ZIGBEE

Từ Thị Huyền, Đặng Thị Nguyện, Hoàng Thị Diệu Thuần

1. Khái quát về Zigbee:

1.1 Khái niệm mạng WPAN:

WPAN là mạng vô tuyến cá nhân. Nhóm này bao gồm các công nghệ vô tuyến có vùng phủ nhỏ tầm vài mét đến hàng chục mét tối đa. Các công nghệ này phục vụ mục đích nối kết các thiết bị ngoại vi như máy in, bàn phím, chuột, đĩa cứng, khóa USB,đồng hồ,...với điện thoại di động, máy tính. Các công nghệ trong nhóm này bao gồm: Bluetooth, Wibree, ZigBee, UWB, Wireless USB, EnOcean...

1.2 Khái niệm về Zigbee:

Là tập hợp các giao thức giao tiếp mạng không dây khoảng cách ngắn có tốc độ truyền dữ liệu thấp. Các thiết bị không dây dựa trên chuẩn Zigbee hoạt động trên 3 dãy tần số là 868MHz, 915 MHz và 2.4GHz.

Cái tên Zigbee được xuất phát từ cách truyền thông tin của các con ong mật đó là kiểu “zig-zag” của loài ong “honey-Bee”. Cái tên Zigbee cũng được ghép từ 2 từ này.

Với những đặc điểm chính :

- Tốc độ truyền dữ liệu thấp 20-250Kbps
- Sử dụng công suất thấp, ít tiêu hao điện năng
- Thời gian sử dụng pin rất dài
- Cài đặt, bảo trì dễ dàng
- Độ tin cậy cao
- Có thể mở rộng đến 65000 node
- Chi phí đầu tư thấp.

Tốc độ dữ liệu là 250kbps ở dải tần 2.4 GHz(toàn cầu), 40 kbps ở dải tần 915 MHz (Mỹ ,Nhật) và 20kbps ở dải tần 868 MHz (Châu Âu)

1.3 Lịch sử phát triển:

Mạng Zigbee được hình thành năm 1998 khi các kỹ sư công nghệ nhận thấy Wifi và Bluetooth không thích hợp với nhiều ứng dụng. Tháng 5 năm 2003, tiêu chuẩn IEEE 802.15.4 được hoàn thành. Tháng 10 năm 2004, Liên minh Zigbee ra đời. Đây là hiệp hội các công ty làm việc cùng nhau để cho phép và kiểm soát các sản phẩm mạng không

dây tốc độ thấp, chi phí thấp, ít tiêu hao năng lượng và có tính bảo mật cao. Là một tổ chức độc lập và hợp tác phi lợi nhuận. Nó tạo ra các tiêu chuẩn kỹ thuật cho Zigbee, cấp các chứng nhận, phát triển thương hiệu, thị trường.

Các phiên bản Zigbee lần lượt ra đời từ đó đến nay:

- Ngày 11/12/2004, phiên bản đầu tiên ra đời: Zigbee 2004. Cũng trong thời gian này điện thoại Zigbee đầu tiên trên thế giới được giới thiệu với những tính năng như điều khiển các thiết bị điện gia dụng, theo dõi nhiệt độ, độ ẩm và hệ thống báo động.

- Tháng 12/2006, Zigbee 2006 ra đời.

- Năm 2007, Zigbee PRO ra đời với những tính năng vượt trội hơn.

1.4 So sánh Zigbee với BlueTooth, Wifi:

	Zigbee™	Wifi	Bluetooth
Tần số	868MHz,915MHz, 2.4 GHz	2.4 GHz	2.4 GHz, 5 GHz
Data rate	20-250Kbps	1-100Mbps	1-3Mbps
Khoảng cách	10-100m	30-100m	2-10m

So sánh Zigbee – Wifi - BlueTooth

Zigbee cho phép truyền thông tin tới nhiều thiết bị cùng lúc (mesh network) thay vì chỉ có 2 sản phẩm tương tác với nhau như Bluetooth và Wibree. Phạm vi hoạt động của Zigbee đang được cải tiến từ 75 mét lên đến vài trăm mét.

Công nghệ này đòi hỏi năng lượng thấp hơn Bluetooth, nhưng tốc độ chỉ đạt 256 Kb/giây, đồng thời Zigbee sử dụng rộng hơn trong các mạng mắt lưới rộng hơn là sử dụng công nghệ Bluetooth. Phạm vi hoạt động của nó có thể đạt từ 10 – 75m trong khi đó Bluetooth chỉ có 10 mét trong trường hợp không có khuếch đại .

2. Ứng dụng:

Năng lượng thông minh: là tiêu chuẩn hàng đầu thế giới cho các sản phẩm tương thích mà theo dõi, kiểm soát, thông báo và tự động hóa việc cung cấp và sử dụng năng lượng nước. Nó giúp tạo ra ngôi nhà xanh hơn bằng cách cho người tiêu dùng những thông tin và tự động hóa cần thiết để giảm mức tiêu thụ của họ một cách dễ dàng và tiết kiệm tiền.

Tiêu chuẩn này hỗ trợ các nhu cầu đa dạng của hệ sinh thái toàn cầu, các nhà sản xuất sản phẩm và những dự án của chính phủ để đáp ứng nhu cầu năng lượng và nước trong tương lai.

Zigbee điều khiển từ xa: cung cấp một tiêu chuẩn toàn cầu tiên tiến và dễ sử dụng điều khiển từ xa RF hoạt động non-line-of-sight, hai chiều, còn phạm vi sử dụng và tuổi thọ pin mở rộng. Nó được thiết kế cho một loạt các thiết bị rạp hát tại nhà, các hộp set-top, thiết bị âm thanh khác.

Điều khiển từ xa ZigBee giải phóng người tiêu dùng từ chỉ điều khiển từ xa ở các thiết bị. Nó cung cấp cho người tiêu dùng linh hoạt hơn, cho phép kiểm soát các thiết bị từ phòng gần đó và vị trí của các thiết bị hầu như bất cứ nơi nào - bao gồm cả phía sau gỗ, tường, trang trí nội thất hoặc thủy tinh.

Zigbee nhà thông minh: ZigBee nhà thông minh cung cấp một tiêu chuẩn toàn cầu cho các sản phẩm tương thích cho phép nhà thông minh có thể kiểm soát thiết bị, chiếu sáng, quản lý môi trường năng lượng, và an ninh, cũng như mở rộng để kết nối với các mạng ZigBee. Nhà thông minh cho phép người tiêu dùng tiết kiệm tiền, cảm thấy an toàn hơn và tận hưởng một loạt các tiện nghi dễ dàng và ít tốn kém để duy trì.

