.
* Mật độ các mạng LoRaWAN: Sự gia tăng của các công nghệ LPWAN, và đặc biệt là LoRaWAN, đặt ra những thách thức cùng nhau tồn tại khi việc triển khai các gateway vào khu vực đô thị.
* Bất lợi của tần số mở là bạn có thể bị nhiễu trên tần số đó và tốc độ dữ liệu có thể thấp. (Đối với GSM hoặc tần số được cấp phép, bạn có thể truyền trên tần số đó mà không bị nhiễu. Các nhà khai thác GSM sử dụng các tần số nhất định mà phải trả một khoản phí cấp phép lớn cho chính phủ để sử dụng các tần số đó. LoRa hoạt động trên các tần số mở và không cần trạng thái Giấy phép. (Hãy nhớ rằng các tần số mở là khác nhau giữa các quốc gia).

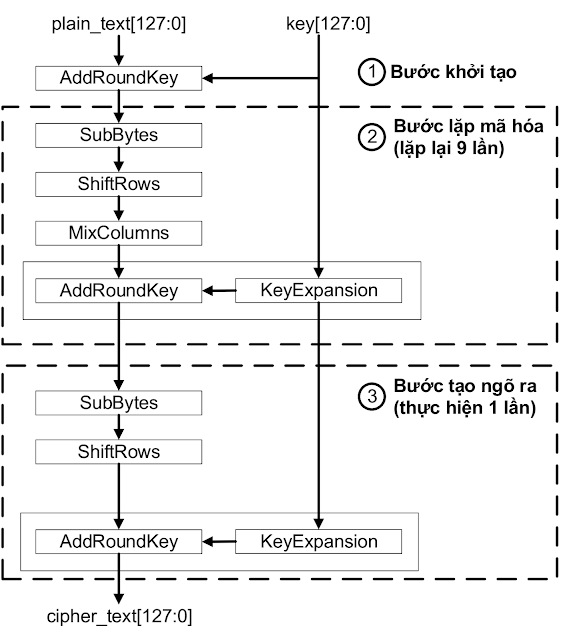
#### **2.3 Mã hóa AES (Advanced Encryption Standard)**

**2.3.1 Tổng quan**

* AES – là một thuật toán mã hóa khối (128 bits dữ liệu) đối xứng (khóa mã hóa và khóa giải mã giống nhau)
* Thuật toán được xây dựng dựa trên Rijndael Cipher phát triển bởi 2 nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen.
* Độ dài khóa là 128, 192 hoặc 256 bits tương ứng AES-128, AES-192, AES-256
* Mỗi khối dữ liệu đầu vào 128bit được chia thành 16byte, có thể xếp thành 4 cột, mỗi cột 4 phần tử hay một ma trận 4x4 của các byte, nó gọi là ma trận trạng thái.
* Mã hóa AES được thực hiện thông qua 5 chức năng chính là AddRoundKey, SubBytes, ShiftRows, MixColumns và KeyExpansion. Năm chức năng này được sắp xếp để thực hiện ba bước cơ bản.
* Bước 1. Bước khởi tạo: dữ liệu cần được mã hóa plain\_text[127:0] kết hợp với key[127:0] bằng chức năng AddRoundKey
* Bước 2. Bước lặp mã hóa: kết quả bước 1 được sử dụng để thực hiện tuần tự các chức năng SubBytes, ShiftRows, MixColumns và AddRoundKey. Bước này được lặp lại 9 lần. Chú ý, KeyExpansion thực hiện song song với bước AddRoundKey để tạo khóa vòng cho chức năng này.
* Bước 3. Bước tạo ngõ ra: Sau 9 lần lặp ở bước 2, kết quả được sử dụng để thực hiện tuần tự các chức năng SubBytes, ShiftRows và AddRoundKey để tạo ngõ ra cipher\_text[127:0].
* Quá trình giải mã được thực hiện qua 5 chức năng cơ bản là AddRoundKey, InvSubBytes, InvShiftRows, InvMixColumns và InvKeyExpansion. Chú ý, InvKeyExpansion không phải là một chức năng được mô tả trong chuẩn mà là một tên gọi được tác giả thêm vào để chỉ quá trình biến đổi ngược giá trị khóa vòng từ khóa vòng số 10 đến khóa mã gốc.
* Bước 1. Bước khởi tạo: Dữ liệu cần được mã hóa cipher text[127:0] kết hợp với khóa vòng thứ 10, round\_key\_10[127:0], bằng chức năng AddRoundKey
* Bước 2. Bước lặp giải mã: kết quả bước 1 được sử dụng để thực hiện tuần tự các chức năng InvShiftRows, InvSubBytes, AddRoundKey và InvMixColumns. Bước này được lặp lại 9 lần. Chú ý, InvKeyExpansion thực hiện song song với bước AddRoundKey để tạo khóa vòng cho chức năng này.
* Bước 3. Bước tạo ngõ ra: Sau 9 lần lặp ở bước 2, kết quả được sử dụng để thực hiện tuần tự các chức năng InvShiftRows, InvSubBytes và AddRoundKey với khóa mã ban đầu để khôi phục lại plain\_text[127:0].

