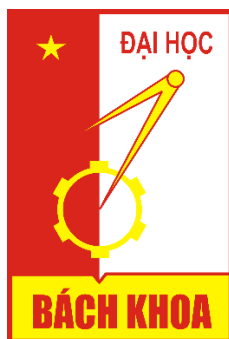


TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

TRƯỜNG ĐIỆN – ĐIỆN TỬ

Khoa Tự Động Hóa

----- ∞  ∞ -----



BÁO CÁO ĐỒ ÁN 2

Đề tài: Thiết kế bộ điều khiển trung tâm

STT	Họ và tên	MSSV
1	Nguyễn Văn Dũng	20191784

Giảng viên hướng dẫn:

Hà Nội, tháng 11/2022

MỤC LỤC

CHƯƠNG 1. TÌM HIỂU CHUNG VỀ BỘ ĐIỀU KHIỂN TRUNG TÂM 1	
CHƯƠNG 2. THIẾT KẾ HỆ THỐNG	9
2.1. Bluetooth Low Energy (BLE)	9
2.1.1. Tổng quan về BLE	9
2.1.2. GAP	10
2.1.3. Attribute Protocol (ATT)	11
2.1.4. Generic Attribute Profile (GATT)	12
2.2. Bluetooth Mesh	13
2.2.1. Tổng quan về Bluetooth Mesh	13
2.2.2. Cấu trúc hệ thống mạng Mesh	14
2.2.3. Các khái niệm trong Bluetooth Mesh	15
2.2.4. Quá trình provisioning	16

CHƯƠNG 1. TÌM HIỂU CHUNG VỀ BỘ ĐIỀU KHIỂN TRUNG TÂM

1.1. Giới thiệu chung

Sự phát triển mạnh mẽ của công nghệ, tỷ lệ phổ cập Internet và Smartphone rất cao, công nghệ 5G, phù hợp với thu nhập giới trung lưu có xu hướng đã khiến thị trường Smart Home ngày càng phát triển mạnh mẽ. Smart Home có thể tự động giúp con người làm những công việc trong nhà, chiếu sáng, đảm bảo an ninh, có thể điều khiển trực tiếp thông qua điện thoại hoặc giọng nói, giúp tiết kiệm được nhiều thời gian.



Với nhiều thiết bị thông minh trong nhà như vậy, để người dùng có thể quản lý và điều khiển chúng thì sẽ phải cần một bộ điều khiển trung tâm đóng vai trò là thiết bị đầu não trong nhà thông minh, tiếp nhận tín hiệu từ cảm biến, người dùng để gửi đến server.

1.2. Khảo sát các bộ điều khiển trung tâm trong thực tế

Hiện nay trên thị trường có nhiều đơn vị đã phát triển bộ điều khiển trung tâm như Lumi, Tuya, Zivix... Các bộ điều khiển này đa số đều sử dụng công nghệ Zigbee 3.0 giúp kết nối và quản lý cùng lúc hàng chục thiết bị, tạo thành một mạng lưới thông minh, cho phép các thiết bị trong cùng một mạng liên kết với nhau. Một số bộ điều khiển mới phát triển còn sử dụng được thêm Bluetooth Mesh và xử lý giọng nói.

Bộ điều khiển trung tâm của Lumi:

- Sử dụng công nghệ Zigbee 3.0 và Bluetooth Mesh.
- Điều khiển các thiết bị bằng ứng dụng Lumi Life và tích hợp được trợ lý ảo.
- Kết nối và quản lý được lên tới 90 thiết bị.
- Thực hiện xử lý các cài đặt tự động: ngữ cảnh, rule, hẹn giờ thiết bị, nhóm thiết bị.
- Sử dụng nguồn điện 220V.



Hình 1.1 Bộ điều khiển trung tâm Zigbee

Bộ điều khiển trung tâm của Tuya:

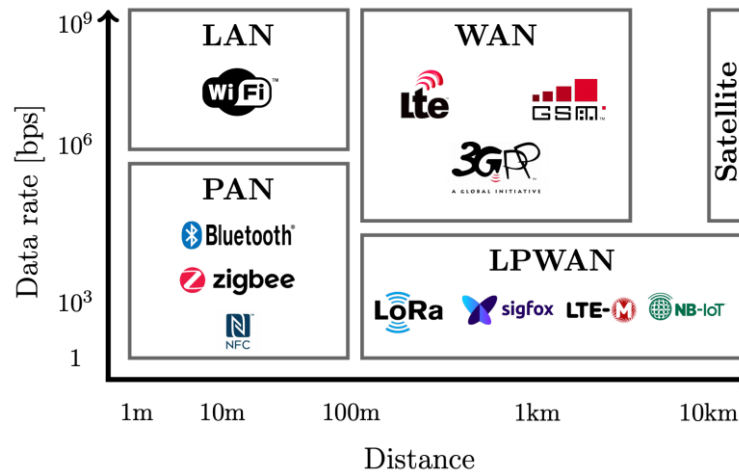
- Sử dụng công nghệ Zigbee 3.0.
- Điều khiển các thiết bị qua ứng dụng trên điện thoại Tuya.
- Hỗ trợ kết nối lên tới 128 thiết bị (dùng LAN) hoặc 50 thiết bị (dùng WiFi)
- Hỗ trợ Google Assistance, Amazon Alexa.
- Sử dụng nguồn điện 220V.