Zigbee nhà thông minh hỗ trợ một hệ sinh thái đa dạng của các nhà cung cấp dịch vụ và các nhà sản xuất sản phẩm khi họ phát minh ra sản phẩm cần thiết để tạo ra ngôi nhà thông minh. Những sản phẩm này là lý tưởng để xây dựng mới thêm các thị trường, và rất dễ sử dụng, duy trì và cài đặt.

Tất cả sản phẩm Zigbee nhà thông minh được chứng nhận để thực hiện. Nhiều công ty đổi mới đã đóng góp chuyên môn của họ vào tiêu chuẩn này, bao gồm Phillips, Control4 và Texas Instruments.

Zigbee chăm sóc sức khỏe: là theo dõi bệnh nhân tại nhà. Ví dụ, huyết áp và nhịp tim của một bệnh nhân được đo bởi các thiết bị đeo trên người. Bệnh nhân mang một thiết bị Zigbee tập hợp các thông tin liên quan đến sức khỏe như huyết áp và nhịp tim. Sau đó dữ liệu được truyền không dây đến một máy chủ địa phương, có thể là một máy tính cá nhân đặt trong nhà bệnh nhân, nơi mà việc phân tích ban đầu được thực hiện. Cuối cùng, thông tin quan trọng được chuyển tới y tá của bệnh nhân hay nhân viên vật lý trị liệu thông qua Internet để phân tích sâu hơn. Chăm sóc sức khỏe hàng đầu và công ty đang hỗ trợ công nghệ cho sự phát triển của ZigBee Chăm sóc sức khỏe, bao gồm Motorola, Phillips, Freescale Semiconductor, Awarepoint và công nghệ RF.

Zigbee xây dựng tự động:

ĐIỀU KHIỂN:

* Tích hợp và tập trung quản lý chiếu sáng, sưởi ấm, làm mát, an ninh.
* Tự động kiểm soát nhiều hệ thống để cải thiện tính linh hoạt và an ninh.

BẢO TỒN

* Giảm chi phí năng lượng thông qua quản lý tối ưu hóa HVAC.
* Phân bổ chi phí tiện ích một cách công bằng dựa trên tiêu thụ thực tế.

LINH HOẠT

* Cấu hình lại hệ thống chiếu sáng một cách nhanh chóng để tạo ra không gian làm việc thích nghi.
* Mở rộng và nâng cấp xây dựng cơ sở hạ tầng.

AN TOÀN

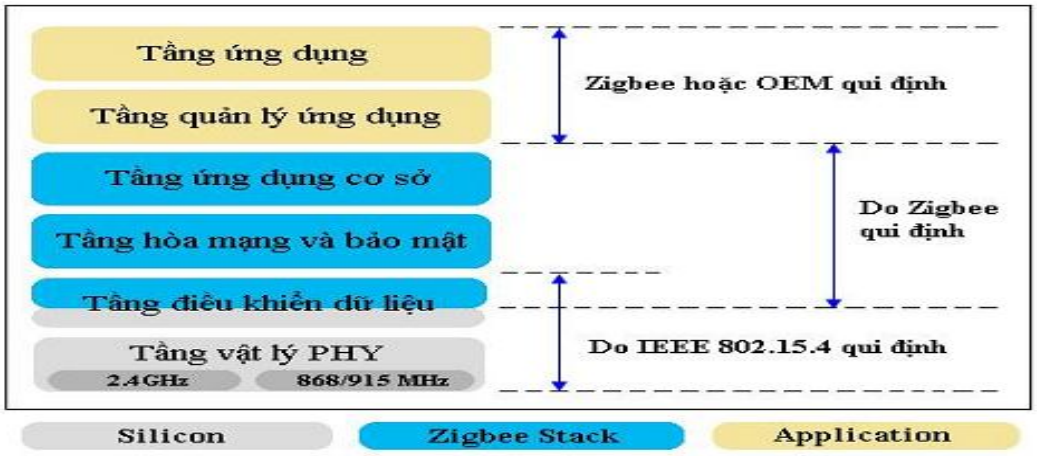
* Mạng và tích hợp dữ liệu từ các điểm kiểm soát truy cập nhiều chiều.
* Triển khai mạng lưới giám sát không dây để tăng cường bảo vệ vòng ngoài.

Zigbee dịch vụ viễn thông: ZigBee Dịch vụ viễn thông cung cấp một tiêu chuẩn toàn cầu cho các sản phẩm tương thích cho phép một loạt các dịch vụ giá trị gia tăng, bao gồm giao thông, chơi game di động, dịch vụ dựa trên địa điểm, thanh toán di động an toàn, quảng cáo di động, thanh toán khu vực, tiếp cận văn phòng di động kiểm soát, thanh toán, và peer-to-peer dịch vụ chia sẻ dữ liệu.

Điều này tiêu chuẩn duy nhất cung cấp một cách hợp lý và dễ dàng để giới thiệu dịch vụ sáng tạo mới mà tất cả mọi người liên lạc hầu như sử dụng điện thoại di động và thiết bị cầm tay điện tử khác. Nó cung cấp nhiều dịch vụ giá trị gia tăng cho các nhà khai thác mạng điện thoại di động, nhà bán lẻ, các doanh nghiệp, và chính phủ. Người tiêu dùng có thể sử dụng điện thoại di động của họ để trả cho các sản phẩm và dịch vụ, tạo ra game riêng của họ và mạng lưới truyền thông, nhận được giảm giá hoặc phiếu giảm giá từ các nhà bán lẻ, và có được hướng dẫn hoặc thông tin về không gian công cộng với GPS.
ZigBee Dịch vụ viễn thông hỗ trợ các nhà sản xuất sản phẩm, các nhà khai thác điện thoại mạng di động, các doanh nghiệp và chính phủ khi họ tìm cách mới để tương tác với công chúng. Tất cả các sản phẩm ZigBee Dịch vụ viễn thông được chứng nhận để thực hiện.
Các công ty viễn thông hàng đầu, các nhà sản xuất sản phẩm và công ty công nghệ dẫn sự phát triển của tiêu chuẩn này, bao gồm cả Phillips, Telecom Italia, Telefonica, OKI, Huawei, Motorola và Texas Instruments.