**2.3.2 Quá trình mã hóa**

**Sơ đồ tổng quát**



Hình : Quá trình mã hóa AES-128

Trong quá trình mã hóa, ma trận dữ liệu ban đầu sẽ bị biến đổi bởi các chức năng AddRoundKey, SubBytes, ShiftRows hoặc MixColumns để tạo ra các dữ liệu trung gian gọi là ma trận trạng thái. Ma trận khóa mã sẽ bị biến đổi bởi chức năng KeyExpansion để tạo ra các khóa mã trung gian gọi là khóa vòng.

**Hàm AddRoundKey()**

Chức năng AddRoundKey thực hiện ở:

1. Bước khởi tạo: XOR khóa mã với ma trận dữ liệu
2. Bước lặp mã hóa và bước tạo ngõ ra: XOR khóa vòng (round key) với ma trận trạng thái.

Đối với bước lặp mã hóa và bước tạo ngõ ra, vị trí "khóa mã" là các "khóa vòng" còn dữ liệu là của lần tính trước đó.

**Hàm *SubBytes()***

Chức năng SubBytes là thực hiện thay thế từng byte của ma trận trạng thái, ngõ ra của AddRoundKey, bằng một giá trị đã quy định trong chuẩn AES. Bảng quy định giá trị thay thế gọi là S-box.

|  |
| --- |
| Ảnh có chứa bàn  Mô tả được tạo tự động  Hình : S-box của mã hóa AES |
|  |

Ví dụ, byte cần thay thế là H08 thì dò ở hàng số 0 và cột số 8 trong bảng S-box sẽ được kết quả là 30.

**Hàm ShiftRows()**

Chức năng ShiftRows thực hiện quay trái từng hàng của ma trận trạng thái, ngõ ra của SubBytes, theo byte với hệ số quay tăng dần từ 0 đến 3. Hàng đầu tiên có hệ số quay là 0 thì các byte được giữ nguyên vị trí. Hàng thứ hai có hệ số quay là 1 thì các byte được quay một byte. Hàng thứ ba quay hai byte và hàng thứ tư quay ba byte.

|  |
| --- |
| Hình : Chức năng ShiftRows |
|  |

**Hàm** MixColumns()

Chức năng MixColumns thực hiện nhân từng cột của ma trận trạng thái, ngõ ra của ShiftRows, với một ma trận chuyển đổi quy định bởi chuẩn AES.

|  |
| --- |
| Ảnh có chứa văn bản  Mô tả được tạo tự động  Hình : Ma trận chuyển đổi sử dụng trong chức năng MixColumns |
| *Ma trận chuyển đổi sử dụng trong chức năng MixColumns* |

Việc biến đổi một cột của ma trận trạng thái được thực hiện bởi hai phép toán là nhân (.) và XOR (+).