Hình 1.2 Bộ điều khiển trung tâm Tuya

1.3. Khảo sát các công nghệ truyền thông không dây phổ biến

1.3.1. Tổng quan



Hình trên mô tả rõ về các công nghệ truyền thông không dây theo biểu đồ của 2 tham số là phạm vi và tốc độ truyền tin. Được chia ra làm 4 loại chính:

- **Local Area Network (LAN):** Đây là mạng cục bộ. Nó cho phép các thiết bị kết nối và giao tiếp với nhau để chia sẻ dữ liệu. Kết nối này được thực hiện thông qua cáp LAN hoặc kết nối WiFi trong một khu vực địa lý giới hạn như văn phòng, trong nhà, khuôn viên...
- **Personal Area Network (PAN):** Là mạng cá nhân có được tạo bởi sự kết nối vô tuyến trong tầm ngắn khoảng vài mét giữa các thiết bị ngoại vi như tai nghe, đồng hồ, máy in, bàn phím, chuột... Các công nghệ không dây phổ biến trong mạng PAN là Bluetooth, Zigbee.
- **Wide Area Network (WAN):** Hay còn gọi là mạng diện rộng được kết hợp giữa các mạng đô thị bao gồm cả mạng MAN và mạng LAN thông qua thiết bị vệ tinh, cáp quang, cáp dây điện. Mạng diện rộng được tạo ra nhằm kết nối trên một diện lớn có quy mô trên quốc gia. Giao thức sử dụng trong mạng WAN là TCP/IP, đường truyền băng thông thay đổi tùy vào vị trí lắp đặt.
- **Low – Power Wide Area Network:** là các công nghệ không dây. Có các đặc điểm phủ sóng rộng, băng thông thấp, kích thước gói tin nhỏ và tuổi thọ pin dài. LPWAN được thiết kế để hỗ trợ việc truyền thông không dây cho sự phát triển của IoT. Nó cung cấp các kết nối công suất thấp với số lượng thiết bị lớn, phân bố rộng. Tập trung hiệu quả về vùng phủ sóng, năng lượng, băng thông thấp. LPWAN sử dụng cho các ứng dụng IoT với các tiêu chí đó. Công nghệ LPWAN cho phép triển khai các cảm biến thông minh trên toàn khu vực rộng lớn. Các công nghệ không dây trong LPWAN phổ biến: LoRa, NB – IoT, LTE – M ...

Với đề tài của đồ án 2 là thiết kế bộ điều khiển trung tâm, em tập trung tìm hiểu các công nghệ không dây thuộc nhóm LAN và PAN.

1.3.2. WiFi

Wi-Fi là viết tắt của Wireless Fidelity. Đây là công nghệ kết nối mạng cục bộ không dây với các thiết bị dựa trên tiêu chuẩn IEEE 802.11. WiFi có 2 loại dải tần là 2.4GHz và 5GHz. Các thiết bị tương thích với Wi-Fi có thể kết nối với Internet qua mạng WLAN và điểm truy cập không dây viết tắt là AP (Access Point). Mọi mạng WLAN đều có một điểm truy cập chịu trách nhiệm nhận và truyền dữ liệu từ / tới người dùng. IEEE đã xác định các thông số kỹ thuật nhất định cho mạng LAN không dây, được gọi là IEEE 802.11 bao gồm các lớp liên kết vật lý và dữ liệu.

Ưu điểm của WiFi:

- Sự tiện lợi: WiFi cho phép các thiết bị kết nối với mạng không dây từ bất kỳ đâu trong phạm vi sóng, vì vậy nó rất tiện lợi cho việc truy cập mạng và chia sẻ dữ liệu.
- Tốc độ cao: WiFi có tốc độ truyền dữ liệu nhanh và hiệu quả, cho phép các thiết bị truyền dữ liệu lớn với tốc độ cao.
- Tính linh hoạt: WiFi cho phép nhiều thiết bị kết nối cùng một lúc, và có thể được cấu hình cho nhiều mục đích sử dụng.
- Độ bảo mật cao: WiFi sử dụng các phương pháp bảo mật để bảo vệ dữ liệu khỏi các mối đe dọa từ bên ngoài.

Nhược điểm:

- Phạm vi sóng hạn chế: Vì WiFi hoạt động trên sóng vô tuyến, nên phạm vi sóng của nó có thể bị hạn chế bởi vật cản, khoảng cách và các tín hiệu khác.
- Năng lượng tiêu thụ cao: WiFi yêu cầu năng lượng lớn để hoạt động, do đó, các thiết bị sử dụng WiFi thường tiêu tốn nhiều năng lượng hơn so với các thiết bị khác.
- Độ ổn định thấp: Khi có quá nhiều thiết bị kết nối đến một điểm truy cập duy nhất, sự ổn định của mạng WiFi có thể bị giảm và gây ra các vấn đề về tốc độ truyền dữ liệu và kết nối.

1.3.3. Zigbee

Zigbee là một giao thức mạng không dây, dùng để kết nối các thiết bị lại với nhau. Đây là tiêu chuẩn khu vực mạng lưới cá nhân 802.15.4 của IEEE, đã tồn tại hơn một thập kỷ. Nó được xem là một giải pháp thay thế cho Wi-Fi và Bluetooth của một số ứng dụng bao gồm các thiết bị sử dụng năng lượng thấp mà không cần nhiều băng thông như các hệ thống cảm biến trong nhà thông minh. Zigbee có dải tần là 2.4GHz sử dụng kỹ thuật điều chế BPSK và QPSK như UWB, có 16 kênh RF. Công nghệ

Zigbee 3.0 mới ra gần đây đã giúp cho các thiết bị khác nhau của mỗi hãng nếu được xây dựng trên nền tảng Zigbee 3.0 thì đều có thể tương tác với nhau.