3. Mô hình giao thức của Zigbee/IEEE802.15:

Đây là công nghệ xây dựng và phát triển các lớp ứng dụng và lớp mạng trên nền tảng là 2 tầng PHY và MAC theo chuẩn IEEE 802.15.4. Nó thừa hưởng được tính tin cậy, đơn giản, tiêu hao ít năng lượng và khả năng thích ứng cao với môi trường mạng.



Hình 2.1: Mô hình giao thức của ZigBee

***3.1 Tầng vật lý*:** cung cấp 2 dịch vụ chính là dịch vụ dữ liệu (PHY) và dịch vụ quản lý (PHY).

- Dịch vụ dữ liệu (PHY) điều khiển việc thu phát của khối dữ liệu PPDU thông qua kênh sóng vô tuyến vật lý.

- Các tính năng của tầng vật lý là: Sự kích hoạt hoặc giảm kích hoạt hoặc giảm của bộ phận nhận sóng , phát hiện năng lượng , chọn kênh , chỉ số đường truyền , giải phóng kênh truyền, thu và phát các gói dữ liệu qua môi trường truyền.

Chuẩn IEEE 802.15.4 định nghĩa 3 dải tần số khác nhau

PHY (MHz)	Băng tần(MHz)	Tốc độ chip (kchips/s)	Điều chế
868	868-868.6	300	BPSK
915	902-928	600	BPSK
2450	2400-2486.5	2000	QPSK

Có tất cả 27 kênh truyền trên các giải tần số khác nhau theo bảng mô tả sau:

Tần số trung tâm(MHz)	Số lượng kênh (N)	kênh	Tần số trung tâm(MHz)
868	1	0	868.3
915	10	1-10	906 + 2(k-1)
2450	16	11-26	5(k-11)

<u>Các thông số kỹ thuật trong tầng vật lý của IEEE 802.15.4:</u>

a. *Chỉ số ED (energy detection):*

Chỉ số ED được đo đạc bởi bộ thu ED. Chỉ số này sẽ được tầng mạng sử dụng như là 1 bước trong thuật toán chọn kênh. Nó là kết quả của sự ước lượng công suất năng lượng của tín hiệu nhận được. Nó không có vai trò trong việc giải mã hay nhận dạng tín hiệu truyền trong kênh này. Thời gian phát hiện và xử lý tương đương 8 symbol.

Giá trị nhỏ nhất của ED (=0) khi mà công suất nhận được ít hơn mức +10 db so với lý thuyết. Độ lớn của khoảng công suất nhận được để hiển thị chỉ số ED tối thiểu là 40db ± 6db.

b. Chỉ số lưu lượng đường truyền (LQI):

Chỉ số này đặc trưng cho chất lượng gói tin nhận được. cùng với chỉ số ED, nó đánh giá tỷ số tín trên tạp SNR. Giá trị của nó được giao cho tầng mạng và tầng ứng dụng xử lý.

c. Chỉ số đánh giá kênh truyền :sử dụng để xem kênh truyền rỗi hay bận. Có 3 phương pháp:

CCA1: "Năng lượng vượt ngưỡng", CCA sẽ thông báo kênh truyền bận.

CCA2: "Cảm biến sóng mang", CCA sẽ thông báo kênh truyền bận khi nhận ra tín hiệu có đặc tính trải phổ và điều chế của IEEE 802.15.4.

CCA3: "Cảm biến sóng mang kết hợp với năng lượng vượt ngưỡng", CCA sẽ thông báo kênh truyền bận khi dò ra tín hiệu có đặc tính trải phổ và điều chế của IEEE 802.15.4 với năng lượng vượt ngưỡng ED.

d. Khung tin PPDU:

Mỗi khung tin PPDU bao gồm các trường thông tin:

. SHR : đồng bộ thiết bị thu và chốt chuỗi bit.

. PHR : chứa thông tin độ dài khung.

. PHY payload: chứa khung tin của tầng MAC.

3.2 Tầng điều khiển dữ liệu Zigbee/IEEE 802.15.4 MAC:

Cung cấp 2 dịch vụ là dịch vụ dữ liệu MAC và quản lý MAC.

Dịch vụ dữ liệu MAC có nhiệm vụ quản lý việc thu phát của khối MPDU (giao thức dữ liệu MAC) thông qua dịch vụ dữ liệu PHY.

Nhiệm vụ của tầng MAC là quản lý việc phát thông tin báo hiệu beacon, định dạng khung tin để truyền đi trong mạng, điều khiển truy nhập kênh, quản lý khe thời gian GTS, điều khiển kết nối và giải phóng kết nối, phát khung Ack.

3.2.1 Cấu trúc siêu khung:

LR-WPAN cho phép sử dụng cấu trúc siêu khung. Mỗi siêu khung được giới hạn bởi từng mạng và được chia thành 16 khe như nhau. Cột mốc báo hiệu dò đường beacon được gửi đi trong khe đầu tiên của mỗi siêu khung, nếu 1 PAN coordinator không muốn sử dụng siêu khung thì nó

phải dừng việc phát mốc beacon. Mốc này có nhiệm vụ đồng bộ các thiết bị đính kèm, nhận dạng PAN và chứa nội dung mô tả cấu trúc siêu khung.

Siêu khung có 2 phần:

- Phần "nghỉ": PAN coordinator không giao tiếp với các thiết bị trong mạng PAN, và làm việc ở các node công suất thấp.

- Phần "hoạt động": gồm 2 giai đoạn là giai đoạn tranh chấp truy cập (CAP) và giai đoạn tranh chấp tự do (CFP), giai đoạn tranh chấp trong mạng chính là khoảng thời gian tranh chấp giữa các trạm để có cơ hội dùng 1 kênh truyền.

Bất kỳ 1 thiết bị nào muốn liên lạc trong thời gian CAP đều phải cạnh tranh với các thiết bị khác bằng cách sử dụng kỹ thuật CSMA-CA. Ngược lại, CFD gồm có các GTSs, các khe thời gian GTS này thường xuất hiện ở cuối siêu khung tích cực mà siêu khung này được bắt đầu ở khe sát ngay sau CAP. PAN coordinator có thể định vị được 7 trong số các GTSs, và mỗi 1 GTS chiếm nhiều hơn 1 khe thời gian.

- *Khung CAP:*

CAP được phát ngay sau mốc beacon và kết thúc trước khi phát CFP. Nếu độ dài của phần CFP=0 thì CAP sẽ kết thúc tại cuối của siêu khung.