Phép nhân với H01 thì giữ nguyên giá trị. Phép nhân với H02 tương đương với việc dịch trái một bit và XOR có điều kiện như sau:

* Nếu bit MSB của giá trị được dịch bằng 1 thì giá trị sau khi dịch được XOR với H1b
* Nếu bit MSB của giá trị được dịch bằng 0 thì giữ giá trị sau khi dịch.

|  |
| --- |
|  |
|  |

##### **2.3.3 Giải thuật sinh khóa phụ (KeyExpansion)**

Tổng quát

Chức năng KeyExpansion thực hiện tính toán khóa vòng cho bước lặp mã hóa và bước tạo ngõ ra. Kết quả của một lần thực thi KeyExpansion là một khóa vòng sử dụng cho chức năng AddRoundKey. Với mã hóa AES-128, số khóa vòng là 10 tương ứng với 9 lần AddRoundKey ở bước lặp mã hóa và 1 lần AddRoundKey ở bước tạo ngõ ra.  
Chức năng KeyExpansion được thực hiện thông qua 4 chức năng là RotWord, SubWord, AddRcon và AddW.

|  |
| --- |
| Hình : Chức năng KeyExpansion |
|  |

Mỗi khóa vòng có 128 bit được chia làm 4 word, mỗi word là 4 byte và ký hiệu là w[j] với j là số nguyên. Mã hóa AES-128 có 1 khóa mã và 10 khóa vòng nên tổng số word là 44 và được đánh số từ 0 đến 43. Khóa mã có 4 word là w[0], w[1], w[2] và w[3]. Khóa vòng 1 có 4 word là w[4], w[5], w[6] và w[7]. Tương tự, khóa vòng 10 có 4 word là w[40], w[41], w[42] và w[43].  
Word w[j] tính theo công thức sau, với 3 < j < 44.

**w[j] = AddW[j - 4] = w[j - 1] + w[j - 4]**

**w[j = 4∗ n] = AddW[j - 4] = (trans(w[j - 1])) + w[j - 4]**

Chú ý, khi tính các word ở vị trí j là bội số của 4, như w[4], w[8],... và w[40], thì w[j-1] phải được biến đổi qua 3 chức năng RotWord, SubWord và AddRcon, gọi là trans(w[j-1]), trước khi XOR với w[j-4].

Hàm RotWord()

Hàm RotWord thực hiện quay trái từ w[j] một byte.

|  |
| --- |
|  |
|  |

Hàm SubWord()

Chức năng SubWord thực hiện thay thế các phi tuyến từng byte của kết quả RotWord theo bảng S-box.

|  |
| --- |
|  |
|  |

Hàm AddRcon()

Chức năng AddRcon thực hiện XOR kết quả SubWord và giá trị Rcon[j/4] với j là bội số của 4. Số lượng giá trị Rcon[j/4] là 10 tương ứng với 10 lần tính khóa vòng. Chức năng AddRcon sẽ tạo ra kết quả cuối cùng của biến đổi trans(w[j-1]).  
  
**Rcon[j/4]**  **Giá trị  HEX**  **Vị trí sử dụng**  
Rcon[1] 01000000        sử dụng cho trans(w[3]) khi tính w[4]  
Rcon[2] 02000000        sử dụng cho trans(w[7]) khi tính w[8]  
Rcon[3] 04000000        sử dụng cho trans(w[11]) khi tính w[12]  
Rcon[4] 08000000        sử dụng cho trans(w[15]) khi tính w[16]  
Rcon[5] 10000000        sử dụng cho trans(w[19]) khi tính w[20]  
Rcon[6] 20000000        sử dụng cho trans(w[23]) khi tính w[24]  
Rcon[7] 40000000        sử dụng cho trans(w[27]) khi tính w[28]  
Rcon[8] 82000000        sử dụng cho trans(w[31]) khi tính w[32]  
Rcon[9] 1b000000        sử dụng cho trans(w[35]) khi tính w[36]  
Rcon[10] 36000000        sử dụng cho trans(w[39]) khi tính w[40]

|  |
| --- |
|  |
|  |

**Hàm AddW()**

Chức năng AddW thực hiện XOR w[j-4] với w[j-1] hoặc trans(w[j-1])

|  |
| --- |
| Ảnh có chứa văn bản, ảnh chụp màn hình, biên lai  Mô tả được tạo tự động  Hình : Thực thi AddW để tạo khóa vòng |