Ưu điểm của Zigbee:

- Tiết kiệm năng lượng: ZigBee tiêu tốn rất ít năng lượng cho nên sẽ giúp tiết kiệm điện tối đa.
- Khả năng mở rộng cực lớn: Các thiết bị cùng hệ thống sẽ có thể kết nối với nhau tạo nên 1 vùng phủ sóng cực lớn, giúp các thiết bị nhà thông minh kết nối với nhau dễ dàng.
- Sử dụng mã hóa AES – 128 mang đến độ bảo mật cao.
- Dễ dàng mở rộng: ZigBee có thể mở rộng tới 65.000 thiết bị trong cùng một hệ thống.

Nhược điểm của Zigbee:

- Không thể phủ rộng hết toàn bộ nhà có diện tích quá rộng, chúng ta sẽ cần một thiết bị ZigBee Repeater để tăng độ phủ sóng.
- Không xuyên tường mạnh được, nếu nhà nhiều phòng thì sẽ bị giảm tín hiệu.

1.3.4. Bluetooth

Bluetooth là một công nghệ không dây giúp các thiết bị truyền dữ liệu qua khoảng cách ngắn. Bluetooth thường được sử dụng để kết nối các thiết bị di động, tai nghe không dây, bàn phím và chuột không dây, thiết bị IoT và nhiều thiết bị khác.

Ưu điểm của Bluetooth:

- Phạm vi ngắn: Bluetooth hoạt động trên khoảng cách ngắn, từ 10 đến 100 mét, do đó nó không ảnh hưởng đến các thiết bị khác trong môi trường xung quanh.
- Tiêu thụ năng lượng thấp: Bluetooth tiêu thụ năng lượng thấp hơn so với WiFi và nhiều công nghệ không dây khác, giúp kéo dài thời lượng pin của thiết bị.
- Tính đa dụng: Bluetooth có thể được sử dụng để kết nối nhiều loại thiết bị, bao gồm điện thoại di động, máy tính bảng, máy tính, thiết bị âm thanh và nhiều thiết bị IoT khác.
- Tính năng tiện ích: Bluetooth cho phép chia sẻ dữ liệu và kết nối các thiết bị một cách đơn giản, không cần sử dụng cáp kết nối.

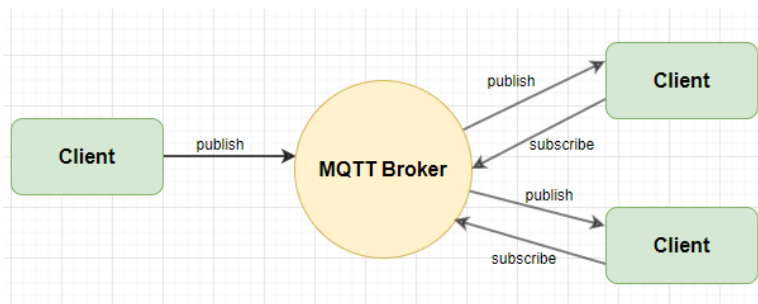
Nhược điểm của Bluetooth:

- Tốc độ truyền dữ liệu chậm: Tốc độ truyền dữ liệu của Bluetooth chậm hơn so với WiFi và một số công nghệ không dây khác.
- Phạm vi truyền tải hạn chế: Phạm vi truyền tải của Bluetooth hạn chế, do đó, các thiết bị phải ở gần nhau để kết nối.

1.4. Tìm hiểu giao thức mạng

1.4.1. MQTT

MQTT là viết tắt của MQ Telemetry Transport. Đây là một giao thức theo dạng publish/subscribe, giao thức cực kì đơn giản và có dung lượng nhẹ, được thiết kế cho các mạng băng thông thấp, độ trễ cao. Nó là một giao thức lý tưởng cho các ứng dụng machine-to-machine (M2M) hoặc trên IoT, và cho các ứng dụng di động có băng thông và năng lượng pin ở mức cao.



Mô hình hoạt động của MQTT được mô tả như trên. Trong hệ thống sử dụng MQTT, các node (client) được kết nối tới một điểm trung gian gọi là broker (server). Mỗi client sẽ đăng ký (subscribe) với một hoặc nhiều topic ví dụ như /home/topic1, /home/topic2. Ngoài ra các client cũng có thể gửi (publish) dữ liệu lên một hoặc một vài topic. Khi một client A publish dữ liệu vào topic1 thì tất cả các client đã subscribe vào topic1 đều nhận được dữ liệu đó.

Giao thức MQTT mang lại nhiều lợi ích khi truy cập dữ liệu IoT, các ưu điểm của MQTT có thể kể đến đó là:

- Truyền thông tin hiệu quả hơn
- Tăng khả năng mở rộng
- Giảm đáng kể tiêu thụ băng thông mạng
- Rất phù hợp cho điều khiển và do thám
- Chi phí thấp
- Rất an toàn, bảo mật
- Được sử dụng trong các ngành công nghiệp dầu khí, các công ty lớn như Amazon, Facebook,...