Tất cả các khung tin ngoại trừ khung Ack và các khung dữ liệu phát ngay sau khung Ack trong lệnh yêu cầu mà chúng được phát trong CAP sẽ được sử dụng thuật toán CSMA-CA để truy cập kênh. Khung chứa lệnh điều khiển MAC sẽ được phát trong phần CAP.

- *Khung CFP:*

Phần CFP sẽ được phát ngay sau CAP và kết thúc trước khi phát beacon của xung kế tiếp. Kích thước của CFP do tổng độ dài các khe GTSs được cấp phát bởi bộ điều phối mạng PAN quyết định.

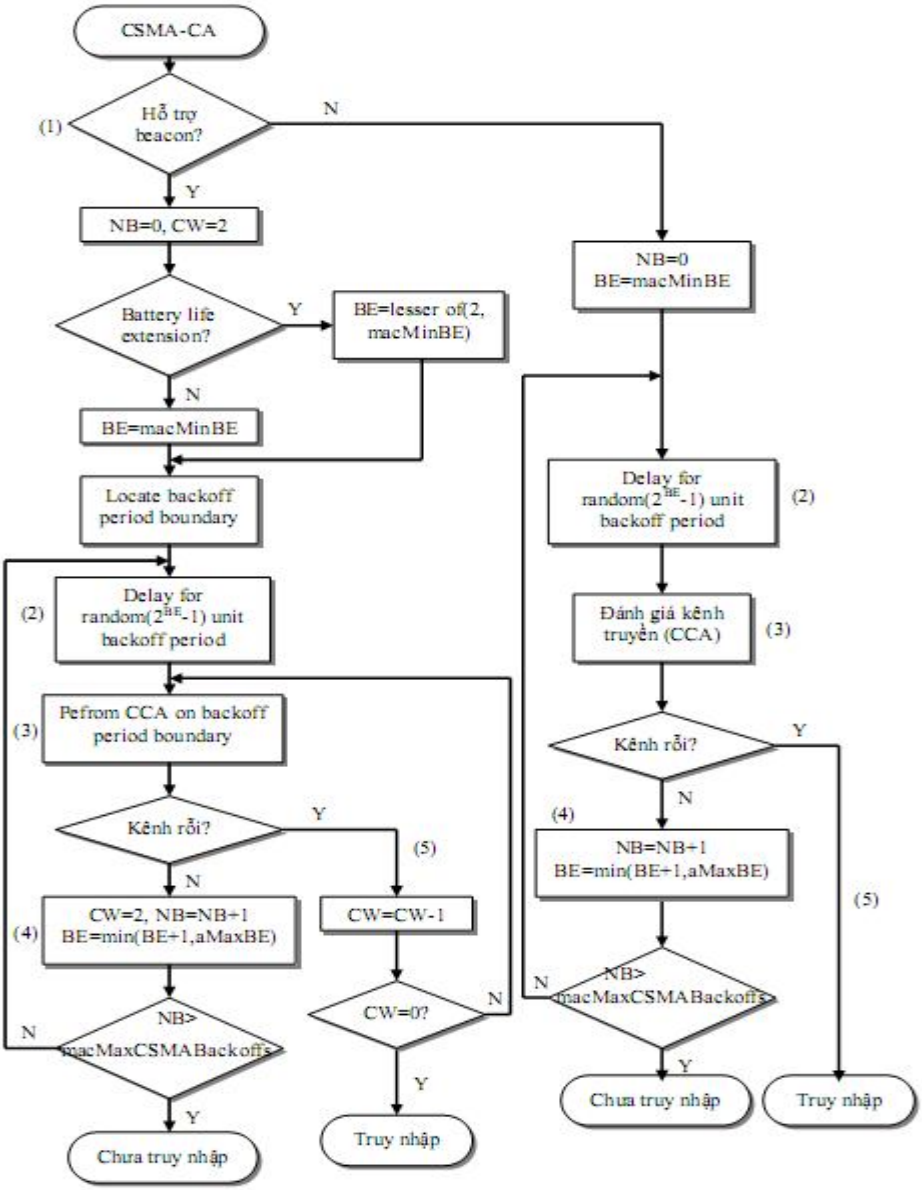
CFP không sử dụng thuật toán CSMA-CA để truy cập kênh

Khoảng cách giữa 2 khung(IFS)

Là khoảng thời gian cần thiết để tầng PHY xử lý 1 gói tin nhận được. Độ dài của nó phụ thuộc vào kích thước của khung vừa được truyền đi.

3.2.2 Thuật toán tránh xung đột đa truy cập sử dụng cảm biến sóng mang CSMA-CA:

Đây là phương pháp tránh xung đột đa truy cập nhờ vào cảm biến sóng. Các node mạng sẽ lắng nghe tín hiệu thông báo trước khi truyền. Nó tránh xung đột bằng cách mỗi node sẽ phát tín hiệu về yêu cầu truyền trước rồi mới truyền thật sự.



Hình 2.7 Lưu đồ thuật toán

3.2.3 Các mô hình truyền dữ liệu:

Có 3 mô hình :từ thiết bị điều phối mạng PAN coordinator tới thiết bị thường, ngược lại, và giữa các thiết bị cùng loại.

3.2.4 Định dạng khung tin MAC:

Mỗi khung gồm các thành phần:

. Đầu khung MHR (MAC header): gồm các trường thông tin về điều khiển khung tin, số chuỗi, và trường địa chỉ.

. Tải trọng khung (MAC payload): chứa thông tin chi tiết về kiểu khung. Khung tin của bản tin xác nhận Ack không có phần này.

. Cuối khung MFR(MAC footer) chứa chuỗi kiểm tra khung FCS.

3.3. Tầng mạng của Zigbee /IEEE 802.15.4:

Dịch vụ mạng:

Tầng vật lý trong mô hình giao thức Zigbee được xây dựng dựa trên tầng điều khiển dữ liệu. Một mạng có thể hoạt động cùng các mạng khác hoặc riêng biệt. Tầng vật lý phải đảm nhận các chức năng là:

- Thiết lập 1 mạng mới.
- Tham gia làm thành viên của 1 mạng đang hoạt động hoặc là tách ra khỏi mạng khi đang là thành viên của 1 mạng nào đó.
- Cấu hình thiết bị mới như hệ thống yêu cầu, gán địa chỉ cho thiết bị mới tham gia vào mạng.
- Đồng bộ hóa các thiết bị trong mạng để có thể truyền tin mà không bị tranh chấp, nó thực hiện đồng bộ hóa này bằng gói tin thông báo beacon.
- Bảo mật: gán các thông tin bảo mật vào gói tin và gửi xuống tầng dưới.
- Định tuyến, giúp gói tin có thể đến được đúng tin mong muốn. Có thể nói rằng thuật toán Zigbee là thuật toán định tuyến phân cấp sử dụng bảng định tuyến phân cấp tối ưu được áp dụng từng trường hợp thích hợp.