##### **2.3.4 Quá trình giải mã**

**Sơ đồ tổng quát**

|  |
| --- |
| *Quá trình giải mã AES-128* |
|  |

Dữ liệu và khóa mã được sắp xếp dưới dạng ma trận với mỗi phần tử là một byte.

|  |
| --- |
| Ảnh có chứa bàn  Mô tả được tạo tự động |
|  |

**Hàm AddRoundKey đảo**

Chức năng AddRoundKey đảo trong quá trình giải mã cũng chính là chức năng AddRoundKey trong quá trình mã hóa nên gọi chung là AddRoundKey.

**Hàm InvShiftRows**

InvShiftRows là đảo của chức năng ShiftRows. InvShiftRows thực hiện quay phải từng hàng của ma trận trạng thái, sinh ra từ bước trước đó, theo byte với hệ số quay tăng dần từ 0 đến 3. Hàng đầu tiên có hệ số quay là 0 thì các byte được giữ nguyên vị trí. Hàng thứ hai có hệ số quay là 1 thì các được quay một byte. Hàng thứ ba quay hai byte và hàng thứ tư quay ba byte.

**Hàm InvSubBytes**

Chức năng InvSubBytes là thực hiện thay thế từng byte của ma trận trạng thái, bằng một giá trị đã quy định trong chuẩn AES. Bảng quy định giá trị thay thế cho InvSubBytes gọi là S-box đảo (Inverse S-box).

|  |
| --- |
| Ảnh có chứa bàn  Mô tả được tạo tự động  Hình : Bảng S-box đảo của chuẩn AES |
|  |

Ví dụ, byte cần thay thế là Ha7 thì dò ở hàng "a" và cột số 7 trong bảng S-box đảo sẽ được kết quả là H89.

**Hàm InvMixColumns**

InvMixColumns của quá trình giả mã là đảo của MixColumns trong quá trình mã hóa. Từng cột của ma trận trạng thái sẽ được nhân với ma trận chuyển đổi sau đây.

|  |
| --- |
| Ảnh có chứa văn bản, đóng  Mô tả được tạo tự động  Hình : Ma trận chuyển đổi dùng trong InvMixColumns |
|  |

Việc biến đổi một cột của ma trận trạng thái được thực hiện bởi hai phép toán là nhân (.) và XOR (+).

Nguyên tắc tính toán InvMixColumns là biến đổi phép nhân với một số thành phép nhân với *H02*và *H01*. Phép nhân với *H01*thì giữ nguyên giá trị. Phép nhân với *H02*tương đương với việc dịch trái một bit và XOR có điều kiện như sau:

* Nếu bit MSB của giá trị được dịch bằng 1 thì giá trị sau khi dịch được XOR với H1b
* Nếu bit MSB của giá trị được dịch bằng 0 thì giữ giá trị sau khi dịch.

Như vậy, việc biến đổi về phép nhân với *H01* và *H02*sẽ giúp dễ dàng thiết kế mạch logic thực hiện chức năng InvMixColumns với tài nguyên được tối ưu hóa.

**Hàm** **InvKeyExpansion**

Chuẩn AES không nói về InvKeyExpansion vì cả mã hóa và giải mã đều dùng chung một khóa mã. KeyExpansion giúp tính tất cả các khóa vòng từ khóa mã. Ví dụ, trong AES-128, chúng ta sẽ có một khóa mã và 10 khóa vòng. Khi mã hóa, các khóa được sử dụng theo thứ tự như sau:

**Khóa mã (key) -> khóa vòng 1 -> khóa vòng 2 -> ... -> khóa vòng 10**

Khi giải mã theo phương pháp nghịch đảo (Inverse cipher), các khóa được sử dụng theo thứ tự như sau:

**Khóa vòng 10 -> khóa vòng 9 -> ... -> khóa vòng 1 -> khóa mã**

Như vậy, trước khi giải mã, tất cả các khóa vòng phải được tính trước và lưu lại trong một bộ nhớ, ví dụ như RAM hay mảng thanh ghi. Tác giả sẽ thực hiện một cách làm khác là chỉ dùng khóa vòng cuối cùng, khóa vòng 10, sau đó áp dụng InvKeyExpansion để tính ngược lại các khóa vòng trước đó và khóa mã. Cách này giúp không tốn tài nguyên bộ nhớ lưu lại tất cả các khóa nhưng tốn logic thực hiện mạch tính InvKeyExpansion.  
Nguyên tắc tính InvKeyExpansion của khóa thứ *n-1* từ khóa thứ *n*như sau (n >= 1, n = 0 là khóa mã gốc) như sau:

* Mỗi khóa gồm 4 word với word 3 là MSB và word 0 là LSB
* word[0] của khóa thứ *n-1* = word[0] của khóa thứ *n*XOR word[1] của khóa thứ *n*
* word[1] của khóa thứ *n-1* = word[1] của khóa thứ *n*XOR word[2] của khóa thứ *n*
* word[2] của khóa thứ *n-1* = word[2] của khóa thứ *n*XOR word[3] của khóa thứ *n*
* word[3] của khóa thứ *n-1* = word[3] của khóa thứ *n*XOR với giá trị sau khi biến đổi word[0] của khóa thứ *n-1* (đã tính trên đây) qua các bước:
  + RotWord
  + SubWord
  + InvAddRcon

Trong đó, RotWord và SubWord áp dụng tương tự như quá trình mã hóa. InvAddRcon là bước XOR kết quả SubWord với Rcon nhưng thứ tự giá trị Rcon được sử dụng sẽ ngược với quá trình mã hóa.

**Rcon      Giá trị HEX Vị trí sử dụng**

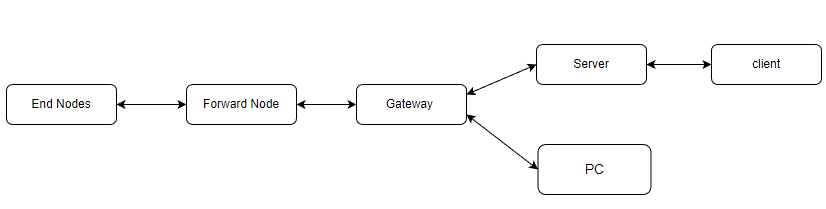
Rcon[1] 36000000 sử dụng cho lần tính khóa thứ 9  
Rcon[2] 1b000000  sử dụng cho lần tính khóa thứ 8  
Rcon[3] 82000000  sử dụng cho lần tính khóa thứ 7  
Rcon[4] 40000000  sử dụng cho lần tính khóa thứ 6  
Rcon[5] 20000000  sử dụng cho lần tính khóa thứ 5  
Rcon[6] 10000000 sử dụng cho lần tính khóa thứ 4  
Rcon[7] 08000000 sử dụng cho lần tính khóa thứ 3  
Rcon[8] 04000000 sử dụng cho lần tính khóa thứ 2  
Rcon[9] 02000000 sử dụng cho lần tính khóa thứ 1  
Rcon[10] 01000000 sử dụng cho lần tính khóa mã gốc

Như vậy, trong AES-128, ở lần tính đầu tiên, tính giá trị khóa vòng số 9 từ khóa vòng số 10 thì giá trị Rcon[1] = H36000000 được sử dụng. Khác với quá trình giải mã, Rcon[1] = H01000000 được dùng cho lần tính đầu tiên.

**3 . Thử nghiệm đánh giá và hoàn thiện sản phẩm**

#### **Sơ đồ khối chức năng và mô hình hệ thống của mạng cảm biến**

* + 1. *Sơ đồ khối chức năng*



Hình : Sơ đồ khối chức năng

**End Nodes**: Bao gồm cảm biến nhiệt độ, vi điều khiển và mạch thu phát RF chịu trách nhiệm đo nhiệt độ.

**Forward Nodes**: Bao gồm cảm biến nhiệt độ, vi điều khiển và mạch thu phát RF chịu trách nhiệm điều khiển hoạt động và thu thập dữ liệu của End Nodes thông qua các tín hiệu điều khiển.