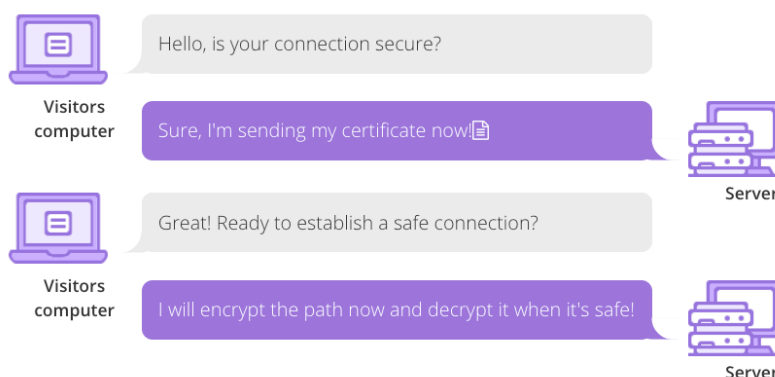
1.4.2. TLS

TLS là viết tắt của Transport Layer Security. Đây là một dạng giao thức bảo mật cung cấp mức độ riêng tư cao, cũng như tính toàn vẹn của dữ liệu khi giao tiếp bằng mạng và internet. TLS là tiêu chuẩn được sử dụng trong việc bảo mật các ứng

dụng web và trang web trên khắp thế giới kể từ khi được giới thiệu vào năm 1999. Nó là sự kế thừa và thay thế cho hệ thống SSL.

Để có thể bảo mật được thông tin, TLS định nghĩa ra chứng chỉ TLS và các private key, public key để mã hóa đường truyền cũng như đảm bảo được người tham gia kết nối. Mục đích của TLS là bảo mật các thông tin nhạy cảm trong quá trình truyền trên internet như thông tin cá nhân, thông tin thanh toán, thông tin đăng nhập. Nó là giải pháp thay thế cho phương pháp truyền thông tin văn bản dạng plain text, văn bản loại này khi truyền trên internet sẽ không được mã hóa, nên việc áp dụng mã hóa vào sẽ khiến các bên thứ ba không xâm nhập được vào thông tin của bạn.

Chứng chỉ TLS hoạt động bằng cách tích hợp key mã hóa vào thông tin định danh. Nó sẽ giúp công ty mã hóa mọi thông tin được truyền mà không bị ảnh hưởng hoặc chỉnh sửa bởi các bên thứ ba.



TLS hoạt động bằng cách sử dụng public và private key, đồng thời các khóa duy nhất của mỗi phiên kết nối (session). Trong phiên kết nối ban đầu, public và private key được dùng để tạo session key, vốn được dùng để mã hóa và giải mã dữ liệu được truyền. Session key được sử dụng trong một khoảng thời gian nhất định và chỉ có thể dùng trong phiên kết nối này.

Khi thực hiện kết nối, máy tính sẽ kiểm tra chứng chỉ và xác nhận những điểm sau đây:

- Certificate là đúng tổ chức có chứng nhận phát hành hay không
- Server đang gửi tin có khớp với thông tin server đang được mô tả trong chứng chỉ hay không. Sau khi xác nhận là đúng server thì an tâm bắt đầu thực hiện truyền tin.

TLS được sử dụng phổ biến nhất với HTTPS, ví dụ rõ nhất đó là mỗi khi sử dụng các trình duyệt web để truy cập một trang web nào đó, các trang sử dụng HTTPS, cụ thể hơn là TLS được đánh dấu bảo mật. Các trang sử dụng HTTP thường được cảnh báo hoặc hạn chế nội dung bởi trình duyệt

1.5. Kết luận chương

Ở chương này, em đã khảo sát các bộ điều khiển trung tâm cùng với đó là tìm hiểu các công nghệ không dây phổ biến trong lĩnh vực Smart Home. Từ đó thấy được một hệ thống nhà thông minh gồm 3 phần chính:

1. Các thiết bị điện thông minh trong nhà.
2. Bộ điều khiển trung tâm để quản lý hệ thống.
3. Cloud lưu trữ thông tin, điều khiển và hiển thị.

Trong phạm vi đề tài của đồ án 2, em sẽ đi vào thiết kế bộ điều khiển trung tâm và một loại thiết bị điện thông minh để demo hoạt động. Ở chương tiếp theo, em sẽ đi vào trình bày tổng thể hệ thống, dựa vào các nguồn lực có sẵn, để từ đó đưa ra các phân tích, lựa chọn phần cứng, phần mềm để xây dựng được bộ điều khiển thông minh.