3.4 Tầng ứng dụng của Zigbee/IEEE 802.15.4:

Chức năng của tầng ứng dụng application Framework của Zigbee là:

- Dò tìm ra xem có nốt hoặc thiết bị nào khác đang hoạt động trong vùng phủ sóng của thiết bị đang hoạt động hay không.
- Duy trì kết nối, chuyển tiếp thông tin giữa các nốt mạng.

Chức năng của application Profiles là:

- Xác định vai trò của các thiết bị trong mạng.
- Thiết lập hoặc trả lời yêu cầu kết nối.
- Thành lập các mối quan hệ giữa các thiết bị trong mạng

4. Phân loại thiết bị:

Trước hết chúng ta tìm hiểu các thuật ngữ:

- Full-function devices (FFDs): là những thiết bị hỗ trợ đầy đủ các chức năng theo chuẩn của IEEE 802.15.4 và có thể đảm nhận bất cứ vai trò nào trong hệ thống. FFD có thể hoạt động trong ba trạng thái: là điều phối viên của toàn mạng PAN, hay là điều phối viên của một mạng con hoặc đơn giản chỉ là một thành viên trong mạng, bổ sung bộ nhớ và sức mạnh tính toán làm cho nó trở thành lý tưởng trong chức năng router mạng hoặc nó có thể sử dụng trong các thiết bị mạng cạnh (nơi mạng chạm thế giới thực).
- Reduced-function devices (RFDs): là những thiết bị giới hạn một số chức năng (chỉ giao tiếp được với FFDs, áp dụng cho các ứng dụng đơn giản, không yêu cầu gửi lượng lớn dữ liệu như tắt, mở đèn) với chi phí thấp hơn và phức tạp hơn.

Một mạng tối thiểu phải có một thiết bị FFD, một FFD có thể làm việc với nhiều RFD hay nhiều FFD trong khi một RFD chỉ có thể làm việc với một FFD.

Có 3 loại thiết bị Zigbee:

4.1 Zigbee Coordinator (ZC): thiết bị này hình thành và duy trì kiến trúc mạng tổng thể, đồng thời nó điều khiển và giám sát mạng, lưu trữ các thông tin về mạng. Vì vậy nó yêu cầu bộ nhớ và sức mạnh tính toán lớn nhất. Nó là thiết bị FFD.

4.2 Zigbee Router (ZR): một thiết bị thông minh có khả năng mở rộng tầm bao phủ của mạng bằng cách định tuyến và cung cấp tuyến dự phòng hoặc phục hồi những tuyến bị nghẽn, hoạt động như một router trung

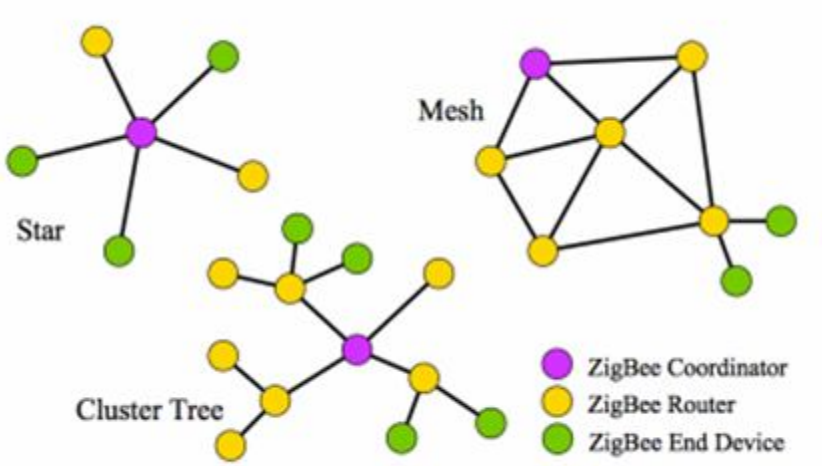
gian, truyền dữ liệu giữa các thiết bị khác nhau. Nó có thể kết nối với ZC, ZR và cả ZED. Nó cũng là thiết bị FFD.

4.3 Zigbee End Device (ZED): đó là các nút cảm biến có các thông tin từ môi trường. Nó có thể nhận tin nhưng không thể chuyển tiếp tin, kết nối được với ZC và ZR nhưng không thể kết nối với nhau. Nó có thể là FFD hoặc RFD.

ZigBee Coordinator và ZigBee EndDevice

5. Các kiểu hình mạng Zigbee:

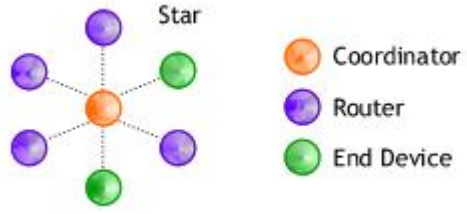
Các node mạng trong một mạng Zigbee có thể liên kết với nhau theo cấu trúc mạng hình sao (Star), lưới (Mesh), cấu trúc bó cụm hình cây (Tree). Sự đa dạng về cấu trúc mạng này cho phép công nghệ Zigbee được ứng dụng một cách rộng rãi.