**Gateway**: Bao gồm vi điều khiển và mạch thu phát RF chịu trách nhiệm điều khiển hoạt động và thu thập dữ liệu của Forward Nodes. Sau khi thu thập dữ liệu khối sẽ chuyển dữ liệu lên Server thông qua Wifi hoặc 3G.

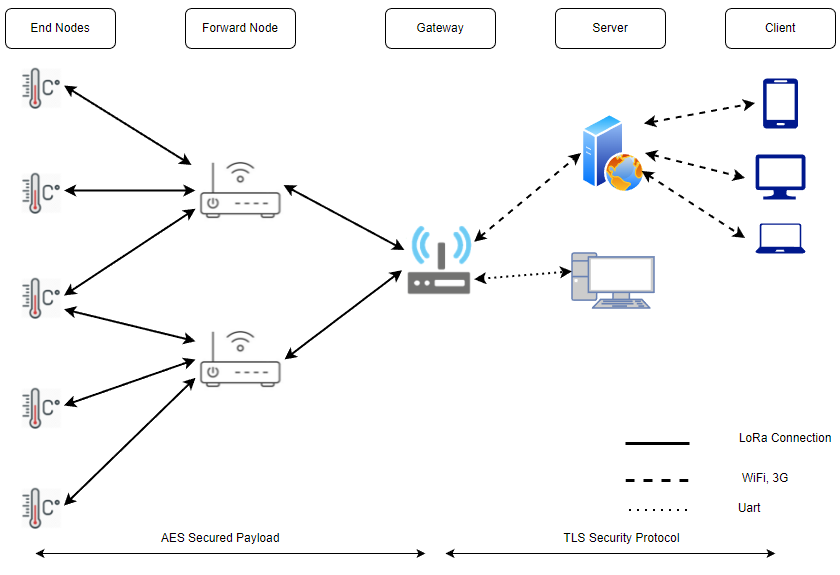
**Server**: Có nhiệm vụ nhận dữ liệu từ Gateway, hiển thị dữ liệu dưới dạng đồ thị và phân tích dữ liệu nếu cần thiết (phục vụ giám sát nhiệt độ từ xa).

**PC**: Có nhiệm vụ nhận dữ liệu từ Gateway hiển thị và lưu trữ dữ liệu dạng file excel, cho phép một node cảm biến mới vào mạng hoặc xóa một node cảm biến ra khỏi mạng, phục vụ cập nhật phần mềm từ xa (OTA).

**Client**: Là các thiết bị có kết nối mạng như điện thoại, laptop để có thể theo dõi nhiệt độ từ xa.

* + 1. **Mô hình hệ thống**

Dựa vào sơ đồ khối chức năng và yêu cầu của dự án ta được mô hình của hệ thống mạng cảm biến như sau:



Hình : Mô hình của hệ thống mạng cảm biến

#### **3.2 Phân tích, lựa chọn linh kiện của mạng cảm biến**

* Lựa chọn mạch thu phát RF

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Thông số | SX1276 | SX1277 | SX1278 | SX1279 |
| Dải tần số | 137 - 1020 MHz | 137 - 1020 MHz | 137 - 525 MHz | -111 to -148 dBm |
| Yếu tố lan truyền (SF) | 6 - 12 | 6 - 9 | 6- 12 | 6- 12 |
| Băng thông (BW) | 7.8 - 500 kHz | 7.8 - 500 kHz | 7.8 - 500 kHz | 7.8 - 500 kHz |
| Tốc độ bit hiệu quả | .018 - 37.5 kbps | 0.11 - 37.5 kbps | .018 - 37.5 kbps | .018 - 37.5 kbps |
| Ngưỡng nhạy | -111 to -148 dBm | -111 to -139 dBm | -111 to -148 dBm | -111 to -148 dBm |

Từ bản trên, các phiên bản lora đều có khoảng cách truyền nhận tưởng đương nhau, nhưng SX1278 lại có giá thành rẻ và dễ dàng tìm mua trong thị trường. Vì vậy trong đề này này chúng em chọn module LoRa1278.