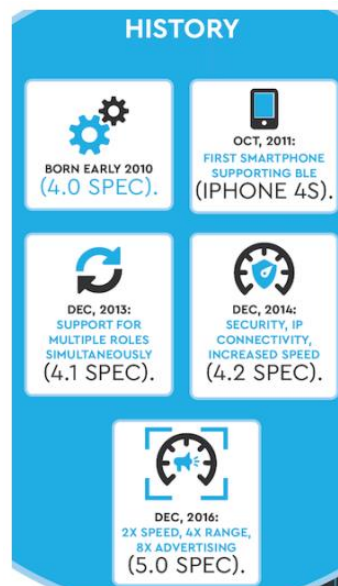
CHƯƠNG 2. THIẾT KẾ HỆ THỐNG

2.1. Mục tiêu

2.2. Bluetooth Low Energy (BLE)

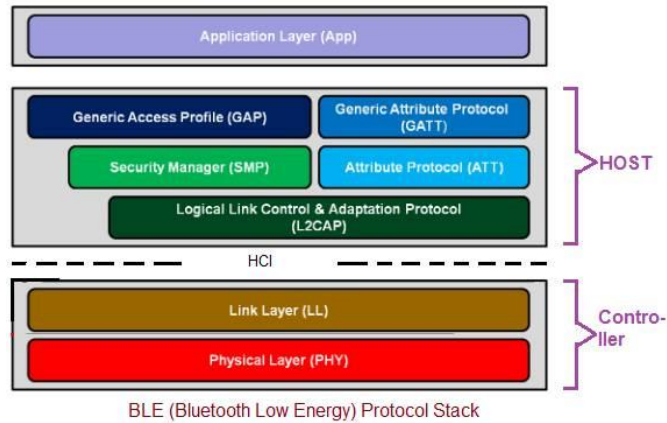
2.2.1. Tổng quan về BLE

Bluetooth Low Energy (BLE) là công nghệ giao tiếp không dây công suất thấp có thể được sử dụng trong một khoảng cách ngắn để cho phép các thiết bị thông minh giao tiếp với nhau. Một số thiết bị bạn tương tác hàng ngày như điện thoại thông minh, đồng hồ thông minh, thiết bị theo dõi thể dục, tai nghe không dây và máy tính đang sử dụng BLE để tạo ra trải nghiệm liền mạch.



Hình 2.1 Lịch sử phát triển của BLE

BLE là một tiêu chuẩn Bluetooth tương đối mới được "định danh" bởi SIG (Bluetooth Special Interest Group) với trọng tâm cải thiện hiệu quả sử dụng năng lượng khi truyền dữ liệu. Công nghệ Bluetooth Low Energy là công nghệ dựa trên sóng radio 2.4GHz, được công bố lần đầu vào năm 2010 trong tên gọi Bluetooth 4.0. Đến nay chuẩn BLE thông dụng đã đạt đến Bluetooth 5.0 với tốc độ hỗ trợ lên tới 2Mbps ở tầng PHY.



Hình 2.2 BLE Stack

Hình trên mô tả cấu trúc của chuẩn BLE. Người lập trình sẽ sử dụng BLE để giao tiếp thông qua các giao thức được cung cấp bao gồm Generic Access Profile (GAP), Attribute Protocol (ATT) và Generic Attribute Profile (GATT).

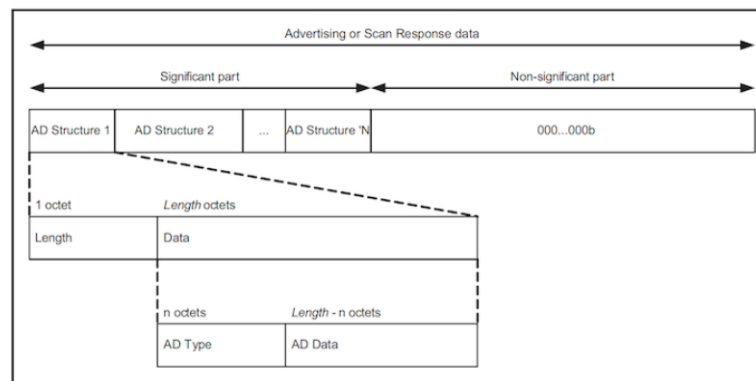
- GAP cung cấp cách để hai thiết bị BLE có thể giao tiếp với nhau bao gồm
 - Các chế độ và các vai trò của thiết bị BLE trong mạng
 - Các thông tin về quá trình advertising và scanning
 - Quá trình thiết lập kết nối
 - Bảo mật
- ATT quy định cách giao tiếp thông tin của hai thiết bị là theo mô hình server và client, cùng với đó định nghĩa cách để server gửi đi các thông tin tới client cũng như cấu trúc của các thông tin đó.
- GATT dựa trên ATT, định nghĩa ba nội dung quan trọng nhất trong BLE mà người lập trình sẽ tiếp xúc rất nhiều xuyên suốt quá trình thiết kế thiết bị BLE:
 - Services
 - Characteristics
 - Profiles

2.2.2. GAP

GAP quy định cách để hai thiết bị có thể biết đến nhau, có được các thông tin cơ bản để quyết định xem có kết nối với nhau hay không. Quá trình sẽ bắt đầu khi một thiết bị phát ra các bản tin và thiết bị còn lại sẽ quét các bản tin đó. Thiết bị phát ra các bản tin sẽ được đặt tên là Peripheral và quá trình phát các bản tin được gọi là advertising. Thiết bị quét các bản tin xung quanh có tên là Central và quá trình đó là quá trình scanning.