Các kiểu mạng của Zigbee

5.1 Cấu trúc mạng hình sao (Star topology): còn được gọi là point-to-point (one-hop)

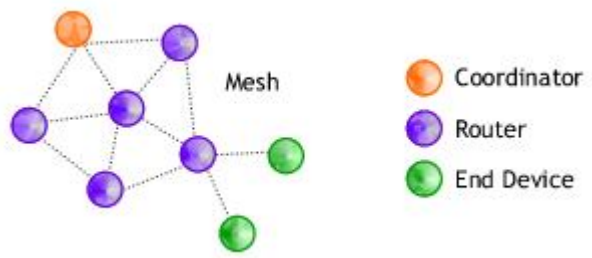
Đối với loại mạng này một kết nối được thành lập bởi các thiết bị với một thiết bị được lập trình để điều khiển trung tâm điều khiển được gọi là bộ điều phối mạng PAN. Sau khi FFD được kích hoạt lần đầu tiên nó có thể tạo nên một mạng độc lập và trở thành một bộ điều phối mạng PAN. Mỗi mạng hình sao đều phải có một chỉ số nhận dạng cá nhân được gọi là PAN ID (PAN identifier), chỉ số này là duy nhất mà không được sử dụng bởi bất kỳ mạng khác trong phạm vi ảnh hưởng của nó – khu vực xung quanh thiết bị mà sóng radio của nó có thể giao tiếp thành công với các thiết bị phát radio khác. Nói cách khác nó đảm bảo rằng PAN ID mà nó chọn không được sử dụng bởi bất kỳ mạng nào gần đấy, cho phép mạng này có thể hoạt động một cách độc lập. Khi đó cả FFD và RFD đều có thể kết nối với bộ điều phối mạng PAN. Các node trong mạng PAN chỉ có thể kết nối với bộ điều phối mạng PAN vì thế mạng này là mạng tập trung, mọi node mạng đều phải thông qua ZC nên ZC sẽ tiêu tốn nhiều năng lượng hơn các node mạng khác và mạng có tầm phủ sóng nhỏ (trong vòng bán kính 100m). Nên sử dụng cấu trúc hình sao này cho các ứng dụng có tầm nhỏ như tự động hóa nhà, thiết bị ngoại vi cho máy tính, đồ chơi và games.



5.2 Cấu trúc mạng lưới (Mesh topology): còn được gọi là peer-to-peer (multi-hop)

Kiểu cấu trúc mạng này cũng có một bộ điều phối mạng PAN. Thực chất đây là kết hợp của hai kiểu cấu trúc mạng hình sao và mạng ngang hàng, ở cấu trúc mạng này thì một thiết bị A có thể tạo kết nối với bất kỳ thiết bị nào khác miễn là thiết bị đó nằm trong phạm vi phủ sóng của thiết bị A. Mạng mắt lưới không tập trung cao độ như mạng hình sao, thay vào đó là các kết nối điểm - điểm nằm trong tầm phủ sóng của các điểm mạng. Mạng hoạt động theo chế độ ad-hoc cho phép chuyển tiếp nhiều chặng qua trung gian là các ZR, điều này đồng nghĩa với việc phải có thuật toán định tuyến để tím ra các đường dẫn tối ưu nhất. Mạng này có thể hoạt động trong tầm rất rộng lớn, tuy nhiên rất khó khăn để giảm thiểu phức tạp trong việc liên kết bất cứ điểm - điểm nào trong mạng do đó khó có thể đảm bảo thời gian truyền tối thiểu được. Các ứng dụng của cấu trúc này có thể ứng dụng trong đo lường và điều khiển, mạng cảm biến không dây, theo dõi cảnh báo và kiểm kê (cảnh báo cháy rừng)...ZR hoạt động như một điều phối viên trong khu vực hoạt động của nó để mở rộng giao tiếp ở cấp độ mạng.

Trong mạng ngang hàng, mỗi thiết bị có thể giao tiếp với thiết bị khác nếu các thiết bị được đặt đủ gần để tạo thành công đường dẫn liên kết. Bất kỳ FFD nào trong mạng ngang hàng có thể đóng vai trò là một điều phối mạng PAN. Một cách để quyết định thiết bị nào sẽ là điều phối mạng PAN là lựa ra thiết bị FFD đầu tiên bắt đầu việc giao tiếp như là một điều phối mạng PAN. Một RFD có thể là một phần của mạng và chỉ giao tiếp với một thiết bị đặc biệt trong mạng (ZC hoặc ZR).



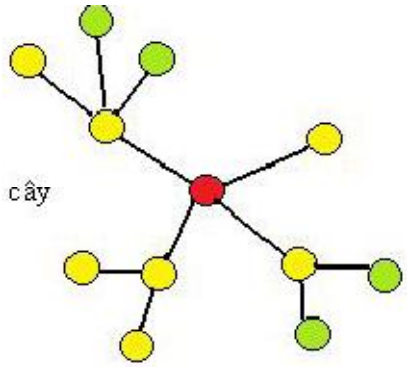
5.3 Cấu trúc mạng hình cây (Cluster Tree topology):

Cấu trúc này là một dạng đặc biệt của cấu trúc mắt lưới trong đó đa số thiết bị là FFD và một RFD có thể kết nối vào hình cây như một node rời rạc ở điểm cuối của nhánh cây. Bất kỳ một FFD nào cũng có thể hoạt

động như là một coordinator và cung cấp tín hiệu đồng bộ cho các thiết bị và các coordinator khác vì thế mà cấu trúc mạng kiểu này có quy mô phủ sóng và tầm mở rộng cao. Trong loại cấu hình này mặc dù có thể có nhiều coordinator nhưng chỉ có duy nhất một bộ điều phối mạng PAN. Các ZR định hình các nhánh và tiếp nhận tin. Các ZED hoạt động như những chiếc lá và không tham gia vào việc định tuyến.

Bộ điều phối mạng PAN tạo ra nhóm đầu tiên bằng cách tự bầu ra người lãnh đạo cho nhóm của mình và gán cho người lãnh đạo đó một chỉ số nhận dạng cá nhân đăc biệt gọi là CID-0 (cluster identifier) bằng cách tự thành lập CLH (cluster head) bằng CID-0. Nó chọn một PAN identifier rỗi và phát khung tin quảng bá nhận dạng tới các thiết bị lân cận. Thiết bị nào nhận được khung tin này có thể yêu cầu kết nối vào mạng CLH. Nếu bộ điều phối viên mạng PAN đồng ý cho thiết bị đó kết nối thì nó sẽ ghi tên thiết bị đó vào danh sách. Cứ thế thiết bị mới kết nối này lại trở thành CLH của nhánh cây mới và bắt đầu phát quảng bá định kỳ để các thiết bị khác có thể kết nối vào mạng. Từ đó hình thành được các CLH1, CLH2...

Mạng hình cây hứa hẹn sẽ đem về ưu điểm của hai mạng trên: mạng hình sao (khả năng đồng bộ, đường truyền tin cậy nhờ vào chế độ GTS) và mạng mắt lưới (co giãn về khoảng cách địa lý, tầm hoạt động rất rộng).