* Lựa chọn vi điều khiển

Nhờ sự phát triển của công nghệ bán dẫn, hiện nay có rất nhiều vi điều khiển với hiệu năng cao cũng như tốc độ xử lý lớn phù hợp cho việc thiết kế một mạng cảm biến không dây. Bảng dưới đây so sánh một số dòng các vi điều khiển nổi bật hiện nay.

|  |  |  |  |
| --- | --- | --- | --- |
| Thông số | PIC | AVR | ARM |
| Chiều rộng bộ nhớ | 8/16/32-bit | 8/32-bit | Chủ yếu 32-bit và cũng có 64-bit |
| Phương thức giao tiếp | PIC, UART, USART, LIN, CAN, Ethernet, SPI, I2S | UART, USART, SPI, I2C, (AVR đặc biệt hỗ trợ CAN, USB, Ethernet) | UART, USART, LIN, I2C, SPI, CAN, USB, Ethernet, I2S, DSP, SAI (giao diện âm thanh nối tiếp), IrDA |
| Tốc độ | 4 chu kỳ xung | 1 chu kỳ xung | 1 chu kỳ xung |
| Bộ nhớ | SRAM, FLASH | Flash, SRAM, EEPROM | Flash, SDRAM, EEPROM |
| Tiêu thụ điện năng | Thấp | Thấp | Thấp |
| Cộng đồng | Rất tốt | Rất tốt | Rộng |
| Nhà sản xuất | Microchip Average | Atmel | Apple, Nvidia, Qualcomm, Samsung Electronics, và TI... |
| Chi phí | Trung bình | Trung bình | Rẻ |
| Các vi điều khiển phổ biến | PIC18fXX8, PIC16f88X, PIC32MXX | Atmega8, 16, 32, Cộng đồng Arduino | LPC2148, ARM Cortex-M0 đến ARM Cortex-M7, ... |

Từ yêu cầu bài toán, vi điều khiển phải đáp ứng được 1 số yêu cầu sau

* + Tốc độ cao
  + Tiêu thụ điện năng thấp
  + Đầy đủ ngoại vi
  + Bộ nhớ chương trình lớn
  + Giá rẻ, thông dụng và phổ biến

Vì vậy ARM là lựa chọn thích hợp nhất. Bài toán yêu cầu khá ít ngoại vi nhưng lại yêu cầu 1 bộ nhớ chương trình lớn (ngủ, định tuyến mạng, OTA) nên STM32F103RCT6 được bọn em sử dụng với thông số cơ bản như sau:

* Tần số tối đa 72MHz
* 256 kB bộ nhớ Flash
* 64KB SRAM
* 51 I/O
* 5 UART, 3 SPI, …
* …
* Lựa chọn cảm biến nhiệt độ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Cảm biến | DHT11 | DHT22 | LM35 | DS18B20 | BME280 | BMP180 |
| Đo lường | Nhiệt độ  Độ ẩm | Nhiệt độ  Độ ẩm | Nhiệt độ | Nhiệt độ | Nhiệt độ  Độ ẩm  Áp suất | Nhiệt độ  Áp suất |
| Giao thức truyền thông | one-wire | one-wire | analog | one-wire | I2C  SPI | I2C |
| Điện áp hoạt động | 3 đến 5.5V DC | 3 đến 6V DC | 4 đến 30V DC | 3 đến 5.5V DC | 1.7 đến 3.6V (cho chip) và 3.3 đến 5V (cho bo) | 1.8 đến 3.6V (cho chip) và 3.3 đến 5V (cho bo) |
| Khoảng nhiệt độ | 0 đến 50ºC | -40 đến 80ºC | -55 đến 150ºC | -55 đến 125ºC | -40 đến 85ºC | 0 đến 65ºC |
| Độ chính xác | +/- 2ºC (ở 0 đến 50ºC) | +/- 0,5ºC (ở -40 đến 80ºC) | +/- 0,5ºC (ở 25ºC) | +/- 0,5ºC (ở -10 đến 85ºC) | +/- 0,5ºC (ở 25ºC) | +/- 0,5ºC (ở 25ºC) |

Do dải nhiệt độ đo từ 0-50 ºC và yêu cầu độ chính xác cao, đơn giản trong việc giao tiếp, đọc dữ liệu, chúng em lựa chọn cảm biến nhiệt độ DS18B20.