- Quá trình advertising sẽ có một số tham số đặc trưng bao gồm:

- Chu kì advertising: được quy định từ 20 mili giây đến 10.24 giây, với độ chia là 625 micro giây. Chu kì advertising cũng cần được lựa chọn kĩ càng, bởi nó sẽ ảnh hưởng trực tiếp đến tuổi thọ pin.
- Bản tin advertising: Trong mỗi chu kì advertising, thiết bị sẽ gửi đi một bản tin với các thông tin phục vụ cho quá trình nhận biết giữa hai thiết bị. Cấu trúc bản tin được mô tả như ở hình 2.9. Dữ liệu được cấu trúc theo TLV (Type – Length – Value), tạm dịch là ba trường kiểu dữ liệu, độ dài và giá trị. Các kiểu dữ liệu phổ biến thường được thêm trong bản tin Advertising là:
 - Local name: chứa tên của thiết bị
 - Tx Power Level: mức năng lượng sử dụng cho việc truyền thông tin, đơn vị dBm
 - Flags: gồm các cờ biểu thị cho các chế độ của thiết bị
 - Service Solicitation: một danh sách của một hoặc nhiều mã UUID đặc trưng cho các service mà thiết bị hỗ trợ. Kiểu dữ liệu này giúp cho thiết bị Central biết được các service mà thiết bị Peripheral hỗ trợ trước khi thiết lập kết nối.
 - Appearance: định nghĩa chức năng của thiết bị ví dụ như điện thoại, cảm biến nhịp tim,... theo chuẩn của [Bluetooth SIG Assigned Numbers](#).



Hình 2.3 Cấu trúc bản tin Advertising

2.2.3. Attribute Protocol (ATT)

ATT định nghĩa ra cấu trúc thông tin mà hai thiết bị cần trao đổi, để hệ thống hóa cũng như dễ dàng hơn trong việc lưu trữ, trao đổi thông tin. Hai thiết bị sử dụng ATT sẽ được gán hai vai trò:

- Server: là thiết bị chứa dữ liệu mà người dùng cần bao gồm cảm biến, vị trí, gia tốc, thời lượng pin Khi được yêu cầu thông tin, server sẽ gửi thông

tin đó đến các thiết bị yêu cầu ví dụ như các Gateway hoặc điện thoại. Ngoài ra, việc gửi thông tin còn có thể thông qua cách Server sẽ tự động gửi đi dữ liệu tới thiết bị đã đăng ký nhận thông báo khi dữ liệu thay đổi từ trước đó. Đó được định nghĩa là notification.

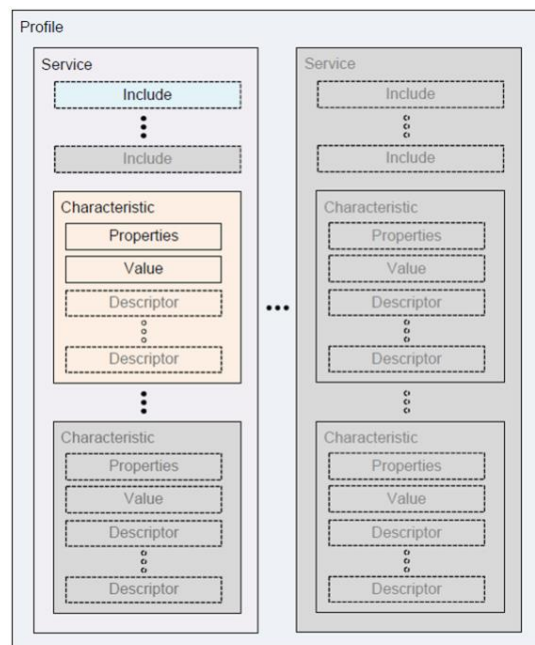
- Client: là thiết bị giao tiếp với server với mục đích đọc dữ liệu, cũng như điều khiển server khi cần thiết. Client cũng là thiết bị đăng ký nhận notification từ phía server từ trước để có thể nhận được dữ liệu gửi từ server sang khi chúng thay đổi.

Các attributes được định danh bởi các yếu tố sau:

- Attribute Type: Các attribute được định danh bởi các UUID (Universally Unique Identifier), có độ dài 16 bits (được quy định bởi Bluetooth SIG) hoặc 128 bits với các attribute do người dùng quy định.
- Attribute Handle: là một giá trị 16 bits mà server gán cho mỗi attribute, giống như một địa chỉ. Giá trị này được client sử dụng để tham chiếu các attributes.
- Attribute Permission: Quy định các hành động có thể làm với attribute đó, ví dụ như đọc, ghi hoặc notify.

2.2.4. Generic Attribute Profile (GATT)

GATT là thuật ngữ sẽ gặp khá nhiều với các lập trình viên BLE, GATT cơ bản dựa trên ATT.



Hình 2.4 Profiles, Services và Characteristics

Hình trên mô tả rõ nhất các cấu trúc dữ liệu của GATT gồm profile, service và characteristic. GATT dựa trên ATT, nên vẫn sẽ có hai vai trò là server và client. Tuy nhiên, một thiết bị có thể chạy song song hai vai trò server và client khi có thể đọc dữ liệu từ một server khác, sau đó gửi dữ liệu đó đi tới một client khác với vai trò một server.

- Service: bao gồm một hoặc nhiều attribute, một trong số đó có thể là characteristic để có thể đáp ứng các chức năng cụ thể của server. Ví dụ, service về pin của SIG bao gồm một characteristic là battery level. Ngoài ra, service còn chứa các attribute khác mà không phải là characteristic, phục vụ việc định nghĩa cũng như các quyền truy cập service.
- Characteristic: là một phần của một service, biểu diễn một phần thông tin mà server muốn chia sẻ tới các client. Characteristic chứa các attribute để định nghĩa các giá trị mà nó giữ:
 - Properties: được biểu diễn bởi một số các bit để định nghĩa các mà các giá trị characteristic có thể được sử dụng như đọc, ghi, ghi không phản hồi, thông báo,...
 - Descriptors: được sử dụng để chứa các thông tin liên quan đến giá trị của các characteristic như các trường sử dụng cho việc đăng ký nhận thông báo từ server, trường về định dạng và đơn vị của giá trị.