6.An ninh Zigbee:

Đặc điểm:

An ninh Zigbee dựa trên nền tảng là một thuật toán AES 128- bit, thêm vào là những mô hình bảo mật được cung cấp bởi IEEE802.15.4, dịch vụ bảo mật của Zigbee bao gồm các phương pháp cho khóa cơ sở, khóa vận chuyển, khóa thiết bị quản lý và khóa bảo vệ khung.

Các đặc điểm kỹ thuật Zigbee định nghĩa bảo mật cho lớp MAC, NWK và APS. Bảo mật cho các ứng dụng thường cung cấp thông qua những ứng dụng sơ lược.

Dịch vụ bảo mật giữa các lớp mạng

- Khi khung tin tầng MAC cần được bảo mật, thì ZigBee sử dụng dịch vụ bảo mật của tầng MAC để bảo vệ các khung lệnh MAC, các thông tin báo hiệu beacon, và các khung tin xác nhận ACK. Đối với các bản tin chỉ phải chuyển qua một bước nhảy đơn, tức là truyền trực tiếp từ nốt mạng này đến nốt mạng lân cận của nó, thì ZigBee chỉ cần sử dụng khung tin bảo mật MAC để mã hóa bảo vệ thông tin. Nhưng đối với các bản tin phải chuyển gián tiếp qua nhiều nốt mạng mới tới được đích thì nó cần phải nhờ vào tầng mạng để làm công việc bảo mật này. Tầng điều khiển dữ liệu MAC sử dụng thuật tóan AES (chuẩn mã hóa cao cấp). Nói chung thì tầng MAC là một quá trình mã hóa, nhưng công việc thiết lập các khóa key, chỉ ra mức độ bảo mật, và điều khiển quá trình mã hóa thì lại thuộc về các tầng trên. Khi tầng MAC phát hoặc nhận một khung tin nào đó được bảo mật, đầu tiên nó sẽ kiểm tra địa chỉ đích hoặc nguồn của khung tin đó, tìm ra cái khóa kết hợp với địa chỉ đích hoặc địa chỉ nguồn, sau đó sử dụng cái khóa này để xử lý khung tin theo qui trình bảo mật mà cái khóa đó qui định. Mỗi khóa key được kết hợp với một qui trình bảo mật đơn lẻ. Ở đầu mỗi khung tin của MAC luôn có 1 bit để chỉ rõ khung tin này có được bảo mật hay không. Khi phát một khung tin, mà khung tin này yêu cầu cần được bảo toàn nguyên vẹn. Khi đó phần đầu khung và phần tải trọng khung MAC sẽ tính tóan cân nhắc để tạo ra một trường mã hóa tin nguyên vẹn (MIC- Message Integrity) phù hợp, MIC gồm khoảng 4,8 hoặc 16 octets. MIC sẽ được gán thêm vào bên phải phần tải trọng của MAC. Khi khung tin phát đi đòi hỏi phải có độ tin cậy cao, thì biện pháp được sử dụng để mã hóa thông tin là số chuỗi và số khung sẽ được gán thêm vào bên trái phần tải trọng khung tin MAC. Trong khi nhận gói tin, nếu phát hiện thấy MIC thì lập tức nó sẽ kiểm tra xem khung tin nào bị mã hóa để giải mã. Cứ mỗi khi có một bản tin gửi đi thì thiết bị phát sẽ tăng số đếm khung lên và thiết bị nhận sẽ theo dõi căn cứ vào số này. Nhờ vậy nếu như có một bản tin nào có số đếm khung tin đã bị nhận dạng một lần thì thiết bị nhận sẽ bật cờ báo lỗi bảo mật.
- Tầng mạng cũng sử dụng chuẩn mã hóa AES. Tuy nhiên khác với tầng điều khiển dữ liệu MAC, bộ mã hóa của tầng mạng làm việc dựa trên trạng thái CCM* của hệ thống. Trạng thái này thực chất là sự cải biên từ CCM của tầng MAC, nó thêm vào chuẩn mã hóa này các chức năng là chỉ mã hóa tính tin cậy và chỉ mã hóa tính nguyên vẹn. Sử dụng CCM* giúp làm đơn giản hóa quá trình mã hóa dữ liệu của tầng mạng, các chuỗi mã

hóa này có thể dùng lại khóa key của chuỗi mã hóa khác. Như vậy thì khóa key này không hoàn toàn còn là ranh giới của các chuỗi mã hóa nữa. Khi tầng mạng phát hoặc nhận một gói tin được mã hóa theo qui ước bởi nhà cung cấp dịch vụ, nó sẽ kiểm tra địa chỉ nguồn hoặc đích của khung tin để tìm ra khóa key liên quan tới địa chỉ đó, sau đó sẽ áp dụng bộ mã hóa này giải mã hoặc mã hóa cho khung tin. Tương tự như quá trình mã hóa tầng MAC, việc điều khiển quá trình mã hóa này được thực hiện bởi các tầng cao hơn, các số đếm khung và MIC cũng được thêm vào để mã hóa khung tin.

- Tầng ứng dụng: Nó chịu trách nhiệm tuyên truyền trên mạng của những thay đổi trong các thiết bị bên trong nó, có thể bắt nguồn từ các thiết bị (ví dụ, một sự thay đổi trạng thái đơn giản) hoặc trong bộ quản lý tin tưởng (có thể thông báo cho các mạng chắc chắn một thiết bị nào đó đã được loại bỏ từ nó). Nó cũng có các tuyến đường định tuyến yêu cầu từ các thiết bị đến trung tâm Trust và sự khôi phục network key từ trung tâm Trust cho tất cả các thiết bị. Bên cạnh đó, ZDO việc duy trì các chính sách bảo mật của thiết bị.

6.1Trust Center:

- Trung tâm Trust quyết định cho phép hoặc không cho phép các thiết bị mới vào mạng lưới hoạt động của mình.
- Trung tâm Trust có thể cập nhật định kỳ và chuyển sang một hệ thống mạng khóa mới. Đầu tiên phát mã khóa mới được mã hóa với mạng khóa cũ. Sau đó, nó sẽ truyền lệnh cho tất cả các thiết bị để chuyển sang khóa mới.
- Trung tâm Trust thường là điều phối viên mạng lưới, nhưng nó còn có thể là một thiết bị chuyên dụng. Đó là nó chịu trách nhiệm vai trò bảo mật sau:

- Trust manager: để xác thực các thiết bị có yêu cầu tham gia vào mạng
- Network manager: để duy trì và phân phối các hệ thống khóa.
- Configuration manager: cho phép end-to-end giữa các thiết bị an ninh.