#### **3.3 Tính vùng phủ của anten**

Theo công thức Friis:

Diagram

Description automatically generated with low confidence

Vùng phủ R của anten bị ảnh hưởng bởi

* + e0: Hiệu suất của anten
  + : Bước sóng
  + Dt, Dr: Độ định hướng của bộ phát và thu
  + Pt, Pr: Công suất phát, thu
  + PLF: Hệ số suy hao do phân cực

Với anten có độ lợi G = 3dBi

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Công suất phát | | Độ nhạy ngưỡng thu | | Vùng Phủ | |
| dBm | mW | Min(dBm) | Max(dBm) | Min(m) | Max(m) |
| +7 | 5.01 | -111 | -148 |  |  |
| +13 | 19.95 | -111 | -148 |  |  |
| +17 | 50.12 | -111 | -148 |  |  |
| +20 | 100 | -111 | -148 |  |  |

#### **3.4 Tính toán công suất tiêu thụ của nút**

Với những linh kiện đã chọn ở trên, dựa vào datasheet ta có bảng công suất tiêu thụ trung bình của 1 node cảm biến

|  |  |  |
| --- | --- | --- |
| **Công suất tiêu thụ (mW)** | | |
| MCU (STM32F103C8T6) | Active mode | 89.1 |
| Sleep mode | 19.43 |
| LoRa SX1278 | Transmit mode | 95.7 |
| Receive mode | 39.6 |
| Sleep mode | 3.3 |
| DS18B20 | Active mode | 5 |

**3.5 Sơ đồ nguyên lý và pcb node cảm biến**

*3.5.1 Schematic gateway*

Ảnh có chứa văn bản, ảnh chụp màn hình, biểu đồ, số

Mô tả được tạo tự động

*Hình 17. Schematic gateway*

*3.5.2 Schematic gateway*

**Ảnh có chứa mạch điện, Linh kiện điện, Kỹ thuật điện, Cấu phần mạch bị động

Mô tả được tạo tự động**

*Hình 18. PCB gateway*

**3.6 Sơ đồ nguyên lý và pcb node cảm biến**

*3.6.1 Schematic node cảm biến*

Ảnh có chứa văn bản, biểu đồ, ảnh chụp màn hình, Song song

Mô tả được tạo tự động

Hình 19. Schematic node cảm biến

*3.6.2 PCB node cảm biến*

Ảnh có chứa mạch điện, văn bản, đồ điện tử, Kỹ thuật điện

Mô tả được tạo tự động

*Hình 20. PCB node cảm biến*

**3.7 Gateway và node cảm biến thực tế**

*3.7.1 Gateway thực tế*

**Ảnh có chứa đồ điện tử, Kỹ thuật điện, Thiết bị điện, Thành phần mạch điện

Mô tả được tạo tự động**

*Hình 21. Gateway*

*3.7.2 Node thực tế*

**Ảnh có chứa đồ điện tử, Kỹ thuật điện, Linh kiện điện, Thành phần mạch điện

Mô tả được tạo tự động**

*Hình 22. Node*

**Kết quả hiển thị**

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, bức thư

Mô tả được tạo tự động

*Hình 23. Nhiệt độ đo dược từ 2 node*

1. **Kết luận và hướng phát triển**

* Trong dự án vừa rồi nhóm chúng em đã hoàn thành được một số yêu cầu đặt ra như: đo được nhiệt độ, gửi nhiệt độ lên server để hiển thị, bảo mật được gói tin, thiết kế được phần mềm quản lý node, …
* Ngoài ra vẫn còn một số điểm chưa hoàn thành như: chưa triển khai được OTA, vẫn còn có xung đột trên đường truyền, mất mát bản tin
* Hướng phát triển cho hệ thống này là: triển khai được OTA cho hệ thống để tiện cho việc cập nhật, mở rộng mô hình mạng tree, mesh … khả năng thêm bớt node linh hoạt hơn, …