Sau khi đã hiểu rõ cách hai thiết bị BLE thiết lập kết nối, trao đổi dữ liệu và cấu trúc dữ liệu, việc lập trình sẽ dựa chủ yếu trên các hoạt động đọc ghi các service, characteristic và descriptor.

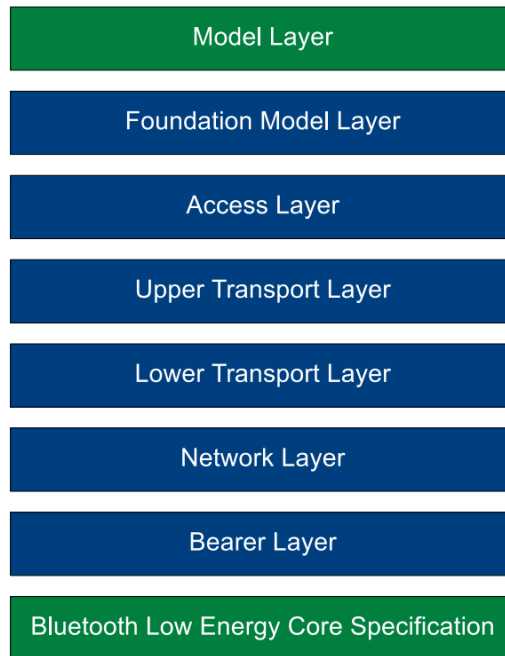
2.3. Bluetooth Mesh

2.3.1. Tổng quan về Bluetooth Mesh

Năm 2017, BLE ra mắt khả năng mạng Mesh. Mạng Mesh cho phép quá trình truyền dữ liệu giữa các node trong mạng một cách tự động và không phân cấp, cho phép chuyển tiếp hiệu quả các message từ node này đến node khác. Nhờ đó công nghệ này là sự thay thế hiệu quả cho các công nghệ mạng truyền thống như mạng hình cây, mạng hình sao. So với các công nghệ hỗ trợ mạng Mesh khác như ZigBee thì

- Bluetooth Mesh không sử dụng Internet Protocol, thay vào đó là được xây dựng ở trên BLE.
- Bluetooth Mesh sử dụng công nghệ có tên là Managed Flooding, không sử dụng công nghệ Routing.
- Bluetooth Mesh có khả năng bảo mật tốt hơn.

2.3.2. Cấu trúc hệ thống mạng Mesh



Hình 2.5 Cấu trúc mạng Bluetooth Mesh

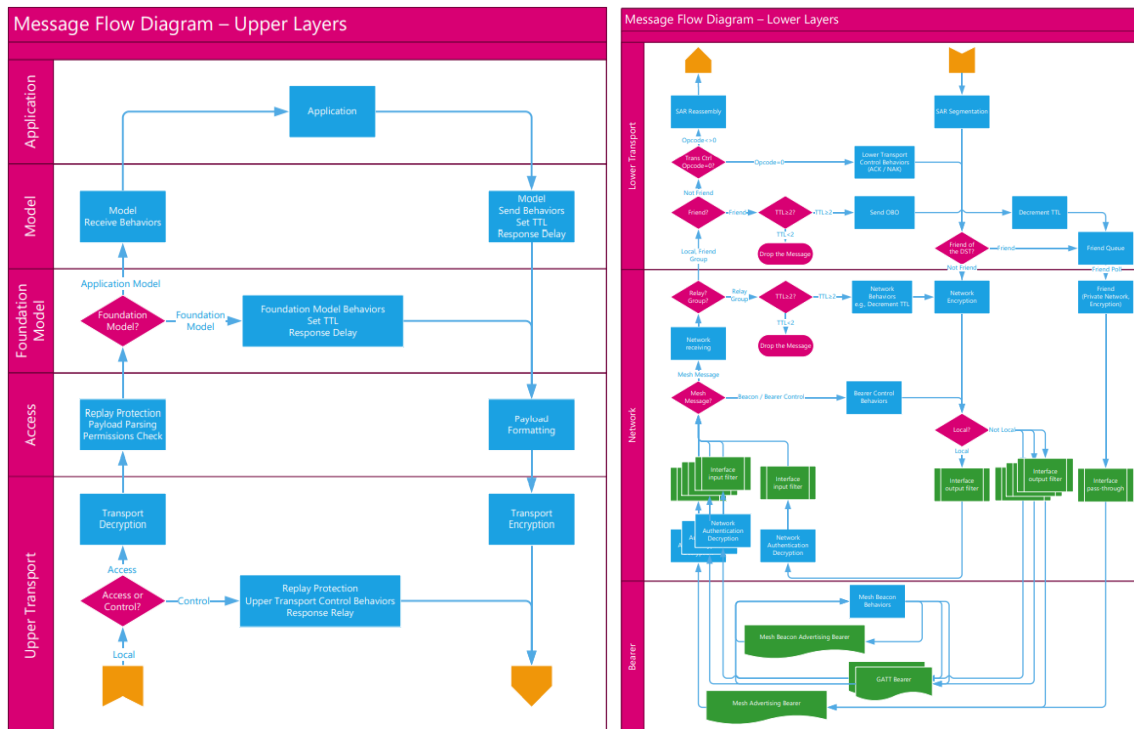
Cấu trúc mạng Bluetooth Mesh gồm có 7 lớp:

1. Model Layer: Định nghĩa các model được sử dụng để tiêu chuẩn hóa các kịch bản hoạt động điển hình. Ví dụ như trong chiếu sáng sẽ có các Lighting Models, với các cảm biến thì có các Sensor Models.
2. Foundation Model Layer: Định nghĩa các state, message và model được yêu cầu để cấu hình và quản lý mạng mesh.
3. Access Layer: Lớp này định nghĩa cách mà các lớp ứng dụng cao hơn có thể sử dụng lớp Upper Transport Layer. Nó định nghĩa các định dạng của dữ liệu, điều khiển các dữ liệu được giải mã và mã hóa ở Upper Transport Layer đồng thời kiểm tra liệu dữ liệu mới nhận được và application key trước khi chuyển tiếp nó đến lớp cao hơn.
4. Upper Transport Layer: Lớp này sẽ mã hóa, giải mã và xác thực dữ liệu, được thiết kế để cung cấp tính bảo mật của các access message. Nó cũng định nghĩa cách mà transport control message được sử dụng để quản lý ở lớp này của các node, bao gồm cả tính năng Friend.
5. Lower Transport Layer: Định nghĩa cách mà các upper transport layer message được phân đoạn và tập hợp lại thành nhiều Lower Transport PDU để chuyển đến các node khác.
6. Network Layer: Xác định cách các transport message được giải quyết đối với một hay nhiều element. Nó xác định định dạng của network message cho phép

Transport PDUs được vận chuyển với Bearer Layer. Network Layer quyết định khi nào sẽ chuyển tiếp các message, khi nào sẽ chấp nhận chúng để xử lý sau đó hoặc từ chối chúng.

7. Bearer Layer: Định nghĩa cách mà các network message được vận chuyển giữa các node. Có 2 loại được định nghĩa là advertising bearer và GATT bearer.

Như đã đề cập thì Bluetooth Mesh được xây dựng ở trên BLE nên sẽ có đủ BLE stack để có thể hoạt động. Bluetooth Mesh khởi tạo trạng thái advertising và scanning để gửi và nhận các message giữa các thiết bị trong mạng.



Hình 2.6 Lưu đồ thuật toán của Bluetooth Mesh

2.3.3. Các khái niệm trong Bluetooth Mesh

Để hiểu rõ về cách Bluetooth Mesh hoạt động thì cần hiểu rõ một số khái niệm sau:

- Mesh node: Là một thiết bị đã gia nhập mạng Bluetooth Mesh. Thiết bị chưa được gia nhập mạng được gọi là “unprovisioned device”. Một khi thiết bị chưa được gia nhập mạng được gia nhập thì sẽ trở thành một node.
- Element: Một node chứa nhiều phần mà chúng có thể được điều khiển độc lập. Ví dụ như một công tắc thông minh thì sẽ có nhiều nút nhấn để bật tắt độc lập. Những phần khác nhau đó trong một node được gọi là các element.

- Model: Một model định nghĩa một vài hoặc tất cả các chức năng của một element. Có 3 loại model chung đó là: server model, client model, control model.
- State:

2.3.4. Quá trình provisioning

Provisioning là quá trình xử lý để một thiết bị có thể gia nhập mạng, được quản lý bởi một thiết bị được gọi là Provisioner. Provisioner cung cấp dữ liệu cấp phát (provisioning data) cho thiết bị chưa được gia nhập mạng để thiết bị đó trở thành một node. Dữ liệu được cung cấp gồm: Network key, Application key, IV index và Unicast address cho mỗi element. AppKey được dùng để bảo mật quá trình giao tiếp ở upper transport layer và Netkey được dùng để bảo mật quá trình giao tiếp ở network layer. AppKey và Netkey được chia sẻ với các node, ngoài ra còn có DevKey. Để thiết bị là một phần của mạng thì nó cần có NetKey. AppKey bị ràng buộc với Netkey, trong một mạng có thể có nhiều hơn một AppKey. Một model có thể bị ràng buộc lên đến 251 AppKey. Điều này được dùng để trong một số ứng dụng như: một công tắc có Generic Onoff Server Model bị ràng buộc 3 AppKey bởi admin, user, guest đều có thể điều khiển công tắc nhưng chỉ có admin có thể cấu hình công tắc nên Configuration Server Model chỉ có admin AppKey ràng buộc với nó.

Để cấp phát cho một thiết bị, một quá trình có tên là Provision Bearer được hình thành giữa Provisioner và thiết bị. Thiết bị có thể được xác định cho provisioner bằng Device UUID của nó.

Quá trình provisioning bao gồm 5 bước:

1. Beaconsing: Thiết bị chưa gia nhập mạng thông báo sự tồn tại để được gia nhập bằng cách gửi các mesh beacon trong advertisement packet.
2. Invitation: Khi provisioner phát hiện được thiết bị chưa gia nhập mạng qua các beacon, nó sẽ gửi một lời mời (provision invite PDU) tới thiết bị đó. Thiết bị sẽ phản hồi lại với thông tin bao gồm:
 - Số lượng element mà thiết bị hỗ trợ.
 -
- 3.