6.2 Khóa bảo vệ:

6.2.1 Khóa đối xứng:

An ninh Zigbee dựa trên nền tảng khóa đối xứng. Cả hai đầu khởi tạo và đầu nhận của một giao dịch bảo vệ cần phải chia sẻ cùng khóa, khóa đó là sử dụng trực tiếp trong bảo mật chuyển đổi thông tin. Thực tế người ta dùng ba phương pháp sau:

- Cài đặt sẵn: là nơi mà các khóa được đặt vào thiết bị sử dụng và sử dụng phương pháp out-of-band. Ví dụ: các thanh công cụ lệnh.

- Vận chuyển: là nơi mà các trung tâm Trust gửi khóa(một cách an toàn nều có thể) đến các thiết bị.
- Khởi tạo: là nơi mà thiết bị thương lượng với trung tâm Trust và các khóa được khởi tạo từ hai đầu mà không bị vận chuyển.

- SKKE(khởi tạo khóa đối xứng)
- CBKE(chứng thực sự khởi tạo khóa đối xứng)
- ASKE(mã an toàn của khóa khởi tạo)

6.2.2 Khóa bảo mật:

Zigbee sử dụng ba loại khóa chính để quản lý an ninh: Master, network , link key

- *Master keys :*
  Là những khóa tùy chọn không được sử dụng để mã hóa khung hình. Thay vào đó, chúng được sử dụng như một bí mật chia sẻ ban đầu giữa hai thiết bị khi chúng thực hiện các thủ tục khóa cơ sở (SKKE) để tạo ra các khóa liên kết.
  Khóa có nguồn gốc từ trung tâm Trust được gọi là trung tâm Trust Master khóa, trong khi tất cả các khóa khác được gọi là lớp ứng dụng Master khóa.
- *Network keys:*
  Những khóa này chỉ thực hiện an ninh lớp bảo mật trên một mạng Zigbee. Tất cả các thiết bị trên một mạng Zigbee chỉa sẻ cùng một khóa.
  Chế độ Bảo mật cao mạng khóa luôn luôn phải được gửi mật mã qua không khí, trong khi các tiêu chuẩn an ninh khóa mạng có thể được gửi hoặc được mã hóa hay không mã hóa. Lưu ý rằng chế độ bảo mật cao chỉ được hỗ trợ cho Zigbee PRO.
- *Link keys:*
  Những khóa tùy chọn an toàn thông điệp giữa hai thiết bị lớp ứng dụng.
  Những khóa có nguồn gốc từ trung tâm Trust được gọi là Trung tâm liên kết khóa Trust, trong khi tất cả các khóa khác gọi là ứng dụng lớp liên kết khóa.

6.3.Chế độ bảo vệ:

6.3.1 Chế độ bảo mật tiêu chuẩn:

Trong chế độ bảo mật tiêu chuẩn, danh sách các thiết bị, các khóa master, các khóa liên kết và các khóa hệ thống có thể được duy trì bởi cả hai trung tâm Trust hoặc bằng các thiết bị riêng của chúng. Trung tâm Trust vẫn còn trách nhiệm duy trì một tiêu chuẩn khóa mạng và nó kiểm

soát các phương thức nạp mạng. Trong chế độ này, các yêu cầu bộ nhớ cho các trung tâm Trust là ít hơn so với nó dùng cho chế độ bảo mật cao.

6.3.2 Chế độ bảo mật cao*:*

Trong chế độ này, trung tâm Trust duy trì một danh sách các thiết bị, các khóa master, các khóa liên kết và các khóa mạng mà nó cần để kiểm soát và thực thi các phương thức của bản cập nhật mạng khóa chính và mạng thu nạp. Vì số lượng thiết bị trong mạng lưới tăng lên, vì vậy nó cũng yêu cầu bộ nhớ cho trung tâm Trust.
Các khả năng bảo mật bổ sung vốn có trong Zigbee PRO rất quan trọng để hoàn thiện khả năng bảo mật của Zigbee được sử dụng rộng rãi trong kiểm soát cơ sở hạ tầng- thương mại, xây dựng, lưới điện, hoặc một hệ thống an ninh trong gia đình không được tổn hại.

7. Hướng phát triển:

7.1 Các phiên bản của Zigbee:

- Zigbee 2004(1.0): phiên bản gốc. Bây giờ ít nhiều đã lỗi thời và không có khả năng tương thích ngược với nhưng chuẩn Zigbee mới trên thị trường
- Zigbee 2006: có tính tương thích ngược với Zigbee 2007
- Zigbee 2007/ Zigbee Pro: cung cấp nhiều tính năng, nhiều định tuyến, nhiều phương thức truy cập và sự bảo mật cao với SKKE. Zigbee 2007 hoàn toàn có tính tương thích ngược với các thiết bị Zigbee 2006.
- Zigbee RF4CE (Radio Frequence four Consumer Electronics): dùng điều khiển từ xa âm thanh, hình ảnh và nhưng đồ điện tử thông dụng trong cuộc sống hàng ngày của con người. Nó có rất nhiều lợi thế trong điều khiển từ xa và bao gồm cả giao tiếp phong phú hơn, độ ổn định, tính năng, tính linh hoạt và khả năng tương tác cao hơn.

7.2 .Hướng phát triển Zigbee trong tương lai:

Zigbee có thể áp dụng cho tất cả các hệ thống điều khiển và cảm biến với các ưu điểm vượt trội: giá thành thấp, tiêu hao ít năng lượng, ít lỗi, dễ mở rộng, khả năng tương thích cao, Zigbee thiết lập cơ sở cho những tầng cao hơn trong giao thức (từ tầng mạng đến tầng ứng dụng) về bảo mật, dữ liệu, chuẩn phát triển để đảm bảo chắc chắn rằng các khách hàng dù mua sản phẩm từ các hãng sản xuất khác nhưng vẫn theo một chuẩn riêng để làm việc cùng nhau được mà không tương tác lẫn nhau.

Tức là trong tương lai, các sản phẩm của Zigbee sẽ được sản xuất tương thích được với chuẩn 802.15 hoặc rộng hơn có thể là 802.

TÀI LIỆU THAM KHẢO

1. *en.wikipedia.org/.../**ZigBee***
2. www.**zigbee**.org/
3. *www.wisegeek.com/what-is-**zigbee**.htm*